04-05-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this paper and the documents and/or fees referred to as attached therein are being deposited with the United States Postal Service on April 3, 2002 in an envelope as "Express Mail Post Office to Addressee" service under 37 CFR §1.10, Mailing Label Number **EL937779717US**, addressed to the Commissioner for Patents, Washington, DC 20231.

Snoriega
Sunshine Noriega

Attorney Docket No.: IGT1P034X1/P-277CIP

First Named Inventor: Nguyen

UTILITY PATENT APPLICATION TRANSMITTAL (37 CFR. § 1.53(b))

(Continuation, Divisional or Continuation-in-part application)

Commissioner for Patents
Box Patent Application
Washington, DC 20231

Sir: This is a request for filing a patent application under 37 CFR. § 1.53(b) in the name of inventors:
Binh Nguyen, Michael M. Oberberger, and Gregory Hopkins Parrott

For: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Assigned to : IGT

This application is a □ Continuation □ Divisional ☒ Continuation-in-part

of prior Application No.: 09/732,650, filed on December 7, 2000, from which priority under 35 U.S.C. §120 is claimed.

Application Elements:

☒ **71** Pages of Specification, Claims and Abstract

☒ **16** Sheets of formal Drawings

☒ Declaration

☒ Newly executed

□ Copy from a prior application (37 CFR 1.63(d) for a continuation or divisional). The entire disclosure of the prior application from which a copy of the declaration is herein supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

□ Deletion of inventors Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

Accompanying Application Parts:

□ Do not publish this application. Nonpublication Request is attached.

☒ Assignment and Assignment Recordation Cover Sheet (recording fee of $40.00 enclosed)

□ Power of Attorney
□ 37 CFR 3.73(b) Statement by Assignee
☒ Information Disclosure Statement with Form PTO-1449 ☒ Copies of IDS Citations
□ Preliminary Amendment (*New claims numbered after highest original claim in prior application.*)
☒ Return Receipt Postcard
□ Other:

Claim For Foreign Priority

□ Priority of Application No. filed on
is claimed under 35 U.S.C. § 119.
□ The certified copy has been filed in prior application U.S. Application No.
□ The certified copy will follow.

Extension of Time for Prior Pending Application

□ A Petition for Extension of Time is being concurrently filed in the prior pending application. A copy of the Petition for Extension of Time is attached.

Amendments

□ Amend the specification by inserting before the first line the sentence: "This is a
□ Continuation □ Continuation-in-part □ Divisional
application of co-pending prior
□ Application No. filed on ,
□ International Application filed on which designated the United States,
the disclosure of which is incorporated herein by reference."

□ Cancel in this application original claims of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

□ Applicant is entitled to Small Entity Status under 37 C.F.R. §1.27.

	(Col. 1) Total Claims		(Col. 2) Claims	(Col. 3) Present Extra	Rate	Additional Fee
TOTAL	129	MINUS	20	= 109	x 18	$1,962.00
INDEP.	7	MINUS	3	= 4	x 84	$336.00
[ ] First presentation of multiple dependent claim					$280	0
Basic Filing Fee under 37 C.F.R. §1.16(a)					$740	740.00
TOTAL						$3,038.00
SMALL ENTITY 50% FILING FEE REDUCTION (if applicable)						0

☒ Check No. 5421 in the amount of $3,078.00 is enclosed.

☒ The Commissioner is authorized to charge any fees beyond the amount enclosed which may be required, or to credit any overpayment, to Deposit Account No. 500388 (Order No. IGT1P034X1).

General Authorization for Petition for Extension of Time (37 CFR §1.136)

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as may be needed for any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as may be needed to Deposit Account No. 500388 (Order No. IGT1P034X1).

☒ Please send correspondence to the following address:

Customer Number 022434

22434
PATENT TRADEMARK OFFICE

Date: 4/3/02

David Olynick
David P. Olynick
Registration No. 48,615

04-05-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this paper and the documents and/or fees referred to as attached therein are being deposited with the United States Postal Service on April 3, 2002 in an envelope as "Express Mail Post Office to Addressee" service under 37 CFR §1.10, Mailing Label Number **EL937779717US**, addressed to the Commissioner for Patents, Washington, DC 20231.

SNoriega
Sunshine Noriega

Attorney Docket No.: IGT1P034X1/P-277CIP

First Named Inventor: Nguyen

UTILITY PATENT APPLICATION TRANSMITTAL (37 CFR. § 1.53(b))

(Continuation, Divisional or Continuation-in-part application)

Commissioner for Patents
Box Patent Application
Washington, DC 20231

Sir: This is a request for filing a patent application under 37 CFR. § 1.53(b) in the name of inventors: **Binh Nguyen, Michael M. Oberberger, and Gregory Hopkins Parrott**

For: **SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT**

Assigned to : IGT

This application is a □ Continuation □ Divisional ☒ Continuation-in-part of prior Application No.: 09/732,650, filed on December 7, 2000, from which priority under 35 U.S.C. §120 is claimed.

Application Elements:

☒ **71** Pages of Specification, Claims and Abstract

☒ **16** Sheets of formal Drawings

☒ Declaration

☒ Newly executed

□ Copy from a prior application (37 CFR 1.63(d) for a continuation or divisional). The entire disclosure of the prior application from which a copy of the declaration is herein supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

□ Deletion of inventors Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

Accompanying Application Parts:

□ Do not publish this application. Nonpublication Request is attached.

☒ Assignment and Assignment Recordation Cover Sheet (recording fee of $40.00 enclosed)

☐ Power of Attorney

☐ 37 CFR 3.73(b) Statement by Assignee

☒ Information Disclosure Statement with Form PTO-1449 ☒ Copies of IDS Citations

☐ Preliminary Amendment (*New claims numbered after highest original claim in prior application.*)

☒ Return Receipt Postcard

☐ Other:

Claim For Foreign Priority

☐ Priority of Application No. filed on is claimed under 35 U.S.C. § 119.

☐ The certified copy has been filed in prior application U.S. Application No.

☐ The certified copy will follow.

Extension of Time for Prior Pending Application

☐ A Petition for Extension of Time is being concurrently filed in the prior pending application. A copy of the Petition for Extension of Time is attached.

Amendments

☐ Amend the specification by inserting before the first line the sentence: "This is a

☐ Continuation ☐ Continuation-in-part ☐ Divisional

application of co-pending prior

☐ Application No. filed on ,

☐ International Application filed on which designated the United States,

the disclosure of which is incorporated herein by reference."

☐ Cancel in this application original claims of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

□ Applicant is entitled to Small Entity Status under 37 C.F.R. §1.27.

	(Col. 1) Total Claims		(Col. 2) Claims	(Col. 3) Present Extra	Rate	Additional Fee
TOTAL	129	MINUS	20	= 109	x 18	$1,962.00
INDEP.	7	MINUS	3	= 4	x 84	$336.00
[ ] First presentation of multiple dependent claim					$280	0
Basic Filing Fee under 37 C.F.R. §1.16(a)					$740	740.00
TOTAL						$3,038.00
SMALL ENTITY 50% FILING FEE REDUCTION (if applicable)						0

☒ Check No. 5421 in the amount of $3,078.00 is enclosed.

☒ The Commissioner is authorized to charge any fees beyond the amount enclosed which may be required, or to credit any overpayment, to Deposit Account No. 500388 (Order No. IGT1P034X1).

General Authorization for Petition for Extension of Time (37 CFR §1.136)

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as may be needed for any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as may be needed to Deposit Account No. 500388 (Order No. IGT1P034X1).

☒ Please send correspondence to the following address:

Customer Number 022434

22434
PATENT TRADEMARK OFFICE

Date: 4/3/02

David P. Olynick
Registration No. 48,615

Attorney Docket No. IGT1P034X1/P-277CIP

PATENT APPLICATION

SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Inventors:
Binh T. Nguyen
1445 Taos Court
Reno, NV 89511
U.S. Citizen

Michael M. Oberberger
4591 Lynnfield Court
Reno, Nevada 89509
U.S. Citizen

Greg Parrott
4955 Foxcreek Trail
Reno, Nevada 89509
U.S. Citizen

Assignee: IGT

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
Telephone (510) 843-6200

SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of US Patent Application No. 09/732,650 entitled "SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT ", filed December 7, 2000, naming Binh Nguyen as inventor, which is incorporated herein by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

This invention relates to game playing services for gaming machines such as slot machines and video poker machines. More particularly, the present invention relates to providing methods of communication for game services such as licensing and accounting on gaming machines.

There are a wide variety of associated devices that can be connected to a gaming machine such as a slot machine or video poker machine. Some examples of these devices are lights, ticket printers, card readers, speakers, bill validators, ticket readers, coin acceptors, display panels, key pads, coin hoppers and button pads. Many of these devices are built into the gaming machine or components associated with the gaming machine such as a top box which usually sits on top of the gaming machine.

Typically, utilizing a master gaming controller, the gaming machine controls various combinations of devices that allow a player to play a game on the gaming machine and also encourage game play on the gaming machine. For example, a game played on a gaming machine usually requires a player to input money or indicia of credit into the gaming machine, indicate a wager amount, and initiate a game play. These steps require the gaming machine to control input devices, such as bill validators and coin acceptors, to accept money into the gaming machine and recognize user inputs from devices, including key pads and button pads, to determine the wager amount and initiate game play. After game play has been initiated, the gaming machine determines a game outcome, presents the game outcome to the player and may dispense an award of some type depending on the outcome of the game.

The operations described above may be carried out on the gaming machine when the gaming machine is operating as a " stand alone" unit or linked in a network of some type to a group of gaming machines. As technology in the gaming industry progresses, more and more gaming services are being provided to gaming machines via communication networks that link groups of gaming machines to a remote computer that provides one or more gaming services. As an example, gaming services that may be provided by a remote computer to a gaming machine via a communication network of some type include player tracking, accounting, cashless award ticketing, lottery, progressive games and bonus games.

Typically, network gaming services enhance the game playing capabilities of the gaming machine or provide some operational advantage in regards to maintaining the gaming machine. Thus, network gaming services provided to groups of gaming machines linked over a dedicated communication network of some type have become very popular in the gaming industry. In general, the dedicated communication network is not accessible to the public. To justify the costs associated with the infrastructure needed to provide network gaming services on a dedicated communication network, a certain critical number of gaming machines linked in a network of some type must utilize the service. Thus, many of the network gaming services are only provided at larger gaming establishments where a large number of gaming machines are deployed.

A progressive game network offering progressive game services is one example where a group of gaming machines are linked together using a dedicated network to provide a network gaming service. The progressive game services enabled by the progressive game network increase the game playing capabilities of a particular gaming machine by enabling a larger jackpot than would be possible if the gaming machine was operating in a "stand alone" mode. The potential size of the jackpot increases as the number gaming machines connected in the progressive network is increased. The size of the jackpot tends to increase game play on gaming machines offering a progressive jackpot which justifies the costs associated with installing and maintaining the dedicated progressive game network.

Within the gaming industry, a particular gaming entity may desire to provide network gaming services and track the performance of all the gaming machines under the control of the entity. The gaming machines under the control of a particular entity may be globally distributed in many different types of establishments. Casinos, convenience stores, supermarkets, bars and boats are a few examples of establishments where gaming machines may be placed.

Figure 1 is a block diagram depicting gaming machines distributed in different establishments partially connected by a dedicated communication network for a typical gaming entity currently operating in the gaming industry. In FIG. 1, the gaming entity utilizes a central office 142. The gaming machines, 102, 104, 106, 114, 116, 136 and 138 for the gaming entity are located in two casinos, 110 and 122, and a store 140. A gaming entity may operate hundreds, thousands or ten of thousands of gaming machines. Since gaming is allowed in many locations throughout the world, the two casinos, 110 and 122, the central office 142 and the store may be distributed over a wide geographic area. For instance, the casino 110 may be located in Atlantic City, New Jersey, the casino 122 may be located in Australia, the central office may be located in Las Vegas, Nevada and the store may be located in Reno, Nevada.

Within the casinos, the gaming machines may be connected to one or more database servers via one or more dedicated networks. The database servers are usually located in the backroom of the casino. For instance, in casino 110, gaming machines 102, 104 and 106 are connected to a database server 100 via a dedicated network 108. The dedicated network 108 may be used to send accounting information and player tracking information from the gaming machines to the database server 110. In casino 122, the gaming machines 114, 116, 118 may send accounting information and player tracking information to a database server using the dedicated network 120. Other dedicated networks (not shown) in casinos, 110 and 112, may provide such network gaming services as bonus game play, progressive game play and cashless ticketing.

In casinos 110 and 122, the database servers 100 and 112 may store and process accounting data from the gaming machines in communication with the database servers. For instance, an accounting report detailing the performance of individual and groups of gaming machines may be generated from the data stored on the database servers 100 and 112. In addition, accounting data or reports may be sent to the database server 124 in the central office 142 from each casino. These reports may contain game performance data collected from a number of gaming machines as well as hotel operations data. The data from the casinos may be sent to the central office using an expensive dedicated leased line 132 using a frame relay network.

The database server 124 may be used to generate reports summarizing the performance of all the gaming machines within the gaming entity (e.g. casino 110, casino 122 and store 140). The reports may be accessed locally using the local access points 126 and 128 via the local network. In addition, reports may be remotely accessed using a dial in number for a limited number of users. For instance, an executive travelling on the road might view gaming machine performance data from the remote access point 134 where the remote access point 134 may be a hotel room.

For the store 140, the gaming machines, 136 and 138 may be leased by the store operator. However, the cost of a dedicated communication network for a small number of gaming machines is usually not justified. Thus, the gaming machines operate in a "stand alone" mode. While operating in "stand alone" mode, network gaming services are not available to these gaming machines. To obtain performance data for the gaming machines, 136 and 138, a route operator may regularly extract performance data from the machines and manually transmit the information to the central office 142. A route may consist of a number gaming machines located in various locations such as bars, convenience stores and supermarkets. Usually, the route operator manually extracts performance data for all of the gaming machines located on their route. For a large route, this process may be both time consuming and costly.

Within the gaming industry, there is some desire to provide centralized network gaming services, centralized data access and centralized data acquisition to all of the gaming machines or a larger proportion of gaming machines within a gaming entity. For the casinos, 110 and 122, the gaming machines are connected via local dedicated networks that do not generally allow, for security reasons, the gaming machines to communicate with devices located outside of the casino. For instance, in FIG. 1, the database server 124 may not directly communicate with gaming machine 102 or gaming machine 114. Further, as described above, a dedicated network is usually not cost effective for smaller gaming establishments. Thus, with the communication infrastructure described in FIG. 1 which is representative of the communication infrastructure currently available in the gaming industry, the implementation of centralized network gaming services, such as centralized data acquisition may be difficult.

A current barrier to providing centralized network gaming services and centralized data acquisition for gaming machines diversely distributed throughout a gaming entity is the complexity and costs of the dedicated communication networks currently used in the gaming industry. The costs of installing and maintaining a dedicated communication network typically limit the application of dedicated networks to large establishments with a large number of gaming machines. Further, even in the larger establishments, the dedicated network are usually only implemented locally and centralized network gaming services (e.g. from a central office) are usually not provided. In view of the above, it would be desirable to provide gaming communication methods for gaming machines that reduce the complexity of the gaming network environment, reduce the costs associated with adding new network gaming services and simplify the data acquisition process for gaming machines widely distributed within a gaming entity.

Another desire within the gaming industry is to electronically download gaming software from one or more remote locations to a gaming machine. The capability to electronically download gaming software is desirable because it may enable gaming machines to be quickly reconfigured to account for changes in popularity of various games played on the gaming machines and it may simplify software maintenance issues on the gaming machine such as gaming software updates. Currently, in a time consuming process, gaming software is manually loaded onto each gaming machine by a technician. The software is manually loaded because the gaming software is usually very highly regulated and in most gaming jurisdictions only approved gaming software may be installed on a gaming machine. Further, the gaming software is manually loaded for security reasons to prevent the source code from being obtained by individuals which might use the source code to try to find ways of cheating the gaming machine. In view of the above, it would be desirable to provide gaming software downloading methods for gaming machines that allow gaming software to be transferred electronically to the gaming machines from a remote location in a secure manner that satisfies regulatory requirements of the gaming jurisdiction where the gaming machine is located.

SUMMARY OF THE INVENTION

This invention addresses the needs indicated above by providing gaming machines that may securely communicate with devices over a public network such as the Internet. The invention provides a combination of symmetric and asymmetric encryption that allows a single gaming machine to securely communicate with a remote server using a public network. The secure communication methods may be used to transfer gaming software and gaming information between two gaming devices such as between a gaming machine and a game server. For regulatory and tracking purposes, the transfer of gaming software between the two gaming devices may be authorized and monitored by a software authorization agent.

One aspect of the present invention describes a software authorization agent capable of generating a gaming software transaction record used to facilitate a transfer of gaming software between two gaming devices. The method may be generally characterized as comprising: 1) receiving a gaming software transaction request from a first gaming device; 2) authenticating an identity of the first gaming device 3) generating a gaming software transaction record comprising gaming software transaction information that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, the gaming software may comprise one or more gaming software components. The gaming software may be used to upgrade a gaming software component on the gaming machine or may be used to correct an error in a gaming software component on the gaming machine. The game of chance may be a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game. The gaming transaction information may be one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number, a gaming software identification number, a gaming software provider identifier, a transaction number, a number of allowable downloads and combinations thereof.

The first gaming device may be at least one of a gaming machine, game server and combinations thereof. The transfer of gaming software may be performed at least one of manually and electronically. The software authorization agent may communicate with the first gaming device using an local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. Further, the software authorization agent and the first gaming device may communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

In other embodiments, the gaming software transaction request comprises access information and gaming software identification information. The access information may be one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device. The gaming software identification information may be one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

In additional embodiments, the method may comprise one or more of the following: a) comparing access information in the gaming software transaction request with access information stored in a database and when the compared access information does not match the access information stored in the database, denying the gaming software transaction request b) comparing gaming software identification information in the gaming software transaction request with gaming software identification information stored in a database and when the gaming software identification information does not match the access information stored in the database, denying the gaming software transaction request, c) generating an identification sequence; encrypting the identification sequence with a public encryption key for the first gaming device wherein information encrypted with the public encryption key is decrypted with a private encryption key used by the first gaming device; sending the encrypted identification sequence to the first gaming device where the identification sequence may a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device, d) receiving from the first gaming device a second identification sequence encrypted with a public encryption key used by the software authorization agent, decrypting the second identification sequence with a private encryption key corresponding to the public encryption key used by the software authorization agent; and comparing the second identification sequence to the identification sequence sent to the first gaming device to authenticate the identity of the first gaming device where the second identification sequence is a symmetric encryption key used to transfer gaming software between the first gaming device and the second gaming device, e) when the second identification sequence received from the first gaming device does not match the identification sequence sent to the first gaming device; denying the gaming software transaction request.

In yet other embodiments, the method may further comprise one or more of the following: i) storing the gaming transaction record information to a transaction database, ii) sending gaming software transaction information to the first gaming device where the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof, iii) sending a notification message to a gaming software provider identified in the gaming software request of a pending gaming software download request and iv) requesting a list of gaming software installed on a gaming device.

Another aspect of the present invention provides a method in a software authorization agent of regulating a transfer of gaming software between two gaming devices. The method may be generally characterized as comprising: 1) receiving a gaming software download request message with gaming software transaction information from a first gaming device; 2) validating the gaming software download request using the gaming software transaction information; 3) sending an authorization message to the first gaming device authorizing the first gaming device to transfer gaming software to a second gaming device; where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine. The game of chance may be a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game. The gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and combinations thereof.

In particular embodiments, the second gaming device may be at least one of a game server and a gaming machine. Further, the first gaming device may be a game server in communication with one or more gaming machines and the second gaming device may be a gaming machine. Also, the first gaming device may be a game server maintained by a gaming software provider and the second gaming device may be a game server in communication with one or more gaming machines. In addition, the first gaming device may be a game server maintained by a gaming software provider and the second gaming device may be a gaming machine. The software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. The software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

The method may also comprise one or more of the following: a) comparing the gaming transaction information in the gaming software download request message with gaming transaction information stored in a transaction database to validate the gaming software download, b) sending a message to the first gaming device denying authorization for the first gaming device to transfer gaming software to the second gaming device, c) decrypting the download request message, d) receiving a first download acknowledgement message from the first gaming device and receiving a second download acknowledgement message from the second gaming device, e) comparing gaming software transaction information in the first download acknowledgement message with gaming software transaction information in the second download acknowledgement message to validate that the gaming software has been correctly transferred where the gaming software transaction information in the first download acknowledgement message includes at least a first digital signature determined for the gaming software and the gaming software transaction information in the second download acknowledgement message includes at least a second digital signature determined for the gaming software, f) receiving the gaming software from the first gaming device; validating the gaming software; and sending the gaming software to the second gaming device, g) determining a digital signature for the gaming software; and comparing the digital signature with an approved digital signature for the gaming software stored in a database to validate the gaming software, h) storing gaming software transaction information indicating that a status of the download request where the status is at least one of authorized, pending, completed and void and i) requesting a list of gaming software installed on a gaming device.

Another aspect of the present invention provides a method in a software authorization agent of distributing gaming software transaction information. The method may be generally characterized as comprising: 1) receiving a gaming software transaction information request from a gaming device; 2) authenticating an identity of the gaming device; 3) querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device where the gaming software transaction database comprises a plurality of records of gaming software transactions; and 4) sending the requested gaming software transaction information to the gaming device where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, each gaming software transaction record may includes gaming software transaction information that describes a transfer of gaming software from a first gaming device to a second gaming device. For instance, the gaming transaction information may be one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time. The gaming software transaction database may also include a record of gaming software installed on one or more gaming devices.

The method may also comprise one or more of: a) generating a gaming transaction report that presents the set of gaming software transaction requested by the gaming device, b) generating a distribution of gaming software on a plurality of gaming machines at a specified time using the gaming software transaction information stored in the gaming software transaction database, c) generating a distribution of gaming software on a plurality of gaming machines for a plurality of times using the gaming software transaction information stored in the gaming software transaction database, d) generating a billing report and requesting a list of gaming software installed on the gaming device and e) storing the list of gaming software installed on the gaming device to the gaming software transaction database.

Another aspect of the present invention provides a method in a first gaming device of requesting a transfer of gaming software from a second gaming device. The method may be generally characterized as comprising: 1) generating a gaming software transaction request; 2) sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and 3) receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, the first gaming device may be a gaming machine and the second gaming device may be a game server. Also, the first gaming device may be a game server in communication with a plurality of gaming machines and the second gaming device may be a game server maintained by a gaming software content provider. The software authorization agent, the first gaming device and the second gaming device may communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. Further, the software authorization agent, the first gaming device and the second gaming device may communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

In other embodiments, the transfer of gaming software may be performed at least one of manually and electronically. The gaming software may comprise one or more gaming software components. The gaming software may be used to upgrade a gaming software component on the gaming machine or may be used to correct an error in a gaming software component on the gaming machine.

The gaming software transaction information in the method may be one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof. The gaming software transaction request may comprise access information and gaming software identification information. The access information may be one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device. The gaming software identification information may be one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

The method may also comprise one or more of the following: a) sending authentication information used to identify the first gaming device to the gaming software authorization agent, b) sending a message requesting the gaming software to the second gaming device, c) receiving the gaming software from the second gaming device, d) determining a digital signature for the gaming software and sending a message with at least the digital signature to the gaming software authorization agent and e) authenticating an identity of the second gaming device.

Another aspect of the present invention provides a method in a first gaming device of transferring gaming software to a second gaming device. The method may be characterized as comprising: 1) receiving a gaming software transaction request; 2) sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software; and 3) transferring the gaming software to the second gaming device; where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, the method may also comprise one or more of the following: i) receiving an approval of the gaming software transaction request from the gaming software authorization agent, ii) prior to transferring the gaming software, receiving a denial of the gaming software transaction request from the gaming software authorization agent; and terminating the transfer of the gaming software and iii) determining a digital signature for the gaming software and sending a message with at least the digital signature to the gaming software authorization agent.

In other embodiments, the first gaming device may be a gaming server and the second gaming device may be a gaming machine. Also, the first gaming device may be a gaming machine and the second gaming device may be a gaming machine. In addition, the first gaming device may be a game server maintained by a gaming software content provider and the second gaming device may be a game server maintained by a gaming entity. Further, the first gaming device may be a game server maintained by a gaming software content provider and the second gaming device may be a gaming machine maintained by a gaming entity. The software authorization agent, the first gaming device and the second gaming device may communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. The software authorization agent, the first gaming device and the second gaming device may be communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

Another aspect of the present invention provides a software authorization agent for facilitating the transfer of gaming software between a plurality of gaming devices. The software authorization agent may be generally characterized as comprising: 1) a network interface allowing the authorization agent to communicate with each of the plurality of gaming devices; and 2) a processor configured or designed to (i) receive gaming software transfer requests via the network interface from a first gaming device for the transfer of gaming software from a second gaming device to a third gaming device (ii) approve or reject the gaming software transaction request wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine. The game of chance may be a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

In particular embodiments, the software authorization agent may further comprise one or more of the following: a) a transaction database containing gaming software transaction information where the gaming software transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time, b) a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software distribution reports based upon the gaming software transaction information, c) a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software billing reports based upon the gaming software transaction information, d) a database storing public encryption keys for one or more of the plurality of gaming devices, e) a database storing identification information for one or more of the plurality of gaming devices and f) a database storing identification information for the gaming software that is transferred from the second gaming device to the third gaming device where the identification information for the gaming software is a digital signature, a title, a manufacturer, an identification number and combinations thereof.

In other embodiments, the first gaming device may be a hand-held computing device, the second gaming device may be a portable memory device storing the gaming software and the third gaming device may be a gaming machine. Also, the first gaming device may be a first gaming machine, the second gaming device may be a second gaming machine and the third gaming device may be the first gaming machine. In addition, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be a first gaming machine. Further, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be the first game server

Another aspect of the present invention may provide a first gaming device. The first gaming device may be generally characterized as comprising: 1) a network interface allowing communications between the first gaming device, a software authorization agent and one or more other gaming devices; and 2) a processor configured or designed to (i) send a request for the transfer of gaming software from a second gaming device to a third gaming device via the network interface to the software authorization agent (ii) receive from the software authorization agent a reply approving or rejecting the request for the transfer of the gaming software where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine. The gaming software may comprise one or more gaming software components. The gaming software may be used to upgrade a gaming software component on one of the gaming devices and may be used to correct an error in a gaming software component on one of the gaming devices.

In particular embodiments, the first gaming device may further comprise one or more of the following: 1) a memory device that stores gaming software, 2) a master gaming controller that controls a game of chance played on the first gaming device where the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game and 3) a memory device that stores public encryption keys for one or more of the plurality of gaming devices and the software authorization agent. The network interface may be connected to at least one of a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof and the network interface may provide at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

In other embodiments, the first gaming device may be a portable gaming device. The first gaming device may be a first gaming machine, the second gaming device may be a second gaming machine and the third gaming device may be the first gaming machine. Alternatively, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be a first gaming machine. Further, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be the first game server.

Another aspect of the invention pertains to computer program products including a machine-readable medium on which is stored program instructions for implementing any of the methods described above. Any of the methods of this invention may be represented as program instructions and/or data structures, databases, etc. that can be provided on such computer readable media.

These and other features of the present invention will be presented in more detail in the following detailed description of the invention and the associated figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE **1** is a block diagram depicting gaming machines distributed in different establishments partially connected by a dedicated communication network for a typical gaming entity currently operating in the gaming industry.

FIGURE **2** is a perspective drawing of a gaming machine having a top box and other devices.

FIGURE **3** is a block diagram depicting gaming machines distributed in different establishments connected using a secure virtual network.

FIGURE **4** is an interaction diagram showing communications between a gaming machine, local server, local ISP and remote server over a public network.

FIGURE **5A** is a flow chart depicting a method of sending transaction data between a gaming machine and one or more remote servers.

FIGURE **5B** is a flow chart depicting a method of receiving transaction data between a gaming machine and one or more remote servers.

FIGURE **6** is a flow chart depicting a method of obtaining a game license on a gaming machine.

FIGURE **7** is a flow chart depicting a method of providing a game license to one or more gaming machines using a remote server.

FIGURE **8** is a block diagram of gaming software distribution network that uses a secure virtual network.

FIGURE **9** is a block diagram depicting software transactions in a gaming software distribution network controlled by a software authorization agent.

FIGURE **10** is an interaction diagram between a gaming software distributor, gaming software provider and a software authorization agent depicting an initialization of a gaming software transaction.

FIGURE **11** is an interaction diagram between a gaming software distributor, a gaming software provider and a software authorization agent depicting a gaming software transaction.

FIGURE **12** is an interaction diagram between a gaming software distributor, a gaming machine and a software authorization agent depicting a gaming software transaction.

FIGURE **13** is flow chart depicting a method in a software authorization agent initializing a gaming software transaction.

FIGURE **14** is flow chart depicting a method in a software authorization agent of authorizing a gaming software transaction.

FIGURE **15** is a block diagram of an interface used to provide information about gaming software transactions generated by a software authorization agent.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning first to FIGURE 2, a video gaming machine 2 of the present invention is shown. Machine 2 includes a main cabinet 4, which generally surrounds the machine interior (not shown) and is viewable by users. The main cabinet includes a main door 8 on the front of the machine, which opens to provide access to the interior of the machine. Attached to the main door are player-input switches or buttons 32, a coin acceptor 28, and a bill validator 30, a coin tray 38, and a belly glass 40. Viewable through the main door is a video display monitor 34 and an information panel 36. The display monitor 34 will typically be a cathode ray tube, high resolution flat-panel LCD, or other conventional electronically controlled video monitor. The information panel 36 may be a back-lit, silk screened glass panel with lettering to indicate general game information including, for example, a game denomination (e.g. $.25 or $1). The bill validator 30, player-input switches 32, video display monitor 34, and information panel are devices used to play a game on the game machine 2. The devices are controlled by circuitry (e.g. the master gaming controller) housed inside the main cabinet 4 of the machine 2. Many possible games, including mechanical slot games, video slot games, video poker, video black jack, video pachinko and lottery, may be provided with gaming machines of this invention.

The gaming machine 2 includes a top box 6, which sits on top of the main cabinet 4. The top box 6 houses a number of devices, which may be used to add features to a game being played on the gaming machine 2, including speakers 10, 12, 14, a ticket printer 18 which prints bar-coded tickets 20, a key pad 22 for entering player tracking information, a florescent display 16 for displaying player tracking information, a card reader 24 for entering a magnetic striped card containing player tracking information, and a video display screen 42. The ticket printer 18 may be used to print tickets for a cashless ticketing system. Further, the top box 6 may house different or additional devices than shown in the FIGs. 1. For example, the top box may contain a bonus wheel or a back-lit silk screened panel which may be used to add bonus features to the game being played on the gaming machine. As another example, the top box may contain a display for a progressive jackpot offered on the gaming machine. During a game, these devices are controlled and powered, in part, by circuitry (e.g. a master gaming controller) housed within the main cabinet 4 of the machine 2.

Understand that gaming machine 2 is but one example from a wide range of gaming machine designs on which the present invention may be implemented. For example, not all suitable gaming machines have top boxes or player tracking features. Further, some gaming machines have two or more game displays – mechanical and/or video. And, some gaming machines are designed for bar tables and have displays that face upwards. As another example, a game may be generated in on a host computer and may be displayed on a remote terminal or a remote gaming device. The remote gaming device may be connected to the host computer via a network of some type such as a local area network, a wide area network, an intranet or the Internet. The remote gaming device may be a portable gaming device such as but not limited to a cell phone, a personal digital assistant, and a wireless game player. Those of skill in the art will understand that the present invention, as described below, can be deployed on most any gaming machine now available or hereafter developed.

Returning to the example of Figure 1, when a user wishes to play the gaming machine 2, he or she inserts cash through the coin acceptor 28 or bill validator 30. Additionally, the bill validator may accept a printed ticket voucher which may be accepted by the bill validator 30 as an indicia of credit when a cashless ticketing system is used. At the start of the game, the player may enter playing tracking information using the card reader 24, the keypad 22, and the florescent display 16. Further, other game preferences of the player playing the game may be read from a card inserted into the card reader. During the game, the player views game information using the video display 34. Other game and prize information may also be displayed in the video display screen 42 located in the top box.

During the course of a game, a player may be required to make a number of decisions, which affect the outcome of the game. For example, a player may vary his or her wager on a particular game, select a prize for a particular game selected from a prize server, or make game decisions which affect the outcome of a particular game. The player may make these choices using the player-input switches 32, the video display screen 34 or using some other device which enables a player to input information into the gaming machine. In some embodiments, the player may be able to access various game services such as concierge services and entertainment content services using the video display screen 34 and one more input devices.

During certain game events, the gaming machine 2 may display visual and auditory effects that can be perceived by the player. These effects add to the excitement of a game, which makes a player more likely to continue playing. Auditory effects include various sounds that are projected by the speakers 10, 12, 14. Visual effects include flashing lights, strobing lights or other patterns displayed from lights on the gaming machine 2 or from lights behind the belly glass 40. After the player has completed a game, the player may receive game tokens from the coin tray 38 or the ticket 20 from the printer 18, which may be used for further games or to redeem a prize. Further, the player may receive a ticket 20 for food, merchandise, or games from the printer 18.

FIGURE 3 is a block diagram depicting gaming machines distributed in different establishments connected using a secure virtual network. Using the secure virtual network, network gaming services, data acquisition and data access may be provided to a large number of gaming machines distributed throughout a gaming entity 350 from a central location such as the central office 142. These services may be provided to gaming machines that have traditionally operated in a "stand alone" mode such as gaming machine 336 and 138 in the store 140. In FIG. 3, some of the communication infrastructure necessary to implement a secure virtual network for one embodiment of the present invention are described.

In one embodiment, the secured virtual network may be an IP based Virtual Private Networks (VPNs). An Internet-based virtual private network (VPN) uses the open, distributed infrastructure of the Internet to transmit data between corporate sites. A VPN may emulate a private IP network over public or shared infrastructures. A VPN that supports only IP traffic is called an IP-VPN. Virtual Private Networks provide advantages to both the service provider and its customers. For its customers, a VPN can extend the IP capabilities of a corporate site to remote offices and/or users with intranet, extranet, and dial-up services. This connectivity may be achieved at a lower cost to the gaming entity with savings in capital equipment, operations, and services. Details of VPN methods that may be used with the present invention are described in the reference, "Virtual Private Networks-Technologies and Solutions," by R. Yueh and T. Strayer, Addison-Wesley, 2001, ISBN#0-201-70209-6, which is incorporated herein by reference and for all purposes.

There are many ways in which IP VPN services may be implemented, such as, for example, Virtual Leased Lines, Virtual Private Routed Networks, Virtual Private Dial Networks, Virtual Private LAN Segments, etc. Additionally VPNs may be implemented using a variety of protocols, such as, for example, IP Security (IPSec) Protocol, Layer 2 Tunneling Protocol, Multiprotocol Label Switching (MPLS) Protocol, etc. Details of these protocols including RFC reports may be found from the VPN Consortium an industry trade group (http://www.vpnc.com, VPNC, Santa Cruz, California).

In FIG. 3, a number of embodiments of IP VPN services are implemented to allow connectivity between the various gaming machines and database servers in the gaming entity. For instance, the gaming machine 336 in the store 140 may directly communicate with the database server 124 in the central office 142 via the internet 304. The communication path between the gaming machine 336 and the database server 124 may be the local ISP 314, a number of routers on the Internet 304, a local ISP 313 accessed by the central office 142, the router 302 and the firewall 300. The firewall may be hardware, software or combinations of both that prevent illegal access of the gaming machine by an outside entity connected to the gaming machine. For instance, an illegal access may be an attempt to plant a program in the database server that alters the operation of the database server or allows someone to steal data. The internal firewall is designed to prevent someone such as a hacker from gaining illegal access to the gaming machine and tampering with it in some manner. Firewalls and routers used in FIG. 3 may be provided by CISCO Systems (San Jose, California).

The network interface between the gaming machine 336 and the local ISP may be a wireline interface, such as a wired Ethernet connection, a wired ATM connection, or a wired frame relay connection, or a wireless interface, such as a wireless cellular interface. For instance, the gaming machine 336 may include a wireless modem and an antenna that allows the gaming machine to connect with the local ISP 314. As another example, the gaming machine may contain a dial-in modem, a DSL modem or a cable modem that allows that gaming machine 336 to connect with the local ISP 314 via a coaxial cable or phone line 337. The gaming machine 336 may also contain an internal firewall to prevent illegal access to the gaming machine. Other gaming machines, such as 338 and 340, located at various locations throughout the gaming entity 350 may also include the hardware described above and transmit information via a local ISP, such as 315 and 320, and the Internet 304, to a remote server such as the database server 124 in the central office 142.

Using the network interface, the gaming machine 336 may send game performance data, game usage information and gaming machine status information or any other information of interest generated on the gaming machine from one or more gaming transactions to the database server 124 located in the central office or some other remote server. Using this method, the need to manually gather data from the gaming machine using a route operator may be eliminated, which may reduce gaming machine operating costs and may provide better tracking of the performance of gaming machines, such as 336, that have traditionally operated in a “ stand alone” mode.

For security purposes, any information transmitted from the gaming machine 336 over a public network to a remote server may be encrypted. The encryption may be performed by the master gaming controller or by another logic device located on the gaming machine. In one embodiment, the information from the gaming machine may be symmetrically encrypted using a symmetric encryption key where the symmetric encryption key is asymmetrically encrypted using a private key. The public key may be obtained by the gaming machine 336 from a remote public key server. The encryption algorithm may reside in processor logic stored on the gaming machine. When a remote server receives a message containing the encrypted data, the symmetric encryption key is decrypted with a private key residing on the remote server and the symmetrically encrypted information sent from the gaming machine is decrypted using the symmetric encryption key. In addition, a different symmetric encryption key is used for each transaction where the key is randomly generated. Symmetric encryption and decryption is applied to most of the information because symmetric encryption algorithms tend to be 100-10,000 faster than asymmetric encryption algorithms.

Information needed to apply the encryption algorithm such as private keys and public keys may be stored on a memory residing in the gaming machine 336 where the memory may be a flash memory, an EPROM, a non-volatile memory, a ROM, a RAM, a CD, a DVD, a tape drive, a hard drive or other memory storage device. Typically, the public keys are stored on a writeable media such as a hard drive while the private keys are stored on a read only memory such as an EPROM or a CD-ROM. The same or a different memory residing on the gaming machine 336 may also include information used to authenticate communications between the gaming machine 336 and a remote server, such as 124. For instance, a serial number or some other identification numbers may be used by the firewall 300 or the database server 124 to authenticate the sender of a message.

The encrypted communications from the gaming machine 336 to a remote server may be implemented using a TCP/IP communication protocol. Thus, the encrypted information from the gaming machine may be encapsulated in multiple information packets and sent to the IP address and/or an unique ID (UID) of a remote server. The gaming machine 336 may contain a memory storing a number of IP addresses and/or unique IDs (UIDs) of remote servers or other devices where the gaming machine may send information. Prior to sending a message, the gaming machine may look up the IP address and/or the UID of the remote server or destination device.

For each information packet, the gaming machine may generate one or more signatures and may append them to the information packet. The signature may allow the recipient of the packet to unambiguously identify the sender of the packet as well as to determine if the correct amount of data was received. For instance, the signature may include a checksum of the data that was sent. Further, the information packet may contain routing information allowing subsequent communication with the gaming machine, such as an IP address and/or an UID of the gaming machine. General details of these types of processes, such as TCP/IP implementation and data authentication, are described in the text "Mobile IP Unplugged" by J. Solomon, Prentice Hall and the text "Computer Networks", A. S. Tanenbaum, Prentice Hall. Both of these references are incorporated herein by reference in their entireties and for all purposes.

Using the communication infrastructure and methods described above a gaming machine or other device connected to a remote server may request one or more gaming services from a remote server. For instance, a gaming machine may send a game license request to the remote server 124. A gaming machine may store code to play one or more games controlled by the master gaming controller such as a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game. Traditionally, installing a new game has involved manually exchanging (e.g., by hand) an EPROM (e.g. a read-only memory) containing the game on the gaming machine. Using the communication infrastructure described above, the gaming machine 336 may request a game license for one or more games stored in the gaming machine from a remote server acting as a game license server such as 124. The game license server may send a game license reply message containing a game license which allows the gaming machine to present the one or more games stored on the gaming machine. These game license requests may be performed prior to each game or the license may allow game play for some finite time period. For instance, the game license may be an annual license, a monthly license, a daily license, a per-use license or a site license. Details of the game license request and reply process between a gaming machine and a remote server are described with reference to FIGs. 6 and 7.

In another example, the gaming machine 336 may send a maintenance request message to a remote server when the gaming machine malfunctions. After receiving the maintenance request message, the remote server may perform one or more remote diagnostics on the gaming machine 336 via one or more diagnostic request messages. The remote diagnostics may include both software and hardware diagnostics. In addition, the remote server may develop service priority list based upon a plurality of maintenance requests received from a group of gaming machines in communication with the remote server. In yet another example, a remote server may obtain software version information or gaming configuration information, from gaming machine 336, by sending a software version request message or a gaming configuration request message to the machine. Information contained in these messages may be used to provide software updates and gaming configuration updates to the gaming machine 336.

In a further example, the gaming machine 336 may generate a digital signature or some other type of unique identification information and may send a digital signature verification request or an identification verification request to a remote server. The verification request may be part of an electronic fund transfer. After receiving authorization from the remote server in an authorization reply, the gaming machine 336 may send a fund transfer request with fund transfer information to the remote server and may receive a fund transfer reply authorizing the gaming transaction.

A remote server may also provide performance reports or other services for the gaming machine 336. For instance, the gaming machine 336 may send a report request message to the remote server 124 requesting a performance report for the gaming machine over some prior time period. After remote server generates the report, it may be sent back to the gaming machine 336 or some other access point for display. For instance, the report may be displayed on a display screen of the gaming machine 336, a computer 316 located in the store 140 or on a portable network access point 134 located outside of the store.

An advantage of the virtual network described above is that it allows gaming services such as data acquisition, game licensing and report generation to be provided a single gaming machine without the use of a dedicated network which are typically expensive. This advantage may potentially increase the utility of a gaming machine while reducing the costs associated with operating and maintaining a machine. In particular, for gaming establishments with a small number of gaming machines operating in a " stand alone" mode, a virtual network may be the only viable way to provide cost effective gaming services via a network. The virtual network is enabled by an encryption scheme which utilizes multiple key encryption and symmetric encryption keys to provide secure communication of sensitive gaming data. For each session, the symmetric encryption keys may be randomly generated or may be rotated by selecting from a pool of keys.

The methods described above may be applied and may be advantageous to any gaming machine in the gaming entity 350. Also, many different embodiments of the methods are possible. For instance, using a wireless network interface, gaming machine 338 in Casino 110 may send game license requests or other requests to the database server via the router 308, the dedicated line 322, router 302 and the firewall 300. As another example, using a wireline network interface, such as a wired Ethernet connection, a wired ATM connection or a wired frame relay connection, gaming machine 340 in casino 122 may send may send a gaming report request to the database server 100 in casino 110 via the database server 112, the firewall 310, the router 312, the local ISP 320, the internet 304, the local ISP 315, the router 308 and the firewall 306. When a dedicated communication network is used, encryption may be optional over the dedicated network, e.g. if a dedicated network was used between the gaming machine 340 and the database server 112, the gaming machine 340 may not use encryption to send information to the database server 112. However, the database server would apply an encryption scheme such as the one described above before sending out information over a public network. Returning to the example, the database server 100 may serve as a regional report server. After generating a gaming report reply message to the gaming report request message from gaming machine 340, the database server 100 may send a message to the database server 124 in the central office 142 acknowledging that a report was generated.

The virtual network may also allow remote access to gaming information such as gaming performance information at various gaming establishments in the gaming entity from mobile access points. For example, the remote access point 134 may be a portable computer with a wireless modem. Typically, the remote access point 134 will have a high level of security such as special access software. Using the remote access point 134, a user such as a travelling employee of the game entity may access gaming information at casino 110 or casino 122 via the local ISP 314. The access may be routed through the central office 142 or may be routed directly to one of the casinos bypassing the central office. In addition, different access privileges may be accorded to different remote users. For instance, one remote user may be able to access information from any establishment in the gaming entity while another may only be able to access information from a particular establishment.

FIGURE 4 is an interaction diagram showing communications between a gaming machine, local server, local ISP and remote server over a public network. The diagram provides some details of a communication process between a gaming machine 340 in casino 122 and the database server 122 in the central office 142 as described with reference to FIG. 3 for one embodiment of the present invention. In 400, the gaming machine 340 may perform a gaming transaction such as a coin-in, initiating a game play or a coin-out. In 402, the gaming machine 340 symmetrically encrypts gaming transaction data from one or more gaming transactions using a symmetric encryption key. In 404, the symmetric encryption key may be encrypted using an asymmetric encryption key such as public key in a public-private encryption scheme which may only be decrypted using a matching private key at the message destination. For each gaming transaction, a symmetric encryption key is selected from a pool of symmetric encryption keys or randomly generated. Thus, the symmetric encryption key varies from gaming transaction to gaming transaction. When a dedicated or private communication network is used and extra security is desired, the symmetric key may also be asymmetrically encrypted with an asymmetric encryption key which is non-public. In 406, a message may be generated and the encrypted data and key may be sent to a local server 112.

As previously described with reference to FIG. 3, the encrypted information may be encapsulated in multiple information packets using a TCP/IP communication protocol. In addition other communication protocols such as a frame relay communication protocol, an ATM communication protocol or combination of protocols may also be utilized. Prior to sending the data, the gaming machine may look up the IP address and/or the UID of the remote server which may be stored in a memory on the gaming machine. When a dedicated communication network is used between the gaming machine and the remote server, such as local server 112, the encryption process performed by the gaming machine may be optional. Prior to sending the message, the gaming machine 340 may generate one or more signatures that allow the receiver of the message to authenticate the sender of the message as well as the accuracy of the data contained in the message. These signatures may be appended to the message or incorporated in the message in some manner.

In one embodiment, the gaming machine 340 may by-pass the local server and may send a message to the remote server 124 via the local ISP 320. In some embodiments, a local server may not be available to the gaming machine, such as gaming machine 336 in the store 140 in FIG. 3. In 438, when communications are not established between the local ISP 320 and the gaming machine 340, the gaming machine may contact the local ISP 320 using a network interface and establish communications with the local ISP 320. In 440, the gaming machine 340 may send a message with the encrypted gaming transaction data and the encrypted symmetric key to the IP address and/or the UID of the remote server 124 via the local ISP 320.

In 408, the local server 112 receives a message from the gaming machine 340. The local server 112 may authenticate that the message was sent from the gaming machine 340 and determine that the data sent in the message is complete. Next, the local server 112 may decrypt the symmetric encryption key using a private asymmetric encryption key stored on the local server. In 410, the local server decrypts the transaction information included in the message using the symmetric encryption key. In 412, the local server 112 may process and store the data generated from the gaming machine.

In 414, gaming transaction data from the gaming machine 340 may again be symmetrically encrypted using a symmetric encryption key. The gaming transaction data may also include additional gaming transaction data from other gaming machines. In one embodiment, the gaming transaction data may include game usage data that allows a game played on a gaming machine to be billed on a per use basis. In 416, the symmetric encryption key may be asymmetrically encrypted using an asymmetric encryption key such as a public key exchanged between the local server and the remote server 124 and a message containing the encrypted data may be generated. Prior to sending the message, the local server 112 may generate one or more signatures that allow the receiver of the message to authenticate the sender of the message as well as the accuracy of the data contained in the message. These signatures may be appended to the message or incorporated in the message in some manner. In 418, when a communication has not been established between the local server 112 and a local ISP 320, the local server may contact the local ISP 320 and establish communications using an appropriate communication protocol such as TCP/IP. In 420, the local server 112 may send a message with the encrypted gaming transaction data and the encrypted symmetric key to the IP address and/or the UID of the remote server 124 via the local ISP 320.

In 422, the local ISP 320 processes and forwards the message from the local server 112 or the gaming machine 340 to the public network 304. In 424, the public network processes the message from the local ISP 320 and forwards it to the remote server 124. Processing of the message by the local ISP 320 and the public network 304 may involve routing multiple data packets comprising the message.

In 426, the remote server receives a message from the gaming machine 340 or the local server 112. The remote server 124 may authenticate the sender of the message using one or more signatures included in the message and determine the accuracy of the data of the message. For instance, the remote server may generate a check sum, CRC, or other verification of the data in the message and compare that with a check sum, CRC, or other verification of the data generated by the sender of the message. Next, the asymmetrically encrypted symmetric encryption key may be decrypted using a private key residing on the remote server124. In 428, the symmetric key may be used to decrypt the symmetrically encrypted data. In 428, the remote server may process and store the data. The message from the gaming machine or local server 112 may include a request of some type for the remote server. In 430, the remote server may implement the request. For instance, the message may contain a request for a game license (See FIG. 6 and 7), a request for a report or a request for some other game service.

In 431, the remote server may generate a reply message. The reply message may include an acknowledgement that the original message was received and may also include requested information. For instance, the remote server may request diagnostic data or a report of some type from the gaming machine. The data in the reply message may be encrypted. Thus, in 442, the transaction reply data may be symmetrically encrypted using a symmetric encryption key and in 443 the symmetric encryption key may be asymmetrically encrypted using the recipient's public key. When the reply message is received by a gaming device, such as the gaming machine 340 or the local server 112, the gaming device may decrypt (e.g., as in 426) the asymmetrically encrypted symmetric encryption key using a private key stored on the gaming device.

In 432, the remote server sends the reply message to the local server 112 and/or the gaming machine 340 via the public network 304. The remote server 124 may access the public network via an ISP local to the remote server 124. In 434, the local server may receive a reply message and store data included in the message. In some embodiments, the acknowledgement may be forwarded to the gaming machine 340. In other embodiments, the local server 112 may be by-passed or a local server 112 may not be available to the gaming machine 340 and the reply message may be received directly by the gaming machine 340 via the local ISP 320.

FIGURE **5A** is a flow chart depicting a method 500 of sending transaction data between a gaming machine and one or more remote servers. Although the method is described on a gaming machine for illustrative purposes, the method is not so limited and may be applied on other gaming devices such as the remote servers described above. Thus, as described with reference to FIG. 4, the gaming machines and remote servers may send messages with encrypted data to one another in a similar manner. In 505, the gaming machine performs one or more gaming transactions. For example, a gaming transaction may be a coin-in or a pay-out on the gaming machine. Information from one or more gaming transactions may be stored in a non-volatile memory located on the gaming machine. In 510, the gaming transaction data may be symmetrically encrypted using a symmetric encryption key. The encrypted gaming transaction data may include data generated from a single gaming transaction or multiple gaming transactions. The symmetric key may be selected from a pool of symmetric keys or may be randomly generated such that the symmetric key is varied each time gaming transaction data is encrypted. In 515, the symmetric encryption key may be asymmetrically encrypted using a public key that was previously exchanged between the gaming machine and the recipient of the message. In the case, where a dedicated network is used the asymmetric encryption key is non-public i.e. it is not readily available to the public.

In 518, the gaming machine generates a message containing the symmetrically encrypted gaming transaction data and the asymmetrically encrypted symmetric encryption key over a communication protocol such as but not limited to TCP/IP. The message may include additional information such as signatures to authenticate the sender of the message, signatures to validate the accuracy of the data included in the message and an IP address and/or an UID of the sender as well as other message routing information. The message may also include a request for the recipient to return information to the gaming machine. For instance, the gaming machine may request a remote server to provide a gaming license that allows a game to be played on the gaming machine.

In 520, when communications have not been established between the gaming machine and a local ISP, the gaming machine may contact a local ISP. The gaming machine may also send messages to a local ISP by sending the message first to a local server which may then forward the message to the local ISP. The gaming machine may contact the local ISP using a communication protocol such as TCP/IP and a network interface such as a wireless modem. In 525, the gaming machine sends the message generated in 518 to a remote site such a game license server, a report server or some other device via the local ISP. In 530, the gaming machine may determine when an acknowledgement message has been received from the remote site. When an acknowledgement message has not been received, the gaming machine may resend the message one or more times. When the acknowledgement message has been received, the gaming machine may repeat process 500.

FIGURE **5B** is a flow chart depicting a method 550 of receiving transaction data between a gaming machine and one or more remote. Although the method is described on a remote server for illustrative purposes, the method is not so limited and may be applied on other gaming devices such as the gaming machines described above. Thus, as described with reference to FIG. 4, the gaming machines and remote servers may receive and process messages with encrypted data from one another in a similar manner.

In 555, the remote server receives a message with encrypted gaming transaction data from a gaming machine, another remote server or some other gaming device. In 560, an asymmetrically encrypted symmetric encryption key included in the message in 555 is decrypted using a private key stored on the remote server. In 565, the decrypted symmetric encryption key may be used to decrypt symmetrically encrypted gaming transaction data included in the message. In 570, the decrypted gaming transaction data or any service requests contained in the message are processed. For instance, gaming transaction data in the message may be archived.

FIGURE **6** is a flow chart depicting a method 600 of obtaining a game license on a gaming machine providing game play of one or more games. In 605, a gaming machine initiates a gaming license request. In one embodiment, the gaming license request may be initiated when a current gaming license on the gaming machine is about to expire. In another embodiment, the gaming license request may be initiated in response to a player on a gaming machine requesting a game play of a particular game. In 610, game license request data used to provide and implement gaming licenses is encrypted. The game license data may be encrypted using a symmetric encryption key and the symmetric encryption key may be asymmetrically encrypted using a public key. The game license request data may include the symmetric encryption key, a serial number of the software corresponding to one or more games or some other software identification number, a serial number of the gaming machine as well as other machine identification information, game owner identification information, game usage data including the number of times a gaming license has been used and license expiration data. The game usage data may be used to bill the gaming entity owning the gaming license for use of the game license. The software identification number in the gaming license data may correspond to one or more games such as a video slot game, a mechanical slot game, a video poker game, video blackjack game and video pachinko game.

In 612, a game license request message is generated with the encrypted game license request data. The game license request message may be sent to a remote server using a TCP/IP protocol. Thus, the game license request message may include an IP address and/or an UID of the remote server as well as an IP address and/or an UID of the gaming machine. The gaming machine may store the IP addresses and/or the UIDS of one or more remote servers in a memory residing on the gaming machine. Prior to sending the gaming license request message, the gaming machine may look-up the IP address and/or the UID of the destination remote server. The gaming license request message may include one or more signatures used by the recipient of the message to unambiguously identify the sender of the message and to validate the accuracy of the data contained in the message. The signatures may be generated by the gaming machine and appended to the message.

In 615, when communications between the gaming machine and a local ISP have not been established, the gaming machine may contact a local ISP and establish communications. In one embodiment, the gaming machine may not directly contact a local ISP. Instead, the gaming machine may contact and may send the gaming license request message to a local server which contacts a local ISP and sends the gaming license request message. In another embodiment, the gaming machine may send unencrypted gaming license request data to the local server. The local server may encrypt the gaming license request data, generate a gaming license request message and send the message to a remote server such as a gaming license request server.

In 620, the gaming machine sends the gaming license request message to a remote site such as a game license server via the local ISP. When a communication protocol such as TCP/IP is used, the message may be encapsulated in multiple information packets. In 625, the gaming machine determines whether an acknowledgement from the remote site has been received. When the acknowledgement from the remote site has not been received, the gaming machine may resend the message according to 620.

In 628, the gaming machine receives a game license reply message. The game license reply message may include a number of signatures used by the gaming machine to authenticate the sender of the message and to validate the data contained in the message. In 630, the gaming machine may decrypt an asymmetrically encrypted symmetric encryption key using a private key stored in memory on the gaming machine and then decrypt the game license reply data with the symmetric encryption key. The game license reply data may include a game license for one or more games available on the gaming machine. The game license may be an identification number of some type that allows software on the gaming machine corresponding to the license to be executed. The game license reply data may also include an expiration date for the license. In 635, the gaming machine may update game license data stored on the gaming machine when a new game license was included in the game license reply data. In one embodiment, the game license request message may include game usage data without a request for a new license. In this case, the game license reply message may include an acknowledgement that the game license request message was received but may not contain a new game license.

An advantage of the game license request method is that a gaming machine owner may be able operate gaming machines including many different types of games but only pay for each game on a per use basis. In a "pay-as-you go" billing scheme, an operator of the gaming machine is charged each time a game is played on the gaming machine. At regular intervals, a usage fee may be paid by the operator of the gaming machine to the owner's of the gaming software used on the gaming machine. The cost per use of each game may be varied from game to game and these costs may change with time. For example, the cost per use charged for newer gaming titles may be higher than the cost per use charged for older gaming titles. Thus, when a particular game is unpopular, the costs to the gaming machine operator are minimized as compared to when the gaming machine operator pays up front for a gaming machine with a game that receives little game play.

Another advantage of the game license request method is that it may also be used for other types of game service requests. For instance, a report request message with encrypted report request data may be generated in the manner described above and sent to a remote server via a local ISP. When a report reply message is received via the local ISP containing a report, the report may be displayed to the gaming machine. In another example, a gaming machine may send a maintenance request message via a local ISP in a manner described above.

FIGURE **7** is a flow chart depicting a method 700 of providing a game license to one or more gaming machines using a remote server. In 705, the remote server receives a game license request message from a gaming machine, local server or some other device. The message may have been received via a local ISP in communication with the remote server. As described above, although not shown in the flow chart, the remote server may also receive a report request, maintenance request or some other transaction request from the gaming machine, local server or remote device. After receiving the message, the remote server may authenticate the sender of the message using one or more signatures contained in the message and validate the accuracy of the data in the message using one or more signatures contained in the message. For instance, the remote server may generate a checksum on the data in the message and compare it with a checksum generated by the gaming machine on the data in the message which was appended to the message.

In 710, the remote server may decrypt a symmetric encryption key included in the game license request message using a private encryption key. With the symmetric encryption key, the remote server may decrypt the game license request data. The game license request data may include a serial number of the software corresponding to one or more games or some other software identification number, a serial number of the gaming machine as well as other machine identification information, game usage data including the number of times a gaming license has been used, license expiration data and game owner identification information.

In 715, using the serial number of the gaming machine and the other machine identification information the remote server may identify the gaming machine. The serial number of the gaming machine is one example of an UID that may be used with the present invention. A table of gaming machine identification information may be stored on the remote server. From the gaming machine identification information, the remote server may be able to determine the type of gaming machine and the games available on the gaming machine. In 720, when appropriate, the remote server may generate a new gaming license for the gaming machine. If the gaming license request message includes a request for a gaming license not available on the gaming machine or not enabled for some reason on the gaming machine, then the gaming license request may be denied. In another example, the game license request may include game usage information for billing purposes and a new game license may not be required.

In 725, when a new game license is generated, the game license reply data including the new game license may be encrypted with a symmetric encryption key and the symmetric encryption key may be asymmetrically encrypted with a public key. In other cases, the game license reply message may include an acknowledgement that the message was received but may not include a new game license. In 730, the information regarding the game license request such as the machine identification information, a type of game license request (e.g. type of game), a time of the request and whether the request was granted may be stored on the remote server.

In 732, a game license reply message with the game license reply data may be generated. In 735, via a local ISP and the Internet, the game license reply message may be sent to the local server and/or the gaming machine. In 740, a billing request message based upon the game usage data contained in the game license request or the type of license requested may generated. In 745, the billing request message may be sent to the gaming machine owner identified in the gaming license request message.

FIGURE **8** is a block diagram of gaming software distribution network that uses a secure virtual network. In the present invention, gaming software may be transferred between various gaming devices, in a gaming software distribution network 90, after receiving authorization from a gaming software authorization agent 50. The gaming software authorization agent 50 may be a conventional data server including but not limited to a database 202, a router 206, a network interface 208, a CPU 204, a memory 205 and a firewall (not shown). The CPU 204 executes software to provide the functions of the authorization agent 50 as will be described below in more detail. In general, the gaming software authorization agent 50 approves all gaming software transactions between two gaming devices in the gaming software distribution network and stores a record of the gaming software transactions. Database 202 may be used to store gaming software transaction records. Details of the gaming devices and network connections used in the gaming distribution network 90 are described in FIGURE 8. Details of the types of gaming software transaction that may be implemented in gaming software distribution network and the implementation of the transactions for some embodiments of the present invention are described with respect to FIGs. 9-14.

In the gaming industry, gaming software that is used to play a game of chance on a gaming machine is typically highly regulated to ensure fair play and prevent cheating. Thus, at any given time, it is important for a gaming regulatory entity to know what gaming software is installed on a gaming machine at any particular time. Currently, gaming software is often programmed into an EEPROM and installed on a gaming machine. When the EEPROM is installed in the gaming machine, it is manually checked by a representative of the gaming regulatory board prior to installation to ensure approved gaming software is being installed on the gaming machine. This process is time consuming and relatively inflexible. In the gaming industry, there is a desire to simplify the gaming software installation process so that gaming machine operators may more easily reconfigure gaming machines with different gaming software to respond to shifting customer tastes and demands. The gaming software authorization agent 50 meets this need by allowing gaming software to be electronically transferred between gaming devices, such as game servers and gaming machines, in a manner that may be easily monitored and regulated. For instance, the software authorization agent 50 may be maintained or supervised by a gaming regulatory agency. However, the software authorization agent 50 may also be maintained by a gaming entity that controls many gaming properties to track software distributions on various gaming machines. In addition, besides monitoring electronic transfers of gaming software, the software authorization agent 50 may also be used to store a record of any change of gaming software on a gaming machine such as changes resulting from a manual installation of gaming software. For instance, a technician may manually load gaming software on to a gaming machine using a portable memory device storing the gaming software.

Details of gaming devices and the network connections in the gaming software distribution network are now described. In the present invention, gaming software may be transferred between gaming software providers, such as 51 and 52, gaming software distributors, such as 53 and 60, and gaming machines, such as 54, 55, 56, 57, 58 and 59. A gaming software provider may be a gaming device, such as a game server, that is maintained by a gaming software developer, such as IGT (Reno, Nevada), that develops gaming software for various gaming platforms. A gaming software content provider, such as 51 and 52, may maintain a plurality of gaming software titles, versions of gaming software titles and gaming software components that may be requested by another gaming device for an electronic download. The gaming software content provider may download gaming software to various customers after the customer has entered a licensing agreement with the content provider. Some details of obtaining game licenses for operating gaming software on a gaming machine have been described above with respect to FIGs. 6 and 7.

A set of gaming software components may be executed on a gaming machine to play a gaming of chance. The game of chance may include gaming software components used to play a bonus game in conjunction with the game of chance. Thus, a complete set of gaming software components used to play a game of chance may be downloaded or a portion of the gaming software components needed to play a game the game of chance may be downloaded. For instance, a complete package of gaming software components may be downloaded to replace a game executed on a gaming machine with a new game. As another example, a single game software component may be downloaded to fix an error in a game of chance executed on the gaming machine. In yet another example, a set of gaming software components may be downloaded to install a new graphical "feel" for the game of chance while other gaming software components for the game are not changed. In the present invention, any gaming device that stores gaming software for downloads may download a complete set of the gaming software components used to play the game of chance or portions of a complete set of the gaming software components. Some examples of gaming software components may include but are not limited to: 1) a banking modules for coin-in, coin-out, credits cards, fund transfers, 2) security modules for tracking security events such as door open, lost power, lost communication, 3) bet modules for handling betting configurations such as a number of paylines, a number of coins per line and denominations, 4) communication modules allowing a gaming device to communicate with other gaming devices using different communication protocols and 5) an operating system modules used in an operating system installed on the gaming machine. Details of some of the gaming software components that may be downloaded in the present invention are described in co-pending U.S. application no. 10/040,239, by LeMay et al., filed on January 3, 2002 and titled "Game Development Architecture That Decouples The Game Logic From The Graphics Logic," which is incorporated herein in its entirety and for all purposes.

Gaming software related to other aspects of game play and operation of a gaming machine may also be authorized and downloaded using the methods and hardware of the present invention. For instance, device drivers used to operate a particular gaming device may be downloaded from a content provider or another gaming device. As another example, gaming software used to provide player tracking services and accounting services may be downloaded from a content provider or another gaming device. Even when the gaming software is not regulated by a gaming entity, it may be useful to perform the authorization process because the transaction records may be used to track the distribution of the gaming software on various gaming devices. The transaction records may be helpful to both providers of gaming software and operators of gaming devices in determining necessary upgrades and maintenance of gaming software on a gaming device such as a gaming machine.

A gaming software distributor, such as 53 and 60, may maintain a plurality of gaming software titles, versions of gaming software titles and gaming software components that may be transferred to another gaming device, such as a gaming device, for an electronic download. The gaming software distributors, such as 53 and 60, may be gaming devices, such as game servers, that are maintained by a gaming entity such as a casino. For instance, game server 53 may be operated by a first casino and game server 60 may be operated by a second casino. The game servers may store gaming software that has been licensed to the gaming entity from one or more gaming software providers such as 51 and 52. In one embodiment, a game server may also be a gaming machine. One example of a game server that may be used with the present invention is described in co-pending U.S. patent application 09/042,192, filed on June 16, 2000, entitled "Using a Gaming Machine as a Server" which is incorporated herein in its entirety and for all purposes.

The game servers operated by a gaming entity may be used to provide gaming software to a plurality of gaming machines. For instance, game server 53 may be used to provide gaming software to gaming machine 54, 55, 56 and game server 60 may be used to provide gaming software to gaming machines 57, 58 and 59. In one embodiment, the game servers may be programmed to download gaming software in response to a software request on a gaming machine. For instance, a game player playing a game on a gaming machine, such as 55, may request to play a particular game of chance on the gaming machine 55 which is downloaded to the gaming machine from the game server 53. In another embodiment, the game servers, such as 53 and 60, may be used to update and reconfigure the gaming software on one or more gaming machines. For instance, the game server 53, may be used to regularly change the games of chance or bonus games of chance available for play on gaming machines 54, 55 and 56.

In the present invention, gaming software transferred between two gaming devices and communications between two gaming devices may use a variety of network architectures including but not limited to local area networks, wide area networks, private networks, a virtual private network, the Internet 304 and combinations thereof. Details of methods of using the Internet 304 in a secure manner have been described with respect with 3, 4, 5A and 5B.

In one embodiment, gaming software and other gaming information may be transferred between two gaming devices using a satellite connection. For instance, the gaming information transferred via satellite may include but is not limited to metering information generated on the gaming machine. In a gaming device using a satellite communication system, the gaming device is connected to a satellite dish. For instance, a gaming machine located in a store, as described with respect to FIG. 3, or a cruise ship may use a satellite connection. Two standard coaxial cables may connect the gaming device to the satellite dish. The gaming device, such as a gaming machine, may include a satellite modem to enable the satellite connection.

The satellite dish may send requests to the Internet 304 and receive Internet content via the satellite 72. The satellite 72, in turn, may communicate with a hub facility 70, which has a direct connection with the Internet 304. Typically, the transfer rate of information from the gaming device, such as gaming machine 59, to the satellite 72 (uplink rate) is less than the transfer of rate of information from the satellite 72 to the gaming device (downlink rate). For example, the uplink rate may be 28 Kilobytes per second while the downlink rate may be 500 kilobytes per second or higher. However, for software downloads, a high downlink rate may only be required for efficient gaming software downloads. Satellite Internet services may be provided by a company such as Starband Corporation (Mclean, Virginia).

In another embodiment, gaming software and other gaming information may be transferred between two gaming devices using an RF connection. The gaming information transferred via the RF connection may include but is not limited metering information generated on the gaming machine. As one example, US Telemetry corporation (UTSC, Dallas, Texas), uses radio frequency transmissions in the 218-222 MHz band to provide communications services to fixed end point devices as well as mobile devices. The fixed end point device may be a gaming machine located in a store or located in a casino, such as gaming machine 54 ,as well as a mobile gaming device such as a gaming machine located in a riverboat or portable gaming device that may be carried by a player and used to play a game of chance.

The RF network in a metropolitan service area may include cell transceiver sites or towers, such as 84 and 86, a system hub or master cell transceiver site, such as 82. The MCTS 82 is connected to a Network Operations Center (NOC) 80, which is essentially a data clearinghouse. Data is transferred from a CTS, such as 84 and 86, to a Master CTS (MCTS) 82 through a Publicly Switched Telephone Network. Data is transferred from the MCTS 82 to the NOC 80 database via an ATM or a Frame Relay. Data transfer protocol and user access to various end-point devices may be provided through web interfaces. Thus, using an RF network and the secured virtual network methods as described with respect to FIG. 3, 4, 5A and 5B, gaming information as well as gaming software may be transferred between various gaming devices. For instance, a remote casino accounting office 142 may obtain information from gaming devices connected to the RF network via the Internet 304.

In the present invention, records of authorizations for the transfer of gaming software between gaming devices may be stored in the database 202. Thus, given an initial distribution of gaming software in the gaming software distribution network 90 for each gaming device, the gaming software authorization records may be used to track the gaming software distribution for gaming devices in the gaming distribution network as a function time. This tracking capability may be useful for various gaming entities such as a gaming regulatory board, a gaming software content provider and gaming operators. For instance, a gaming regulatory board may be able to see the gaming software installed on all gaming devices it regulates at any given time using the database 202. As another example, a gaming software content provider, such as 51 and 52, may be able to view gaming software requests for their gaming software products as a function of time. In yet another example, a remote casino accounting office 142 may be view the distribution of their gaming software on the gaming machine under their control.

The database 202 may be partitioned and include various security protocols to limit access of the data in transaction database according to various criteria. For instance, a gaming software provider 51 may be able to view records only of gaming software transactions involving their products but not of a competitors products. As another example, a gaming entity may be able to view records of gaming software transactions involving gaming machine that they operate but not view gaming software transactions for gaming machines that another competitor controls. Further details of an interface for providing gaming software distributions is described with respect to FIG. 15.

FIGURE **9** is a block diagram depicting software transactions in a gaming software distribution network controlled by a software authorization agent. Gaming software transactions between a software authorization agent 50, a gaming software distributor 53, a gaming software content provider 51 and two gaming machines, 54 and 55 in a gaming software distribution network are described. In FIG. 9, the number and types of gaming devices are provided for illustrative purposes only and the present invention is not limited to the gaming devices shown in the Figure.

As described with respect to FIG. 8, the software authorization agent 50 is used to authorize gaming software transfer between two gaming devices. For instance, in 214, the gaming software distributor 53, which may be a game server maintained by a casino, may contact the software authorization agent 50 to request a transfer of gaming software from the gaming software provider 51 to the gaming distributor 53. The gaming distributor may also contact the software authorization agent to request a transfer of gaming software from the gaming software provider 51 to another gaming device such as gaming machine. The software authorization agent 50 may approve or deny the request depending on the gaming software transaction information contained in the request. For instance, if a gaming device, such as the gaming software distributor 53, can not be identified and authenticated by the software authorization agent 50, then the software authorization agent 50 will deny the request for the transfer of gaming software. As another example, if the gaming device, has requested a software title that is unknown to the software authorization agent 50, then the software authorization agent will deny the request for the transfer of gaming software. Some details of this gaming software transaction are described with respect to FIG. 11, 13 and 14.

After receiving authorization from the software agent, the gaming software distributor 53 may contact the gaming software content provider 51 and receive an electronically download of gaming software from the content provider via an electronic transfer in 210. The electronic transfer may use the network infrastructure and communication methods including encryption described with respect to FIGs.3, 4, 5A, 5B and 8. Details of this gaming software transaction are described with respect to FIG. 11. The gaming software may also be manually shipped to the gaming software content distributor 53, such as through the mail or by a courier, and then locally loaded onto a gaming device.

In one embodiment of the present invention, gaming software transfers involving the actual transfer of gaming software occur directly between two gaming devices as shown in 210. In another embodiment of the present invention, gaming software transfers may be routed through the software authorization agent 50. For instance, to transfer gaming software to the gaming software distributor 53, the gaming software content provider 51 sends the gaming software to the software authorization agent 50 which then forwards the software to the gaming software distributor. When the software authorization agent 50 receives the gaming software it may perform one or more checks on the gaming software to insure it has been approved for use or just simply forward to the destination gaming device without additional checks. All or a portion of the gaming software transfers may be routed through the software authorization agent 50.

In 212, prior to downloading gaming software to the gaming distributor or any other gaming device, the gaming software content provider 51, which may be a game server maintained by a company that develops gaming software or owns the rights to gaming software, may validate the gaming software transaction with the software authorization agent 50. The gaming software content provider 51 may send gaming software transaction information received in a request for a transfer of gaming software received from a gaming device, such as the gaming software distributor 53, to the gaming software authorization agent 50. The software authorization agent 50 may use the gaming software transaction information to approve or reject the transfer of the gaming software. The details of this gaming software transaction are described with respect to FIG. 11.

After sending the gaming software to the gaming software distributor 53, the gaming software content provider 51 may report details of this transaction to the software authorization agent 50 in 212. For instance, the gaming software provider may generate a gaming software transaction receipt that includes a unique digital signature for the gaming software that was sent. Similarly, after receiving the gaming software from the gaming software content provider 51, the gaming software distributor 53 may report details of this transaction to the software authorization agent 50 in 214. For instance, the gaming software distributor 53 may generate a gaming software transaction receipt that includes a unique digital signature for the gaming software that was received. The software authorization agent 50 may compare receipts from the sender and the receiver of the gaming software to insure the correct gaming software has been transferred between the sender and the receiver.

The gaming software distributor 53 may be connected to a plurality of gaming machines and other gaming devices that use gaming software such as gaming machine 54 and 55. The connection between the gaming distributor 53 and the gaming machines, 54 and 55 may be a local area network within a casino but is not limited to local area network within a casino. In one embodiment, gaming software transferred from the gaming software provider may be targeted to a particular gaming machine, such as 55, and the gaming software distributor 55 may forward the gaming software to the gaming machine 55 after receiving it from the gaming software content provider 51. The gaming machine 55 may unpack the gaming software and calculate a digital signature. The digital signature may be sent to the gaming distributor 53 through the local area network and forwarded to the software authorization agent 50 to complete the transaction.

In another embodiment, after a request from a gaming software distributor 53, in 220, a gaming software content provider 51 may download gaming software directly to a gaming machine 54 bypassing the gaming software distributor 53. For example, a gaming software provider 51 may download software to a gaming machine located in a store as described with respect to FIG. 3 via a satellite connection described with respect to FIG. 8. The gaming machine may unpack the software, which may have been compressed, and send acknowledgements of the transfer directly to the gaming software content provider 51, the gaming software distributor and the software authorization agent.

In yet other embodiments, a game server, such as the gaming software distributor 53, may be used to reconfigure the gaming software on a group of gaming machines, such as 54 and 55 via software downloads 218. The game server 53 may transfer a plurality of gaming software titles from one or more gaming software content providers, such as 51 and store these titles on the game server. When the gaming software is transferred from the gaming software content provider, the gaming software content provider and the gaming software distributor may agree to a license (see FIGs. 6 and 7) that allows for a certain number of gaming software downloads over a specific period of time. A gaming machine operator controlling a number of gaming machine may use a game server storing the plurality of gaming software titles to regularly re-distribute gaming software on gaming machines. The redistribution of gaming software via electronic downloads may be performed automatically, i.e., a distribution pattern may be programmed into the game server. Also, gaming software programs may be distributed to a gaming machine via a request from the gaming machine. For instance, a player may request to play a certain game on the gaming machine and the game server may transfer the requested gaming software to the gaming machine.

The transfer of gaming software from the game server to the gaming machine may require an approval from the software authorization agent 50. Further, even if the an approval is not required, gaming software transaction information may be sent to the software authorization agent so that the gaming software residing on any gaming machine at a particular time may be known. Details of a gaming software transaction between a gaming machine 54, a game server 53 and software authorization agent 50 are described with respect to FIG. 12.

The present invention is not limited to only electronic transfers of gaming software between gaming devices. The authorization methods may be also be applied to the manual installation of gaming software. For example, prior to manually installing gaming software on a gaming machine, an installation technician may request approval of the gaming software transaction from a software authorization agent 50 using a hand-held wireless device. The gaming software, which may be stored on a memory device such as CD-ROM may been shipped to gaming machine operator. Gaming software information regarding the gaming software to be manually installed on a gaming machine and information regarding the gaming machine may be entered into the hand-held wireless device and then sent to the software authorization agent. The software authorization agent may use this information to approve the gaming software transaction and to track the gaming software installed on gaming machines.

In another example, a technician may use the software authorization agent to manually check gaming software installed on a gaming machine. The technician may read gaming software information from a particular gaming machine and then using a hand-held wireless device relay the gaming machine software information and gaming machine information to the software authorization agent 50. The software authorization agent 50 may compare the information received from the hand-held wireless device with gaming software information stored in a gaming software registration database to determine whether the gaming machine has the correct software installed on it. The software authorization agent may send a message to the hand-held wireless gaming device indicating whether or not the correct gaming software is installed on a gaming machine. Further, the gaming software registration database may contain information regarding what software is installed on a particular gaming machine and what gaming software upgrades are available. When performing gaming machine maintenance, a gaming machine operator may request this information from the software authorization agent 50 to aid in the maintenance process.

Gaming software may be transferred between two gaming devices using a wireless communication connection. For example, within a casino, a game server may download gaming software to a plurality of gaming machines using a wireless network located within the casino. In another example, gaming software may be downloaded from a hand-held device to a gaming machine using an infrared communication interface. Examples of wireless communication standards that may be supported by a wireless communication connection and associated hardware/software include but are not limited to Bluetooth, IEEE 802.11a, IEEE 802.11b, IEEE 802.11x (e.g. other IEEE 802.11 standards such as IEEE 802.11c, IEEE 802.11d, IEEE 802.11e, etc.), hiperlan/2, HomeRF and IrDA. Wireless communications may also be performed using cellular communication technologies with cellular communication standards used in the cellular communication industry.

As described with respect to FIG. 8, the software authorization agent 50 may include a gaming software transaction database. The gaming software transaction database may be used to track the distribution of gaming software on various gaming machines. For instance, in 216, a gaming software content provider may request a report regarding downloads of their gaming software from game servers to gaming machines. The software authorization agent 50 may receive the request, query the gaming software transaction database and generate a report for the gaming software content provider. This type of report may also be generated for a casino operator with many game servers distributed over gaming properties. Advantages of the gaming software transaction database is that it may provide an electronic data trail for billing, security, auditing, dispute resolution, game usage and market trending involving the transfer and the use of gaming software.

FIGURE **10** is an interaction diagram between a gaming software distributor 53, gaming software provider 51 and a software authorization agent 50 depicting an initialization of a gaming software transaction for one embodiment of the present invention. The example is provided for illustrative purposes only. A number of operations used to perform a given function in the gaming software transaction process, an order of the operations and information used in each operation may be varied and is not limited to the examples described with respect to FIGs. 10-15.

In 902, the distributor 53 generates a session request message for the transfer of gaming software and sends the session request message to the agent 50. The initial session request message may comprise gaming software information that is used by the agent 50 to authenticate the identity of the gaming device requesting the session. For instance, prior to beginning the session request, the distributor 53 and the agent 50 may have exchanged public encryption keys and other security information that may be used to establish the identity of the sender of a message to the agent 50 and to identify messages sent from the agent 50. Details of exchanging encryption keys in a secure manner which may be applied to the present invention are described in co-pending U.S. application no. 09/993,163, by Rowe et al., filed November 16, 2001 and entitled "A Cashless Transaction Clearinghouse," which are incorporated herein by reference in its entirety and for all purposes. The message request may also include additional information that is used in a later software transfer request such as a software title, information regarding the sender of the gaming software and information regarding the receiver of the gaming software. The additional information may be used by the agent 50 after the identity of the session requestor has been authenticated.

In 906, the agent 50 receives the session request message from the distributor 53. The agent 50 may attempt to validate the distributor 53 by checking information about the distributor 53, such as its licensing status and access status to the agent 50. Transfers s of gaming software may be a revocable privilege that is granted to a gaming operator. Thus, status checks of session requestor may be necessary. When the session requestor, e.g., the distributor has been validated, the agent may initialize an authentication sequence.

In 908, the agent 50 may send an authentication message containing a symmetric encryption key, K(M). K(M) is stored by the agent 50. A symmetric encryption key is used to decrypt information encrypted with the symmetric encryption key. The authentication message including K(M) and any other additional information is encrypted with a public encryption key, M(P), used by the distributor 53. M(P) was previously received, authenticated and stored by the agent 50. The public encryption key M(P) is part of a public-private asymmetric encryption key pair comprising M(P) and M(PP), where only the distributor 53 should have knowledge of the private key. In an asymmetric encryption key pair, only the private key of the encryption public-private key pair may be used to decrypt information encrypted with the public key.

In 910, when the distributor 53 receives the authentication message, it decrypts the message with its private key, M(PP) which corresponds to the public encryption key M(P). In 912, the distributor 53 generates and sends an acknowledgement message encrypted with K(M). In 914, when the agent 50 receives the acknowledgement message, it decrypts it with the session key K(M) stored in 906.

Since only the distributor has the private key M(PP) needed to decrypt K(M), when a correct acknowledgement message is received, the distributor 53 is authenticated. The agent 50 may generate and send an additional message acknowledging the distributor has been authenticated and may now proceed with a gaming software download request.

In 916 and 918, the distributor 53 may generate a software download request message and send it to the agent. The download request message may include combinations of gaming software transaction information selected from but not limited to: a) operator identification information for the gaming device to receive the gaming software, b) machine identification information for the gaming device to receive the gaming software (e.g., an identification number for a gaming machine or a game server), c) operator identification information for the gaming device that is to send the gaming software, d) machine identification information for the second gaming device, e) a gaming software title or gaming software titles to be transferred, f) a gaming software provider identifier such as a name of a company (e.g., IGT) , g) a gaming software version number, h) a gaming software identification number and i) information on gaming software currently installed on the gaming device to receive the gaming software. The download request message may be encrypted with symmetric encryption key, K(M). In addition, the download request message may be encrypted with the public encryption key of the agent 50. In one embodiment, the agent 50 may send a request to a gaming device requesting the software currently installed on the gaming device for tracking and regulatory purposes. Further, once it is determined what gaming software is installed on a plurality of gaming machine, the process of upgrading and fixing errors in gaming software may be simplified.

In 920, the agent 50 receives the download request message, decrypts the message and evaluates the request. In one embodiment, the download request information may be included in the session request message sent in 904. Thus, after authenticating and identity of the distributor 53, the agent 50 may begin processing the request in 920 without receiving additional information from the distributor 53. To evaluate the download request, the agent 50 may compare gaming software transaction information in the request message with information stored in a database. For instance, the request message may include a location, address and identification number for a gaming device that is to receive the gaming software. The agent 50 may compare this information with information from a database containing information for gaming devices that are allowed to receive gaming software downloads. The agent 50 may only authorize the download request when the gaming device identification information in the request message matches the gaming device identification information stored in the database. In another example, the request message may include gaming software identification information such as a title, version number and manufacturer. The agent 50 may only authorize the download request when the gaming software identification information in the request message matches gaming software identification information contained in a database used by the agent 50.

In 922, when the download request is approved, the software authorization agent creates a gaming software transaction record and stores the record to a gaming software transaction database. The gaming software transaction record may include but is not limited to gaming software transaction information such as: a) a symmetric encryption key, K(S), that will be used to transfer the gaming software from a first gaming device to a second gaming device, b) a time that the transaction was initiated, c) transaction expiration time, d) a destination ID number (e.g., a number identifying a casino), e) an identification number of the gaming device on which the software is to be installed, f) a gaming software identification number, g) a software title, h) a game signature for the gaming software such as from a CRC or a hash, i) a manufacturer's identification number, j) a public encryption key used by the manufacturer and k) a transaction number for the record. In some embodiments, the gaming software transaction record may include a number of permitted downloads of the gaming software. For instance, a gaming software program may be loaded to a game server. Each time the game server downloads the gaming software to a gaming machine, it may request permission from the software authorization agent 50 using the transaction number in the original record. The software authorization agent may authorize the game server to download the software to a gaming machine as long as the number of permitted downloads has not been exceeded.

In 922 and 923, the software authorization agent may send an approval message with all or a portion of the gaming software transaction information stored in the gaming software transaction record to the gaming software distributor. The message may be encrypted with the session key, K(M), generated in 906. In 924, the distributor 53 may receive the message, decrypt it using the session key, K(M), and generate an acknowledgement message. In 926, the software distributor 53 may send the acknowledgement message to the authorization agent 50. In 928, the authorization agent 50 may receive the acknowledgement and store the record for the gaming software transaction. In 930, the gaming software agent may send a notification message to the gaming software provider 51. The message may notify the gaming software content provider 51 that a gaming software transaction has been authorized that allows some of the provider's 51 to be transferred to another gaming device.

FIGURE **11** is an interaction diagram between a gaming software distributor, a gaming software provider and a software authorization agent depicting a gaming software transaction. In 850, the distributor may generate a software download request message. The download request message may include gaming software transaction information generated in the gaming software transaction request described with respect to FIG. 10. The download request message may also include a session key, K(S), encrypted with the provider's public encryption key. In 852, the distributor 53 sends the request to the provider 51. In 854, the provider 51 receives the message and decrypts the session key, K(S), with the provider's private encryption key. In 854, the provider generates an acknowledgement message encrypted with the session key K(S). In 856, the provider 51 sends the message to the distributor 53. In 857, the distributor receives the message and decrypts it with the K(S) received from the software authorization agent 50 in the authorization message.

In 859, the software provider 51 may optionally generate a download request message to validate the gaming software transaction requested by the distributor. The download request message may include gaming software transaction information, such as a transaction number, received from the distributor 53. In 858, the provider 51 may optionally send the download request message to the authorization agent 50. The message may be encrypted with the agent's public encryption key. In 860, the agent 50 may receive the download request message from the provider, decrypt it and compare the gaming software transaction information in the message with a gaming software transaction information stored in a gaming software transaction record corresponding to the request. When the request is valid, the agent 50 may generate a download reply message authorizing the provider 51 to transfer the gaming software. When the request is invalid, the agent 50 may generate a download reply message requesting the provider 51 not to send the gaming software to the distributor 53. In 864, the agent sends the download request message to the provider 51. In 862, the agent may store a record of the download request and whether it was authorized or not authorized.

In 866, the provider 51 may generate a download reply with a receipt. In one embodiment, the download reply may require the authorization of the agent 50. In another embodiment, the download reply may be sent without approval from the agent 50. The download reply may include but is not limited to a game package with the following information: 1) the requested game software, 2) the expiration date of the game or a number of plays until expiration which may be built into the gaming software, 3) a destination machine number (in some embodiments, the gaming software may be designed to operate only on a particular machine), 4) a destination address (e.g., a casino name), 5) a time stamp for the transaction, 6) a digital signature generated for the game (e.g., a CRC or a Hash of the game software), 7) the transaction number received from the distributor. The download reply may also include a separate receipt including but not limited to the following information: a) game title or identification number, b) original game transfer request data received in the request from the distributor 53, c) destination machine's identification number, d) destination address and e) a transaction number.

The download reply may be compressed to reduce the information transferred. The download reply may also include information regarding the compression algorithm used so that the destination device may properly uncompress the download reply. The download package and the download receipt may be encrypted with combinations of a public encryption key used by the destination gaming device and the session encryption key, K(S). In one embodiment, the download package and reply may be routed through the software authorization agent 50 which may perform checks on the gaming software before forwarding it to the destination gaming machine. Thus, the download package and receipt may be encrypted with the public encryption key used by the software authorization agent 50.

The download package and the download receipt may go to separate gaming devices. In one embodiment, the download package may be forwarded by the distributor 53 to a destination gaming device such as a gaming machine and the receipt may be forwarded to another gaming device for accounting purposes. In another embodiment, the receipt and download package may go to the same gaming device such as a game server operated by the gaming software distributor 53. In 868, the content provider 51 may send a receipt encrypted with the session key, K(S) to the agent 50. Since only the provider 51 and the distributor have the session key, K(S), the identity of the provider 51 may be authenticated. In 870, the agent 50 may receive the receipt, decrypt it and store gaming software transaction information contained in the receipt.

In 872, the provider sends the download reply with the gaming software and receipt to the distributor 53. In 874, the distributor 53 receives the download message, the message may be forwarded to a destination gaming device or may be stored on a game server. The destination gaming device may decrypt the download message, unpack the gaming software, which may include uncompressing the gaming software, and generate a digital signature for the gaming software. The digital signature may be generated using an algorithm such as a CRC or a Hash. In 876, the destination gaming device may send an acknowledgement message to provider indicating it has received the download message with the gaming software.

In 878, the gaming software distributor 53 generates a receipt. The receipt may include but is not limited to the following information: a) game title or identification number, b) original game transfer request data received in the request from the agent, c) destination machine's identification number, d) destination address and e) a transaction number. The receipt may be encrypted with the session encryption key, K(M), exchanged between the agent 50 in the distributor as described with respect to FIG. 10. Thus, when the agent 50 receives the receipt and decrypts it with K(M), the identity of the distributor may be authenticated.

In 879, the distributor 53 sends the receipt to the agent 50, the agent decrypts the receipt. In 880, the agent 50 may compare gaming software transaction information in the receipt received from the provider 51 in 868 with gaming software transaction information from the receipt received from the distributor 53 in 879. For example, to validate the gaming software transaction, the agent 50 may compare the digital signature for the gaming software received from the provider 51 in the receipt with the digital signature for the gaming software received from the distributor 53. When the digital signatures match, the gaming software transaction is completed and communications are terminated. As an additional check, the agent may compare the digital signatures for the gaming software with a digital signature for an approved copy of the gaming software stored in a database maintained by the agent 50. When the transaction is complete, the agent 50 may store a record of the transaction in a database. As described with respect to FIG. 9, the database may be used to track the distribution of gaming software on various gaming devices that use the authorization agent 50. Also, the records may be used for billing and auditing purposes.

In 880, when gaming software transaction information in the receipts does not match, the agent 50 may send messages to the provider 51 and the distributor 53 revoking the transaction. The message to the provider 51 may be encrypted with the session key, K(S) and the message to the distributor 53 may be encrypted with the session key, K(M). The messages may also be encrypted with public keys of public-private key pairs used by the distributor 53 and the provider 51. In response to receiving the revocation message, the content provider 51 and the distributor 53 may repeat the transaction. For example, the digital signatures for the gaming software may not match because of a transmission error. In another embodiment, the entire gaming software transaction may be revoked and the distributor 53 may have to initiate an entirely new transaction as was described with respect to FIG. 9.

FIGURE **12** is an interaction diagram between a gaming software distributor 53, a gaming machine 54 and a software authorization agent 50 depicting a gaming software transaction. In this example, the distributor 53 may be a game server operated by a casino and the gaming machine 54 may be one of a plurality of gaming machine in communication with the gaming server. The game server may have been loaded with gaming software provided by various content providers using gaming software transactions as described with respect to FIG. 11. In general, the operations shown in FIG. 12 are similar to those described with respect to FIG. 11.

In 950, the gaming machine 54 may generate a gaming software request. The gaming software request may be in response to different gaming events that occur on the gaming machine. For example, a request may be initiated when a game player using the gaming machine requests to play a game of chance currently not installed on a gaming machine. As another example, the gaming machines may include software programs that request gaming software at particular times of the day or the week. For instance, particular bonus games may only be provided on the gaming machines at certain times of the day to increase player interest. In yet another example, a software request may be generated when a game license (see FIGs. 6 and 7) installed on a gaming machine has expired.

In 952, the gaming machine 54 sends the software transfer request to the distributor 53 which in this case is a game server. In 954, the distributor 53 receives the gaming software request message and generates an acknowledgement message. The message may or may not be decrypted. When the gaming machine and the game server communicate via a private local area network, such as within a casino, encryption procedures may not be necessary. However, the game server may communicate with a gaming machine located at different gaming properties, such as stores, via a virtual private network, as was described with respect to FIG. 3. In this case, encryption procedures such as the use of public-private key pairs and symmetric encryption keys may be used. In 956, the distributor 53 sends the acknowledgement message to the gaming machine 54. In 957, the gaming machine 54 receives the acknowledgement message and may authenticate the sender of the message.

In another embodiment of the present invention, the gaming software download request may be initiated by the game server. For example, the game server may be used to regularly redistribute gaming software on gaming machine distributed on a gaming floor according to perceived customer desires and market trends. A market trend may be a "hot" game that is desired by a lot of customers. Further, the gaming server may be also used to provide regularly software upgrades and error fixes to gaming software executed on various gaming machines. The software upgrades and error fixes may be prompted by notices of upgrades and fixes received from a content provider. When the distributor 53 initiates the gaming software transaction, the gaming machine 54 may be simply sent the gaming software. An authentication process may or may not proceed the game server sending the gaming software to the gaming machine.

In 959, the distributor 53 may generate a download request message for the requested gaming software. The request message may have been initiated by the gaming machine 54 or the distributor 53. In 958, the distributor sends the download request to the agent 50. In 960, the agent 50 may generate a reply message that authorizes or denies the transaction and store a record of the gaming software transaction 962. In some embodiments, the distributor 53 may simply send a record of the gaming software transaction to the agent but not ask for or expect an approval message from the agent 50. The agent 50 may store this record. In another embodiment, the agent 50 may have previously approved a certain number of gaming software transfers and may determine if additional downloads are available.

In 964, the distributor receives the download reply from the agent 50. When an authorization has been requested and it has been approved, the gaming distributor 53 may generate a download reply message containing the gaming software. In this embodiment, a receipt may not be required since the gaming software downloaded to the gaming distributor may have already been approved by the agent 50 in a previous gaming software transaction. In 972, the download reply with the gaming software is sent to the gaming machine 54. In 974, the gaming machine receives the download reply and may decrypt and unpack the gaming software. The gaming machine may also calculate one or more digital signatures for the gaming software which may be used to validate that the software has been successfully transferred. In 976, the gaming machine 54 may send an acknowledgement message to the game server of the distributor 53 that it has received the requested gaming software. The gaming machine 54 may also store a gaming software transaction record of the gaming software download in a non-volatile memory device. The gaming software transaction record may be used for used for auditing and security purposes.

Optionally, in 978, the gaming machine 54 may generate a receipt or some other type of acknowledgement message that it has received the gaming software and send it to the authorization agent 50. In 968, the game server of the distributor 53 may also send a receipt or acknowledgement message to the agent 50. In 970 and 980, the agent 50 may receive the acknowledgement messages from the gaming machine 50 and the distributor 53 and store a record of the gaming software transaction. The agent may also use gaming software transaction information included with the acknowledgement messages to determine if the gaming software transaction has been correctly carried out.

FIGURE 13 is flow chart depicting a method in a software authorization agent initializing a gaming software transaction. In 1000, the agent receives a gaming software transaction session request message from a gaming software distributor or another gaming entity desiring a transfer of gaming software. The transfer of gaming software may be implemented electronically or manually. In a manual transmission, the gaming software may be shipped to the distributor and loaded locally onto a gaming device, such as a gaming machine. In 1002, the authorization may check to determine if the requestor identified in the message is in a local of database of gaming entities that are authorized to request transfers of gaming software. When the requestor is not in the database, in 1004, the agent may terminate the transaction and generate a record of the attempted transaction and store the record. Records of failed transactions may be analyzed for security purposes.

When the requestor is in a local database, the agent may generate a symmetric encryption key that may be used to encrypt messages sent between the agent and the requestor and store the symmetric encryption key. Further, for authentication purposes, the agent may encrypt the symmetric encryption key with a public encryption key used by the requestor and send a message with the encrypted symmetric encryption key to the requestor. In one embodiment, prior to the session request, the requestor and the agent may have exchanged public encryption keys of public-private encryption key pairs. In 1008, the agent receives a reply message from the requestor. The message may contain a symmetric encryption key encrypted with the agents public key. The agent decrypts the symmetric encryption key with the agent's private key.

In 1010, the agent compares the symmetric encryption key to the symmetric encryption key sent to the requestor in 1006. When the encryption keys agree, the identity of the requestor is assumed to be authenticated. In addition to a symmetric encryption key, other types of information, such as passwords or random bits, may be encrypted and exchanged between the requestor and agent. The other types of exchanged information may be compared as part of the authentication process. When the requestor is not authenticated, in 1004, the transaction is terminated and a record of the failed transaction may be generated.

When the identity of the requestor is authenticated, in 1012, the agent may evaluate and validate one or more parts of a download request for gaming software from the requestor. For instance, the agent may determine if a requested gaming software title has been approved for downloads or transfers. As another example, the download request may include identification information for a gaming device that will receive the requested gaming software. The agent may compare identification information for the destination gaming device with identification information from a database of gaming devices approved for receiving gaming software. In 1014, when the information in the download request is not valid, the agent may generate an error message and it to the requestor. The error message may indicate detected errors in the request such as missing information or a request for a gaming software title unknown to the agent.

In 1016, when information in the download request has been validated, the agent may generate an authorization record for the gaming software transaction as previously described with respect to FIG. 9. The agent may also generate an acknowledgement message and send it to the requestor. In 1018, the agent may check to determine whether a reply has been received for the acknowledgement message. In 1014, when an acknowledgement reply message has not been received, the agent may generate an error message and send it to the requestor. In 1020, when the acknowledgement reply message has been received, the agent may store a record of the authorized transaction to a database. In one embodiment, the agent may also notify a software content provider that has been authorized to transfer the gaming software of the pending gaming software transaction that has been authorized.

FIGURE **14** is flow chart depicting a method in a software authorization agent of authorizing a gaming software transaction. In 1100, the agent receives a gaming software transfer request form a gaming device. The transfer request may describe a gaming software transaction previously generated and authorized by the agent. The gaming device may be a game server, a gaming machine or any other gaming device that is allowed to receive gaming software. Further, the gaming device may request a transfer of the gaming software to another gaming device different from itself. For instance, a game server may request a transfer of gaming software to a gaming machine. In 1102, the agent may determine whether the transfer request is a valid gaming software transaction. For example, the transfer request may contain a transaction number and the agent may use this transaction number to locate a gaming software transaction record including gaming software transaction information describing the transaction. The agent may compare the information from the gaming software transaction record with gaming software transaction information contained in the transfer request. The transaction record may also include status information such as whether the transaction has been completed or is pending and an expiration date for the transaction, which may be checked by the agent.

In 1104, when the gaming software transaction is invalid the agent denies the transfer request, may send an error message and may also store a record of the denied transfer request. In 1106, when the gaming software transaction has been validated, the agent may change the status of the transaction to pending and store the status. In 1108, the agent may send a transfer reply to the gaming device requesting the gaming device to proceed with the transaction. In 1110, the agent may receive acknowledgement messages from the gaming device that has sent the gaming software (e.g., a content provider) and from the gaming device that has received the gaming software (e.g., a gaming machine or a game server). The acknowledgement messages may include information about the transferred gaming software. For example, the acknowledgement message may include a digital game signature for the gaming software generated by the both the sender and the receiver of the gaming software.

In 1112, the agent may validate the transaction by comparing gaming software transaction information received from both the receiver and the sender of the gaming software. For instance, the agent may compare digital signatures for the gaming software generated by the sender and the receiver. In 1114, when the transaction is invalid, the agent may change the status of the transaction from pending and generate an error message. The error message may be sent to the requestor of the gaming software and the sender of the gaming software and identify any deficiencies detected by the agent. In 1116, when the transaction is valid, the agent may change the status of the transaction to downloaded and store additional information in the transaction record such as the time that the transaction was completed. In 1118, the agent may optionally notify the requestor of the gaming software and the provider of the gaming software that the transaction has been successfully completed. In some embodiments, the agent may even bill the requestor of the gaming software and arrange for an electronic fund transfer or other payment method.

FIGURE **15** is a block diagram of an interface 1200 used to provide information about gaming software transactions generated by a software authorization agent. The interface menu 1210 may allow a user to view information in different formats, perform queries of a gaming software transaction and perform other operations on gaming software transaction data such as analyzing market trends. The interface may be used from a remote site to access gaming software transaction stored in a database. The access to the gaming software transaction database may be limited according to the identity of a particular user. For example, a gaming regulatory agency maintaining the transaction database may be able to look at all of the gaming software transactions stored in a database. A gaming software content provider may be able to access transactions involving the transfer of their gaming software. A gaming entity such as a casino operator may be able to access transactions involving gaming devices operated by the casino.

In 1202, 1204, 1206 and 1208, a few examples of plots that may be derived form a gaming software transaction database are shown. The plots are shown for illustrative purposes only and are not limited to the examples shown in the figure. In 1202, a total number of game downloads as a function of location are shown. This type of plot may be generated for a gaming entity with gaming devices at locations A, B, C and D or even a content provider that provides gaming software to each of these locations via gaming software transactions. In 1204, a number of game downloads as a function of time are plotted for property A. The plot shows the variation in game downloads from month to month. In 1206, a gaming software distribution for five different types of games at property A are shown. As described with respect to FIG. 9, if an initial distribution of gaming software on different gaming devices are known, then the gaming software transaction records may be used to track the distribution of games on the gaming devices. In 1208, a game distribution for the five different types of games is shown across multiple gaming properties.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, while the gaming machines of this invention have been depicted as having top box mounted on top of the main gaming machine cabinet, the use of gaming devices in accordance with this invention is not so limited. For example, gaming machine may be provided without a top box.

What is claimed is:

1. In a software authorization agent, a method of generating a gaming software transaction record used to facilitate a transfer of gaming software between two gaming devices, the method comprising:

receiving a gaming software transaction request from a first gaming device;

authenticating an identity of the first gaming device;

generating a gaming software transaction record comprising gaming software transaction information that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on the gaming machine.

2. The method of claim 1, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

3. The method of claim 1, wherein the first gaming device is at least one of a gaming machine, game server and combinations thereof.

4. The method of claim 1, wherein the gaming software transaction request comprises access information and gaming software identification information.

5. The method of claim 4, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

6. The method of claim 4, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

7. The method of claim 1, further comprising:

comparing access information in the gaming software transaction request with access information stored in a database.

8. The method of claim 7, when the compared access information does not match the access information stored in the database,

denying the gaming software transaction request.

9. The method of claim 1, further comprising:

comparing gaming software identification information in the gaming software transaction request with gaming software identification information stored in a database.

10. The method of claim 9, when the gaming software identification information does not match the access information stored in the database,

denying the gaming software transaction request.

11. The method of claim 1, further comprising:

generating an identification sequence;

encrypting the identification sequence with a public encryption key for the first gaming device wherein information encrypted with the public encryption key is decrypted with a private encryption key used by the first gaming device;

sending the encrypted identification sequence to the first gaming device.

12. The method of claim 11, wherein the identification sequence is a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device.

13. The method of claim 11, further comprising:

receiving from the first gaming device a second identification sequence encrypted with a public encryption key used by the software authorization agent,

decrypting the second identification sequence with a private encryption key corresponding to the public encryption key used by the software authorization agent;

comparing the second identification sequence to the identification sequence sent to the first gaming device to authenticate the identity of the first gaming device.

14. The method of claim 13, wherein the second identification sequence is a symmetric encryption key used to transfer gaming software between the first gaming device and the second gaming device.

15. The method of claim 13, when the second identification sequence received from the first gaming device does not match the identification sequence sent to the first gaming device;

denying the gaming software transaction request.

16. The method of claim 1, wherein the gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number, a gaming software identification number, a gaming software provider identifier, a transaction number, a number of allowable downloads and combinations thereof.

17. The method of claim 1, further comprising:

storing the gaming transaction record information to a transaction database.

18. The method of claim 1, further comprising:

sending gaming software transaction information to the first gaming device.

19. The method of claim 18, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

20. The method of claim 1, further comprising:

sending a notification message to a gaming software provider identified in the gaming software request of a pending gaming software download request.

21. The method of claim 1, wherein the software authorization agent communicates with the first gaming device using an local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

22. The method of claim 1, wherein the software authorization agent and the first gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

23. The method of claim 1, wherein the transfer of gaming software is performed at least one of manually and electronically.

24. The method of claim 1, wherein the gaming software comprises one or more gaming software components for the game of chance, the bonus game of chance, the device driver, the player tracking service and the operating system.

25. The method of claim 1, wherein the gaming software is used to upgrade a gaming software component on the first gaming device.

26. The method of claim 1, wherein the gaming software is used to correct an error in a gaming software component on the second gaming device.

27. The method of claim 1, further comprising:

requesting a list of gaming software installed on a gaming device.

28. In a software authorization agent, a method of regulating a transfer of gaming software between two gaming devices, the method comprising:

receiving a gaming software download request message with gaming software transaction information from a first gaming device;

validating the gaming software download request using the gaming software transaction information;

sending an authorization message to the first gaming device authorizing the first gaming device to transfer gaming software to a second gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

29. The method of claim 28, wherein the second gaming device is at least one of a game server and a gaming machine.

30. The method of claim 28, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

31. The method of claim 28, wherein the gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a

transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and combinations thereof.

32. The method of claim 28, further comprising:

comparing the gaming transaction information in the gaming software download request message with gaming transaction information stored in a transaction database to validate the gaming software download request.

33. The method of claim 28, further comprising:

sending a message to the first gaming device denying authorization for the first gaming device to transfer gaming software to the second gaming device.

34. The method of claim 28, further comprising:

decrypting the download request message.

35. The method of claim 28, further comprising:

receiving a first download acknowledgement message from the first gaming device and receiving a second download acknowledgement message from the second gaming device.

36. The method of claim 35, further comprising:

comparing gaming software transaction information in the first download acknowledgement message with gaming software transaction information in the second download acknowledgement message to validate that the gaming software has been correctly transferred.

37. The method of claim 36, wherein the gaming software transaction information in the first download acknowledgement message includes at least a first digital signature determined for the gaming software and the gaming software transaction information in the second download acknowledgement message includes at least a second digital signature determined for the gaming software.

38. The method of claim 28, wherein the first gaming device a game server in communication with one or more gaming machines and the second gaming device is a gaming machine.

39. The method of claim 28, wherein the first gaming device is a game server maintained by a gaming software provider and the second gaming device is a game server in communication with one or more gaming machines.

40. The method of claim 28, wherein the first gaming device is a game server maintained by a gaming software provider and the second gaming device is a gaming machine.

41. The method of claim 28, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

42. The method of claim 28, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

43. The method of claim 28, further comprising:

receiving the gaming software from the first gaming device;

validating the gaming software; and

sending the gaming software to the second gaming device.

44. The method of claim 43, further comprising:

determining a digital signature for the gaming software; and

comparing the digital signature with an approved digital signature for the gaming software stored in a database to validate the gaming software.

45. The method of claim 28, further comprising:

storing gaming software transaction information indicating that a status of the download request.

46. The method of claim 28, wherein the status is at least one of authorized, pending, completed and void.

47. The method of claim 28, wherein the transfer of gaming software is performed at least one of manually and electronically.

48. The method of claim 28, wherein the gaming software comprises one or more gaming software components for the game of chance, the bonus game of chance, the device driver, the player tracking service and the operating system.

49. The method of claim 28, wherein the gaming software is used to upgrade a gaming software component on the second gaming device.

50. The method of claim 28, wherein the gaming software is used to correct an error in a gaming software component on the second gaming device.

51. The method of claim 28, further comprising:

requesting a list of gaming software installed on a gaming device.

52. In a software authorization agent, a method of providing gaming software transaction information, the method comprising:

receiving a gaming software transaction information request from a gaming device;

authenticating an identity of the gaming device;

querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device, said gaming software transaction database comprising a plurality of records of gaming software transactions; and

sending the requested gaming software transaction information to the gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

53. The method of claim 52,

wherein each gaming software transaction record includes gaming software transaction information that describes a transfer of gaming software from a first gaming device to a second gaming device.

54. The method of claim 52,

wherein the gaming software transaction database includes a record of gaming software installed on one or more gaming devices.

55. The method of claim 52, wherein the gaming software transaction database includes a record of gaming software usage on one or more gaming devices.

56. The method of claim 52, wherein the gaming transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time.

57. The method of claim 52, further comprising:

generating a gaming transaction report that presents the set of gaming software transaction requested by the gaming device.

58. The method of claim 52, further comprising:

generating a distribution of gaming software on a plurality of gaming machines at a specified time using the gaming software transaction information stored in the gaming software transaction database.

59. The method of claim 52, further comprising:

generating a distribution of gaming software on a plurality of gaming machines for a plurality of times using the gaming software transaction information stored in the gaming software transaction database.

60. The method of claim 52, further comprising:

generating a billing report.

61. The method of claim 60, further comprising:

generating a fee for the billing report based upon a number of times a first gaming software has been used on the gaming device.

62. The method of claim 61, wherein a usage fee charged each time the first gaming software is used varies with time.

63. The method of claim 52, further comprising:

requesting a list of gaming software installed on the gaming device.

64. The method of claim 63, further comprising:

storing the list of gaming software installed on the gaming device to the gaming software transaction database.

65. In a first gaming device, a method of requesting a transfer of gaming software from a second gaming device, said method comprising:

generating a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and

receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

66. The method of claim 65, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

67. The method of claim 65, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

68. The method of claim 65, wherein the gaming software transaction request comprises access information and gaming software identification information.

69. The method of claim 68, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

70. The method of claim 68, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider

identifier, a gaming software version number and a gaming software identification number.

71. The method of claim 65, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

72. The method of claim 65, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

73. The method of claim 65, further comprising:
sending authentication information used to identify the first gaming device to the gaming software authorization agent.

74. The method of claim 65, further comprising:
sending a message requesting the gaming software to the second gaming device.

75. The method of claim 65, further comprising:
receiving the gaming software from the second gaming device.

76. The method of claim 75, further comprising:
determining a digital signature for the gaming software and
sending a message with at least the digital signature to the gaming software authorization agent.

77. The method of claim 65, further comprising:
authenticating an identity of the second gaming device.

78. The method of claim 65, wherein the first gaming device is a gaming machine and the second gaming device is a game server.

79. The method of claim 65, wherein the first gaming device is a game server in communication with a plurality of gaming machines and the second gaming device is a game server maintained by a gaming software content provider.

80. The method of claim 65, wherein the transfer of gaming software is performed at least one of manually and electronically.

81. The method of claim 65, wherein the gaming software comprises one or more gaming software components.

82. The method of claim 65, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

83. The method of claim 65, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

84. In a first gaming device, a method of transferring gaming software to a second gaming device, said method comprising:

receiving a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software; and

transferring the gaming software to the second gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

85. The method of claim 84, further comprising:

receiving an approval of the gaming software transaction request from the gaming software authorization agent.

86. The method of claim 84, further comprising:

prior to transferring the gaming software, receiving a denial of the gaming software transaction request from the gaming software authorization agent; and

terminating the transfer of the gaming software.

87. The method of claim 84, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local

area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

88. The method of claim 84, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection, an infrared communication connection and combinations thereof.

89. The method of claim 84, wherein the gaming software transaction request comprises access information and gaming software identification information.

90. The method of claim 89, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

91. The method of claim 89, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

92. The method of claim 84, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

93. The method of claim 84, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

94. The method of claim 84, further comprising:

determining a digital signature for the gaming software and

sending a message with at least the digital signature to the gaming software authorization agent.

95. The method of claim 84, wherein the first gaming device is a gaming server and the second gaming device is a gaming machine.

96. The method of claim 84, wherein the first gaming device is a gaming machine and the second gaming device is a gaming machine.

97. The method of claim 84, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a game server maintained by a gaming entity.

98. The method of claim 84, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a gaming machine maintained by a gaming entity.

99. The method of claim 84, wherein the transfer of gaming software is performed at least one of manually and electronically.

100. The method of claim 84, wherein the gaming software comprises one or more gaming software components.

101. The method of claim 84, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

102. The method of claim 84, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

103. A software authorization agent for facilitating the transfer of gaming software between a plurality of gaming devices, the software authorization agent comprising:

a network interface allowing the authorization agent to communicate with each of the plurality of gaming devices; and

a processor configured or designed to (i) receive gaming software transfer requests via the network interface from a first gaming device for the transfer of gaming software from a second gaming device to a third gaming device (ii) approve or reject the gaming software transaction request

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

104. The software authorization agent of claim 103, further comprising:
a transaction database containing gaming software transaction information.

105. The software authorization agent of claim 104, wherein the gaming software transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time.

106. The software authorization agent of claim 105, further comprising a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software distribution reports based upon the gaming software transaction information.

107. The software authorization agent of claim 105, further comprising:
a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software billing reports based upon the gaming software transaction information.

108. The software authorization agent of claim 103, further comprising:
a database storing public encryption keys for one or more of the plurality of gaming devices.

109. The software authorization agent of claim 103, further comprising:
a database storing identification information for one or more of the plurality of gaming devices.

110. The software authorization agent of claim 103, further comprising:
a database storing identification information for the gaming software that is transferred from the second gaming device to the third gaming device.

111. The software authorization agent of claim 110, wherein the identification information for the gaming software is a digital signature, a title, a manufacturer, an identification number and combinations thereof.

112. The software authorization agent of claim 103, wherein the first gaming device is a hand-held computing device, the second gaming device is a portable memory device storing the gaming software and the third gaming device is a gaming machine.

113. The software authorization agent of claim 103, wherein the first gaming device is a first gaming machine, the second gaming device is a second gaming machine and the third gaming device is the first gaming machine.

114. The software authorization agent of claim 103, wherein the first gaming device is a first game server, the second gaming device is a second game server and the third gaming device is a first gaming machine.

115. The software authorization agent of claim 103, wherein the first gaming device is a first game server, the second gaming device is a second game server and the third gaming device is the first game server.

116. The software authorization agent of claim 103, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

117. The software authorization agent of claim 103, wherein the software authorization agent, the first gaming device, the second gaming device and the third gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

118. The software authorization agent of claim 103, wherein the software authorization agent, the first gaming device, the second gaming device and the third gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

119. The software authorization agent of claim 103, wherein the transfer of gaming software is performed at least one of manually and electronically.

120. The software authorization agent of claim 103, wherein the gaming software comprises one or more gaming software components.

121. The software authorization agent of claim 103, wherein the gaming software is used to upgrade a gaming software component on one of the gaming devices.

122. The software authorization agent of claim 103, wherein the gaming software is used to correct an error in a gaming software component on one of the gaming devices.

123. A first gaming device comprising:

a network interface allowing communications between the first gaming device, a software authorization agent and one or more other gaming devices; and

a processor configured or designed to (i) send a request for the transfer of gaming software from a second gaming device to a third gaming device via the network interface to the software authorization agent (ii) receive from the software authorization agent a reply approving or rejecting the request for the transfer of the gaming software

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

124. The first gaming device of claim 123, further comprising:

a memory device that stores gaming software.

125. The first gaming device of claim 123, further comprising:

a master gaming controller that controls a game of chance played on the first gaming device.

126. The first gaming device of claim 123, further comprising:

a memory device that stores public encryption keys for one or more of the plurality of gaming devices and the software authorization agent.

127. The first gaming device of claim 123, wherein the network interface is connected to at least one of a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

128. The first gaming device of claim 123, wherein the network interface provides at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

129. The first gaming device of claim 123, wherein the first gaming device is a portable gaming device.

130. The first gaming device of claim 123, wherein the first gaming device is a first gaming machine, the second gaming device is a second gaming machine and the third gaming device is the first gaming machine.

131. The first gaming device of claim 123, wherein the first gaming device is a first game server, the second gaming device is a second game server and the third gaming device is a first gaming machine.

132. The first gaming device of claim 123, wherein the first gaming device is a first game server, the second gaming device is a second game server and the third gaming device is the first game server.

133. The first gaming device of claim 123, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

134. The first gaming device of claim 123, wherein the gaming software comprises one or more gaming software components.

135. The first gaming device of claim 123, wherein the gaming software is used to upgrade a gaming software component on one of the gaming devices.

136. The first gaming device of claim 123, wherein the gaming software is used to correct an error in a gaming software component on one of the gaming devices.

SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

ABSTRACT OF THE DISCLOSURE

A disclosed gaming machine may securely communicate with devices over a public network such as the Internet. The gaming machine utilizes a combination of symmetric and asymmetric encryption that allows a single gaming machine to securely communicate with a remote server using a public network. The secure communication methods may be used to transfer gaming software and gaming information between two gaming devices, such as between a game server and a gaming machine. For regulatory and tracking purposes, the transfer of gaming software between the two gaming devices may be authorized and monitored by a software authorization agent.

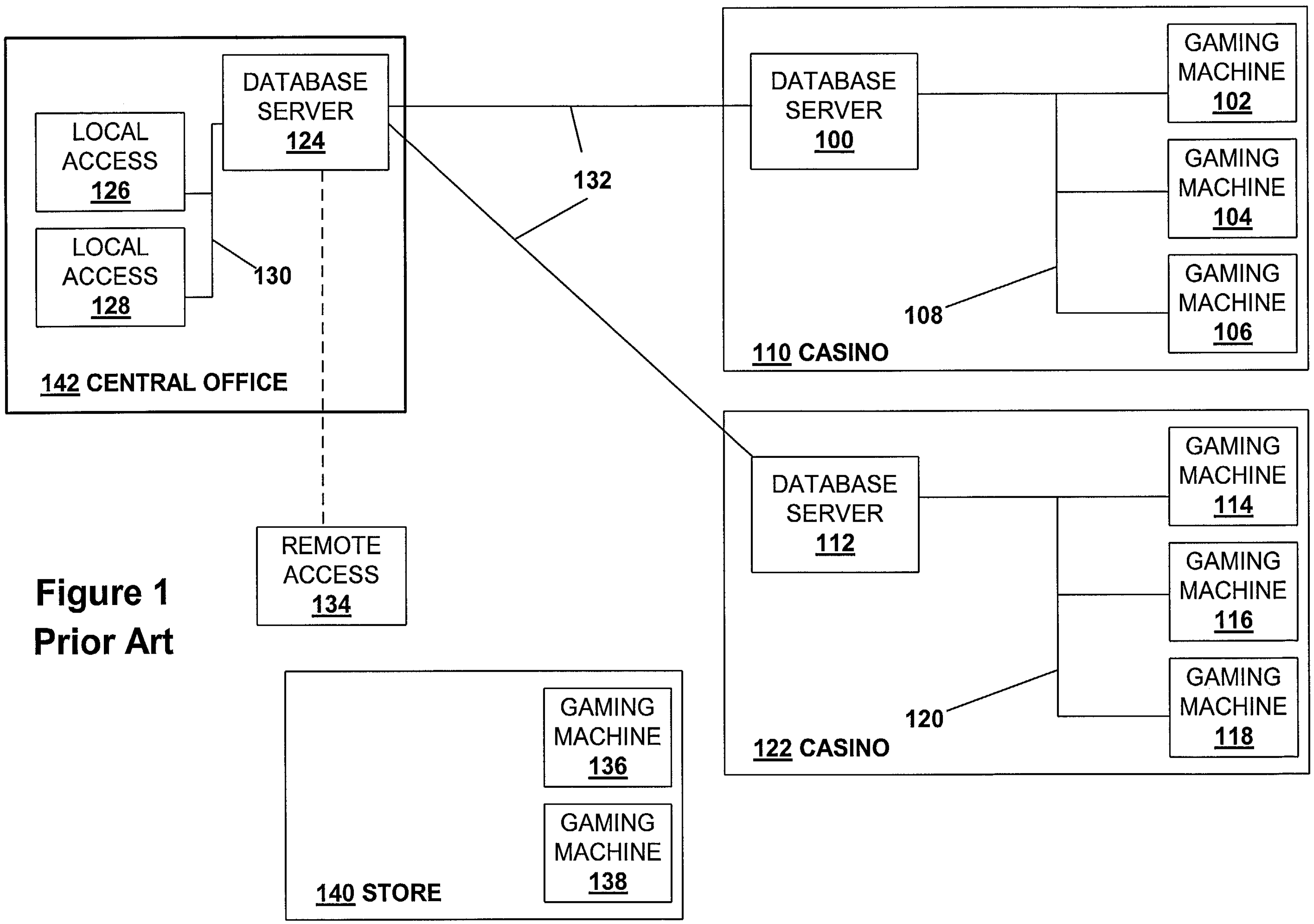


Figure 1
Prior Art

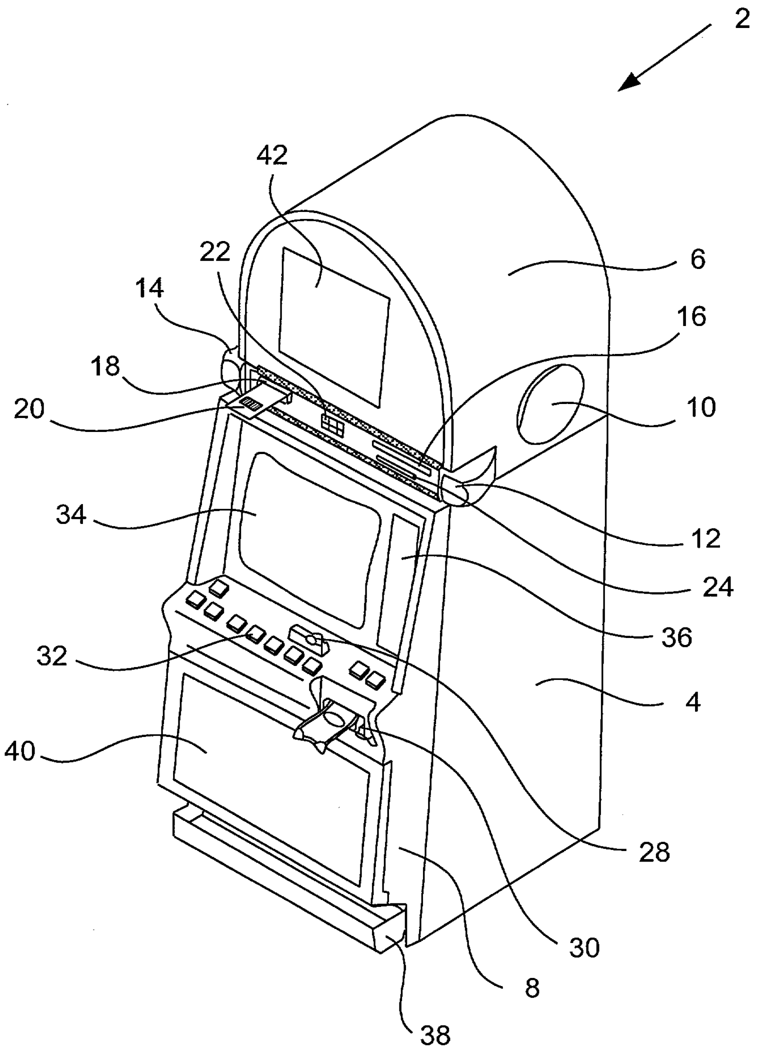


FIGURE 2

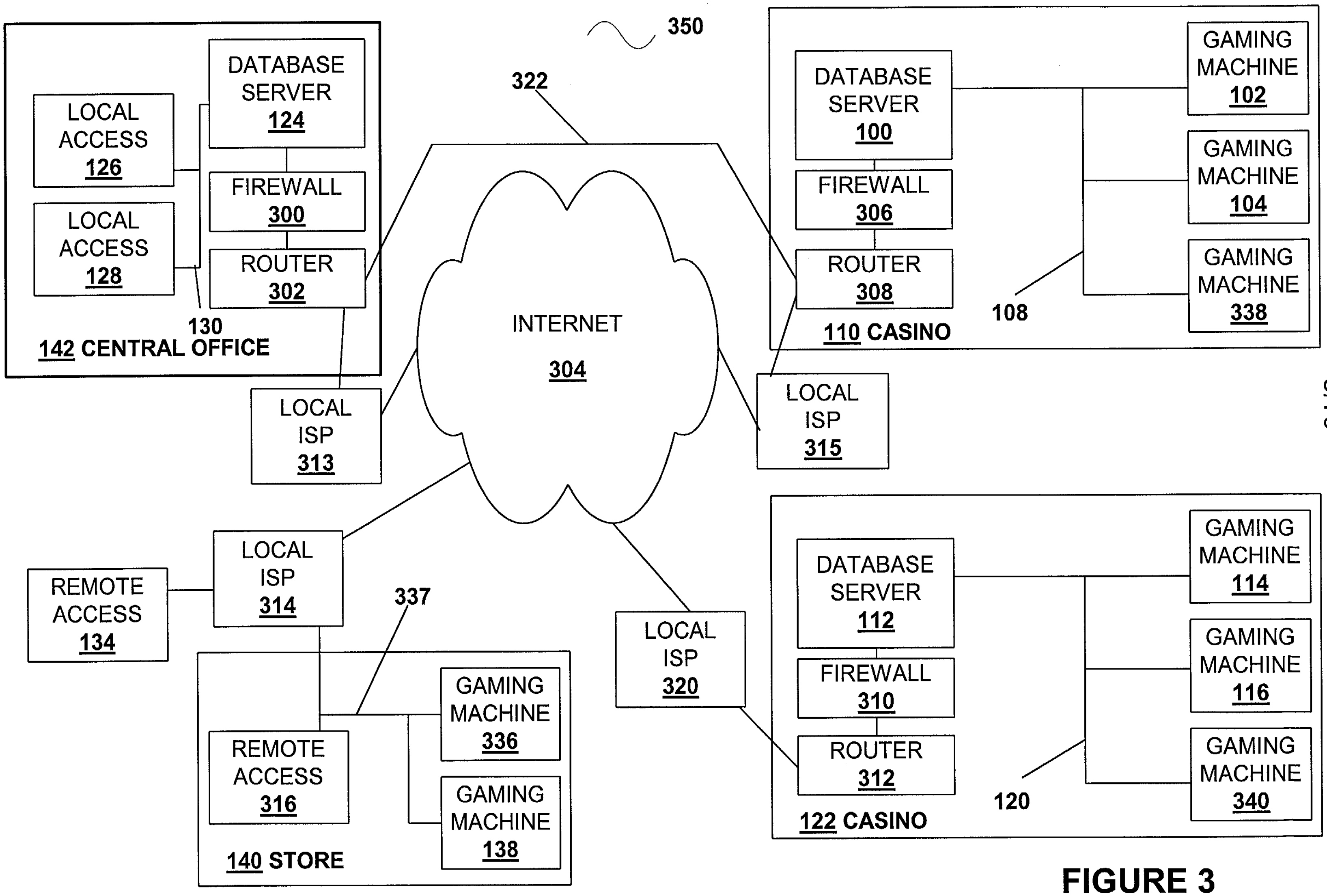

350
322
LOCAL ACCESS 126
LOCAL ACCESS 128
DATABASE SERVER 124
FIREWALL 300
ROUTER 302
130
142 CENTRAL OFFICE
LOCAL ISP 313
INTERNET 304
DATABASE SERVER 100
FIREWALL 306
ROUTER 308
110 CASINO
GAMING MACHINE 102
GAMING MACHINE 104
GAMING MACHINE 338
108
LOCAL ISP 315
REMOTE ACCESS 134
LOCAL ISP 314
337
REMOTE ACCESS 316
GAMING MACHINE 336
GAMING MACHINE 138
140 STORE
LOCAL ISP 320
DATABASE SERVER 112
FIREWALL 310
ROUTER 312
122 CASINO
GAMING MACHINE 114
GAMING MACHINE 116
GAMING MACHINE 340
120

FIGURE 3

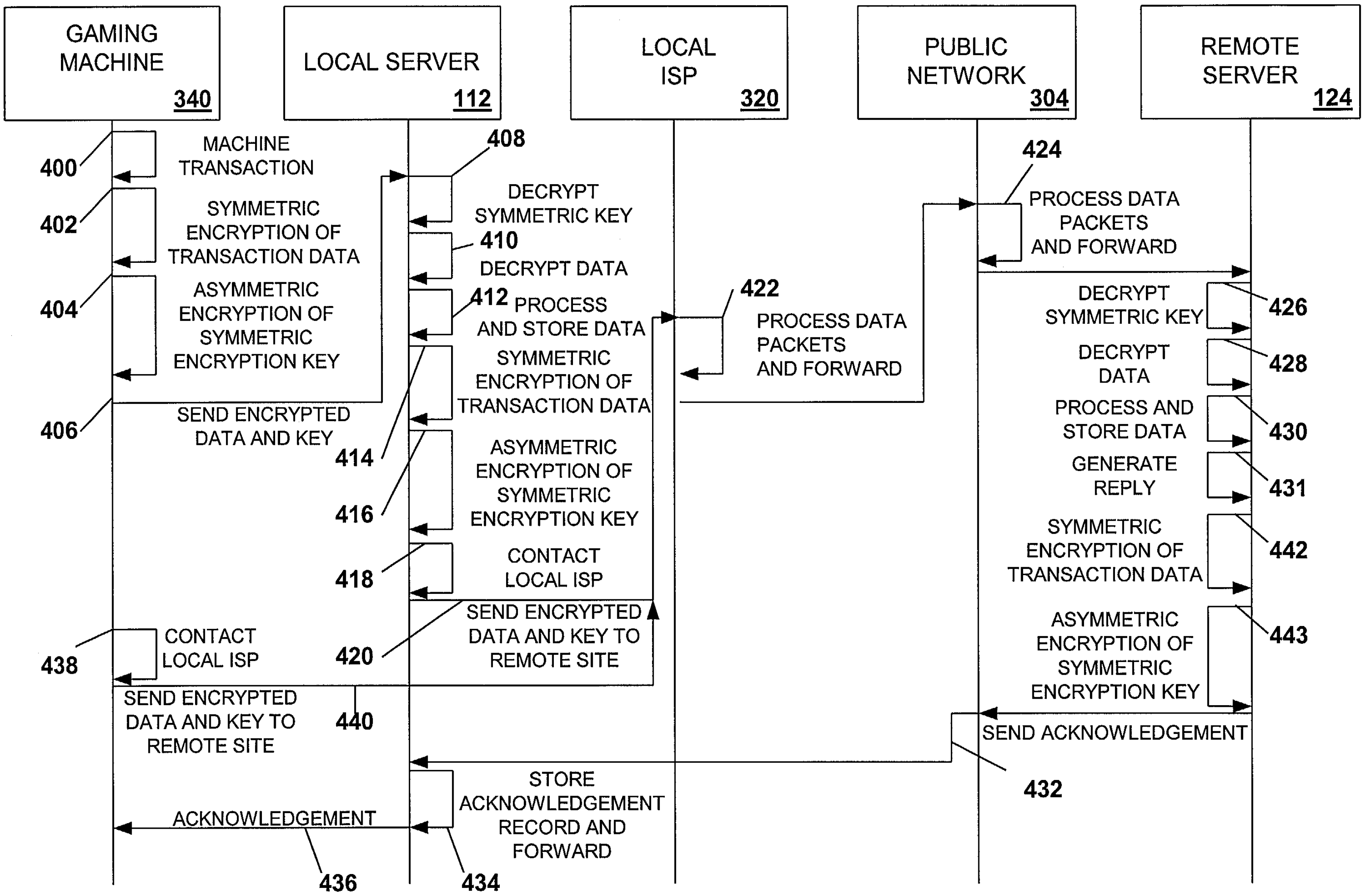

GAMING MACHINE 340
LOCAL SERVER 112
LOCAL ISP 320
PUBLIC NETWORK 304
REMOTE SERVER 124
400
MACHINE TRANSACTION
402
SYMMETRIC ENCRYPTION OF TRANSACTION DATA
404
ASYMMETRIC ENCRYPTION OF SYMMETRIC ENCRYPTION KEY
406
SEND ENCRYPTED DATA AND KEY
408
DECRYPT SYMMETRIC KEY
410
DECRYPT DATA
412
PROCESS AND STORE DATA
414
SYMMETRIC ENCRYPTION OF TRANSACTION DATA
416
ASYMMETRIC ENCRYPTION OF SYMMETRIC ENCRYPTION KEY
418
CONTACT LOCAL ISP
420
SEND ENCRYPTED DATA AND KEY TO REMOTE SITE
422
PROCESS DATA PACKETS AND FORWARD
424
PROCESS DATA PACKETS AND FORWARD
426
DECRYPT SYMMETRIC KEY
428
DECRYPT DATA
430
PROCESS AND STORE DATA
431
GENERATE REPLY
442
SYMMETRIC ENCRYPTION OF TRANSACTION DATA
443
ASYMMETRIC ENCRYPTION OF SYMMETRIC ENCRYPTION KEY
SEND ACKNOWLEDGEMENT
432
438
CONTACT LOCAL ISP
SEND ENCRYPTED DATA AND KEY TO REMOTE SITE
440
STORE ACKNOWLEDGEMENT RECORD AND FORWARD
434
ACKNOWLEDGEMENT
436

FIGURE 4

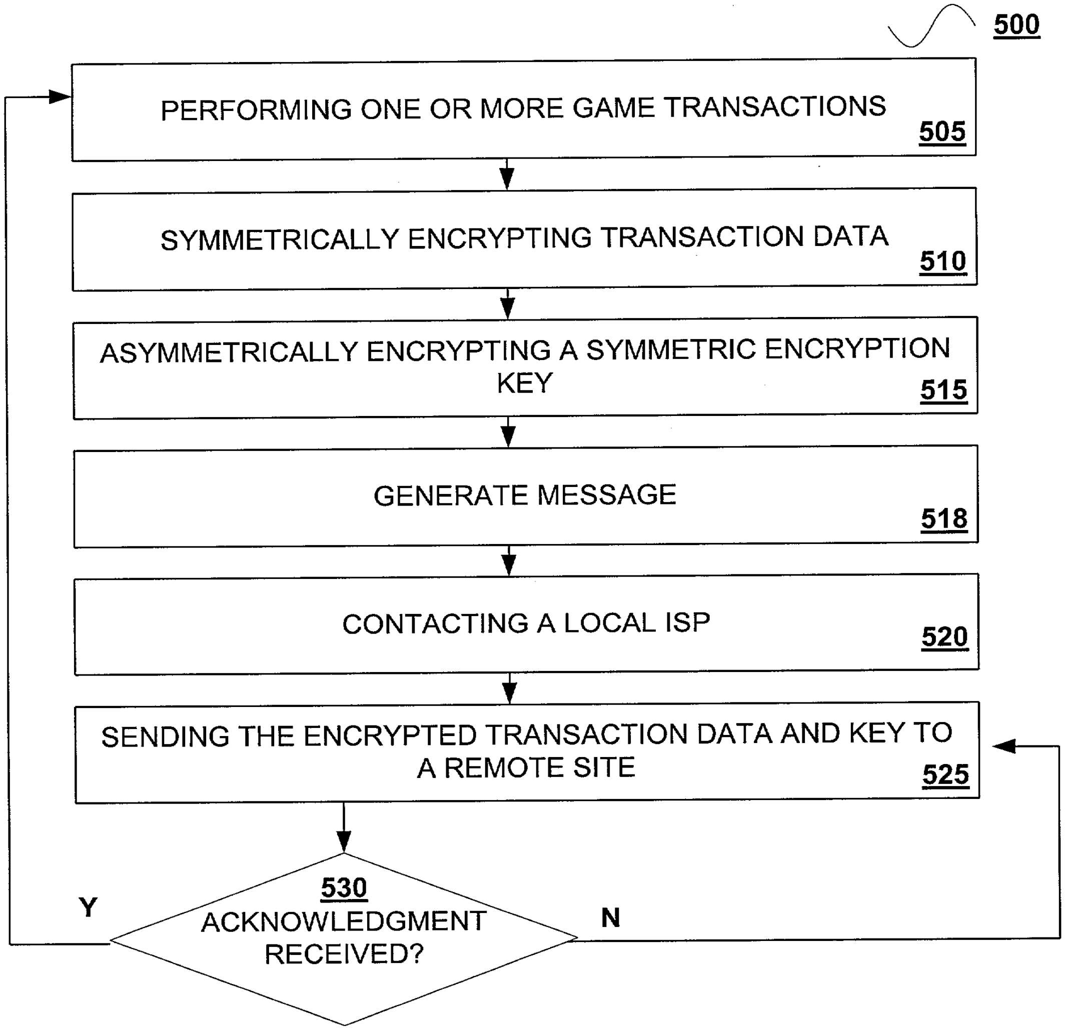

500
PERFORMING ONE OR MORE GAME TRANSACTIONS
505
SYMMETRICALLY ENCRYPTING TRANSACTION DATA
510
ASYMMETRICALLY ENCRYPTING A SYMMETRIC ENCRYPTION KEY
515
GENERATE MESSAGE
518
CONTACTING A LOCAL ISP
520
SENDING THE ENCRYPTED TRANSACTION DATA AND KEY TO A REMOTE SITE
525
530
ACKNOWLEDGMENT RECEIVED?
Y
N

FIGURE 5A

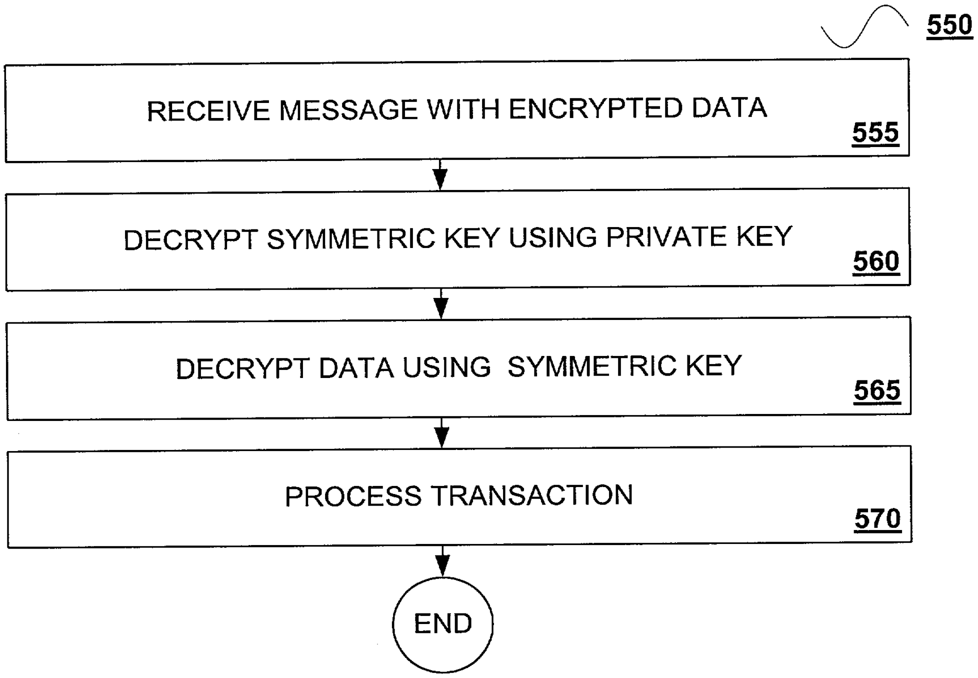

550
RECEIVE MESSAGE WITH ENCRYPTED DATA
555
DECRYPT SYMMETRIC KEY USING PRIVATE KEY
560
DECRYPT DATA USING SYMMETRIC KEY
565
PROCESS TRANSACTION
570
END

FIGURE 5B

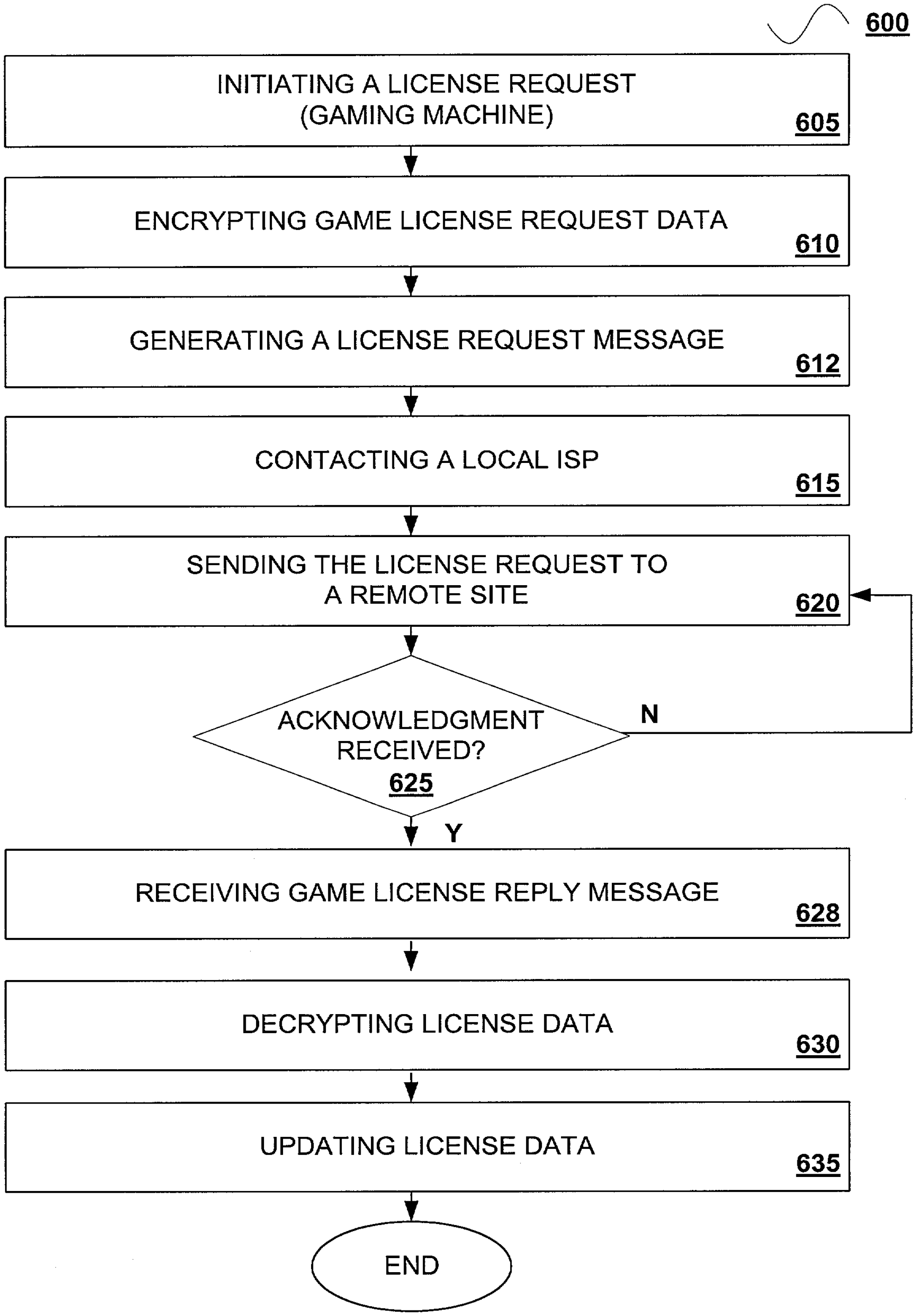

600
INITIATING A LICENSE REQUEST (GAMING MACHINE)
605
ENCRYPTING GAME LICENSE REQUEST DATA
610
GENERATING A LICENSE REQUEST MESSAGE
612
CONTACTING A LOCAL ISP
615
SENDING THE LICENSE REQUEST TO A REMOTE SITE
620
ACKNOWLEDGMENT RECEIVED?
625
N
Y
RECEIVING GAME LICENSE REPLY MESSAGE
628
DECRYPTING LICENSE DATA
630
UPDATING LICENSE DATA
635
END

FIGURE 6

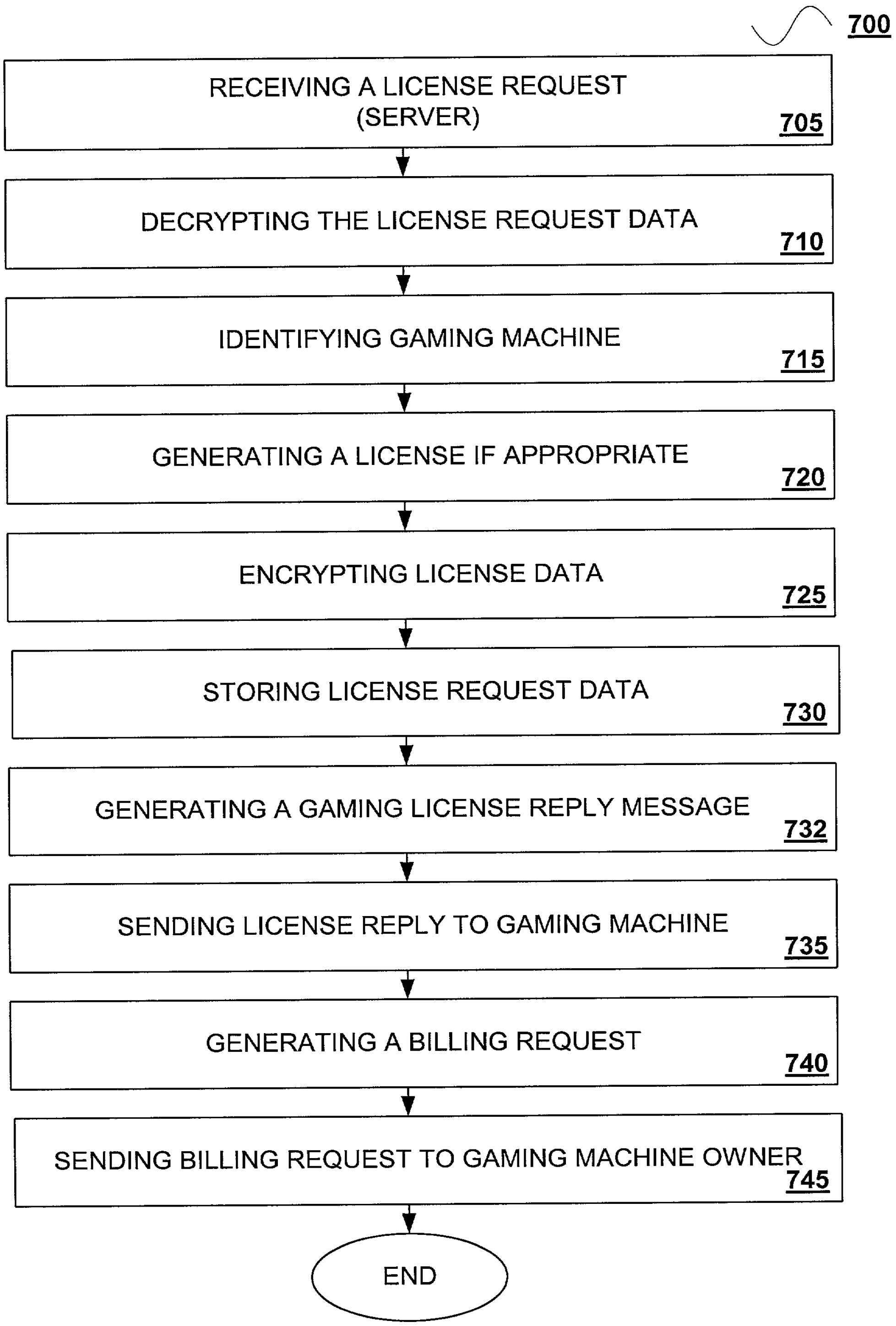

700
RECEIVING A LICENSE REQUEST (SERVER)
705
DECRYPTING THE LICENSE REQUEST DATA
710
IDENTIFYING GAMING MACHINE
715
GENERATING A LICENSE IF APPROPRIATE
720
ENCRYPTING LICENSE DATA
725
STORING LICENSE REQUEST DATA
730
GENERATING A GAMING LICENSE REPLY MESSAGE
732
SENDING LICENSE REPLY TO GAMING MACHINE
735
GENERATING A BILLING REQUEST
740
SENDING BILLING REQUEST TO GAMING MACHINE OWNER
745
END

FIGURE 7

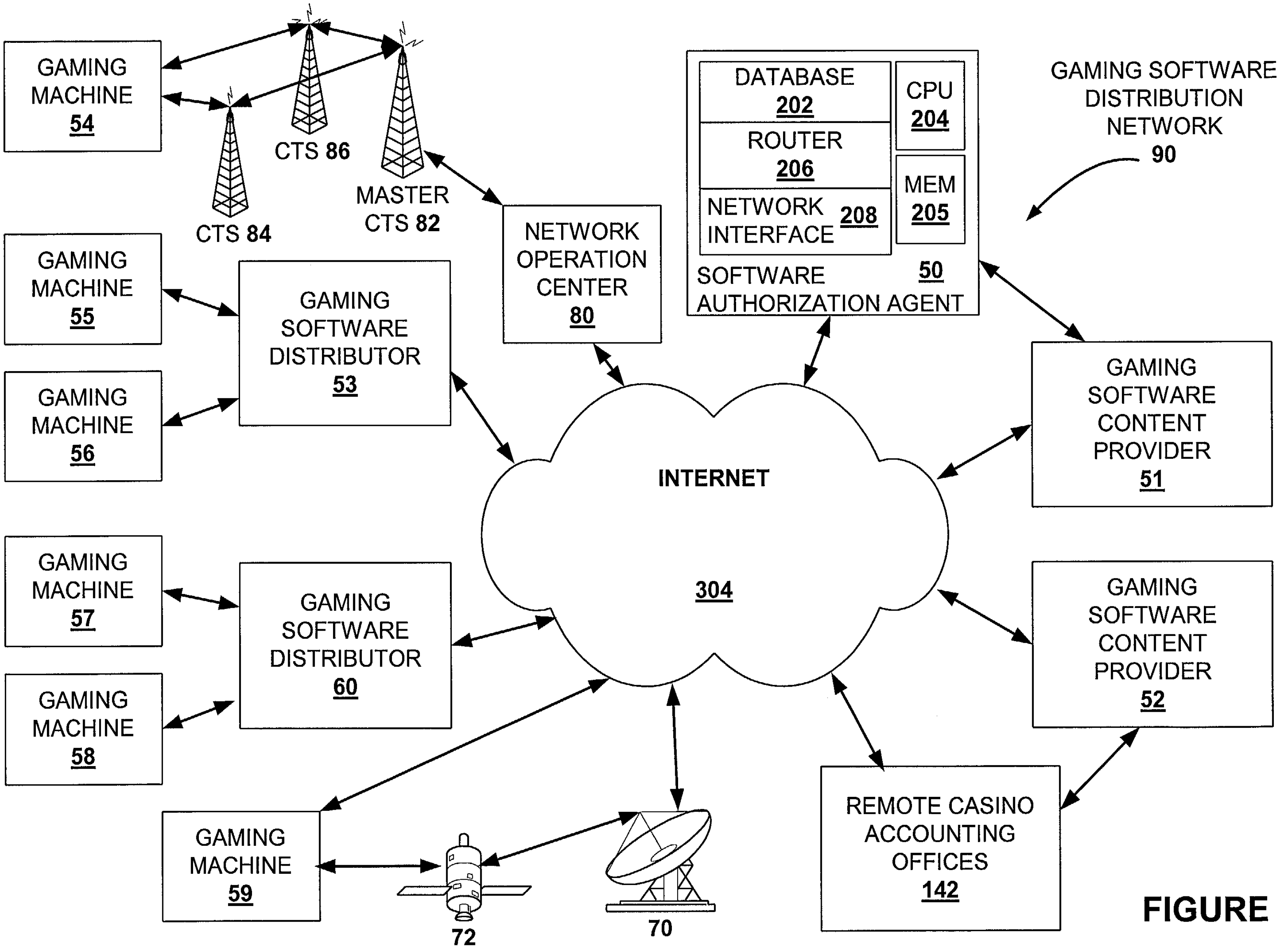

GAMING MACHINE 54
CTS 86
CTS 84
MASTER CTS 82
NETWORK OPERATION CENTER 80
DATABASE 202
ROUTER 206
NETWORK INTERFACE 208
CPU 204
MEM 205
SOFTWARE AUTHORIZATION AGENT 50
GAMING SOFTWARE DISTRIBUTION NETWORK 90
GAMING MACHINE 55
GAMING MACHINE 56
GAMING SOFTWARE DISTRIBUTOR 53
INTERNET
304
GAMING SOFTWARE CONTENT PROVIDER 51
GAMING MACHINE 57
GAMING MACHINE 58
GAMING SOFTWARE DISTRIBUTOR 60
GAMING SOFTWARE CONTENT PROVIDER 52
GAMING MACHINE 59
72
70
REMOTE CASINO ACCOUNTING OFFICES 142

FIGURE 8

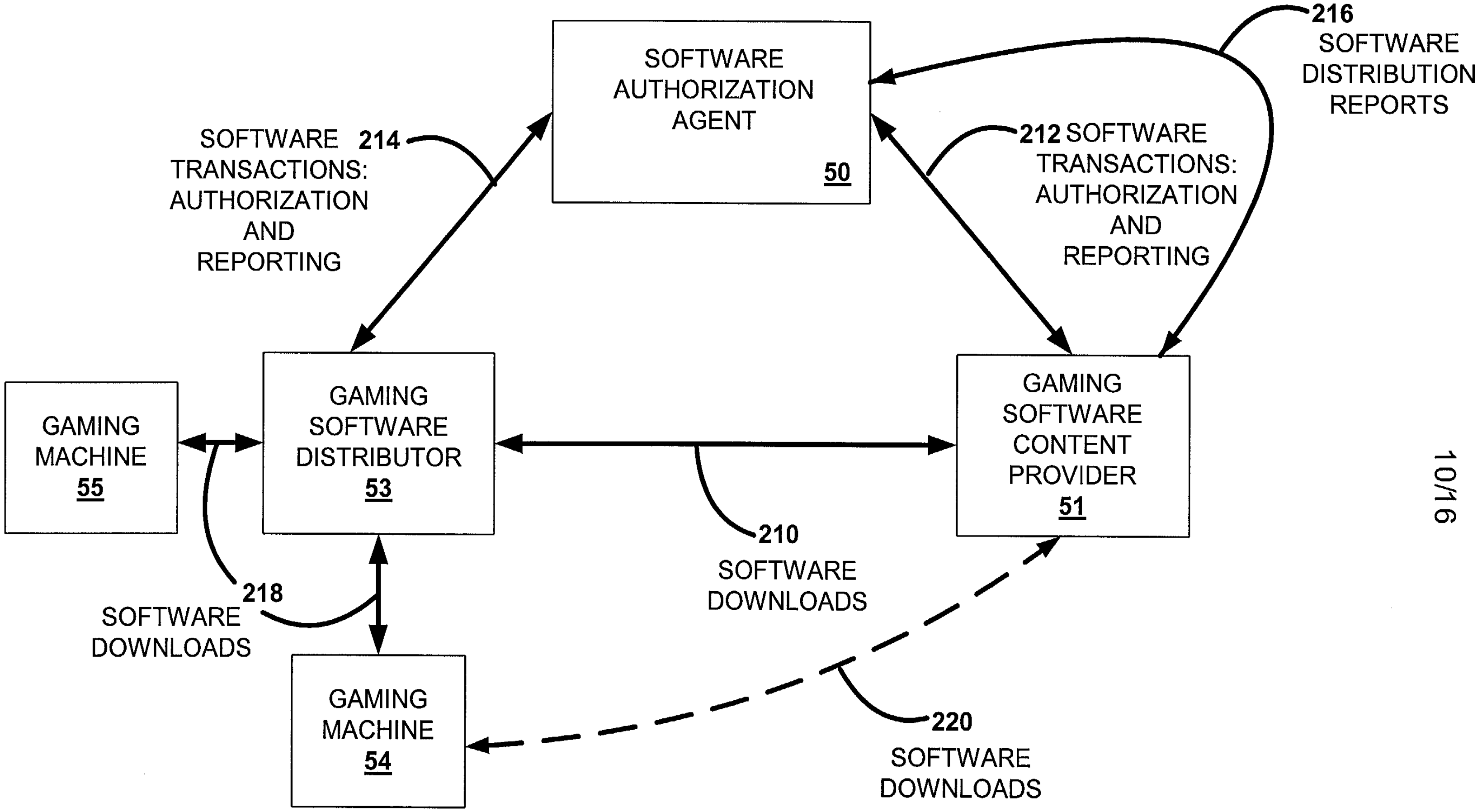

SOFTWARE AUTHORIZATION AGENT
50
216
SOFTWARE DISTRIBUTION REPORTS
SOFTWARE 214
TRANSACTIONS: AUTHORIZATION AND REPORTING
212 SOFTWARE TRANSACTIONS: AUTHORIZATION AND REPORTING
GAMING MACHINE
55
GAMING SOFTWARE DISTRIBUTOR
53
GAMING SOFTWARE CONTENT PROVIDER
51
210
SOFTWARE DOWNLOADS
218
SOFTWARE DOWNLOADS
GAMING MACHINE
54
220
SOFTWARE DOWNLOADS

FIGURE 9

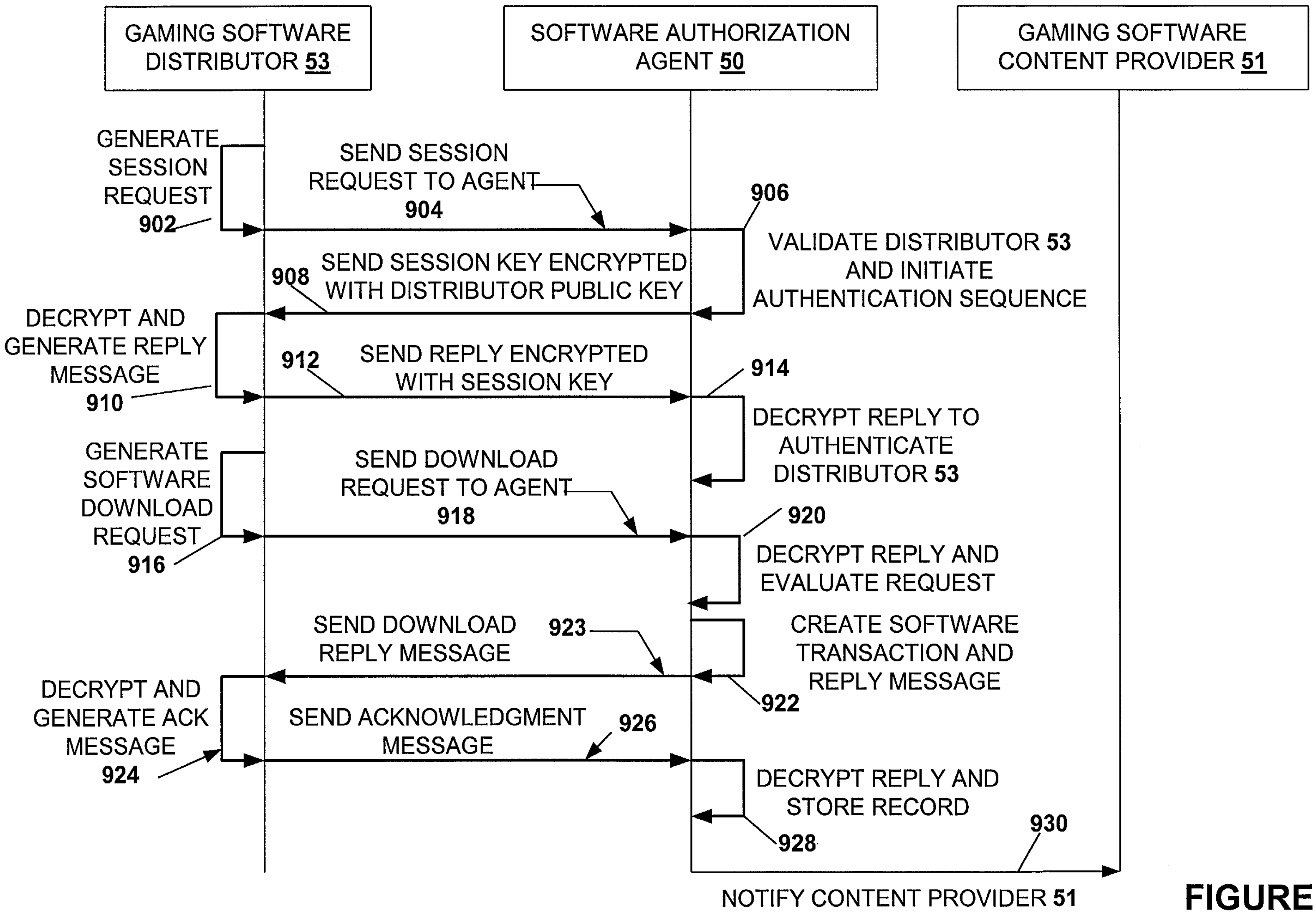

GAMING SOFTWARE DISTRIBUTOR 53
SOFTWARE AUTHORIZATION AGENT 50
GAMING SOFTWARE CONTENT PROVIDER 51
GENERATE SESSION REQUEST
902
SEND SESSION REQUEST TO AGENT
904
906
VALIDATE DISTRIBUTOR 53 AND INITIATE AUTHENTICATION SEQUENCE
908
SEND SESSION KEY ENCRYPTED WITH DISTRIBUTOR PUBLIC KEY
DECRYPT AND GENERATE REPLY MESSAGE
910
912
SEND REPLY ENCRYPTED WITH SESSION KEY
914
DECRYPT REPLY TO AUTHENTICATE DISTRIBUTOR 53
GENERATE SOFTWARE DOWNLOAD REQUEST
916
SEND DOWNLOAD REQUEST TO AGENT
918
920
DECRYPT REPLY AND EVALUATE REQUEST
SEND DOWNLOAD REPLY MESSAGE
923
CREATE SOFTWARE TRANSACTION AND REPLY MESSAGE
922
DECRYPT AND GENERATE ACK MESSAGE
924
SEND ACKNOWLEDGMENT MESSAGE
926
DECRYPT REPLY AND STORE RECORD
928
930
NOTIFY CONTENT PROVIDER 51

FIGURE 10

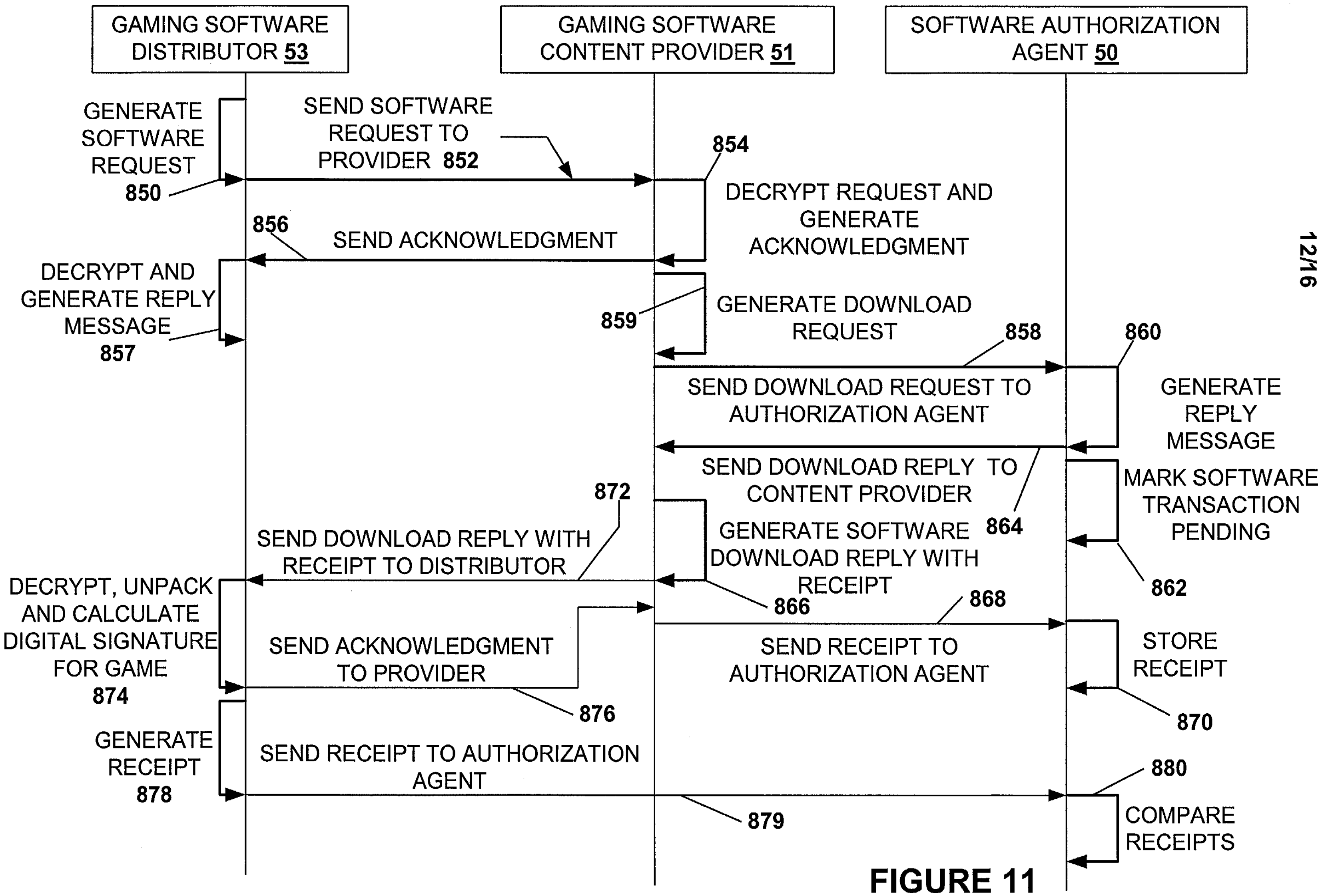

GAMING SOFTWARE DISTRIBUTOR 53
GAMING SOFTWARE CONTENT PROVIDER 51
SOFTWARE AUTHORIZATION AGENT 50
GENERATE SOFTWARE REQUEST
850
SEND SOFTWARE REQUEST TO PROVIDER 852
854
DECRYPT REQUEST AND GENERATE ACKNOWLEDGMENT
856
SEND ACKNOWLEDGMENT
DECRYPT AND GENERATE REPLY MESSAGE
857
859
GENERATE DOWNLOAD REQUEST
858
860
SEND DOWNLOAD REQUEST TO AUTHORIZATION AGENT
GENERATE REPLY MESSAGE
SEND DOWNLOAD REPLY TO CONTENT PROVIDER
MARK SOFTWARE TRANSACTION PENDING
872
864
SEND DOWNLOAD REPLY WITH RECEIPT TO DISTRIBUTOR
GENERATE SOFTWARE DOWNLOAD REPLY WITH RECEIPT
862
DECRYPT, UNPACK AND CALCULATE DIGITAL SIGNATURE FOR GAME
874
866
868
SEND ACKNOWLEDGMENT TO PROVIDER
SEND RECEIPT TO AUTHORIZATION AGENT
STORE RECEIPT
876
870
GENERATE RECEIPT
878
SEND RECEIPT TO AUTHORIZATION AGENT
880
879
COMPARE RECEIPTS

FIGURE 11

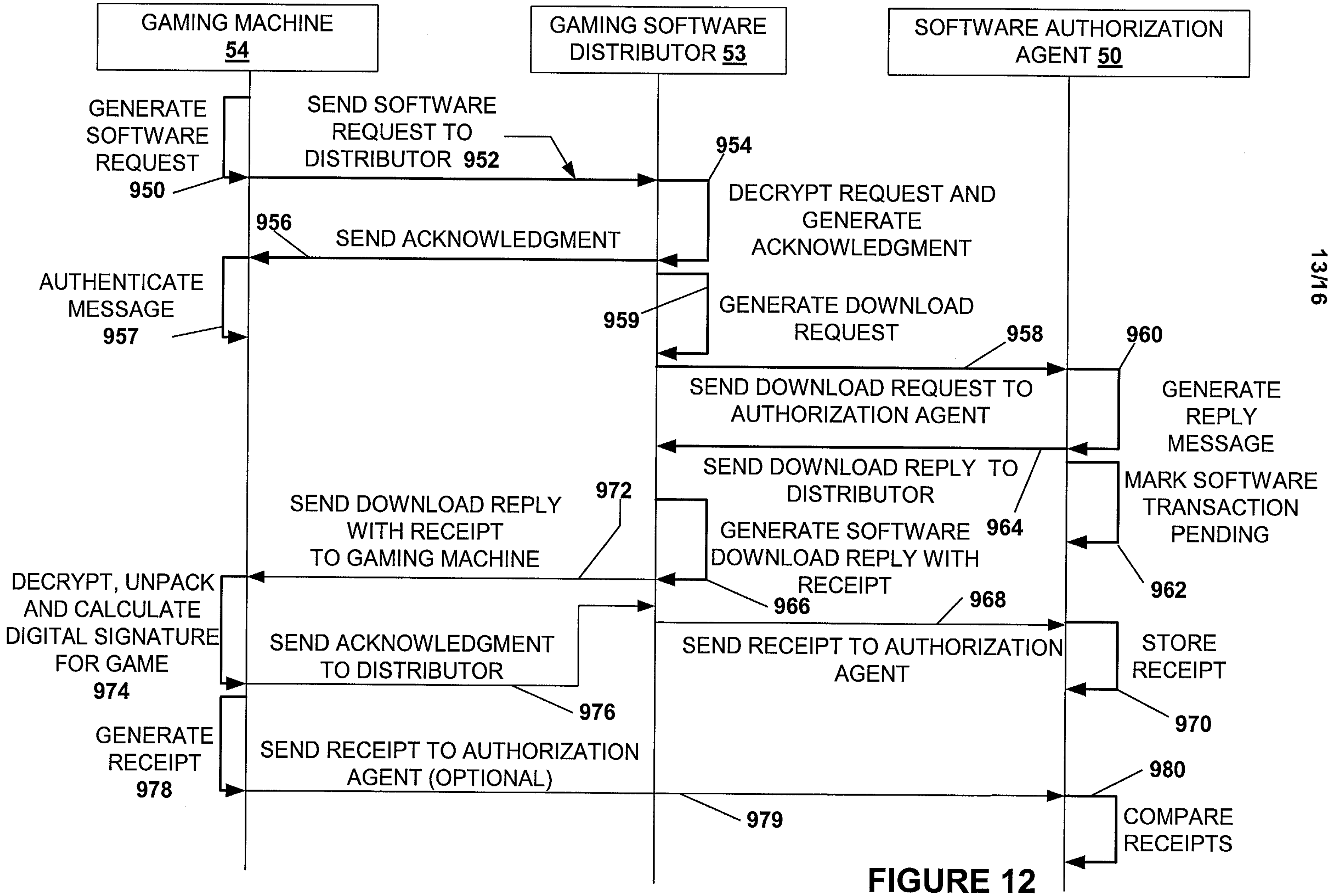

GAMING MACHINE 54
GAMING SOFTWARE DISTRIBUTOR 53
SOFTWARE AUTHORIZATION AGENT 50
GENERATE SOFTWARE REQUEST 950
SEND SOFTWARE REQUEST TO DISTRIBUTOR 952
954
DECRYPT REQUEST AND GENERATE ACKNOWLEDGMENT
956
SEND ACKNOWLEDGMENT
AUTHENTICATE MESSAGE 957
959
GENERATE DOWNLOAD REQUEST
958
960
SEND DOWNLOAD REQUEST TO AUTHORIZATION AGENT
GENERATE REPLY MESSAGE
SEND DOWNLOAD REPLY TO DISTRIBUTOR
964
MARK SOFTWARE TRANSACTION PENDING
962
SEND DOWNLOAD REPLY WITH RECEIPT TO GAMING MACHINE
972
GENERATE SOFTWARE DOWNLOAD REPLY WITH RECEIPT
966
968
DECRYPT, UNPACK AND CALCULATE DIGITAL SIGNATURE FOR GAME 974
SEND ACKNOWLEDGMENT TO DISTRIBUTOR
976
SEND RECEIPT TO AUTHORIZATION AGENT
STORE RECEIPT
970
GENERATE RECEIPT 978
SEND RECEIPT TO AUTHORIZATION AGENT (OPTIONAL)
979
980
COMPARE RECEIPTS

FIGURE 12

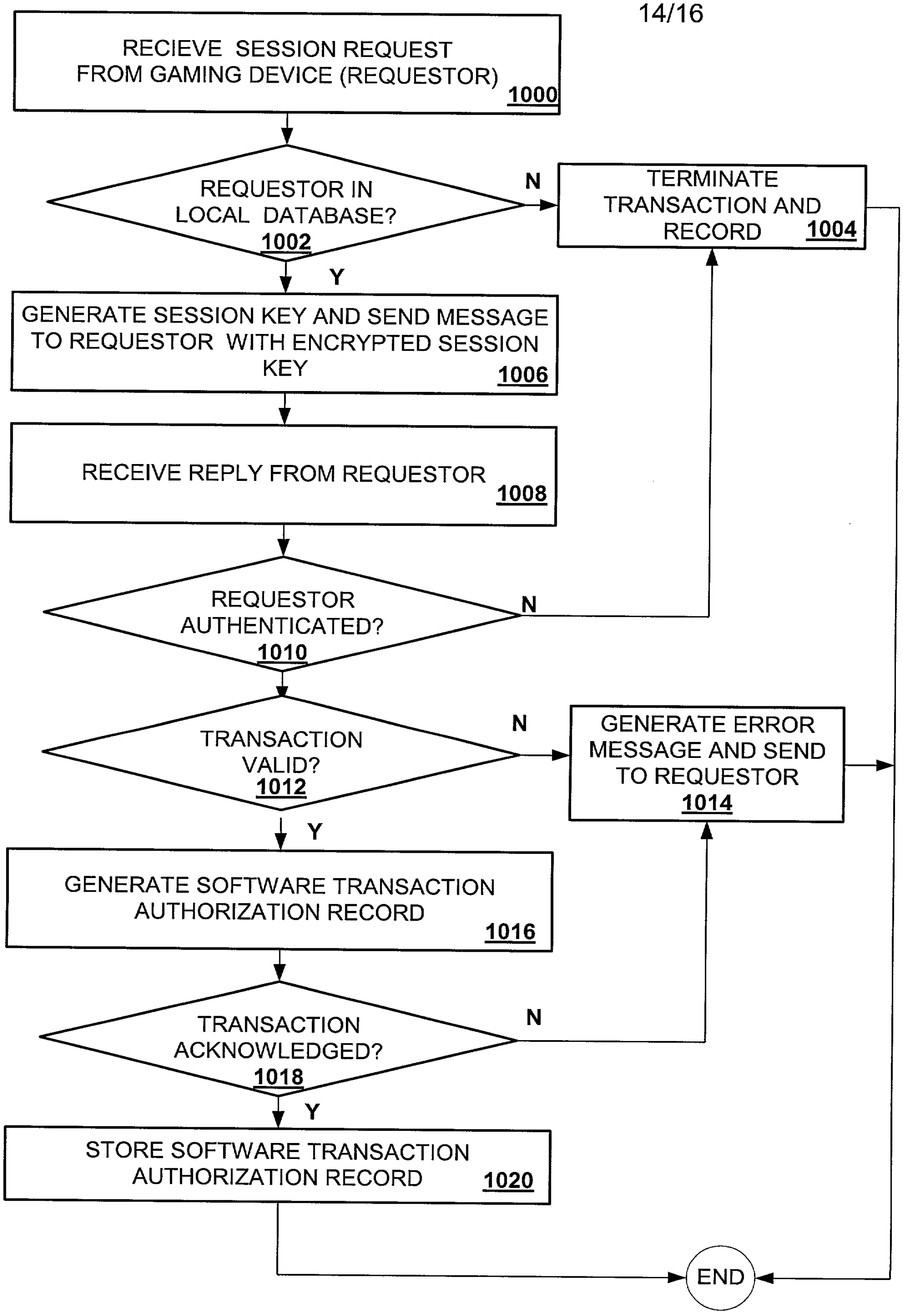

RECIEVE SESSION REQUEST FROM GAMING DEVICE (REQUESTOR)
1000
REQUESTOR IN LOCAL DATABASE?
1002
N
TERMINATE TRANSACTION AND RECORD
1004
Y
GENERATE SESSION KEY AND SEND MESSAGE TO REQUESTOR WITH ENCRYPTED SESSION KEY
1006
RECEIVE REPLY FROM REQUESTOR
1008
REQUESTOR AUTHENTICATED?
1010
N
TRANSACTION VALID?
1012
N
GENERATE ERROR MESSAGE AND SEND TO REQUESTOR
1014
Y
GENERATE SOFTWARE TRANSACTION AUTHORIZATION RECORD
1016
TRANSACTION ACKNOWLEDGED?
1018
N
Y
STORE SOFTWARE TRANSACTION AUTHORIZATION RECORD
1020
END

FIGURE 13

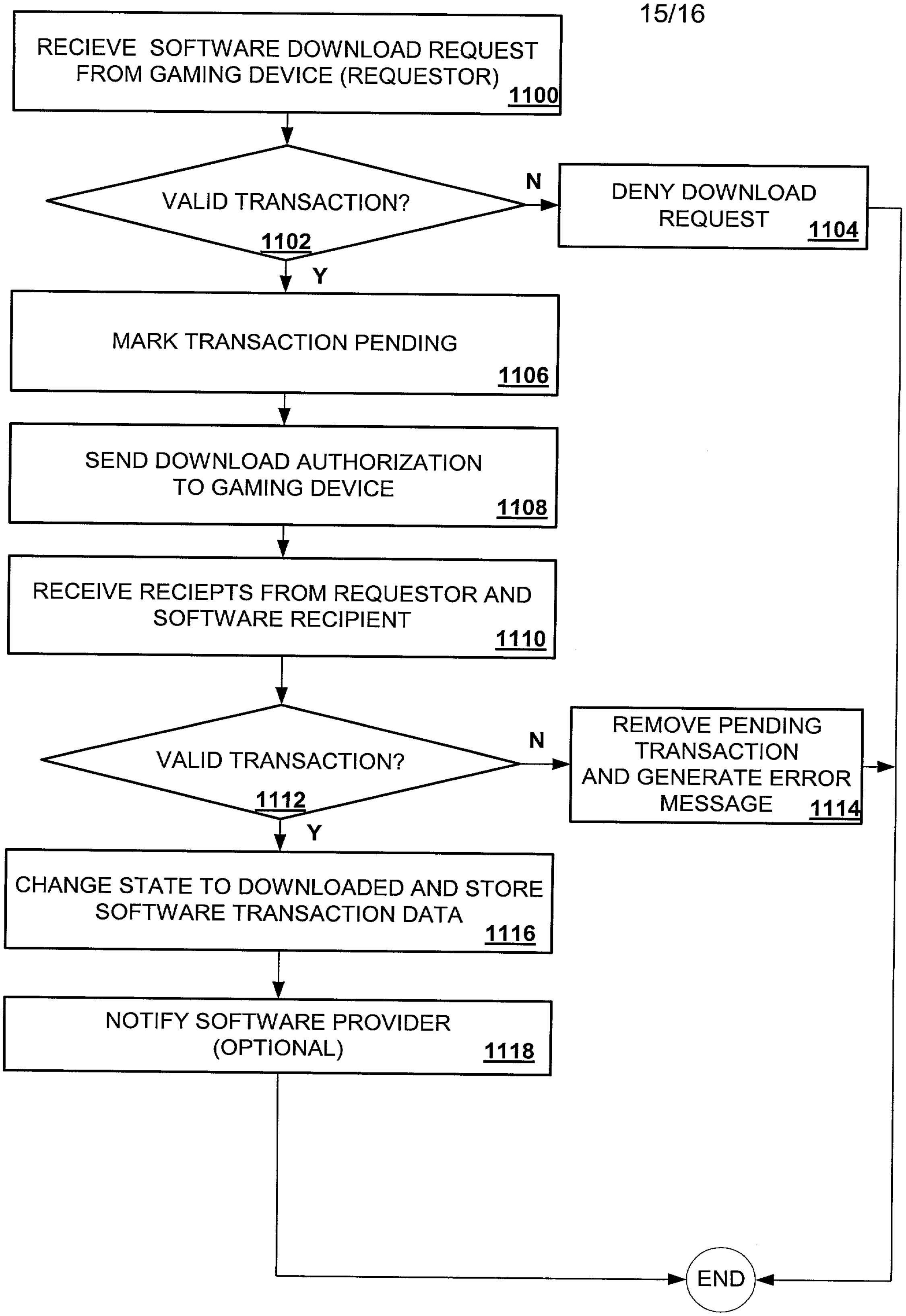

RECIEVE SOFTWARE DOWNLOAD REQUEST FROM GAMING DEVICE (REQUESTOR)
1100
VALID TRANSACTION?
1102
N
DENY DOWNLOAD REQUEST
1104
Y
MARK TRANSACTION PENDING
1106
SEND DOWNLOAD AUTHORIZATION TO GAMING DEVICE
1108
RECEIVE RECIEPTS FROM REQUESTOR AND SOFTWARE RECIPIENT
1110
VALID TRANSACTION?
1112
N
REMOVE PENDING TRANSACTION AND GENERATE ERROR MESSAGE
1114
Y
CHANGE STATE TO DOWNLOADED AND STORE SOFTWARE TRANSACTION DATA
1116
NOTIFY SOFTWARE PROVIDER (OPTIONAL)
1118
END

FIGURE 14

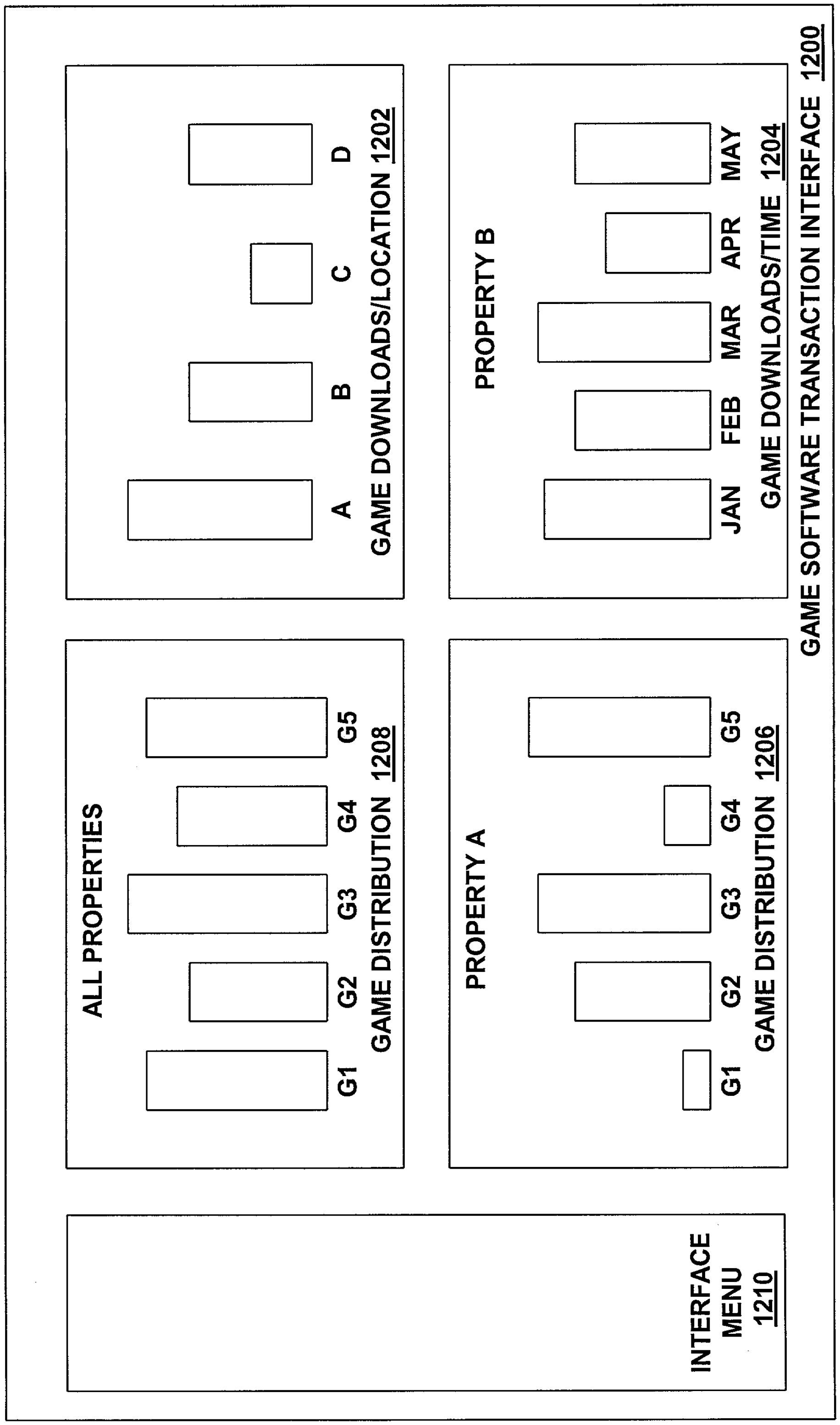

GAME SOFTWARE TRANSACTION INTERFACE 1200
ALL PROPERTIES
G1
G2
G3
G4
G5
GAME DISTRIBUTION 1208
A
B
C
D
GAME DOWNLOADS/LOCATION 1202
PROPERTY A
G1
G2
G3
G4
G5
GAME DISTRIBUTION 1206
PROPERTY B
JAN
FEB
MAR
APR
MAY
GAME DOWNLOADS/TIME 1204
INTERFACE
MENU
1210

FIGURE 15

DECLARATION AND POWER OF ATTORNEY
FOR ORIGINAL U.S. PATENT APPLICATION

Attorney's Docket No. **IGT1P034X1/P-277CIP**

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT** the specification of which,

(check one) 1. ☒ is attached hereto.

2. □ was filed on ______________________ as
U.S. Application No. ______________________
and was amended on ______________________.

3. □ was filed on ______________________ as
International PCT Application No. ______________________
and was amended on ______________________.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, CFR § 1.56.

Prior Foreign Application(s)

I hereby claim foreign priority benefits under Title 35, United States code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

			Priority Benefits Claimed?
______________	__________	______________	Yes ___ No ___
(Application No.)	(Country)	(Filing Date)	
______________	__________	______________	Yes ___ No ___
(Application No.)	(Country)	(Filing Date)	

Provisional Application(s)

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

______________________ ______________
(Application No.) (Filing Date)

______________________ ______________
(Application No.) (Filing Date)

Prior U.S. Application(s)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

09/732,650	December 7, 2000	Pending
(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)
(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)

Power of Attorney

And I hereby appoint the law firm of **Beyer Weaver & Thomas, LLP** and all practitioners who are associated with the Customer Number 022434 as my principal attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Direct Correspondence To: **Customer Number: 022434**

22434
PATENT TRADEMARK OFFICE

Direct Telephone Calls To: **David P. Olynick at telephone number (510) 843-6200**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Typewritten Full Name of
Sole or First Inventor: **Binh T. Nguyen** Citizenship: **U.S.**

Inventor's signature: **Date of Signature:** 4/2/02

Residence: (City) **Reno** (State/Country) **Nevada/U.S.**

Post Office Address: **1445 Taos Court, Reno, Nevada 89511**

Second Inventor: **Michael M. Oberberger** Citizenship: **U.S.**

Inventor's signature: **Date of Signature:** 4/2/02

Residence: (City) **Reno** (State/Country) **Nevada/U.S.**

Post Office Address: **4591 Lynnfield Court, Reno, Nevada 89509**

Second Inventor: **Gregory Hopkins Parrott** Citizenship: **U.S.**

Inventor's signature: Gregory Parrott **Date of Signature**: 4\2\02

Residence: (City) **Reno** (State/Country) **Nevada/U.S.**

Post Office Address: **4955 Foxcreek Trail, Reno, Nevada 89509**

PATENT APPLICATION SERIAL NO. ____________________

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

```
04/09/2002 MAHMED1  00000050 500388   10116424

01 FC:101                      740.00 OP
02 FC:102                      336.00 OP
03 FC:103        86.00 CH     2002.00 OP
```

PTO-1556
(5/87)

*U.S. Government Printing Office: 2001 — 481-697/59173

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

Application or Docket Number

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	136	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	136 minus 20=	* 116
INDEPENDENT CLAIMS	7 minus 3 =	* 4
MULTIPLE DEPENDENT CLAIM PRESENT		□

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE □ OR OTHER THAN SMALL ENTITY

RATE	FEE			RATE	FEE
BASIC FEE	370.00	OR		BASIC FEE	740.00
X$ 9=		OR	116	X$18=	2088
X42=		OR	4	X84=	336
+140=		OR		+280=	
TOTAL		OR		TOTAL	3164

CLAIMS AS AMENDED - PART II

SMALL ENTITY OR OTHER THAN SMALL ENTITY

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM □				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM □				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM □				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

☆U S GPO 2001 482-124 / 59197

CLAIMS ONLY

SERIAL NO.

FILING DATE

APPLICANT(S)

CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT			*		*		*	
	IND.	DEP.	IND.	DEP.	IND.	DEP.		IND.	DEP.	IND.	DEP.	IND.	DEP.
|01		|					51						
2		|	/				52						
3	1 /						53						
4		|					54						
5		|					55						
6		|					56						
7		|	/				57						
8		|					58						
9		|					59						
10		|					60						
11		|	/				61						
12		|					62						
13		|					63						
14		|					64						
15		|	/				65						
16		|					66						
17		|					67						
18		|					68						
19		|					69						
20		|	/				70						
21		|					71						
22		|	/				72						
23	1 /						73						
24		|					74						
25		|					75						
26		|					76						
27		|					77						
28		|	/				78						
29		|					79						
30		|					80						
31		|	/				81						
32		|					82						
33		|					83						
34		|					84						
35		|	/				85						
36		|	/				86						
37							87						
38							88						
39							89						
40							90						
41							91						
42							92						
43							93						
44							94						
45							95						
46							96						
47							97						
48							98						
49							99						
50							100						
TOTAL IND.	7	⬇ ⬅		⬇ ⬅		⬇ ⬅	TOTAL IND.		⬇ ⬅		⬇ ⬅		⬇ ⬅
TOTAL DEP.	129						TOTAL DEP.						
TOTAL CLAIMS	136	■		■		■	TOTAL CLAIMS		■		■		■

*MAY BE USED FOR ADDITIONAL CLAIMS OR ADMENDMENTS

FORM PTO-2022 (1-98)

U.S.DEPARTMENT OF COMMERCE
Patent and Trademark Office

*U.S. Government Printing Office: 1998 - 433-214/70303

CLAIMS ONLY

SERIAL NO.

FILING DATE

APPLICANT(S)

CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
1	1 /					
2		1				
3		1				
4		1				
5		1				
6		1				
7		1	/			
8		1				
9		1				
10		1				
11		1				
12		1				
13		1				
14		1	/			
15		1				
16		1				
17		1				
18		1				
19		1				
20		1				
21		1				
22		1	/			
23		1				
24		1				
25		1				
26		1				
27		1	/			
28	1 /					
29		1				
30		1				
31		1	/			
32		1				
33		1				
34		1				
35		1				
36		1				
37		1				
38		1	/			
39		1				
40		1				
41		1				
42		1				
43		1	/			
44		1				
45		1				
46		1				
47		1	/			
48		1				
49		1				
50		1				
TOTAL IND.						
TOTAL DEP.						
TOTAL CLAIMS						

	*		*		*	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
51		1	/			
52	1 /					
53		1				
54		1	/			
55		1				
56		1				
57		1				
58		1				
59		1				
60		1				
61		1				
62		1				
63		1				
64		1	/			
65	1 /					
66		1				
67		1				
68		1				
69		1				
70		1	/			
71		1				
72		1				
73		1				
74		1				
75		1				
76		1				
77		1				
78		1	/			
79		1				
80		1				
81		1				
82		1				
83		1	/			
84	1 /					
85		1				
86		1				
87		1	/			
88		1				
89		1				
90		1				
91		1				
92		1				
93		1				
94		1	/			
95		1				
96		1				
97		1				
98		1				
99		1				
100		1	/			
TOTAL IND.						
TOTAL DEP.						
TOTAL CLAIMS						

MAY BE USED FOR ADDITIONAL CLAIMS OR AMENDMENTS

FORM PTO-2022 (1-98)

U.S.DEPARTMENT OF COMMERCE
Patent and Trademark Office

*U.S. Government Printing Office: 1998 - 433-214/70303

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen et al.	Attorney Docket No.: IGT1P034X1
Application No.: New	Examiner: Not yet assigned
Filed: Herewith	Group: Not yet assigned

#2
6-11-02

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this paper and the documents and/or fees referred to as attached therein are being deposited with the United States Postal Service on April 03, 2002 in an envelope as "Express Mail Post Office to Addressee" service under 37 CFR §1.10, Mailing Label Number EL937779717US, addressed to the Commissioner for Patents, Washington, DC 20231.

Snoriega
Sunshine Noriega

INFORMATION DISCLOSURE STATEMENT
37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
Washington, DC 20231

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David Olynick
David P. Olynick
Registration No. 48,615

P.O. Box 778
Berkeley, CA 94704-0778

Form 1449 (Modified)	Atty Docket No. IGT1P034X1	Application No.: New
Information Disclosure Statement By Applicant	Applicant: Nguyen et al.	
(Use Several Sheets if Necessary)	Filing Date Herewith	Group Not yet assigned

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	6,149,522	11/21/00	Alcorn et al.	463	29	06/29/98
	A2	6,106,396	08/22/00	Alcorn et al.	463	29	06/17/96
	A3	6,104,815	08/15/00	Alcorn et al.	380	251	01/09/98
	A4	5,836,817	11/17/98	Acres et al.	463	26	06/06/95
	A5	5,643,086	07/01/97	Alcorn et al.	463	29	06/29/95
	A6	6,178,510	1/23/01	O'Connor et al.	713	201	9/4/97
	A7	6,099,408	8/8/00	Schneier et al.	463	29	12/31/96
	A8	5,768,382	6/16/98	Schneier et al.	380	23	11/22/95
	A9	6,285,868	9/4/01	LaDue	455	410	1/10/97
	A10	5,761,647	6/2/98	Boushy	705	10	5/24/96
	A11	5,999,808	12/7/99	LaDue	455	412	1/7/96
	A12	5,770,533	6/23/98	Franchi	463	42	5/2/94
	A13	6,270,410	8/7/01	DeMar et al.	463	20	2/10/99
	A14	5,779,545	7/14/98	Berg et al.	463	22	9/10/96

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	B1	WO 96/00950	11/1/96	WIPO	G06F	155/00	X	
	B2	WO 95/24689	14/9/95	WIPO	G06F	155/00	X	
	B3	WO 99/01188	14/1/99	WIPO	A63F		X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 155/00, 161/00

A1

(11) International Publication Number: WO 95/24689

(43) International Publication Date: 14 September 1995 (14.09.95)

(21) International Application Number: PCT/US95/02939

(22) International Filing Date: 7 March 1995 (07.03.95)

(30) Priority Data:

08/212,348	11 March 1994 (11.03.94)	US
08/269,248	30 June 1994 (30.06.94)	US

(71) Applicant: WALKER ASSET MANAGEMENT LIMITED PARTNERSHIP [US/US]; 125 Elm Street, New Canaan, CT 06840 (US).

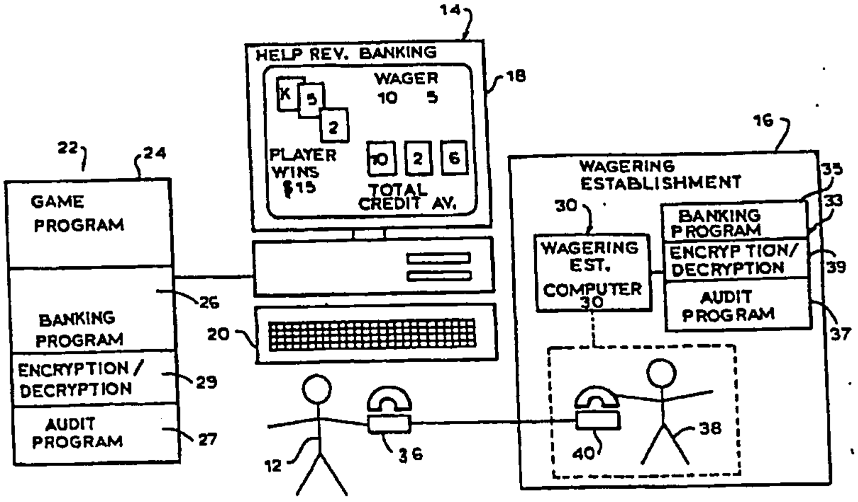
(72) Inventor: WALKER, Jay; 124 Spectacle Lane, Ridgefield, CT 06877 (US).

(74) Agents: ROTHSTEIN, Jesse et al.; Amster, Rothstein & Ebenstein, 90 Park Avenue, New York, NY 10016 (US).

(81) Designated States: AM, BG, BY, CZ, EE, GE, HU, KG, KZ, LT, LV, MD, MG, MN, MW, PL, RO, SD, SI, SK, TJ, UA, UG, UZ, VN.

Published
With international search report.

(54) Title: IMPROVED REMOTE GAMING SYSTEM



(57) Abstract

A remote gaming system whereby a player (12) can gamble against a wagering establishment (16) or lottery from a remote location on a personal computer or portable computer device (14) where it is unnecessary to establish an on-line connection with a host computer associated with the wagering establishment, the gaming computer providing at least one wagering opportunity and enabling the player to obtain credit and cash-out any winnings, the host computer (30) enabling the player to purchase and redeem credit at the remote location through a series of encrypted code exchanges between the player and the wagering establishment, or alternatively the gaming computer or a credit module for use with a personal computer being provided to the player with pre-installed credit.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

IMPROVED REMOTE GAMING SYSTEM

This Application is a continuation-in-part of copending Application Serial No. 08/212,348, filed on March 11, 1994.

BACKGROUND

1. Field of the Invention

The present invention relates generally to a remote gaming system, and more particularly, to a remote gaming system by which a player can wager on a plurality of games of chance and/or future public events of which the outcome is uncertain, offered by a casino, government lottery organization, or other wagering establishment.

2. Description of the Prior Art

In the past, a player wishing to wager on a game of chance such as those offered in a casino or on a public event of which the outcome is uncertain such as sporting events, had a limited number of options. In order to wager on casino games such as roulette, blackjack, poker and the like, the player had to physically travel to a gaming establishment specifically engaged in such activities or to a location where stand-alone gambling devices such as video poker terminals or slot machines were available. Although public events such as horse races may be wagered on by telephone contact with an authorized "off-track betting" gaming establishment or its agent, such methods utilizing telephone contact have not been amenable to typical casino games.

As a result of advances in computer technology and telecommunications, remote gaming systems have been devised in which a player can participate in a plurality of games of chance being offered by a gambling establishment without having to be physically located on the premises. An example is found in U.S. Patent Nos. 4,339,798 and 4,467,424, both to Hedges et al. The Hedges Patents disclose a remote gaming system wherein a player proceeds to gamble against the casino at a remote player station which includes a live game display to permit the player to engage in actual games of chance as they are being played in real-time at a croupier station comprised of one or more gaming tables in the casino. The player station includes a changeable keyboard communicating with a microprocessor for displaying a selected one of a plurality of wagering possibilities corresponding to a selected one of the plurality of games being played and for displaying the results of the game being played. The player becomes part of the game as if he or she were actually present at the gaming table in the casino. To provide a secure communications link, the remote gaming station communicates with the croupier station and a credit control station through an encryption/decryption device to prevent tampering by unauthorized sources.

While such a system provides a means by which a player can gamble from a remote location, its primary disadvantage resides in the fact that the player can gamble only by participating in games being actually conducted in the gaming establishment and monitored over real-time closed circuit video. Moreover, such a system has limited practicality since the player can only gamble on a specialized gaming station which must be electronically linked to the casino. It would therefore be highly desirable to provide a remote gaming system by which a player could engage in gambling on a gaming computer at a remote location at the player's convenience where the casino provides for the purchase and redemption of casino credit, notwithstanding the absence of any direct electronic communication link between the gaming computer and the casino.

Accordingly, it is an object of the present invention to provide a remote gaming system by which the player can wager on any one of a plurality of games of chance typically offered by a wagering establishment (e.g., a casino) at the player's convenience.

It is another object of the present invention to provide a remote gaming system by which the player can wager against the wagering establishment on any one of a plurality of wagering opportunities such as games of chance generated by computer software on any personal computer.

It is a further object of the invention to provide a remote gaming system by which a player can wager against the wagering establishment on a conventional multi-media apparatus (e.g., a Nintendo apparatus coupled to a television set) through compatible plug-in data storage media.

It is yet another object of the invention to provide a remote gaming system by which a player can purchase and redeem wagering credit from remote locations without the need for an electronic communications link to be established between the player's gaming computer and the wagering establishment.

It is still another object of the invention to provide a remote gaming system by which a player can wager on any one of a plurality of games of chance generated on a dedicated gambling computer, including a hand-held portable device, which can be provided to the player, yet need not be electronically linked to the wagering establishment for purposes of gambling, and/or purchasing and redeeming wagering credit.

It is yet another object of the invention to provide a remote gaming system wherein encryption and decryption of codes transferred between a remote gaming computer and the wagering establishment, either on-line (including wireless electronic communication hardware) or off-line (orally with an agent or electronic communications over the telephone, but where no connection is necessary between the gaming computer and the wagering establishment), prevents unauthorized users from gaining access to or fraudulently obtaining or redeeming wagering credit.

It is still another object of the invention to provide a remote gaming system by which a player receives a tamper-proof read/write device from the wagering establishment containing data storage media for dedicated gaming software which can be linked to any personal computer, yet prevents unauthorized manipulation of the software.

It is still another object of the invention to provide a remote gaming system in which the gaming and/or banking software is embodied in a computer disk where the unique magnetic signature of that disk is readable by the disk drive in the gaming computer for encryption to make detectable unauthorized duplication of the disk.

It is still another object of the invention to provide a remote gaming system by which a player can wager on future public events of which the outcome is uncertain such as a lottery, either through an on-line connection between a gaming computer and the gambling establishment, or off-line where the player's wager is time-stamped to generate an encrypted registration code, representing the player's choice of wagering elements (i.e., numbers) for a given lottery event (occurring at some time in the future), which code is known only to the lottery authority.

It is yet another object of the invention to provide a remote gaming system by which a player can obtain and redeem wagering credit from the wagering establishment embodied in tamper-proof physical data memory media which interface with a remote gaming computer.

It is still another object of the invention to provide a remote gaming system by which a completely self-contained dedicated gambling personal digital assistant may be obtained with a preprogrammed and predetermined amount of non-renewable credit.

It is a further object of the invention to provide a remote gaming system by which a player can engage in a game of skill (e.g., a crossword puzzle) made available on a dedicated gambling personal digital assistant having a preprogrammed and predetermined amount of non-renewable credit.

It is still another object of the invention to provide a remote gaming system in which a premium application enables a player who purchases a product such as a computer, or software on data storage media, to win something as determined by the output of a gaming program embedded within such product.

It is yet another object of the invention to provide a remote gaming system by which a player wagering at a remote location is subject to predetermined limitations on winnings by a wagering establishment.

SUMMARY OF THE INVENTION

In accordance with the above objects and other objects which will become apparent hereinafter, the present invention provides a remote gaming system which enables a player to gamble against a wagering establishment using a gaming computer at a remote location. The gaming computer may or may not be electronically linked (i.e., "on-line") to a wagering establishment computer while gambling takes place. The gaming computer can be any personal computer, hand-held computer device (e.g., a personal digital assistant), or multi-media apparatus which functions as the gaming computer (e.g., a nintendo or like apparatus) and may or may not be a dedicated gambling computer provided by the wagering establishment. If provided by the wagering establishment, the gaming computer is pre-loaded with gaming software. If the gaming computer is a conventional personal computer, the gaming software is either pre-installed on a secure data storage media device (e.g., a hard disk, CD-ROM, etc.) or module provided by the wagering establishment or installed directly on the computer by the player.

The gaming software includes a game program and a banking program. The game program generates a plurality of games of chance typically offered by the wagering establishment (e.g., blackjack, roulette, craps, poker, slots, etc.), or makes available wagering on future public events of which the outcome is uncertain (e.g., a lottery). The banking program provides for the purchase or loading of credit, from the wagering establishment to enable gambling and increments or decrements the player's account balance to enable the player to cash-out any gambling winnings. The gaming software may also include an audit program which records the outcome of each wager and transactions between the player and the wagering establishment as entered into and output from the gaming computer to purchase and redeem credit.

The wagering establishment computer includes a banking program which enables the player to purchase and redeem wagering credit at the remote location, even if no on-line communications are established with the gaming computer and an audit program for recording such transactions. This may be accomplished through a plurality of encrypted code exchanges which take place between the player and the casino, either by oral communications between the player and an agent of the casino, or by communications between the player and an automated answering service at the casino (i.e., using a touch-tone phone), or by providing credit "built-in" or pre-installed on a tamper-proof module for installation on a conventional personal computer, or pre-installed on a dedicated gaming computer provided by the wagering establishment. In the off-line embodiment, the automated "agent" is associated with the wagering establishment computer but there is no direct electronic connection between the gaming computer and the wagering establishment computer. Encryption provides a means by which such exchanges are made secure to prevent a third party from gaining unauthorized access or fraudulently obtaining or redeeming such credit.

If the gaming computer is networked to the wagering establishment computer, the connection may or may not serve to regulate or control the gaming software simulation of casino games on the gaming computer. For example, the connection may serve to have the wagering establishment computer keep a record of all or selected activities taking place at the gaming computer for purposes of additional verification or security. Alternatively, the connection may be of a controlled nature to vary the odds of a given wager based upon any of a variety of factors such as gambling duration or a progressively increasing jackpot (e.g., in a slot machine simulation). In such an on-line embodiment, security and player verification can be obtained by utilizing a stand-alone encryption device such as commonly employed in wireless money transfers. This device generates an encrypted verification code based upon the user's personal identification code and a second code provided to the user by the casino or stored in the stand-alone encryption device to prevent an unauthorized user from obtaining on-line access upon having stolen a user's personal identification code.

At all times, each wager by the player generates an encrypted electronic audit-trail on the gaming computer and/or on any networked computers by recording the amount of each wager, the outcome of each gambling event and any resulting gambling earnings or losses. The financial resolution of each wager is cumulatively tracked by the software on the gaming computer and perhaps also on any networked computers and the player is able to constantly monitor his casino credit balance.

A player gambles in substantially the same way he or she does in a casino. The player chooses which games to play as presented by the gaming software, the amount of each wager and the length of time each game is played. The player may remain active over several different gaming sessions which may take place at several different times and/or places. The player may at any time place wagers which are for practice only which do not affect the player's wagering credit balance. As an option, the player's wagering credit balance may be transferred and stored on data storage media which can be installed on other computers where software has been or can be installed to recognize the player's wagering credits and credit balance. The player may then continue to wager on any of such other computers. At any time the player wishes to cash-out his or her wagering credits or winnings, they can be redeemed from the wagering establishment by contacting the wagering establishment either by telephone in an off-line embodiment, or by direct electronic communication in an on-line embodiment. In one embodiment described above, a series of encrypted codes are then exchanged with the wagering establishment, either by telephone or transmitted electronically. In the off-line embodiment, these codes are generated by the gaming computer software and the casino computer software to verify the player's identity prior to cashing-out gambling winners. In the on-line embodiment, a stand-alone encryption device generates an encrypted log-on or confirmation code for verification. Alternatively, where the gaming computer itself (e.g., a personal digital assistant) is provided to the player by the wagering establishment, it or a tamper-proof plug-in module may be physically returned to the wagering establishment for credit redemption. Such credits can be redeemed from the wagering establishment in any of a variety of forms of payment including but not limited to cash, bank-wire transfers, credits or some other form of payment mutually agreed to by the player and the wagering establishment.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A is a schematic view of the remote gaming system in a first off-line embodiment;

FIG. 1B is a schematic view of the remote gaming system in a second off-line embodiment;

FIG. 1C is a schematic view of the remote gaming system in a third off-line embodiment;

FIG. 2 is a schematic view of the remote gaming system in an on-line embodiment;

FIG. 3 is a schematic view of a gaming computer connected to a tamper-proof read/write data storage media device provided by the casino;

FIG. 4 is a flowchart of the start-up and registration sequence in the off-line embodiment;

FIG. 5 is a flowchart of the handshake recognition sequence in the off-line embodiment;

FIG. 6 is a flowchart of the purchase credit sequence in the off-line embodiment;

FIG. 7A is a flowchart of the wagering sequence for games of chance generated by the game program in the off-line embodiment;

FIG. 7B-1-2 is a flowchart of the wagering sequence for an off-line non-registered lottery system embodiment;

FIG. 7C-1-5 is a flowchart of the wagering sequence in an off-line registered lottery system embodiment;

FIG. 8 is a flowchart of the credit cash-out sequence in the off-line embodiment;

FIG. 9 is a flowchart of the registration and start-up sequence in the on-line embodiment;

FIG. 10 is the purchase credit sequence in the on-line embodiment;

FIG. 11 is a flowchart of the wagering sequence in the on-line embodiment;

FIG. 12 is a flowchart of the credit cash-out sequence in the on-line embodiment;

FIG. 13 is a schematic of a memory chip made secure by an external tamper-proof structure;

FIG. 14 is a schematic of a first means for verifying the integrity of the gaming software;

FIG. 15A is a schematic of a second means for verifying the integrity of the gaming software;

FIG. 15B is a schematic of a third means for verifying the integrity of the gaming software;

FIG. 15C is a schematic of a fourth means for verifying the integrity of the gaming software; and

FIG. 15D is a schematic of a fifth means for verifying the integrity of the gaming software.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference to the several views of the drawings, there is depicted a remote gaming system generally characterized by the reference numeral 10 in which a player 12 with access to a computer 14 ("the gaming computer") wagers on a plurality of games of chance or on future public events where the outcome of such events is uncertain, offered by a casino, government lottery organization or other wagering establishment 16. For convenience, these will be generally referred to herein as "the wagering establishment".

Referring now to FIG. 1A, player 12 has access to gaming computer 14 having a video display 18 and a keyboard 20. Gaming computer 14 can be a personal home computer, lap-top, or hand-held personal digital assistant device which may or may not be a dedicated gaming apparatus provided by wagering establishment 16 or a multi-media apparatus (e.g., a nintendo or similar device for use with a television or the like). Gaming computer 14 can be located either off-site at a remote location, at wagering establishment 16 or some other establishment (e.g., a lottery ticket vendor). A gaming computer 14 located at the wagering establishment 16 can still be classified as "remote" for the purpose of the disclosure and claims herein. It is anticipated that a casino could provide players, in for example, the hotel where the casino is located, with a dedicated gaming computer 14 which could be used to gamble within and outside of the physical boundaries of the casino. A primary advantage of providing player 12 with a wagering establishment-furnished gaming computer 14 is greater security, specifically with regard to making unauthorized access to the data storage media such as a computer disk drive or module more difficult. Moreover, in a dedicated gaming computer, the keyboard 20 can be customized with specialized function keys identifying commands (e.g., keys dedicated to blackjack might have indicia stating "hit me", "stand", "purchase insurance", etc.) which the player selects to proceed to gamble on the various games of chance being offered by the wagering establishment 16. Gaming computer 14 operates special gaming software 22 comprised of a game program 24, a banking program 26 and optionally, an audit program 27. Gaming software 22 can be pre-installed on a dedicated gaming computer 14 provided by the wagering establishment 16, pre-installed in a tamper-proof read/write data storage media device 28 provided by wagering establishment 16 which interfaces with a personal computer functioning as the gaming computer 14 as shown in FIG. 3, or installed directly on the personal computer by the player. Furthermore, the gaming software 22 may be made available on a tamper-proof plug-in data storage media module for use with a conventional multi-media apparatus which functions as the gaming computer 14, to be described in more detail hereinbelow.

It is critical that the wagering establishment 16 be able to determine if the software itself or data thereon was copied, tampered with or in any way altered, otherwise a player could make a plurality of copies and keep playing with identical disks until such time that one of the copied disks was a winner, or the player could alter the software itself in an attempt to control the outcome, the winnings or losses, or a combination thereof, i.e., a dishonest player 12 modifies the software code of the gaming software 22 in such a way as to make the software generate a winning outcome more frequently than chance would dictate (e.g., in a roulette simultation, causing the roulette wheel to land on a more favorable number more frequently). This could be achieved by replacing the software in its entirety or by modifying certain code lines of the program, either physically or by some other externally applied influence such as high-intensity electromagnetic radiation (e.g., an RF field). Of course, the most secure system is an on-line arrangement where the gaming software 22 resides in a gaming computer 30 on the premises of the wagering establishment (FIG. 2). The most difficult security issues with regard to tampering arise in embodiments where the wagering establishment provides the player 12 with software for use on a remotely disposed gaming computer 14 or with a dedicated gaming computer 14 itself (e.g., a PDA). In this connection, a variety of means for ensuring security may be provided.

In one application, software directing the gaming computer through the disk drive to read the unique magnetic signature of the specific disk on which gaming software 22 is made available for installation, and encrypt the same for decryption by the wagering establishment can reveal unauthorized duplication of data on that disk. Alternatively, a plug-in device can interface with the disk drive to read a portion of the disk to acquire the unique magnetic signature of the disk. This encrypted data can be registered with or required by the wagering establishment 16 prior to cashing out.

In another embodiment as shown schematically in FIG. 13, the gaming software 22 resides on a chip 23 disposed within the gaming computer 14 (i.e., where a dedicated device is provided by the wagering establishment 16). The chip 23 could be situated within a physical casing 84 which is isolated and unaccessible from any external data port connection. In an exemplary embodiment, the chip 23 can be housed within special seals, insulation, wrapping, or the like 86 to reveal any authorized attempts to remove or tamper with the chip 23. Thus, the wagering establishment 16 can readily ascertain if the player tampered with the gaming software and, if such tampering is discovered, it could deny such player any claimed winnings and/or future credit.

In yet another embodiment shown schematically in FIG. 14, unique mathematical attributes are derived from certain characteristics of the software code in a self-test process. To perform such a test, the characteristics of the code are kept secret and known only to the wagering establishment 16 (e.g., a check-digit type algorithm based upon the sum of the bits located in, for example, lines 476 through 655 of the code). Alternatively, the self-test can verify special codes which are embedded within the code instructions in some predetermined random manner known only to the wagering establishment 16.

In a variation of the above as shown schematically in FIG. 15A, external keys known only to the wagering establishment 16 can be applied to intermittently or continuously verify whether the software code has been or is being tampered with by causing altered software to malfunction and shut down the gaming application in the computer 14. This can be implemented in several ways, including, but not limited to: (1) broadcasting a continuous encoded or encrypted external signal (e.g., RF) from the wagering establishment 16, received by receiving means 88 in the gaming computer where such signals are subsequently decoded or decrypted by the gaming computer 14 and input to the gaming software 22 (FIG. 15B); (2) having the player 12 physically enter a code on an intermittent basis (FIG. 15C); or (3) utilizing an internally generated clock signal provided by a tamper-proof clock 89 (FIG. 15D). In this connection, the chip 23 or even the gaming computer 14 (if provided by the wagering establishment 16) may be shielded from electromagnetic interference to prevent unauthorized attempts to influence the gaming software with electromagnetic radiation. The use of external keys may or may not employ encryption to safeguard against their being somehow forged by the player 12.

Aside from the use of external keys, the gaming software 22 can be made to require the acquisition of data from an external source in order to function. For example, a wireless broadcast or like stream of random numbers (possibly encrypted) might be accessed by the gaming software 22 such that these random numbers are called upon by the program as a basis to select a wagering outcome in a predictable or unpre- dictable manner. Such external input may be incorporated into a tamper-proof plug-in device or module which interfaces with the gaming computer 14.

Another way to prevent fraudulent attempts to alteration of the gaming software 22 is the use of an audit program 27 which can only be accessed by the wagering establishment 16. To prevent a forged audit trail, the audit program 37 might, by way of example, create dozens or even hundreds of data strings (e.g., such as in a roulette simulation, data strings corresponding to spins of the roulette wheel each time the wheel is spun) where all such data is then recorded for future verification should the wagering establishment 16 suspect tampering with the gaming software 22.

It will be appreciated by persons skilled in the art that the gaming software 22 can be arranged such that a data-string of alphanumeric codes, either pre-loaded into each gaming computer 14, provided on a disk or alternatively furnished on a plug-in uncopyable module, can be used to discover any tampering with the software, disk or module by the player 12. In this connection, the code sequence can be made different for each gaming computer 14 or module and copies of such codes can be kept by the wagering establishment 16. These codes can provide the basis for randomness in the outcome of each gaming event, and can thereby provide evidence of tampering. In other words, a specific arrangement of codes might correspond to a certain outcome of a wagering event (e.g., the Roulette wheel lands on "5"). Even though these codes are known to the wagering establishment 16, they are sequenced to ensure a random outcome - something which could be verified by an independent third party. If a player 12 seeks to modify the gaming software, the altered software codes could be discovered upon comparison of the same with the originals known only to the wagering establishment 16.

As another means of preventing player fraud, an element of "double-randomness" can be implemented by requiring the player 12 to press a button for each selection or desired response on the gaming computer 14 twice, with the time interval between selections (i.e., in milliseconds) used to address a specific preprogrammed random outcome codified in corresponding software codes.

Game program 24 permits player 12 to wager on any one of a plurality of wagering opportunities, including games of chance, future public events where the outcome is uncertain or games of skill (e.g., a crossword puzzle). The games of chance are created on gaming computer 14 by game program 24 in accordance with conventional techniques and include, but are not limited to, common casino wagering activities such as blackjack, craps, roulette, poker, slots or the like.

Each game offers opportunities for player 12 to place wagers on one or more various wagering elements within a given wagering event depending upon the rules applicable to that game. This will be described in more detail below.

Game program 24 can be made to accept wagers on future public events where the outcome of such events are uncertain as in, for example, sporting events such as a football game or a boxing match, or a state-run or other lottery. This can be implemented by establishing communications orally or electronically with the wagering establishment 16 in order to place, register and confirm bets. The wager is placed on the gaming computer 14, which produces a code for registration with the wagering establishment 16. This code is then time stamped by the wagering establishment 16 to form an encrypted code using appropriate software instructions to lock in the bet or fix the time of the wager for the purpose of ascertaining the proper payoff. This implementation will be described in detail below. Similarly, games of skill such as a crossword puzzle can be implemented where a date/time stamp fixes the time of completion such that prizes are later awarded based upon the first player to complete the game.

Banking program 26 enables player 12 to wager with available credit, and "cash-out" in order to redeem any gambling winnings. In certain embodiments, the banking program 26 facilitates the purchase of credit from the wagering establishment 16 where such credit is "loaded" into the gaming computer in the form of codes. Alternatively, as shown in FIG. 1C the banking program can receive instructions from an electronic card reader 91 compatible with credit or debit cards 93 in a conventional manner, or the banking program can receive credit from a plug-in credit module 90.

As one way of ensuring security in the credit purchase/redemption procedure, banking program 26 or a dedicated encryption/decryption device provides, for example, an encryption and decryption algorithm 29 of the type known in the art (e.g., utilizing a public-key) to encrypt and decrypt certain alphanumeric codes exchanged between player 12 and casino 16 which are input to and generated by playing computer 14 and the wagering establishment computer 30. These codes are exchanged between player 12 and an agent of the wagering establishment 38 through telephone 40. The term "agent" is intended to include an automated telephone or like system which generates computerized instructions for communication to player 12 by means of a touch-tone telephone 36 to prompt player 12 to communicate responses to the wagering establishment 16 by pressing the appropriate numbers or symbols. Such generated instructions can be provided by the wagering establishment computer 30 over the telephone in accordance with well-known techniques.

The wagering establishment computer 30 has gaming software 33 which includes a banking program 35 and audit program 37. The computer 30 either includes or communicates with a dedicated device or software for implementing an encryption and decryption algorithm 39 known only to the wagering establishment 16 to encrypt and decrypt these codes. In this manner, the wagering establishment 16 enables a verified player 12 to purchase and redeem wagering credit at the remote location. The sequence of steps to purchase and redeem such credits by exchanging encrypted codes are described in greater detail below.

In the usual course of practicing the invention, FIG. 4 depicts a flowchart of the start-up and registration sequence in an off-line embodiment which must occur prior to wagering. Player 12 first registers various personal information with wagering establishment 16 and obtains an alphanumeric personal identification code 32. The wagering establishment 16 provides player 12 with gaming software 22 comprised of game program 24 and banking program 26 as described above, accompanied by an alphanumeric software identification code 34. Gaming software 22 may be independently tested, verified and provided on data storage media in a sealed envelope by a third party. Such data storage media can include a hard disk, floppy disk, CD-ROM and the like. The wagering establishment 16 then provides an alphanumeric start-up identification code 33 which player 12 enters to actuate the gaming software 22. Optionally, the gaming computer 14 may include voice recognition means such as a voice chip or voice recognition software for recognizing the unique characteristics of the player's voice to deny access to any unauthorized user. Such hardware and/or software is known in the art. Gaming software 22 is programmed to prompt player 12 with an inquiry as to whether the current session is for practice or to place a wager. If it is a practice session, game program 24 generates a plurality of game choices and a confirmation that the games are being played for practice only. If player 12 chooses to engage in gambling, banking program 26 will permit actual wagering to the extent that there are sufficient wagering credits available in the player's account. If there are insufficient credits, player 12 must contact the wagering establishment 16 and go through the purchase credit sequence described below. As noted above, gaming computer 14 may or may not be on-line with the wagering establishment computer 30. If gaming computer 14 is off-line, greater flexibility in terms of being able to engage in gambling at virtually any location is possible. In an exemplary embodiment, a series of encrypted communication exchanges of, for example, alphanumeric codes, between player 12 and the agent 38 permit credit purchase and redemption at a remote location to be governed by the wagering establishment 16 notwithstanding the absence of an electronic link between the gaming computer 14 and the wagering establishment computer 30. Alternatively, gaming computer 14 can be networked to the wagering establishment computer 30 through the communications link 29 such that computer 30 monitors and controls all or part of the activities taking place on the remote gaming computer.

In the off-line embodiment shown in FIG. 1, player 12 places a call to the wagering establishment 16 by way of telephone 36 and communicates with agent 38 through telephone 40 to obtain or redeem gambling credit. If player 12 already has credit, gaming software 22 will permit wagering on any of the games of chance provided by game program 24 upon receiving player 12's personal identification code 32. If player 12 requires credit to play, the wagering establishment 16 must be contacted and the following series of steps are followed for the purpose of verifying the player's identity and confirming that the player is utilizing gaming software 22 registered to his or her personal identification code 32.

Whenever player 12 contacts the wagering establishment 16, he or she goes through what is referred to as a handshake recognition sequence, the verification of the player's identity with the wagering establishment. In this regard, as depicted in the flowchart of FIG. 5, player 12 first calls the wagering establishment 16 on telephone 36 and agent 38 who communicates through telephone 40, queries player

12 for his or her unique personal identification code 32 and software identification code 34. Agent 38 enters these codes into the computer 30 which generates an encrypted handshake code 42 which is provided to player 12 for entry into gaming computer 14. Gaming computer 14 decrypts handshake code 42 and then generates an encrypted recognition response code 44 which is then provided to the wagering establishment 16. Agent 38 enters recognition response code 44 into computer 30 which decrypts recognition response code 44 to verify player 12's identity and confirm that the specific gaming software 22 registered to player 12 is in use. Verified player 12 then proceeds with appropriate casino interaction.

FIG. 6 is a flowchart depicting a first embodiment of a purchase credit sequence in the off-line embodiment. Player 12 first contacts the wagering establishment 16 and establishes his or her identification through the handshake sequence depicted in FIG. 5 and described above. Agent 38 obtains an encrypted banking program activation code 46 from computer 30 and provides the same to player 12 for the purpose of allowing player 12 to access the credit purchasing/redemption function of banking program 26 in gaming computer 14. Player 12 then enters the amount of wagering credit requested. For security purposes, banking program 26 utilizes personal identification code 32 and software identification code 34 along with an encryption algorithm to generate a credit request code 48, which code embodies the numeric value of the amount of credit requested and is unique to player 12 and his or her gaming software 22. Credit request code 48 is displayed to player 12 on gaming computer 14, who then provides credit request code 48 to agent 38 for entry into the wagering establishment computer 30. The computer 30 applies a decryption key known only to the wagering establishment 16 to decrypt the credit request code 48 to reveal the amount of credit requested by player 12. Agent 38 orally confirms this amount with player 12. The wagering establishment 16 then decides whether or not to provide all or part of the credit requested. If the credit request is denied, player 12 is given an encrypted reactivation code 50 which is decrypted by gaming computer 14 to enable player 12 to continue wagering with any available credit balance (or player 12 has the option to cash-out any gambling winnings in accordance with the sequence depicted in FIG. 8 and described below). If the credit request is partially or fully granted, the process continues for the amount of wagering credit the wagering establishment 16 is willing to sell to player 12. The computer 30 generates an encrypted new credit code 52 which is provided to player 12 for the purposes of loading a pending amount of credit requested into the player's gaming computer 14 via the banking program 26 of the gambling software 22. Player 12 then enters new credit code 52 into gaming computer 14 which decrypts the code and reveals the exact amount of new credit being added to player 12's available credit balance. The amount of new credits are shown to player 12 as pending, but are not yet available for use. Banking program 26 then generates an encrypted credit pending code 54 which is based in part on the monetary value of the new credits pending. Player 12 provides this credit pending code 54 to agent 38 who enters the same into the wagering establishment computer 30, which then decrypts the credit pending code 54 to positively and irrefutably verify that the specific amount of credit requested was loaded into player 12's banking program 26. The wagering establishment computer 30 then generates an encrypted credit release code 56. This credit release code 56 is provided to player 12 who then enters it into gaming computer 14. The amount of pending credits are then released for use by player 12. The banking program 26 then generates an encrypted credit release verification code 58 which player 12 provides to agent 38. Agent 38 enters the credit release verification code 58 into computer 30 which decrypts the same and generates an encrypted program reactivation code 60. Player 12 receives the program reactivation code 60 and then enters the same into gaming computer 14 and gaming program 24 is reactivated for use. Simultaneously, the wagering establishment 16 charges player 12 for the value of credits purchased in a manner mutually agreed upon by the player and the casino. For example, a credit card may be charged, a bank transfer authorized, or some other form of payment or delayed payment may be made to the casino in exchange for the credits purchased. If at any point during this process one or more of the various encrypted codes do not match those expected by the casino encryption software, the player would be unable to access such credits. The gaming software 22 in such cases is disabled until the dispute is resolved. In this manner, the correct generation of each of the various codes by gaming computer 14 and casino computer 30 serves to positively confirm the amount and value of credits received by player 12 and that such credits were released and made available for player 12's use.

It will be appreciated that credit can also be provided to the player 12 in predetermined amounts, pre-installed on a dedicated gaming computer 14 (e.g., a personal digital assistant) provided by the wagering establishment 16. Alternatively, a player 12 could obtain a disk or module 90 having a given amount of authorized credit which is then "loaded" into the banking program gaming computer 14 to enable wagering until such time that this credit amount is exhausted. Alternatively, as shown in FIG. 1C and mentioned above can obtain credit by merely using his or her own credit card 93, either through communications with agent 38 or an electronic card-reader apparatus 91 connected to the issuing bank 95 as is well known in the art.

After player 12 has obtained wagering credit, he or she may place wagers by selecting wagering elements within various wagering events in any one of a plurality of games of chance offered by gaming software 22. Each game provides opportunities for player 12 to place wagers on one or more various wagering elements within a given wagering event depending upon the rules applicable to that game. As an example, the casino game of roulette involves a series of wagering events based upon the outcome of a random number selected by a ball spun within a roulette wheel. Each spin of the wheel is a single wagering event. Within that event, the player 12 may bet on many different wagering elements such as red and black colors, single numbers, groups of numbers and the like. All wagers for each event are placed prior to the spin of the wheel.

FIG. 7A is a flowchart depicting the wagering sequence for games of chance created by game program 24 which proceeds as follows. Player 12 first enters game program 24 of gaming software 22 and chooses a particular game on which to wager. Player 12 can wager on one or more events within the game as described above. Game program 24 prompts player 12 to confirm the placement of wagers made and the total amounts of wagers entered. Such wagers may be withdrawn or modified until such time as they are confirmed. Confirmation is typically made by having player 12 enter a confirmation code 62 prior to closing of all bets. Confirmation code 62 is provided by game program 24 and can be made different for every wager for security reasons. It can be a simple one or two digit alphanumeric code which is entered into game software 24 to confirm that each bet placed for any wagering event is what was intended and has not been placed in error. Game program 24 can be set up such that confirmation code 62 may be simplified further to a single key stroke in certain highly repetitive games such as slots or when the total value of all wagers falls below a certain predetermined level. After confirmation code 62 is entered by player 12, game program 24, in accordance with the rules of a given casino game, generates a specific outcome for a given wagerable event (e.g., cards are dealt, the wheel is spun, etc.). Game program 24 determines the outcome of each wager placed (win, lose or draw), calculates and then displays player 12's proposed correct payoff for that wager on gaming computer 14. Player 12 has the option to type in a yes/no code to accept the payoff outcome of all wagers or to dispute any payoff which player 12 believes is incorrect in some fashion. Any dispute can be handled by suspending the wagering process and calling agent 38 to resolve the matter by telephone or by some other means of dispute resolution. Once player 12 accepts the resolution of a given wagering event, the correct amount of credit is added or subtracted from player 12's wagering credit balance by banking program 26 of gaming software 22. Player 12 can then begin the wagering process all over again on a subsequent wagering event, or choose to end the gambling session. At any time, player 12 may select a review mode in game program 24 and review the amount and resolution of each and every wager made by player 12 and the results of such wagers in chronological order. At any time, player 12 can choose to redeem or cash-out all or part of the balance of wagering credits stored in banking program 26 through a credit cash-out sequence. Game program 24 can also contain special built-in instructions to place limitations on winnings at the discretion of the wagering establishment. It is also anticipated that such gaming software 22 could be embedded in another product, such as in a computer or other software, to provide a premium application which enables the purchaser of unrelated products to win something as governed by such an embedded program (e.g., a cash prize awarded).

FIGS. 7B-7C are flowcharts of wagering sequences for future public events of which the outcome is uncertain, such as a lottery, in the off-line embodiment. With regard to the description of lotteries herein, the wagering establishment will be hereinafter identified as a "lottery authority". The player 12 selects, by means of the gaming software 22, a particular lottery event (i.e., a drawing) on which to wager. The gaming computer 14 then generates a lottery "ticket" layout unique to the specific lottery and the player selects the desired wagering elements (i.e., numbers).

There are two types of exemplary lotteries described herein, the first being an instant type analogous to common scratch-off tickets, and the second being a future event of which the outcome is uncertain (i.e., a drawing takes place). In the case of instant lotteries, verification of the date/time of the wager is not important by definition since the essentially instantaneous output of the program determines the outcome. On the other hand, with future events, the date and time of the wager is critical in certain embodiments. It will be appreciated by the persons skilled in the art that a remote gaming arrangement whereby the player 12 participates in a lottery can be classified as either: (1) a non-registration system (by which the player wagers independently of the lottery authority 16 and the wager need not be registered with the lottery authority since the gaming computer 14 provides a means of time-stamping the wager) or (2) a registration system (by which the player 12 chooses the wagering elements on the remote gaming computer 14, but then must contact the lottery authority 16 to "register" the wager).

In a non-registration embodiment such as depicted in FIG. 7B, a wager is placed in the following manner: Player 12 logs on to the lottery application in the gaming computer 14 with his or her personal identification code 204, which is preassigned by the lottery authority 16 with whom the player 12 has preregistered. In this regard, an encryption/decryption device 82, depicted in FIG. 2 and described in more detail below, can be used to prevent minors from accessing the lottery program. Such device could utilize fingerprint or voice recognition hardware for additional verification. Player 12 then selects a specific lottery to play (e.g., Lotto). Player 12 then chooses the desired wagering elements 206 in a conventional manner, which choice may be confirmed upon the player receiving a suitable prompt. The gaming computer 14 then generates an encrypted, compressed multi-digit ticket code 208 representing the selected wagering elements 206, and an unforgeable date/time stamp 210. Optionally, such ticket code 208 may include a personal identification code 204 or software identification code 212. The ticket code 208 is stored in the gaming computer 14 and can be decrypted only by the lottery authority 16 for authentication. If desired, a physical "ticket" representing the player's choice in the encrypted ticket code could be printed by conventional printing means associated with the gaming computer 14. This procedure may be repeated as many times as necessary to participate in multiple lottery events or to chose wagering elements for a single event. Such an arrangement allows wagering to take place independent from the lottery authority 16. The unforgeable date/time stamp ensures that the player 12 cannot tamper with the wager "after the fact" (i.e., after the drawing, the player cannot modify the numbers selected). To cash-out, the player 12 provides the encrypted ticket code 208 to the lottery authority 16 which decrypts the ticket code to reveal the selected wagering elements and date/time of the wager. Winnings are then awarded in a conventional manner. It is anticipated that large winnings will require that the Player 12 return the physical device to the lottery authority 16 for verification.

FIG. 7C depicts a registration sequence whereby the player 12 registers his or her lottery choice(s) with the lottery authority 16. When player 12 is ready to do so, the lottery authority 16 is contacted through agent 38. The player 12 then enters his or her pin 204, either by pressing corresponding keys of the telephone, or on the gaming computer 14 (if these are placed on-line in either a temporary or permanent connection), or by speaking the selections through the telephone for acquisition by a voice recognition program of the type known in the art. For additional verification, player 12 can be asked to enter the computer or software identification code 212. The lottery authority 16 will request that the player 12 choose from a menu of lotteries which are still open for wagering, and the player then makes the desired selection(s). The player 12 then indicates the method of payment. In certain applications, credit can be pre-installed on the gaming computer 14 or module 90, as described above, in which case such credit can be included and represented in an encrypted ticket code 208. Normally, ticket-code 208 need not be encrypted in a registration embodiment (i.e., it merely represents the choice of wagering elements). If the ticket code is encrypted, it is then decrypted with a key known only to the lottery authority 16. This ensures and verifies that a valid lottery selection and sufficient credit were entered. The lottery authority 16 may confirm the transaction by reading back the wagering elements embodied in the code. After the lottery authority 16 accepts the ticket code 208, it generates a registration code 218 (encrypted or non-encrypted) which embodies the ticket code 208 and a current date/time stamp 220. The registration code 218 can be provided to the player 12 and is stored by the lottery authority 16 in the lottery authority computer 30 for future reference. The lottery authority 16 can then prompt the player to confirm the wager by entering a simple yes/no response. If desired, the lottery authority 16 can impose a limit on the number of wagers per player or per given time period and reject wagers exceeding set amounts. Optionally, the player 12 may obtain printed ticket receipts which include the registration code 218 from the gaming computer 14. The wagering process may be repeated for each "ticket" registered. When he or she is finished, the player 12 simply hangs up or terminates the connection with the lottery authority 16. After the lottery drawing or process, the lottery authority 16 compares any winning numbers against all registered tickets in accordance with conventional practice. If the prize is below a specific threshold (e.g., $100), then such prize can be credited to the player's account or credit card, or, if above a certain threshold, payouts can be made in a conventional manner.

In general, there are several ways by which the player 12 can cash-out winnings when such winnings are embodied or stored in the gaming computer 14. FIG. 8A is a flowchart diagram of the credit cash-out sequence in a first off-line embodiment. Player 12 first goes through the handshake sequence depicted in FIG. 5 and described above. Once player 12's identity is confirmed, the wagering establishment 16 provides player 12 with an encrypted banking activation code 64. Player 12 then activates banking program 26 and enters banking activation code 64 which is decrypted by gaming computer 14 to access the banking purchasing/redemption function. Player 12 then enters the amount of wagering credit he or she wants to cash-out into banking program 26. The amount to be cashed out is placed by banking program 26 into a cash out pending field. The player's banking program 26 then generates an encrypted credit cash-out code 66 which player 12 provides to wagering establishment 16. The agent 38 enters the credit cash-out code 66 into the wagering establishment computer 30 which decrypts the credit cash-out code 66 to reveal the amount of credit that player 12 is requesting to be cashed out, which amount is orally confirmed by casino agent 38. The wagering establishment computer 30 then generates an encrypted cash-out acknowledgment code 68 and provides this code to the player 12. Player 12 enters a cash-out acknowledgment code 68 into gaming computer 14 which decrypts the same, and banking program 26 then deducts the amount of credits to be cashed out of the player's credit balance available for future wagers. Banking program 26 then generates an encrypted deduction verification code 70 which indicates that the correct amount was deducted from the player's account. This code is then provided to agent 38 who enters it into computer 30. The wagering establishment computer 30 decrypts deduction verification code 70 and generates an encrypted program reactivation code 72 which is provided to player 12 to enable game program 24 to permit continued gambling with any available credits. The wagering establishment 16 then issues payment to player 12 for the amount of all wagering credit cashed out. The payment may be in the form of a credit to the player's credit card, a banking wire or some other mutually agreed-upon method of payment. It is also contemplated that where the player 12 has been provided with a dedicated gaming computer 14 (e.g., a hand-held device) credit may be cashed-out by simply bringing such gaming computer 14 to the wagering establishment 16 or its agent, where either the entire device itself is physically returned or a plug-in credit module 90 (tamper-proof, as described above) is exchanged.

FIGS. 9-12 contain flowcharts of an on-line embodiment schematically depicted in FIG. 2, whereby gaming computer 14 communicates directly through a communications link 29, such as a modem, with the wagering establishment computer 30. Computer 30 includes gaming software 74 comprised of a game program 76, banking program 77, audit program 78 and encryption/decryption algorithm 79. To prevent unauthorized access, an encryption/decryption device 82, such as that shown schematically in FIG. 2, is used by player 12 to generate a unique alphanumeric identification code 83 to log-on to computer 30 in order to obtain access to on-line gambling and/or purchasing and redeeming wagering credit. In one embodiment, device 82 looks like a credit-card calculator and includes a display 84, an integral keyboard 86 and internal encryption/decryption hardware and/or software. Such a device is currently used for making wireless money transfers, for example by Fleet Bank. Codes input and output to and from device 82 could be embodied in specific sounds identified through a dedicated sound recognition program which are transmitted to and received from computer 30. The encryption/decryption device 82 is used to generate encrypted log-on code 83 by encrypting player 12's personal identification code 32 with a separate verification code 88 provided to player 12 by computer 30. Alternatively, verification code 88 can be built into encryption/decryption device 82. Thus, knowledge of player 12's personal identification code 32 in and of itself is insufficient to enable an unauthorized third party such as a minor or known compulsive gambler to obtain access to gambling and/or purchasing and redeeming wagering credit. The computer 30 could contain appropriate instructions to, in such a case, terminate the on-line connection and prevent further attempts to gain access with that particular personal identification code 32. Moreover, the device 82 can have the banking program 26 associated therewith in order to store wagering credit independent of the gaming computer 14, in which case the exchange of codes between the device 82 and the gaming computer 14 would represent the actual "money". Thus, credit can be embodied in an apparatus structurally independent of the gaming computer.

FIG. 9 is a flowchart of the registration and start-up sequence. Initially, player 12 through gaming computer 14, dials up and connects through communications link 29 with computer 30. Player 12 then enters the requested registration information and is assigned a personal identification code 32. Player 12 then logs-on as described above. If player 12's identity is confirmed, computer 30 then permits wagering and/or credit purchase and redemption.

As shown in FIG. 10, the purchase credit sequence in the on-line embodiment is comprised of the following series of exchanges between player 12 and computer 30. Computer 30 first queries the player as to how much credit is desired for the particular gambling session. Player 12 responds at the prompt with the amount of wagering credit requested. The wagering establishment 16 then gets authorization for the requested amount through agreed upon methods of credit such as a credit card or the like. The approved credit amount is then deposited into player 12's wagering credit account in banking program 77. At such stage, player 12 can then wager on a plurality of games offered by the wagering establishment 16. In this connection, player 12 may at the end of each session, request an encrypted code number that verifies the amount of credit he or she has available from the wagering establishment 16 at that time for purposes of any future dispute resolution.

FIG. 11 is a flowchart of the gambling sequence in the on-line embodiment. Player 12 first activates gaming computer 14, establishes electronic communications with the wagering establishment computer 30 through communications link 29, and proceeds with the secure log-on procedure described above. Gaming computer 14 then registers a gambling session code 80 with the wagering establishment 16. The computer 30 then displays a choice of games of chance or future public events where the outcome is uncertain to be wagered upon.

FIG. 12 is a flowchart of the credit cash-out sequence in the on-line embodiment. Player 12 first requests to cash-out all or part of the credit balance in the wagering credit account maintained on casino computer 30. The wagering establishment 16 requests confirmation for the amount of credit to be cashed-out by player 12. Player 12 then keys in his or her personal identification code 32 to reconfirm that amount. The amount is then deducted from player 12's credit account and the wagering establishment 16 then authorizes a credit to be made to the player's preassigned credit card, or makes some other agreed-upon method of payment. For additional verification, the encryption/decryption device 82 can be used to provide a verification code to the wagering establishment 16 prior to cashing-out. Moreover, the wagering establishment 16 can be provided with a special telephone number to call-back player 12 to confirm the cash-out which can only then occur when player 12 calls the wagering establishment 16 back from that number, to provide an additional measure of security.

Alternatively, in another on-line embodiment, the gaming computer 14 includes gaming software 22 as in the first embodiment of FIG. 1, but the wagering establishment computer 30, through communications line 29 may or may not serve to regulate or control the gaming software simulation of casino games on gaming computer 14. For example, the wagering establishment computer 30 can directly keep a record of all or selected activates taking place at gaming computer 14 for purposes of additional verification or security. Alternatively, the electronic link can be of a control nature to vary the odds of a given wager based upon any of a variety of factors such as gambling duration or other factors such as a progressively increasing jackpot (e.g., in a slot machine simulation).

In the off-line embodiment, at all times, an encrypted audit-trail of all transactions can be recorded on storage media associated with the wagering establishment computer 30, and independently in gaming computer 14 to be ultimately downloaded to or accessed by the wagering establishment 16. Such an audit-trail can also be recorded in the tamper-proof read/write data storage media device 28 provided by the wagering establishment 16 to player 12 the wagering establishment in the embodiment shown in FIG. 3.

The present invention has been shown and described in what are considered to be the most practical and preferred embodiments. It is anticipated, however, that departures may be made therefrom and that obvious modifications will occur to persons skilled in the art.

WHAT IS CLAIMED IS:

1. A gaming system, comprising:

a host computer which enables a player at a remote location to purchase and redeem gambling credit and which generates at least one encrypted code to be provided from said host computer and which decrypts at least one encrypted code to be provided to said host computer;

an off-line gaming computer remotely disposed from said host computer on which the player wagers on at least one wagering opportunity, said gaming computer for generating at least one wagering opportunity and enabling the purchasing, storing and redeeming of gambling credit, said gaming computer further generating said at least one encrypted code to be provided to said host computer and decrypting said at least one encrypted code to be provided from said host computer, wherein said encrypted codes exchanged between said host computer and said gaming computer enable the player to at least one of purchase and redeem gambling credit.

2. The gaming system recited in Claim 1, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity and enabling said purchasing, storing and redeeming of gambling credit, provided on data storage media.

3. The gaming system recited in Claim 1, wherein said gaming computer communicates with data memory media disposed within a tamper-proof read/write apparatus.

4. The gaming system recited in Claim 2, wherein said gaming computer reads the unique magnetic characteristics of said data storage media for the purposes of creating a unique encrypted code to thereby prevent undetectable duplication of data stored on said data storage media.

5. The gaming system recited in Claim 1, wherein said gaming computer records and stores said codes provided to and from said gaming computer to generate an audit-trail.

6. The remote gaming system recited in Claim 1, wherein said host computer records and stores said codes provided to and from said host computer to generate an audit-trail.

7. The remote gaming system recited in Claim 1, wherein said gaming computer is provided with a predetermined amount of casino credit embodied in at least one of data storage media permanently installed on said gaming computer and data storage media removably installed on said gaming computer.

8. The remote gaming system recited in Claim 1, wherein said gaming computer includes at least one of voice recognition means for identifying the unique voice characteristics of the player and fingerprint identification means for identifying the unique fingerprint of the player.

9. The remote gaming system recited in Claim 1, wherein said wagering opportunity is a game of skill.

10. A gaming system, comprising:

a host computer which enables a player networked at a remote location to purchase and redeem gambling credit and wager on at least one wagering opportunity, said host computer generating at least one code to be communicated from said host computer and decrypting at least one encrypted code communicated to said host computer;

a gaming computer on which the player wagers on said at least one wagering opportunity where said gaming computer is remotely disposed from said host computer; and

means for generating at least one

encrypted code for communication to and decryption by said host computer to enable the player to access said host computer from said gaming computer.

11. The remote gaming system recited in Claim 10, wherein said means for generating said at least one encrypted code is embodied in an apparatus which is structurally independent of said gaming computer.

12. A gaming computer for use in a gaming system for wagering against a wagering establishment;

wherein said gaming computer generates and provides at least one wagering opportunity and enables a player at a remote location to wager on said at least one wagering opportunity and to purchase and redeem gambling credit from said wagering establishment.

13. The gaming computer recited in Claim 12, wherein a predetermined amount of said credit is pre-installed in said gaming computer by said wagering establishment.

14. The gaming computer recited in Claim 12, wherein said credit is redeemed from said wagering establishment by providing said wagering establishment with said gaming computer.

15. The gaming computer recited in Claim 12, wherein said credit is stored on detachable data memory media which interface with said gaming computer and where said data memory media are provided to said wagering establishment for credit redemption.

16. A gaming method by which a player gambles on a gaming computer against a wagering establishment where no on-line connection exists between the gaming computer and the wagering establishment, comprising the steps of:

(A) purchasing gambling credit from said wagering establishment and at least one of loading and preloading said gambling credit into said gaming computer;

(B) generating at least one wagering opportunity on said gaming computer;

(C) proceeding to wager on said at least one wagering opportunity presented on said gaming computer;

(D) accumulating wagering credits or debits on said gaming computer as a result of the outcome of said at least one wagering opportunity; and

(E) redeeming gambling credit from said wagering establishment by entering codes provided from said wagering establishment, at least one of which is encrypted, into said gaming computer which decrypts said at least one encrypted code and generates codes provided to said wagering establishment, at least one of which is encrypted, for decryption by said wagering establishment.

17. A gaming method by which a player having a personal identification code gambles against a wagering establishment on a gaming computer which presents a computer generated wagering opportunity where the gaming computer is at a remote location and networked to a host computer associated with the gaming establishment, comprising the steps of:

(A) establishing a secure on-line link between said gaming computer and said host computer by generating an encrypted log-on code embodying an identification code known only to the player and the wagering establishment and a separate code, said host computer then decrypting said encrypted log-on code for verification;

(B) purchasing gambling credit from said wagering establishment;

(C) generating at least one wagering opportunity on said gaming computer;

(D) proceeding to wager on said at least one wagering opportunity presented on said gaming computer; (E) accumulating wagering credits or debits as a result of the outcome of said at least one wagering opportunity; and

(F) redeeming gambling credit from said wagering establishment.

18. The method recited in Claim 17, wherein Step (F) further comprises generating an encrypted verification code embodying an identification code known only to the player and the wagering establishment and a separate code, to be decrypted by said host computer for verification prior to redeeming said gambling credit.

19. The method recited in Claim 17, wherein said encrypted log-on code is generated by an encryption/ decryption apparatus which is structurally independent of said gaming computer.

20. The method recited in Claim 17, wherein said gambling credit is embodied in an encryption/decryption apparatus which is structurally independent of said gaming computer.

21. A gaming system which enables a player at a remote location to wager against a wagering establishment, wherein the player wagers on a gaming computer where said gaming computer generates at least one wagering opportunity and enables the player to at least one of purchase gambling credit and redeem gambling winnings.

22. The gaming system recited in Claim 21, wherein said purchased pre-installed credit is embodied in a tamper-proof plug-in module, provided by the wagering establishment and interfaced with said gaming computer.

23. The gaming system recited in Claim 21, wherein said gambling winnings are electronically stored on a tamper-proof plug-in module provided by

the wagering establishment and interfaced with said gaming computer.

24. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity, and said gaming software resides on a tamper-proof chip disposed in an inspectable casing.

25. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity which includes a random distribution of codes known only to the wagering establishment to prevent unauthorized tampering with said gaming software.

26. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity, and means for receiving external keys input to said gaming software, said keys being used by said gaming software to function and which disable said gaming program if said gaming software has been tampered with.

27. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity upon receiving data from a source external to said gaming computer.

28. A gaming system which enables a player at a remote location to participate in a lottery by choosing a selection of wagering elements in a lottery on a gaming computer.

29. The gaming system recited in Claim 28, wherein said selection is combined, with at least one of a date/time stamp, player's identification code, and computer/software identification code, into a compressed ticket-code to be decrypted by a lottery authority for registration.

30. The gaming system recited in Claim 28,

wherein said selection is date/time stamped to form an encrypted ticket code for decryption by a lottery authority to reveal a valid wager.

31. A method by which a player participates in a lottery offered by a lottery authority, comprising the steps of:

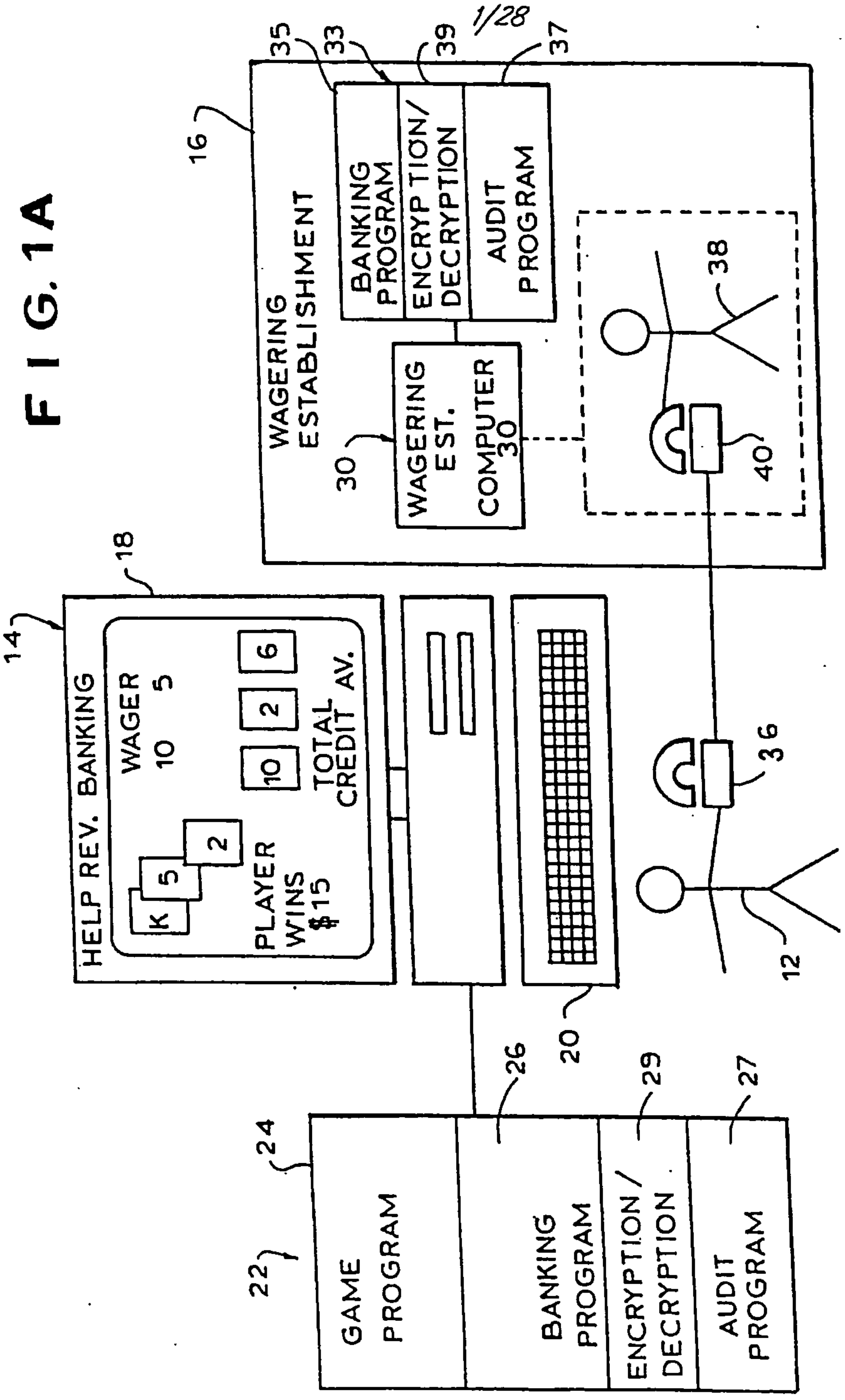
(A) choosing wagering elements for a given lottery event on a gaming computer;

(B) generating a ticket code on said gaming computer which embodies the choice of said wagering elements and at least one of a time/date stamp, player's identification code, computer identification code, and software identification code;

(C) registering the wager with the lottery authority by communicating said ticket code to the lottery authority, where said lottery authority has a host computer which decrypts said ticket code to reveal the player's choice of wagering elements;

(D) confirming the wager by generating an encrypted registration code on said host computer by encrypting said ticket code with a time/date stamp using an encryption algorithm known only to the lottery authority.

F I G. 1A


16
WAGERING ESTABLISHMENT
35
33
39
37
BANKING PROGRAM
ENCRYPTION/ DECRYPTION
AUDIT PROGRAM
30
WAGERING EST. COMPUTER 30
38
40
14
18
HELP REV. BANKING
K
5
2
PLAYER WINS $15
WAGER
10 5
10
2
6
TOTAL CREDIT AV.
36
12
20
26
29
27
22
24
GAME PROGRAM
BANKING PROGRAM
ENCRYPTION / DECRYPTION
AUDIT PROGRAM

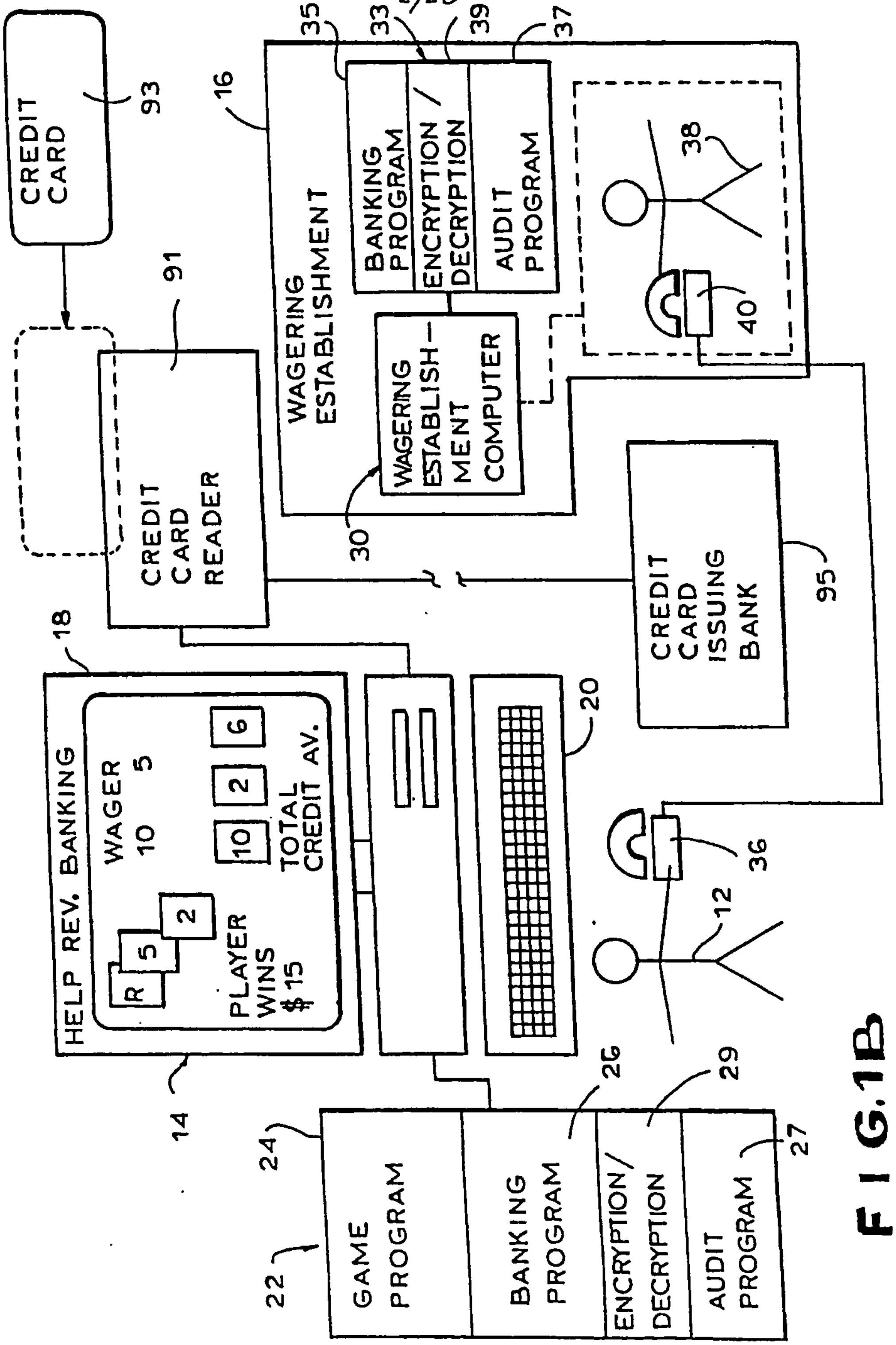

CREDIT CARD
93
91
CREDIT CARD READER
16
WAGERING ESTABLISHMENT
35
33
39
37
BANKING PROGRAM
ENCRYPTION / DECRYPTION
AUDIT PROGRAM
38
40
WAGERING ESTABLISH-MENT COMPUTER
30
CREDIT CARD ISSUING BANK
95
18
HELP REV. BANKING
WAGER
10
5
R
5
2
PLAYER WINS $15
10
2
6
TOTAL CREDIT AV.
14
20
36
12
26
29
24
27
22
GAME PROGRAM
BANKING PROGRAM
ENCRYPTION/ DECRYPTION
AUDIT PROGRAM

FIG.1B

FIG.1C

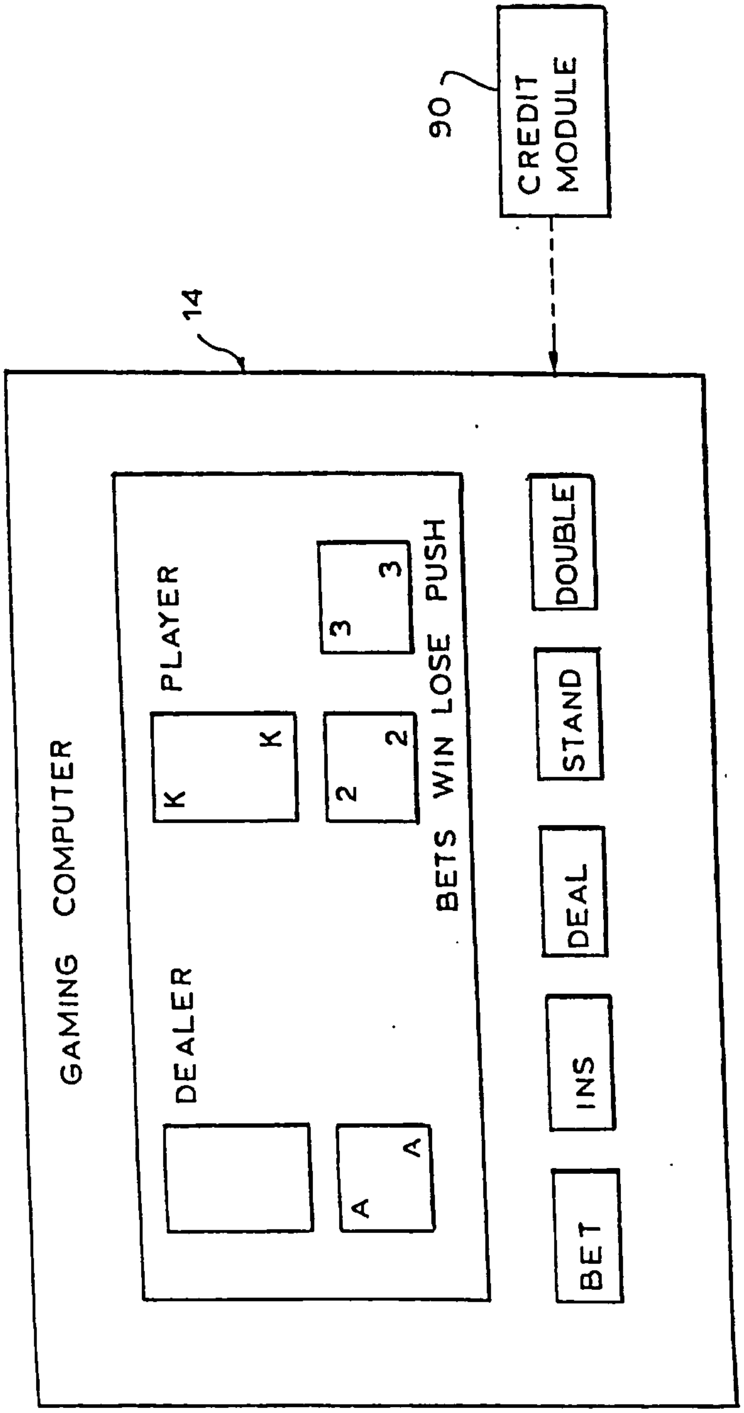
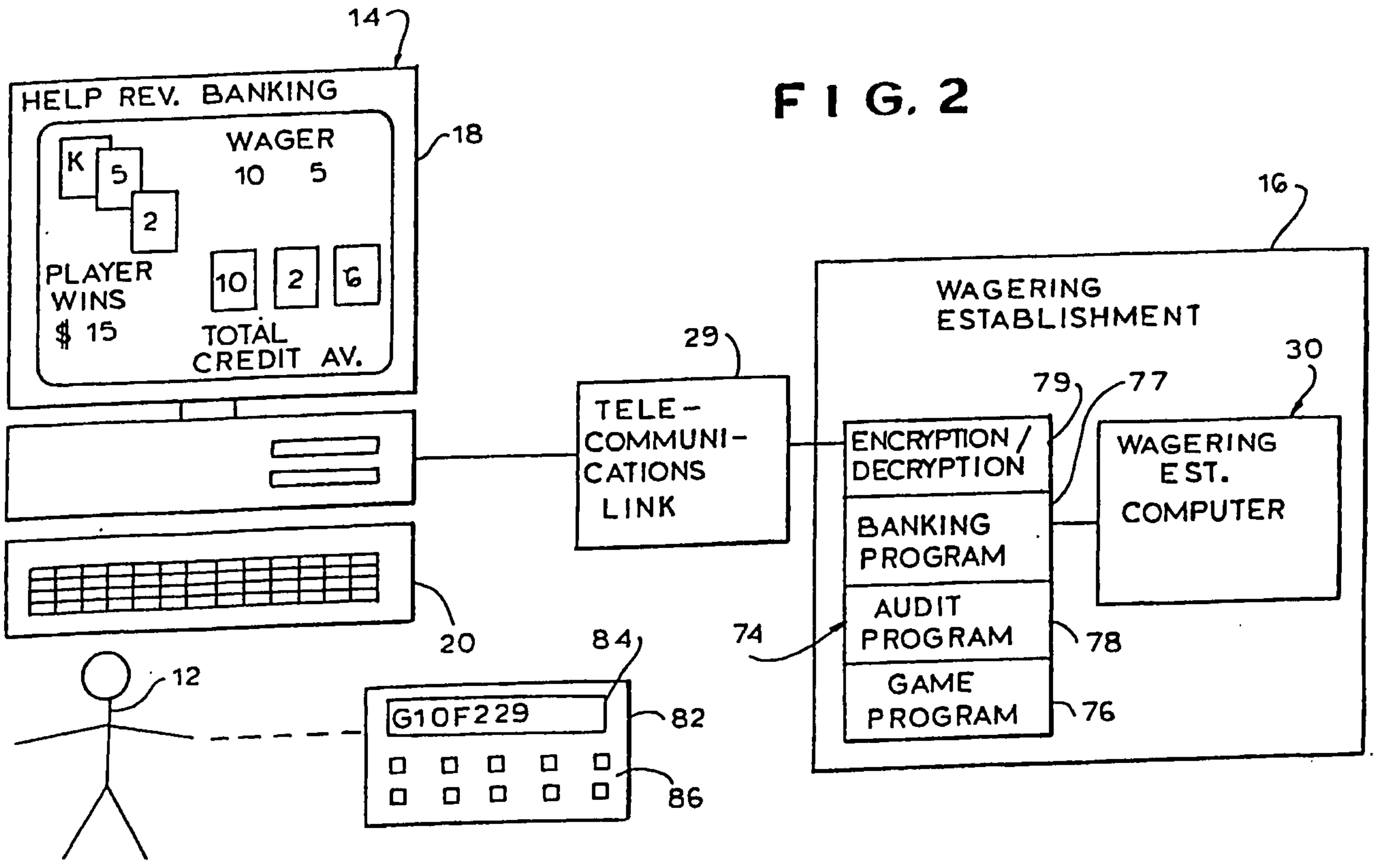
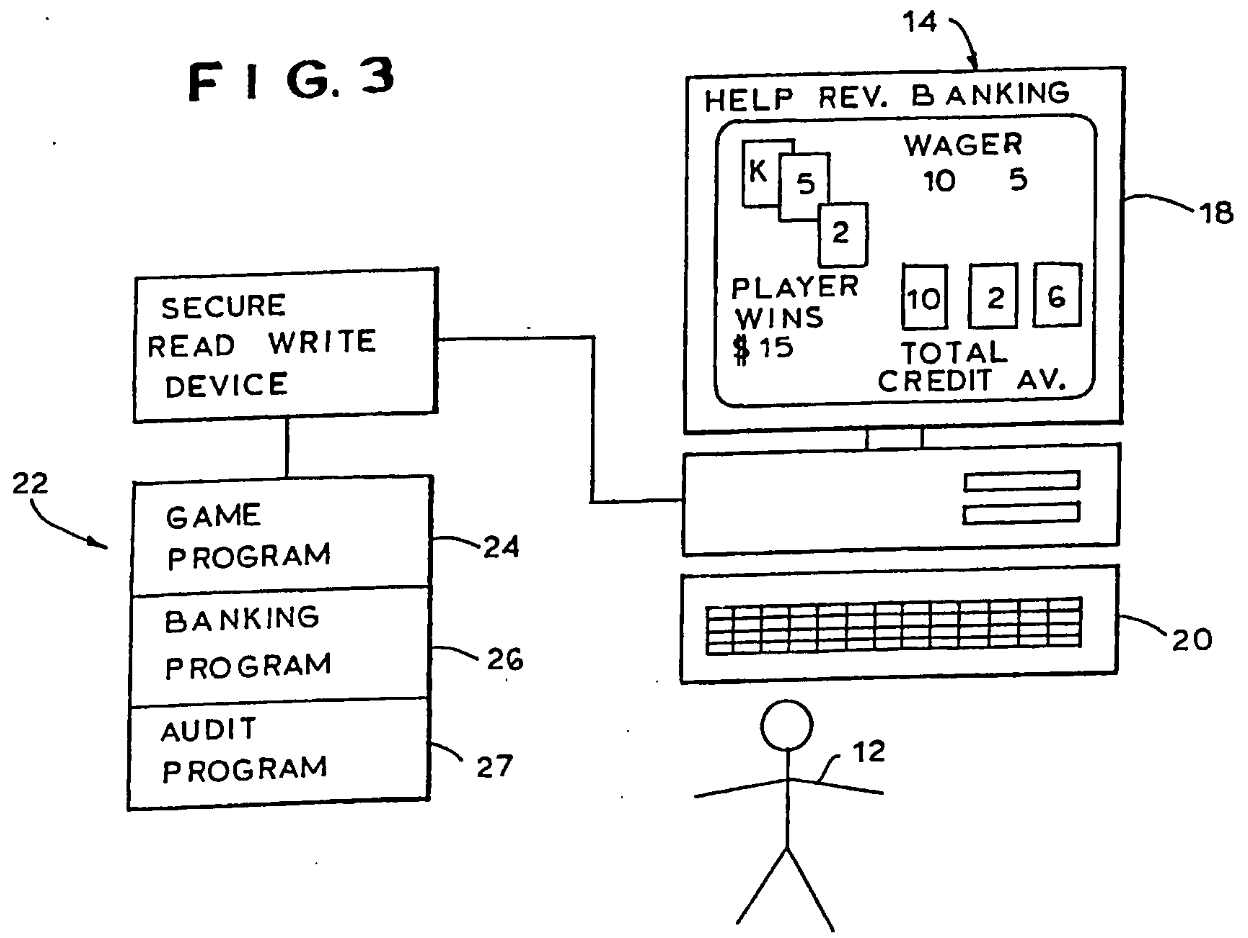

90
CREDIT MODULE
14
GAMING COMPUTER
DEALER
PLAYER
K
K
2
2
3
3
A
A
BETS WIN LOSE PUSH
BET
INS
DEAL
STAND
DOUBLE

FIG. 2


14
HELP REV. BANKING
18
K
5
2
WAGER
10 5
PLAYER
WINS
$ 15
10
2
6
TOTAL
CREDIT AV.
20
12
84
G1OF229
82
86
29
TELE-
COMMUNI-
CATIONS
LINK
16
WAGERING
ESTABLISHMENT
79
77
30
ENCRYPTION /
DECRYPTION
BANKING
PROGRAM
AUDIT
PROGRAM
GAME
PROGRAM
74
78
76
WAGERING
EST.
COMPUTER

F I G. 3


14
HELP REV. BANKING
K
5
2
WAGER
10 5
PLAYER
WINS
$15
10
2
6
TOTAL
CREDIT AV.
18
20
12
SECURE
READ WRITE
DEVICE
22
GAME
PROGRAM
24
BANKING
PROGRAM
26
AUDIT
PROGRAM
27

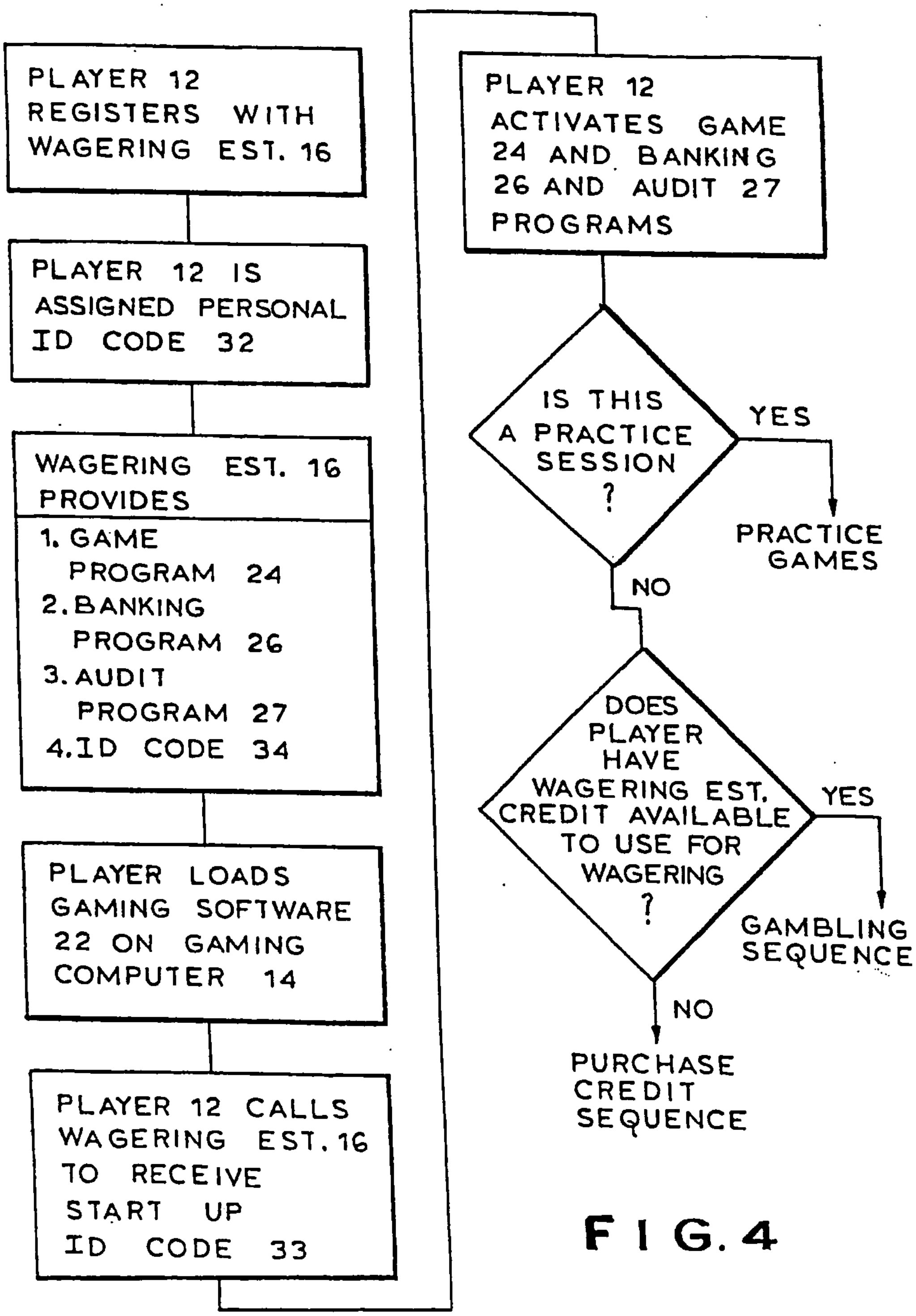

PLAYER 12 REGISTERS WITH WAGERING EST. 16
PLAYER 12 IS ASSIGNED PERSONAL ID CODE 32
WAGERING EST. 16 PROVIDES
1. GAME PROGRAM 24
2. BANKING PROGRAM 26
3. AUDIT PROGRAM 27
4. ID CODE 34
PLAYER LOADS GAMING SOFTWARE 22 ON GAMING COMPUTER 14
PLAYER 12 CALLS WAGERING EST. 16 TO RECEIVE START UP ID CODE 33
PLAYER 12 ACTIVATES GAME 24 AND BANKING 26 AND AUDIT 27 PROGRAMS
IS THIS A PRACTICE SESSION ?
YES
PRACTICE GAMES
NO
DOES PLAYER HAVE WAGERING EST. CREDIT AVAILABLE TO USE FOR WAGERING ?
YES
GAMBLING SEQUENCE
NO
PURCHASE CREDIT SEQUENCE

FIG. 4

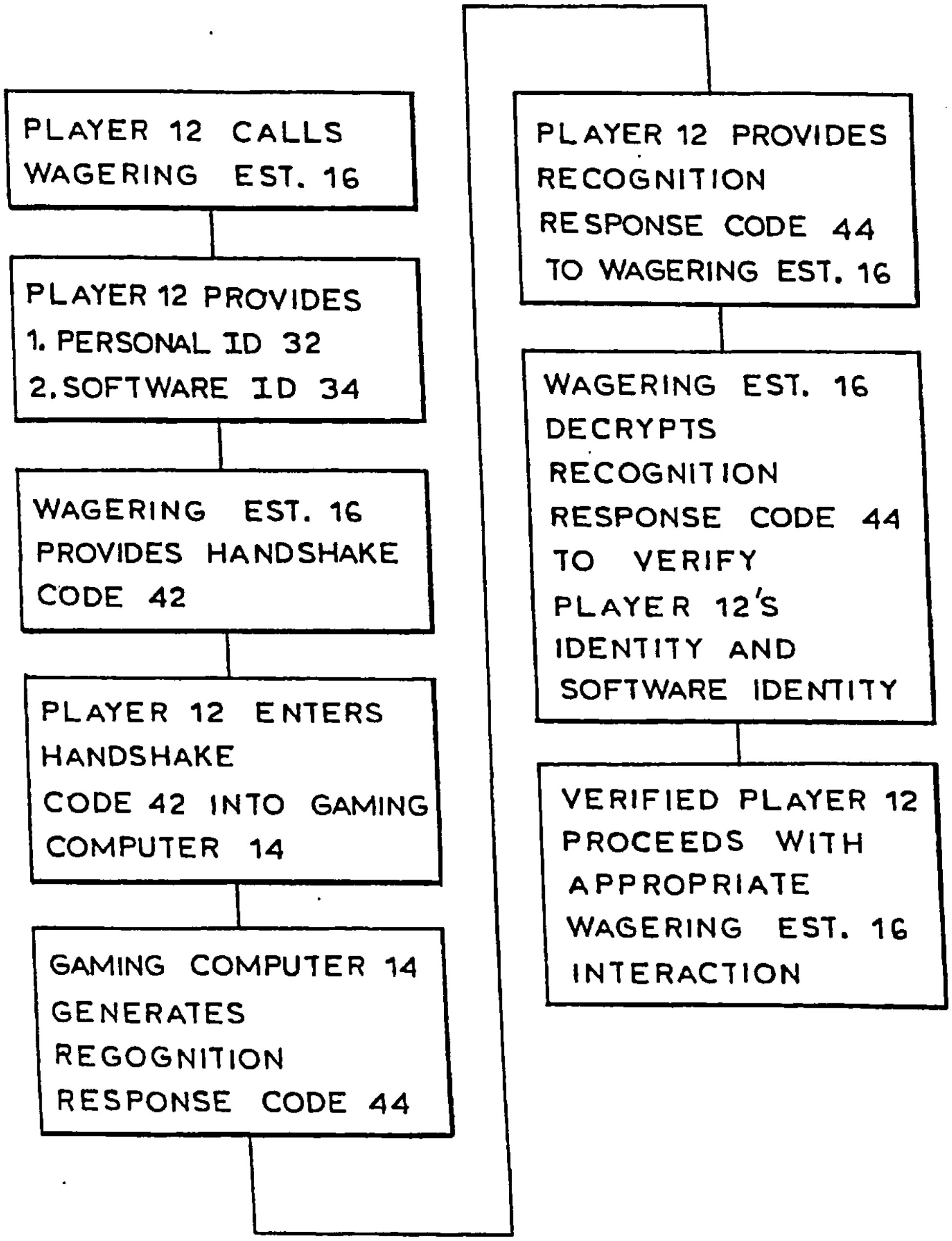
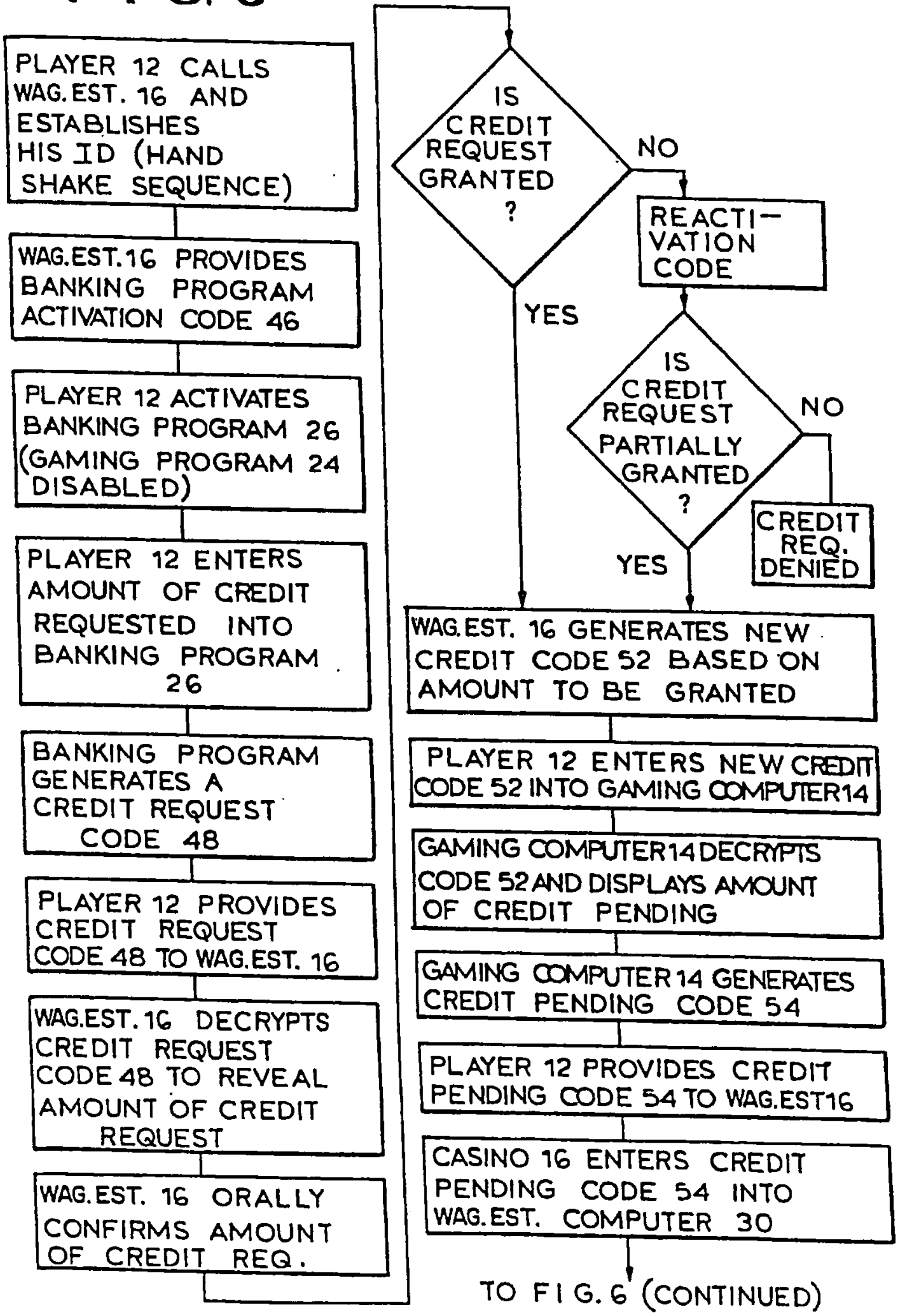

PLAYER 12 CALLS WAGERING EST. 16
PLAYER 12 PROVIDES 1. PERSONAL ID 32 2. SOFTWARE ID 34
WAGERING EST. 16 PROVIDES HANDSHAKE CODE 42
PLAYER 12 ENTERS HANDSHAKE CODE 42 INTO GAMING COMPUTER 14
GAMING COMPUTER 14 GENERATES REGOGNITION RESPONSE CODE 44
PLAYER 12 PROVIDES RECOGNITION RESPONSE CODE 44 TO WAGERING EST. 16
WAGERING EST. 16 DECRYPTS RECOGNITION RESPONSE CODE 44 TO VERIFY PLAYER 12'S IDENTITY AND SOFTWARE IDENTITY
VERIFIED PLAYER 12 PROCEEDS WITH APPROPRIATE WAGERING EST. 16 INTERACTION

FIG. 5

FIG. 6


PLAYER 12 CALLS WAG.EST. 16 AND ESTABLISHES HIS ID (HAND SHAKE SEQUENCE)
WAG.EST.16 PROVIDES BANKING PROGRAM ACTIVATION CODE 46
PLAYER 12 ACTIVATES BANKING PROGRAM 26 (GAMING PROGRAM 24 DISABLED)
PLAYER 12 ENTERS AMOUNT OF CREDIT REQUESTED INTO BANKING PROGRAM 26
BANKING PROGRAM GENERATES A CREDIT REQUEST CODE 48
PLAYER 12 PROVIDES CREDIT REQUEST CODE 48 TO WAG.EST. 16
WAG.EST.16 DECRYPTS CREDIT REQUEST CODE 48 TO REVEAL AMOUNT OF CREDIT REQUEST
WAG.EST. 16 ORALLY CONFIRMS AMOUNT OF CREDIT REQ.
IS CREDIT REQUEST GRANTED ?
NO
REACTI-VATION CODE
YES
IS CREDIT REQUEST PARTIALLY GRANTED ?
NO
CREDIT REQ. DENIED
YES
WAG.EST. 16 GENERATES NEW CREDIT CODE 52 BASED ON AMOUNT TO BE GRANTED
PLAYER 12 ENTERS NEW CREDIT CODE 52 INTO GAMING COMPUTER 14
GAMING COMPUTER 14 DECRYPTS CODE 52 AND DISPLAYS AMOUNT OF CREDIT PENDING
GAMING COMPUTER 14 GENERATES CREDIT PENDING CODE 54
PLAYER 12 PROVIDES CREDIT PENDING CODE 54 TO WAG.EST16
CASINO 16 ENTERS CREDIT PENDING CODE 54 INTO WAG. EST. COMPUTER 30

TO FIG. 6 (CONTINUED)

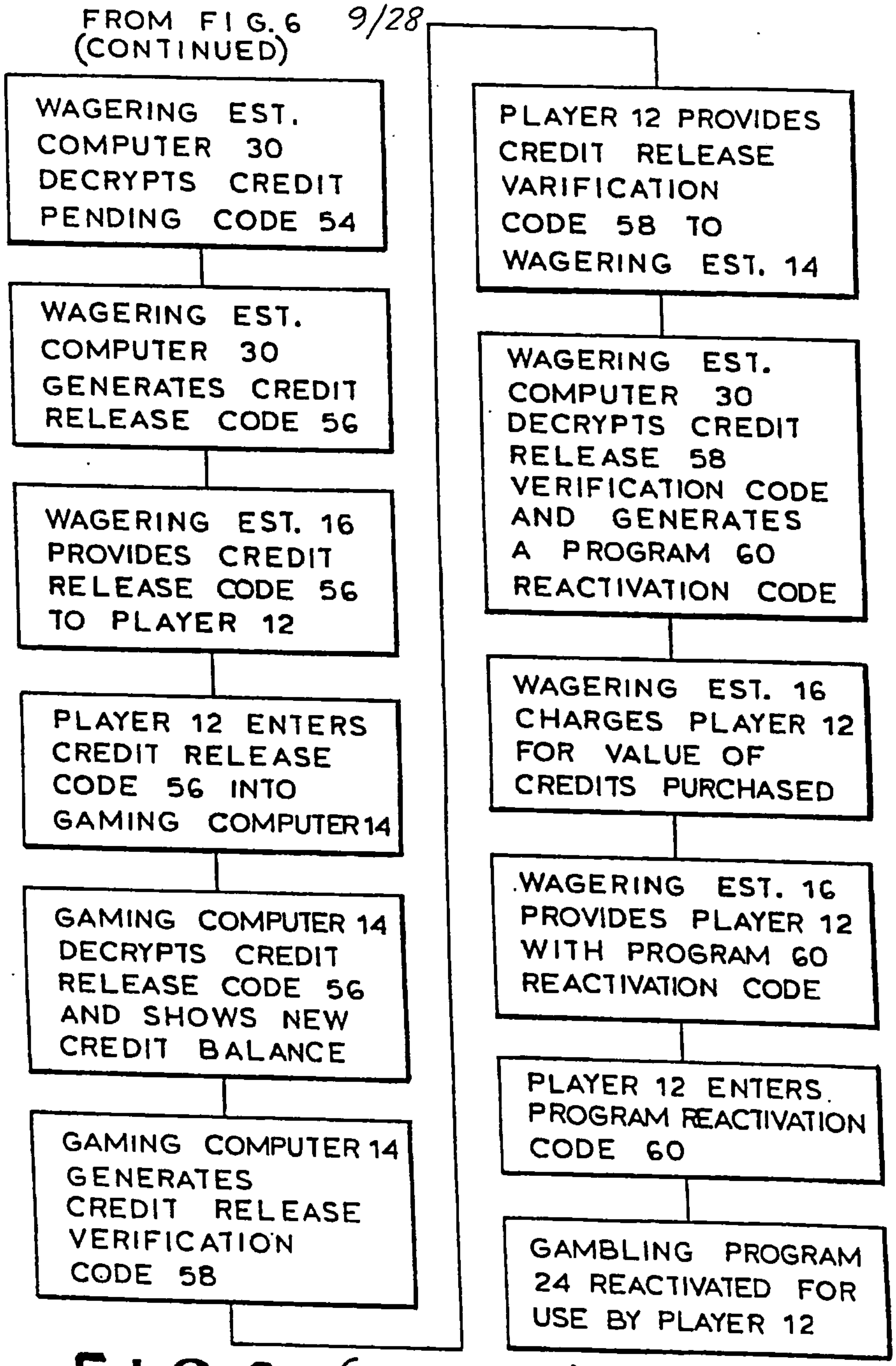
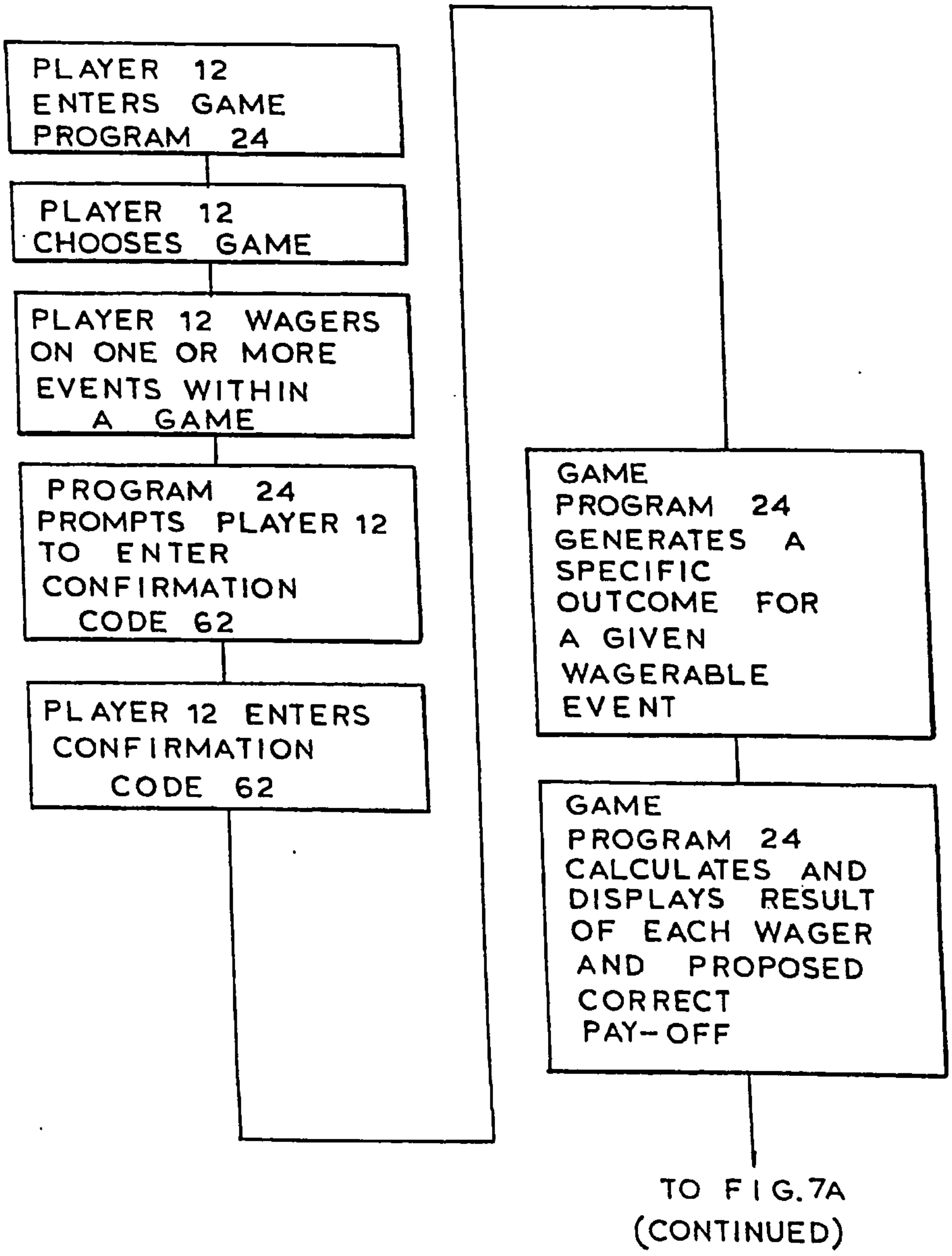

FROM FIG. 6 (CONTINUED)
WAGERING EST. COMPUTER 30 DECRYPTS CREDIT PENDING CODE 54
WAGERING EST. COMPUTER 30 GENERATES CREDIT RELEASE CODE 56
WAGERING EST. 16 PROVIDES CREDIT RELEASE CODE 56 TO PLAYER 12
PLAYER 12 ENTERS CREDIT RELEASE CODE 56 INTO GAMING COMPUTER 14
GAMING COMPUTER 14 DECRYPTS CREDIT RELEASE CODE 56 AND SHOWS NEW CREDIT BALANCE
GAMING COMPUTER 14 GENERATES CREDIT RELEASE VERIFICATION CODE 58
PLAYER 12 PROVIDES CREDIT RELEASE VARIFICATION CODE 58 TO WAGERING EST. 14
WAGERING EST. COMPUTER 30 DECRYPTS CREDIT RELEASE 58 VERIFICATION CODE AND GENERATES A PROGRAM 60 REACTIVATION CODE
WAGERING EST. 16 CHARGES PLAYER 12 FOR VALUE OF CREDITS PURCHASED
WAGERING EST. 16 PROVIDES PLAYER 12 WITH PROGRAM 60 REACTIVATION CODE
PLAYER 12 ENTERS PROGRAM REACTIVATION CODE 60
GAMBLING PROGRAM 24 REACTIVATED FOR USE BY PLAYER 12

FIG. 6 (CONTINUED)

FIG. 7A


PLAYER 12 ENTERS GAME PROGRAM 24
PLAYER 12 CHOOSES GAME
PLAYER 12 WAGERS ON ONE OR MORE EVENTS WITHIN A GAME
PROGRAM 24 PROMPTS PLAYER 12 TO ENTER CONFIRMATION CODE 62
PLAYER 12 ENTERS CONFIRMATION CODE 62
GAME PROGRAM 24 GENERATES A SPECIFIC OUTCOME FOR A GIVEN WAGERABLE EVENT
GAME PROGRAM 24 CALCULATES AND DISPLAYS RESULT OF EACH WAGER AND PROPOSED CORRECT PAY-OFF
TO FIG.7A (CONTINUED)

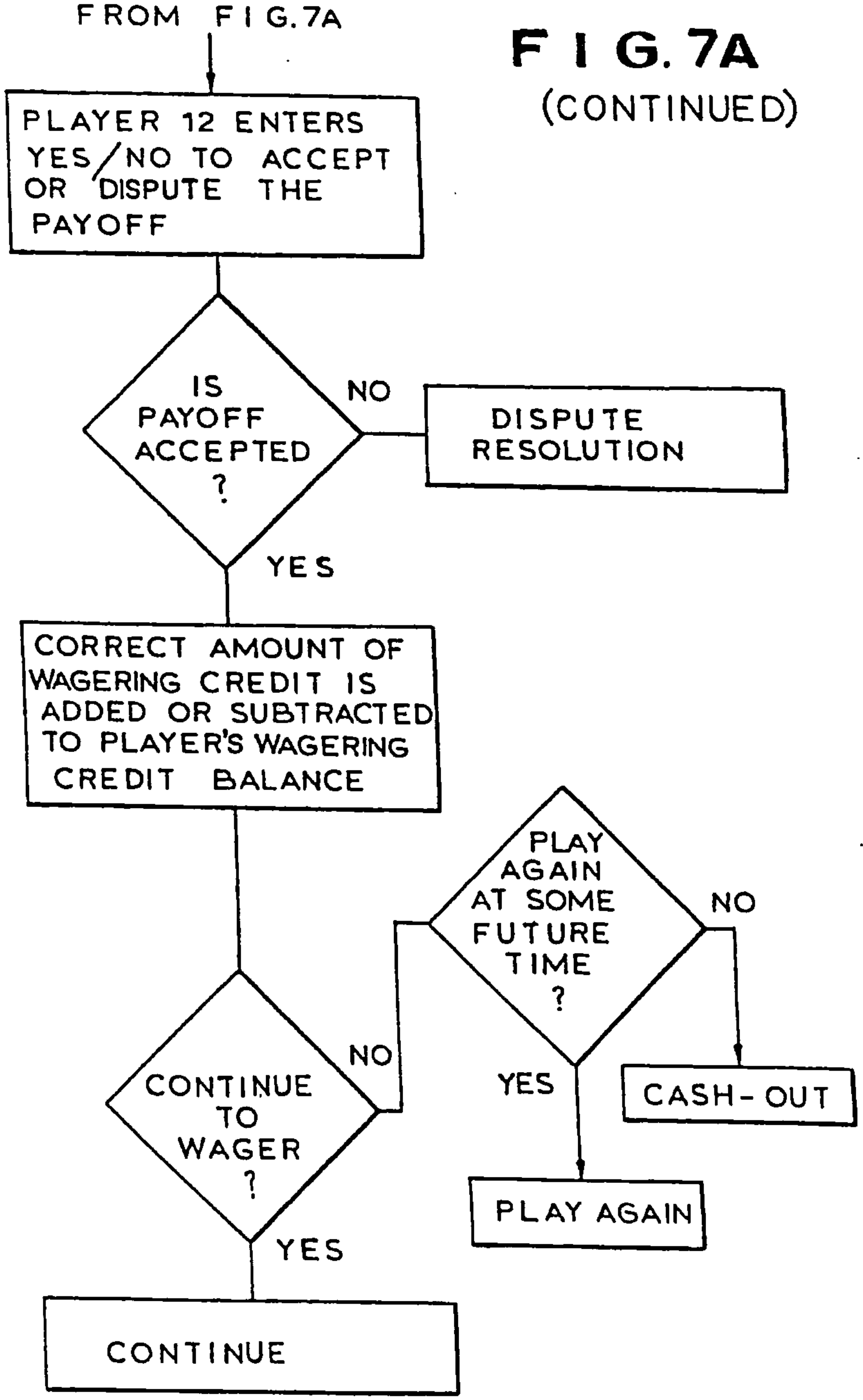

FROM FIG.7A
PLAYER 12 ENTERS YES/NO TO ACCEPT OR DISPUTE THE PAYOFF
IS PAYOFF ACCEPTED ?
NO
DISPUTE RESOLUTION
YES
CORRECT AMOUNT OF WAGERING CREDIT IS ADDED OR SUBTRACTED TO PLAYER'S WAGERING CREDIT BALANCE
PLAY AGAIN AT SOME FUTURE TIME ?
NO
CASH-OUT
YES
PLAY AGAIN
CONTINUE TO WAGER ?
NO
YES
CONTINUE

FIG.7A (CONTINUED)

FIG. 7B-1

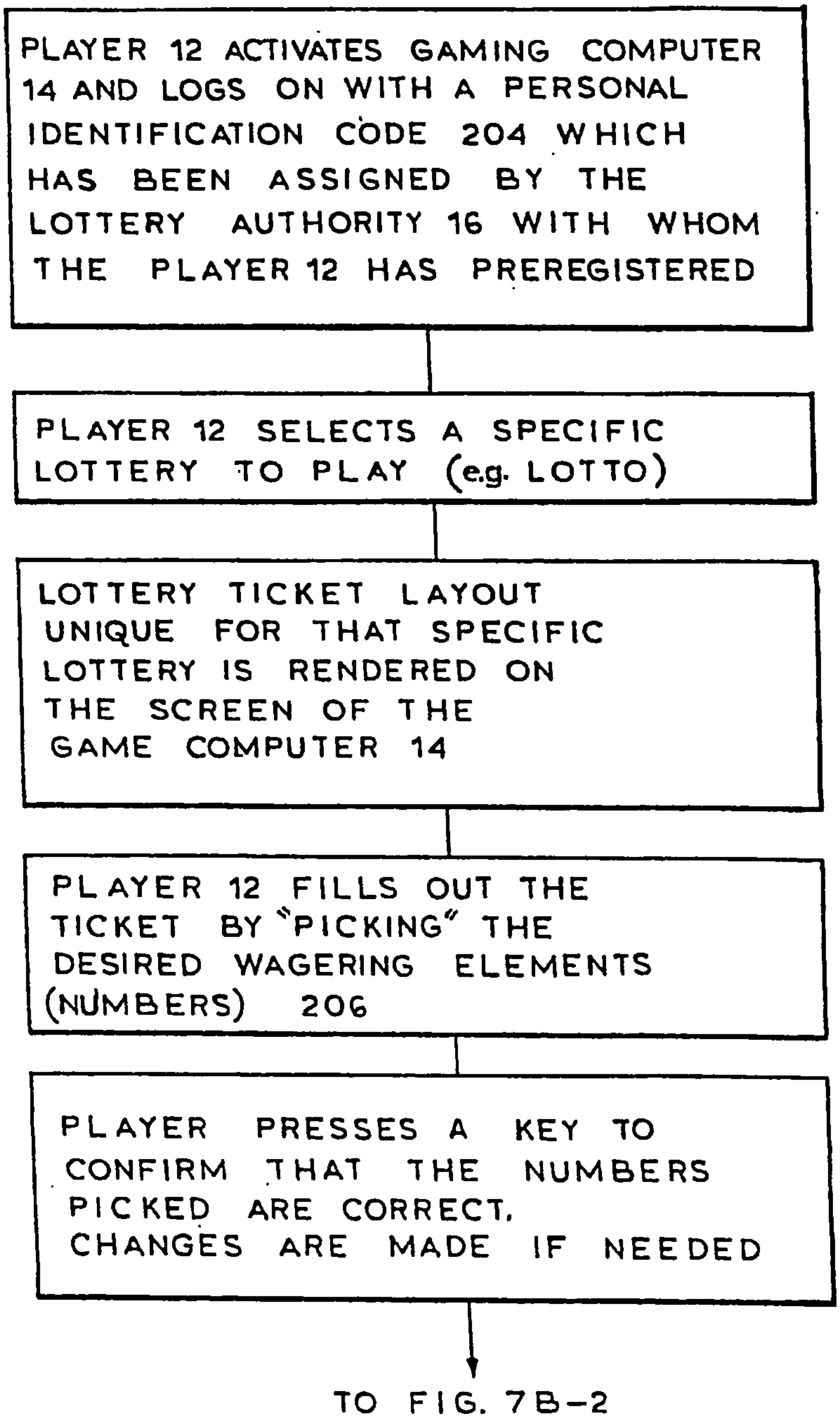

PLAYER 12 ACTIVATES GAMING COMPUTER 14 AND LOGS ON WITH A PERSONAL IDENTIFICATION CODE 204 WHICH HAS BEEN ASSIGNED BY THE LOTTERY AUTHORITY 16 WITH WHOM THE PLAYER 12 HAS PREREGISTERED
PLAYER 12 SELECTS A SPECIFIC LOTTERY TO PLAY (e.g. LOTTO)
LOTTERY TICKET LAYOUT UNIQUE FOR THAT SPECIFIC LOTTERY IS RENDERED ON THE SCREEN OF THE GAME COMPUTER 14
PLAYER 12 FILLS OUT THE TICKET BY "PICKING" THE DESIRED WAGERING ELEMENTS (NUMBERS) 206
PLAYER PRESSES A KEY TO CONFIRM THAT THE NUMBERS PICKED ARE CORRECT. CHANGES ARE MADE IF NEEDED
TO FIG. 7B-2

FIG. 7B-2

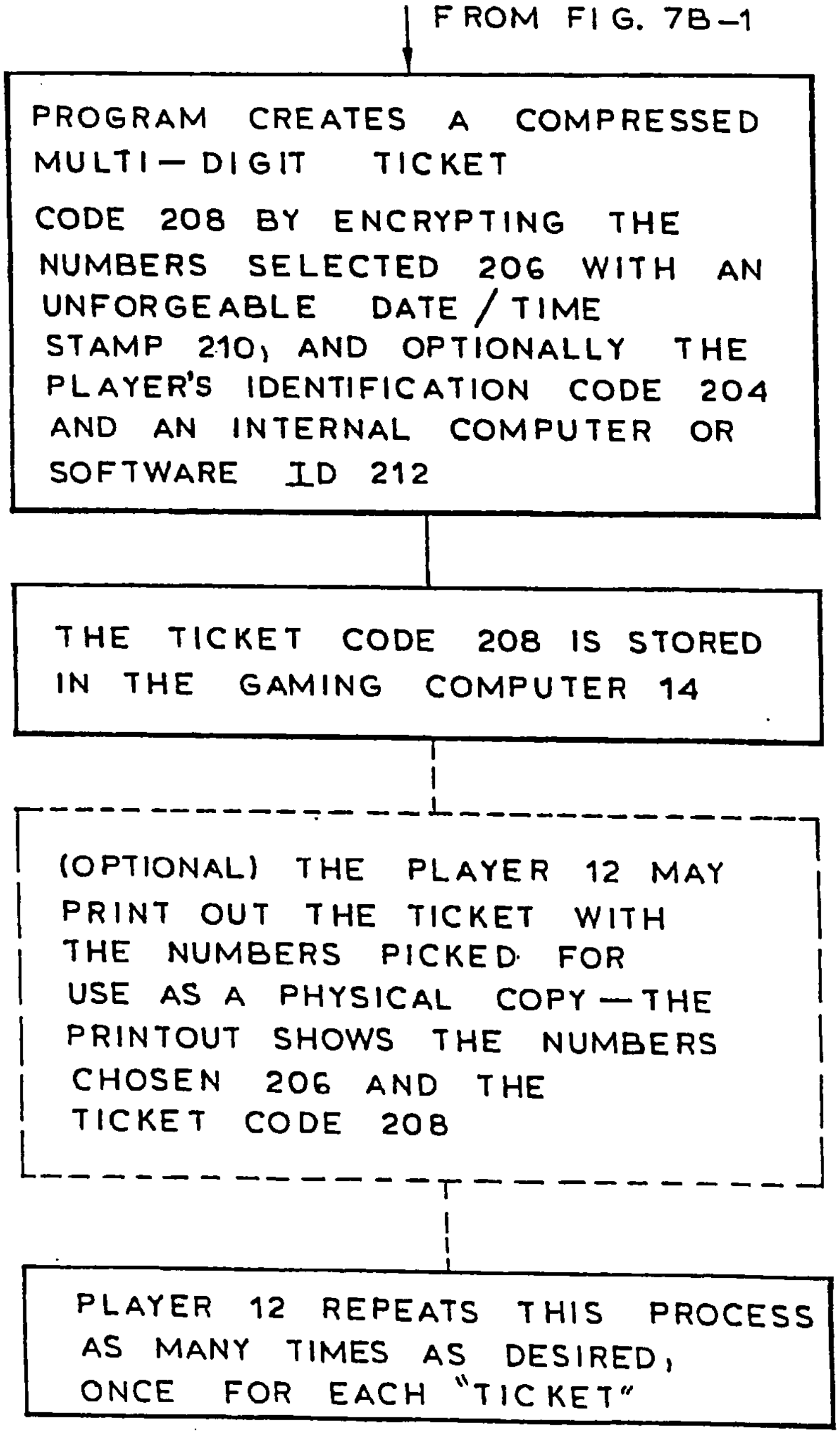
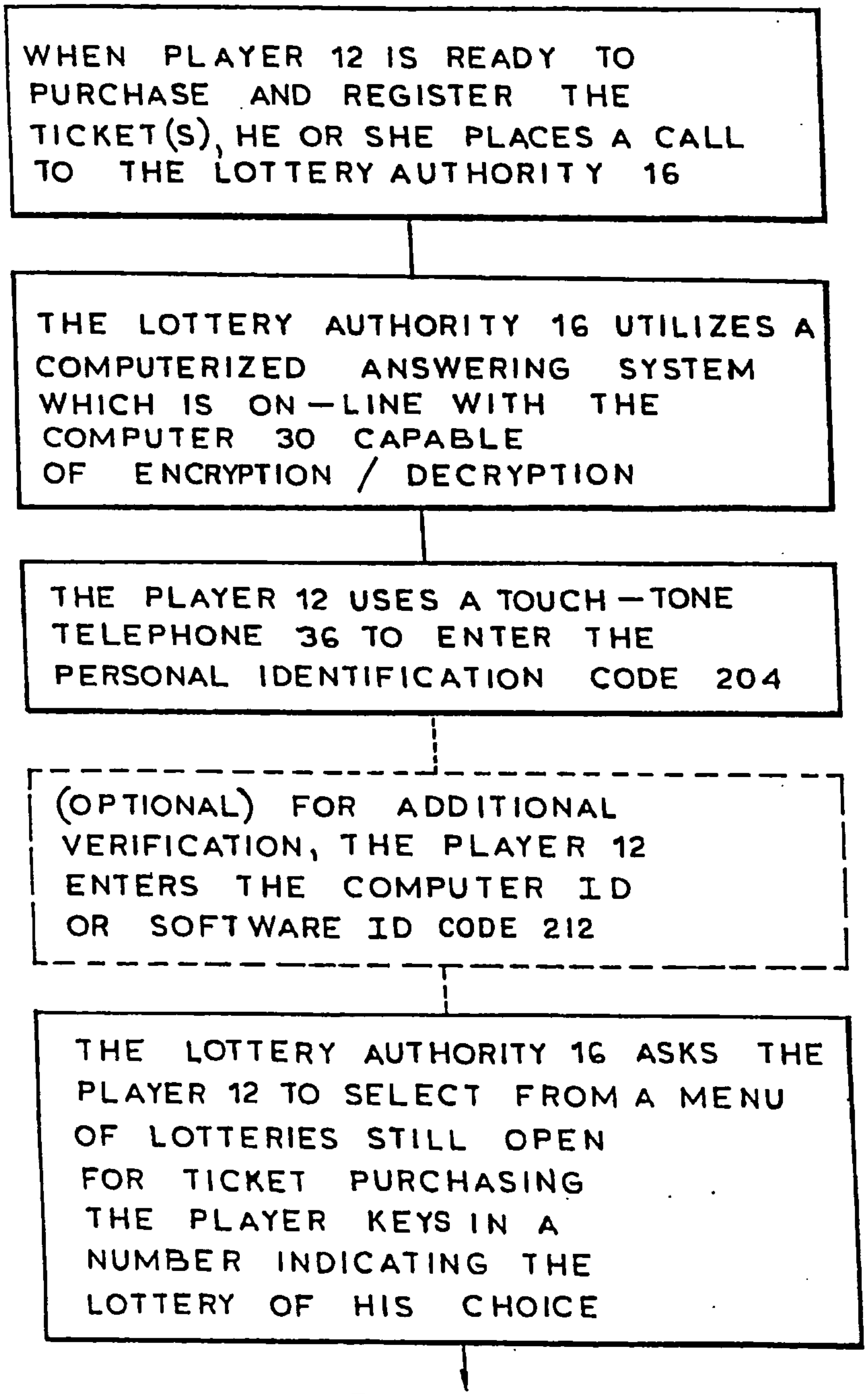

FROM FIG. 7B-1
PROGRAM CREATES A COMPRESSED MULTI-DIGIT TICKET CODE 208 BY ENCRYPTING THE NUMBERS SELECTED 206 WITH AN UNFORGEABLE DATE / TIME STAMP 210, AND OPTIONALLY THE PLAYER'S IDENTIFICATION CODE 204 AND AN INTERNAL COMPUTER OR SOFTWARE ID 212
THE TICKET CODE 208 IS STORED IN THE GAMING COMPUTER 14
(OPTIONAL) THE PLAYER 12 MAY PRINT OUT THE TICKET WITH THE NUMBERS PICKED FOR USE AS A PHYSICAL COPY — THE PRINTOUT SHOWS THE NUMBERS CHOSEN 206 AND THE TICKET CODE 208
PLAYER 12 REPEATS THIS PROCESS AS MANY TIMES AS DESIRED, ONCE FOR EACH "TICKET"

FIG. 7C-1



WHEN PLAYER 12 IS READY TO PURCHASE AND REGISTER THE TICKET(S), HE OR SHE PLACES A CALL TO THE LOTTERY AUTHORITY 16

THE LOTTERY AUTHORITY 16 UTILIZES A COMPUTERIZED ANSWERING SYSTEM WHICH IS ON-LINE WITH THE COMPUTER 30 CAPABLE OF ENCRYPTION / DECRYPTION

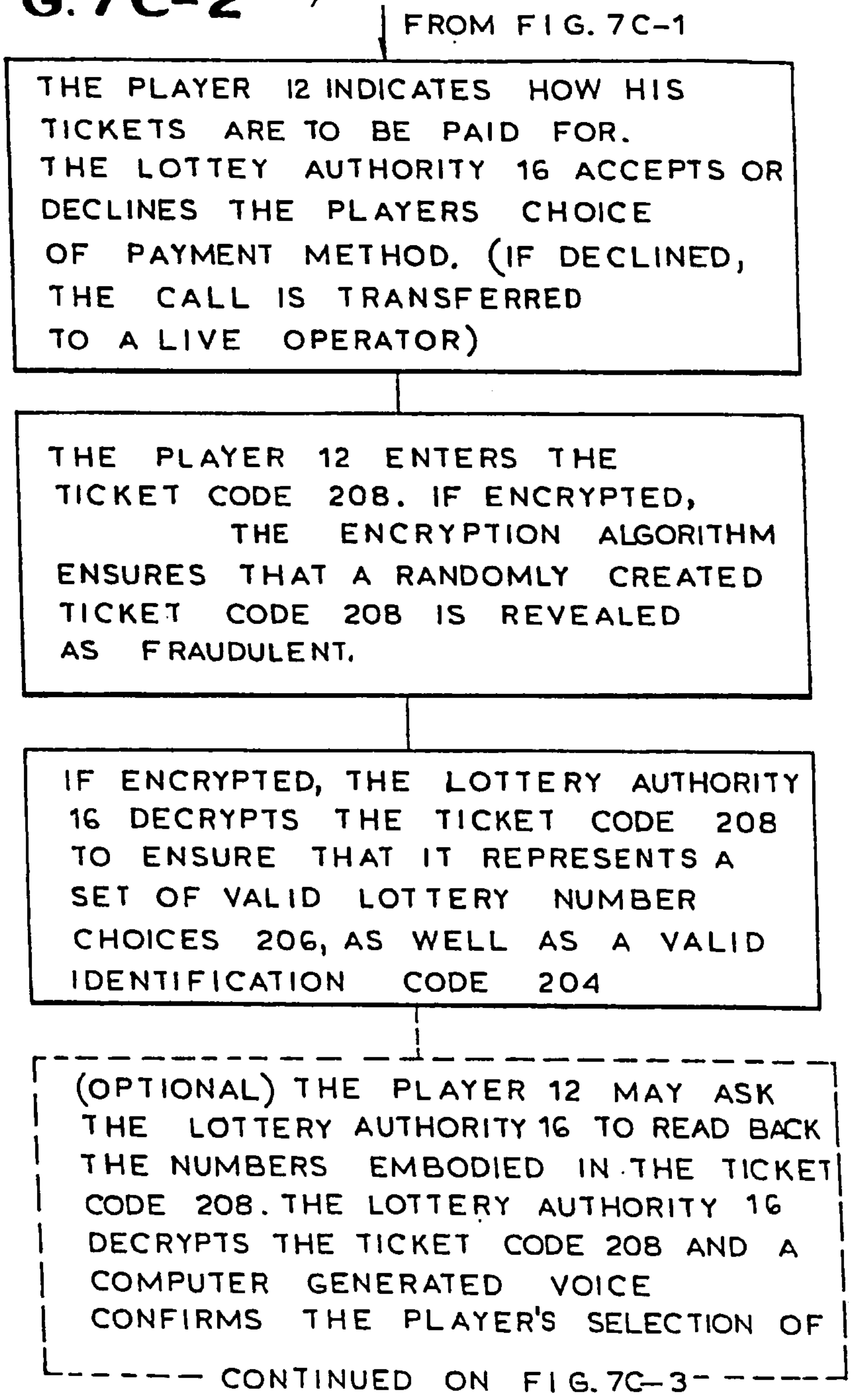
THE PLAYER 12 USES A TOUCH-TONE TELEPHONE 36 TO ENTER THE PERSONAL IDENTIFICATION CODE 204

(OPTIONAL) FOR ADDITIONAL VERIFICATION, THE PLAYER 12 ENTERS THE COMPUTER ID OR SOFTWARE ID CODE 212

THE LOTTERY AUTHORITY 16 ASKS THE PLAYER 12 TO SELECT FROM A MENU OF LOTTERIES STILL OPEN FOR TICKET PURCHASING THE PLAYER KEYS IN A NUMBER INDICATING THE LOTTERY OF HIS CHOICE

TO FIG. 7C-2

FIG.7C-2



FROM FIG. 7C-1

THE PLAYER 12 INDICATES HOW HIS TICKETS ARE TO BE PAID FOR. THE LOTTEY AUTHORITY 16 ACCEPTS OR DECLINES THE PLAYERS CHOICE OF PAYMENT METHOD. (IF DECLINED, THE CALL IS TRANSFERRED TO A LIVE OPERATOR)

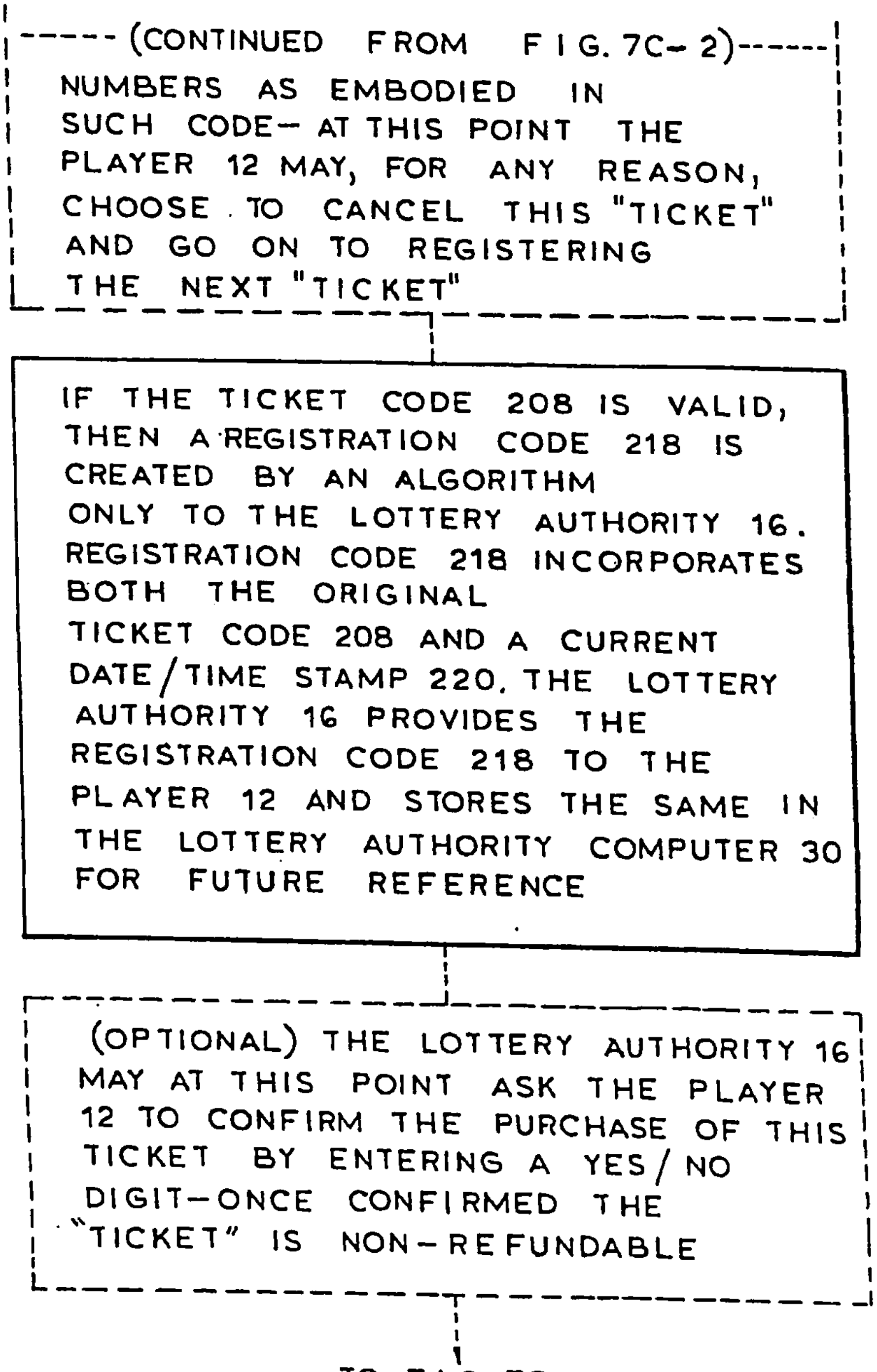
THE PLAYER 12 ENTERS THE TICKET CODE 208. IF ENCRYPTED, THE ENCRYPTION ALGORITHM ENSURES THAT A RANDOMLY CREATED TICKET CODE 208 IS REVEALED AS FRAUDULENT.

IF ENCRYPTED, THE LOTTERY AUTHORITY 16 DECRYPTS THE TICKET CODE 208 TO ENSURE THAT IT REPRESENTS A SET OF VALID LOTTERY NUMBER CHOICES 206, AS WELL AS A VALID IDENTIFICATION CODE 204

(OPTIONAL) THE PLAYER 12 MAY ASK THE LOTTERY AUTHORITY 16 TO READ BACK THE NUMBERS EMBODIED IN THE TICKET CODE 208. THE LOTTERY AUTHORITY 16 DECRYPTS THE TICKET CODE 208 AND A COMPUTER GENERATED VOICE CONFIRMS THE PLAYER'S SELECTION OF

CONTINUED ON FIG. 7C-3

FIG. 7C-3



(CONTINUED FROM FIG. 7C-2)

NUMBERS AS EMBODIED IN SUCH CODE— AT THIS POINT THE PLAYER 12 MAY, FOR ANY REASON, CHOOSE TO CANCEL THIS "TICKET" AND GO ON TO REGISTERING THE NEXT "TICKET"

IF THE TICKET CODE 208 IS VALID, THEN A REGISTRATION CODE 218 IS CREATED BY AN ALGORITHM ONLY TO THE LOTTERY AUTHORITY 16. REGISTRATION CODE 218 INCORPORATES BOTH THE ORIGINAL TICKET CODE 208 AND A CURRENT DATE/TIME STAMP 220. THE LOTTERY AUTHORITY 16 PROVIDES THE REGISTRATION CODE 218 TO THE PLAYER 12 AND STORES THE SAME IN THE LOTTERY AUTHORITY COMPUTER 30 FOR FUTURE REFERENCE

(OPTIONAL) THE LOTTERY AUTHORITY 16 MAY AT THIS POINT ASK THE PLAYER 12 TO CONFIRM THE PURCHASE OF THIS TICKET BY ENTERING A YES/NO DIGIT—ONCE CONFIRMED THE "TICKET" IS NON-REFUNDABLE

TO FIG. 7C-4

FIG.7C-4

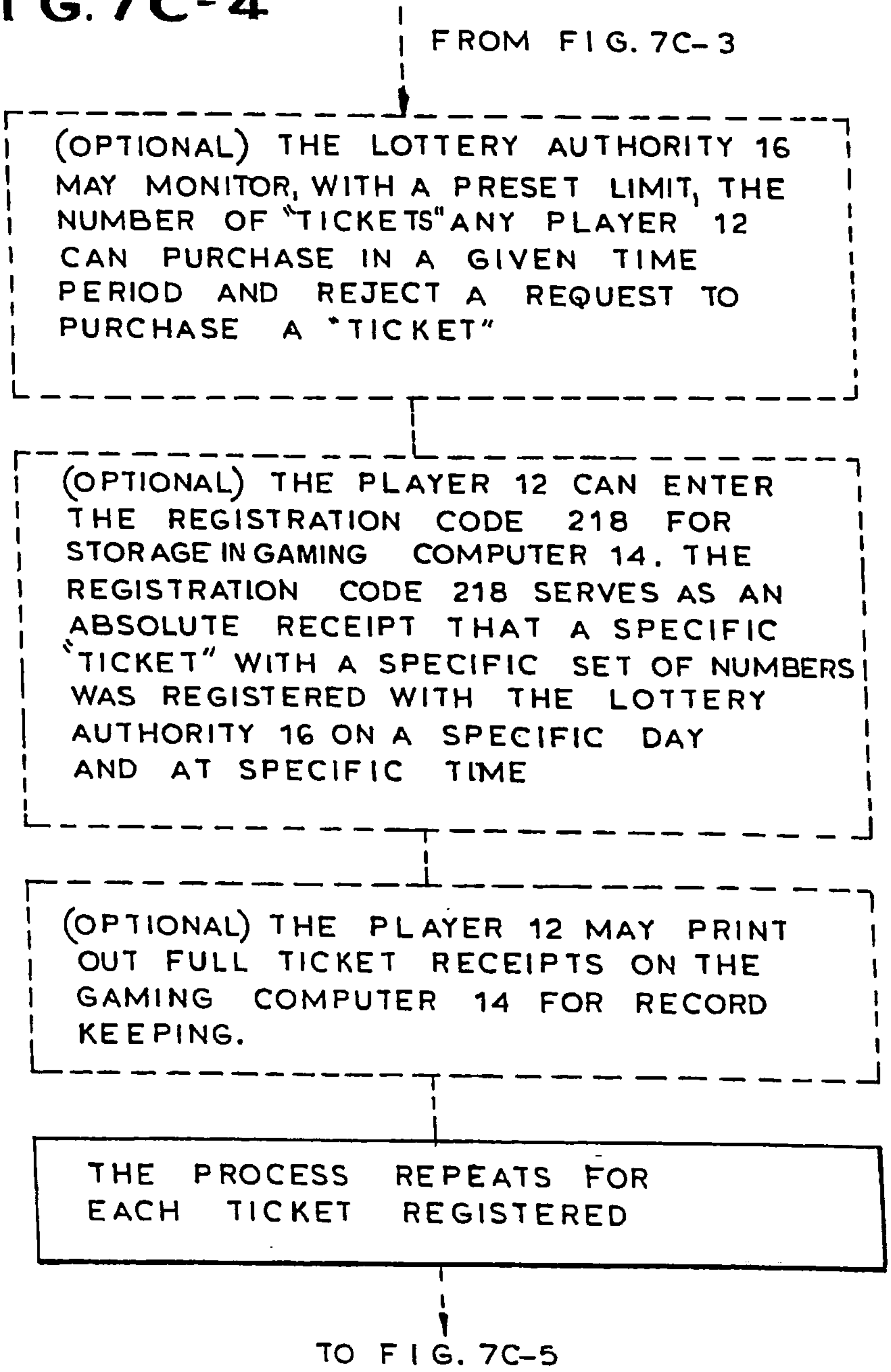

FROM FIG. 7C-3
(OPTIONAL) THE LOTTERY AUTHORITY 16 MAY MONITOR, WITH A PRESET LIMIT, THE NUMBER OF "TICKETS" ANY PLAYER 12 CAN PURCHASE IN A GIVEN TIME PERIOD AND REJECT A REQUEST TO PURCHASE A "TICKET"
(OPTIONAL) THE PLAYER 12 CAN ENTER THE REGISTRATION CODE 218 FOR STORAGE IN GAMING COMPUTER 14. THE REGISTRATION CODE 218 SERVES AS AN ABSOLUTE RECEIPT THAT A SPECIFIC "TICKET" WITH A SPECIFIC SET OF NUMBERS WAS REGISTERED WITH THE LOTTERY AUTHORITY 16 ON A SPECIFIC DAY AND AT SPECIFIC TIME
(OPTIONAL) THE PLAYER 12 MAY PRINT OUT FULL TICKET RECEIPTS ON THE GAMING COMPUTER 14 FOR RECORD KEEPING.
THE PROCESS REPEATS FOR EACH TICKET REGISTERED
TO FIG. 7C-5

FIG. 7C-5

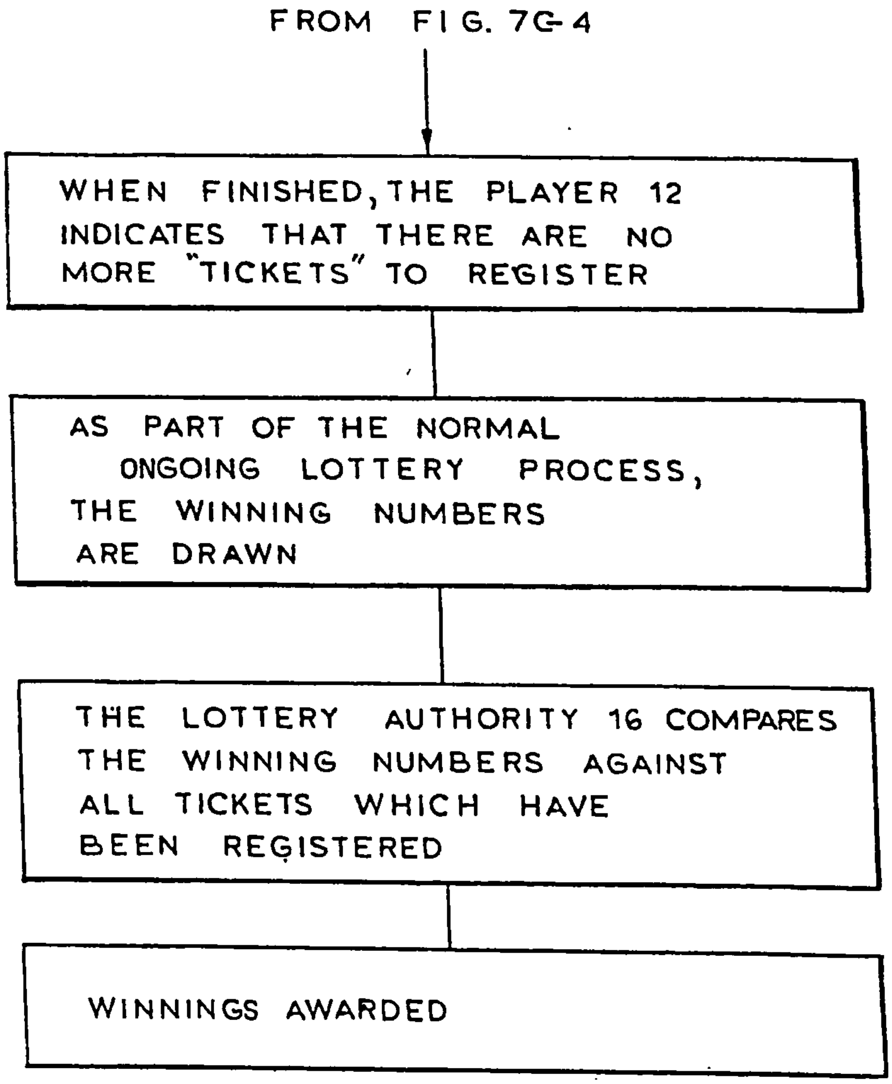
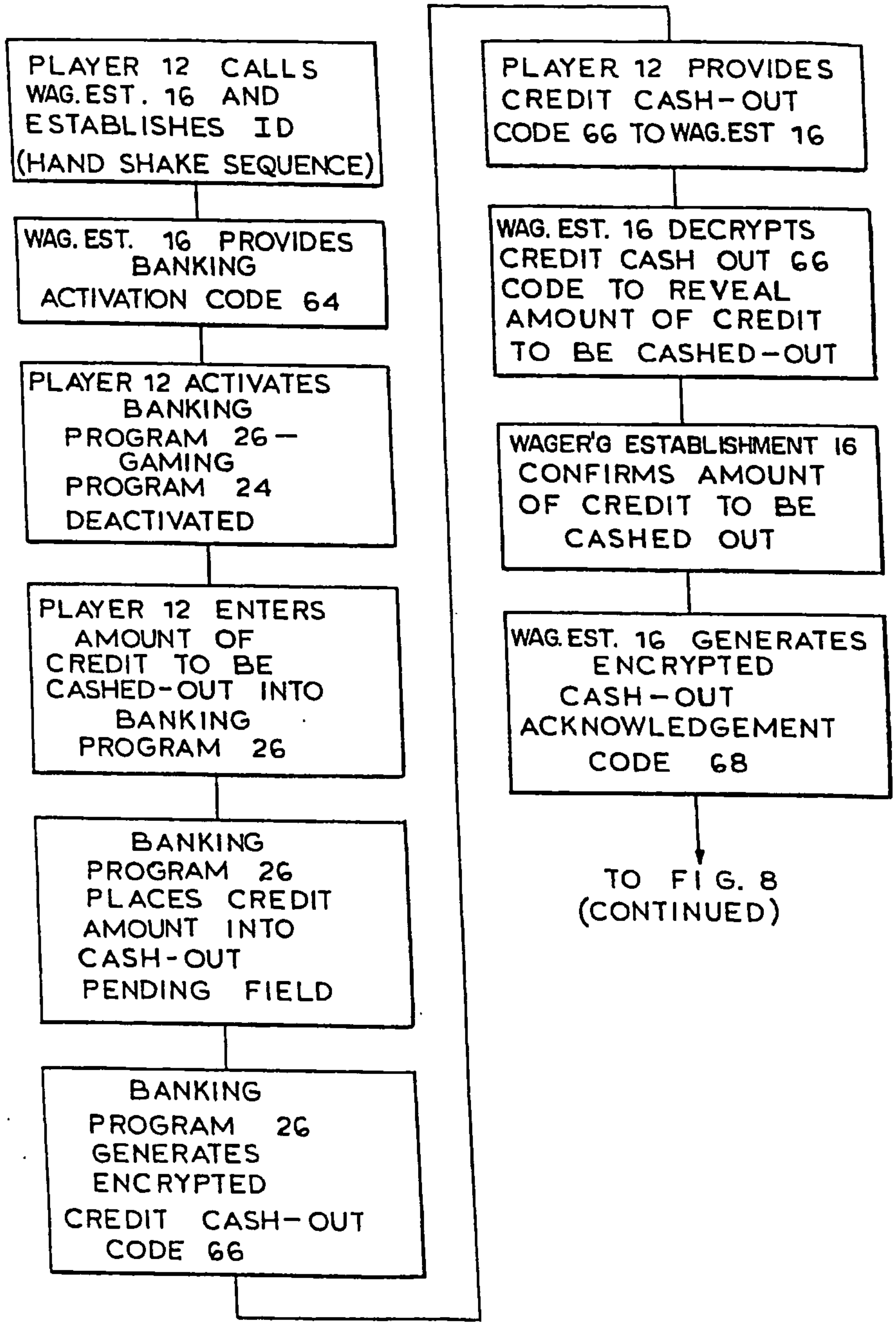

FROM FIG. 7C-4
WHEN FINISHED, THE PLAYER 12 INDICATES THAT THERE ARE NO MORE "TICKETS" TO REGISTER
AS PART OF THE NORMAL ONGOING LOTTERY PROCESS, THE WINNING NUMBERS ARE DRAWN
THE LOTTERY AUTHORITY 16 COMPARES THE WINNING NUMBERS AGAINST ALL TICKETS WHICH HAVE BEEN REGISTERED
WINNINGS AWARDED

FIG. 8


PLAYER 12 CALLS WAG. EST. 16 AND ESTABLISHES ID (HAND SHAKE SEQUENCE)
WAG. EST. 16 PROVIDES BANKING ACTIVATION CODE 64
PLAYER 12 ACTIVATES BANKING PROGRAM 26 – GAMING PROGRAM 24 DEACTIVATED
PLAYER 12 ENTERS AMOUNT OF CREDIT TO BE CASHED-OUT INTO BANKING PROGRAM 26
BANKING PROGRAM 26 PLACES CREDIT AMOUNT INTO CASH-OUT PENDING FIELD
BANKING PROGRAM 26 GENERATES ENCRYPTED CREDIT CASH-OUT CODE 66
PLAYER 12 PROVIDES CREDIT CASH-OUT CODE 66 TO WAG. EST 16
WAG. EST. 16 DECRYPTS CREDIT CASH OUT 66 CODE TO REVEAL AMOUNT OF CREDIT TO BE CASHED-OUT
WAGER'G ESTABLISHMENT 16 CONFIRMS AMOUNT OF CREDIT TO BE CASHED OUT
WAG. EST. 16 GENERATES ENCRYPTED CASH-OUT ACKNOWLEDGEMENT CODE 68
TO FIG. 8 (CONTINUED)

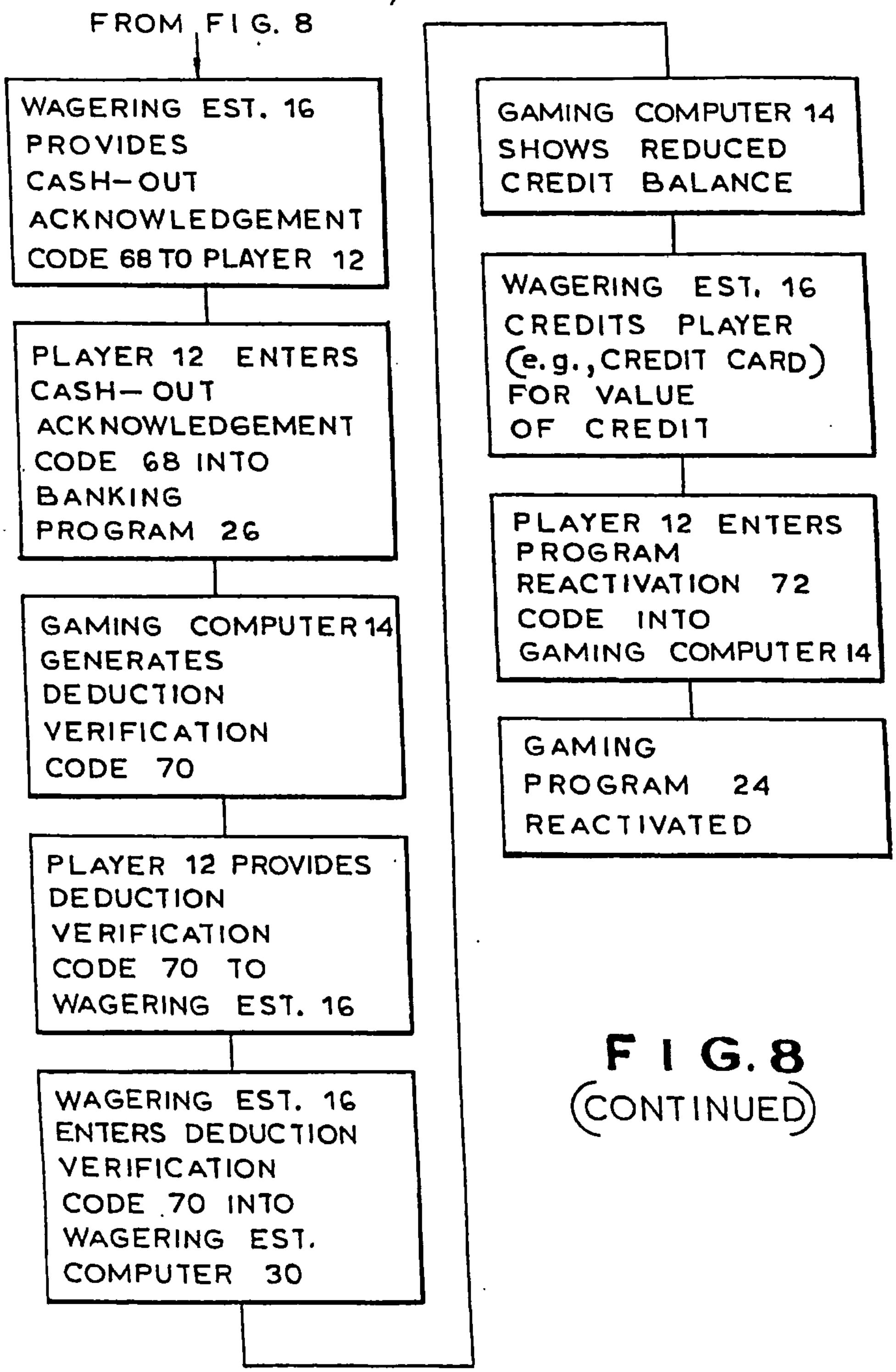
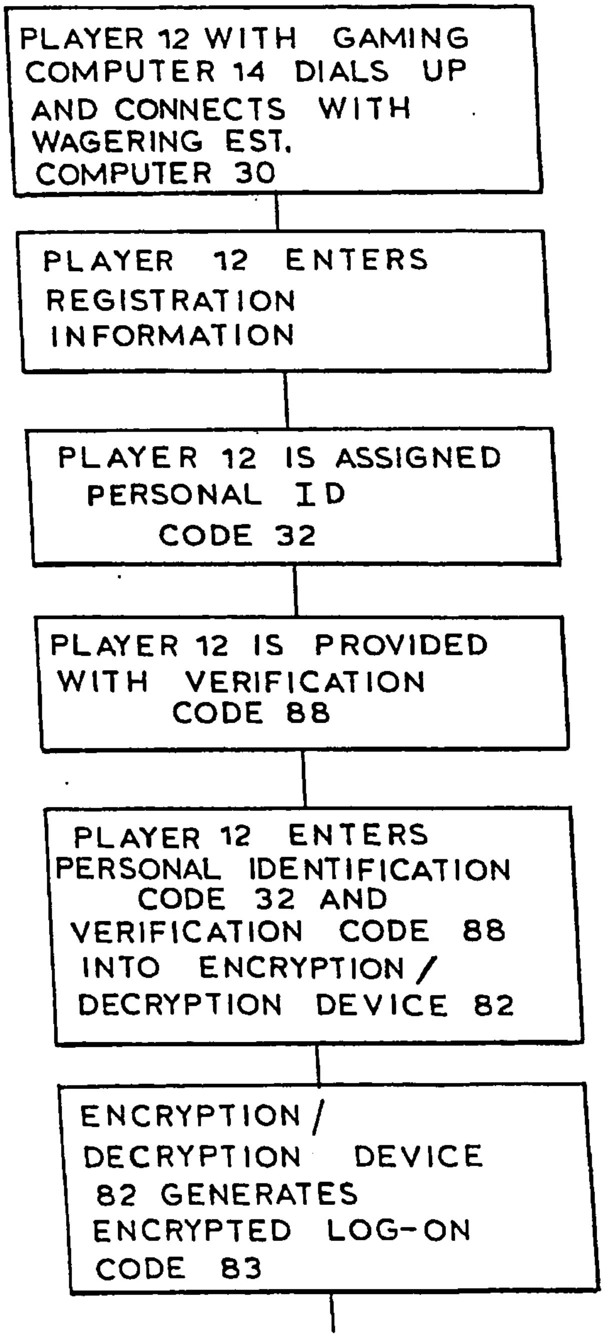

FROM FIG. 8
WAGERING EST. 16 PROVIDES CASH-OUT ACKNOWLEDGEMENT CODE 68 TO PLAYER 12
PLAYER 12 ENTERS CASH-OUT ACKNOWLEDGEMENT CODE 68 INTO BANKING PROGRAM 26
GAMING COMPUTER 14 GENERATES DEDUCTION VERIFICATION CODE 70
PLAYER 12 PROVIDES DEDUCTION VERIFICATION CODE 70 TO WAGERING EST. 16
WAGERING EST. 16 ENTERS DEDUCTION VERIFICATION CODE 70 INTO WAGERING EST. COMPUTER 30
GAMING COMPUTER 14 SHOWS REDUCED CREDIT BALANCE
WAGERING EST. 16 CREDITS PLAYER (e.g., CREDIT CARD) FOR VALUE OF CREDIT
PLAYER 12 ENTERS PROGRAM REACTIVATION 72 CODE INTO GAMING COMPUTER 14
GAMING PROGRAM 24 REACTIVATED

FIG. 8 (CONTINUED)

FIG. 9


PLAYER 12 WITH GAMING COMPUTER 14 DIALS UP AND CONNECTS WITH WAGERING EST. COMPUTER 30
PLAYER 12 ENTERS REGISTRATION INFORMATION
PLAYER 12 IS ASSIGNED PERSONAL ID CODE 32
PLAYER 12 IS PROVIDED WITH VERIFICATION CODE 88
PLAYER 12 ENTERS PERSONAL IDENTIFICATION CODE 32 AND VERIFICATION CODE 88 INTO ENCRYPTION / DECRYPTION DEVICE 82
ENCRYPTION / DECRYPTION DEVICE 82 GENERATES ENCRYPTED LOG-ON CODE 83

TO FIG. 9 (CONTINUED)

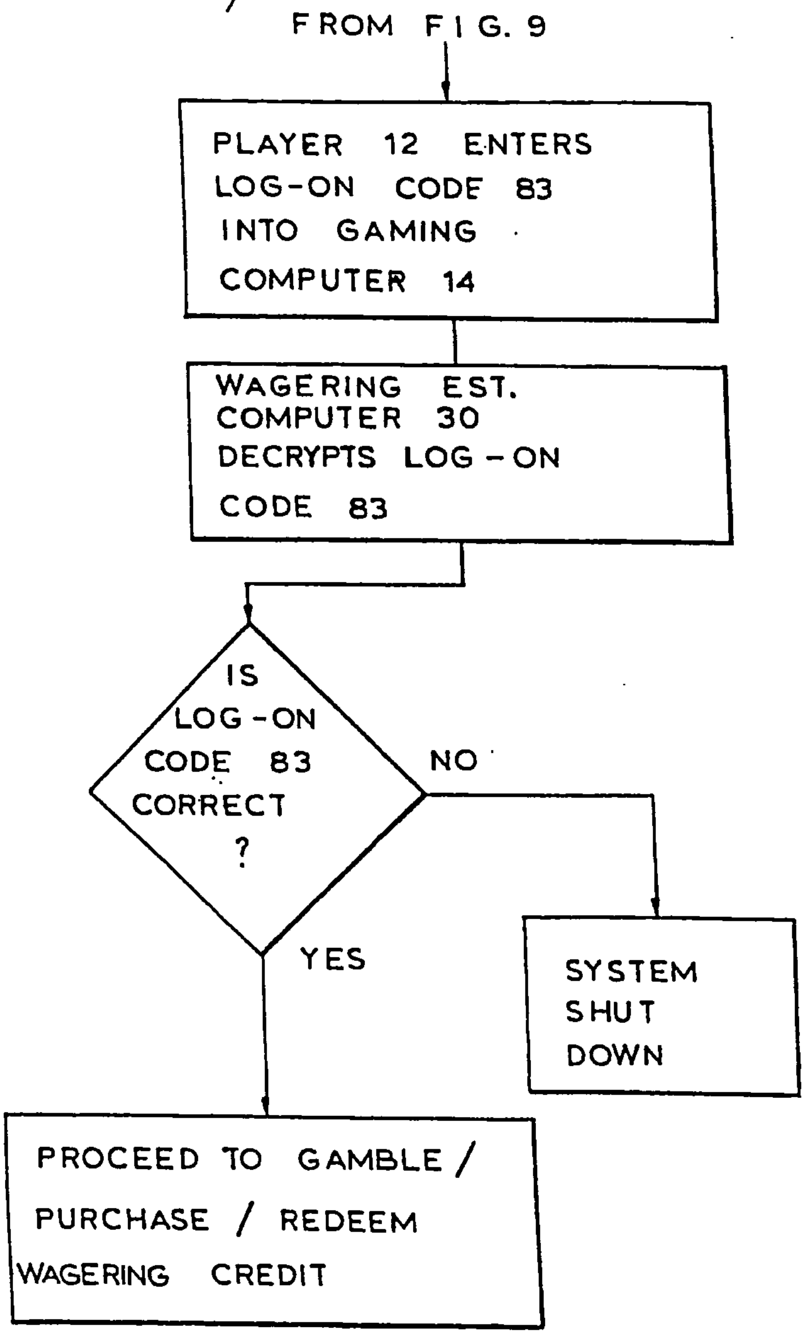

FROM FIG. 9
PLAYER 12 ENTERS LOG-ON CODE 83 INTO GAMING COMPUTER 14
WAGERING EST. COMPUTER 30 DECRYPTS LOG-ON CODE 83
IS LOG-ON CODE 83 CORRECT ?
NO
YES
SYSTEM SHUT DOWN
PROCEED TO GAMBLE / PURCHASE / REDEEM WAGERING CREDIT

FIG. 9 (CONTINUED)

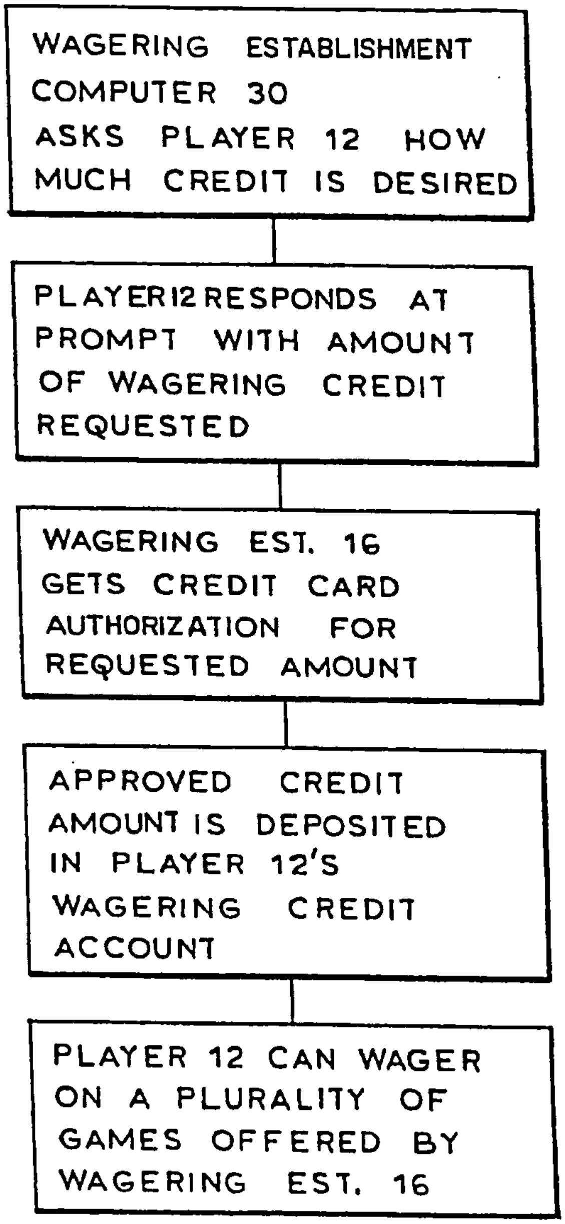

WAGERING ESTABLISHMENT COMPUTER 30 ASKS PLAYER 12 HOW MUCH CREDIT IS DESIRED
PLAYER 12 RESPONDS AT PROMPT WITH AMOUNT OF WAGERING CREDIT REQUESTED
WAGERING EST. 16 GETS CREDIT CARD AUTHORIZATION FOR REQUESTED AMOUNT
APPROVED CREDIT AMOUNT IS DEPOSITED IN PLAYER 12'S WAGERING CREDIT ACCOUNT
PLAYER 12 CAN WAGER ON A PLURALITY OF GAMES OFFERED BY WAGERING EST. 16

FIG.10

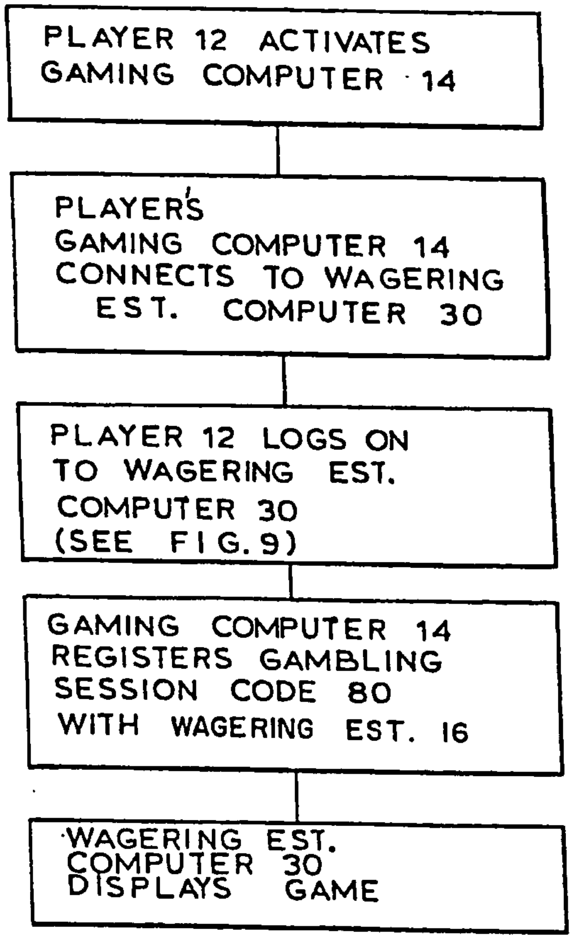

PLAYER 12 ACTIVATES GAMING COMPUTER 14
PLAYER'S GAMING COMPUTER 14 CONNECTS TO WAGERING EST. COMPUTER 30
PLAYER 12 LOGS ON TO WAGERING EST. COMPUTER 30 (SEE FIG. 9)
GAMING COMPUTER 14 REGISTERS GAMBLING SESSION CODE 80 WITH WAGERING EST. 16
WAGERING EST. COMPUTER 30 DISPLAYS GAME

FIG.11

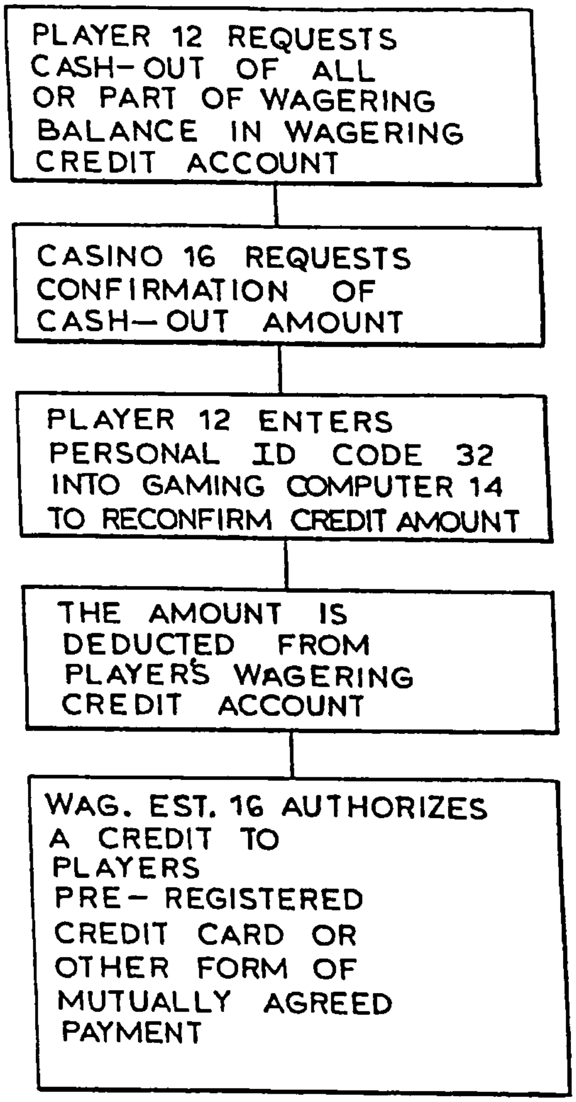

PLAYER 12 REQUESTS CASH-OUT OF ALL OR PART OF WAGERING BALANCE IN WAGERING CREDIT ACCOUNT
CASINO 16 REQUESTS CONFIRMATION OF CASH-OUT AMOUNT
PLAYER 12 ENTERS PERSONAL ID CODE 32 INTO GAMING COMPUTER 14 TO RECONFIRM CREDIT AMOUNT
THE AMOUNT IS DEDUCTED FROM PLAYER'S WAGERING CREDIT ACCOUNT
WAG. EST. 16 AUTHORIZES A CREDIT TO PLAYERS PRE- REGISTERED CREDIT CARD OR OTHER FORM OF MUTUALLY AGREED PAYMENT

FIG.12

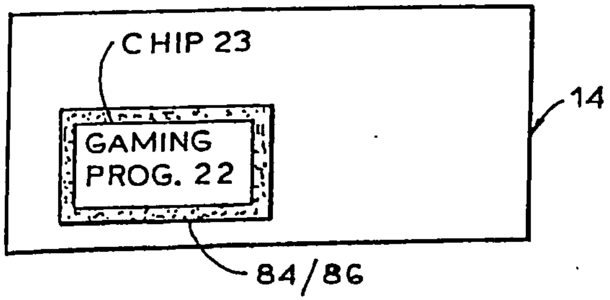

CHIP 23
GAMING
PROG. 22
14
84/86

FIG.13

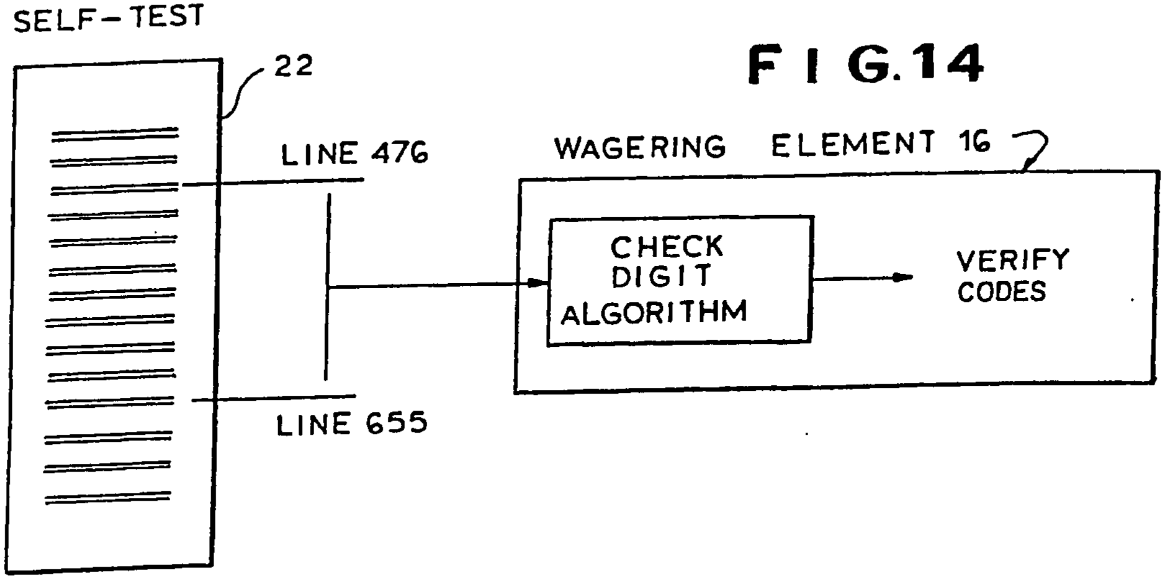
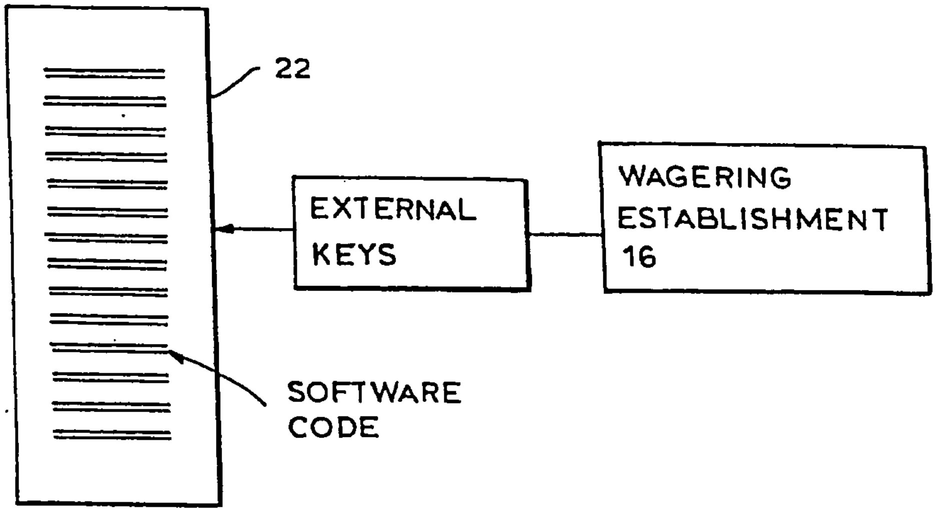

SELF-TEST
22
LINE 476
LINE 655
WAGERING ELEMENT 16
CHECK
DIGIT
ALGORITHM
VERIFY
CODES

FIG.14

F I G.15A



F I G.15B

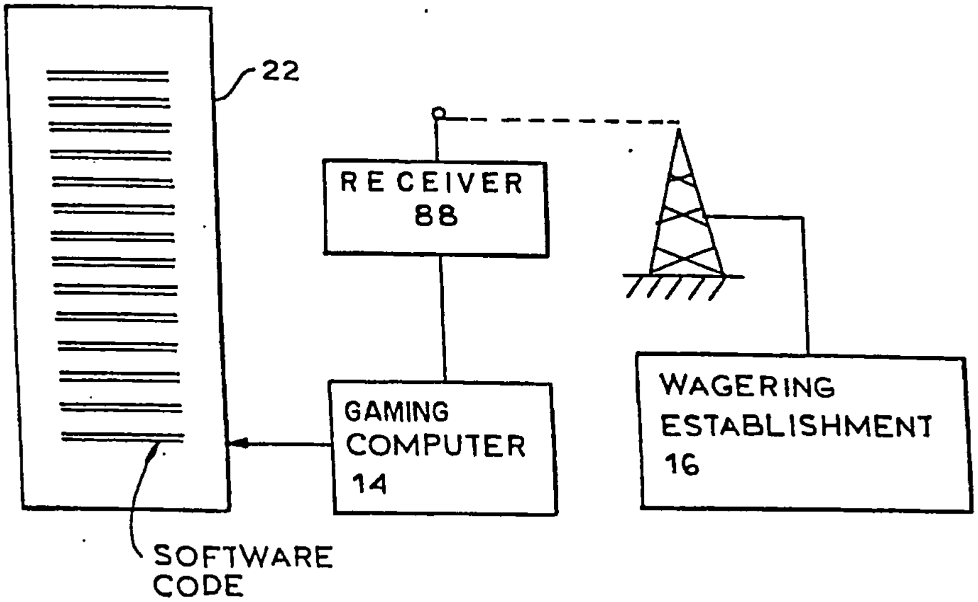


FIG.15C

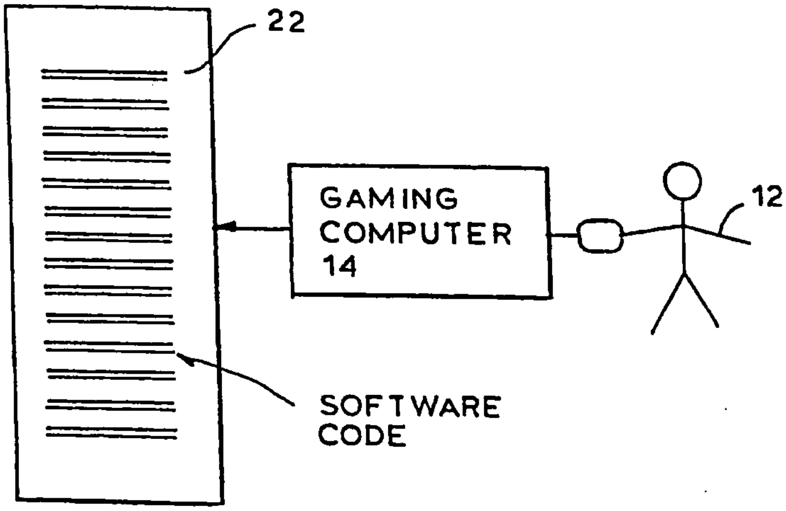
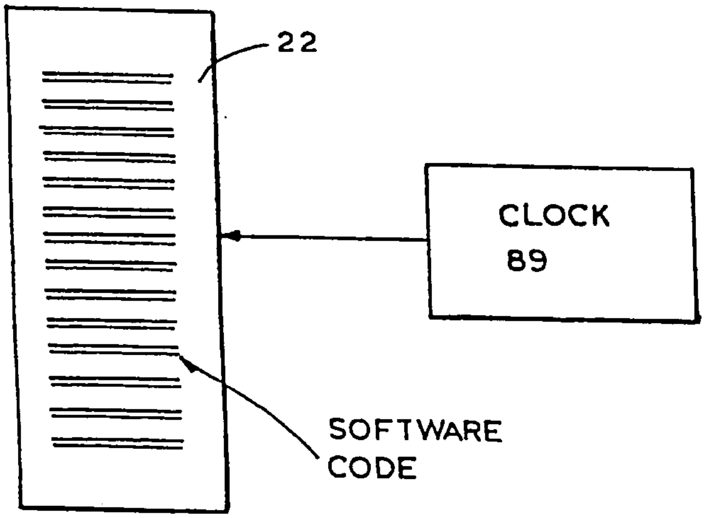


FIG.15D



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/02939

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 155:00, 161:00
US CL : 364/412; 273/138A
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/410-412; 273/138A, 138R, 433-435; 380/3, 4, 22-25; 235/375, 379, 380, 381; 382/2, 4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,038,022 (LUCERO) 06 August 1991, see the abstract, figs. 1-4, and col. 3 line 14 to col. 4 line 20.	1-30
Y	US, A, 4,317,957 (SENDROW) 02 March 1982, see the abstract and fig. 2.	1-30
Y	US, A, 5,083,271 (THACHER ET AL) 21 January 1992, see the abstract, fig. 1 and col. 2 lines 29-66.	10-11, 17-20
Y,P	US, A, 5,380,007 (TRAVIS ET AL) 10 January 1995, see the abstract and figs. 1-3.	31
Y	US, A, 5,096,195 (GIMMON) 17 March 1992, see the abstract and figs. 1-3.	1-30

☒ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 12 MAY 1995	Date of mailing of the international search report 08 JUN 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer B. Harder ROBERT A. WEINHARDT for Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/02939

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US, A, 5,351,970 (FIORETTI) 04 October 1994, see the abstract.	1-30
A,E	US,'A, 5,413,357 (SCHULZE ET AL) 09 May 1995, see the abstract.	1-30

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
A63F

A2

(11) International Publication Number: WO 99/01188

(43) International Publication Date: 14 January 1999 (14.01.99)

(21) International Application Number: PCT/US98/13909

(22) International Filing Date: 2 July 1998 (02.07.98)

(30) Priority Data:
08/888,049 3 July 1997 (03.07.97) US

(71) Applicant: WALKER ASSET MANAGEMENT LIMITED PARTNERSHIP [US/US]; 5 High Ridge Park, Stamford, CT 06905-1325 (US).

(72) Inventors: WALKER, Jay, S.; 124 Spectacle Lane, Ridgefield, CT 06877 (US). SCHNEIER, Bruce; 101 East Minnehaha Parkway, Minneapolis, MN 55419 (US). JORASCH, James, A.; Apartment 5G, 25 Forest Street, Stamford, CT 06901 (US). VAN LUCHENE, Andrew, S.; 13-2A Clarmore Drive, Norwalk, CT 06850 (US).

(74) Agent: ANDERSON, Jay, H.; Fitzpatrick, Cella, Harper & Scinto, 30 Rockefeller Plaza, New York, NY 10112-3801 (US).

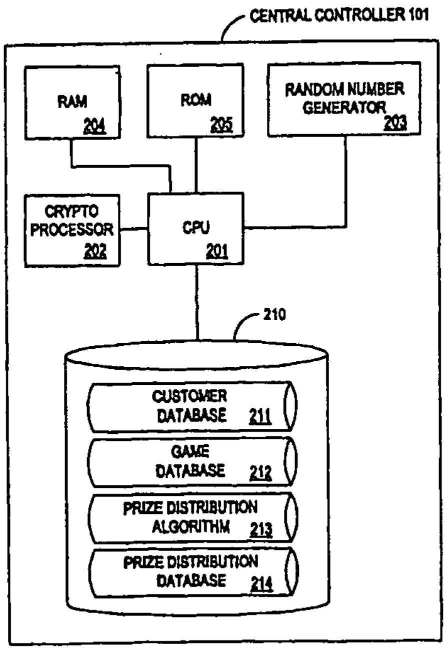
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR SECURING ON-LINE VIRTUAL PUNCHBOARD TRANSACTIONS

(57) Abstract

A system is described for facilitating an Internet-based game of chance, particularly a computer-based version of a punchboard game having a grid with prizes associated with the various grid locations. The user can pay a central controller for each selection by providing a credit card number, or through other Internet transaction means. The central controller sends the user a fresh virtual punchboard (i.e. a game in which no selections have yet been made). The user selects a grid location, encrypts it, and then transmits it to the central controller. The central controller then generates prize values for the grid that it sent to the player. The user's computer stores the locations of each prize and determines whether the player's selection was a winner. If he has won, the player sends the decryption key to the central controller to decrypt his grid selection and authenticate his selection. The central controller then initiates a payment to the user.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

TITLE

METHOD AND APPARATUS FOR SECURING ON-LINE VIRTUAL PUNCHBOARD TRANSACTIONS

BACKGROUND OF THE INVENTION

This invention relates to an electronic gambling game in which a player selects from a series of possible outcomes. The player and game provider may interact in a variety of ways, including over the Internet.

A number of well-known gambling games are based on a player selecting from a series of possible outcomes, where the winning outcome is randomly generated using some physical or mechanical device furnished by the game operator. Examples of such games are roulette, slot machines, and bingo. In the classical embodiments of these games, the player sees and/or hears the outcome generated (as in bingo and roulette), or even has a hand in generating the outcome himself (as in slot machines). The player's trust in the fairness of these games (that is, his belief that the outcome is random and that his selection, if a winner, will be honored) is largely based on his personal observation. Similarly, the game operator can use various methods to prevent cheating by a player if the player is personally present; for example, a bingo player claiming to be a winner is required to offer his card for inspection.

A well-known example of an entertainment/gambling device is the "punchboard." A punchboard consists of a board with a square grid of holes. Each hole contains a small rolled-up piece of paper. The player takes a pin and pushes through the board, pushing a selected piece of paper through the other side. This paper is then unrolled by the player to reveal whether or not he has won a prize. In a typical punchboard game, a player pays a small sum (approximately $1) to make a selection; prizes are determined by the size of the board and the fees, and may run hundreds of dollars.

Here, too, the player's confidence in the fairness of the game is largely based on his observation of the board; since he selects a piece of paper and can immediately read the message on it, he can be sure that the paper is not switched or tampered with after he selects it. In addition, by watching a number of plays he can eventually satisfy himself that there are indeed winning locations somewhere on the board. A successful electronic version of a punchboard game (a "virtual punchboard") must offer the player similar assurance that the game is not rigged, and must also prevent cheating the player.

Various forms of electronic games of chance have been available for many years. The way these games are played, however, is changing dramatically with the use of digital computers operating on electronic networks such as the Internet. Players can now connect to a remote server and wager electronically. Rather than traveling to the game (casino, bingo hall, etc.), a player can log into an electronic game and wager from the comfort of his own home. While this remote playing has many advantages, it raises several security issues. In a typical electronic gambling game, the player enters his selection and then learns whether he has won, without observing the winning selection being generated. For example, when playing card games at a casino, a player can observe the dealer shuffle and deal the cards and thus has some confidence that the outcome was generated randomly. In an electronic casino, the shuffling process is typically digitally generated, driven by random number generators which the player cannot see. The player cannot know whether the random number generated is truly random or was selected by the casino to give it an advantage.

Furthermore, a player desiring to play an electronic game remotely (for example, communicating with a game provider on the Internet) must send his selection and receive the winning selection over a communication network. In this instance, both the player and game provider require assurance that the communications are secure and that the game is conducted fairly.

Electronic game providers have tried to increase players' confidence in the legitimacy of games by assuring players that gaming software has not been tampered with. For example, an electronic game provider may allow an independent third party to perform an audit of the software. This is a time-consuming and expensive process, however. With complex software running into the hundreds of thousands of lines of code, it is very difficult to find a few lines of code that alter the randomness of the outcomes. Also, use of an independent, third party auditor shifts the need for trust to another party, and does not guarantee the legitimacy of the game.

Some electronic lottery systems have used methods for securing communications between remote player terminals and a central controller. For example, U.S. Patent No. 4,652,998 to Koza et al. ("Video Gaming System With Pool Prize Structures") describes cryptographic methods for securing these communications. In games dependent on the use of random numbers, however, simply securing against the transmission of a fraudulent random number does not solve the problem of assuring the player that the game is fairly conducted. Nor does it solve the problem of preventing multiple players from cooperating to gain an advantage over the game provider.

U.S. Patent No. 5,326,104 to Pease et al. ("Secure Automated Electronic Casino Gaming System") describes a system whereby a number of keno playing devices, all within the same playing area, are connected to a central controller. A player can play a device by inserting a player account card into it which is registered and confirmed by the central controller. Security in this system is directed primarily to ensuring that players will not tamper with the keno terminals, and that employees will not enter false tickets into the system. Apparently it is assumed that the central controller is trusted and will not try to cheat the players.

U.S. Patent No. 5,569,082 to Kayer ("Personal Computer Lottery Game") describes a game whereby a player can purchase a game piece containing an encrypted code which determines whether the piece is a winning one. The player logs onto a central site, via a PC or a kiosk, and types in the code. The site runs a game which reveals to the player if he is a winner in "an exciting fashion." If the player is a winner, he will be given instructions by the site as to where to pick up his prize. Although the system described in this patent provides encryption to protect the site from fraud, it offers no encryption to protect the player.

U.S. Patent No. 5,547,202 to Tsumura ("Computer Game Device") describes a system whereby a player can pay for the usage of games transmitted to his PC or to a kiosk via satellite from a central controller. The games are scrambled until payment is made. The central controller can store a game so that a player can take breaks from a game, return to it and continue play from the point in the game at which he left it. This system has neither a gambling element nor is it cryptographically enabled.

U.S. Patent No. 5,269,521 to Rossides ("Expected Value Payment Method and System For Reducing the Expected Per Unit Costs of Paying and/or Receiving a Given Amount of Commodity") describes a system where a customer exchanges encoded numbers with a product vendor. After being decoded, the two numbers are combined to determine a result. (See column 30, lines 1 to 5, as well as column 30, line 35, to column 31, line 55). The transactions described are not conducted in an online manner. Additionally, both parties must encode their numbers before exchanging them. No game results are ever exchanged in encoded form.

U.S. Patent No. 4,309,569 to Merkle ("Method of providing digital signatures") describes a system for digital signatures utilizing hash trees.

The proliferation of electronic network technology, along with the ease of user access to networks such as the Internet, has dramatically increased electronic communications and the exchange of information. Among a myriad of other uses, these networks facilitate the playing of games, including gambling activities. They are particularly well suited for such gaming because of their ability to collapse geographic distances while linking distributed players. As discussed above, however, the electronic implementation of games, and particularly gambling activities, often results in the loss of confidence and validity otherwise imbued in players from their personal observation of traditional gaming procedures (for example, dealing cards, spinning roulette wheels, etc.).

There thus exists a need in the art for systems and procedures which can both actually and in the perception of players improve the security and operation of electronic gambling and games. Such systems and procedures would not only foster the perception of on-line gaming as legitimate, but also increase player participation in such activities. This would further increase the commercial value of what is already a substantial online business.

SUMMARY OF THE INVENTION

In accordance with the present invention there is provided a new and improved method and apparatus for facilitating computer-based games of chance on electronic networks such as the Internet. A key feature of the invention comprises the use of encoding techniques, including various encryption schemes, to validate the operation of the games and prevent cheating by either the player or the game provider. Although encryption methods are described, it should be noted that any encoding scheme which prevents the recipient of a message from deciphering its contents will suffice.

In accordance with one embodiment of the invention, a method of generating and verifying the results of a computer-based game of chance is implemented by transmitting to a player computer a plurality of available game selections, each identified by a unique selection identifier. A player selection identifier is received from the player computer, and a winning selection identifier transmitted to the player computer. The player selection identifier and the winning selection identifier are compared to determine if the player has won the game. In accordance with the invention, verification is made that the winning selection identifier and the player selection identifier were independently generated.

Game operation is preferably managed by a central controller, with players communicating with the controller through player computers connected over an electronic network. In different embodiments of the invention, verification of authenticity is provided in the central controller, the player computer, some combination of both, or with the involvement of a third party.

Games supported include all games of chance which permit a user to select from amongst a plurality of potentially winning selections. Applicable games include, but are not limited to a punchboard having punch locations, a roulette wheel having wheel numbers, a bingo game having user-selected card numbers, and a slot machine having user-selectable outcomes.

Verification is provided through a variety of techniques, including the use of encryption such as key-based encryption, and hash-based encryption. The invention further contemplates the use of a third-party trusted agent to monitor and verify that the player and winning selections were independently generated.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram showing an overview of the system of the present invention.

Figure 2 is a block diagram of the central controller of Figure 1.

Figure 3 is a block diagram of the user computer of Figure 1.

Figure 4 is a block diagram of a trusted third party computer.

Figure 5 is a schematic representation of the punchboard game area before a game has been played.

Figure 6 is a schematic representation of the punchboard game area after a game has been played.

Figure 7A shows in tabular form the fields of the customer database of the central controller.

Figure 7B shows in tabular form the information in the prize distribution database of the central controller.

Figure 8 is a flowchart describing initiation of a game according to the preferred embodiments of the present invention.

Figure 9A shows in tabular form the information in the audit database of the user computer according to the first embodiment of the invention.

Figure 9B shows in tabular form the information in the game database of the central controller according to the first embodiment of the invention.

Figures 10A and 10B are connected flowcharts describing the flow of play between the central controller and user computer according to the first embodiment of the invention.

Figure 11A shows in tabular form the information in the audit database of the user computer according to the second embodiment of the invention.

Figure 11B shows in tabular form the information in the game database of the central controller according to the second embodiment of the invention.

Figures 12A and 12B are connected flowcharts describing the flow of play between the user computer and the central controller according to the second embodiment of the invention.

Figure 13A shows in tabular form the information in the audit database of the user computer according to the third embodiment of the invention.

Figure 13B shows in tabular form the information in the game database of the central controller according to the third embodiment of the invention.

Figures 14A, 14B and 14C are connected flowcharts describing the flow of play between the user computer and the central controller according to the third embodiment of the invention.

Figure 15A shows in tabular form the information in the audit database of the user computer according to the fourth embodiment of the invention.

Figure 15B shows in tabular form the information in the game database of the central controller according to the fourth embodiment of the invention.

Figure 16 is a flowchart describing the flow of play between the user computer and the central controller according to the fourth embodiment of the invention.

Figure 17A shows in tabular form the information in the audit database of the third party according to the fifth embodiment of the invention.

Figure 17B shows in tabular form the information in the game database of the central controller according to the fifth embodiment of the invention.

Figures 18A and 18B are connected flowcharts describing the flow of play between the user computer, the central controller, and the third party computer according to the fifth embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An overview of the system in the preferred embodiments of the present invention is shown in Figure 1. The central controller 101, operated by the game provider, communicates with the user computer 102 (operated by the game player) over the Internet 100. Figure 2 is a schematic diagram of the structure of the central controller 101. The central controller includes a CPU 201, connected to a cryptoprocessor 202, a random number generator 203, RAM 204, ROM 205 and a data storage device 210. The CPU 201 connects to the Internet for communication with the player's computer. The data storage device 210 includes a customer database 211, a game database 212, storage for the prize distribution algorithm 213 and a prize distribution database 214. To perform the various functions described in more detail below, the CPU 201 executes a program or programs stored in RAM 204 and/or ROM 205.

Cryptographic processor 202 supports the encoding and decoding of communications with players, as well as the authentication of players. An MC68HC16 microcontroller, commonly manufactured by Motorola Inc., may be used for cryptographic processor 202. This microcontroller utilizes a 16-bit multiply-and-accumulate instruction in the 16 MHZ configuration and requires less than one second to perform a 512-bit private key operation. Other exemplary commercially available specialized cryptographic processors include VLSI Technology's 33MHz 6868 or Semaphore Communications' 40 MHZ Roadrunner 284. Alternatively, cryptographic processor 202 may be configured as part of CPU 201.

A conventional random number generating processor may be used for random number generator 203. The HEMT integrated circuit manufactured by Fujitsu, for example, is capable of generating over one billion random numbers per second. Alternatively, random number generator 203 may be incorporated into CPU 201. Data storage device 210 may include hard disk, magnetic, or optical storage units, as well as CD-ROM drives or flash memory.

The user computer 102 is shown schematically in Figure 3. The user computer includes a CPU 301, connected to a cryptoprocessor 302, a random number generator 303, RAM 304, ROM 305 and a data storage device 310. The CPU 301 is also connected to an input device 320 and to the Internet, for communication with the user and the central controller respectively. In addition, the CPU 301 is connected to a display device 330 for displaying a virtual punchboard to the user. The data storage device 310 includes an audit database 311. The CPU 301, cryptoprocessor 302, random number generator 303 and data storage device 310 may have the same features as CPU 201, cryptoprocessor 202, random number generator 203 and data storage device 210 discussed just above.

Figure 4 is a schematic diagram of a trusted third party computer 400, which is used in an embodiment of the invention discussed in more detail below. This computer includes a CPU 401, RAM 404, ROM 405 and data storage device 410, similar to central controller 101 and user computer 102. The data storage device includes an audit database 411. The CPU 401 is connected for communication with the user computer 102 and the central controller 101.

Figure 5 shows the appearance of a virtual punchboard display 500, displayed to a user on the display device 330, before a game is played. The game is identified by a number 510, and an empty grid 511 is shown (in this case, a 12 x 12 square). A box 512 appears where the player may enter his selected grid locations. The player's current credits 513 (how much he has paid for the present game, plus his winnings so far) may also be displayed; in the example shown, the player has no winning balance and has just made an electronic payment of $1 to play game # 6465484564.

Figure 6 shows a results display 600, similarly displayed to the user by display device 330, after the game is played. The winning locations are displayed in a table 610 and on the grid 611, with the player's selection circled on the grid and displayed in a box 612. Also displayed is the result of the game (in this case the player is told, "YOU WIN!") and the balance 613 of the player's winnings. Finally, the display includes a box 620 labeled "PLAY AGAIN?" The CPU 301 may advantageously execute interactive display software (stored in RAM 304 or ROM 305) which enables "click boxes" and the like. In that case, the player would click on the "PLAY AGAIN?" box to order a new game.

Figure 7A shows the fields of the customer database 211 maintained by the central controller 101. Each customer is identified by name 701 and is assigned an ID number 702. Each customer entry in the database also includes a credit card number 703, the customer's e-mail address 704 and postal mailing address 705, the total amount the customer has spent 706, and the customer's total winnings to that point 707. The database stores the grid selection preferences 708 for each customer (so that a player who regularly plays the same location on the grid need not enter that location in every game), and the customer's preferred method 709 of receiving his winnings.

The fields of the prize distribution database 214, maintained by the central controller 101, are shown in Figure 7B. Each prize distribution is assigned an identification number 711. Each entry in the database includes the size 712 of the grid, the denomination of the game 713 (that is, the cost to the customer for one play) and the number and amount of prizes 714 to be awarded. Generally, a larger grid has more prizes associated therewith, and a grid with larger prizes has a larger associated denomination.

To create a new game, the central controller 101 employs a prize distribution algorithm 213 having the following steps: The central controller 101 retrieves the prize structure 714 and grid size 712 from the prize distribution database 214 by searching for the prize distribution ID number 711. The CPU 201 instructs the random number generator 203 to produce enough random numbers to cover the number of grid locations for the game. Each random number is appended to a grid location. The format might be (x,y,r), where "x" is the x-coordinate of the grid location, "y" is the y-coordinate of the grid location, and "r" is the assigned random number. The random numbers are then ranked numerically. Prizes are then appended to each grid location. The format might be (x,y,r,p), with "p" the prize value (which may be zero) assigned to the grid location (x,y). The game is then assigned an ID number. The winning grid locations for the game, and the prizes associated with those locations, are then stored in the game database 212, detailed embodiments of which are described below. Those skilled in the art will appreciate that there are many possible algorithms by which the prices may be randomly assigned. The above algorithm is merely illustrative

First Embodiment (User Computer Encryption)

In the first embodiment of the invention, the fields of the audit database 311 (stored in the user computer 102) are as shown in Figure 9A. Each record in the audit database 311 corresponds to one game played by the user, and is filled in as the game progresses (as described in detail below). A record includes an identification number 901 for the game, the grid location or locations 902 selected by the player, the winning grid locations 903, the game denomination 713, and a random key 904 which the player uses to encrypt his grid location selections.

In this embodiment, the fields of the game database 212 (stored in the central controller 101) are as shown in Figure 9B. Each record in the game database corresponds to one game (having an ID number 901) played by one player (having an ID number 702). Each record includes the winning grid locations 903, the player's selected and encrypted grid location 910, the corresponding decrypted grid location 920, and the player key 904.

A game conducted according to the first embodiment of the invention begins with the steps shown in the flowchart of Figure 8. Initially, the player (using his computer 102) logs on to the central controller 101 via the Internet 100 (step 801). If the player does not yet have an account (that is, an entry in the customer database 211), an account is opened at this time; the player provides the necessary information (step 804), and the central controller 101 assigns him an ID number and stores the new record in the customer database 211 (step 805). If the player already has an account, he enters his customer ID number 702 (step 810).

The player then selects the amount of money he wishes to play--that is, the denomination of the game; for example, $1, $3, or $5 (step 820). The user computer 102 updates the denomination field 713 in the audit database 311 (step 830). The central controller 101 debits the credit card account of the player for the amount of money played (step 840). The central controller 101 retrieves a new game grid from the prize distribution database 214 (step 850). Using the prize distribution algorithm 213 described above, the central controller 101 generates the winning grid locations 903, assigns the game identification number 901 and stores the game in the game database 212 (step 860).

In this embodiment, the game continues with the steps shown in the flowcharts of Figures 10A and 10B. In step 1001 of Figure 10A, a "blank" punchboard 500 including the game identification number 510 is made available to the player. The player selects a grid location 902 and enters it into the user computer 102 using input device 320 (step 1002). The cryptographic processor 302 of the user computer 102 generates a player key 904, preferably based on a random number generated by random number generator 303 (step 1003). The cryptographic processor 302 encrypts the grid location selection 902 with the player key (step 1004). The user computer 102 stores the game identification number, player key, and grid location selection in the audit database 311 (step 1005).

In step 1006, the encrypted grid location and game identification number are transmitted to the central controller 101. The central controller then retrieves the record in the game database 212 corresponding to the game identification number received from the user computer 102 (step 1007). The central controller 101 stores the encrypted grid location 910 in the game database 212 (step 1008).

At this point, the central controller 101 has the player's grid location selection, but only in an encrypted form. The central controller 101 then transmits the winning grid locations 903 to the user computer 102 (step 1010 of Figure 10B).

If the player has not won, he may proceed to select a new game (step 1061). If the player has won, the user computer 102 transmits the player key 904 and game identification number to the central controller 101 (step 1051). The central controller decrypts the encrypted grid location 910, and stores the decryption result 920 (the player's selected, winning grid location) and player key 904 in the game database 212 (step 1052).

The amount of money won by the player is retrieved from winning grid location field 903 of the game database 212 (step 1053). The central controller 101 then sends the game result message 600 to the user computer 102, indicating that the player has won (step 1054). The central controller then proceeds to generate the next game (step 1055).

At the end of the billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1056). If money is due the customer, the central controller 101 initiates a payment to the customer according to the customer's preferred payment method 709 (step 1057).

It should be noted that a key element of this embodiment is that the user sends his grid location selection in encrypted form (thus unreadable by the central controller 101) to the central controller before receiving the winning grid locations. The player is thereby assured that the game provider cannot change the winning locations based upon knowledge of his selection. On the other hand, the central controller holds the player's encrypted selection before the player is given the winning locations, and the player must provide the key to decrypt his selection before the central controller awards him a prize. The encryption of the player's selection thus assures both parties that the game has been fairly conducted, and that the two numbers were independently generated.

A transmission between the central controller and the player may include a digital signature to provide further assurance of the authenticity of the transmission, and to prevent repudiation by the sender. The uses and advantages of digital signatures are discussed generally in Schneier, "Applied Cryptography" (2d ed. 1996), chapter 2.

The above embodiment is also applicable to a game such as roulette. Instead of encoding his grid location selection, the player encrypts his number selection (representing any of the 38 wheel slots). The central controller then transmits the result of the wheel spin to the player.

The game of bingo could be simulated as follows. The player selects a board and then encrypts his selection before sending it to the central controller. The central controller then sends out each bingo number until one of the players claims a win. The winning player sends his key to the central controller so that his selection can be verified.

To simulate a slot machine, the player simply selects one of the possible reel combinations of the slot machine. In a slot machine with three reels and 20 stops per reel, there are 8,000 (20 X 20 X 20) possible outcomes, so the player could select one of these at random, encrypting the selection and sending it to the central controller. The central controller then distributes the prizes among the possible outcomes and sends the complete set of outcomes to the player so that he can determine whether or not he has won.

Second Embodiment (One-Way Hash)

In the second embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 11A. As in the first embodiment, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, winning grid locations 903 and the game denomination 713, similar to the record shown in Figure 9A. In this embodiment, the record also includes the hash value 1101 of the winning grid locations 903.

The structure of the game database 212 in this embodiment is shown in Figure 11B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the first embodiment. The entry also has the user-selected grid location 902 and the hash value 1101 of the winning grid locations 903.

A game conducted according to the second embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 12A and 12B. In step 1201 of Figure 12A, the cryptoprocessor 202 of the central controller 101 retrieves the winning grid locations 903 of the game from the game database 212, and uses a one-way hash function to hash the winning grid locations 903, thereby generating the hash value 1101. The hash value 1101 represents a one-way transformation of the winning grid locations 903.

An important feature of the one-way hash function is that it is computationally simple (given the hash function) to generate the hash value, but computationally unfeasible to recreate the winning grid locations from the hash value alone. The hash value 1101 thus serves as a unique identifier for the winning grid locations 903, without the winning grid locations themselves being revealed. Further details on one-way hash functions are given in Schneier, "Applied Cryptography" (2d ed. 1996), chapter 18.

The central controller 101 distributes the hash value 1101 to the user computer 102, along with a "blank" punchboard 500 with game identification number 510 (step 1202). The user computer 102 stores the hash value and game ID number in the audit database 311 (step 1203). In step 1204, the player selects a grid location and enters it into the user computer 102; the player may make additional grid location selections. Once the player has made all of his selections, the user computer 102 stores the game identification number 901, the selected grid locations 902 and the hash value 1101 in the audit database 311 (step 1211). The user computer 102 transmits the selected grid locations 902 to the central controller 101 along with the game ID number (step 1212). It should be noted that at this point the central controller 101 has the player's selections, but has already provided the player with a representation of the winning grid locations in the form of the hash value 1101. In step 1213, the central controller 101 determines whether the player has chosen a winning grid location by comparing the selected locations 902 with the winning grid locations 903 for that game.

Referring now to Figure 12B, the central controller 101 sends the winning grid locations 903 to the user computer 102 (step 1251). In step 1252, the user computer 102 verifies the fairness of the game. Specifically, the cryptographic processor 302 of the user computer 102 applies the one-way hash function to the received winning grid locations to verify that the hash value 1101 given to him before sending his selection is equal to the new hash value calculated by applying the one-way hash function to the winning grid locations.

If the player has not won, the central controller 101 proceeds to generate the next game (step 1270). If the player has won, the central controller 101 updates the total money awarded 707 in the customer database 211 to reflect the amount the player has just won (step 1260), and then generates the next game. In addition, at the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1280). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1281).

It should be noted that in this embodiment the punchboard cannot be reused; it must be replaced with a fresh punchboard after each player selection. If the punchboard were not replaced, the player could continue to select grid locations after receiving the winning grid locations 903 (see step 1251). The player could, however, make more than one selection during a game session (see step 1204), as long as each selection was received by the central controller 101 before the winning locations were transmitted to the player.

With minor modifications, this embodiment of the invention can accommodate any number of players. By delaying the transmission of the winning grid locations until after all grid location selections have been received, any number of players can be accommodated with one punchboard. Alternatively, games could be conducted at great speed, preventing players from cheating by sharing winning locations. For example, two players might make selections on the same punchboard nearly simultaneously. The first player sends his grid location selection and then receives the winning grid locations. A fraction of a second later the second player sends his grid location selection. If the first player can communicate with the second player he can inform the second player of the winning grid locations, ensuring a win for the second player. If the time difference between the two plays is small enough, however, the first player will not have enough time to communicate the winning locations.

Third Embodiment (Hash Tree)

The third embodiment of the invention uses hash trees to accommodate multiple players in a single punchboard game. Details of hash tree techniques are well known in the art and for reference purposes are discussed in Merkle (U.S. Patent No. 4,309,569).

In this embodiment, each grid location is represented by $(x,y,p,h_{xy'})$, where x and y are the coordinates, p is the prize associated with that location, h_{xy} is the hash value of that location, and $h_{xy'}$ is an aggregate hash value for all the other locations. Furthermore, a hash value, h, is calculated for the entire grid (including all locations) using hash function H. This function has the property $H(h) = H(h_{xy},h_{xy'})$ That is, the hash value for the entire grid is equal to the hash value of one location combined with the locations's $h_{xy'}$ value. For additional security, a random number may be attached to each grid location to provide greater variation in the resulting hash values.

In this embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 13A. As in the previous embodiments, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, winning grid locations 903 and the game denomination 713, similar to the records shown in Figures 9A and 11A. In this embodiment, the record also includes the hash value 1101 for all grid locations (both winning and losing), and an aggregate hash value 1301, representing the hash value of the aggregate of all the grid locations not selected by the player (i.e. the h_{xy}, values of all the grid locations selected by the player).

The structure of the game database 212 in this embodiment is shown in Figure 13B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the previous embodiments. The entry also has the user-selected grid location 902, the denomination 713 of the game, the hash value 1101 for all grid locations, and the aggregate hash value 1301.

A game conducted according to the third embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 14A, 14B and 14C.

In step 1401, the cryptoprocessor 202 of the central controller 101 retrieves the value of all grid locations of the game from the game database 212, and uses one-way hash function H stored in the memory (RAM

204 or ROM 205) of the central controller to hash these grid locations, thereby generating h, the hash value 1101 (i.e. the hash value of all grid locations). The central controller 101 then (step 1402) distributes the hash value 1101 to the user computer 102, along with a "blank" punchboard 500 including the game identification number 510. The user computer 102 stores the hash value 1101 in the audit database 311 (step 1403). The player selects a grid location 902 and enters it into the user computer 102, using the input device 320 (step 1404). The player may enter additional selections if he so desires. After the player has made all of the selections for that game, a new record is entered in the audit database 311 of the user computer 102, reflecting the ID number for the game and the player's selected grid locations (step 1410). The user computer 102 then transmits the player's grid selections 902 and game ID number to the central controller 101 along with the game ID number (step 1411).

The central controller then (step 1451) queries the game database 212 to obtain the winning grid locations 903, to determine whether or not the player's grid selections correspond to the winning grid locations. The central controller 101 sends a message to the user computer 102 relating whether the player has won (step 1452).

The integrity of the game is verified in steps 1453 through 1457. Using the hash tree algorithm, the cryptoprocessor 202 of the central controller 101 generates (step 1453) an aggregate hash value 1301; this value is the hash value of the aggregate of all the grid locations that the player did not pick (i.e. $h_{xy'}$). The aggregate hash value 1301 is stored in the game database 212 of the central controller (step

1454). In step 1455, the central controller 101 sends the aggregate hash value 1301 to the user computer 102, which updates the aggregate hash value field of the audit database 311.

Using hash tree techniques, the cryptoprocessor 302 of the user computer 102 takes both the information relating to the prize value corresponding to the player's selection (i.e. h_{xy}) and the aggregate hash value 1301 to calculate a hash value for the entire grid (step 1456). In step 1457, the user computer 102 uses hash tree techniques to compare this hash value for the entire grid to the hash value 1101 stored in the audit database 311. If the two values match, the integrity of the game is confirmed.

At this point, the player does not know the location of any winning locations on the grid, and therefore cannot help any other player to win. The winning grid locations are not revealed until all players have made all of their selections.

When all grid locations have been selected by all the players, the central controller 101 sends the winning grid locations to the user computer 102 (step 1458). The user computer stores the winning grid locations in the audit database 311 (step 1481). At the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1482). If money is due the customer, the central controller 101 initiates a payment to the customer according to the customer's preferred payment method 709 (step 1483).

Fourth Embodiment (Central Controller Encryption)

In the fourth embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 15A. As in the previous embodiments, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, and the game denomination 713. In this embodiment, the record also includes a random key 1510, and encrypted and decrypted versions (1520 and 1530 respectively) of the winning grid locations.

The structure of the game database 212 in this embodiment is shown in Figure 15B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the previous embodiments. The entry also has the user-selected grid location 902, the game denomination 713 and the random key 1510.

A game conducted according to the fourth embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowchart of Figure 16.

In step 1601, the central controller 101 retrieves the winning grid locations 903 for a game from the game database 212; the cryptoprocessor 202 encrypts these locations using the random key 1510. The central controller 101 then transmits the encrypted grid locations to the user computer 102 along with the "blank" electronic game board (step 1602). The player enters his grid location selections into the user computer 102, using the input device 320 (step 1603). The user computer 102 transmits the player's grid location selection to the central controller along with the game ID number (step 1604). In step 1605, the central controller stores the player's selections in the selected grid locations field 902 of the game database 212, and then transmits the key 1510 to the user computer 102. The central controller 101 then (step 1606) compares the user selected grid locations 902 with the winning grid locations 903.

If the player is not a winner, the central controller proceeds to generate the next game (step 1650). If the player is a winner, the central controller 101 updates the total money awarded 707 in the customer database 211 to reflect the amount the player has just won (step 1610). In addition, at the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1620). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1630).

It should be noted that a key element of this embodiment is that the central controller 101 sends the winning grid locations to the user computer 102 (though encrypted and thus unreadable by the user computer) before receiving the user's grid location selection. The player is thereby assured that the game provider cannot change the winning locations based upon knowledge of his selection. On the other hand, the central controller holds the player's selection before the player is provided with the key to decrypt the winning locations. The encryption of the winning locations thus assures both parties that the game has been fairly conducted.

This embodiment is particularly applicable to games such as blackjack, in which the central controller could randomly arrange an electronic deck of cards, encrypt them, and transmit them to the player. The player then sends card selections and play decisions to the central controller.

Fifth Embodiment (Trusted Third Party)

In the fifth embodiment of the invention, a trusted third party computer 400 is used to assure the integrity of the game. The audit database 311 in the user computer 102, the audit database 411 in the trusted third party computer 400 (both shown in Figure 17A) and the game database 212 in the central controller 212 (shown in Figure 17B) have the same structure. Each record in these databases corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, the winning grid locations 903, the game denomination 713 and the customer identification number 702.

A game conducted according to the fifth embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 18A and 18B. In step 1801, the central controller 101 transmits the game identification number 901 and the winning grid locations 903 to the trusted third party 400. The central controller 101 then sends a "blank" punchboard 500 to the user computer 102 (step 1802). The player selects a grid location 902 and enters it into the user computer 102, using the input device 320 (step 1803). The player may enter additional selections if he so desires. After the player has made all of the selections for that game, the user computer 102 transmits the player's grid selections 902 to the central controller 101 (step 1810). The central controller queries the winning grid location field 903 of the game database 212 to determine if the player's grid selection is a winner (step 1811). If the selection is a winner (step 1812), the controller notifies the player and updates the total money awarded field 707 of the customer database 211 accordingly.

The user computer 102 then transmits the game identification number to the trusted third party 400 (step 1813). The CPU 401 of the third party computer 400 queries the game identification number field 901 of the audit database 411 and retrieves the requested game identification number (step 1814). The third party computer 400 then sends the winning grid locations corresponding to the requested game identification number to the user computer 102 (step 1815).

In step 1851, the player uses the information from the trusted third party 400 to verify that the game provided by the central controller 101 was legitimate. In this embodiment, the use of the trusted third party makes encryption of player selected grid locations and winning grid locations unnecessary.

At the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1852). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1853).

Many variations of the embodiments discussed above are possible. For example, the central controller can track the amount of play engaged in by individual users for marketing purposes. In particular, special advertisements could be transmitted over the Internet targeted to high volume players. The central controller may offer demonstration games for new users so that they learn how to play. The game may be configured as a "pulltab" game, rather than punchboard. A user may be offered discounts on subsequent game, to provide him with an incentive to play again.

Although the above embodiments have been described with reference to a remote player making payments by credit card, a number of payment methods are possible. For example, the player may maintain an account with the game provider, or make payments with digital cash. Furthermore, rather than interact remotely with the central controller, the player may make his payment to a live cashier, who then enters the amount of credit into the central controller using an input device.

In addition, although the above embodiments have been described with reference to communication over the Internet, it will be appreciated that the practice of our invention is not limited to Internet communications, but is applicable to a variety of possible modes of communication between the game provider and the player. Commercial online services such as CompuServe and America Online could implement the systems and methods of the present invention.

Each of the above-described embodiments of the virtual punchboard is generally applicable to a game in which a player predicts a random outcome. One skilled in the art will appreciate how the various aspects of the virtual punchboard may be implemented in other games of chance (roulette, bingo, slot machines, blackjack, craps, lottery, etc.).

While the present invention has been described above in terms of specific embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. On the contrary, the present invention is intended to cover various modifications and equivalent structures included within the spirit and scope of the appended claims.

We claim:

1. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein player selection identifier is encrypted, said computing device transmits the winning selection identifier in an unencrypted format after receiving the encrypted player selection identifier, said computing device receives the decryption key after transmitting the winning selection identifier, said computing device decrypts the encrypted player selection identifier using the cryptoprocessor and decryption key, and afterwards performs said comparing by comparing the decrypted player selection identifier with the winning selection identifier.

2. A system according to claim 1, wherein said game of chance comprises an electronically implemented punchboard.

3. A system according to claim 1, wherein said game of chance comprises an electronically implemented roulette wheel.

4. A system according to claim 1, wherein said game of chance comprises an electronically implemented bingo game.

5. A system according to claim 1, wherein said game of chance comprises an electronically implemented slot machine.

6. A system according to claim 1, wherein said game of chance comprises an electronically implemented lottery.

7. A system according to claim 1, wherein said transmitting and receiving are performed on the Internet.

8. A system according to claim 1, wherein the memory device includes a game database containing the winning selection identifier and a prize amount associated therewith.

9. A system according to claim 1, wherein said computing device further comprises a random number generator for generating a random number for use in selecting the winning selection from the plurality of available selections.

10. A system according to claim 1, wherein the memory device includes a customer database containing a customer identifier and information regarding a credit account of a customer, and the program is further adapted to initiate a charge against the credit account in accordance with the player selection and to initiate a payment to the credit account of the prize amount in accordance with the result of said game.

11. A system according to claim 1, wherein said encryption key and said decryption key are identical.

12. A system according to claim 1, wherein the encryption key is based on a random number.

13. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor generates a first value based on the winning selection identifier, and said computing device transmits the first value with the plurality of available game selections for comparison with a second value based on the transmitted winning selection identifier, the winning selection identifier transmitted after receipt of the player selection identifier, where said comparison is used to verify that the winning selection identifier and the player selection identifier were independently generated.

14. A system according to claim 13, wherein the first value and the second value are one-way hash values.

15. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor generates a first value based on the winning selection identifier, said computing device transmits the first value with the plurality of available game selections, the cryptoprocessor generates a second value based on the available game selections other than the player selection after said computing device receives the player selection identifier, and said computing device before transmitting the winning selection identifier transmits the second value, where comparison of a third value based on the player selection and the second value with the first value verifies that the winning selection identifier and the player selection identifier were independently generated.

16. A system according to claim 15, wherein the first value, the second value and the third value are one-way hash values, and the third value is generated using a hash tree algorithm.

17. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor encrypts the winning selection identifier using a selected encryption key, said computing device transmits the encrypted winning selection identifier before receiving the player selection identifier, and said computing device transmits the selected encryption key after receiving the player selection.

18. A system according to claim 17, wherein said computing device transmits a digital signed encrypted winning selection identifier.

19. A system according to claim 17, wherein the encryption key is based on a random number.

20. A system for facilitating a computer-based game of chance, comprising:

a first computing device including a first processor and a first memory device connected to the first processor; and

a second computing device, including a second processor and a second memory device connected to the second processor,

the first memory device containing a first program, adapted to be executed by the first processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier,and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

and

the second memory device containing a second program, adapted to be executed by the second processor, for receiving the winning selection identifier from said first computing device and transmitting the winning selection identifier after said first computing device receives the player selection identified by the player selection identifier.

21. A system for facilitating a computer-based game of chance, comprising:

a first computing device including a first processor, a first cryptoprocessor connected to the first processor and a first memory device connected to the first processor, the first memory device containing a first program, adapted to be executed by the first processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier,and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance; and

a second computing device, including a second processor, a second cryptoprocessor connected to the second processor and a second memory device connected to the second processor, the second memory device containing a second program, adapted to be executed by the second processor, for receiving the plurality of available game selections from said first computing device, transmitting to the first computing device the player selection identified by the player selection identifier, and receiving the winning selection identifier from the first computing device.

22. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

transmitting to said player computer a winning selection identifier;

comparing said player selection identifier with said winning selection identifier to determine if said player has won said game of chance; and

verifying that said winning selection identifier and said player selection identifier were independently generated.

23. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

a first transmitting step of transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

a first receiving step of receiving from said player computer an encrypted player selection using a selected encryption key to generate an encrypted player selection identifier;

transmitting, after said first receiving step, to said player computer a winning selection identifier in an unencrypted format;

comparing said player selection identifier with said winning selection identifier to determine if said player has won said game of chance;

a second receiving step of receiving from said player computer said selected encryption method;

decrypting said encrypted selected selection identifier using said selected encryption key; and

comparing the decrypted player selection identifier with said winning selection identifier to verify that said player has won said game of chance.

24. A method according to claim 22; wherein said game of chance comprises an electronically implemented punchboard.

25. A method according to claim 22, wherein said game of chance comprises an electronically implemented roulette wheel.

26. A method according to claim 22, wherein said game of chance comprises an electronically implemented bingo game.

27. A method according to claim 22, wherein said game of chance comprises an electronically implemented slot machine.

28. A method according to claim 22, wherein said game of chance comprises an electronically implemented lottery.

29. A method according to claim 22, wherein said transmitting and receiving are performed on an electronic network.

30. A method according to claim 29, wherein said electronic network includes a commercial online service provider

31. A method according to claim 22, wherein the selected encryption key is based on a random number.

32. A method for generating and verifying results of a computer-based game of chance, the method comprising the steps of:

generating a winning selection identifier and a first value based thereon;

transmitting to a player computer the first value and a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

transmitting the winning selection identifier to said player computer after receiving said player selection identifier;

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance; and

said first value for comparison with a second value based on said transmitted winning selection identifier to verify that the winning selection identifier and the player selection identifier were independently generated.

33. A method according to claim 32, wherein the first value and the second value are one-way hash values.

34. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

generating a winning selection identifier and a first value based thereon;

transmitting to a player computer the first value and a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

generating, after said receiving step, a second value based on the available game selections other than the player selection;

transmitting the second value to said player computer;

transmitting a winning selection identifier, after said step of transmitting the second value;

generating a third value based on the player selection and the second value;

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance; and

comparing the third value with the first value to verify that the winning selection identifier and the player selection identifier were independently generated.

35. A method according to claim 34, wherein the first value, the second value and the third value are one-way hash values, and the third value is generated using a hash tree algorithm.

36. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

encrypting a winning selection identifier using a selected encryption key;

transmitting the encrypted winning selection identifier to said player computer;

receiving, after said step of transmitting the encrypted winning selection identifier, a player selection identified by a player selection identifier;

transmitting, after said step of receiving the player selection, the selected encryption key to said player computer; and

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance.

37. A method according to claim 36, wherein said step of transmitting the encrypted selection identifier includes digitally signing said encrypted selection identifier.

38. A method according to claim 36, wherein the encryption key is based on a random number.

39. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

transmitting to a third-party computer a winning selection identifier;

receiving, after said step of transmitting the winning selection identifier, from said player computer a player selection identified by a player selection identifier;

transmitting, after said receiving step, the winning selection identifier to said player computer; and

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance.

40. A device for facilitating a game of chance, comprising:

a first computing device including a first processor, a first cryptoprocessor connected to the first processor and a first memory device connected to the first processor and containing a first program and a database containing information regarding a player of said game and a distribution of prizes for said game; and

a second computing device including a second processor, a second cryptoprocessor connected to the second processor, a second memory device connected to the second processor and containing a second program and a database containing information regarding game selections made by the player during said game, an input device connected to the second processor for inputting the game selections, and a display device connected to the second processor for displaying a result of said game,

the first program being adapted to be executed by the first processor for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine the result of said game, and

the second program being adapted to be executed by the second processor for receiving the plurality of available game selections from said first computing device, transmitting to the first computing device the player selection identified by the player selection identifier, and receiving the winning selection identifier from the first computing device.

41. A device according to claim 40, wherein said first computing device and said second computing device each further comprise means for communicating on the Internet.

42. A device according to claim 40, wherein said first computing device further comprises a first random number generator for generating a random number used by the first cryptoprocessor, and said second computing device further comprises a second random number generator for generating a random number used by the second cryptoprocessor.

43. A computer readable medium in which is stored computer readable code to be executed by a computer, said computer readable code performing a method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

transmitting to said player computer a winning selection identifier;

comparing said player selection identifier with said winning selection identifier to determine if said player has won said game of chance; and

verifying that said winning selection identifier and said player selection identifier were independently generated.

44. A computer readable medium according to claim 43, wherein communication between said computer and said player computer is performed on the Internet.

45. A method of participating in a computer-based game of chance, comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier;

transmitting a player selection identified by a player selection identifier;

receiving a winning selection identifier identifying a winning selection; and

verifying that the winning selection identifier and the player selection identifier were independently generated.

46. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier input from the input device, encrypting the player selection identifier using the cryptoprocessor according to an encryption key, transmitting the encrypted player selection identifier, receiving a winning selection identifier, transmitting the encryption key, comparing the player selection identifier with the winning selection identifier and displaying on the display device a result of said game of chance,

wherein said computing device receives the winning selection identifier in an unencrypted format after transmitting the encrypted player selection identifier, transmits the encryption key after receiving the winning selection identifier, and performs said comparing to verify the result of said game of chance.

47. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier, storing the first value in the memory device, receiving a player selection identified by a player selection identifier input from the input device, transmitting the player selection identifier, receiving the winning selection identifier, generating a second value using the cryptoprocessor based on the received winning selection identifier, comparing said first value with said second value and displaying on the display device a result of said game of chance,

wherein the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier, and said computing device compares said first value with said second value to verify that the winning selection identifier and the player selection identifier were independently generated.

48. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier, storing the first value in the memory device, receiving a player selection identified by a player selection identifier input from the input device, transmitting the player selection identifier, receiving a second value based on the available game selections other than the player selection, generating a third value based on the player selection and the second value using the cryptoprocessor, comparing the third value with the first value, receiving the winning selection identifier, and displaying on the display device a result of said game of chance,

wherein the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier, said computing device receives the second value before receiving the winning selection identifier, and said computing device compares the third value with the first value to verify that the winning selection identifier and the player selection identifier were independently generated.

49. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier input from the input device, receiving a winning selection identifier in an encrypted format, transmitting the player selection identifier, receiving an encryption key, decrypting the encrypted winning selection identifier using the cryptoprocessor and the encryption key, and displaying on the display device a result of said game of chance,

wherein said computing device receives the encrypted winning selection identifier before transmitting the player selection identifier and receives the encryption key after transmitting the player selection identifier, and the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier.

50. A system for facilitating a computer-based game of chance, comprising:

a first computing device including a first processor, an input device connected to the first processor, a display device connected to the first processor and a first memory device connected to the first processor; and

a second computing device, including a second processor and a second memory device connected to the second processor,

the first memory device containing a first program, adapted to be executed by the first processor, for receiving a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier input from the input device, transmitting the player selection identifier, receiving a winning selection identifier from said second computing device, and displaying on the display device a result of said game of chance, and

the second memory device containing a second program, adapted to be executed by the second processor, for transmitting the winning selection identifier to said first computing device after said first computing device transmits the player selection identifier,

wherein the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier.

51. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier;

inputting a player selection identified by a player selection identifier;

encrypting the player selection identifier using an encryption key;

transmitting the encrypted player selection identifier;

receiving a winning selection identifier;

comparing the player selection identifier with the winning selection identifier to determine if said player has won said game of chance; and

transmitting the encryption key,

wherein the winning selection identifier is received in an unencrypted format after the encrypted player selection identifier is transmitted, the encryption key is transmitted after the winning selection identifier is received, and a comparison of the player selection identifier with the winning selection identifier verifies that said player has won said game of chance.

52. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier;

inputting a player selection identified by a player selection identifier;

transmitting the player selection identifier;

receiving the winning selection identifier;

generating a second value based on the received winning selection identifier; and

comparing said first value with said second value to verify that the winning selection identifier and the player selection identifier were independently generated.

53. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier;

inputting a player selection identified by a player selection identifier;

transmitting the player selection identifier;

receiving a second value based on the available game selections other than the player selection;

generating a third value based on the player selection and the second value;

comparing the third value with the first value; and

receiving the winning selection identifier;

wherein the second value is received before the winning selection identifier is received, and said step of comparing the third value with the first value verifies that the winning selection identifier and the player selection identifier were independently generated.

54. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier;

inputting a player selection identified by a player selection identifier;

receiving a winning selection identifier in an encrypted format;

transmitting the player selection identifier;

receiving an encryption key; and

decrypting the encrypted winning selection identifier in accordance with the encryption key,

wherein the encrypted winning selection identifier is received before the player selection identifier is transmitted, the encryption key is received after the player selection identifier is transmitted, and a comparison of the player selection identifier with the winning selection identifier decrypted according to the encryption key verifies that said player has won said game of chance.

55. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving from a game server computer a plurality of available game selections each identified by a unique selection identifier;

inputting a player selection identified by a player selection identifier;

transmitting the player selection identifier to the game server computer; and

receiving from a third-party computer a winning selection identifier,

wherein the winning selection identifier is received from the third-party computer after said step of transmitting the player selection identifier.

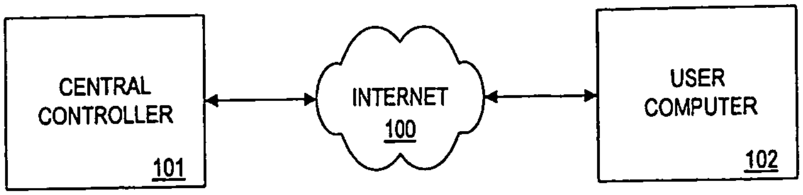

CENTRAL CONTROLLER
101
INTERNET
100
USER COMPUTER
102

FIG. 1

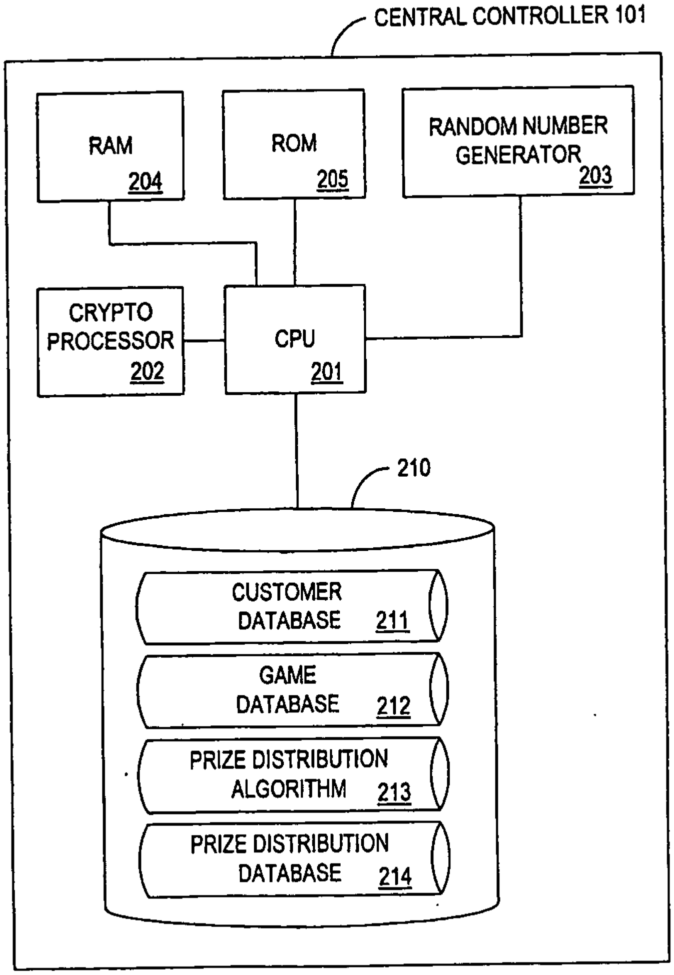

CENTRAL CONTROLLER 101
RAM
204
ROM
205
RANDOM NUMBER GENERATOR
203
CRYPTO PROCESSOR
202
CPU
201
210
CUSTOMER DATABASE
211
GAME DATABASE
212
PRIZE DISTRIBUTION ALGORITHM
213
PRIZE DISTRIBUTION DATABASE
214

FIG. 2

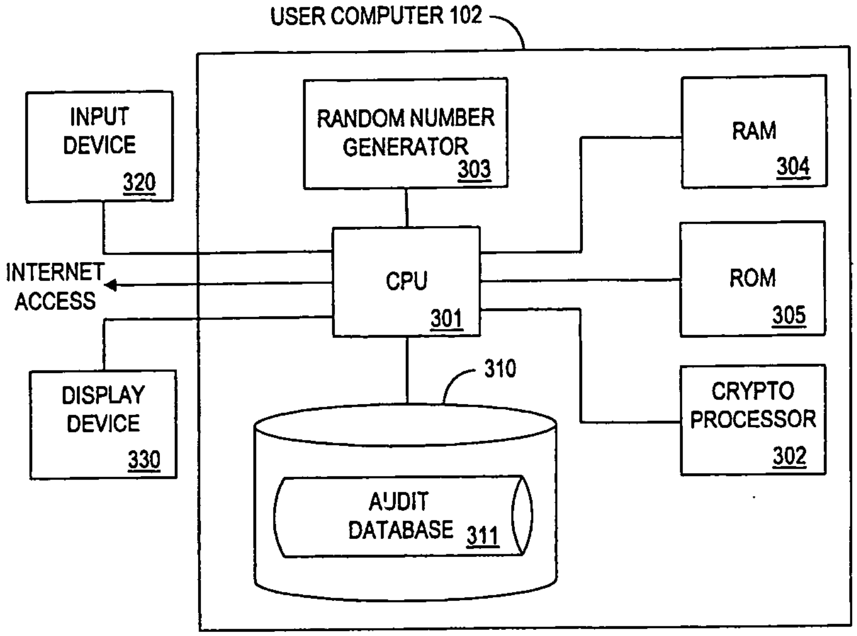

USER COMPUTER 102
INPUT DEVICE 320
RANDOM NUMBER GENERATOR 303
RAM 304
INTERNET ACCESS
CPU 301
ROM 305
310
DISPLAY DEVICE 330
CRYPTO PROCESSOR 302
AUDIT DATABASE 311

FIG. 3

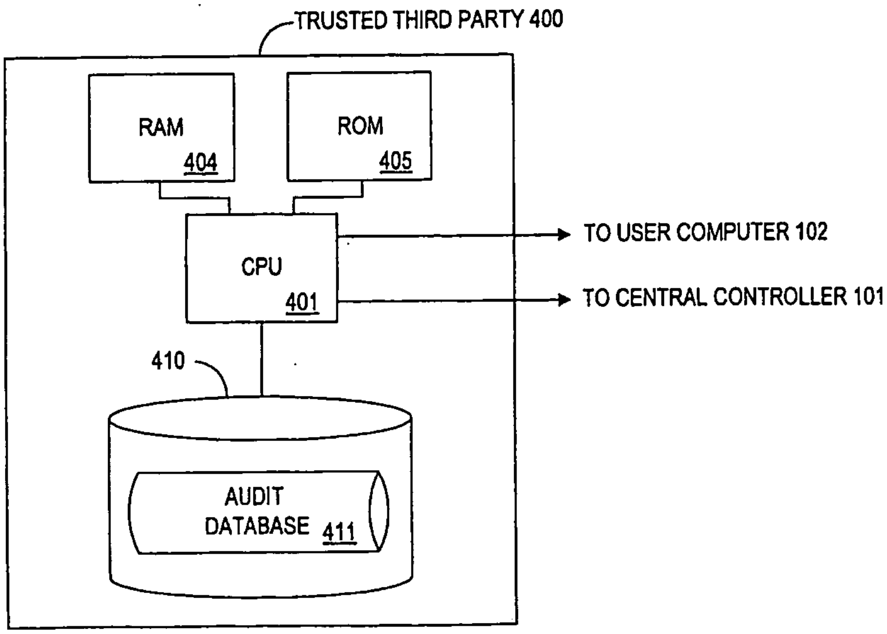

TRUSTED THIRD PARTY 400
RAM 404
ROM 405
CPU 401
TO USER COMPUTER 102
TO CENTRAL CONTROLLER 101
410
AUDIT DATABASE 411

FIG. 4

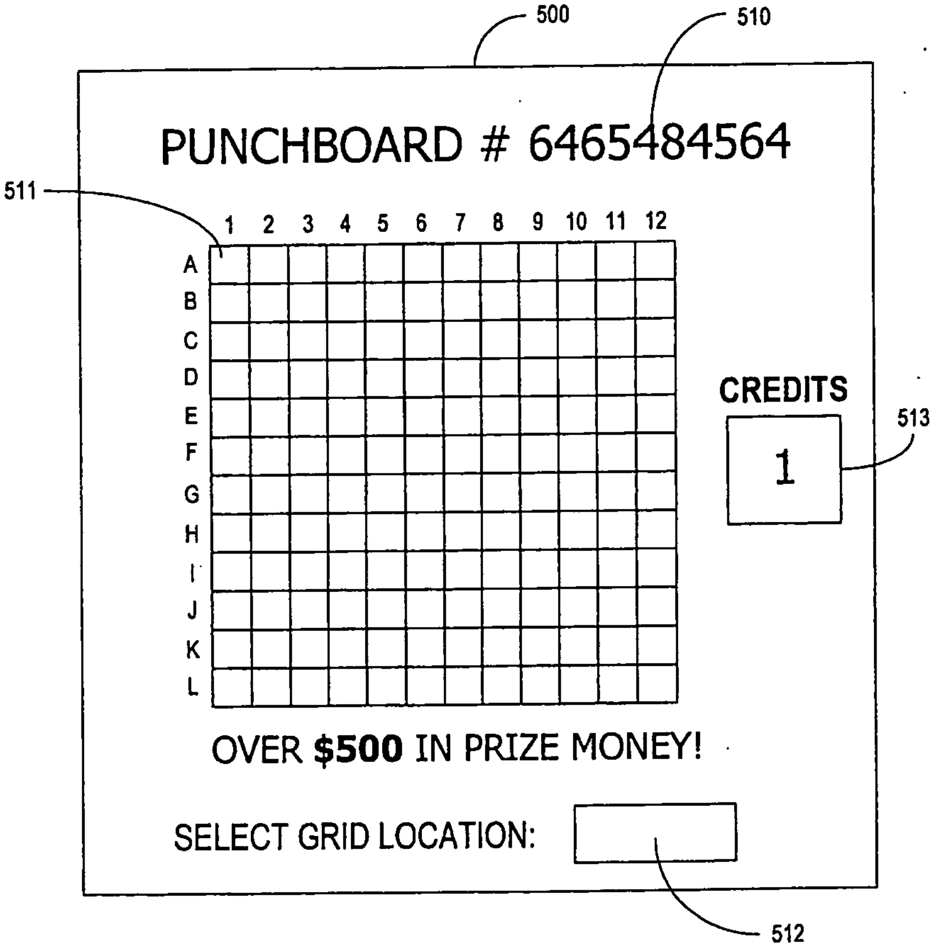
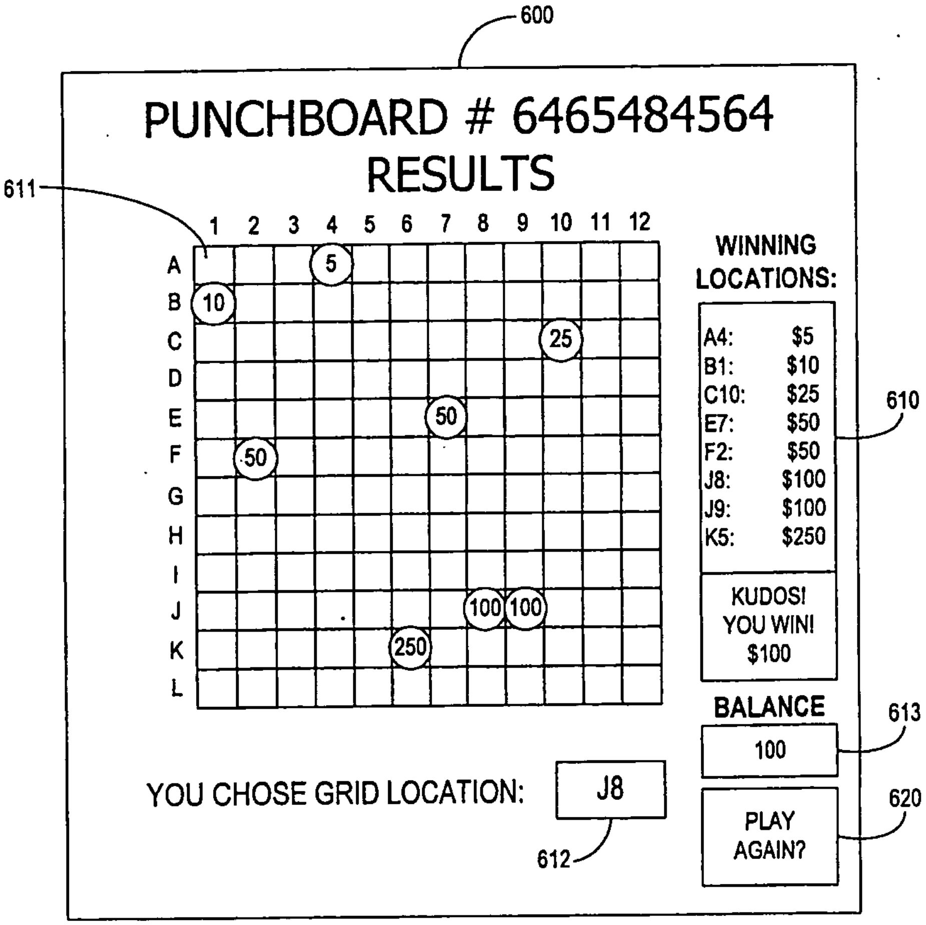

500
510
PUNCHBOARD # 6465484564
511
1 2 3 4 5 6 7 8 9 10 11 12
A B C D E F G H I J K L
CREDITS
1
513
OVER $500 IN PRIZE MONEY!
SELECT GRID LOCATION:
512

FIG. 5



PUNCHBOARD # 6465484564
RESULTS

	1	2	3	4	5	6	7	8	9	10	11	12
A				5								
B	10											
C										25		
D												
E							50					
F		50										
G												
H												
I												
J								100	100			
K						250						
L												

WINNING LOCATIONS:

A4:	$5
B1:	$10
C10:	$25
E7:	$50
F2:	$50
J8:	$100
J9:	$100
K5:	$250

KUDOS! YOU WIN! $100

BALANCE

100

YOU CHOSE GRID LOCATION: J8

PLAY AGAIN?

FIG. 6

CUSTOMER DATABASE 211

CUSTOMER NAME 701	CUSTOMER ID NUMBER 702	CREDIT CARD NUMBER 703	CUSTOMER E-MAIL ADDRESS 704	CUSTOMER ADDRESS 705	TOTAL MONEY SPENT 706	TOTAL MONEY AWARDED 707	SELECTION PREFERENCES 708	PRIZE AWARD PAYMENT PREFERENCE 709
BILL SMITH	4588	6465 4645 6546 5648	SMITH@AOL.COM	4 RED ST.	$75.00	$100.00	J8	CHECK BY MAIL
ANGEL STAR	4544	6546 5465 4688 4589	ANGEL@UNIVERSITY .EDU	6 BLUE RD.	$15.00	$0.00	A4, B4, C4, D4	TRANSFER TO CREDIT CARD ACCOUNT
JOE BEAD	4321	0103 1831 8555 1215	JBEAD@WIDGET.COM	87 PINK LN.	$36.00	$350.00	NONE	CHECK BY MAIL

FIG. 7A

PRIZE DISTRIBUTION DATABASE 214

PRIZE DISTRIBUTION IDENTIFICATION NUMBER 711	GRID SIZE 712	DENOMINATION 713	PRIZE ALLOCATION 714
001	10 X 10	$1.00	$50, $5, $10, $25, $50, $100, $25, $5
002	20 X 30	$3.00	$5, $10, $25, $50, $50, $100, $100, $250
003	30 X 30	$5.00	$100, $25, $50, $100, $100, $250, $500, $5
004	30 X 30	$5.00	$1,000, $500, $500, $250, $250, $100, $100, $100, $50, $50, $50, $25, $15, $5, $5

FIG. 7B

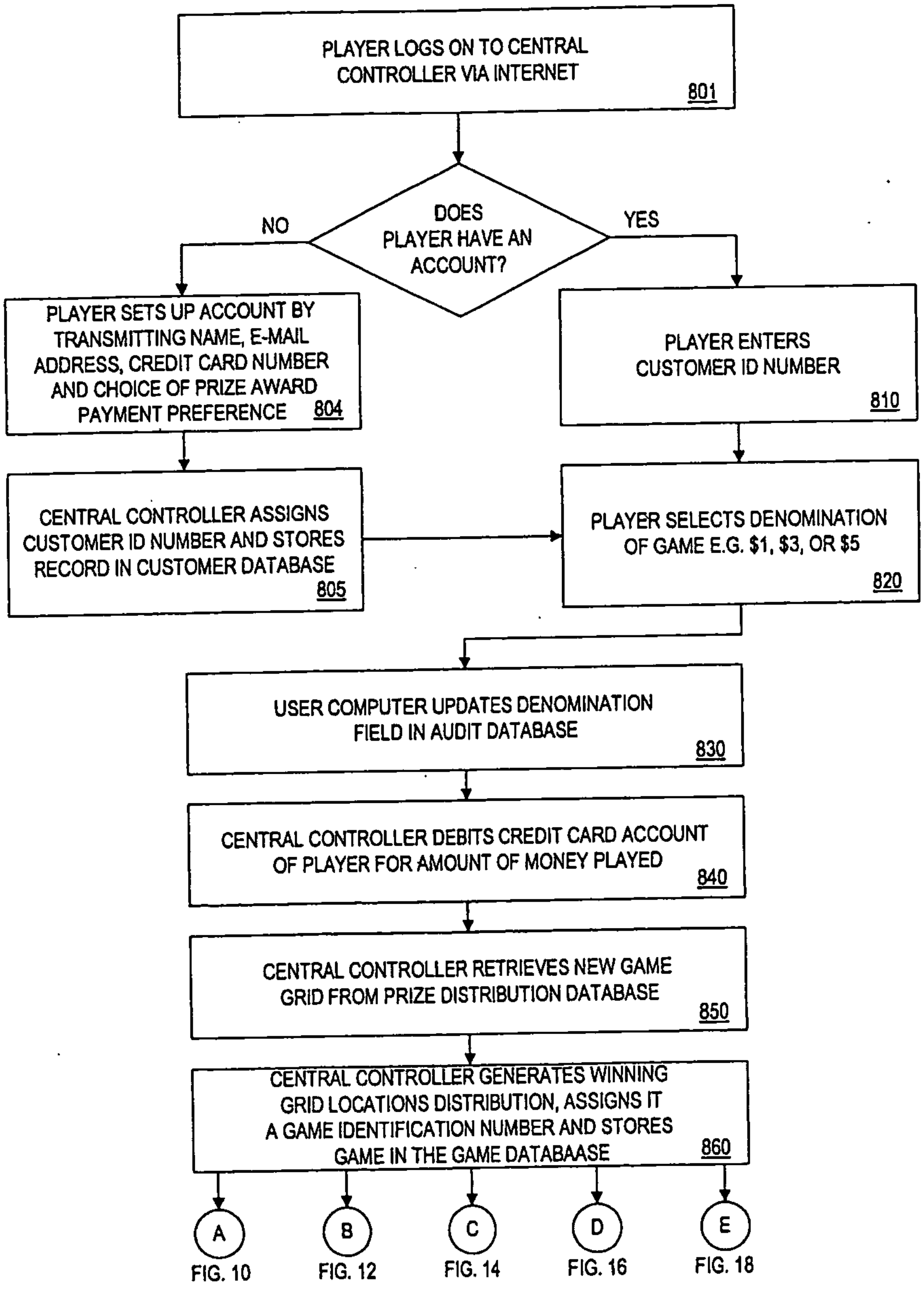

PLAYER LOGS ON TO CENTRAL CONTROLLER VIA INTERNET
801
DOES PLAYER HAVE AN ACCOUNT?
NO
YES
PLAYER SETS UP ACCOUNT BY TRANSMITTING NAME, E-MAIL ADDRESS, CREDIT CARD NUMBER AND CHOICE OF PRIZE AWARD PAYMENT PREFERENCE
804
PLAYER ENTERS CUSTOMER ID NUMBER
810
CENTRAL CONTROLLER ASSIGNS CUSTOMER ID NUMBER AND STORES RECORD IN CUSTOMER DATABASE
805
PLAYER SELECTS DENOMINATION OF GAME E.G. $1, $3, OR $5
820
USER COMPUTER UPDATES DENOMINATION FIELD IN AUDIT DATABASE
830
CENTRAL CONTROLLER DEBITS CREDIT CARD ACCOUNT OF PLAYER FOR AMOUNT OF MONEY PLAYED
840
CENTRAL CONTROLLER RETRIEVES NEW GAME GRID FROM PRIZE DISTRIBUTION DATABASE
850
CENTRAL CONTROLLER GENERATES WINNING GRID LOCATIONS DISTRIBUTION, ASSIGNS IT A GAME IDENTIFICATION NUMBER AND STORES GAME IN THE GAME DATABAASE
860
A
FIG. 10
B
FIG. 12
C
FIG. 14
D
FIG. 16
E
FIG. 18

FIG. 8

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION(S) 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	PLAYER KEY 904
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$3.00	11000101011010 01101101011...
6465486546	A4, I2, K1	A5 $100, D7 $25, E8 $25, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	$5.00	1100011001111 01011010101...
6214563168		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	$1.00	

FIG. 9A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATION 903	ENCRYPTED GRID LOCATION 910	DECRYPTED GRID LOCATION 920	PLAYER KEY 930
6465484564	4588	A4 $5, B1 $10, C 10 $25, E7 $50, J8 $100, J9 $100, K5 $250	AS498DF...	J8	101010101111011...
6465484565	4544	A2 $5, B3 $10, B4 $100, D6 $250, D7 $25, E2 $50, G1 $50	ADSFU90A8 FLDJ0D...		
	4321	A9 $100, C5 $50, D1 $100,E9 $25, F5 $25, G4 $50, G8 $25, H1 $250			
		A8 $25, B3 $50, C1 $5, D2 $10, G4 $100, H6 $250, J11 $25, K3 $100			

FIG. 9B

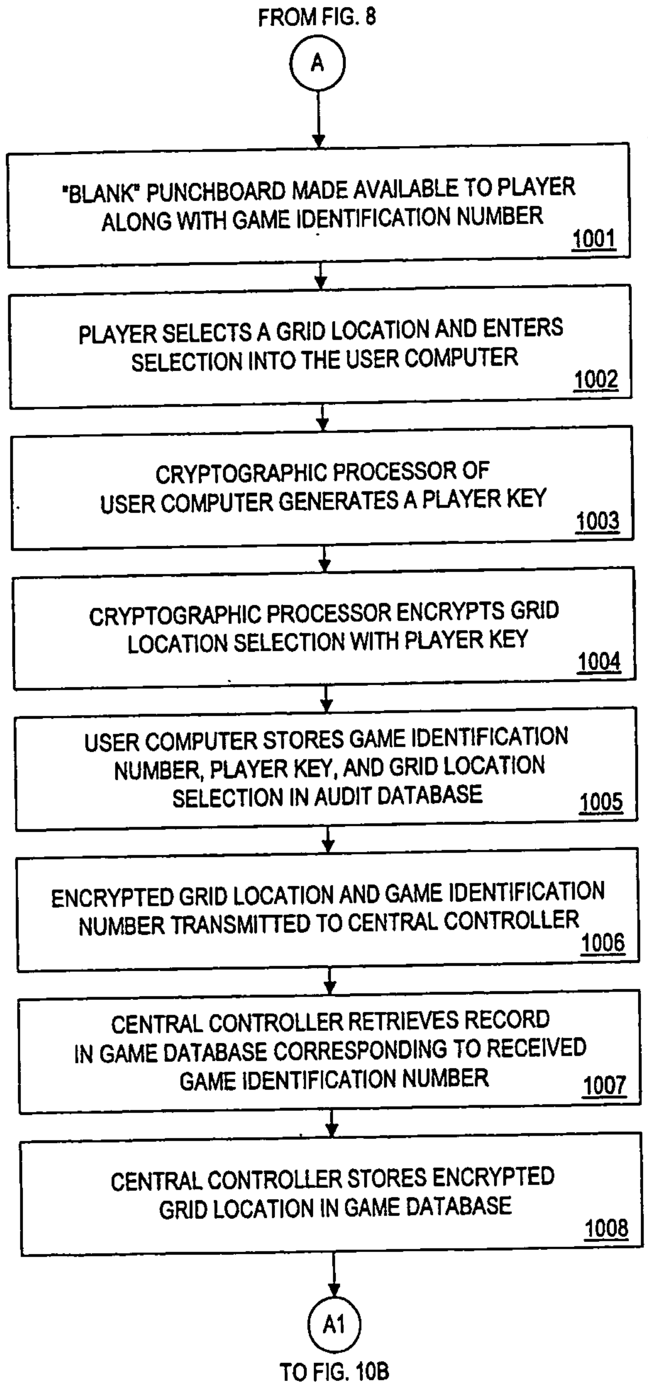

FROM FIG. 8
A
"BLANK" PUNCHBOARD MADE AVAILABLE TO PLAYER ALONG WITH GAME IDENTIFICATION NUMBER
1001
PLAYER SELECTS A GRID LOCATION AND ENTERS SELECTION INTO THE USER COMPUTER
1002
CRYPTOGRAPHIC PROCESSOR OF USER COMPUTER GENERATES A PLAYER KEY
1003
CRYPTOGRAPHIC PROCESSOR ENCRYPTS GRID LOCATION SELECTION WITH PLAYER KEY
1004
USER COMPUTER STORES GAME IDENTIFICATION NUMBER, PLAYER KEY, AND GRID LOCATION SELECTION IN AUDIT DATABASE
1005
ENCRYPTED GRID LOCATION AND GAME IDENTIFICATION NUMBER TRANSMITTED TO CENTRAL CONTROLLER
1006
CENTRAL CONTROLLER RETRIEVES RECORD IN GAME DATABASE CORRESPONDING TO RECEIVED GAME IDENTIFICATION NUMBER
1007
CENTRAL CONTROLLER STORES ENCRYPTED GRID LOCATION IN GAME DATABASE
1008
A1
TO FIG. 10B

FIG. 10A

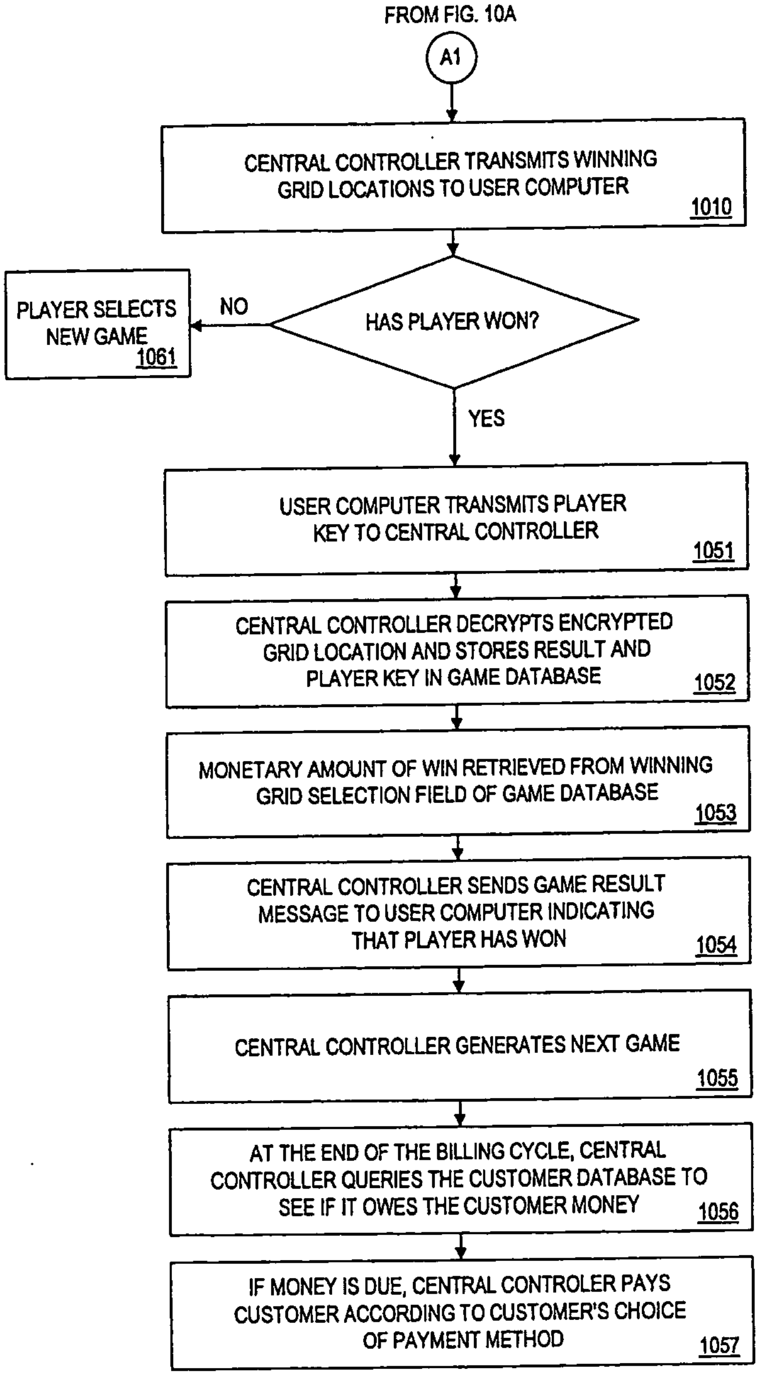
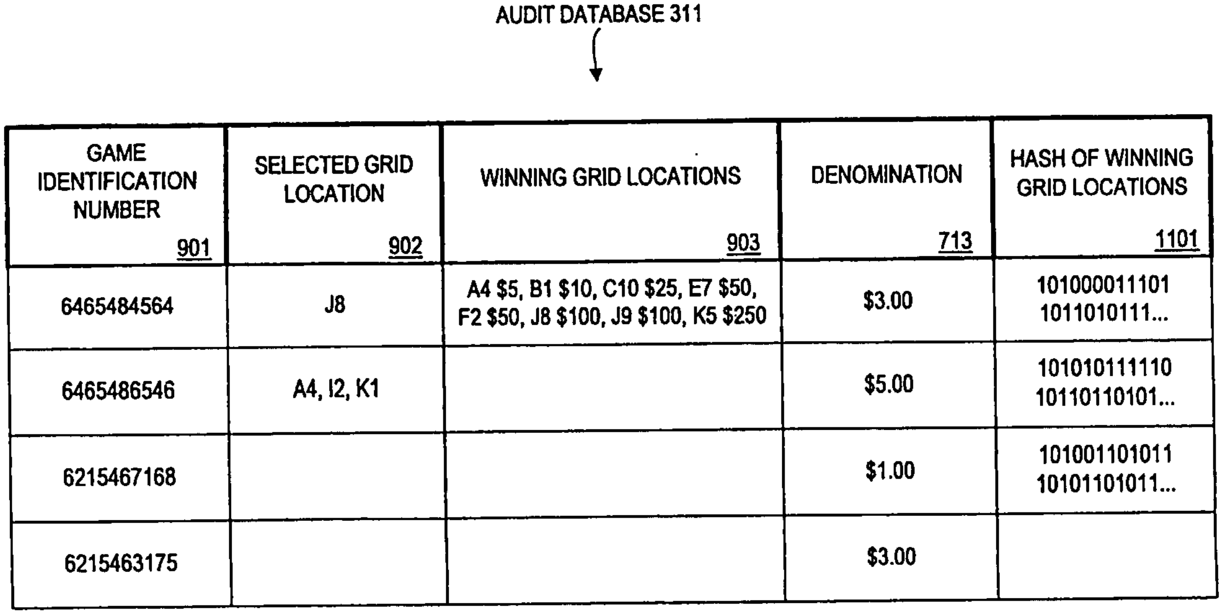

FROM FIG. 10A
A1
CENTRAL CONTROLLER TRANSMITS WINNING GRID LOCATIONS TO USER COMPUTER
1010
HAS PLAYER WON?
NO
PLAYER SELECTS NEW GAME
1061
YES
USER COMPUTER TRANSMITS PLAYER KEY TO CENTRAL CONTROLLER
1051
CENTRAL CONTROLLER DECRYPTS ENCRYPTED GRID LOCATION AND STORES RESULT AND PLAYER KEY IN GAME DATABASE
1052
MONETARY AMOUNT OF WIN RETRIEVED FROM WINNING GRID SELECTION FIELD OF GAME DATABASE
1053
CENTRAL CONTROLLER SENDS GAME RESULT MESSAGE TO USER COMPUTER INDICATING THAT PLAYER HAS WON
1054
CENTRAL CONTROLLER GENERATES NEXT GAME
1055
AT THE END OF THE BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1056
IF MONEY IS DUE, CENTRAL CONTROLER PAYS CUSTOMER ACCORDING TO CUSTOMER'S CHOICE OF PAYMENT METHOD
1057

FIG. 10B


AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	HASH OF WINNING GRID LOCATIONS 1101
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$3.00	101000011101 1011010111...
6465486546	A4, I2, K1		$5.00	101010111110 10110110101...
6215467168			$1.00	101001101011 10101101011...
6215463175			$3.00	

FIG. 11A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATIONS 903	USER GRID SELECTION 902	HASH OF WINNING GRID LOCATION 1101
6465484564	4588	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	J8	101000111010...
6465484565	4544	A2 $5, B3 $10, B4 $100, D6 $250, D7 $25, E2 $50, G1 $50		101010111110...
64654845666	4321	A9 $100, C5 $50, D1 $100, E9 $25, F5 $25, G4 $50, G8 $25, H1 $250		
64654845667		A8, $25, B3 $$50, C1 $5, D2 $10, G4 $100,H6 $250, J11, $25, K3 $100		

FIG. 11B

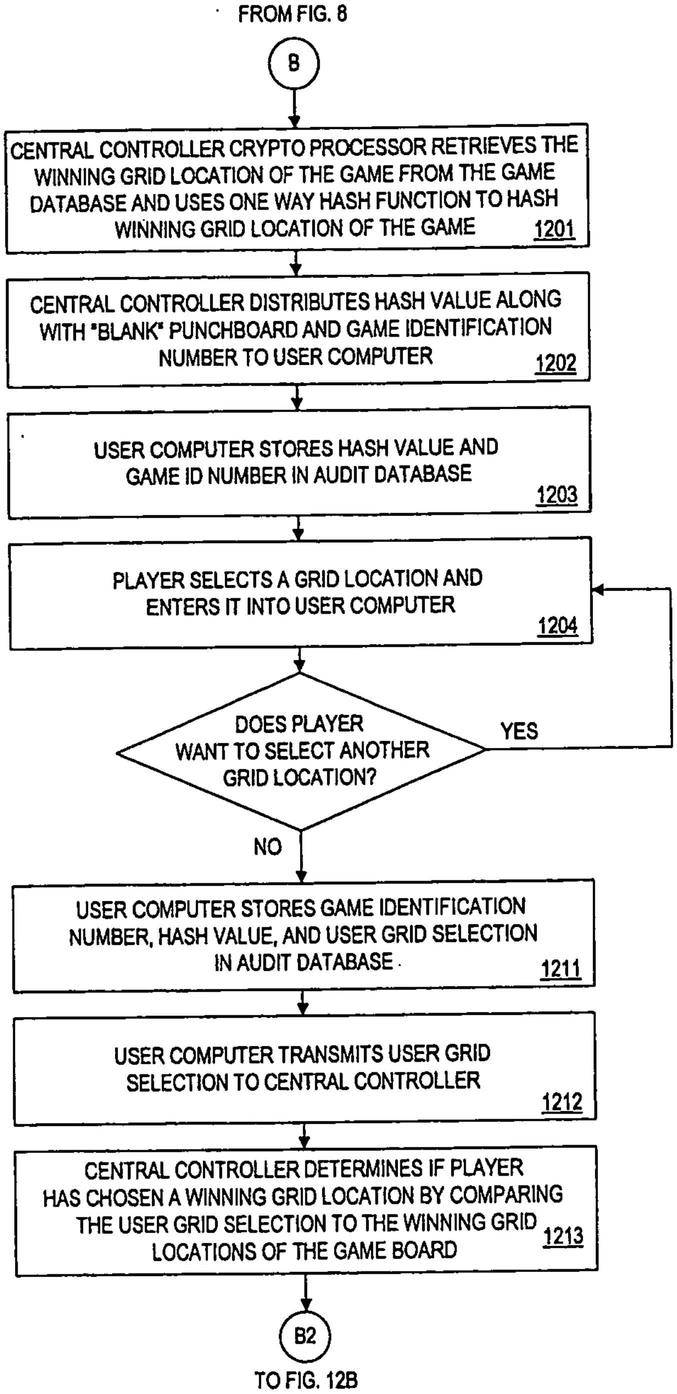

FROM FIG. 8
B
CENTRAL CONTROLLER CRYPTO PROCESSOR RETRIEVES THE WINNING GRID LOCATION OF THE GAME FROM THE GAME DATABASE AND USES ONE WAY HASH FUNCTION TO HASH WINNING GRID LOCATION OF THE GAME 1201
CENTRAL CONTROLLER DISTRIBUTES HASH VALUE ALONG WITH "BLANK" PUNCHBOARD AND GAME IDENTIFICATION NUMBER TO USER COMPUTER 1202
USER COMPUTER STORES HASH VALUE AND GAME ID NUMBER IN AUDIT DATABASE 1203
PLAYER SELECTS A GRID LOCATION AND ENTERS IT INTO USER COMPUTER 1204
DOES PLAYER WANT TO SELECT ANOTHER GRID LOCATION?
YES
NO
USER COMPUTER STORES GAME IDENTIFICATION NUMBER, HASH VALUE, AND USER GRID SELECTION IN AUDIT DATABASE 1211
USER COMPUTER TRANSMITS USER GRID SELECTION TO CENTRAL CONTROLLER 1212
CENTRAL CONTROLLER DETERMINES IF PLAYER HAS CHOSEN A WINNING GRID LOCATION BY COMPARING THE USER GRID SELECTION TO THE WINNING GRID LOCATIONS OF THE GAME BOARD 1213
B2
TO FIG. 12B

FIG. 12A

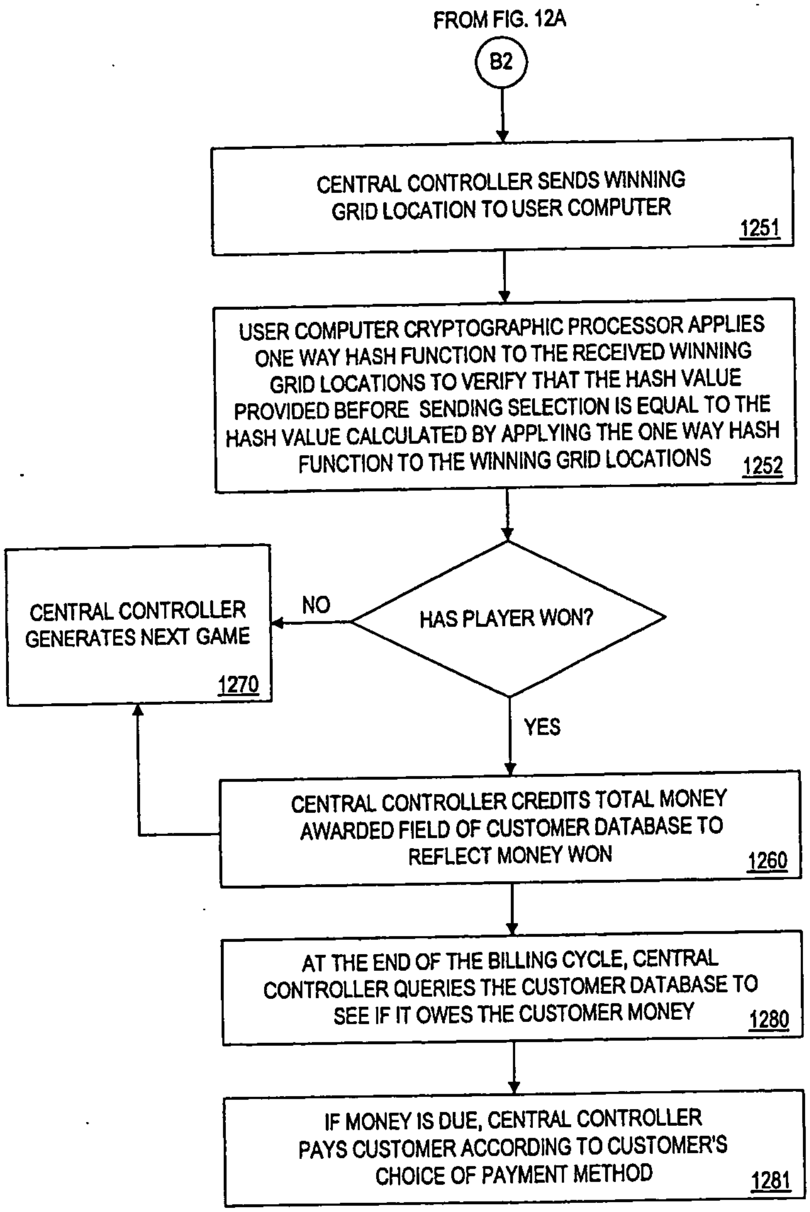
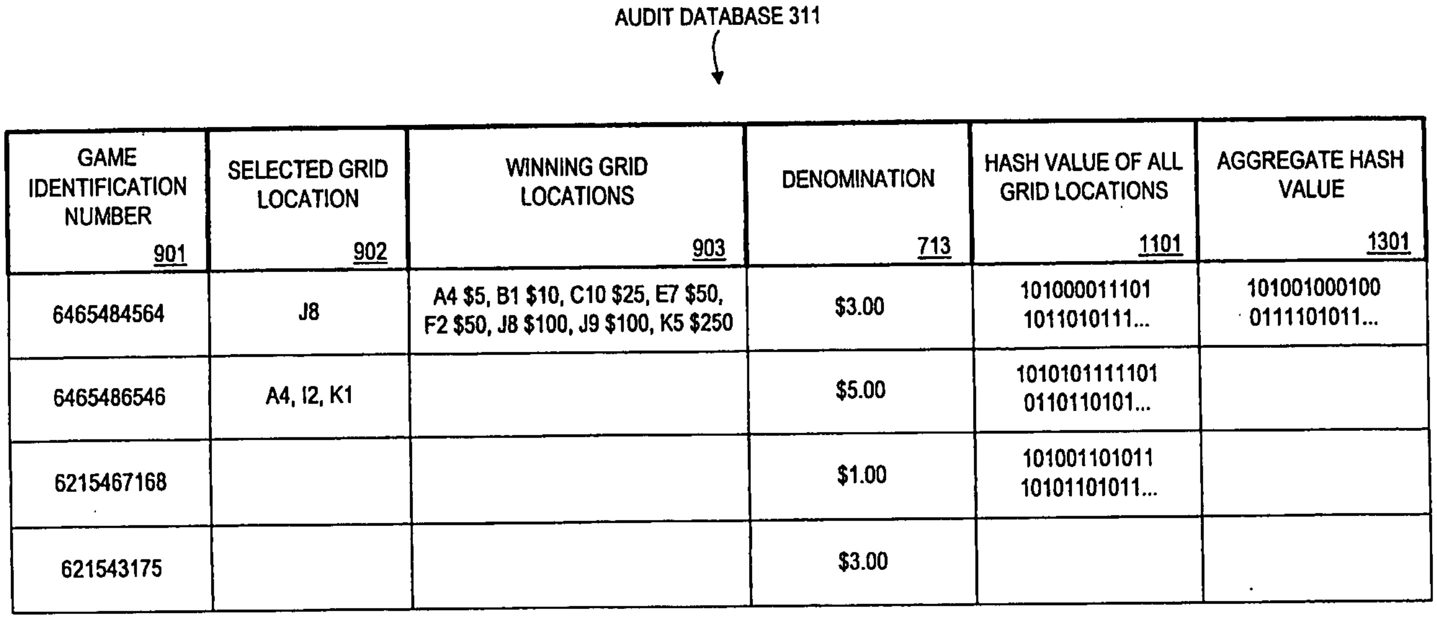

FROM FIG. 12A
B2
CENTRAL CONTROLLER SENDS WINNING GRID LOCATION TO USER COMPUTER
1251
USER COMPUTER CRYPTOGRAPHIC PROCESSOR APPLIES ONE WAY HASH FUNCTION TO THE RECEIVED WINNING GRID LOCATIONS TO VERIFY THAT THE HASH VALUE PROVIDED BEFORE SENDING SELECTION IS EQUAL TO THE HASH VALUE CALCULATED BY APPLYING THE ONE WAY HASH FUNCTION TO THE WINNING GRID LOCATIONS
1252
HAS PLAYER WON?
NO
CENTRAL CONTROLLER GENERATES NEXT GAME
1270
YES
CENTRAL CONTROLLER CREDITS TOTAL MONEY AWARDED FIELD OF CUSTOMER DATABASE TO REFLECT MONEY WON
1260
AT THE END OF THE BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1280
IF MONEY IS DUE, CENTRAL CONTROLLER PAYS CUSTOMER ACCORDING TO CUSTOMER'S CHOICE OF PAYMENT METHOD
1281

FIG. 12B


AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	HASH VALUE OF ALL GRID LOCATIONS 1101	AGGREGATE HASH VALUE 1301
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$3.00	101000011101 1011010111...	101001000100 0111101011...
6465486546	A4, I2, K1		$5.00	1010101111101 0110110101...	
6215467168			$1.00	101001101011 10101101011...	
621543175			$3.00		

FIG. 13A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATIONS 903	USER SELECTED GRID LOCATIONS 902	HASH VALUE OF ENTIRE GRID 1101	AGGREGATE HASH VALUE 1301	DENOMINATION 713
6465484564	4588	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	J8	101000111010...	10100100010 0110011110...	$3.00
6465484564	4589	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	C2	101010111110...	10100000111 1101110000...	$3.00
6465484564	3218	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	C12, D13	101001101011...		$3.00
6465484564		A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250				$3.00

FIG. 13B

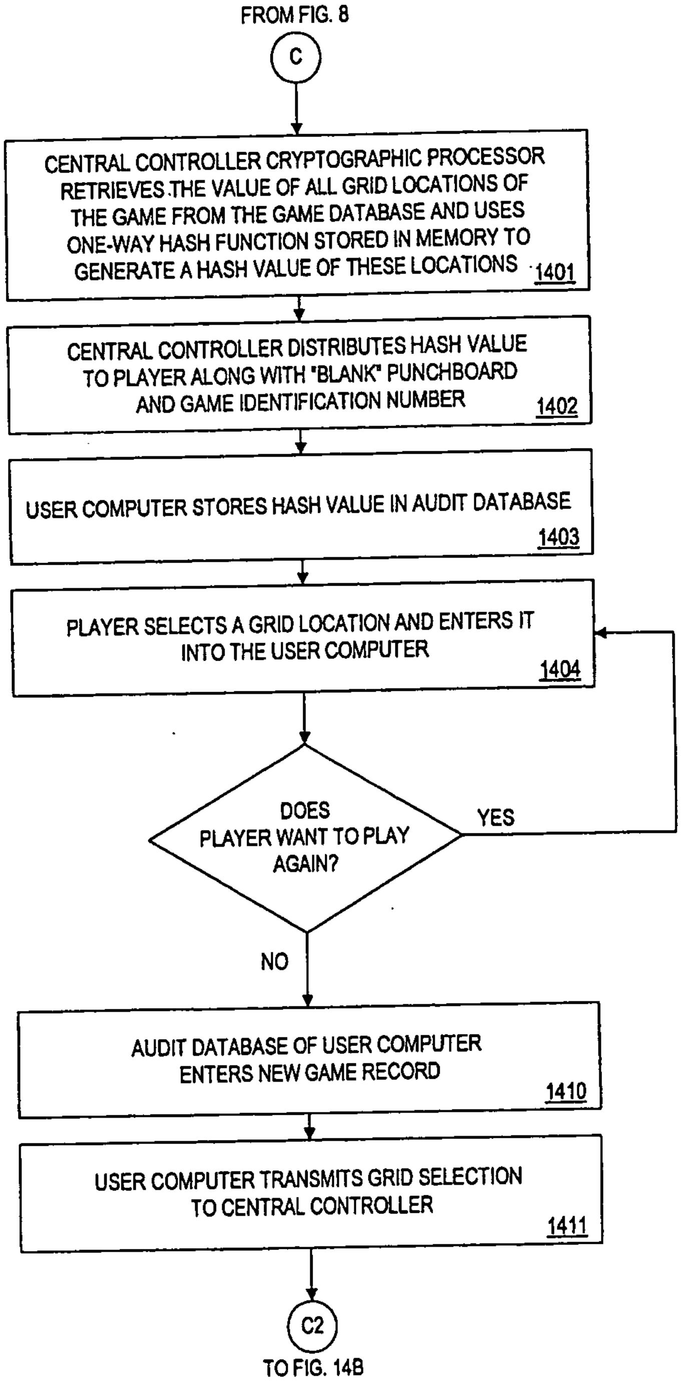

FROM FIG. 8
C
CENTRAL CONTROLLER CRYPTOGRAPHIC PROCESSOR RETRIEVES THE VALUE OF ALL GRID LOCATIONS OF THE GAME FROM THE GAME DATABASE AND USES ONE-WAY HASH FUNCTION STORED IN MEMORY TO GENERATE A HASH VALUE OF THESE LOCATIONS
1401
CENTRAL CONTROLLER DISTRIBUTES HASH VALUE TO PLAYER ALONG WITH "BLANK" PUNCHBOARD AND GAME IDENTIFICATION NUMBER
1402
USER COMPUTER STORES HASH VALUE IN AUDIT DATABASE
1403
PLAYER SELECTS A GRID LOCATION AND ENTERS IT INTO THE USER COMPUTER
1404
DOES PLAYER WANT TO PLAY AGAIN?
YES
NO
AUDIT DATABASE OF USER COMPUTER ENTERS NEW GAME RECORD
1410
USER COMPUTER TRANSMITS GRID SELECTION TO CENTRAL CONTROLLER
1411
C2
TO FIG. 14B

FIG. 14A

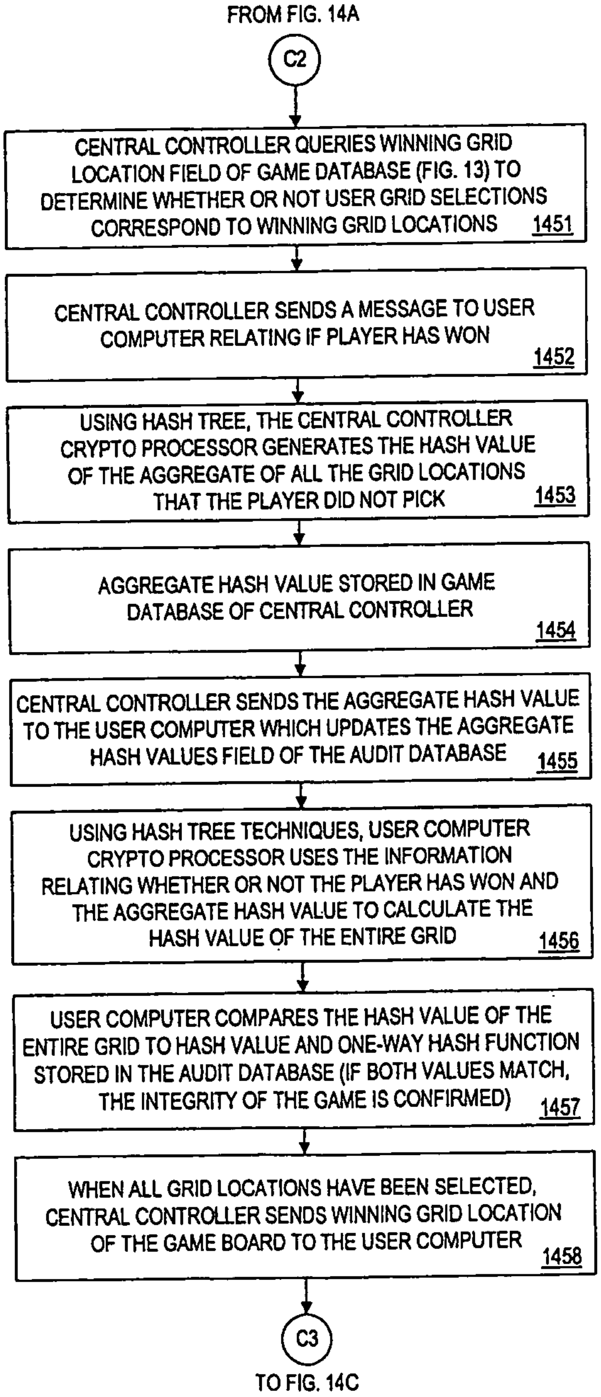

FROM FIG. 14A
C2
CENTRAL CONTROLLER QUERIES WINNING GRID LOCATION FIELD OF GAME DATABASE (FIG. 13) TO DETERMINE WHETHER OR NOT USER GRID SELECTIONS CORRESPOND TO WINNING GRID LOCATIONS 1451
CENTRAL CONTROLLER SENDS A MESSAGE TO USER COMPUTER RELATING IF PLAYER HAS WON 1452
USING HASH TREE, THE CENTRAL CONTROLLER CRYPTO PROCESSOR GENERATES THE HASH VALUE OF THE AGGREGATE OF ALL THE GRID LOCATIONS THAT THE PLAYER DID NOT PICK 1453
AGGREGATE HASH VALUE STORED IN GAME DATABASE OF CENTRAL CONTROLLER 1454
CENTRAL CONTROLLER SENDS THE AGGREGATE HASH VALUE TO THE USER COMPUTER WHICH UPDATES THE AGGREGATE HASH VALUES FIELD OF THE AUDIT DATABASE 1455
USING HASH TREE TECHNIQUES, USER COMPUTER CRYPTO PROCESSOR USES THE INFORMATION RELATING WHETHER OR NOT THE PLAYER HAS WON AND THE AGGREGATE HASH VALUE TO CALCULATE THE HASH VALUE OF THE ENTIRE GRID 1456
USER COMPUTER COMPARES THE HASH VALUE OF THE ENTIRE GRID TO HASH VALUE AND ONE-WAY HASH FUNCTION STORED IN THE AUDIT DATABASE (IF BOTH VALUES MATCH, THE INTEGRITY OF THE GAME IS CONFIRMED) 1457
WHEN ALL GRID LOCATIONS HAVE BEEN SELECTED, CENTRAL CONTROLLER SENDS WINNING GRID LOCATION OF THE GAME BOARD TO THE USER COMPUTER 1458
C3
TO FIG. 14C

FIG. 14B

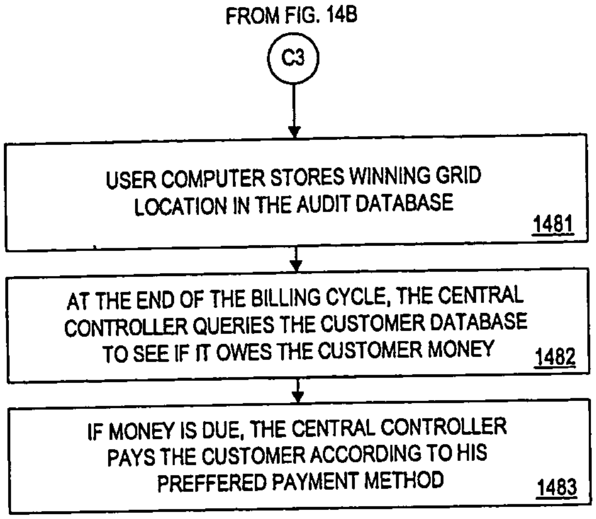
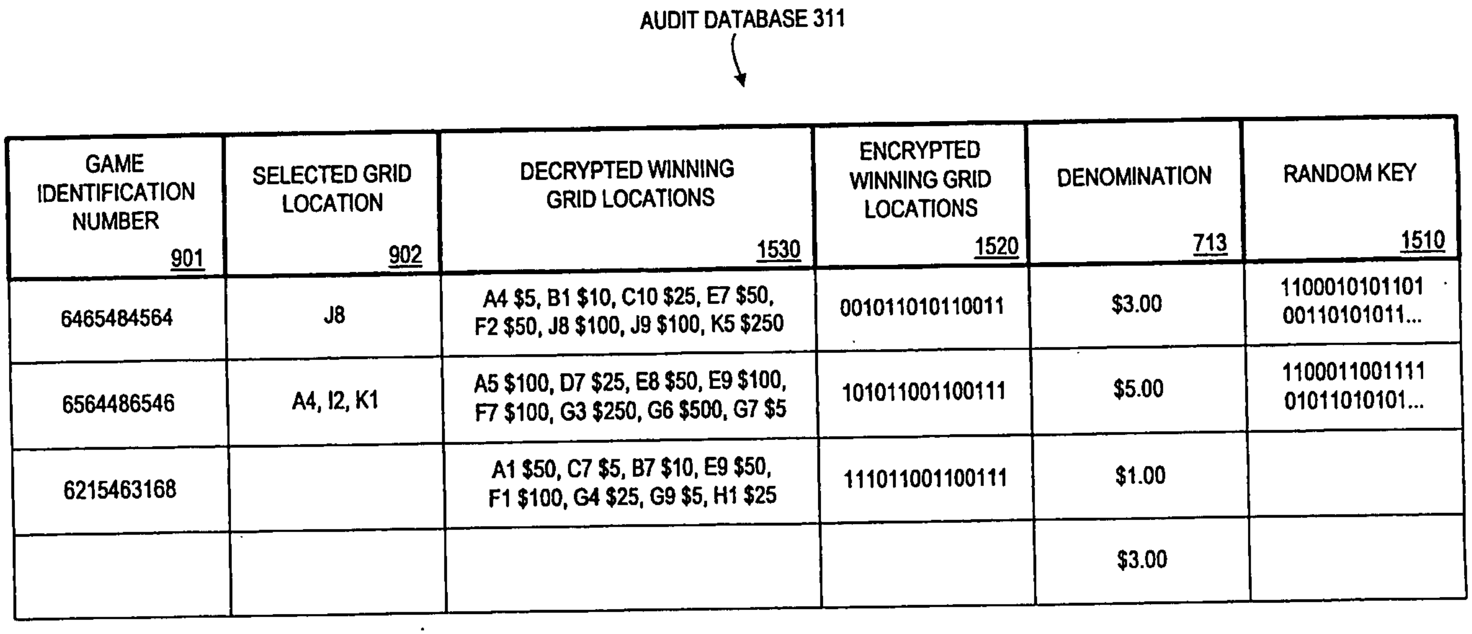

FROM FIG. 14B
C3
USER COMPUTER STORES WINNING GRID LOCATION IN THE AUDIT DATABASE
1481
AT THE END OF THE BILLING CYCLE, THE CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1482
IF MONEY IS DUE, THE CENTRAL CONTROLLER PAYS THE CUSTOMER ACCORDING TO HIS PREFFERED PAYMENT METHOD
1483

FIG. 14C


AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	DECRYPTED WINNING GRID LOCATIONS 1530	ENCRYPTED WINNING GRID LOCATIONS 1520	DENOMINATION 713	RANDOM KEY 1510
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	001011010110011	$3.00	1100010101101 00110101011...
6564486546	A4, I2, K1	A5 $100, D7 $25, E8 $50, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	101011001100111	$5.00	1100011001111 01011010101...
6215463168		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	111011001100111	$1.00	
				$3.00	

FIG. 15A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATIONS 903	USER SELECTED GRID LOCATION 902	RANDOM KEY 1510	DENOMINATION OF GAME 713
6465484564	4588	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	J8	110001010110 100110101011...	$3.00
6465484565	4544	A2 $5, B3 $10, B4 $100, D6 $250, D7 $25 E2 $50, G1 $50	A4, I2, K1	110001100111 101011010101...	$5.00
	4321	A9 $100, C5 $50, D1 $100, E9 $25, F5 $25, G4 $50, G8 $25, H1 $250			
		A8 $25, B3 $50, C1 $5, D2 $10, G4 $100, H6 $250, J11 $25, K3 $100			

FIG. 15B

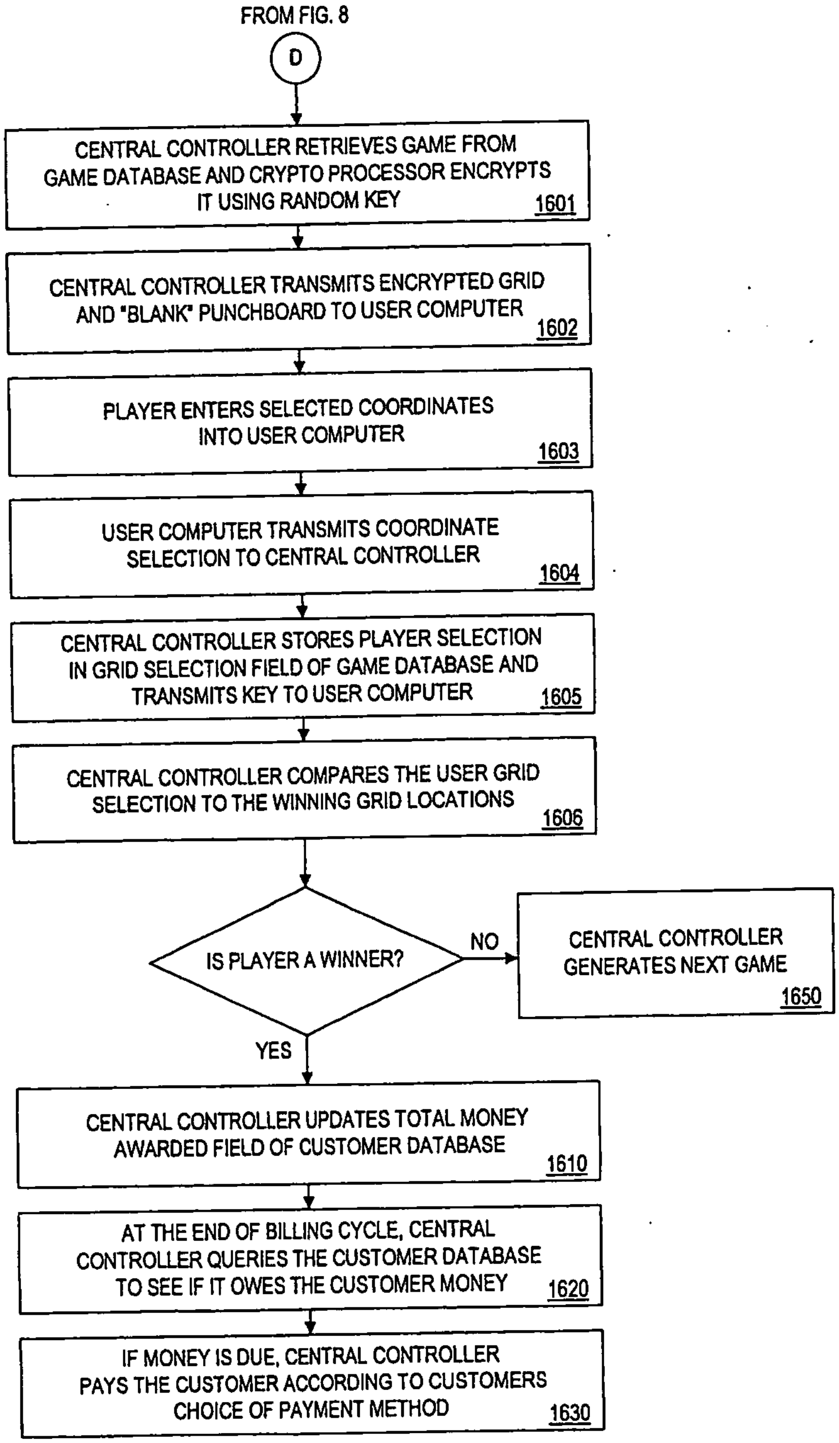

FROM FIG. 8
D
CENTRAL CONTROLLER RETRIEVES GAME FROM GAME DATABASE AND CRYPTO PROCESSOR ENCRYPTS IT USING RANDOM KEY 1601
CENTRAL CONTROLLER TRANSMITS ENCRYPTED GRID AND "BLANK" PUNCHBOARD TO USER COMPUTER 1602
PLAYER ENTERS SELECTED COORDINATES INTO USER COMPUTER 1603
USER COMPUTER TRANSMITS COORDINATE SELECTION TO CENTRAL CONTROLLER 1604
CENTRAL CONTROLLER STORES PLAYER SELECTION IN GRID SELECTION FIELD OF GAME DATABASE AND TRANSMITS KEY TO USER COMPUTER 1605
CENTRAL CONTROLLER COMPARES THE USER GRID SELECTION TO THE WINNING GRID LOCATIONS 1606
IS PLAYER A WINNER?
NO
CENTRAL CONTROLLER GENERATES NEXT GAME 1650
YES
CENTRAL CONTROLLER UPDATES TOTAL MONEY AWARDED FIELD OF CUSTOMER DATABASE 1610
AT THE END OF BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY 1620
IF MONEY IS DUE, CENTRAL CONTROLLER PAYS THE CUSTOMER ACCORDING TO CUSTOMERS CHOICE OF PAYMENT METHOD 1630

FIG. 16

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	CUSTOMER ID NUMBER 702
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$1.00	4588
6465484565	A4, I2, K1	A5 $100, D7 $25, E8 $50, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	$3.00	4544
6465484566		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	$5.00	4321

FIG. 17A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	CUSTOMER ID NUMBER 702
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$1.00	4588
6465484565	A4, I2, K1	A5 $100, D7 $25, E8 $50, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	$3.00	4544
6465484566		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	$5.00	4321

FIG. 17B

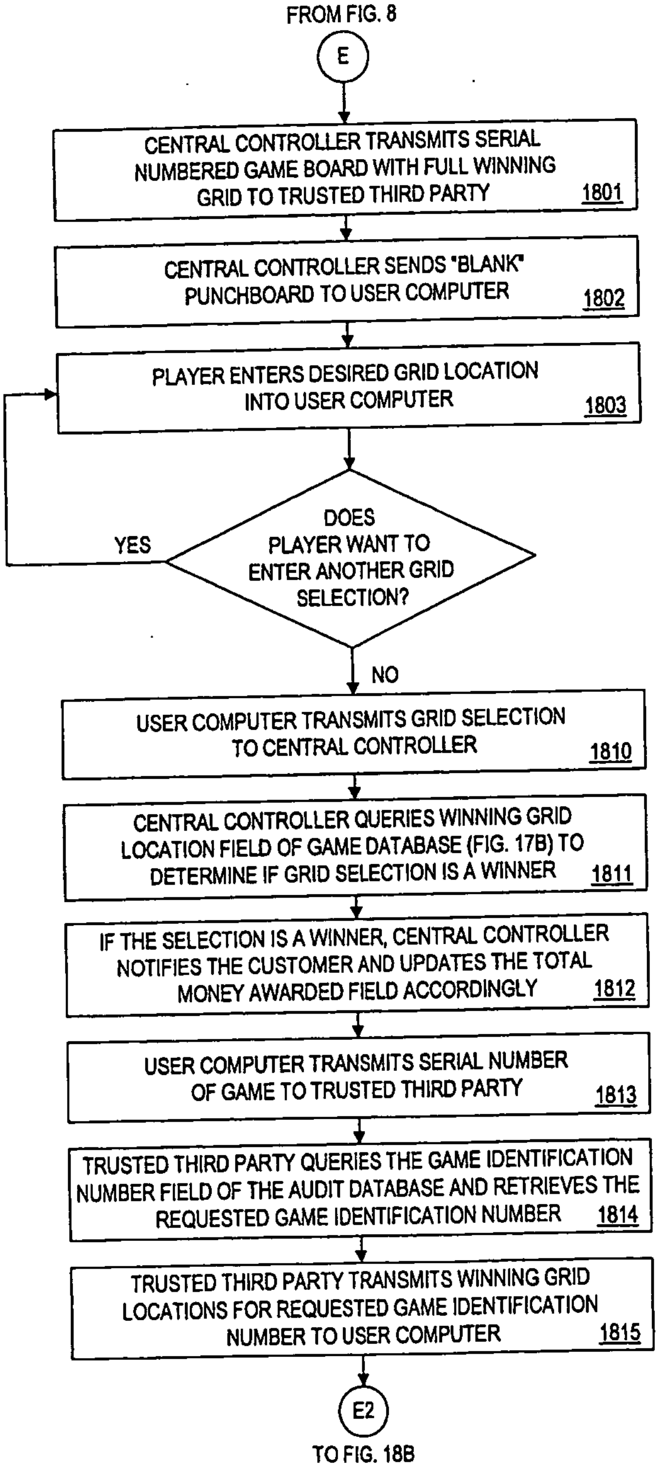

FROM FIG. 8
E
CENTRAL CONTROLLER TRANSMITS SERIAL NUMBERED GAME BOARD WITH FULL WINNING GRID TO TRUSTED THIRD PARTY 1801
CENTRAL CONTROLLER SENDS "BLANK" PUNCHBOARD TO USER COMPUTER 1802
PLAYER ENTERS DESIRED GRID LOCATION INTO USER COMPUTER 1803
DOES PLAYER WANT TO ENTER ANOTHER GRID SELECTION?
YES
NO
USER COMPUTER TRANSMITS GRID SELECTION TO CENTRAL CONTROLLER 1810
CENTRAL CONTROLLER QUERIES WINNING GRID LOCATION FIELD OF GAME DATABASE (FIG. 17B) TO DETERMINE IF GRID SELECTION IS A WINNER 1811
IF THE SELECTION IS A WINNER, CENTRAL CONTROLLER NOTIFIES THE CUSTOMER AND UPDATES THE TOTAL MONEY AWARDED FIELD ACCORDINGLY 1812
USER COMPUTER TRANSMITS SERIAL NUMBER OF GAME TO TRUSTED THIRD PARTY 1813
TRUSTED THIRD PARTY QUERIES THE GAME IDENTIFICATION NUMBER FIELD OF THE AUDIT DATABASE AND RETRIEVES THE REQUESTED GAME IDENTIFICATION NUMBER 1814
TRUSTED THIRD PARTY TRANSMITS WINNING GRID LOCATIONS FOR REQUESTED GAME IDENTIFICATION NUMBER TO USER COMPUTER 1815
E2
TO FIG. 18B

FIG. 18A

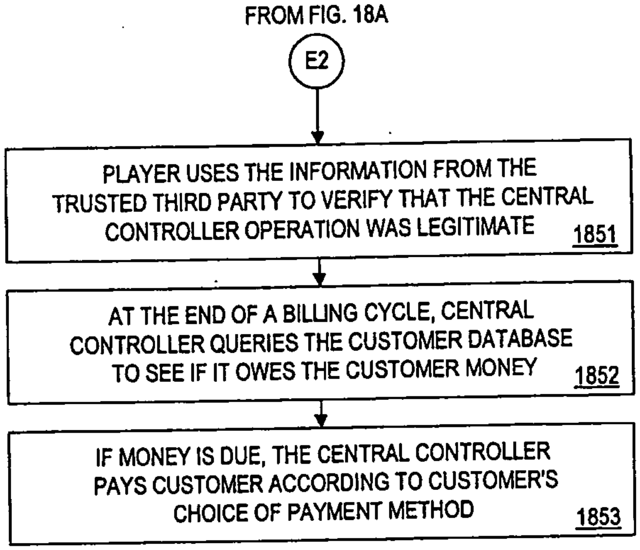

FROM FIG. 18A
E2
PLAYER USES THE INFORMATION FROM THE TRUSTED THIRD PARTY TO VERIFY THAT THE CENTRAL CONTROLLER OPERATION WAS LEGITIMATE
1851
AT THE END OF A BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1852
IF MONEY IS DUE, THE CENTRAL CONTROLLER PAYS CUSTOMER ACCORDING TO CUSTOMER'S CHOICE OF PAYMENT METHOD
1853

FIG. 18B

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 155/00, 161/00	A1	(11) International Publication Number: WO 96/00950 (43) International Publication Date: 11 January 1996 (11.01.96)

(21) International Application Number: PCT/US95/08206

(22) International Filing Date: 28 June 1995 (28.06.95)

(30) Priority Data:

08/269,248	30 June 1994 (30.06.94)	US
08/406,224	16 March 1995 (16.03.95)	US

(71) Applicant: WALKER ASSET MANAGEMENT LIMITED PARTNERSHIP [US/US]; 125 Elm Street, New Canaan, CT 06840 (US).

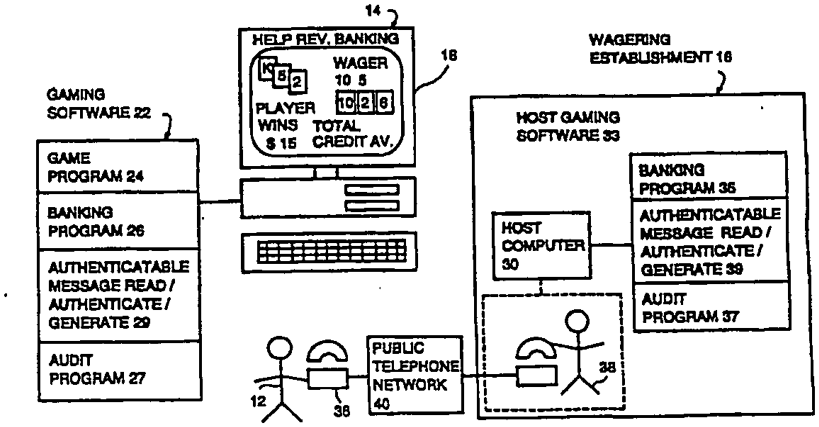
(72) Inventors: WALKER, Jay; 124 Spectacle Lane, Ridgefield, CT 06877 (US). SCHNEIER, Bruce; 730 Fair Oaks Avenue, Oak Park, IL 60302 (US).

(74) Agents: ROTHSTEIN, Jesse et al.; Amster, Rothstein & Ebenstein, 90 Park Avenue, New York, NY 10016 (US).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KR, KZ, LK, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SECURE IMPROVED REMOTE GAMING SYSTEM



(57) Abstract

A remote gaming system whereby a player can gamble against a wagering establishment (16) or state-run lottery from a remote location on a personal computer or portable computer device (14) where it is unnecessary to establish an on-line connection with a host computer associated with the wagering establishment, the gaming computer having gaming software (22) for providing a wagering opportunity and enabling the player to obtain gambling credit and cash-out any winnings, the host computer (30) enabling the player to purchase and redeem gambling credit at the remote lcoation using cryptographic protocols through a series of authenticatable message exchanges between the player and the establishment, the gaming computer and the host computer directly on-line, or the gaming computer having a detachable tamper-resistant or tamper-evident credit module associated therewith or for use with a personal computer being provided to the player with preloaded gambling credit.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Larvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

SECURE IMPROVED REMOTE GAMING SYSTEM

This Application is a continuation-in-part of copending Application Serial No. 08/269,248, filed on June 30, 1994, which is a continuation-in-part of copending Application Serial No. 08/212,348, filed on March 11, 1994.

BACKGROUND

1. Field of the Invention

The present invention relates generally to a remote gaming system, and more particularly, to a remote gaming system by which a player can wager on a plurality of games of chance and/or future public events of which the outcome is uncertain, offered by a casino, government lottery organization, or other wagering establishment.

2. Description of the Prior Art

In the past, a player wishing to wager on a game of chance such as those offered in a casino or on a public event of which the outcome is uncertain such as sporting events, had a limited number of options. In order to wager on casino games such as roulette, blackjack, poker and the like, the player had to physically travel to a gaming establishment specifically engaged in such activities or to a location where stand-alone gambling devices such as video poker terminals or slot machines were available. Although public events such as horse races may be wagered on by telephone contact with an authorized "off-track betting" gaming establishment or its agent, such methods utilizing telephone contact have not been amenable to typical casino games.

As a result of advances in computer technology and telecommunications, remote gaming systems have been devised in which a player can participate in a plurality of games of chance being offered by a gambling establishment without having to be physically located on the premises. An example is found in U.S.

Patent Nos. 4,339,798 and 4,467,424, both to Hedges et al. The Hedges Patents disclose a remote gaming system wherein a player proceeds to gamble against the casino at a remote player station which includes a live game display to permit the player to engage in actual games of chance as they are being played in real-time at a croupier station comprised of one or more gaming tables in the casino. The player station includes a changeable keyboard communicating with a microprocessor for displaying a selected one of a plurality of wagering possibilities corresponding to a selected one of the plurality of games being played and for displaying the results of the game being played. The player becomes part of the game as if he or she were actually present at the gaming table in the casino. To provide a secure communications link, the remote gaming station communicates with the croupier station and a credit control station through an encryption/decryption device to prevent tampering by unauthorized sources.

While such a system provides a means by which a player can gamble from a remote location, its primary disadvantage resides in the fact that the player can gamble only by participating in games being actually conducted in the gaming establishment and monitored over real-time closed circuit video. Moreover, such a system has limited practicality since the player can only gamble on a specialized gaming station which must be electronically linked to the casino. It would therefore be highly desirable to provide a remote gaming system by which a player could engage in gambling on a gaming computer at a remote location at the player's convenience where the casino provides for the purchase and redemption of casino credit, notwithstanding the absence of any direct electronic communication link between the gaming computer and the casino.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide a remote gaming system by which the player can wager on any one of a plurality of games of chance typically offered by a wagering establishment (e.g., a casino or whatever entity is offering to bet against the player) at the player's convenience.

It is another object of the present invention to provide a remote gaming system by which the player can wager against the wagering establishment on any one of a plurality of wagering opportunities such as games of chance generated by computer software installed or loaded on any personal computer.

It is a further object of the invention to provide a remote gaming system by which a player can wager against the wagering establishment on a conventional multi-media apparatus (e.g., a NINTENDO apparatus coupled to a television set) through compatible plug-in data storage media.

It is yet another object of the invention to provide a remote gaming system by which a player can purchase and redeem wagering credit from remote locations without the need for an on-line electronic communications link to be established between the player's gaming computer and the wagering establishment,

It is still another object of the invention to provide a remote gaming system by which a player can wager on any one of a plurality of games of chance generated by software installed or loaded on a dedicated gaming computer, including a hand-held portable device, which can be provided to the player, yet need not be electronically linked on-line to the wagering establishment for purposes of gambling, purchasing and redeeming gambling credit.

It is yet another object of the invention to provide a remote gaming system wherein authenticatable messages communicated between, read and authenticated by a remote gaming computer, including a dedicated machine for wagering, a general-purpose game machine, a personal computer or personal digital assistant (PDA), or any other device for computing and communicating with the house or wagering establishment, and a host computer associated with the wagering establishment, either on-line (including wireless electronic communication hardware) or off-line (orally with an agent or electronic communications over the telephone, but where no connection is necessary between the gaming computer and the wagering establishment), prevent unauthorized users from gaining access to or fraudulently obtaining or redeeming gambling credit.

It is another object of the present invention to provide a remote gaming system in which a gaming computer and/or host computer associated with the wagering establishment restricts access to wagering opportunities by means of hardware or software for authenticating a personal identification number (PIN) or passphrase.

It is still another object of the present invention to provide a remote gaming system in which a gaming computer and/or host computer associated with the wagering establishment restricts access to wagering opportunities, using authentication from some external credit card, smart card, funds transfer system, digital cash system, or other payment system.

It is yet another object of the invention to provide a remote gaming system in which a gaming computer and/or host computer associated with the wagering establishment restricts access to wagering opportunities utilizing biometrics including, but not limited to, fingerprints, voiceprints, retinal-prints and the like.

It is still another object of the invention to provide a remote gaming system in which a gaming computer and/or host computer associated with the wagering establishment restricts access to wagering opportunities using a physical access token or physical key.

It is a further object of the invention to provide a remote gaming system in which a gaming computer and/or a host computer associated with the wagering establishment restricts access to wagering opportunities using authorization transferred from a remote system, whether or not that system is working as and agent or provider of the wagering opportunities.

It is another object of the invention to provide a remote gaming system in which a gaming computer and/or host computer associated with the wagering establishment, in addition to or in lieu of other security measures, restricts access to wagering opportunities by consulting an internal or external database having stored lists of banned and/or valid identification codes, including but not limited to EFT account numbers, userIDs, credit card account numbers, and the like.

It is a further object of the present invention to provide a remote gaming system which is made secure by incorporating cryptographic protocols or methods such as digital signatures, one-way hashes, zero-knowledge proofs, encryption, message-authentication codes, bit-commitment protocols and the like

It is a further object of the present invention to provide a remote gaming system which is made secure by utilizing internal checksums and audit sums.

It is another object of the invention to provide a remote gaming system which is made secure by using hardened "agents" of the "house", i.e., the wagering establishment, in the form of software and/or hardware devices, humans, or any or all of these, in a remote or nearby location, or installed in or on a remote gaming computer.

It is still another object of the invention to provide a remote gaming system which is made secure by utilizing digital time stamping to generate authenticatable messages to be read and authenticated by a host computer associated with the wagering establishment for verification.

It is a further object of the invention to provide a remote gaming system which is made secure by incorporating secure timers, counters, running hashes or checksums, digital signatures, or other hidden values to frustrate attempts to defraud or tamper with the gaming software of data storage media associated with the gaming computer.

It is yet another object of the invention to provide a remote gaming system which is made secure by employing batch communications between the gaming computer and the wagering establishment.

It is still another object of the invention to provide a remote gaming system in which a player receives a tamper-resistant or tamper-evident read/write device from the wagering establishment containing data storage media for dedicated gaming software which can be linked to or installed on any personal computer, yet is inspectable by the wagering establishment to prevent unauthorized manipulation of, or alteration to, the software.

It is still another object of the invention to provide a remote gaming system in which the gaming and/or banking software is embodied in data storage media such as, for example, a computer disk, where the unique magnetic signature of that disk is readable by the gaming computer as an authenticatable message for authentication by the gaming computer and/or the wagering establishment host computer to make unauthorized duplication of the disk or alteration to data on the disk detectable by the wagering establishment.

It is still another object of the invention to provide a remote gaming system by which a player can wager on future public or external events of which the outcome is uncertain such as a lottery, either through an on-line connection between a gaming computer and the wagering establishment, or off-line where the player's wager is time-stamped to generate an authenticatable message, representing the player's choice of wagering elements (i.e., numbers) for a given lottery event (occurring at some time in the future) and, including, at least one of a date/time stamp or authenticated time message, player's identification code, and computer/software identification code.

It is yet another object of the invention to provide a remote gaming system by which a player can obtain and redeem wagering credit from the wagering establishment embodied in tamper-resistant or tamper-evident data memory media which interface with a remote gaming computer.

It is still another object of the invention to provide a remote gaming system by which a completely self-contained, dedicated gambling personal digital assistant may be obtained with a preprogrammed and/or predetermined amount of non-renewable credit embodied in gaming software installed on or loadable into the digital assistant.

It is a further object of the invention to provide a remote gaming system by which a player can engage in a game of skill (e.g., a crossword puzzle) residing in software installed on a dedicated gambling personal digital assistant having a preprogrammed and/or predetermined amount of non-renewable gambling credit.

It is yet another object of the invention to provide a remote gaming system in which winnings and collection on losses may be authorized by means of a digital cash protocol.

It is a further object of the invention to provide a remote gaming system in which payment of winnings and collection on losses is authorized by means of an electronic funds transfer mechanism.

It is still another object of the invention to provide a remote gaming system in which payment of winnings and collection on losses is authorized by means of a credit card authorization mechanism.

It is yet another object of the invention to provide a remote gaming system in which payment of winnings and collection on losses is authorized through the wagering establishment or its agents through communication between a remote gaming computer and a host computer associated with the wagering establishment.

It is still another object of the invention to provide a remote gaming system in which winnings and collection on losses are paid directly in currency form.

It is a further object of the invention to provide a remote gaming system in which all gambling credit is loaded into a gaming computer by the wagering establishment or its agent(s) prior to providing the player with the gaming computer.

It is still another object of the invention to provide a remote gaming system in which a premium application enables a player who purchases a product such as a computer, or software on data storage media, to win something as determined by the output of a gaming program embedded within such product.

It is yet another object of the invention to provide a remote gaming system by which a player wagering at a remote location is subject to predetermined limitations on winnings by a wagering establishment.

In accordance with the above objects and other objects which will become apparent hereinafter, the present invention provides a remote gaming system which enables a player to gamble against a wagering establishment using a gaming computer at a remote location. The gaming computer may or may not be electronically linked, i.e., "on-line", to a host computer associated with the wagering establishment while gambling takes place. The term "wagering establishment" as used herein is intended to include authorized agents or other parties which act on behalf of the wagering establishment to implement the gaming process. The term "host computer" includes a single device, multiple devices and/or computer networks and systems. The gaming computer can be any personal computer, hand-held computer device (e.g., a personal digital assistant), or multi-media apparatus which functions as the gaming computer (e.g., a NINTENDO or like apparatus), and may or may not be a dedicated gambling computer provided by the wagering establishment. If provided by the wagering establishment, the gaming computer can be preloaded with gaming software. If the gaming computer is a conventional personal computer, the gaming software is either preinstalled on a secure data storage media device, e.g. a hard disk, CD-ROM, etc., or module provided by the wagering establishment, or installed directly on the gaming computer by the player.

The gaming software includes a game program and a banking program. The game program generates a plurality of games of chance typically offered by the wagering establishment, e.g., blackjack, roulette, craps, poker, slots, etc., games of skill or makes available wagering on external events or future public events of which the outcome is uncertain, e.g., a lottery. The banking program provides for the purchase or loading of gambling credit into a banking file from the wagering establishment to enable gambling, and increments or decrements the player's account balance to enable the player to cash-out any gambling winnings. The term "gambling credit" as used herein, means purchased credit, accumulated gambling winnings, collection on losses and the like. The gaming software may also include an audit program which records the outcome of each wager and the data communicated between the player and the wagering establishment as read, authenticated and /or generated by the gaming computer in order to effect gambling, and the purchase and redemption of gambling credit.

The wagering establishment has a host computer with software containing a banking program which enables players to purchase, accumulate and redeem gambling credit at remote locations, even if no on-line communications exist with the gaming computer, and an audit program for recording such transactions. This may be accomplished, in one preferred embodiment of the invention, by communicating a plurality of authenticatable messages between the gaming computer and the host computer, which messages are respectively read and authenticated by each device, either through oral communications between the player and the wagering establishment, e.g., such as via an automated public telephone network having interactive voice capabilities using a touch-tone phone. The words "authenticatable", and "authenticate" as disclosed and claimed herein include cryptographic protocols such as encryption and decryption, digital signatures, one-way hashes, checksums and the like. The utilization of authenticatable messages is one way to prevent a third party or a verified player from gaining unauthorized access to the system and then attempting to fraudulently obtain or redeem gambling credit and/or tamper with the game program to produce altered wagering opportunities having only a favorable outcome. Alternatively, gambling credit can be "built-in" or preinstalled on a tamper-evident or tamper-resistant module for installation on a conventional personal computer, or pre-installed on a dedicated gaming computer provided by the wagering establishment. In the off-line embodiment, the automated public telephone network or "agent" is associated with the host computer of the wagering establishment, but it is not necessary to have a direct electronic on-line connection between the gaming computer and the host computer.

If the gaming computer is networked to the host computer, the connection may or may not serve to regulate or control the simulation of casino games on the gaming computer by the gaming software. For example, the connection may serve to have the host computer keep a record or audit-trail of all or selected activities taking place at the gaming computer for purposes of additional verification or security. Alternatively, the connection may be of a controlled nature to vary the odds of a given wager based upon any of a variety of factors such as gambling duration or a progressively increasing jackpot (e.g., in a slot machine simulation). In such an on-line embodiment, security and player verification can be obtained by utilizing a stand-alone secure message generation and authentication device, such as, for example, an encryption/decryption unit of the type commonly employed in making wireless money transfers. This device generates an authenticatable verification code based upon the user's personal identification code and possibly a second code provided to the user from the host computer or stored in the stand-alone authentication device to prevent an unauthorized user from obtaining on-line access upon having stolen a user's personal identification code.

At all times, each wager by the player generates an electronic audit-trail on the gaming computer, the host computer and/or on any networked computers by recording the amount of each wager, the outcome of each gambling event and any resulting gambling earnings or losses, in an authenticatable message or a series of messages which are read and authenticated by the host computer and/or the gaming computer. The financial resolution of each wager is cumulatively tracked by the software on the gaming computer and perhaps also on any networked computers, so that the player is able to constantly monitor his or her gambling credit balance with the wagering establishment.

A player gambles in substantially the same way he or she does in a casino. The player chooses which games to play as presented by the gaming software, the amount of each wager and the length of time each game is played. The player may remain active over several different gaming sessions which may take place at several different times and/or places. The player may at any time place wagers which are for practice only which do not affect the player's gambling credit balance. As an option, the player's gambling credit balance may be transferred and stored on data storage media which can be installed on other computers where software has been, or can be, installed to recognize the player's gambling credit balance. The player may then continue to wager on any of such other computers. Whenever the player wishes to cash-out his or her gambling credit, redemption from the wagering establishment may be implemented by contacting the wagering establishment by telephone in an "off-line" embodiment, either through an automated telephone network with voice capabilities, or a live agent, or by communicating on-line in an "on-line" embodiment.

In one embodiment described above, when the player desires to cash out, a series of authenticatable messages are exchanged with the host computer, such as orally through an automated telephone network, or are transmitted electronically on-line by conventional means in the on-line embodiment. In the off-line embodiment, these authenticatable messages are generated by the gaming computer software and the host computer software, and communicated between and read by the gaming computer and host computer for authentication to verify the player's identity and authenticity of the player's gambling credit account prior to cashing-out gambling credit. In the on-line embodiment, a stand-alone device or software associated with the gaming computer generates an authenticatable log-on or confirmation message for verification by the host computer. Alternatively, where the gaming computer itself, e.g., a personal digital assistant, is provided to the player by the wagering establishment, it or a tamper-resistant or tamper-evident plug-in module may be physically returned to the wagering establishment for credit redemption. The module includes data-storage media preferably disposed in an inspectable tamper-resistant or tamper-evident casing which can be examined by the wagering establishment for any indication of tampering. Such gambling credit can be redeemed from the wagering establishment in any of a variety of forms of payment including, but not limited to, cash, bank-wire transfers, credits or some other form of payment mutually agreed to by the player and the wagering establishment.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A is a schematic view of the remote gaming system in a first off-line embodiment;

FIG. 1B is a schematic view of the remote gaming system in a second off-line embodiment;

FIG. 1C is a schematic view of the remote gaming system in a third off-line embodiment;

FIG. 2 is a schematic view of the remote gaming system in an on-line embodiment;

FIG. 3 is a schematic view of a gaming computer connected to a tamper-resistant or tamper-evident read/write data storage media device provided by the wagering establishment;

FIG. 4 is a flowchart of the start-up and registration sequence in the off-line embodiment;

FIG. 5 is a flowchart of the handshake recognition sequence in the off-line embodiment;

FIG. 6 is a flowchart of the purchase credit sequence in the off-line embodiment;

FIG. 7A is a flowchart of the wagering sequence for games of chance generated by the game program in the off-line embodiment;

FIG. 7B-1-2 is a flowchart of the wagering sequence for an off-line non-registered lottery system embodiment;

FIG. 7C-1-5 is a flowchart of the wagering sequence in an off-line registered lottery system embodiment;

FIG. 8 is a flowchart of the credit cash-out sequence in the off-line embodiment;

FIG. 9 is a flowchart of the registration and start-up sequence in the on-line embodiment;

FIG. 10 is the purchase credit sequence in the on-line embodiment;

FIG. 11 is a flowchart of the wagering sequence in the on-line embodiment;

FIG. 12 is a flowchart of the credit cash-out sequence in the on-line embodiment;

FIG. 13 is a schematic of a memory chip made secure by an external tamper-resistant or tamper-evident structure;

FIG. 14 is a schematic of a first means for verifying the integrity of the gaming software;

FIG. 15A is a schematic of a second means for verifying the integrity of the gaming software;

FIG. 15B is a schematic of a third means for verifying the integrity of the gaming software;

FIG. 15C is a schematic of a fourth means for verifying the integrity of the gaming software; and

FIG. 15D is a schematic of a fifth means for verifying the integrity of the gaming software.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference to the several views of the drawings, there is depicted a remote gaming system generally characterized by the reference numeral 10 by which a player 12 with access to a computer 14 ("the gaming computer") wagers on a plurality of games of chance, or on future public events where the outcome of such events is uncertain, offered by a casino, government lottery organization or other wagering establishment 16. For convenience, these and any authorized agent thereof will be generally referred to hereinafter as "the wagering establishment."

Referring now to FIG. 1A, the player 12 has access to gaming computer 14 having a video display 18 and a keyboard 20. The gaming computer 14 can be a personal home computer, lap-top, or hand-held personal digital assistant device, which may or may not be a dedicated gaming apparatus provided by wagering establishment 16, or may be a multi-media apparatus, e.g., a NINTENDO or similar device for use with a television or the like. The gaming computer 14 can be located at the wagering establishment 16 or some other establishment, e.g., a lottery ticket vendor, or off-site at a remote location. A gaming computer 14 which is located at the wagering establishment 16 can still be classified as "remote" in the context of the invention claimed herein. In this regard, it is anticipated that a casino could provide players, in for example the hotel where the casino is located, with a dedicated gaming computer 14 which could be used to gamble either within or outside of the physical boundaries of the casino. A primary advantage of providing the player 12 with a wagering establishment-furnished gaming computer 14 is greater security, specifically with regard to making unauthorized access to the data storage media such as a computer disk drive or module more difficult. Moreover, in a dedicated gaming computer, the keyboard 20 can be customized with specialized function keys identifying commands, e.g., keys dedicated to blackjack might have indicia stating "hit me", "stand", "purchase insurance", etc., which the player selects to proceed to gamble on the various games of chance, games of skill or future events of which the outcome is uncertain, offered by the wagering establishment 16. Gaming computer 14 operates special gaming software 22 comprised of a game program 24, a banking program 26 and optionally, an audit program 27. Gaming software 22 can be preinstalled on a dedicated gaming computer 14 provided by the wagering establishment 16, preinstalled in an external tamper-resistant or tamper-evident read/write data storage media apparatus 28 provided by wagering establishment 16 which interfaces with a personal computer functioning as the gaming computer 14 as shown in FIG. 3, or installed directly on the personal computer by the player 12. Furthermore, the gaming software 22 may be made available to the player 12 in a tamper-resistant or tamper-evident plug-in module for use with a conventional personal computer or multi-media apparatus which functions as the gaming computer 14, to be described in more detail hereinbelow.

It is critical that the wagering establishment 16 be able to determine if the software itself or data associated therewith was copied, tampered with or in any way altered, otherwise an unscrupulous player 12 could make a plurality of copies and keep playing with identical disks until such time that one of the copied disks produced a favorable outcome, or the player 12 could alter the software itself in an attempt to control the outcome, the winnings or losses, or a combination thereof, i.e., a dishonest player 12 modifies the software code of the gaming software 22 in such a way as to make the software generate a winning outcome more frequently than chance would dictate (e.g., in a roulette simulation, causing the roulette wheel to land on a more favorable number more frequently). This could be achieved by replacing the software in its entirety or by modifying certain code lines or software instructions of the program, either physically or by some other externally applied influence such as high-intensity electromagnetic radiation, e.g., an RF field. Of course, the most secure system is an on-line arrangement where the gaming software 74 resides in a host computer 30 associated with and/or on the premises of the wagering establishment (FIG. 2). The most difficult security issues with regard to tampering arise in embodiments where the wagering establishment 16 provides the player 12 with software for use on a remotely disposed gaming computer 14 or with a dedicated gaming computer 14 itself (e.g., a PDA). In this connection, the present invention provides a variety of means for ensuring that system security and integrity are not compromised.

In one application, software can be provided which instructs the gaming computer 14 to read the unique magnetic characteristics, i.e., "fingerprint," of the specific disk or data storage media on which gaming software 22 is made available for installation, for the purpose of creating a unique authenticatable message to be read and authenticated by the wagering establishment 16 to reveal to the wagering establishment 16 any unauthorized duplication of, or tampering with, data on that disk or data storage media. Alternatively, a plug-in device can interface with the gaming computer disk drive to read a portion of the disk to acquire the unique magnetic characteristics of the disk, or the wagering establishment 16 can utilize the same hardware and/or software to obtain this magnetic signature and keep this information on file for use at some future time should tampering be suspected, or as a prerequisite to authorizing any gambling functions to a specific player 12, e.g., this data can be registered with or required by the wagering establishment 16 prior to allowing the player 12 to cash-out any gambling winnings.

In another embodiment shown schematically in FIG. 13, the gaming software 22 resides on a tamper-resistant or tamper-evident chip 23 disposed within or otherwise associated with the gaming computer 14, i.e., where a dedicated device is provided by the wagering establishment 16, or otherwise connected to the gaming computer 14, e.g., a secure, external disk drive connected to a conventional personal computer. The chip 23 can be situated within a physical casing 84 which is isolated and unaccessible from any external data port connection. In an exemplary embodiment, the chip 23 can be housed within special seals, insulation, wrapping, or the like 86, which can be inspected by the wagering establishment 16 to reveal whether any authorized attempts were made to remove, alter or otherwise tamper with the chip 23. Thus, the wagering establishment 16 can readily ascertain if the player tampered with the gaming software and, if such tampering is discovered, it can deny such player any claimed winnings and/or future gambling credit.

In yet another embodiment shown schematically in FIG. 14, unique mathematical attributes can be derived from certain characteristics of the software code in a self-test process.. To perform such a test, the characteristics of the code are kept secret and are known only to the wagering establishment 16 by using checksums, one-way hashes and other cryptographic protocols, including, for example, a check-digit type algorithm based upon the sum of the bits located in certain parts of the program, for example, lines 476 through 655 of the code as shown. Alternatively, the self-test can verify special codes which are embedded within the software or code instructions in some predetermined random manner known only to the wagering establishment 16.

In a variation of the above shown schematically in FIG. 15A, external keys known only to the wagering establishment 16 can be applied to intermittently or continuously verify whether the software code has been or is being tampered with, by causing altered software to malfunction and shut down the gaming application in the computer 14. The use of external keys may or may not employ cryptographic protocols such as encryption to safeguard against their being somehow forged by the player 12. This can be implemented in several ways, including, but not limited to: (1) broadcasting a continuous or intermittent authenticatable message, such as an encoded or encrypted external signal, e.g., RF, from the wagering establishment 16, which is received by receiving means 88 operably associated with the gaming computer 14, where such signals are subsequently authenticated by the gaming computer 14, converted into the appropriate form and used by the gaming software 22 to verify or enable the same (FIG. 15B); (2) having the player 12 physically enter a message on an intermittent basis (FIG. 15C); or (3) utilizing an internally generated clock signal furnished by a hardened, tamper-resistant or tamper-evident clock 89 (FIG. 15D). In this connection, the chip 23, or even the gaming computer 14 (if provided by the wagering establishment 16), may be shielded from electromagnetic interference (EMI) by conventional methods to prevent unauthorized attempts to influence the gaming software with externally generated electromagnetic radiation.

Aside from the use of external keys, the gaming software 22 can be made to require the acquisition of data from an external source in order to function. For example, a wireless broadcast of an authenticatable message comprised of random numbers and/or alphanumeric data (possibly encrypted) might be accessed by the gaming software 22 such that these random numbers are called upon by the program as a basis to select and/or generate a wagering outcome in a predictable or unpredictable manner. Such external input may be incorporated into a hardened, tamper-resistant or tamper-evident plug-in device or module, which interfaces with the gaming computer 14.

Another way to prevent fraudulent attempts to alter the gaming software 22, is through the use of an audit program 27 which can only be accessed by the wagering establishment 16. To prevent a forged audit trail, the audit program 37 might, by way of example, create dozens or even hundreds of data strings (e.g., such as in a roulette simulation, data strings corresponding to spins of the roulette wheel each time the wheel is spun), where all such data is then recorded for future verification should the wagering establishment 16 suspect tampering with the gaming software 22.

It will be appreciated by persons skilled in the art that the gaming software 22 can be arranged such that a message or data-string of alphanumeric codes, which are either preloaded into each gaming computer 14, or provided on a disk or plug-in uncopyable module, can be used to discover any tampering with the software, disk or module by the player 12. In this connection, the code sequence can be made different for each gaming computer 14 or module, and copies of such codes can be kept on file by the wagering establishment 16. These codes may be used to provide the basis for generating a random outcome of each gaming event, and can thereby provide evidence of tampering. In other words, a specific arrangement of codes might correspond to a certain outcome of a wagering event (e.g., the Roulette wheel lands on "5"). Even though these codes are known to the wagering establishment 16, they are sequenced to ensure a random outcome - something which could be verified by an independent third party. If a player 12 seeks to modify the gaming software, the altered software instructions and/or codes could be discovered upon comparison of the same with the originals on file with, and known only to, the wagering establishment 16.

As another means of preventing player fraud, an element of "double-randomness" can be implemented by requiring the player 12 to press a button for each selection or desired response on the gaming computer 14 twice, with the time interval between selections (i.e., in milliseconds) used to address and enable a specific preprogrammed random outcome codified in corresponding software codes.

The game program 24 permits player 12 to wager on any one of a plurality of wagering opportunities, including games of chance, future public or external events where the outcome is uncertain or games of skill, e.g., a crossword puzzle. The games of chance are generated on gaming computer 14 by game program 24 in accordance with conventional techniques and include, but are not limited to, common casino wagering activities such as blackjack, craps, roulette, poker, slots and the like. Each game offers opportunities for the player 12 to place wagers on one or more various wagering elements within a given wagering event depending upon the rules applicable to that game. This will be described in more detail below.

Game program 24 can be made to accept wagers on future public or external events where the outcomes of such events are uncertain as in, for example, sporting events such as a football game or a boxing match, or a state-run or other lottery. This can be implemented by establishing communications, either orally via a public telephone network, or electronically, with the wagering establishment 16 in order to place, register and confirm bets. The wager is placed on the gaming computer 14, which, through the gaming software 22 produces a message for registration with the wagering establishment 16. This message is then time stamped by the wagering establishment 16 to form an authenticatable message, which authenticatable message can only be authenticated by the wagering establishment 16, using appropriate software instructions or hardware to lock in the bet or fix the time of the wager for the purpose of ascertaining the proper payoff. This implementation will be described in detail below. Similarly, games of skill such as a crossword puzzle can be verified through the use of an authenticated date/time message which fixes the time of completion of the game, such that prizes are later awarded based upon the first player to complete that game.

The banking program 26 enables the player 12 to wager with available gambling credit and "cash-out" any gambling winnings. In certain embodiments, the banking program 26 facilitates the purchase of credit from the wagering establishment 16 where such credit is "loaded" into an appropriate datafile in the gaming computer in the form of an authenticatable message or a series of authenticatable messages. Alternatively, as shown in FIG. 1C, the banking program can receive gambling credit electronically, such as from an electronic card reader 91 compatible with credit or debit cards 93 in a conventional manner, or by downloading the credit from a plug-in tamper resistant or tamper-evident credit module 90.

As one way of ensuring security in the credit purchase/redemption process, the banking program 26 or a dedicated authentication device provides for the authentication and generation of authenticatable messages, such as, for example, an encryption/decryption apparatus utilizing an encryption and decryption algorithm of the type known in the art, e.g., public-key, to encrypt and decrypt alphanumeric messages exchanged between the player 12 and the wagering establishment 16 which are input to, communicated between and generated by the gaming computer 14 and the host computer 30. These messages can be communicated between the player 12 and the wagering establishment 16, including its authorized "agent" 38 through a public telephone network 40. The term "agent" is intended to include an automated telephone or like system having interactive voice capabilities, which generates computerized instructions communicated to the player 12 over the phone to prompt the player 12 to communicate responses to the wagering establishment 16 by pressing the appropriate numbers or symbols on the touch-tone phone 36 by conventional methods which are well known.

The host computer 30 has gaming software 33 operably associated therewith, which software includes a banking program 35 and an audit program 37. The host computer 30 either includes or communicates with a dedicated device or software 39 for generating and authenticating authenticatable messages using cryptographic protocols with keys or secret algorithms known only to the wagering establishment 16. In this manner, the wagering establishment 16 enables a verified player 12 to purchase and redeem gambling credit at the remote location, notwithstanding the absence of any on-line link to the wagering establishment 16 and/or the host computer 30 associated with the wagering establishment 16. The sequence of steps in the illustrative embodiment required to purchase and cash-out gambling credit by exchanging and authenticating authenticatable messages off-line are described in greater detail below.

In the usual course of practicing the invention, FIG. 4 depicts a flowchart of a representative start-up and registration sequence in an off-line embodiment which must occur prior to wagering. Player 12 first registers various personal information with the wagering establishment 16 and obtains an alphanumeric personal identification message or code 32. The wagering establishment 16 provides player 12 with gaming software 22 containing a game program 24, a banking program 26, and an audit program 27 as described above, having an associated software identification message or code 34. The gaming software 22 may be independently tested, verified and provided on data storage media in a sealed envelope by a third party. Such data storage media can include a hard disk, floppy disk, CD-ROM and the like. The wagering establishment 16 then provides an alphanumeric start-up identification message or code 33 which the player 12 enters into the gaming computer to run the gaming software 22. Optionally, the gaming computer 14 may utilize biometrics including, but not limited to, fingerprints, voiceprints, retinal-prints and the like, using an appropriate chip or recognition software, to deny access to any unauthorized user. Such hardware and/or software is known in the art.

The gaming software 22 is programmed to prompt the player 12 with an inquiry as to whether a current session is for practice or to place a wager. If it is a practice session, the game program 24 generates a plurality of game choices and a confirmation that the games are being played for practice only. If the player 12 chooses to engage in gambling, the banking program 26 will permit actual wagering to the extent that there is sufficient gambling credit available in the player's account to cover all bets. If there is insufficient gambling credit, the player 12 must contact the wagering establishment 16 and go through the purchase credit sequence described below. As noted above, the gaming computer 14 may or may not be on-line with the wagering establishment computer 30. If gaming computer 14 is off-line, greater flexibility in terms of being able to engage in gambling at virtually any location is possible. As discussed above, a series of authenticatable messages are communicated between the player 12 and the wagering establishment 16 permit credit purchase and redemption at a remote location to be governed by the wagering establishment 16 notwithstanding the absence of an on-line link between the gaming computer 14 and the host computer 30. Alternatively, gaming computer 14 can be networked on-line to the host computer 30 through a public telephone network 29 such that host computer 30 monitors and controls all or part of the activities taking place on the remote gaming computer 14 (see FIG. 2).

In the off-line embodiment shown in FIG. 1, the player 12 places a call to the wagering establishment 16 by way of telephone 36 and communicates via the public telephone network 40 to obtain or redeem gambling credit. If player 12 already has credit, gaming software 22 will permit wagering on any of the games of chance, future or external events or games of skill, provided by game program 24 upon receiving player 12's appropriate personal identification message 32. If player 12 requires credit to play, the wagering establishment 16 must be contacted and the following series of steps are followed for the purpose of verifying the player's identity and confirming that the player is utilizing gaming software 22 registered to his or her personal identification message 32.

Whenever player 12 contacts the wagering establishment 16, he or she goes through what is referred to as a handshake recognition sequence, the verification of the player's identity with the wagering establishment 16. In this regard, as depicted in the flowchart of FIG. 5, player 12 first calls the wagering establishment 16 on telephone 36. The wagering establishment 16 queries player 12 for his or her unique personal identification message 32 and software identification message 34. These are provided to the wagering establishment 16, and are read by and authenticated by the host computer 30, which in turn generates an authenticatable handshake message 42 which is provided to player 12 for entry into gaming computer 14. Gaming computer 14 reads and authenticates handshake message 42 and then generates an authenticatable recognition response message 44 which is provided to the wagering establishment 16. The host computer 30 reads and authenticates recognition response message 44 to verify the player 12's identity and to confirm that the specific gaming software 22 is registered to that player 12. The verified player 12 then proceeds with appropriate interaction by the wagering establishment 16.

FIG. 6 is a flowchart depicting a first embodiment of a purchase credit sequence in the off-line embodiment. Player 12 first contacts the wagering establishment 16 and establishes his or her identification through the handshake sequence depicted in FIG. 5 and described above. The host computer 30 generates an authenticatable banking program activation message 46, and the wagering establishment 16 provides the activation message 46 to the player 12 for the purpose of allowing player 12 to access the credit purchasing/redemption function of the banking program 26 in gaming computer 14. Player 12 then enters the amount of gambling credit requested, and the authentication software 29 combines the personal identification message 32 and software identification message 34 to generate an authenticatable credit request message 48, which embodies the numeric value of the amount of gambling credit requested and is unique to player 12 and his or her gaming software 22. The player 12 communicates the credit request message 48 to the wagering establishment 16, where the host computer 30 reads and authenticates the credit request message 48 to reveal the amount of credit requested by the player 12. The amount of gambling credit requested is confirmed with the player 12. The wagering establishment 16 then decides whether or not to provide all or part of the gambling credit requested. If the credit request is denied, player 12 is given an authenticatable reactivation message 50 which is read and authenticated by gaming computer 14 to enable player 12 to continue wagering with any available gambling credit balance. Alternatively, the player 12 has the option to cash-out any gambling winnings in accordance with the sequence depicted in FIG. 8 and described below. If the credit request is partially or fully granted, the process continues for the amount of gambling credit the wagering establishment 16 is willing to sell to the player 12. The host computer 30 generates an authenticatable new credit message 52 which is provided to player 12 for the purposes of loading a pending amount of credit requested into the player's gaming computer 14 via the banking program 26 of the gambling software 22. The gaming computer 14 reads and authenticates the new credit message 52 and displays the exact amount of new credit added to player 12's available gambling credit balance. The amount of new gambling credit is shown to player 12 as pending, but is not yet available for use. Banking program 26 then instructs authentication software 29 to generate an authenticatable credit pending message 54 which is based in part on the monetary value of the new credits pending. The player 12 communicates this credit pending message 54 to the wagering establishment 16 where it is read and authenticated by the host computer 30 to positively and irrefutably verify that the specific amount of gambling credit requested was properly loaded into player 12's banking program 26. The host computer 30 then generates an authenticatable credit release message 56. This credit release message 56 is provided to the player 12, and then read and authenticated by the gaming computer 14 to release the amount of pending gambling credit in banking program 26. The gaming computer generates an authenticatable credit release verification message 58 which the player 12 provides to the wagering establishment 16. The host computer 30 then reads and authenticates the credit release verification message 58 and in turn generates an authenticatable program reactivation message 60. The reactivation message 58 is communicated to the player 12, and thereafter read and authenticated by the gaming computer 14 to enable the game program 24. Simultaneously or subsequently, the wagering establishment 16 charges the player 12 for the value of gambling credit purchased in a manner mutually agreed upon by the player and the wagering establishment 16. For example, a credit card may be charged, a bank transfer authorized, or some other form of payment or delayed payment may be made to the casino in exchange for the credits purchased. If at any point during this process one or more of the various authenticatable messages do not match those expected by the respective authentication software and/or hardware associated with the gaming computer 14 and the host computer 30, the player 12 is denied access to the banking program and associated gambling credit, and the gaming software 22 in such cases is disabled until the dispute is resolved. In this manner, the correct generation and authentication of each of the various messages communicated between the gaming computer 14 and the host computer 30 positively confirms the amount, value and authenticity of gambling credit obtained by or made available to the player 12.

It will be appreciated that gambling credit can also be furnished to the player 12 in predetermined amounts and/or preinstalled on a dedicated gaming computer 14, e.g., a personal digital assistant, provided by the wagering establishment 16. Alternatively, the player 12 can obtain a disk or module 90 having a specified amount of authorized credit which is then "loaded" into the banking program 26 associated with the gaming computer 14 to enable wagering to the extent of the available gambling credit balance. Alternatively, as shown in FIG. 1C, the player 12 can obtain gambling credit using his or her own credit card 93, either through oral or electronic communications with the wagering establishment 16, or via an electronic card-reader apparatus 91 connected to the credit card issuing bank 95 in the conventional manner.

Once the player 12 has obtained gambling credit, he or she may place wagers by selecting wagering elements within various wagering events in any one of a plurality of games of chance offered by the game program 24 of gaming software 22. Each game provides opportunities for player 12 to place wagers on one or more various wagering elements within a given wagering event depending upon the rules applicable to that game. As an example, the casino game of roulette involves a series of wagering events based upon the outcome of a random number selected by a ball spun within a roulette wheel. Each spin of the wheel is a single wagering event. Within that event, the player 12 may bet on many different wagering elements such as red and black colors, single numbers, groups of numbers and the like. All wagers for each event are placed prior to the spin of the wheel.

FIG. 7A is a flowchart depicting the wagering sequence for games of chance created by the game program 24 which proceeds as follows. The player 12 first makes the appropriate selections on the gaming computer 14 to enter the game program 24 of the gaming software 22, and then chooses a particular game on which to wager. The player 12 can wager on one or more events within the game as described above. The game program 24 prompts the player 12 to confirm the placement of wagers made and the total amounts of wagers entered. Such wagers may be withdrawn or modified until such time as they are confirmed. Confirmation is typically made by having the player 12 enter a confirmation message 62 prior to closing of all bets. The confirmation message 62 is generated by the gaming software 24, and can be made different for every wager for security reasons. It can be a simple one or two digit alphanumeric message which is read and used by the game program 24 to confirm that each bet placed for any wagering event was, in fact, what was intended by the player 12 and not placed in error. The game program 24 can be set up such that the confirmation message 62 may be simplified further to a single key stroke in certain highly repetitive games such as, for example, slots, or when the total value of all wagers falls below a certain predetermined level. After confirmation message 62 has been entered by player 12, the game program 24, in accordance with the rules of a given casino game, generates a specific outcome for a given wagerable event (e.g., cards are dealt, the wheel is spun, etc.). The game program 24 determines the outcome of each wager placed (win, lose or draw), calculates and then displays the proposed correct payoff for that wager on the gaming computer 14. The player 12 has the option to type in a yes/no message to accept the payoff outcome of all wagers or to dispute any payoff which the player 12 believes to be incorrect in some fashion. Any dispute can be handled by suspending the wagering process and calling the wagering authority 16 to resolve the matter by telephone or by some other means of dispute resolution. Once the player 12 accepts the resolution of a given wagering event, the correct amount of gambling credit is added or subtracted from player 12's gambling credit balance by the banking program 26. Player 12 can then begin the wagering process all over again on a subsequent wagering event, or choose to end the gambling session. At any time, the player 12 may select a review mode in the game program 24, and can review the amount and resolution of each and every wager made by the player 12 and the results of such wagers in chronological order. At any time, the player 12 can choose to redeem or cash-out all or part of the balance of gambling credit stored in banking program 26 through a credit cash-out sequence. If desired, the game program 24 may contain special built-in instructions to place limitations on winnings at the discretion of the wagering establishment. It is also anticipated that such gaming software 22 could be embedded in another product, such as in a computer or other software, to provide a premium application which enables the purchaser of unrelated products to win something as governed by such an embedded program (e.g., a cash prize awarded).

FIGS. 7B-7C are flowcharts of wagering sequences for future public events of which the outcome is uncertain, such as a lottery, in the off-line embodiment. With regard to the following discussion and appended claims with respect to lotteries, the wagering establishment will be hereinafter identified as a "lottery authority" for clarity. To participate in a lottery, the player 12 selects a particular lottery event, i.e., a drawing, generated by the game program 24 on which to wager. The gaming computer 14 then generates a lottery "ticket" layout unique to the specific lottery and the player selects the desired wagering elements (i.e., numbers).

There are two types of exemplary lotteries described herein, the first classified as an instant type analogous to common scratch-off tickets, and the second characterized as future or external events of which the outcome is uncertain, i.e., a drawing takes place. It will be appreciated by the persons skilled in the art that a remote gaming arrangement whereby the player 12 participates in a lottery can be classified as either: (1) a non-registration system (by which the player wagers independently of the lottery authority 16 and where the wager need not be registered with the lottery authority since the gaming software 22 or some other software or device associated with the gaming computer 14 provides a means of time-stamping the wager); or (2) a registration system (by which the player 12 chooses the wagering elements on the remote gaming computer 14, but then must contact the lottery authority 16 in order to "register" the wager). In the case of instant lotteries, verification of the date/time of the wager is not important, since, by definition, the essentially instantaneous output of the game program 24 determines the outcome. On the other hand, in lotteries based upon future events, the date and time of the wager is critical in a non-registration embodiment. A non-registration embodiment is depicted in FIG. 7B, and the wagering sequence associated therewith proceeds in the following manner. The player 12 logs onto the lottery application in the gaming computer 14 with his or her unique personal identification message 204, which has been preassigned by the lottery authority 16 with whom the player 12 has preregistered. In this regard, an external authentication apparatus such as an encryption/decryption device 82, depicted in FIG. 2 and described in more detail below, can be used to prevent minors from accessing the lottery program. Such a device can also employ, for additional verification, biometrics such as fingerprint, voiceprint or retinal-print recognition hardware and/or software. The player 12 then selects a specific lottery to play (e.g., Lotto), and selects the desired wagering elements 206 in a conventional manner, which choice(s) may be confirmed upon the player receiving a suitable prompt. The gaming computer 14 then generates an authenticatable ticket message 208 representing the selected wagering elements 206, and uses a hardened, tamper-proof or tamper-resistant clock to generate an authenticatable date/time message 210. This ticket message 208 may include a personal identification message 204 and/or software identification message 212. The ticket message 208 is stored in the gaming computer 14 and can be read and authenticated only by the host computer 30 associated with the lottery authority for verification. If desired, a physical "ticket" representing the player's choice of wagering elements as embodied in the authenticatable ticket message 208 can be printed out by conventional printing means associated with the gaming computer 14. This procedure may be repeated as many times as necessary to participate in multiple lottery events or to chose wagering elements for a single event. Such an arrangement allows wagering to take place independent from the lottery authority 16. The authenticatable date/time message 210 ensures that the player 12 cannot tamper with the wager "after the fact", i.e., after the drawing, the player cannot modify the numbers selected to produce a "winning ticket." To cash-out, the player 12 provides the authenticatable ticket message 208 to the lottery authority 16 and the host computer 30 reads and authenticates the ticket message 208 to reveal the selected wagering elements and the date/time of the wager. Winnings are then awarded in a conventional manner. It is anticipated that large payoffs will require that the player 12 physically return the gaming computer 14, if provided thereby, or any detachable data memory media, to the lottery authority 16 to enable inspection for any indication of tampering.

FIG. 7C depicts a registration sequence whereby the player 12 registers his or her lottery choice(s) with the lottery authority 16 prior to a lottery drawing. When the player 12 is ready to do so, the lottery authority 16 is called through a public telephone network. The player 12 then enters his or her unique PIN message 204, either by pressing the appropriate keys on the telephone pad, on the gaming computer 14 (if these are placed on-line in either a temporary or permanent connection), or by speaking the selections through the telephone for acquisition by a voice recognition program of the type known in the art. For additional verification, the player 12 can be asked to enter a computer or software identification message 212. The lottery authority 16 then requests that the player 12 choose from a menu of lotteries which are still open for wagering, make the desired selection(s), and indicate the method of payment. In certain applications, gambling credit can be preinstalled on the gaming computer 14 or module 90, as described above, in which case such credit can be included and represented in the authenticatable ticket message 208. Normally, the ticket-message 208 need not be authenticatable in a registration embodiment (i.e., it merely represents the choice of wagering elements). If the ticket message is authenticatable, it is then read and authenticated with a means known only to the lottery authority 16. This ensures and verifies that a valid lottery selection and sufficient credit were entered. The lottery authority 16 may confirm the transaction by reading back the wagering elements embodied in the message. After the lottery authority 16 accepts the ticket message 208, it generates a registration message 218 (authenticatable or non-authenticatable) which embodies the ticket message 208 and a current authenticatable date/time message 220, i.e., a "timestamp". The registration message 218 can be provided to the player 12 and is stored by the lottery authority 16 in the host computer 30 for future reference. The lottery authority 16 can then prompt the player to confirm the wager by entering a simple yes/no response. If desired, the lottery authority 16 can impose a limit on the number of wagers per player or per given time period and reject wagers exceeding set amounts. Optionally, the player 12 may obtain printed ticket receipts which include the registration message 218 from the gaming computer 14. The wagering process may be repeated for each "ticket" registered. When he or she is finished, the player 12 simply hangs up or terminates the connection with the lottery authority 16. After the lottery drawing or process, the lottery authority 16 compares any winning numbers against all registered tickets in accordance with conventional practice. If the prize is below a specific threshold (e.g., $100), then such prize can be credited to the player's account or credit card, or, if above a certain threshold, payouts can be made in a conventional manner.

In general, there are several ways by which the player 12 can cash-out winnings when such winnings are embodied or stored in the gaming computer 14. FIG. 8A is a flowchart diagram of the credit cash-out sequence in a first off-line embodiment. Player 12 first goes through the handshake sequence depicted in FIG. 5 and described above. Once player 12's identity is confirmed, the wagering establishment 16 provides the player 12 with an authenticatable banking activation message 64. The player 12 then activates banking program 26 and enters the banking activation message 64, which is read and authenticated by the gaming computer 14 to access the banking purchasing/redemption function. Player 12 then enters the amount of gambling credit he or she wants to cash-out into banking program 26. The amount to be cashed-out is placed by the banking program 26 into a cash-out pending field. The player's banking program 26 then generates an authenticatable credit cash-out message 66 which the player 12 provides to wagering establishment 16. The host computer 30 reads and authenticates the credit cash-out message 66 to reveal the amount of credit that the player 12 is requesting be cashed out, which amount is confirmed to the player 12 by wagering establishment 16. The host computer 30 then generates an authenticatable cash-out acknowledgment message 68 and provides this message to the player 12. Player 12 enters the cash-out acknowledgment message 68 into gaming computer 14 which reads and authenticates the same, and banking program 26 then deducts the amount of gambling credit to be cashed-out of the player's available gambling credit balance. Banking program 26 then generates an authenticatable deduction verification message 70 which indicates that the correct amount was deducted from the player's account. This message is provided to the wagering establishment 16 and read and authenticated by the host computer 30. The host computer thereafter generates an authenticatable program reactivation message 72 which is provided to the player 12 for entry into the gaming computer 14 to enable the game program 24 to permit continued gambling with any available gambling credit. The wagering establishment 16 then issues payment to the player 12 for the amount of gambling credit cashed-out, in the form of a credit to the player's credit card, a banking wire or some other mutually agreed-upon method of payment. It is also contemplated that where the player 12 has been provided with a dedicated gaming computer 14 (e.g., a hand-held device) gambling credit may be cashed-out by simply bringing the gaming computer 14 to the wagering establishment 16 (or its agent), where either the entire device or a credit module associated therewith is physically returned to facilitate inspection of the apparatus to determine whether any attempts have been made to tamper with or modify the unit or the software.

FIGS. 9-12 contain flowcharts of an on-line embodiment schematically depicted in FIG. 2, whereby gaming computer 14 communicates directly through a public telephone network or like communications link 29, such as via a modem, with the host computer 30. The host computer 30 includes gaming software 74 comprised of a game program 76, banking program 77, audit program 78 and authenticatable message read, authenticate and generate software 79. To prevent unauthorized access, an external authentication device such as the encryption/decryption device 82 shown schematically in FIG. 2, is used by the player 12 to generate a unique alphanumeric identification message 83. to provide a secure log-on message to obtain access to host computer 30 to participate in on-line gambling and/or purchase and redeem gambling credit. In one embodiment, device 82, which looks like a credit-card calculator, includes a display 84, an integral keyboard 86 and internal encryption/decryption hardware and/or software. Such a device is currently used for making wireless money transfers, for example, by Fleet Bank. Messages input and output to and from device 82 could be embodied in specific sounds identified through a dedicated sound recognition program which are transmitted to and received from computer 30. The encryption/decryption device 82 is used to generate an authenticatable log-on message 83 by encrypting player 12's personal identification message 32 with a separate verification message 88 provided to player 12 by computer 30. Alternatively, verification message 88 can be "built into" encryption/decryption device 82, such as stored in a ROM chip. Thus, knowledge of the player 12's personal identification message 32, in and of itself, is insufficient to enable an unauthorized third party such as a minor or known compulsive gambler to obtain access to gambling or to purchase and/or cash-out gambling credit. The gaming software 33 in the host computer 30 can contain appropriate instructions to, in such a case, terminate the on-line connection and prevent further attempts to gain access with that particular personal identification message 32. Moreover, the device 82 can have the banking program 26 associated therewith in order to store gambling credit independent of the gaming computer 14, in which case the exchange of messages between the device 82 and the gaming computer 14 would represent the actual "money". In this manner, gambling credit can be embodied in an apparatus which is structurally independent from the gaming computer 14.

FIG. 9 is a flowchart of the registration and start-up sequence. Initially, the player 12 through gaming computer 14, dials up and connects through the public telephone network 29 to the host computer 30. Player 12 then enters the requested registration information and is assigned a unique personal identification message 32. The player 12 then logs-on as described above. If player 12's identity is confirmed, the host computer 30 then permits wagering to the extent of any available gambling credit, and credit purchase and/or redemption.

As shown in FIG. 10, the purchase credit sequence in the on-line embodiment is comprised of the following series of exchanges between the gaming computer 14 and the host computer 30. The host computer 30 first generates a message which queries the player as to how much gambling credit is desired for the particular gambling session. The player 12 responds at the prompt with the amount of wagering credit requested. The wagering establishment 16 then obtains authorization for the requested amount through agreed upon methods of credit such as a credit card or the like. The approved credit amount is then deposited into player 12's wagering credit account in banking program 77. At this point, the player 12 can proceed to wager on a plurality of games offered by the wagering establishment 16. In this connection, player 12 may at the end of each session, request an authenticatable message number that verifies the amount of credit he or she has available from the wagering establishment 16 at that time for purposes of any future dispute resolution.

FIG. 11 is a flowchart of the gambling sequence in the on-line embodiment. The player 12 first activates gaming computer 14, establishes electronic communications with the wagering establishment computer 30 through the public telephone network 29, and proceeds with the secure log-on procedure described above. The gaming computer 14 then registers a gambling session message 80 with the host computer 30, which, in turn, makes available to the player 12 for wagering a choice of games of chance, skill or future public events where the outcome is uncertain.

FIG. 12 is a flowchart of the credit cash-out sequence in the on-line embodiment. The player 12 first requests to cash-out all or part of the credit balance in the wagering credit account maintained on host computer 30. The wagering establishment 16 then requests confirmation of the amount of credit to be cashed-out. The player 12 then keys in his or her unique personal identification message 32 to reconfirm that amount. This amount is then deducted from the player 12's credit account and the wagering establishment 16 then authorizes a credit to be made to the player's preassigned credit card, or makes some other agreed-upon method of payment. For additional verification, the encryption/decryption device 82 can be used to provide a verification message to the wagering establishment 16 prior to cashing-out. Moreover, the wagering establishment 16 can be provided with a special telephone number to call-back the player 12 to confirm the cash-out which can only then occur when the player 12 calls the wagering establishment 16 back from that number, to provide an additional measure of security.

Alternatively, in another on-line embodiment, the gaming computer 14 includes gaming software 22 as in the first embodiment of FIG. 1, but is on-line with the host computer 30 and, through the public telephone network 29, the host computer 30 may or may not serve to regulate or control the gaming software simulation of casino games on the gaming computer 14. For example, the host computer 30 can directly keep a record of all or selected activities taking place on the gaming computer 14 for the purpose of additional verification or security. Alternatively, the electronic link can be of a control nature to vary the odds of a given wager based upon any of a variety of factors such as gambling duration or other factors such as a progressively increasing jackpot (e.g., in a slot machine simulation).

In the off-line embodiment, at all times, an audit-trail of all transactions can be recorded on data storage media associated with the host computer 30, and optionally, in gaming computer 14 to be ultimately downloaded to or accessed by the wagering establishment 16. Such an audit-trail can also be recorded in the tamper-resistant or tamper-evident read/write data storage media device 28 provided by the wagering establishment 16 to player 12 in the embodiment shown in FIG. 3.

The present invention has been shown and described in what are considered to be the most practical and preferred embodiments. It is anticipated, however, that departures may be made therefrom and that obvious modifications will occur to persons skilled in the art.

CLAIMS

We Claim:

1. A gaming system, comprising:

a host computer which enables a player at a remote location to purchase and redeem gambling credit and which generates at least one authenticatable message to be provided from said host computer and which reads and authenticates at least one authenticatable message to be provided to said host computer;

an off-line gaming computer remotely disposed from said host computer on which the player wagers on at least one wagering opportunity, said gaming computer for generating at least one wagering opportunity and enabling the purchasing, storing and redeeming of gambling credit, said gaming computer further generating said at least one authenticatable message to be provided to said host computer and which reads and authenticates said at least one authenticatable message to be provided from said host computer, wherein said authenticatable messages exchanged between said host computer and said gaming computer enable the player to at least one of purchase and redeem gambling credit.

2. The gaming system recited in Claim 1, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity and enabling said purchasing, storing and redeeming of gambling credit, provided on data storage media.

3. The gaming system recited in Claim 1, wherein said gaming computer communicates with data memory media disposed within a tamper-proof read/write apparatus.

4. The gaming system recited in Claim 2, wherein said gaming computer reads the unique magnetic characteristics of said data storage media for the purpose of creating a unique authenticatable message

to thereby prevent undetectable duplication of data stored on said data storage media.

5. The gaming system recited in Claim 1, wherein said gaming computer includes at least one of tamper-resistant and tamper-evident data storage media for recording said authenticatable messages provided to and from said gaming computer to generate an audit trail.

6. The remote gaming system recited in Claim 1, wherein said host computer records and stores said messages provided to and from said host computer to generate an audit-trail.

7. The remote gaming system recited in Claim 1, wherein said gaming computer is provided with a predetermined amount of casino credit embodied in at least one of data storage media permanently installed on said gaming computer and data storage media removably installed on said gaming computer.

8. The remote gaming system recited in Claim 1, wherein said gaming computer includes at least one of voice recognition means for identifying the unique voice characteristics of the player and fingerprint identification means for identifying the unique fingerprint of the player.

9. The remote gaming system recited in Claim 1, wherein said wagering opportunity is a game of skill.

10. A gaming system, comprising:

a host computer which enables a player networked at a remote location to purchase and redeem gambling credit and wager on at least one wagering opportunity, said host computer generating at least one authenticatable message to be communicated from said host computer and reading and authenticating at least one authenticatable message communicated to said host computer;

a gaming computer on which the player wagers on said at least one wagering opportunity where said gaming computer is remotely disposed from said host computer; and

means for generating at least one authenticatable message for communication to and reading and authentication by said host computer to enable the player to access said host computer from said gaming computer.

11. The remote gaming system recited in Claim 10, wherein said means for generating said at least one authenticatable message is embodied in an apparatus which is structurally independent of said gaming computer.

12. A gaming computer for use in a gaming system for wagering against a wagering establishment;

said gaming computer for generating at least one wagering opportunity and enabling a player at a remote location from said wagering establishment to wager on and accumulate any winnings from said at least one wagering opportunity with gambling credit from said wagering establishment, said gaming computer having gambling credit pre-installed in said gaming computer by at least one of said wagering establishment and an authorized agent of said wagering establishment, said at least one wagering opportunity and gambling credit being enabled by software residing in at least one of tamper-resistant and tamper-evident memory means.

13. The gaming computer recited in Claim 12, wherein a predetermined amount of said credit is pre-installed in said gaming computer by said wagering establishment.

14. The gaming computer recited in Claim 12, wherein said credit is redeemed from said wagering establishment by providing said wagering establishment with said gaming computer, and said wagering establishment utilizes secure means for checking said gaming computer hardware and software to reveal at

least one of any fraud and tampering.

15. The gaming computer recited in Claim 12, wherein said credit is stored on detachable and at least one of tamper-resistant and tamper-evident data memory media which interface with said gaming computer and where said data memory media are provided to said wagering establishment for credit redemption.

16. A gaming method by which a player gambles on a gaming computer against a wagering establishment where no on-line connection exists between the gaming computer and the wagering establishment, comprising the steps of:

(A)purchasing gambling credit from said wagering establishment and at least one of loading and preloading said gambling credit into said gaming computer;

(B)generating at least one wagering opportunity on said gaming computer;

(C)proceeding to wager on said at least one wagering opportunity presented on said gaming computer;

(D)accumulating wagering credits or debits on said gaming computer as a result of the outcome of said at least one wagering opportunity; and

(E)redeeming gambling credit from said wagering establishment by communicating at least one authenticatable message provided from said wagering establishment to said gaming computer which reads and authenticates said at least one authenticatable message, and communicating at least one authenticatable message to said wagering establishment, where at least one of said authenticatable messages is read and authenticated by said wagering establishment.

17. A gaming method by which a player having a personal identification message gambles against a wagering establishment on a gaming computer which

presents a computer generated wagering opportunity, where the gaming computer is at a remote location and networked to a host computer associated with the gaming establishment, comprising the steps of:

(A)establishing a secure on-line link between said gaming computer and said host computer by generating an authenticatable message embodying an identification message known only to the player and the wagering establishment and a separate message, said host computer then authenticating said authenticatable message for verification;

(B)purchasing gambling credit from said wagering establishment;

(C)generating at least one wagering opportunity on said gaming computer;

(D)proceeding to wager on said at least one wagering opportunity presented on said gaming computer;

(E)accumulating at least one of wagering credits band debits as a result of the outcome of said at least one wagering opportunity; and

(F)redeeming gambling credit from said wagering establishment.

18. The method recited in Claim 17, wherein Step (F) further comprises generating an authenticatable message on said gaming computer embodying an identification message known only to the player and the wagering establishment, said message to be communicated to, read and authenticated by said host computer for verification prior to redeeming said gambling credit.

19. The method recited in Claim 17, wherein said authenticatable message is authenticatable and generated by an encryption/decryption apparatus which is structurally independent of said gaming computer.

20. The method recited in Claim 17, wherein said gambling credit is embodied in an

encryption/decryption apparatus which is structurally independent of said gaming computer.

21. A gaming system which enables a player at a remote location to wager against a wagering establishment, wherein the player wagers on a gaming computer where said gaming computer generates at least one wagering opportunity and enables the player to at least one of purchase gambling credit and redeem gambling winnings.

22. The gaming system recited in Claim 21, wherein said purchased pre-installed credit is embodied in a tamper-proof plug-in module, provided by the wagering establishment and interfaced with said gaming computer.

23. The gaming system recited in Claim 32, wherein said gambling winnings are electronically stored on at least one of a tamper-resistant and tamper-evident plug-in module provided by the wagering establishment and interfaced with said gaming computer.

24. The gaming system recited in Claim 21; wherein said gaming computer includes gaming software for generating said at least one wagering opportunity, and said gaming software resides on a tamper-proof chip disposed in an inspectable casing.

25. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity which includes a random distribution of messages known only to the wagering establishment to prevent unauthorized tampering with said gaming software.

26. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity, and means for receiving external keys input to said gaming software, said keys being used by said gaming software to function and which disable said gaming

program if said gaming software has been tampered with.

27. The gaming system recited in Claim 21, wherein said gaming computer includes gaming software for generating said at least one wagering opportunity upon receiving data from a source external to said gaming computer.

28. A gaming system which enables a player at a remote location to participate in a lottery by choosing a selection of wagering elements in a lottery on a gaming computer, where said selection of wagering elements is combined with at least one of an authenticatable date/time message, player's identification message, and computer/software identification message, into an authenticatable message representing the player's selection to be read and authenticated by a lottery authority for registration.

29. The gaming system recited in Claim 28, wherein said selection is combined, with at least one of a date/time stamp, player's identification message, and computer/software identification message, into a compressed ticket-message to be reads and authenticates by a lottery authority for registration.

30. The gaming system recited in Claim 28, wherein said selection is date/time stamped to form an encrypted ticket message for decryption by a lottery authority to reveal a valid wager.

31. A method by which a player participates in a lottery offered by a lottery authority, comprising the steps of:

(A) choosing wagering elements for a given lottery event on a gaming computer;

(B) generating an authenticatable message on said gaming computer which embodies the choice of said wagering elements and at least one of an authenticatable date/time message player's identification message, computer identification message, and software identification message;

(C)registering the wager with the lottery authority by communicating said authenticatable message to the lottery authority, where said lottery authority has a host computer which reads and authenticates said authenticatable message to reveal the player's valid choice of wagering elements; and

(D)confirming the wager by generating an authenticatable registration message on said host computer by combining said authenticatable message with an authenticatable date/time message using a means known only to the lottery authority.

32. A gaming computer for use in a gaming system for wagering against a wagering establishment, said gaming computer for generating at least one wagering opportunity and enabling a player at a remote location to wager on and accumulate any winnings from said at least one wagering opportunity with purchased gambling credit embodied in at least one of a tamper-resistant and tamper-evident module provided to said player by said wagering establishment.

33. A gaming computer for use in a gaming system for wagering against a wagering establishment, said gaming computer having gaming software for generating at least one wagering opportunity and enabling a player at a remote location to wager on and accumulate any winnings from said at least one wagering opportunity with purchased gambling credit, said gaming software residing on at least one of tamper-resistant and tamper-evident data storage media disposed in an inspectable casing.

34. A gaming computer for use in a gaming system for wagering against a wagering establishment, said gaming computer having gaming software for generating at least one wagering opportunity and enabling a player at a remote location to wager on and accumulate

any winnings from said at least one wagering opportunity with purchased gambling credit, said gaming software including a random distribution of messages known only to the wagering establishment to enable the wagering establishment to check said distribution of messages to reveal unauthorized tampering with said gaming software.

35. A gaming computer for use in a gaming system for wagering against a wagering establishment, said gaming computer having gaming software for generating at least one wagering opportunity and enabling a player at a remote location to wager on and accumulate any winnings from said at least one wagering opportunity with purchased gambling credit, said gaming computer further including means for receiving external keys for input to said gaming software to enable said gaming software and disable said gaming software if said gaming software has been tampered with.

36. A gaming computer for use in a gaming system for wagering against a wagering establishment, said gaming computer having gaming software for generating at least one wagering opportunity and enabling a player at a remote location to wager on and accumulate any winnings from said at least one wagering opportunity with purchased gambling credit, said gaming software further including means for receiving data from a source external to said gaming computer to enable said gaming software.

37. The gaming system recited in Claim 1, wherein said authenticatable messages are encrypted with an encryption key known only to said wagering establishment for decryption by at least one of said host computer and said gaming computer.

38. The gaming system recited in Claim 10, wherein said authenticatable messages are encrypted with an encryption key known only to said wagering

establishment for decryption by at least one of said host computer and said gaming computer.

39. The gaming system recited in Claim 17, wherein said authenticatable messages are encrypted with an encryption key known only to said wagering establishment for decryption by at least one of said host computer and said gaming computer.

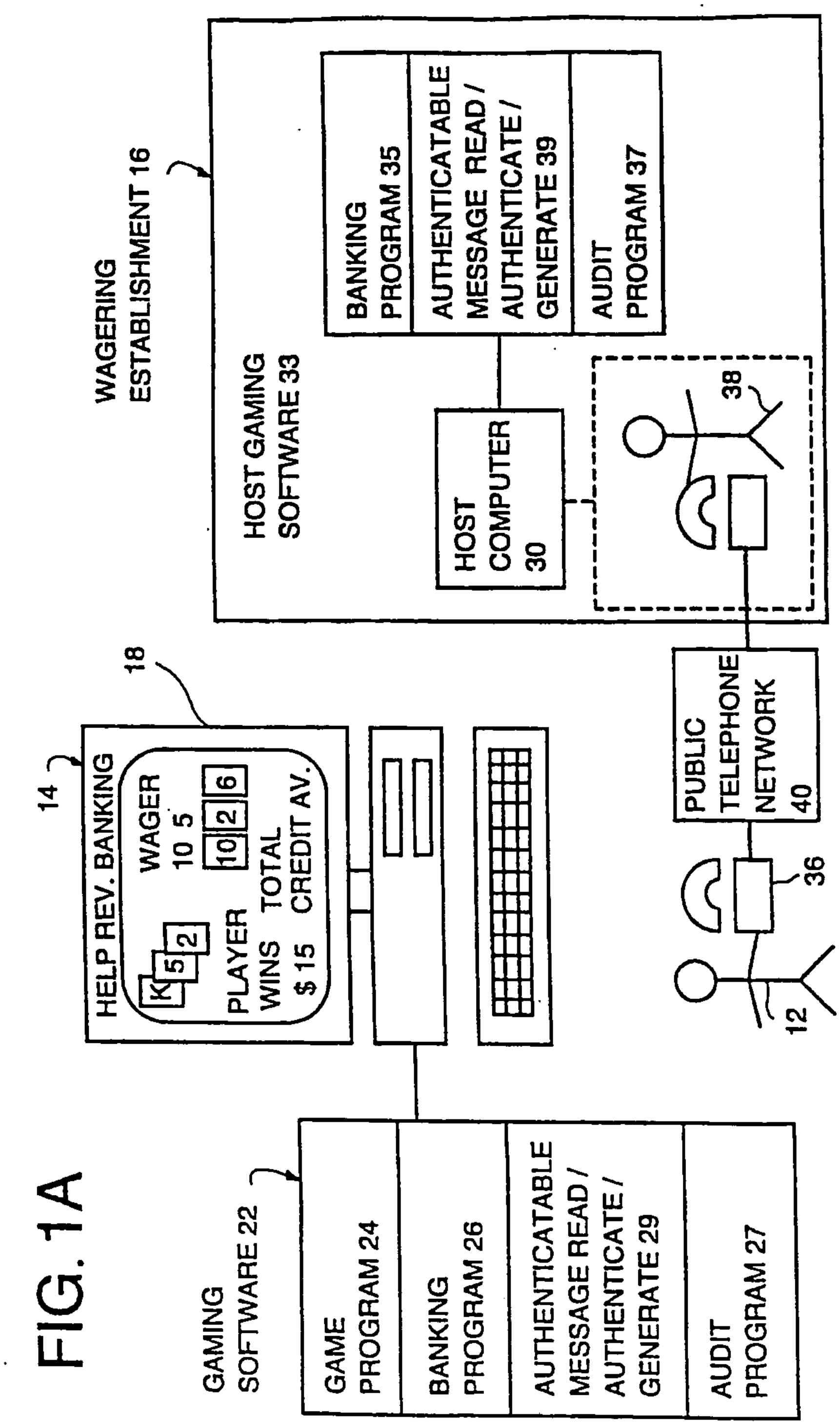

WAGERING
ESTABLISHMENT 16
BANKING
PROGRAM 35
AUTHENTICATABLE
MESSAGE READ /
AUTHENTICATE /
GENERATE 39
AUDIT
PROGRAM 37
HOST GAMING
SOFTWARE 33
HOST
COMPUTER
30
38
18
14
HELP REV. BANKING
K
5
2
WAGER
10 5
10
2
6
PLAYER
WINS
$ 15
TOTAL
CREDIT AV.
PUBLIC
TELEPHONE
NETWORK
40
36
12
GAMING
SOFTWARE 22
GAME
PROGRAM 24
BANKING
PROGRAM 26
AUTHENTICATABLE
MESSAGE READ /
AUTHENTICATE /
GENERATE 29
AUDIT
PROGRAM 27

FIG. 1A

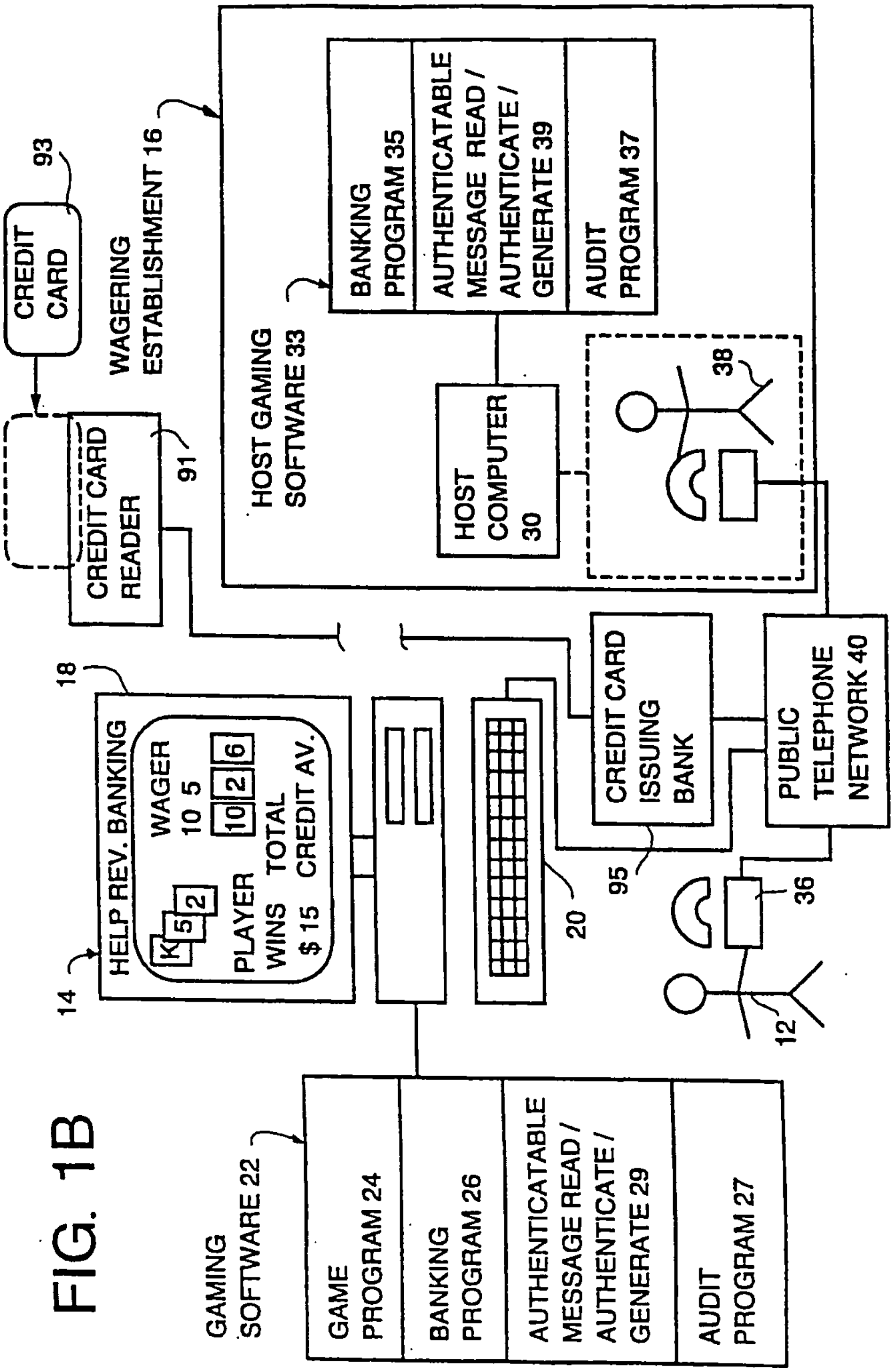

CREDIT CARD
93
WAGERING ESTABLISHMENT 16
BANKING PROGRAM 35
AUTHENTICATABLE MESSAGE READ / AUTHENTICATE / GENERATE 39
AUDIT PROGRAM 37
HOST GAMING SOFTWARE 33
CREDIT CARD READER
91
HOST COMPUTER 30
38
CREDIT CARD ISSUING BANK
PUBLIC TELEPHONE NETWORK 40
95
36
12
20
18
14
HELP REV. BANKING
WAGER
10 5
K 5 2
10 2 6
PLAYER WINS $ 15
TOTAL CREDIT AV.
GAMING SOFTWARE 22
GAME PROGRAM 24
BANKING PROGRAM 26
AUTHENTICATABLE MESSAGE READ / AUTHENTICATE / GENERATE 29
AUDIT PROGRAM 27

FIG. 1B

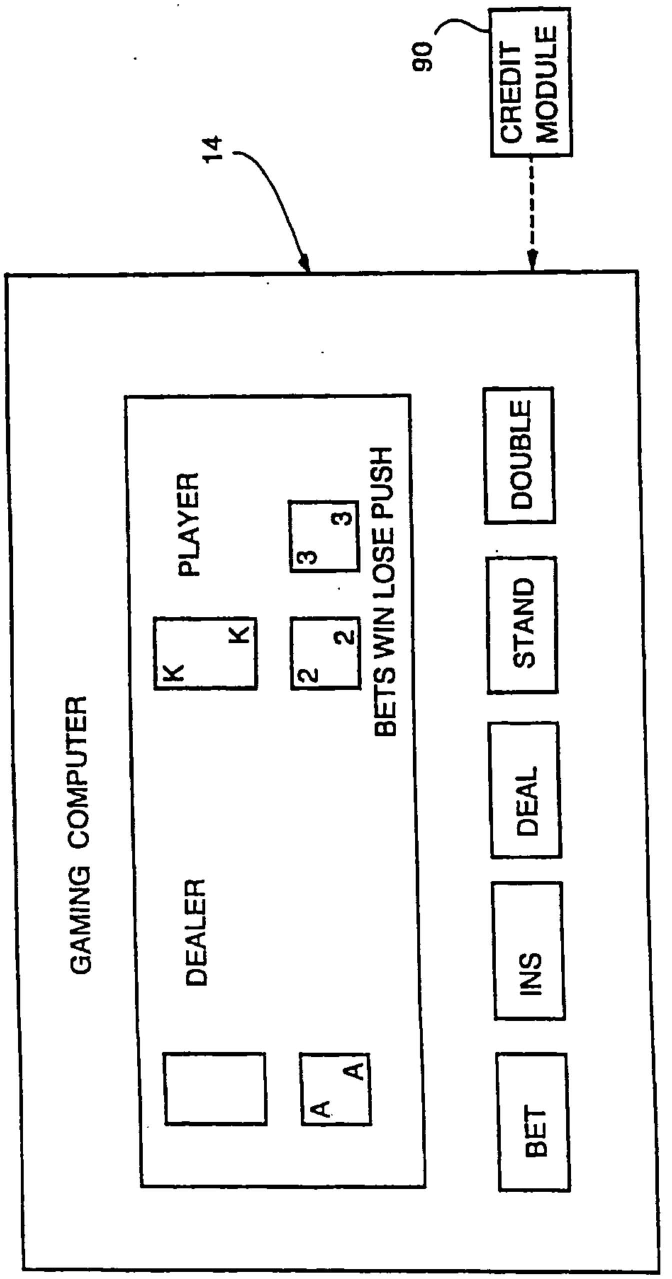

14
90
CREDIT MODULE
GAMING COMPUTER
DEALER
A
A
PLAYER
K
K
2
2
3
3
BETS WIN LOSE PUSH
BET
INS
DEAL
STAND
DOUBLE

FIG. 1C

FIG. 2

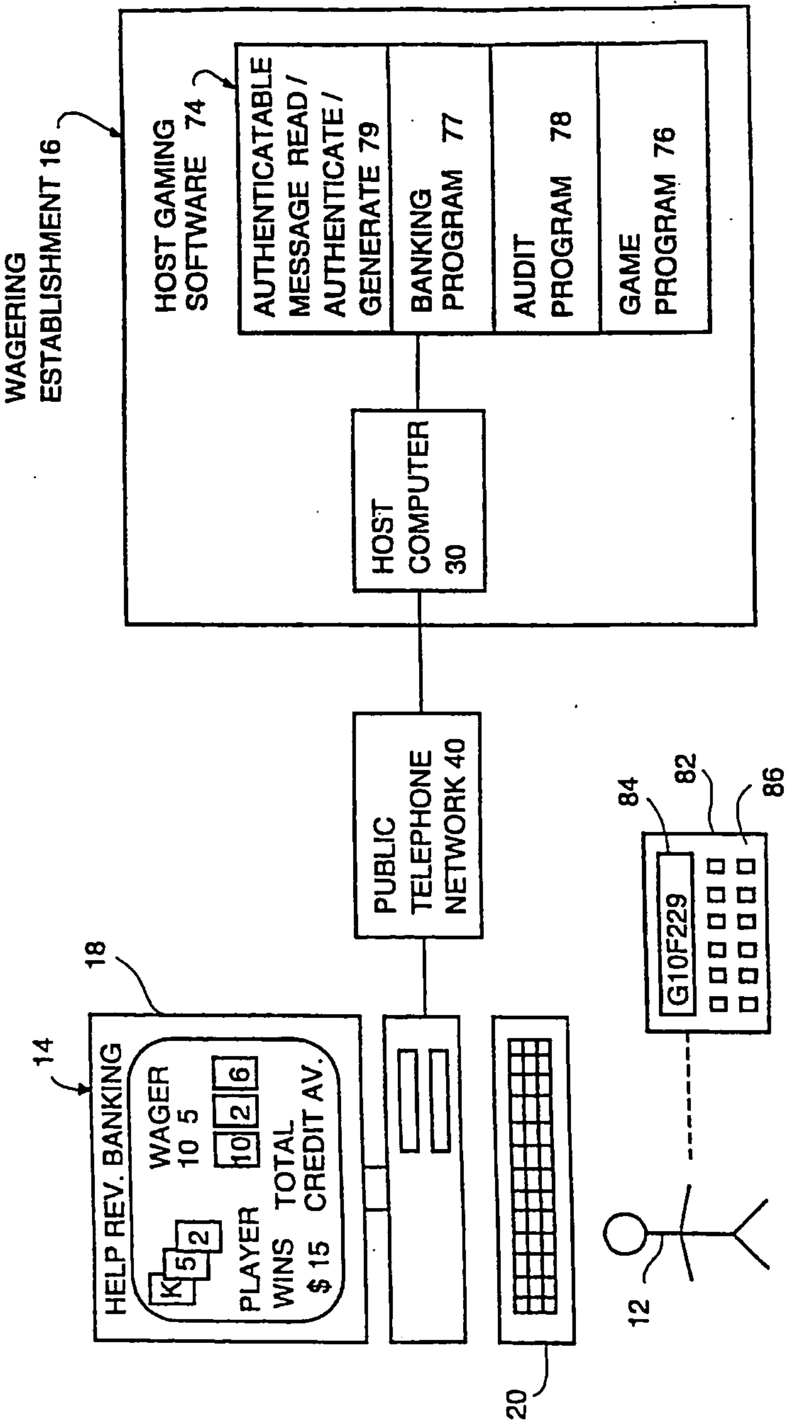
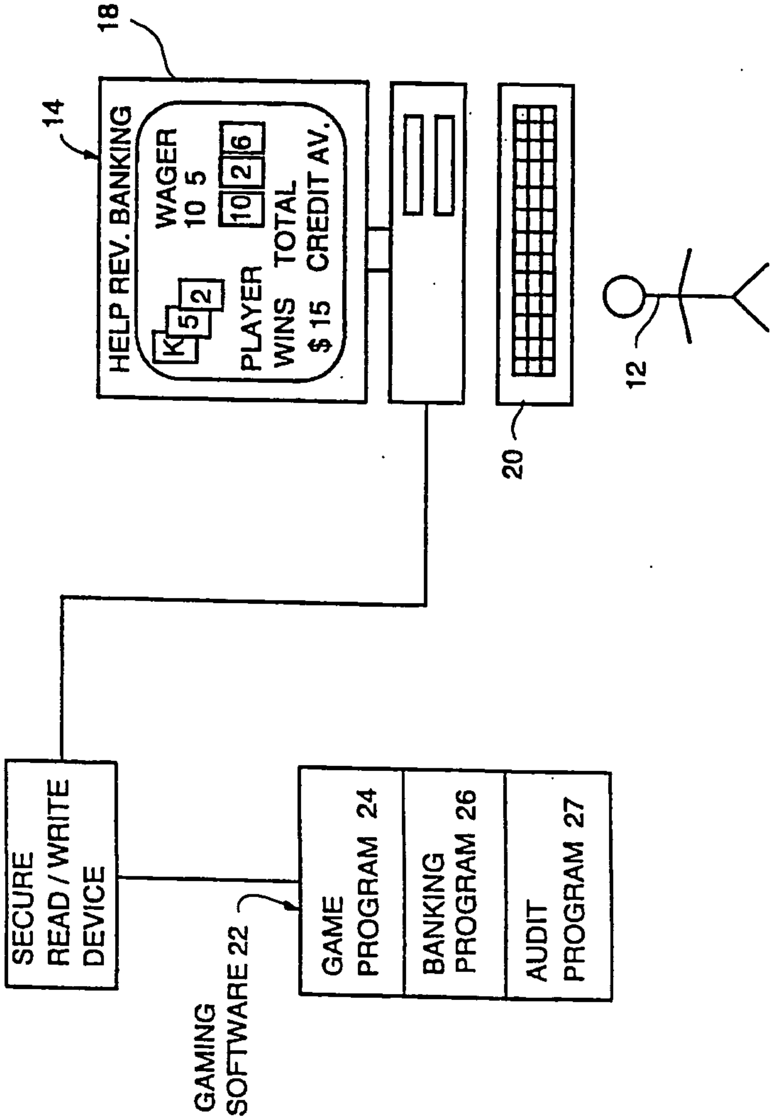

WAGERING ESTABLISHMENT 16
HOST GAMING SOFTWARE 74
AUTHENTICATABLE MESSAGE READ / AUTHENTICATE / GENERATE 79
BANKING PROGRAM 77
AUDIT PROGRAM 78
GAME PROGRAM 76
HOST COMPUTER 30
PUBLIC TELEPHONE NETWORK 40
18
14
HELP REV. BANKING
K
5
2
WAGER
10 5
10
2
6
PLAYER WINS $ 15
TOTAL CREDIT AV.
84
82
86
G10F229
12
20

FIG. 3


18
14
HELP REV. BANKING
K
5
2
WAGER
10 5
10
2
6
PLAYER
WINS
$ 15
TOTAL
CREDIT AV.
20
12
SECURE
READ / WRITE
DEVICE
GAME
PROGRAM 24
BANKING
PROGRAM 26
AUDIT
PROGRAM 27
GAMING
SOFTWARE 22

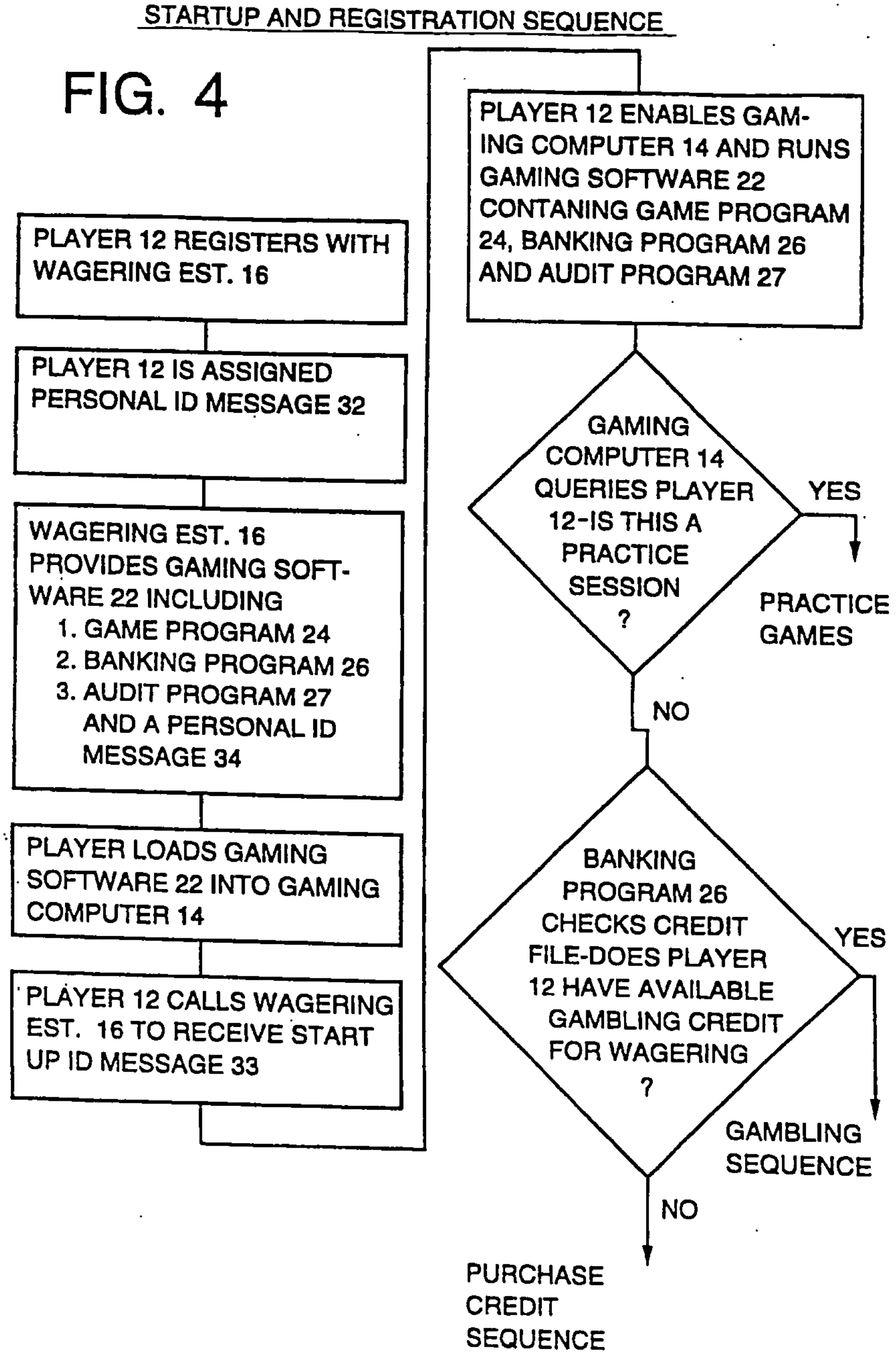

STARTUP AND REGISTRATION SEQUENCE
PLAYER 12 REGISTERS WITH WAGERING EST. 16
PLAYER 12 IS ASSIGNED PERSONAL ID MESSAGE 32
WAGERING EST. 16 PROVIDES GAMING SOFTWARE 22 INCLUDING
1. GAME PROGRAM 24
2. BANKING PROGRAM 26
3. AUDIT PROGRAM 27 AND A PERSONAL ID MESSAGE 34
PLAYER LOADS GAMING SOFTWARE 22 INTO GAMING COMPUTER 14
PLAYER 12 CALLS WAGERING EST. 16 TO RECEIVE START UP ID MESSAGE 33
PLAYER 12 ENABLES GAMING COMPUTER 14 AND RUNS GAMING SOFTWARE 22 CONTANING GAME PROGRAM 24, BANKING PROGRAM 26 AND AUDIT PROGRAM 27
GAMING COMPUTER 14 QUERIES PLAYER 12-IS THIS A PRACTICE SESSION ?
YES
PRACTICE GAMES
NO
BANKING PROGRAM 26 CHECKS CREDIT FILE-DOES PLAYER 12 HAVE AVAILABLE GAMBLING CREDIT FOR WAGERING ?
YES
GAMBLING SEQUENCE
NO
PURCHASE CREDIT SEQUENCE

FIG. 4

HANDSHAKE RECOGNITION SEQUENCE

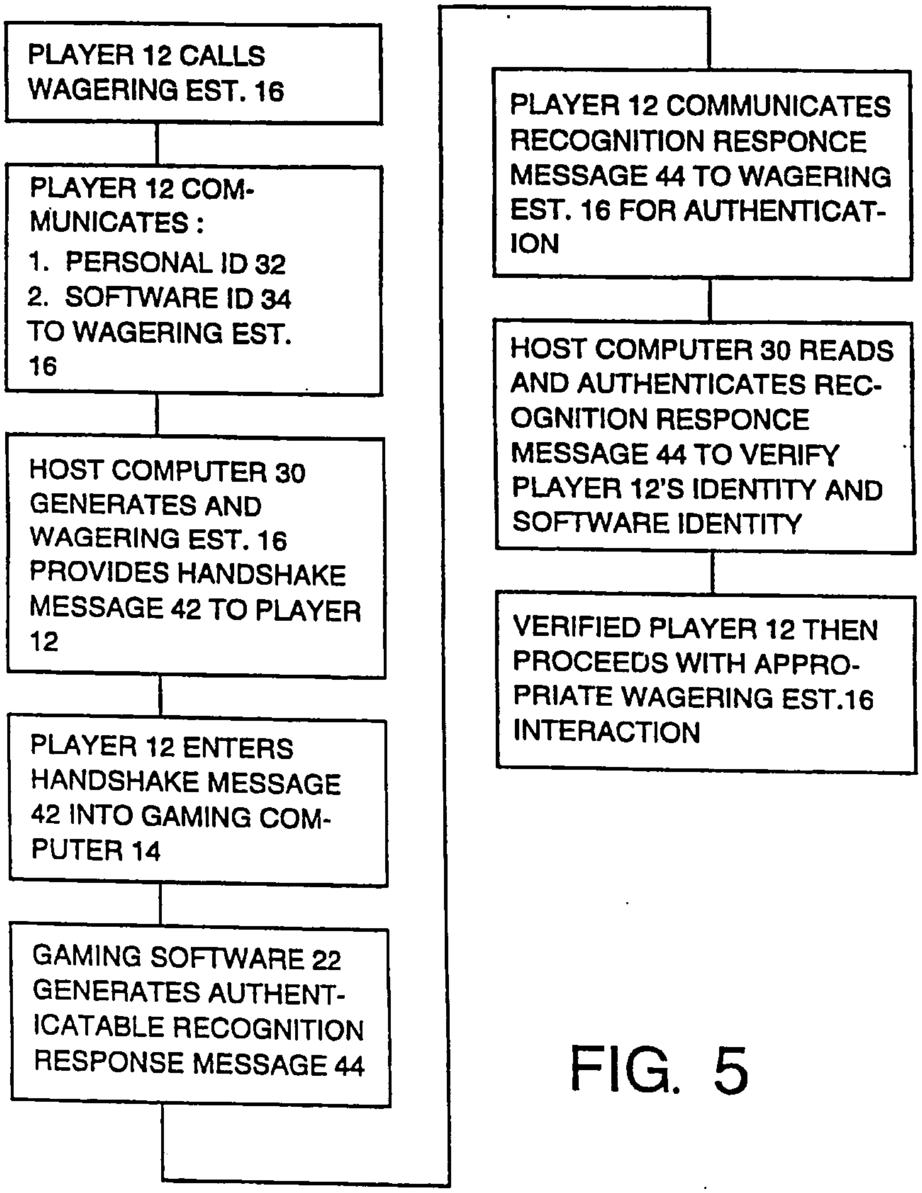
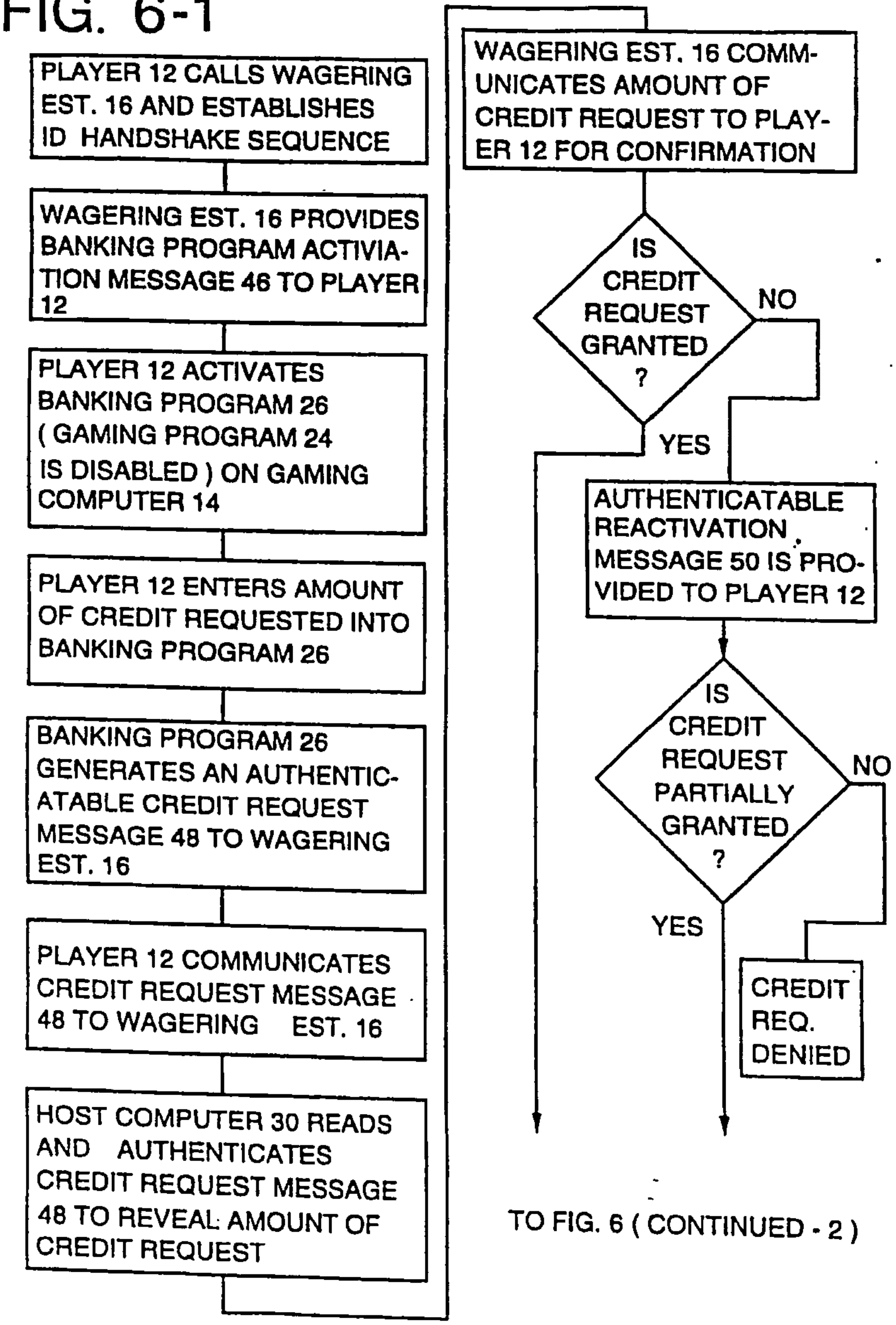

PLAYER 12 CALLS WAGERING EST. 16
PLAYER 12 COMMUNICATES : 1. PERSONAL ID 32 2. SOFTWARE ID 34 TO WAGERING EST. 16
HOST COMPUTER 30 GENERATES AND WAGERING EST. 16 PROVIDES HANDSHAKE MESSAGE 42 TO PLAYER 12
PLAYER 12 ENTERS HANDSHAKE MESSAGE 42 INTO GAMING COMPUTER 14
GAMING SOFTWARE 22 GENERATES AUTHENTICATABLE RECOGNITION RESPONSE MESSAGE 44
PLAYER 12 COMMUNICATES RECOGNITION RESPONCE MESSAGE 44 TO WAGERING EST. 16 FOR AUTHENTICATION
HOST COMPUTER 30 READS AND AUTHENTICATES RECOGNITION RESPONCE MESSAGE 44 TO VERIFY PLAYER 12'S IDENTITY AND SOFTWARE IDENTITY
VERIFIED PLAYER 12 THEN PROCEEDS WITH APPROPRIATE WAGERING EST.16 INTERACTION

FIG. 5

PURCHASE CREDIT SEQUENCE - OFF - LINE EMBODIMENT

FIG. 6-1


PLAYER 12 CALLS WAGERING EST. 16 AND ESTABLISHES ID HANDSHAKE SEQUENCE
WAGERING EST. 16 PROVIDES BANKING PROGRAM ACTIVIATION MESSAGE 46 TO PLAYER 12
PLAYER 12 ACTIVATES BANKING PROGRAM 26 (GAMING PROGRAM 24 IS DISABLED) ON GAMING COMPUTER 14
PLAYER 12 ENTERS AMOUNT OF CREDIT REQUESTED INTO BANKING PROGRAM 26
BANKING PROGRAM 26 GENERATES AN AUTHENTICATABLE CREDIT REQUEST MESSAGE 48 TO WAGERING EST. 16
PLAYER 12 COMMUNICATES CREDIT REQUEST MESSAGE 48 TO WAGERING EST. 16
HOST COMPUTER 30 READS AND AUTHENTICATES CREDIT REQUEST MESSAGE 48 TO REVEAL AMOUNT OF CREDIT REQUEST
WAGERING EST. 16 COMMUNICATES AMOUNT OF CREDIT REQUEST TO PLAYER 12 FOR CONFIRMATION
IS CREDIT REQUEST GRANTED ?
NO
YES
AUTHENTICATABLE REACTIVATION MESSAGE 50 IS PROVIDED TO PLAYER 12
IS CREDIT REQUEST PARTIALLY GRANTED ?
NO
YES
CREDIT REQ. DENIED

TO FIG. 6 (CONTINUED - 2)

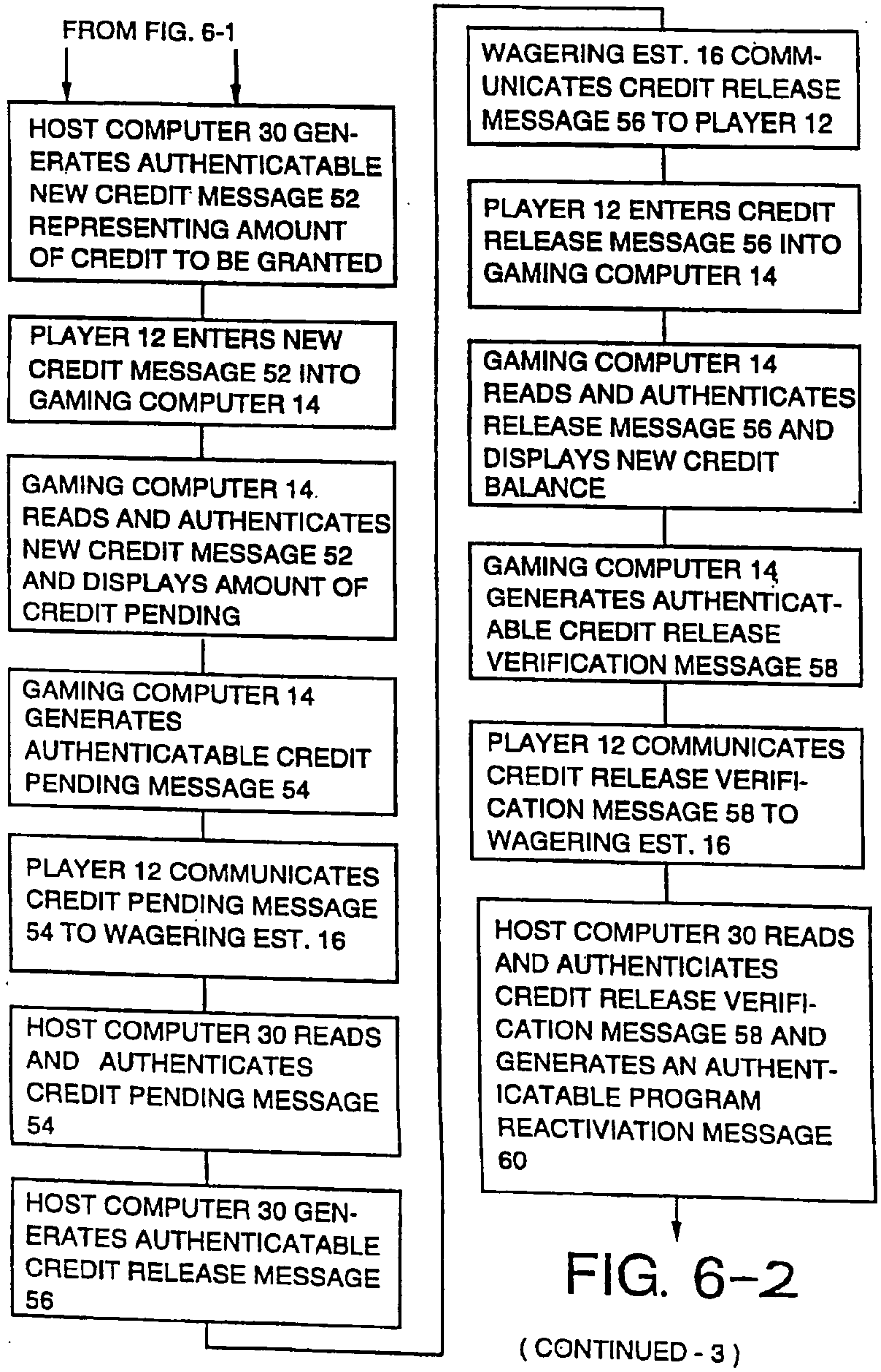
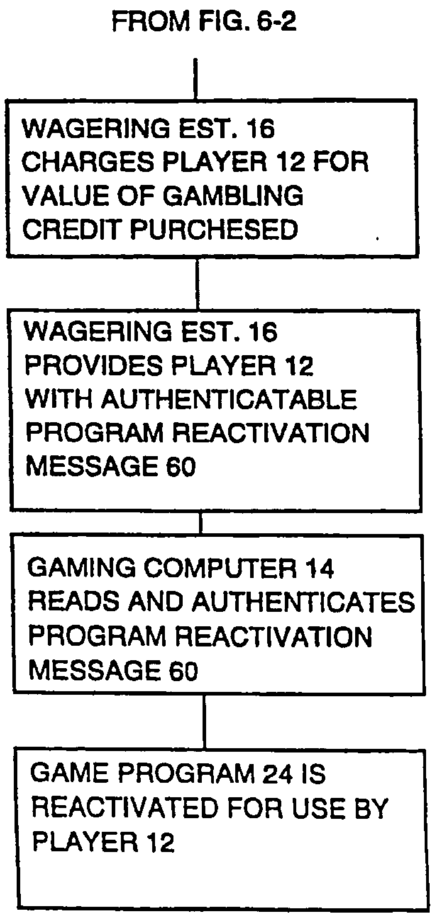

FROM FIG. 6-1
HOST COMPUTER 30 GENERATES AUTHENTICATABLE NEW CREDIT MESSAGE 52 REPRESENTING AMOUNT OF CREDIT TO BE GRANTED
PLAYER 12 ENTERS NEW CREDIT MESSAGE 52 INTO GAMING COMPUTER 14
GAMING COMPUTER 14 READS AND AUTHENTICATES NEW CREDIT MESSAGE 52 AND DISPLAYS AMOUNT OF CREDIT PENDING
GAMING COMPUTER 14 GENERATES AUTHENTICATABLE CREDIT PENDING MESSAGE 54
PLAYER 12 COMMUNICATES CREDIT PENDING MESSAGE 54 TO WAGERING EST. 16
HOST COMPUTER 30 READS AND AUTHENTICATES CREDIT PENDING MESSAGE 54
HOST COMPUTER 30 GENERATES AUTHENTICATABLE CREDIT RELEASE MESSAGE 56
WAGERING EST. 16 COMMUNICATES CREDIT RELEASE MESSAGE 56 TO PLAYER 12
PLAYER 12 ENTERS CREDIT RELEASE MESSAGE 56 INTO GAMING COMPUTER 14
GAMING COMPUTER 14 READS AND AUTHENTICATES RELEASE MESSAGE 56 AND DISPLAYS NEW CREDIT BALANCE
GAMING COMPUTER 14 GENERATES AUTHENTICATABLE CREDIT RELEASE VERIFICATION MESSAGE 58
PLAYER 12 COMMUNICATES CREDIT RELEASE VERIFICATION MESSAGE 58 TO WAGERING EST. 16
HOST COMPUTER 30 READS AND AUTHENTICIATES CREDIT RELEASE VERIFICATION MESSAGE 58 AND GENERATES AN AUTHENTICATABLE PROGRAM REACTIVIATION MESSAGE 60

FIG. 6-2

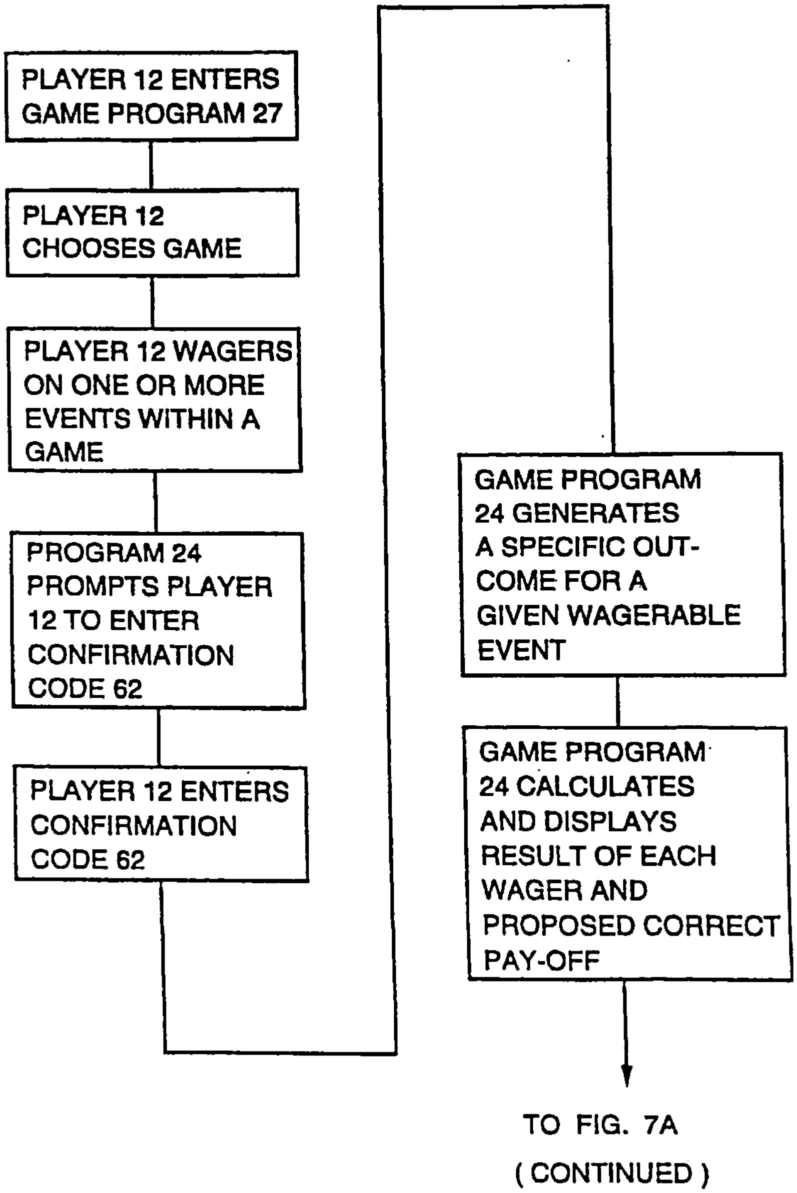
(CONTINUED - 3)

FIG. 6-3


FROM FIG. 6-2
WAGERING EST. 16 CHARGES PLAYER 12 FOR VALUE OF GAMBLING CREDIT PURCHESED
WAGERING EST. 16 PROVIDES PLAYER 12 WITH AUTHENTICATABLE PROGRAM REACTIVATION MESSAGE 60
GAMING COMPUTER 14 READS AND AUTHENTICATES PROGRAM REACTIVATION MESSAGE 60
GAME PROGRAM 24 IS REACTIVATED FOR USE BY PLAYER 12

WAGERING SEQUENCE (OFF-LINE)

FIG. 7A


PLAYER 12 ENTERS GAME PROGRAM 27
PLAYER 12 CHOOSES GAME
PLAYER 12 WAGERS ON ONE OR MORE EVENTS WITHIN A GAME
PROGRAM 24 PROMPTS PLAYER 12 TO ENTER CONFIRMATION CODE 62
PLAYER 12 ENTERS CONFIRMATION CODE 62
GAME PROGRAM 24 GENERATES A SPECIFIC OUT-COME FOR A GIVEN WAGERABLE EVENT
GAME PROGRAM 24 CALCULATES AND DISPLAYS RESULT OF EACH WAGER AND PROPOSED CORRECT PAY-OFF
TO FIG. 7A (CONTINUED)

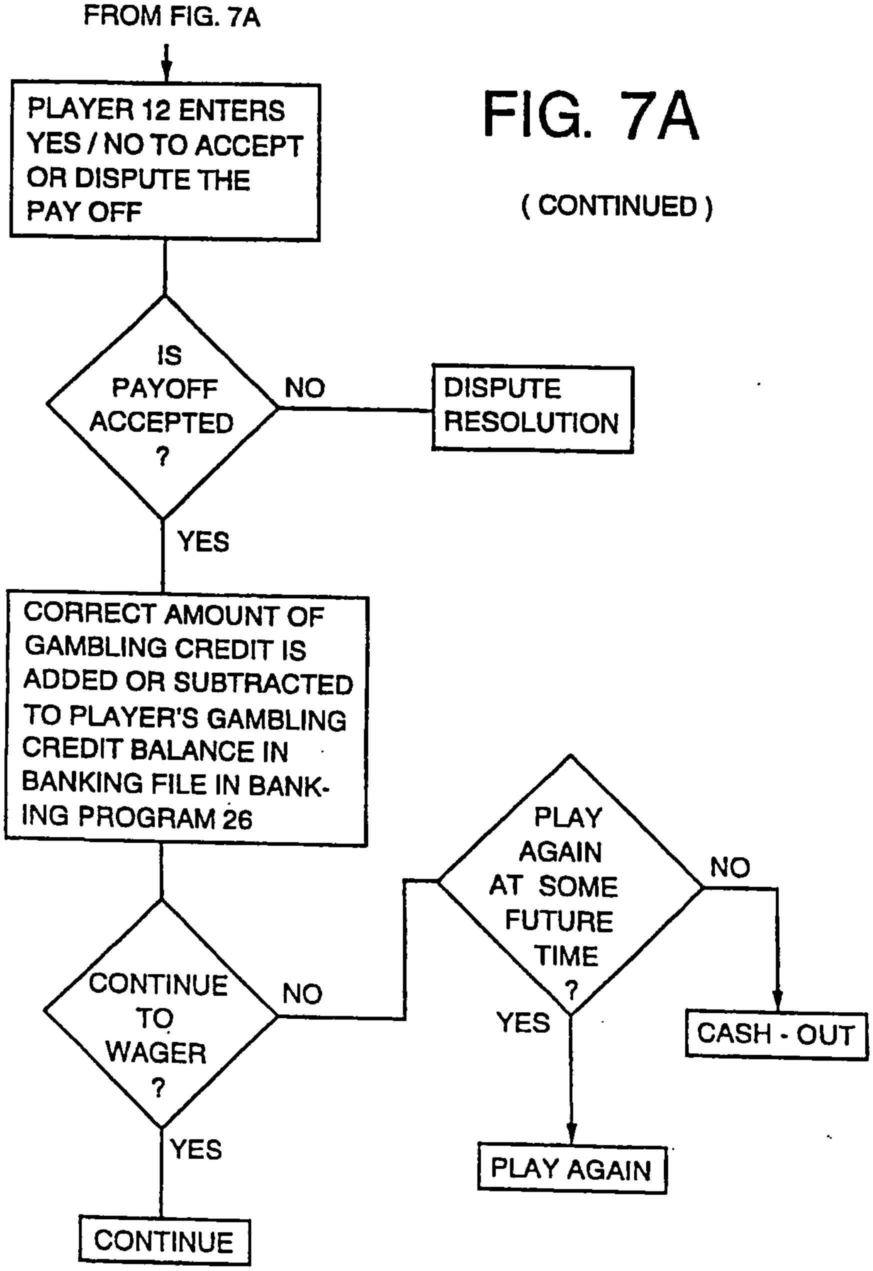
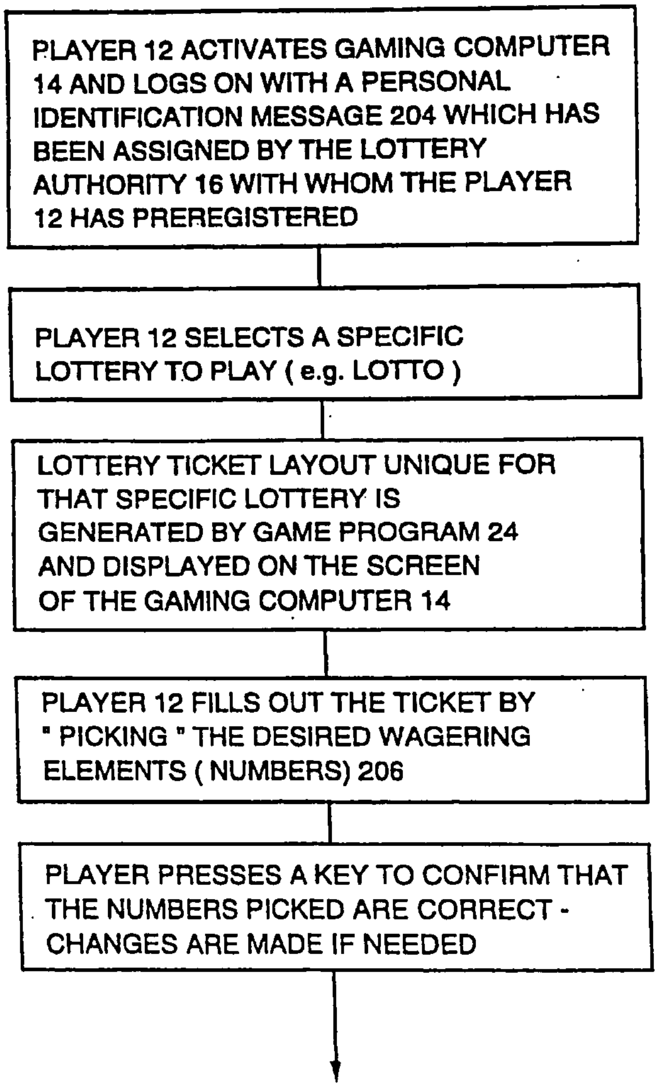

FROM FIG. 7A
PLAYER 12 ENTERS YES / NO TO ACCEPT OR DISPUTE THE PAY OFF
IS PAYOFF ACCEPTED ?
NO
DISPUTE RESOLUTION
YES
CORRECT AMOUNT OF GAMBLING CREDIT IS ADDED OR SUBTRACTED TO PLAYER'S GAMBLING CREDIT BALANCE IN BANKING FILE IN BANK-ING PROGRAM 26
CONTINUE TO WAGER ?
NO
YES
CONTINUE
PLAY AGAIN AT SOME FUTURE TIME ?
NO
YES
CASH - OUT
PLAY AGAIN

FIG. 7A

(CONTINUED)

WAGERING SEQUENCE (OFF-LINE) NON-REGISTERED LOTTERY

FIG. 7B-1



PLAYER 12 ACTIVATES GAMING COMPUTER 14 AND LOGS ON WITH A PERSONAL IDENTIFICATION MESSAGE 204 WHICH HAS BEEN ASSIGNED BY THE LOTTERY AUTHORITY 16 WITH WHOM THE PLAYER 12 HAS PREREGISTERED

PLAYER 12 SELECTS A SPECIFIC LOTTERY TO PLAY (e.g. LOTTO)

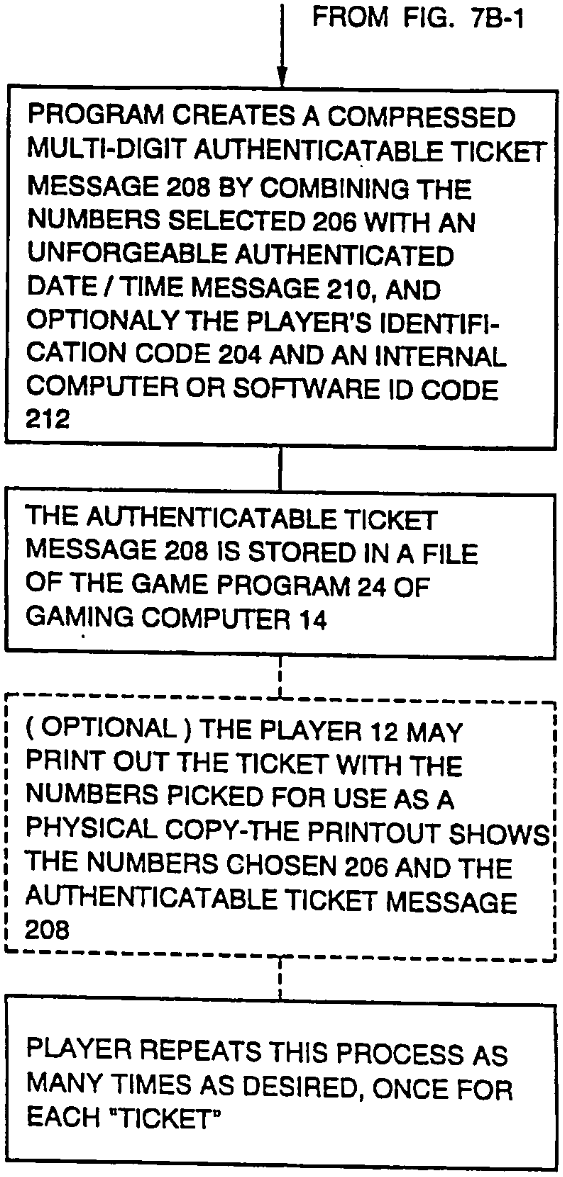
LOTTERY TICKET LAYOUT UNIQUE FOR THAT SPECIFIC LOTTERY IS GENERATED BY GAME PROGRAM 24 AND DISPLAYED ON THE SCREEN OF THE GAMING COMPUTER 14

PLAYER 12 FILLS OUT THE TICKET BY " PICKING " THE DESIRED WAGERING ELEMENTS (NUMBERS) 206

PLAYER PRESSES A KEY TO CONFIRM THAT THE NUMBERS PICKED ARE CORRECT - CHANGES ARE MADE IF NEEDED

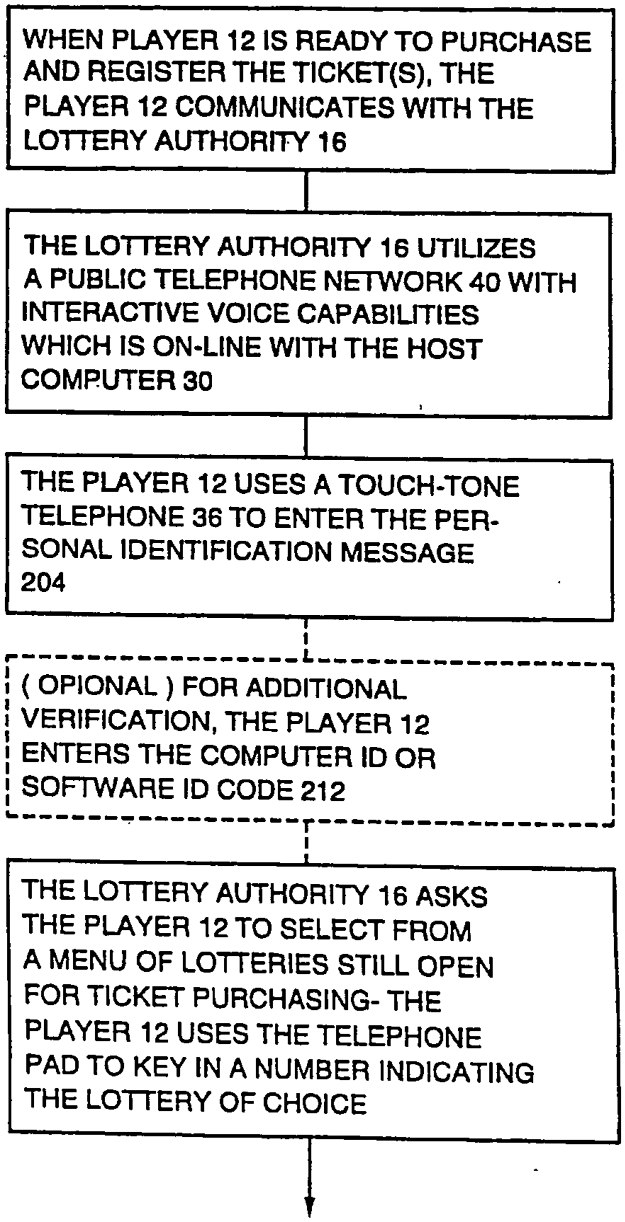
TO FIG. 7B-2

FIG. 7B-2


FROM FIG. 7B-1
PROGRAM CREATES A COMPRESSED MULTI-DIGIT AUTHENTICATABLE TICKET MESSAGE 208 BY COMBINING THE NUMBERS SELECTED 206 WITH AN UNFORGEABLE AUTHENTICATED DATE / TIME MESSAGE 210, AND OPTIONALY THE PLAYER'S IDENTIFICATION CODE 204 AND AN INTERNAL COMPUTER OR SOFTWARE ID CODE 212
THE AUTHENTICATABLE TICKET MESSAGE 208 IS STORED IN A FILE OF THE GAME PROGRAM 24 OF GAMING COMPUTER 14
(OPTIONAL) THE PLAYER 12 MAY PRINT OUT THE TICKET WITH THE NUMBERS PICKED FOR USE AS A PHYSICAL COPY-THE PRINTOUT SHOWS THE NUMBERS CHOSEN 206 AND THE AUTHENTICATABLE TICKET MESSAGE 208
PLAYER REPEATS THIS PROCESS AS MANY TIMES AS DESIRED, ONCE FOR EACH "TICKET"

WAGERING SEQUENCE (OFF-LINE) REGISTERED LOTTERY

FIG. 7C-1



WHEN PLAYER 12 IS READY TO PURCHASE AND REGISTER THE TICKET(S), THE PLAYER 12 COMMUNICATES WITH THE LOTTERY AUTHORITY 16

THE LOTTERY AUTHORITY 16 UTILIZES A PUBLIC TELEPHONE NETWORK 40 WITH INTERACTIVE VOICE CAPABILITIES WHICH IS ON-LINE WITH THE HOST COMPUTER 30

THE PLAYER 12 USES A TOUCH-TONE TELEPHONE 36 TO ENTER THE PERSONAL IDENTIFICATION MESSAGE 204

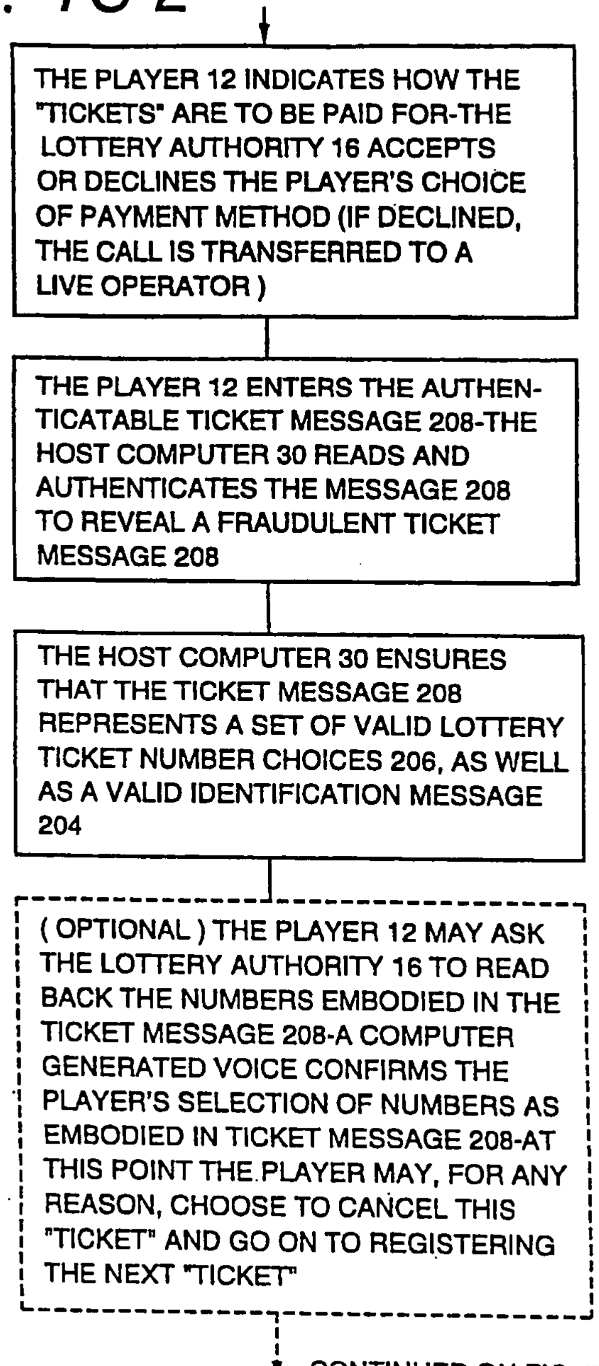
(OPIONAL) FOR ADDITIONAL VERIFICATION, THE PLAYER 12 ENTERS THE COMPUTER ID OR SOFTWARE ID CODE 212

THE LOTTERY AUTHORITY 16 ASKS THE PLAYER 12 TO SELECT FROM A MENU OF LOTTERIES STILL OPEN FOR TICKET PURCHASING- THE PLAYER 12 USES THE TELEPHONE PAD TO KEY IN A NUMBER INDICATING THE LOTTERY OF CHOICE

TO FIG. 7C-2

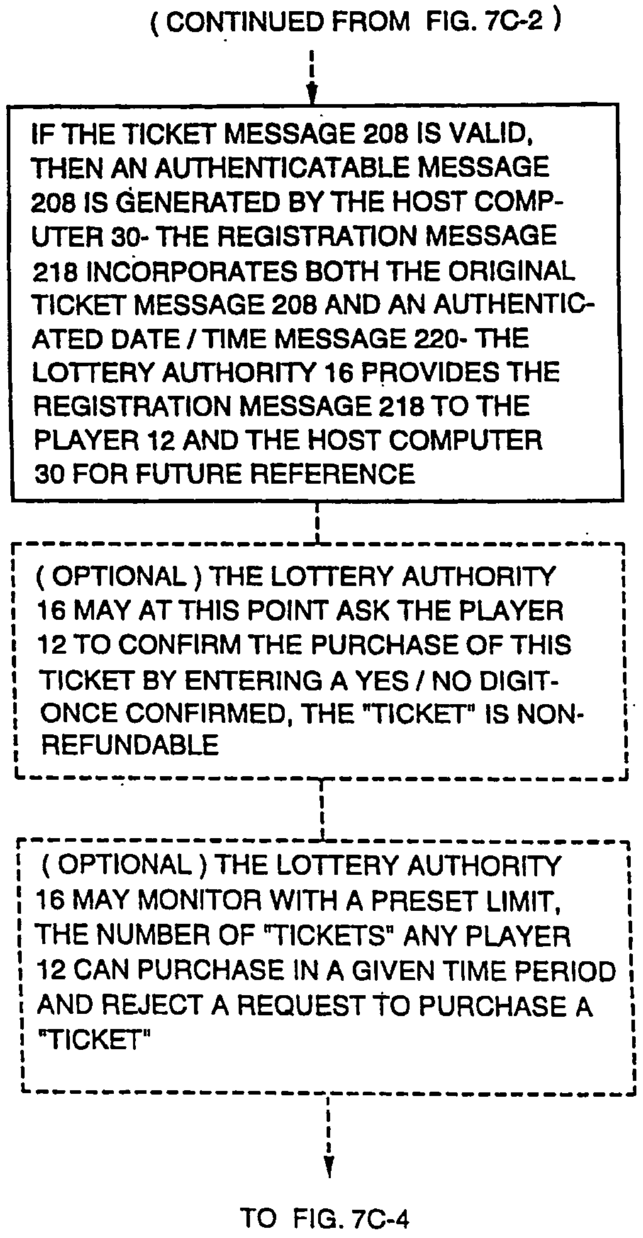
FIG. 7C-2

FROM FIG. 7C-1


THE PLAYER 12 INDICATES HOW THE "TICKETS" ARE TO BE PAID FOR-THE LOTTERY AUTHORITY 16 ACCEPTS OR DECLINES THE PLAYER'S CHOICE OF PAYMENT METHOD (IF DECLINED, THE CALL IS TRANSFERRED TO A LIVE OPERATOR)
THE PLAYER 12 ENTERS THE AUTHENTICATABLE TICKET MESSAGE 208-THE HOST COMPUTER 30 READS AND AUTHENTICATES THE MESSAGE 208 TO REVEAL A FRAUDULENT TICKET MESSAGE 208
THE HOST COMPUTER 30 ENSURES THAT THE TICKET MESSAGE 208 REPRESENTS A SET OF VALID LOTTERY TICKET NUMBER CHOICES 206, AS WELL AS A VALID IDENTIFICATION MESSAGE 204
(OPTIONAL) THE PLAYER 12 MAY ASK THE LOTTERY AUTHORITY 16 TO READ BACK THE NUMBERS EMBODIED IN THE TICKET MESSAGE 208-A COMPUTER GENERATED VOICE CONFIRMS THE PLAYER'S SELECTION OF NUMBERS AS EMBODIED IN TICKET MESSAGE 208-AT THIS POINT THE PLAYER MAY, FOR ANY REASON, CHOOSE TO CANCEL THIS "TICKET" AND GO ON TO REGISTERING THE NEXT "TICKET"

CONTINUED ON FIG. 7C-3

FIG. 7C-3



(CONTINUED FROM FIG. 7C-2)

IF THE TICKET MESSAGE 208 IS VALID, THEN AN AUTHENTICATABLE MESSAGE 208 IS GENERATED BY THE HOST COMPUTER 30- THE REGISTRATION MESSAGE 218 INCORPORATES BOTH THE ORIGINAL TICKET MESSAGE 208 AND AN AUTHENTICATED DATE / TIME MESSAGE 220- THE LOTTERY AUTHORITY 16 PROVIDES THE REGISTRATION MESSAGE 218 TO THE PLAYER 12 AND THE HOST COMPUTER 30 FOR FUTURE REFERENCE

(OPTIONAL) THE LOTTERY AUTHORITY 16 MAY AT THIS POINT ASK THE PLAYER 12 TO CONFIRM THE PURCHASE OF THIS TICKET BY ENTERING A YES / NO DIGIT- ONCE CONFIRMED, THE "TICKET" IS NON-REFUNDABLE

(OPTIONAL) THE LOTTERY AUTHORITY 16 MAY MONITOR WITH A PRESET LIMIT, THE NUMBER OF "TICKETS" ANY PLAYER 12 CAN PURCHASE IN A GIVEN TIME PERIOD AND REJECT A REQUEST TO PURCHASE A "TICKET"

TO FIG. 7C-4

FIG 7C-4

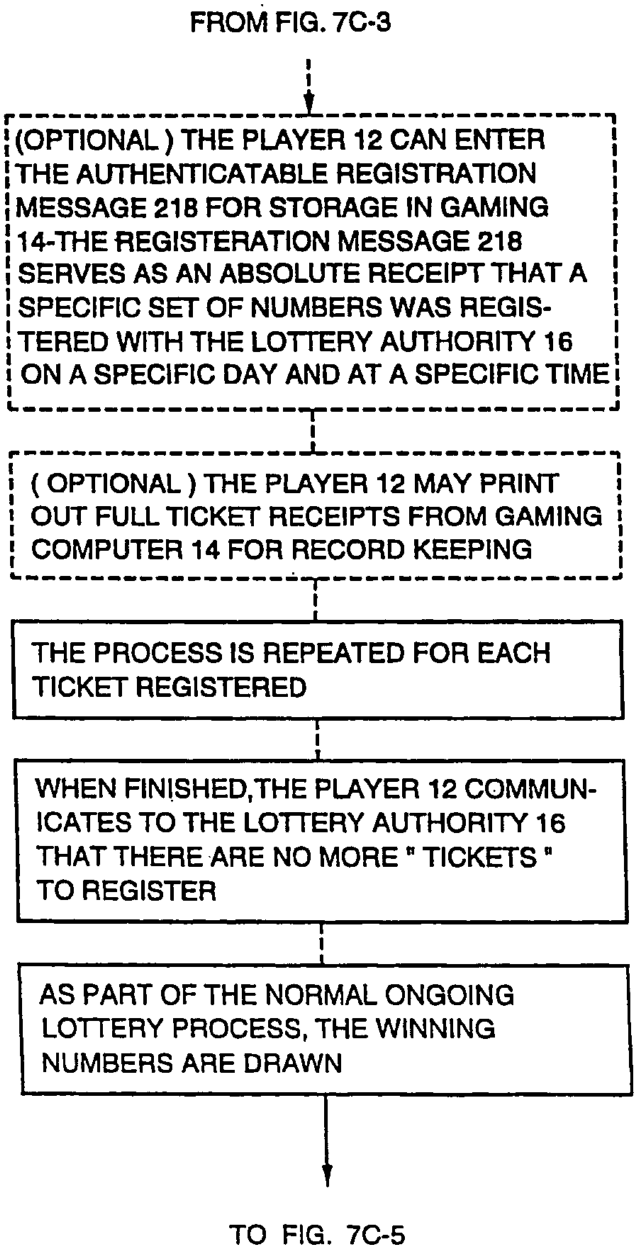
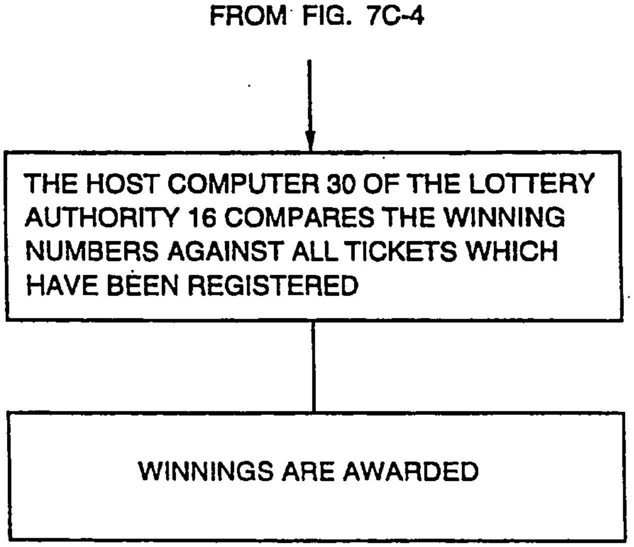
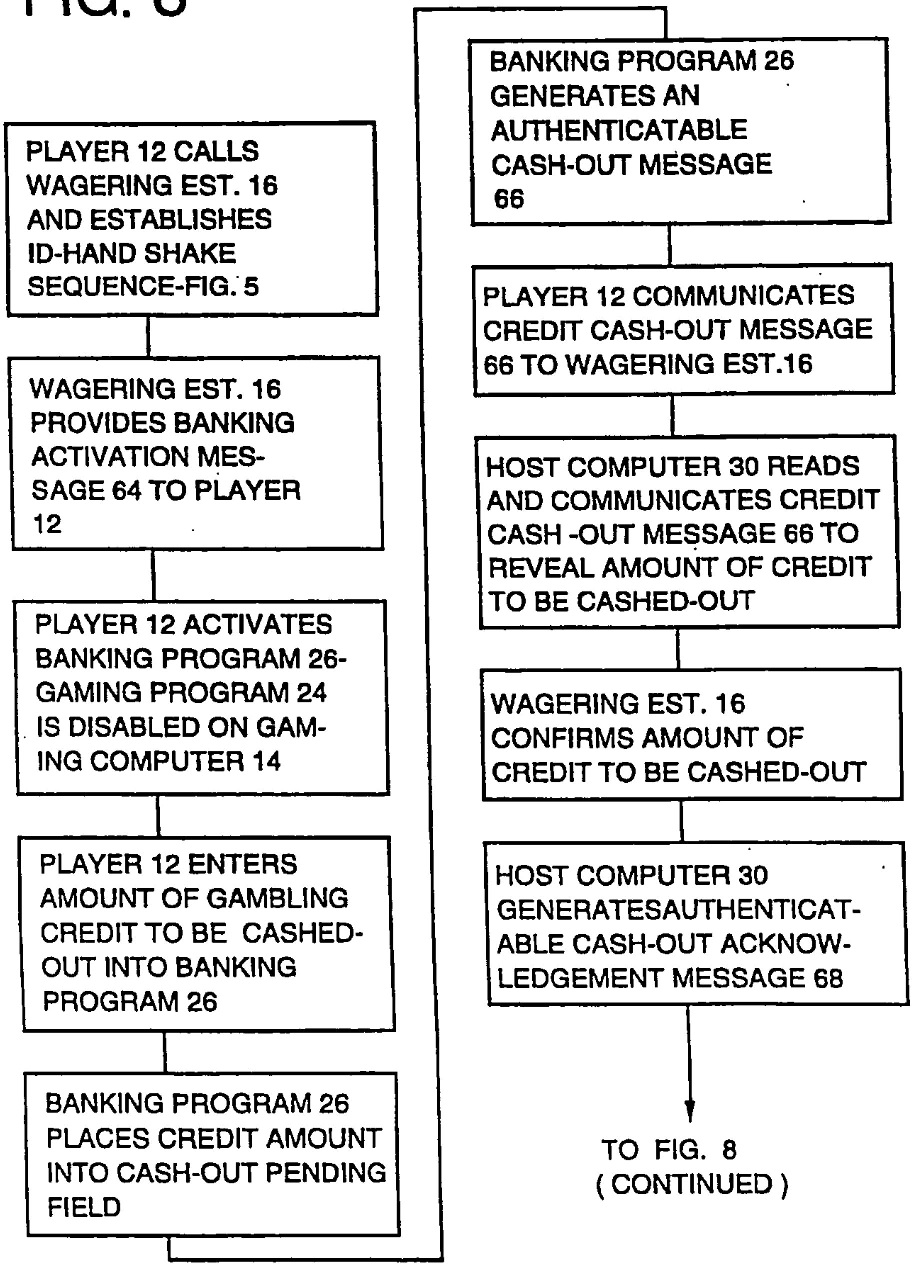

FROM FIG. 7C-3
(OPTIONAL) THE PLAYER 12 CAN ENTER THE AUTHENTICATABLE REGISTRATION MESSAGE 218 FOR STORAGE IN GAMING 14-THE REGISTERATION MESSAGE 218 SERVES AS AN ABSOLUTE RECEIPT THAT A SPECIFIC SET OF NUMBERS WAS REGISTERED WITH THE LOTTERY AUTHORITY 16 ON A SPECIFIC DAY AND AT A SPECIFIC TIME
(OPTIONAL) THE PLAYER 12 MAY PRINT OUT FULL TICKET RECEIPTS FROM GAMING COMPUTER 14 FOR RECORD KEEPING
THE PROCESS IS REPEATED FOR EACH TICKET REGISTERED
WHEN FINISHED,THE PLAYER 12 COMMUNICATES TO THE LOTTERY AUTHORITY 16 THAT THERE ARE NO MORE " TICKETS " TO REGISTER
AS PART OF THE NORMAL ONGOING LOTTERY PROCESS, THE WINNING NUMBERS ARE DRAWN
TO FIG. 7C-5

FIG. 7C-5


FROM FIG. 7C-4
THE HOST COMPUTER 30 OF THE LOTTERY AUTHORITY 16 COMPARES THE WINNING NUMBERS AGAINST ALL TICKETS WHICH HAVE BEEN REGISTERED
WINNINGS ARE AWARDED

CREDIT CASH-OUT SEQUENCE (OFF-LINE)

FIG. 8


PLAYER 12 CALLS WAGERING EST. 16 AND ESTABLISHES ID-HAND SHAKE SEQUENCE-FIG. 5
WAGERING EST. 16 PROVIDES BANKING ACTIVATION MES- SAGE 64 TO PLAYER 12
PLAYER 12 ACTIVATES BANKING PROGRAM 26- GAMING PROGRAM 24 IS DISABLED ON GAM- ING COMPUTER 14
PLAYER 12 ENTERS AMOUNT OF GAMBLING CREDIT TO BE CASHED- OUT INTO BANKING PROGRAM 26
BANKING PROGRAM 26 PLACES CREDIT AMOUNT INTO CASH-OUT PENDING FIELD
BANKING PROGRAM 26 GENERATES AN AUTHENTICATABLE CASH-OUT MESSAGE 66
PLAYER 12 COMMUNICATES CREDIT CASH-OUT MESSAGE 66 TO WAGERING EST.16
HOST COMPUTER 30 READS AND COMMUNICATES CREDIT CASH -OUT MESSAGE 66 TO REVEAL AMOUNT OF CREDIT TO BE CASHED-OUT
WAGERING EST. 16 CONFIRMS AMOUNT OF CREDIT TO BE CASHED-OUT
HOST COMPUTER 30 GENERATESAUTHENTICAT- ABLE CASH-OUT ACKNOW- LEDGEMENT MESSAGE 68
TO FIG. 8 (CONTINUED)

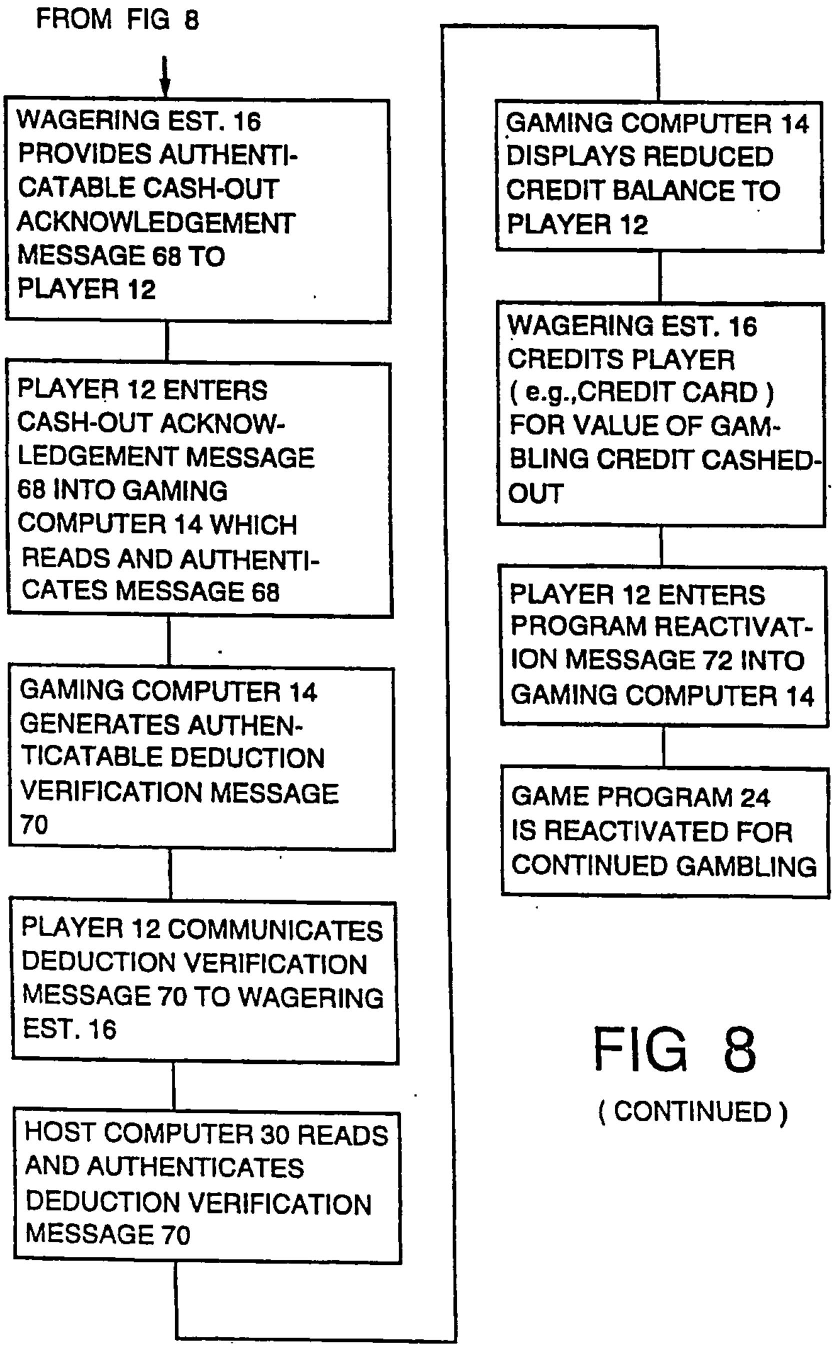
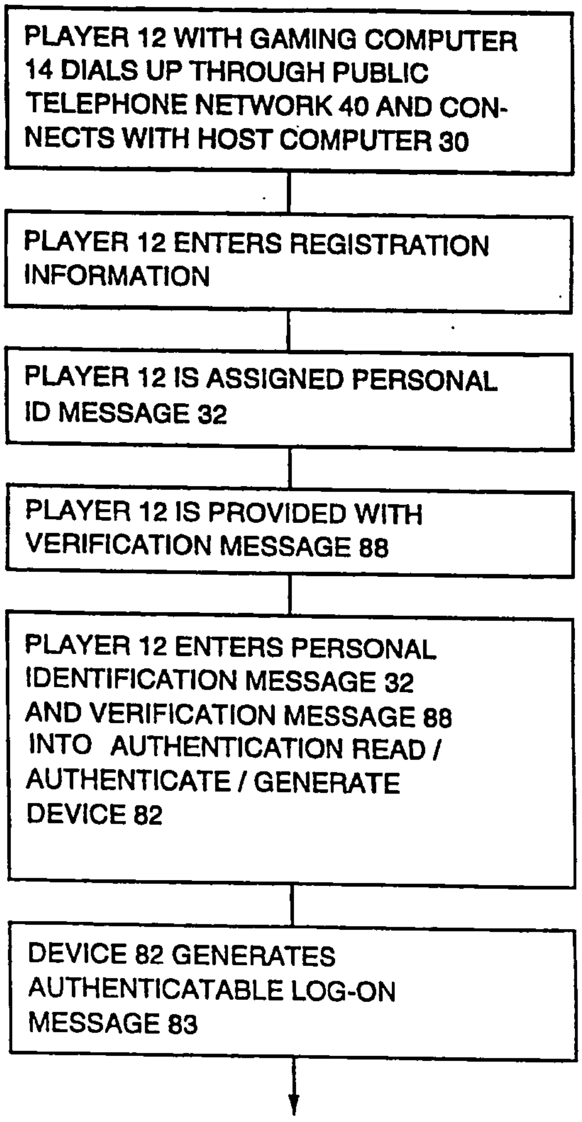

FROM FIG 8
WAGERING EST. 16 PROVIDES AUTHENTICATABLE CASH-OUT ACKNOWLEDGEMENT MESSAGE 68 TO PLAYER 12
PLAYER 12 ENTERS CASH-OUT ACKNOWLEDGEMENT MESSAGE 68 INTO GAMING COMPUTER 14 WHICH READS AND AUTHENTICATES MESSAGE 68
GAMING COMPUTER 14 GENERATES AUTHENTICATABLE DEDUCTION VERIFICATION MESSAGE 70
PLAYER 12 COMMUNICATES DEDUCTION VERIFICATION MESSAGE 70 TO WAGERING EST. 16
HOST COMPUTER 30 READS AND AUTHENTICATES DEDUCTION VERIFICATION MESSAGE 70
GAMING COMPUTER 14 DISPLAYS REDUCED CREDIT BALANCE TO PLAYER 12
WAGERING EST. 16 CREDITS PLAYER (e.g.,CREDIT CARD) FOR VALUE OF GAMBLING CREDIT CASHED-OUT
PLAYER 12 ENTERS PROGRAM REACTIVATION MESSAGE 72 INTO GAMING COMPUTER 14
GAME PROGRAM 24 IS REACTIVATED FOR CONTINUED GAMBLING

FIG 8

(CONTINUED)

START-UP AND REGISTRATION SEQUENCE

FIG. 9


PLAYER 12 WITH GAMING COMPUTER 14 DIALS UP THROUGH PUBLIC TELEPHONE NETWORK 40 AND CONNECTS WITH HOST COMPUTER 30
PLAYER 12 ENTERS REGISTRATION INFORMATION
PLAYER 12 IS ASSIGNED PERSONAL ID MESSAGE 32
PLAYER 12 IS PROVIDED WITH VERIFICATION MESSAGE 88
PLAYER 12 ENTERS PERSONAL IDENTIFICATION MESSAGE 32 AND VERIFICATION MESSAGE 88 INTO AUTHENTICATION READ / AUTHENTICATE / GENERATE DEVICE 82
DEVICE 82 GENERATES AUTHENTICATABLE LOG-ON MESSAGE 83

TO FIG. 9 (CONTINUED)

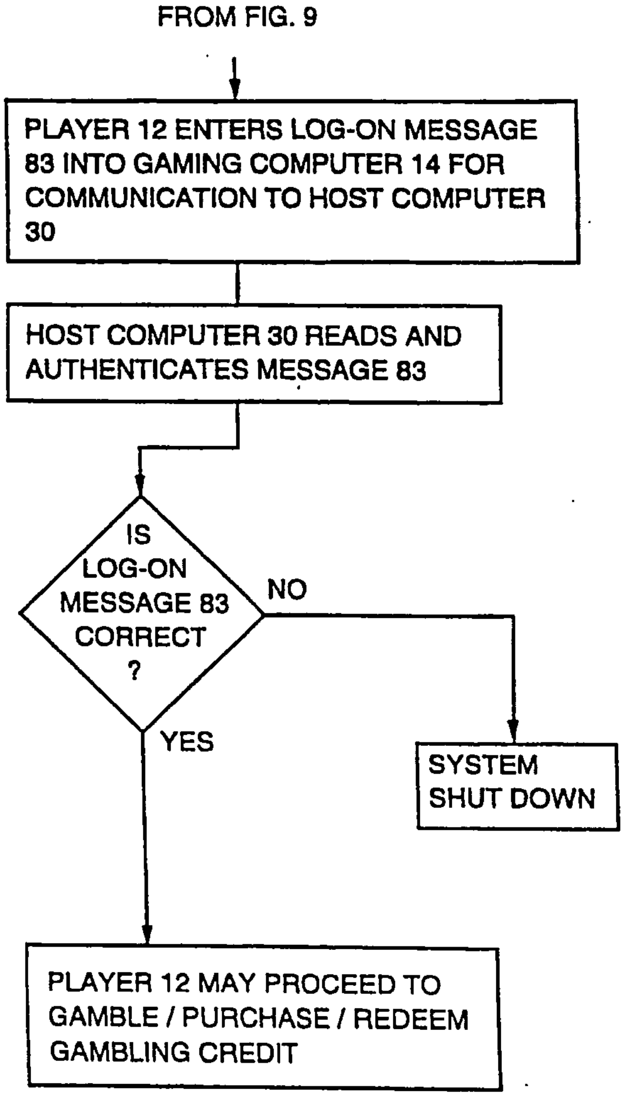
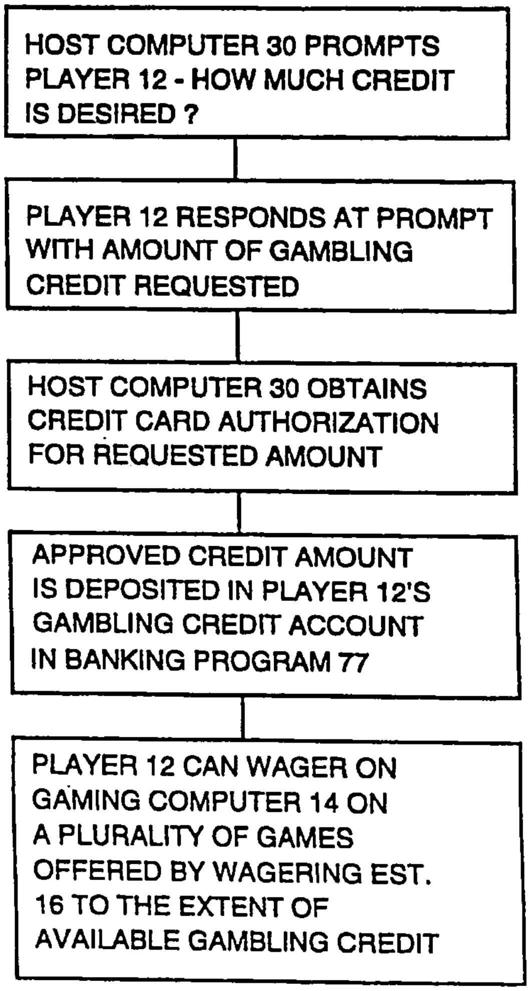

FROM FIG. 9
PLAYER 12 ENTERS LOG-ON MESSAGE 83 INTO GAMING COMPUTER 14 FOR COMMUNICATION TO HOST COMPUTER 30
HOST COMPUTER 30 READS AND AUTHENTICATES MESSAGE 83
IS LOG-ON MESSAGE 83 CORRECT ?
NO
SYSTEM SHUT DOWN
YES
PLAYER 12 MAY PROCEED TO GAMBLE / PURCHASE / REDEEM GAMBLING CREDIT

FIG. 9

(CONTINUED)

PURCHASE CREDIT SEQUENCE (ON-LINE)

FIG. 10



HOST COMPUTER 30 PROMPTS PLAYER 12 - HOW MUCH CREDIT IS DESIRED ?

PLAYER 12 RESPONDS AT PROMPT WITH AMOUNT OF GAMBLING CREDIT REQUESTED

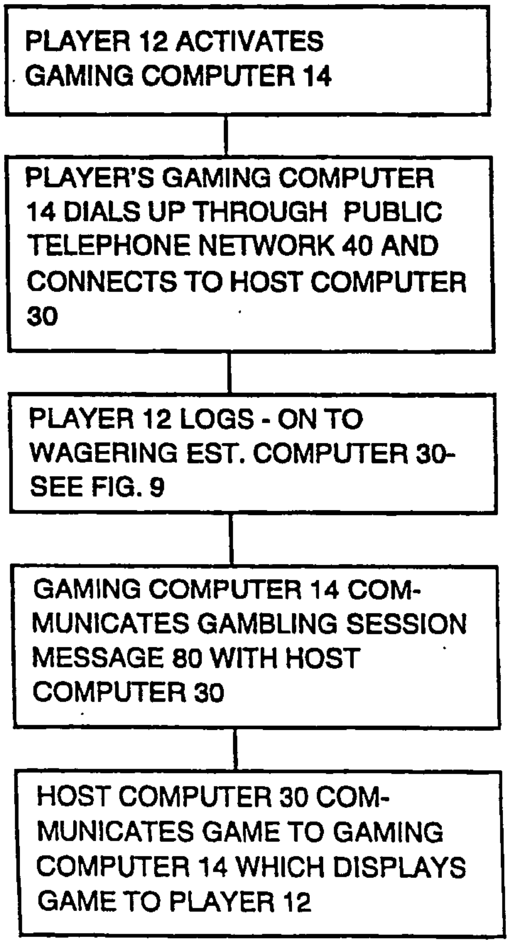
HOST COMPUTER 30 OBTAINS CREDIT CARD AUTHORIZATION FOR REQUESTED AMOUNT

APPROVED CREDIT AMOUNT IS DEPOSITED IN PLAYER 12'S GAMBLING CREDIT ACCOUNT IN BANKING PROGRAM 77

PLAYER 12 CAN WAGER ON GAMING COMPUTER 14 ON A PLURALITY OF GAMES OFFERED BY WAGERING EST. 16 TO THE EXTENT OF AVAILABLE GAMBLING CREDIT

WAGERING SEQUENCE (ON-LINE)

FIG. 11



PLAYER 12 ACTIVATES GAMING COMPUTER 14

PLAYER'S GAMING COMPUTER 14 DIALS UP THROUGH PUBLIC TELEPHONE NETWORK 40 AND CONNECTS TO HOST COMPUTER 30

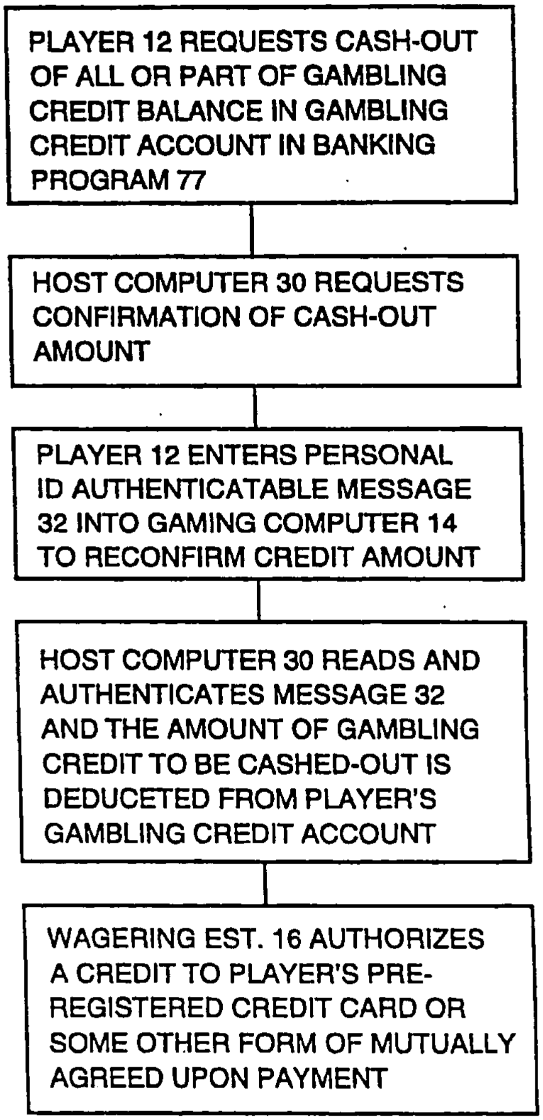
PLAYER 12 LOGS - ON TO WAGERING EST. COMPUTER 30- SEE FIG. 9

GAMING COMPUTER 14 COMMUNICATES GAMBLING SESSION MESSAGE 80 WITH HOST COMPUTER 30

HOST COMPUTER 30 COMMUNICATES GAME TO GAMING COMPUTER 14 WHICH DISPLAYS GAME TO PLAYER 12

CREDIT CASH-OUT SEQUENCE (ON-LINE)

FIG. 12


PLAYER 12 REQUESTS CASH-OUT OF ALL OR PART OF GAMBLING CREDIT BALANCE IN GAMBLING CREDIT ACCOUNT IN BANKING PROGRAM 77
HOST COMPUTER 30 REQUESTS CONFIRMATION OF CASH-OUT AMOUNT
PLAYER 12 ENTERS PERSONAL ID AUTHENTICATABLE MESSAGE 32 INTO GAMING COMPUTER 14 TO RECONFIRM CREDIT AMOUNT
HOST COMPUTER 30 READS AND AUTHENTICATES MESSAGE 32 AND THE AMOUNT OF GAMBLING CREDIT TO BE CASHED-OUT IS DEDUCETED FROM PLAYER'S GAMBLING CREDIT ACCOUNT
WAGERING EST. 16 AUTHORIZES A CREDIT TO PLAYER'S PRE-REGISTERED CREDIT CARD OR SOME OTHER FORM OF MUTUALLY AGREED UPON PAYMENT

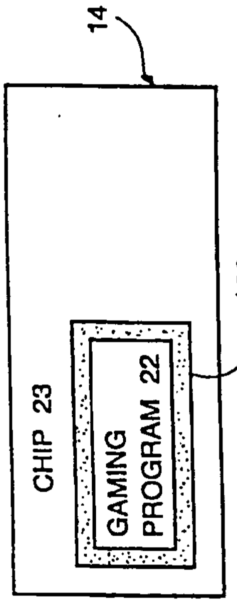

14
CHIP 23
GAMING PROGRAM 22
84 / 86

FIG. 13

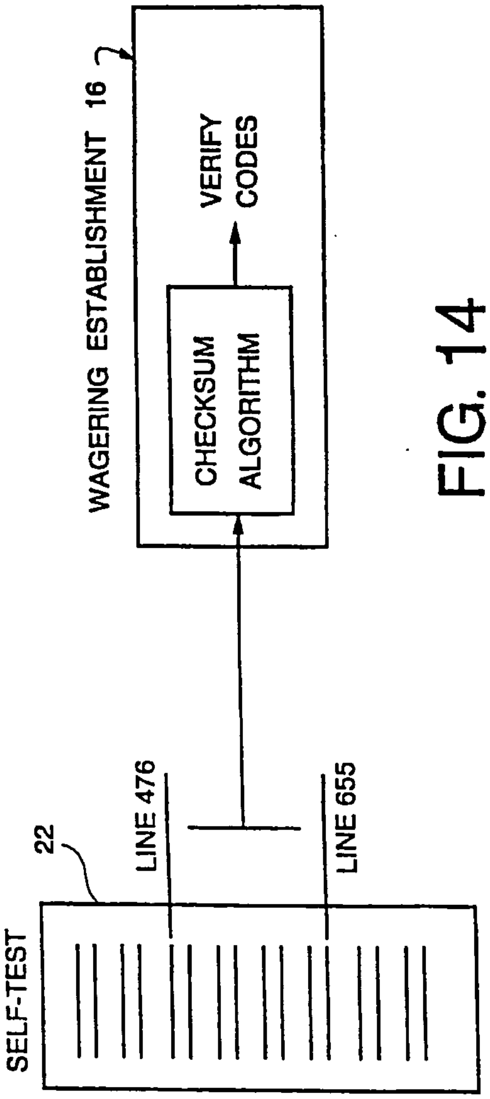

WAGERING ESTABLISHMENT 16
CHECKSUM ALGORITHM
VERIFY CODES
22
SELF-TEST
LINE 476
LINE 655

FIG. 14

FIG. 15A

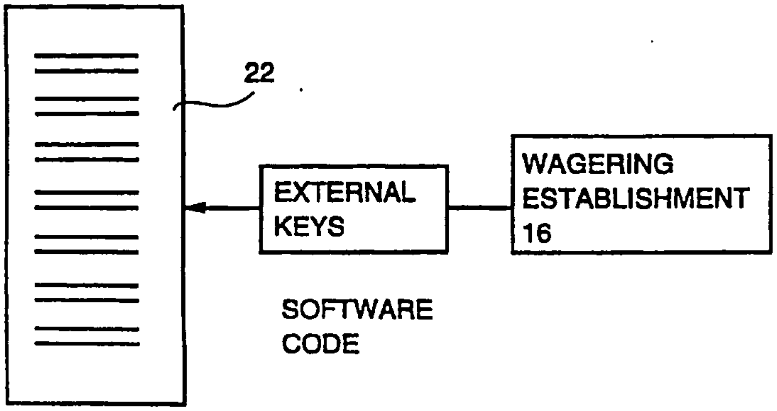


FIG. 15B

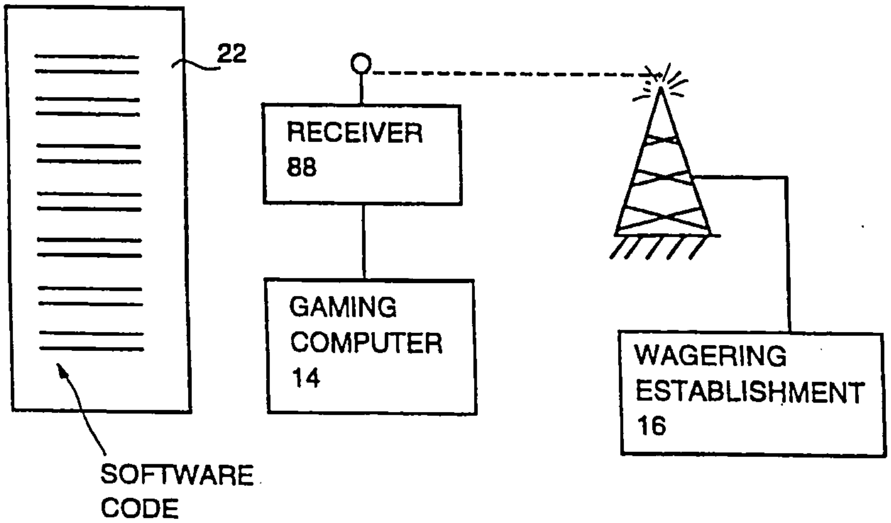


FIG. 15C

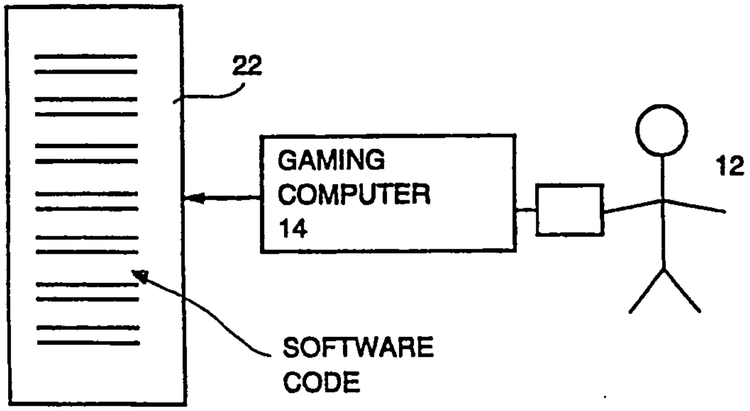
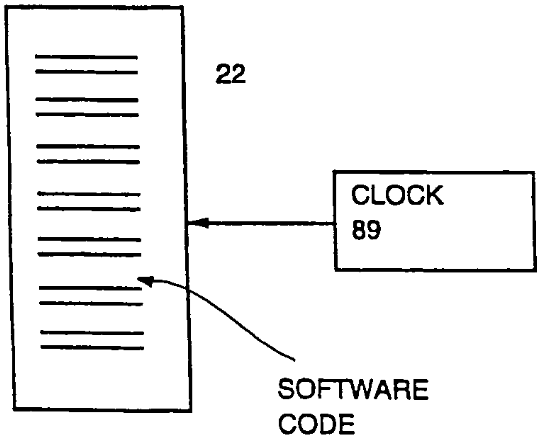


FIG. 15D



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/08206

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 155:00, 161:00
US CL :364/410
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/410, 411, 412; 235/375, 379, 380, 381; 380/3-4, 22-25; 273/433-436, 439, 138A, 138R; 382/115, 124

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,038,022 (LUCERO) 06 August 1991, see the abstract and figs. 1-4.	1-3, 5-11, 16-20, 37-39
Y	US, A, 4,317,957 (SENDROW) 02 March 1982, see the abstract, figs. 1-2.	1-3, 5-11, 16-20, 37-39
Y	US, A, 5,083,271 (THACHER ET AL) 21 January 1992, see the abstract and figs. 1-2.	10-11, 17-20, 38-39
Y	US, A, 5,096,195 (GIMMON) 17 March 1992, see the abstract and figs. 1-4.	12-15, 21-36
A, P	US, A, 5,351,970 (FIORETTI) 04 October 1994, see the abstract and fig. 2.	1-39
A, P	US, A, 5,413,357 (SCHULZE ET AL) 09 May 1995, see the abstract .	1-39

☒ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

11 SEPTEMBER 1995

Date of mailing of the international search report

25SEP1995

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
ROBERT A. WEINHARDT
Telephone No. (703) 305-3800

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/08206

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US, A, 5,380,007 (TRAVIS ET AL) 10 January 1995, see the abstract.	1-39

#3
3711

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277CIP

Examiner: Not yet assigned

Group: 3711

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail to: Commissioner for Patents, Washington, DC 20231 on July 26, 2002.

Signed: ______________
Mia Mitchell-Haynes

INFORMATION DISCLOSURE STATEMENT
37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
Washington, DC 20231

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 778
Berkeley, CA 94704-0778

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1/P-277CIP Applicant: Nguyen et al. Filing Date 4/3/02	Application No.: 10/116,424 Group 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	6,364,769	4/2/02	Weiss et al.	463	29	5/22/00
	A2	6,368,219	4/9/02	Szrek et al.	463	42	10/15/99
	A3	6,285,886	9/4/01	Kamel et al.	455	522	7/8/99

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	B1	US 2002/0049909	4/25/02	United States	713	188	X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

3711 #4 BI
11-29-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277CIP

Examiner: Not yet assigned

Group: 3711

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail to: Commissioner for Patents, Washington, DC 20231 on November 6, 2002.

Signed: ______________________
Latrice R. Williams

INFORMATION DISCLOSURE STATEMENT
37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
Washington, DC 20231

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 778
Berkeley, CA 94704-0778

Form 1449 (Modified)	Atty Docket No. IGT1P034X1/P-277CIP	Application No.: 10/116,424
Information Disclosure Statement By Applicant	Applicant: Nguyen et al.	
(Use Several Sheets if Necessary)	Filing Date April 3, 2002	Group 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	5,762,552	06/09/98	Vuong et al.	463	25	12/05/95
	A2						
	A3						
	A4						
	A5						
	A6						
	A7						
	A8						
	A9						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	B1							
	B2							
	B3							
	B4							
	B5							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	C1	
	C2	
	C3	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Pg. 1 of 1

3711

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277CIP

Examiner: Not yet assigned

Group: 3711

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail to: Commissioner for Patents, Washington, DC 20231 on January 10, 2003.

Signed:
Mia Mitchell-Haynes

INFORMATION DISCLOSURE STATEMENT
37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
Washington, DC 20231

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 778
Berkeley, CA 94704-0778

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1/P-277CIP Applicant: Nguyen et al. Filing Date April 3, 2002	Application No.: 10/116,424 Group 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	4,454,594	6/12/84	Heffron et al.	364	900	11/25/81
	A2	4,430,728	2/7/84	Beitel et al.	364	900	12/29/81
	A3	5,851,149	12/22/98	Xidos et al.	463	42	8/4/95
	A4	6,446,257	9/3/02	Pradhan et al.	717	154	2/4/99
	A5	6,099,408	8/8/00	Schneier et al.	463	29	12/31/96
	A6	6,453,319	9/17/02	Mattis et al.	707	100	4/5/00
	A7	6,449,687	9/10/02	Moriya	711	112	10/28/99
	A8	3,931,504	1/6/76	Jacoby	235	153	12/12/73
	A9	6,253,374	6/26/01	Dresevic et al.	717	11	7/2/98
	A10	6,454,648	9/24/02	Kelly et al.	463	16	11/3/99

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

3711

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Binh T. Nguyen, *et al.*

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277CIP

Examiner: Unassigned

Group: 3711

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on August 27, 2003 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Tomika Thomas
Tomika Thomas

INFORMATION DISCLOSURE STATEMENT
(37 CFR §§ 1.56 AND 1.97(c))

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Accompanying this Information Disclosure Statement is

☒ a statement as specified in 37 CFR 1.97(e); or

□ the fee set forth in 37 CFR 1.17(p).

The undersigned hereby states:

☒ that each item of information contained in the Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application no more than three months prior to the filing of the Information Disclosure Statement; or

□ that no item of information contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the Information Disclosure Statement.

Statement Under 37 CFR §1.704(d)

Each item of information contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application; this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 778
Berkeley, CA 94704-0778
(510) 843-6200

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277CIP **Applicant:** Binh T. Nguyen, *et al.* **Filing Date** April 3, 2002	**Application No.:** 10/116,424 **Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A	6,002,772	Dec. 14, 1999	Saito			Apr. 2, 1997
	B						
	C						
	D						
	E						
	F						
	G						
	H						
	I						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	J	1074955A2	07/02/2001	EPO			X	
	K	1061430A1	20/12/2000	EPO			X	
	L	0715245A1	05/06/1996	EPO			X	
	M	02/05229A2	17/01/2002	WIPO			X	
	N							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	O	
	P	
	Q	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 074 955 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
07.02.2001 Bulletin 2001/06

(51) Int Cl.7: G07F 17/32

(21) Application number: 00306668.5

(22) Date of filing: 04.08.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 04.08.1999 GB 9918427

(71) Applicant: MAYGAY MACHINES LIMITED
Wolverhampton, West Midlands WV10 9NL (GB)

(72) Inventor: Powell, David John
Wem, Shropshire SY4 5NX (GB)

(74) Representative: Hackney, Nigel John et al
Mewburn Ellis,
York House,
23 Kingsway
London WC2B 6HP (GB)

(54) Data transfer devices and methods

(57) In one aspect, the present invention provides a network of game machines (506, 508, 510, 514) including a central controller (500). The central controller is useable to receive data from the game machines and also to transmit data to the game machines, for example to upload new or corrected software to the game machines. Some of the game machines may be connected to the network via radio link (512). Higher baud rates, such as 10,000 baud, are acheivable with the network of the present invention.

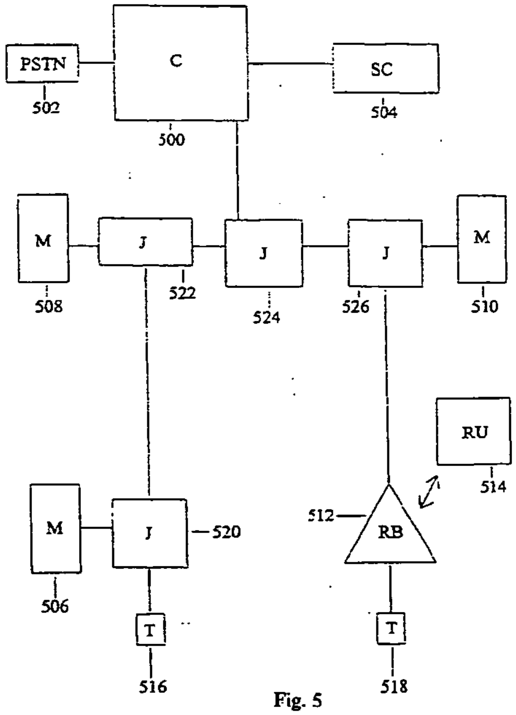


Fig. 5

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to transferring data to or from a cash or token operated machine, or between a plurality of cash or token operated machines. Each cash or token operated machine may, for example, be a vending machine or a game machine, for example a game machine used for gambling. The invention further relates to a network of cash or token operated machines, and a method of transferring data within the network.

[0002] A single site, e.g. a public place such as a public house, amusement arcade or railway station, may be provided with many cash or token operated machines, such as vending machines or game machines. In this context the term "cash or token operated machine" is traditionally used to mean any machine which delivers goods or a service upon receiving a payment (e.g. by a coin, a banknote, or a token such as a pre-purchased token or a credit or debit card), but nowadays can also include machines for which 'payment' is made remotely e.g. at a bar in a pub, and the machine is then given appropriate 'credits' and also machines which may be operated wholly or periodically without payment. The term is used in this specification in this broader sense.

[0003] Nowadays many, though not all, cash or token operated machines include a data processing unit. For example, a modern game machine conventionally includes a CPU communicating with many information output devices (lights, sounders etc.) and input devices (e.g. push buttons) based on game software which it reads from a memory device. Each coin or token operated machine at a given site may be designed, installed, or maintained by a different supplier, yet it is desirable for them to be able to communicate with a central location, to allow control, security or accounting operations to be performed centrally.

[0004] For example, it is known to connect a plurality of machines to a coordinator ("server") at a central location, so that each machine can transmit signals to the central location. The signals may include alarm signals (e.g. to indicate that a machine is being interfered with), financial information about the money taken by the machine, or information about the usage of the machine, e.g. statistical information concerning the number of plays made. The latter type of information is useful to identify when a machine is not being frequently used, to determine that it should be updated or replaced.

[0005] This data would be useful also off-site, for example to a designer of game machines, and for this reason it is known for the server to transmit data out of the network by telephone. In practise, however, the expense of doing this means that only a selection of the data available to the server is transmitted.

[0006] Conventionally the data received by the server is accumulated for later analysis. For example, in a case that it is to be transmitted out of the server by telephone, it is accumulated during the day and transmitted at night to reduce costs. Thus, if there is a power failure at the central location, the accumulated data may be lost or corrupted.

[0007] A known interface which transmits data out of a game machine (to the server) is called a "datapak". It is connected to the main processor of the game machine and receives data from the main processor at a standard rate of up to 1200 baud. No higher transmission rate is possible, due to the low power of a typical game machine processor. This interface can transmit data either by a permanent electrical connection (e.g. a wire to the server), or to at intervals a recording medium connected to the game machine by an operator.

[0008] In fact, since the concept of transferring data via an interface into a game machine has not so far been realised, local parameters are actually input by inserting an extra physical unit into the game machine, such as an extra ROM memory device or a mechanical "key".

[0009] At this point we should distinguish between game machines which merely entertain the user by sound and visual stimuli (for example video racing games), and those which provide the user with a potential financial return (i.e. gambling machines). The latter type are here referred to as "gaming machines".

[0010] An example of a game machine which is not conventionally a gaming machine is a pool table (a term used here to include a snooker or billiards table or similar). Conventionally pool tables contain little or no electronic circuitry, even the coin receiving mechanism being mechanical, so pool machines are not integrated into a site-wide accountancy system.

[0011] A popular form of gaming machine (often called a "fruit machine") employs spinning reels which are at least partly visible to a user, and generates complex electronic control signals to operate sounders and lights.

[0012] In the complex software of game machines (especially gaming machines) it is inevitable that bugs of various kinds will occur, leading to unwanted behaviour of the game machine. Some such bugs will come to light as the designer tests the software on a PC which emulates the low power processor of a game machine. The designer may eradicate these bugs by interrogating the emulator in the PC to determine exactly what has gone wrong, i.e. exactly what state the emulated the processor was in when the unwanted behaviour of the game machine occurred.

[0013] However, other bugs only become evident after extensive actual use of the game machine. For example, in the case of gaming machines, some bugs only generate unwanted effects in the event that the gaming machine reaches a rare configuration.

[0014] Furthermore, if the unwanted behaviour occurs after the game machine has been commercially released, or even during pre-release testing of the game at a commercial site, the game may acquire a commercial reputation for unreliability. In this case, even if the bug is corrected, the reputation of the game is hard to restore. For example, in the case of gaming machines, it is an unfortunate fact that many perfectly adequate gaming machines, which have been developed at great expense, are withdrawn from the market place and discarded simply because of an adverse commercial reputation caused by bug which has already been corrected.

[0015] Game software is frequently written so that it automatically produces run-time indicators of the usage and operation of the game machine, such as statistical information about how often a particular button is pushed or the values of (e.g. critical) registers at certain moments. These indicators are used when the game software is written, but once the software is installed in a real game machine it is hopeless to try to extract it using the interface since the volume of data is much greater than the capacity of the interface. Even if it were possible to transfer the indicator data out of the game machine into the network as mentioned above, it would not be practical to transmit it out of the network (e.g. to the writer of game machine software). For example, a given machine may generate 4Kbytes of indicator data every 10 minutes and the network may contain 127 machines, so that each day more than 20Mbytes of data would be generated

[0016] Apart from correcting bugs, there are other reasons why a game manufacturer modifies existing game software One of these is when he releases an improved version of a game In this case existing game machines are usually not supplied with the new game software; instead the new software is only provided in new game machines One reason for this is the sheer technical difficulty of installing replacement memory chips in off-site (i e away from the manufacturer's base) game machines Also. there are security issues involved in supplying memory chips containing proprietary software separately from game machines. Another reason for modifying software is to bring it into line with (e.g. new) legal requirements.

[0017] Security is of great importance in the installation of any cash or token operated machine, since there is a great potential (dishonest) profit available to an operative who succeeds in installing a machine incorrectly. Furthermore, an inadvertent installation error (operatives are not always highly skilled) may also lead to a loss by the operator of the machines. There is therefore a general need to control installation of machines to make it more secure and reliable, and to improve the accountability of operatives.

[0018] The present invention seeks to provide a new and useful game machine, and especially (though not exclusively) a game machine which is a gaming machine.

[0019] The invention further seeks to provide new and useful methods and devices for transferring data to and/or from a game machine or a cash or token operated machine.

[0020] The concept of transmitting game software to a game machine constitutes an independent aspect of the invention, which is a game machine including:

payment receiving means;
a writeable memory;
a processor for processing game software stored in the memory; and
an interface for receiving game software from outside the game machine, and writing it to the memory.

[0021] An operator may be able to program (usually re-program) the game machine, for example updating some or all of the game software to modify the game (e.g. to correct bugs, or to improve the pleasure of the game). For example, the game operator may be able to provide data to keep the game topical (e.g. with references to contemporary world events, personalities or other news), or with updated quiz questions.

[0022] If the manufacturer devises an improvement to the game software in the game machine (e.g. corrects a bug in the game software) he or she may be able to implement that improvement (e.g. correct the bug) by transmitting to the game machine through the interface replacement game software which includes the improvement (e.g. a debugged portion of the game software).

[0023] Within the scope of this aspect of the invention, a game machine which is a part of a network may be able to input the game software which it is to process from a central location (e.g. server)in the network, e.g. according to an instruction generated at the central location. This gives the operator of the network great flexibility, in determining which of a plurality of game machines is used to play which of a plurality of games stored at the cental location. The game manufacturer may be able to update the game software at the central location, for subsequent transmission to game machines.

[0024] Indeed, it is possible for new game software to be transmitted (e.g. from the central location of a network) whenever the game is used. That is, a plurality of games may be stored in a central location in communication with the central location, and an operator or the user may select one game which is then transferred to the machine for the user to play.

[0025] In a further aspect, the present invention provides a method of reprogramming a game machine according to this aspect of the invention by transmitting game software to the game machine.

[0026] In an aspect the invention proposes a game machine, having a data interface for transferring data into and/or out of the game machine or cash or token operated machine.

[0027] Preferably the interface permits a data transfer rate which is e.g. at least 10,000 baud, at least 100,000 baud, or at least, 1,000,000 baud. Preferably the baud rate is not over 10,000,000

[0028] Preferably, the interface transmits information both into and out of the machine.

[0029] In the case that the interface transmits information out of the machine, the interface preferably transmits indicators characterizing the operation of the game software. The indicators may include any one or more of (i) data characterizing when the machine is used, (ii) data (e.g. statistical data) on the timings at which the user inserts money or operates information input devices (e.g. buttons), (iii) the state of the display and/or sound generated by the machine at times when the user inserts money or operates information input devices, (iv) financial information concerning the cash or tokens received by the machine, and (v) data concerning the internal running of the game software (e.g. values stored in particular registers).

[0030] Preferably, enough information is transmitted out of the interface to reconstruct the play of the game. For example, at least enough information may be transmitted to reconstruct the display generated to a user of the machine and his reactions to that display. More preferably, the transmitted data allows identification of bugs in the software or other portions of the software which should be improved.

[0031] The information may be transmitted in real time (as the game is played) or stored in the memory and transmitted in bursts, e.g. with a predetermined timing (e.g. periodically) or in response to a triggering signal received from outside of the machine, e.g. through the interface.

[0032] The possibility of transmitting large amounts of data into a game machine or cash or token operated machine makes it possible to conceive of a possibility not envisaged in the literature, of transmitting not just parameters into the game machine but actually applications (that is game software consisting of instructions).

[0033] As a separate independent aspect of the invention, the interface may include data storage means e.g. memory. The data storage means may also have a battery backup power supply or other suitable power means in order to retain data in the data storage means in the event of a mains power failure. In this way data relating to, for example, the operation of the interface e. g. the protocols to be used, can be stored and updated as necessary.

[0034] Further independent aspects of the invention relate to using radio communication to transfer data into and/or out of a cash or token operated machine (especially a game machine), or between networks of cash or token operated machines. In some embodiments radio communication gives the advantage of secrecy, while in some embodiments it gives the advantage that one or more game machines can be easily integrated into a network (e.g. on a single site). In some embodiments, the radio communication device is a mobile telephone which can exchange data with a conventional mobile telephone network.

[0035] Specifically, in a third aspect, the invention provides (e.g. a cash or token operated) game machine including:

payment receiving means;
means for analysing usage of the game machine to generate usage data; and
a radio communication device for transmitting signals carrying said usage data out of the machine.

[0036] In a first embodiment, the data may be transmitted to a radio receiver on the same site, so that the game machine can be integrated with the data collection at that site. That is, one or more machines according to the third aspect of the invention may compose part of a system which includes a collating device (server) which receives radio signals from the machines and collates them.

[0037] For example, the game machine may be a pool table, such as a pool table which is not controlled by a processor. However, even though the game machine is not controlled by a processor, the means for analysing the usage of the game machine may include device(s) to monitor the usage of the game machine (e.g. a measuring device, such as an optoelectronic device, to measure when coins are inserted into a mechanical coin receiving device (so that the total take of the machine can be transmitted out of the machine), or to indicate the fall of the final ball of the game). The game machine may include a processor to analyse the usage data before it is transmitted out of the game machine.

[0038] This aspect of the invention can be particularly useful for game machines (e.g. a pool table) which are not powered by mains electricity or, even if they are capable of being powered by mains electricity, are situation in a location to which it is inconvenient to supply mains power. For such machines, in the absence of mains power it may be difficult to operate data transfer apparatus in accordance with other aspects of the invention. Often it will be more convenient to transfer data using a radio communication device in accordance with this aspect of the invention.

[0039] In a second embodiment, the data may be transmitted off-site, for example to a manufacturer of game machines.

[0040] Preferably, as in the first aspect of the invention, the game machine of the third embodiment includes a processor running game software.

[0041] In either embodiment, the communication device may just emit a certain signal once whenever the game software is run. Thus, an operator (on site or off site) can count how often the game is played by counting the emitted signals. Alternatively, the game machine might include means for storing information on how often the game is played and the communication device may transmit this stored information, for example periodically or in response to an interrogation signal (e.g. received by the radio device).

[0042] Alternatively or additionally, the data may be data (indicators) concerning the state of the game. For example, the data may be sufficient that an operator can use the signals to follow the play of the game from a remote location. A further possibility is that the data may describe any problems which have arisen during play (e.g. due to software bugs), and the configuration (internal state) of the game machine at that time, so that the receiver of the data can attempt to deduce the reason for the problem. In any of these cases, the receiver of the data may monitor features of the play, even if the game machine is located out of the premises of the manufacturer, for example during commercial testing of the game machine, or even once the game machine has been commercially released.

[0043] In fact, a fourth independent aspect of the present invention is a method of monitoring a game machine according to the third aspect of the invention, by receiving and analysing signals transmitted from it.

[0044] The communication device of the machine of the third aspect may also be capable of receiving radio signals. These signals may be signals to control the game machine. For example, the signal may be a signal activating the game machine (e.g. transmitted to the game machine to tum it on), or a signal which enables the game machine to indicate that the user has paid to use it. In this case the payment receiving means may just be a register recording that the enablement signal has been transmitted.

[0045] In a further example, the game apparatus may be arranged to run one of a number of games according to a signal received by the game machine via an interface.

[0046] Altematively, and preferably, the signals include game software, for example as described above. This may, for example, be done even without the knowledge of the keeper of the game machine. Thus, de-bugging is possible without even making public the existence of the bug.

[0047] The third aspect of the invention has been explained above in relation to transferring data by radio to or from a single game machine. However, alternatively there may be a plurality of game machines, arranged into one or more networks of electrically connected machines. Each network may optionally also include other components, such as other cash or token operated machines or data collators and storage devices. The one or more networks may transfer data off-site or between themselves by radio. In the latter case this means that even physically separated networks at a single site (e.g. on different storeys of the same building) can be coordinated.

[0048] Specifically, in a fifth aspect the invention may provide a network of game machines (e.g. cash or token operated machines), each including:

payment receiving means; and
means for analysing usage of the machine to generate usage data;
said machines being arranged in one or more groups of electrically connected groups, each group being provided with a radio communication device for receiving and/or transmitting signals carrying said usage data (e.g. off-site or to another of the groups).

[0049] Sixth, seventh and eighth aspects of the invention relate to transferring data into or out of a game machine or a network of game machines by providing them with an interface for communicating with a physical recording medium. In the case of the sixth and seventh aspects of the invention, the data is input to the game machine or network of game machines to configure the machine(s). Preferably, the data is accompanied by data identifying the operator (the holder of the recording medium).

[0050] Specifically, in a sixth aspect, the invention proposes that a (e.g. cash or token operated machine) game machine having payment receiving means includes a reader interface for reading data from a physical recording medium, the data including configuration data for determining operation of the machine.

[0051] Preferably, the recording medium is a smart card, and the reader interface is a smart card reader device for reading data from the smart card.

[0052] By means of the invention, an operative can install a new game machine by supplying it and then allowing it to read configuration data from the recording medium to configure it. Since the data is read from a recording medium, the installation is relatively simple compared to inserting extra mechanical components into the machine.

[0053] Furthermore, the recording medium (smart card) preferably includes identification data identifying the holder of the recording medium. The game machine may store this identification data, so that in the future it is possible to determine which operative set up the machine. Alternatively or additionally, if the game machine is part of a network of game machines, it may communicate the identification data out of the game machine into the network, so that (e.g. at a central location) the identity of the operative may be checked and optionally recorded. Since the operative must supply the identification data in order to complete the set-up of the game machine, the system is open to less abuse than the conventional system described above. Furthermore, the identification data can be used to check that the correct recording medium (smart card) is being used, thus reducing the chance of an error being made in set-up.

[0054] In a further aspect, the invention proposes a network of game machines, each machine having payment receiving means and being electrically connected to at least one coordinating device (e.g. at a central location of the site), the coordinating device including a reader interface for reading data from a physical recording medium, the data including configuration data for determining operation of the network.

[0055] The recording medium read by the coordinating device may carry the local information about the site, for example the price per unit of the game. The coordinating unit may transfer this data to the machine(s), for example when the machine is first installed or when the machine is first turned on. Thus, the recording medium read by the coordinating device may function as a key for the control of the entire network.

[0056] Preferably the recording medium read by the coordinating device contains identification data, so that it can be checked that it is the correct recording medium for that network. This makes it more difficult to incorrectly configure the network by using the recording medium of another site.

[0057] Preferably, the sixth and seventh aspects of the invention are combined, so that both a coordinating device (server) of a network has an interface for reading from the first recording medium, and at least one cash or token operated game machine includes an interface for reading data from a (e.g. respective) second recording medium. The installation of a new game device can then involve a coordinated process in which the operative inserts a second recording medium into the game machine(s) which transmits information to the coordinating device to identify the type of game machine which has been inserted The coordinating device reads local information from the first recording medium, and transmits it back to the game machine to configure it to operate according to the local standards.

[0058] The eighth and ninth aspects of the invention each relate to methods of handling reliably and economically within a network a high volume of generated data, such as the volume of data which can be generated by one or more game machines according to the first aspect of the invention

[0059] In an eighth aspect, the present invention proposes a network of

> one or more game machines, each machine generating data characterising the operation of the machine;
>
> at least one collating device receiving said data from the machines and including a data storage device, the collating device further including a writer interface for transferring the data to a recording medium.

[0060] The present invention makes it possible to transfer large amounts of data economically out of a network by incrementally. e.g. periodically, transferring it to a recording medium Thus it makes possible for example economical transmission out of the network of the volume of indicator data which one or more game machines according to the first aspect of the invention can transmit into the network, and which may then optionally be sent to a producer of game software.

[0061] In other words, in the eighth aspect of the invention the machines are preferably game machines according to the first aspect of the invention. That is, in contrast to a conventional game machine which transmits such a small amount of data into a network that telecommunications may be adequate to transmit the data out of the network, even if the game machines in the eight aspect of the invention are capable of transmitting a high level of data into the network (e.g. a game machine according to the first aspect of the invention) a network according to the eighth aspect of the invention is capable of transmitting it out.

[0062] In a ninth aspect, the present invention proposes a network of:

> one or more game machines, each machine including a writable memory device and each machine generating data characterising the operation of the machine;
>
> at least one collating device in two-way communication with the machines and including a writable memory device, the collating device receiving said data from the machines, writing data to its memory device, and re-transmitting data to the machines to store it in the respective memory devices of at least one (preferably more than one) of the machines, whereby if there is a power failure to one of the machines or to the collating device the data is not lost.

[0063] Preferably, the collating device also processes the data, and it is the processed data which it stores in its own memory device and stores in the respective memory devices of at least one of the machines.

[0064] Alternatively, instead of or in addition to the network including the collating device (and the data storage device associated with the collating device), one or more of the machines may each include data storage means (e.g. memory) for storing the type of data which would otherwise be transmitted on the network. In effect the data storage means can act as a buffer to store data relating to certain events or a certain time period, for example for later or periodic transmission over the network.

[0065] The feature of the data storage means is also particularly advantageous where some or all of the machines each include an external data port via which data can be accessed other than over the network.

[0066] In practical embodiments, this may be used for manual collection of the data e.g. at periodic intervals. For example, someone could connect to the data port a data collection device e.g. a hand-held unit and go to each machine in turn collecting the appropriate data. The data thus stored by the hand-held unit can then be processed remotely. In some embodiments, the data collection unit may also write data to the data storage means, for example, the date and time at which the data is collected. The internal clock of the data collection means may of course not be consistent with the clock of the network and so it could cause problems if these two clock times were confused. Accordingly, the data storage means preferably records the clock time of the hand-held storage device and compares it to the current clock time according to a network.

[0067] A further aspect of the present invention relates to the architecture and/or topology of the network used to link the machines. More particularly, the network includes a plurality of machines and each machines is linked to at least one other machine. Preferably only one of the machines (or one point on the portion of the network connecting the machines to each other) is in turn also connected to a controller e.g. a server. The server may be connected e.g. via a PSTN, ADSL or ISDN link to an external network. As described previously, the server may then be used to read and/or write data to each or all of the machines. This topology enables improved data communication as compared to the prior art topology.

[0068] As mentioned previously, one or more of the machines in the network may in fact be substituted by radio communication means for radio communication with equipment not directly included in the network. Preferably the machines of the network are connected in a line i.e. each of the machines is connected to only two other machines with the exception of the two machines one at each end of the network which are of course connected to only one machine. Preferably the or each end of the network is terminated in a suitable impedance. Preferably each machine receives all of the data being transmitted on the network. In a separate embodiment the machines may be connected in a loop i.e. each machine is connected to only two other machines.

[0069] As a separate aspect, one or more of the machines in a network may each include backup power supply means e.g. one or more batteries. The purpose of such a backup power supply is of course to enable some or all of the machine to continue to be able to function in the event of a mains power supply failure. Preferably the network controller includes power management means for managing the power consumption of a machine connected to the network in the event that the machine is disconnected from mains power. Preferably in the event of such a disconnection, the machine affected sends a suitable notification signal to the controller. The controller may then instruct the machine to terminate certain functions whilst maintaining other functions in order to conserve power consumption. Typically, the functions which will be maintained will be those relating to monitoring the security of the machine e.g. a tamper alarm etc.

[0070] The term "payment receiving means" is used throughout this document to include a coin receiving device (e.g. having a coin authenticating function), a banknote receiving device, a token receiving device which receives a pre-purchased token representing money or a credit or debit card (which is here regarded as a kind of token). In fact, it includes any device by which the user can pay to use the machine, or by which a signal is transmitted to the machine (e.g. through a network) to indicate that the user has paid to use the machine.

[0071] Preferably the game machine of the invention is a gaming machine, and includes payment dispensing means, such as coin dispensers, token dispensers, or means for transmitting a signal to an external device which acts on the signals to make a payment to the user. The game machine preferably includes information output devices (lights, sounders, spinning reels, etc), and information input devices (buttons, arms, pedals, etc).

[0072] It will be appreciated that while the above aspects have been explained in relation to game machines, preferably each or all are also applicable more generally to coin or token operated machines.

[0073] Any of the above aspects of the invention may be used in conjunction with any or all of the other aspects.

[0074] Embodiments of the invention will now be described, for the sake of example only, by reference to the accompanying figures, in which:

Fig. 1 shows schematically a first game machine according to the invention;

Fig. 2 shows schematically a network of cash or token operated machines;

Fig. 3 shows a second game machine according to the invention.

Fig. 4 shows a prior art network;

Fig. 5 shows a second embodiment of a network of the machines according to the present invention.

[0075] A first embodiment of a game machine 1 according to the invention is shown schematically in Fig. 1. It includes a coordinator unit (gate) 3 which coordinates transfer of data between a memory device 5 and a processor 7 (which may in fact consist of several physically separate processing units). The memory 5 includes at least a component of writeable memory.

[0076] The processor may for example be a Hitachi 32bit microprocessor from the family known as Super "H". The gate 3 may be a custom gate array. This gate is also able to provide a high speed multi element interchange interface for external I/O devices. The interface runs at 571KHz and can fully service all external resources in 128uS. The main system processor 7 has no connection with this process, all transfers are performed by the ASIC and data is read or written directly to/from the main battery backed static RAMs.

[0077] The game machine also includes a payment receiving device 9 (e.g. a coin receiver), and output devices such as sounders and lights (not shown). These may all be controlled by the processor 7, for example via the coordinator unit 3.

[0078] The game machine further includes a smart card reader 15, which can read data from a smart card inserted into it. The smart card data includes set-up data, for example setting a first configuration of the game machine, and/or portions of game software. The smart card data further includes identification data identifying the holder of the smart card.

[0079] The game machine further includes an interface 17 for interfacing the game machine with leads 19 which connect the game machine to a coordinating/collating device ("server") 21 (described below in relation to Fig. 2).

[0080] The coordinator device can read data (e.g. game software) from the network through electrical leads 19 and transfer it into the memory 5 without interaction by the processor 7 (e.g. on a time scale which is independent of the clock speed of the processor 7).

[0081] On receiving data from a smart card using the reader 15, the game machine can exchange data via the interface 17 with the rest of the network, for example to send information to the coordinating device 21 to identify the game machine. In particular, the identification data on the smart card may be stored within the memory device 5 and/or in the data storage device which is part of the coordinating device 21.

[0082] The game machine further includes a radio receiver and transmitter, including an aerial 11 and signal processing device 13.

[0083] The coordinator 3 may transmit data (e.g. statistical data) out of the game machine using radio signals transmitted by the aerial 11. It may receive data via radio signals received by the aerial 11. These radio signals may include control instructions (e.g. when the game machine is turned on or off) and/or game software. The coordinator 3 can transmit the game software into the writeable portion of the memory 5.

[0084] The aerial 11 and processor 13 may, in fact, be technologically compatible with a mobile telephone network. Thus, an operator of the game machine may be able to transmit or receive radio signals using a conventional mobile telephone network, for example by dialling a telephone number associated with the game machine. Similarly, the radio apparatus 11,13 may be able to dial up the game machine operator by transmitting a dialling request to a conventional mobile telephone network.

[0085] Turning to Fig. 2, a network of coin operated machines is shown, including a plurality of game machines 1 illustrated in Fig. 2. The network further includes an aerial 23 and corresponding signal processor 25 for receiving data transmitted from an on-site game machine which is not in electrical contact with the network (as described below in relation to Fig. 3), and a cash or token operated machine 27 which is not a game machine. In the figure, the various machines are shown connected to the coordinating device 21 by a single cable 19 arranged along a closed path, but there may in fact be many cables arranged in other formations (see for example Fig. 5).

[0086] The coordinating device 21 includes a processor 22 a data storage device 29, a smart card reader 31, a connection to a telephone line 33 and an aerial 35.

[0087] The coordinating unit 21 receives various data from the game machines 1 via the cables 19. For example, it may receive set-up data transmitted by the game machines from the smart card operator. At the same time, the coordinating device 21 may receive data identifying the game machine 1, for example data characterizing its requirements. Also, at this time the coordinating device 21 receives via the cables 19 from the game machine(s) identification data from a smart card read by the game machine. The coordinating unit 21 may store this identification data in a storage device 29, or alternatively transmit it (e.g. by telephone line 33), to the supplier of game machines for example.

[0088] A smart card stored on-site can be read by the reader 31 to insert a local information into the network. The coordinating device 21 may transmit this local information via the cables 19 to machines 1, 27, 40.

[0089] Information may be sent out of the network, e. g. to an adjacent network of equivalent form, using optional radio aerial 35.

[0090] When it is decided to update the software in the game machines, this can be done by a telephone signal transmitted by the supplier of games software along telephone cable 33 to the coordinating device 21, which re-transmits it along cable 19 to the game machine 1, where the game software is transferred through interface 17 and coordinator unit 3 to the memory 5.

[0091] In use, the game machines 1 generate large volumes of data (e.g. at least tens of Kbytes), and this is transmitted (e.g. after a temporary storage in the memory device 5) via the interface 17 to the network through cable 19, so that it is received by the coordinating device 21, optionally collated (e.g. formatted and analysed), and stored in the storage device 29. Accumulated data may be transferred using a data writing device 37 to a recording medium such as a diskette or zip disk, so that the recording medium can be transferred to the writer of games software to enable improvements to be made. Although as shown above, the smart card reader 31 and the writer 37 are separate units, it is alternatively possible to form them as a single unit which both reads from and writes to a recording medium.

[0092] The coordinating device (e.g. periodically) backs up the data stored in the storage device 2a by copying it to at least one of the game machines 1 to be written into the memory 5. Thus, even if the memory devices 29,5 are volatile the redundancy of storage means that the network as a whole is less vulnerable to loss of power (or other influences) at one or more points in the network. Optionally, the storage device 29 can be omitted and the system can rely entirely on the memory devices 5 of the game machines 1.

[0093] The game machine shown in Fig. 3 is a machine such as a pool table in which the game is not controlled (or only to a limited extent) by a processor. A measuring device 110 (e.g. an optical switch for counting coin input) is provided for obtaining measurements about the insertion of money into a payment receiving device (not' shown) or for measuring characteristics of the play. The measuring device 110 transfers data to a processor 117 which processes it, and transmits it to a signal processor 113 for generating a radio signal to be transmitted from the game machine using aerial 111.

The signal transmitted from aerial 111 is received by the aerial 23 of the network (shown on Fig. 2), decoded by the unit 25 and transmitted to the coordinating unit 21. Thus, the coordinating unit 21 is able to derive information (e.g. financial information) from the game machine 40 without a wire connection existing between the game machine 40 and the coordinating unit 21.

[0094] Fig. 4 shows a prior art network used to connect four gaming machines 400. Each of the gaming machines 400 is connected directly to a server 402 which in tum may be connected to a telephone line for transmission of data out of the network. Such a network typically had a maximum transmission rate of 1200 board.

[0095] By way of contrast, Fig. 5 shows a second embodiment of a network according to an aspect of the present invention. A central controller or server 500 is connected or connectable to an external network 502 (for example a PSTN or ISDN link). The server 500 also includes a smart card device 504 for reading or writing data to a suitable smart card.

[0096] Three game machines 506, 508 and 510 are connected to the network and thereby indirectly connected to the controller 500. As will be seen, machine 508 is effectively connected to both machines 506 and 510. Machine 506 is effectively at one end of the network and is therefore connected only to machine 508. Machine 510 is connected to machine 508 and a RF base station 512 which can be considered to take the place of a further fourth machine. Base station 512 is effectively at the other end of the network and is therefore only connected to machine 510.

[0097] Associated with RF base station 512 is an RF unit 514 which may be located in a further machine, possibly one which does not have ready access to mains power for example a pool table. Effectively therefore the pool table or other remote machine is incorporated into the network via an RF link between the base station 512 and the unit 514.

[0098] As will be seen from Fig. 5, the network can be considered to be in a "horseshoe" arrangement and the respective ends of the network are terminated by impedance terminations 516, 518. The impedance of terminations 516, 518 may be selected or adjusted so as to minimise reflections in the network.

[0099] In fact, as will be seen in Fig. 5, the machines 506, 508, 510 and RF base station 512 are not connected directly to each other by single cable runs but instead are interconnected via a series of junction boxes 520, 522, 524 and 526. Machines 506, 508 and 510 are associated with junction boxes 520, 522 and 526 respectively, whilst commander 500 is connected to the remainder of the network via junction box 524.

[0100] The embodiments above have been given for the sake of example only, and various modifications are possible within the scope of the invention.

Claims

1. A game machine including:

   payment receiving means;
   a writeable memory;
   a processor for processing game software stored in the memory; and
   an interface for receiving game software from outside the game machine, and writing it to the memory.

2. A network including a plurality of game machines according to claim 1 and a server for transferring the game software to the game machines.

3. A network according to claim 2 wherein the server is provided with a plurality of games selected ones of which are transferrable to selected machines for the users to play.

4. A cash or token operated game machine, having a data interface for transferring data into and/or out of the machine at a data rate of at least 10,000 baud.

5. A machine according to claim 4 wherein the interface is usable to transmit indicators characterizing the operation of the game software including any one or more of (i) data characterising when the machine is used, (ii) data on the timings at which the user inserts money or operates information input devices, (iii) the state of the display and/or sound generated by the machine at times when the user inserts money or operates information input devices, (iv) financial information concerning the cash or tokens received by the machine, and (v) data concerning the internal running of the game software.

6. A machine according to claim 4 wherein the interface is usable to transmit enough information to reconstruct a play of the game.

7. A machine according to claim 5 or claim 6 wherein the information is transmittable in real time (as the game is played) or is stored in a memory and transmitted periodically or in response to a triggering signal received from outside of the machine.

8. A machine according to any one of claims 4 to 7 wherein the interface includes data storage means and a backup power supply means in order to retain data in the data storage means in the event of a mains power failure.

9. A cash or token operated or game machine including:

   payment receiving means;

means for analysing usage of the machine to generate usage data; and
a radio communication device for transmitting signals carrying said usage data out of the machine.

10. A machine according to claim 9 which is not powered by mains electricity.

11. A machine according to claim 9 or 10 including means for storing information relating to operation of the machine and wherein the communication device is usable to transmit this stored information periodically or in response to an interrogation signal.

12. A machine according to claims 9 to 11 wherein the communication device is also capable of receiving radio signals.

13. A network including a machine according to any of claims 8 to 11 and a radio receiver and/or transmitter for receipt and/or transmission of radio signals to/from the machine.

14. A cash or token operated machine or game machine including a reader interface for reading data from a physical recording medium, the data including configuration data for determining operation of the machine.

15. A machine according to claim 14 wherein the recording medium is a smart card, and the reader interface is a smart card reader device for reading data from the smart card.

16. A machine according to claim 14 or 15 wherein the recording medium includes identification data identifying the holder of the recording medium.

17. A network including a plurality of cash or token operated machines being electrically connected to at least one coordinating device, the co-ordinating device including a reader interface for reading data from a physical recording medium, the data including configuration data.

18. A network including one or more cash or token operated machines, each machine including:

means for generating data characterising the operation of the machine;
at least one collating device receiving said data from the machines and including a data storage device, the collating device further including a writer interface for transferring the data to a recording medium.

19. A network according to claim 18 wherein each machine includes a writeable memory device and the collating device is in two-way communication with the machines and includes a writeable memory device, the collating device including means for receiving said data from the machines and writing data to its memory device, and means for re-transmitting data to the machines to store it in the respective memory devices of at least one of the machines, whereby if there is a power failure to one of the machines or to the collating device the data is not lost.

20. A network according to claim 18 or 19 wherein some or all of the machines each include an external data port via which data can be accessed other than over the network.

21. A network including a plurality of game machines, wherein each machine is linked to at least one other machine and only one of the machines is in turn connected to a controller.

22. A network according to claim 21 wherein each of the machines is connected to only two other machines with the exception of two machines one at each end of the network which are connected to only one machine.

23. A network according to claim 22 wherein the or each end of the network is terminated in a suitable impedance.

24. A network according to claims 21 to 23 wherein each machine receives all of the data being transmitted on the network.

25. A network according to claims 21 to 24 wherein one or more of the machines includes backup power supply means.

26. A network according to claim 25 wherein a network controller includes power management means for managing the power consumption of a machine connected to the network in the event that the machine is disconnected from mains power.

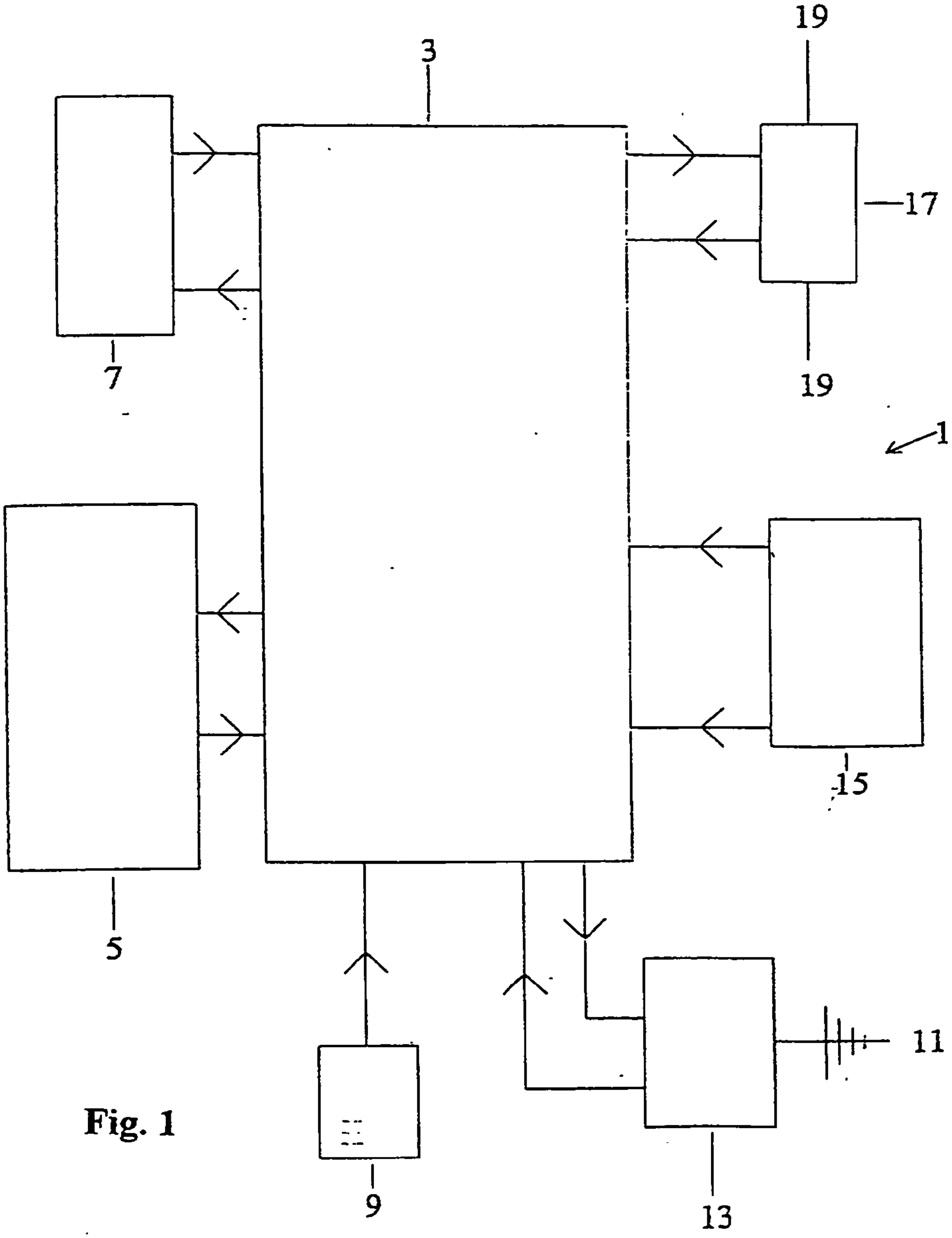


Fig. 1

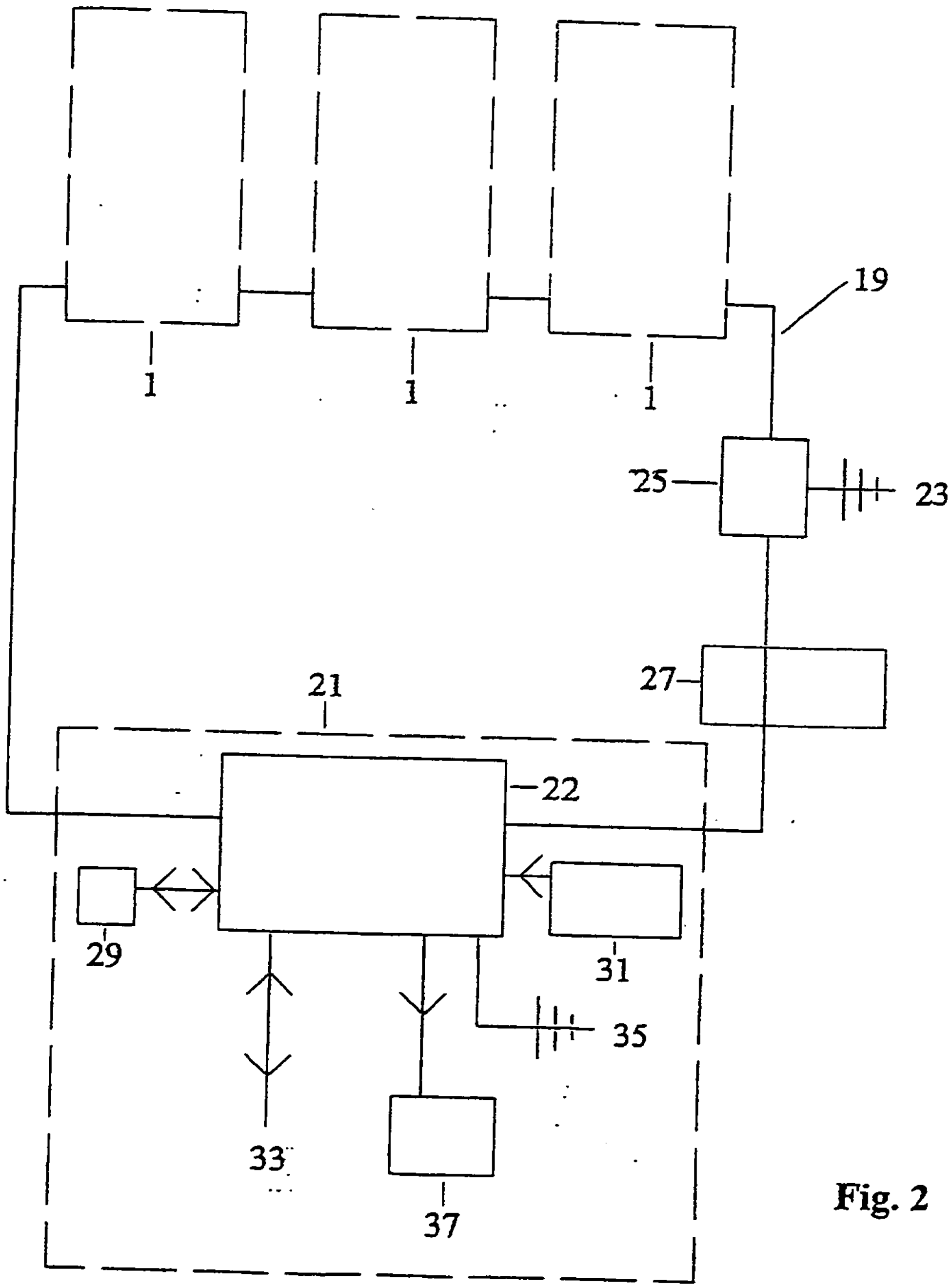
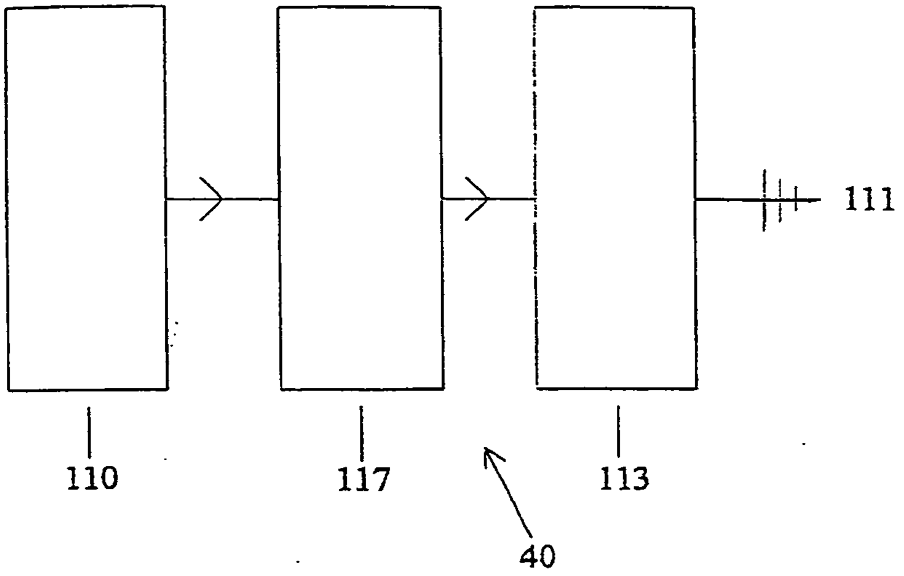


Fig. 2

Fig. 3



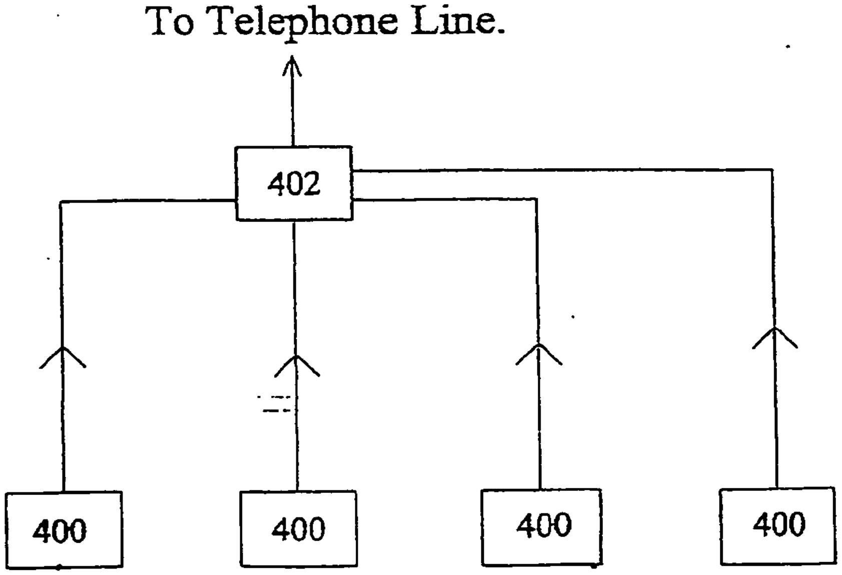


Fig. 4

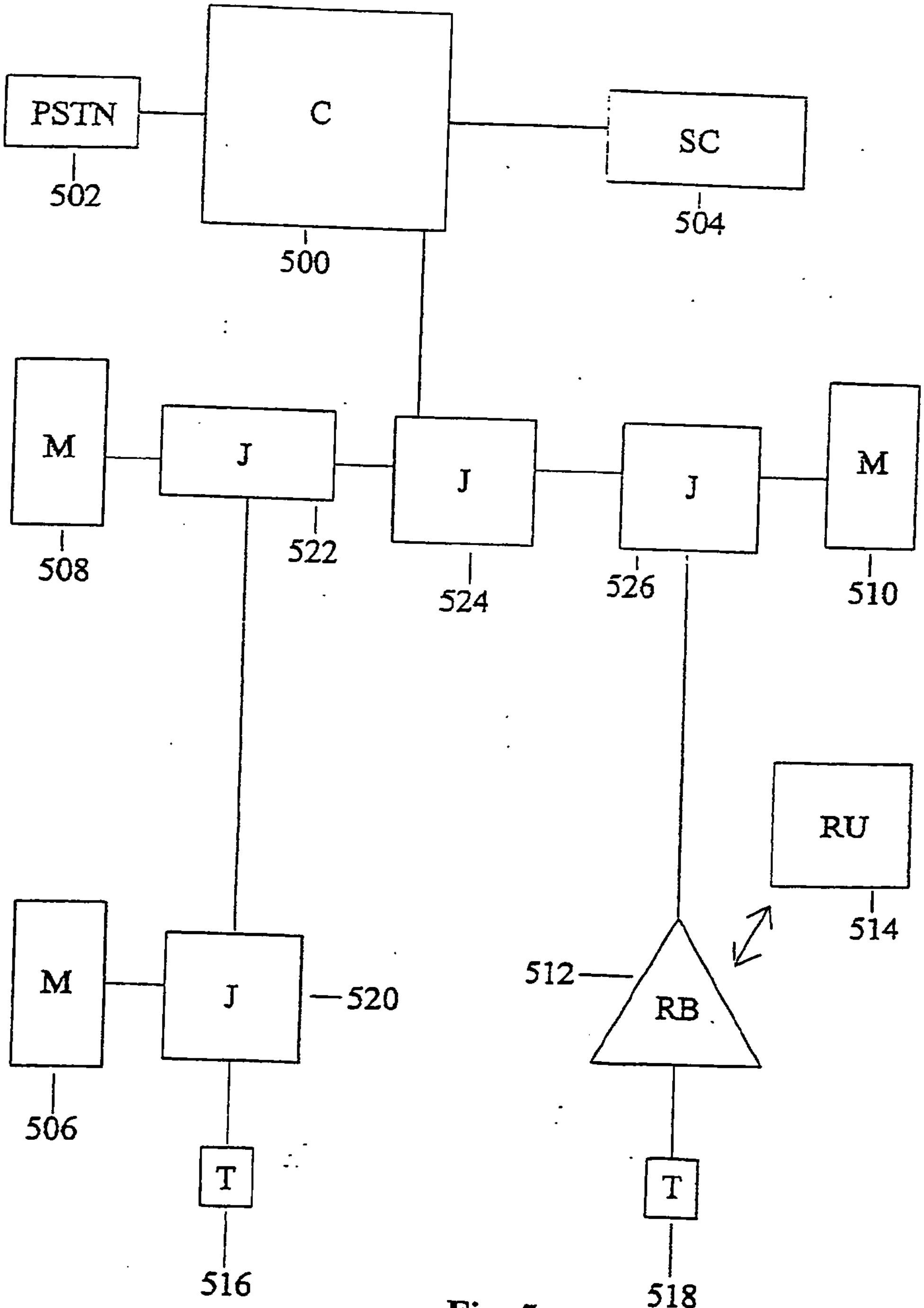

PSTN
502
C
500
SC
504
M
508
J
522
J
524
J
526
M
510
RU
514
512
RB
M
J
520
506
T
516
T
518

Fig. 5

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 061 430 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
20.12.2000 Bulletin 2000/51

(51) Int. Cl.^{7}: **G06F 1/00**

(21) Application number: **00109236.0**

(22) Date of filing: **28.04.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.06.1999 US 334436**

(71) Applicant:
Pulse Entertainment, Inc.
San Francisco, California 94105 (US)

(72) Inventors:
- **Bean, Richard**
  Cupertino, California 95014 (US)
- **Harvill, Young**
  San Mateo, California 94403 (US)

(74) Representative: **Betten & Resch**
Reichenbachstrasse 19
80469 München (DE)

(54) Software authorization system and method

(57) A system and method for controlling the access to one or more pieces of software developed using the developer's software is provided. The system permits the developer to receive revenue for use of the software without inconveniencing the customer or the user.

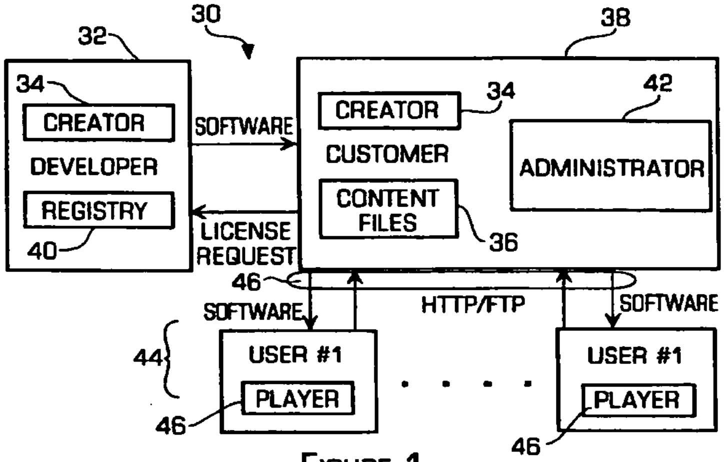


FIGURE 1

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

Background of the Invention

[0001] This invention relates generally to a system and method for controlling the access and use of a piece of software and in particular to a system and method for metering the access and downloading of a piece of software or content from a site.

[0002] For a developer of software, it is desirable to be able to track the usage of the software by users and customers in order to prevent piracy and ensure that the developer receives the licensing fee for the use of the software. In this description, the term "software" may refer to both software applications and content files, such as three dimensional animation files, video files, sound files and the like. It is especially hard to track the use of a piece of content since the content may be easily moved from one computer to another computer. The problem of trying to reduce piracy and to ensure the developer receives the appropriate compensation for use of the software is exacerbated by the World Wide Web (the Web) in which it is very easy to access a Web site and downloao a piece of software or content file.

[0003] In the past, developers required a person who purchased the software to attach a hardware dongle (a piece of hardware connected to a computer with a particular hardwired key inside it) to the computer so that only that computer is able to access the software. In particular, whenever the software is executed by the user, the software checked to determine if a hardware dongle is connected to the computer and to determine whether the key within the hardware dongle is correct. After the software confirmed that the hardware dongle with the correct key is attached to the computer, the software permit the user to use the software. The conventional hardware dongle does limit the use of the software, but is very cumbersome and annoying to the user. The hardware dongle requires the software developer to purchase the dongle and then either absorb the cost of the dongle or pass it on to the client so that it is most often used for more expensive software. In addition, the client may find the hardware dongle a major inconvenience since it makes it difficult to transfer the software to another computer if needed. The hardware dongle does work well for a single computer executing the software, but is less suited to a Web-based system in which the user of the computer may be downloading a piece of software from a Web site.

[0004] Another conventional software access limiter system involves forcing the user to go to an authorized Web site each time the user wanted a new piece of software. For example, a developer may sell a piece of software to a customer. The customer may want to display various content developed by the customer using the developer's piece of software. The developer wants to limit the display of that content in order to receive a license fee for its display. With this system, each time that a user wanted to view a particular piece of content, such as a three dimensional animation character, the user would be required to go to the developer's authorized Web site/server and enter a password in order to download and then view the content. This system is a major inconvenience for the user since the user does not want to have to go to a completely different Web site and enter a password in order to download the new content. This system may discourage a user from using the software.

[0005] Another conventional system involves a piece of security software resident on the server of the customer who creates the content or software. The security software meters the access to the content or software on the customer's site created using the developer's software. This system requires that the developer is permitted to install a piece of security software on the server of the customer. This system is therefore a major inconvenience to the customer as well as a security risk. In summary, the above systems do not permit the developer to receive his compensation for use of the software or content without becoming a major inconvenience to either the user or the third party. Thus, it is desirable to provide a software authorization system and method which avoids the above problems and limitations of the conventional systems and it is to this end that the present invention is directed.

Summary of the Invention

[0006] The software authorization system and method in accordance with the invention permits a developer to provide licensed software or content files to a customer where the license revenues to the developer increase as the scale of the customer's site expands because the authorization system is easily scaleable. The system may also permit license-free content to be displayed in a way that encourages customers to purchase a license. The system is transparent to the user of the customer's site so that the user is not inconvenienced. The customer also does not need to store an executable software application on the customer's site. The system also does not require a piece of hardware, such as a hardware dongle. The system also eliminates the need for the developer's site to be involved in any authorization transactions. The license granted by the system may be limited to a predetermined number or locations of the copies, such of a predetermined number of Web pages or a predetermined number of Uniform Resource Locators (URL's). The license granted using the system may also be time-limited. The system also ensures that an author of a software or content file is identified and that the file cannot be accessed without the author's permission.

[0007] In more detail, a developer may be paid a license fee by the customer so that a customer may display or execute the developer's software or content on the customer's Web site. The ability to display or execute the software or content is limited to a predetermined number of locations, such as Web pages, within a site, such as the Web site, of the customer. For example, the customer may pay for the right to display or execute the software or content on 10 Web pages which permits the customer to store the licensed software or content on ten different Web pages on the customer's site. To specify the locations of the licensed software or content, the customer may enter the addresses of the locations (e.g., the URL's of the Web pages) into a master key provided by the developer. The customer may update the master key at any time to increase the number of authorized locations. When a user downloads the licensed software or content from the customer's site, the software executing on the user's computer (known as the Player) may also download the master key and compare the master key to the downloaded licensed software or content file. Based on the comparison, the player application in the user's computer determines whether or not the software or content may be executed or displayed.

[0008] Thus, in accordance with the invention, a system for controlling the execution of a piece of software developed by a developer on a site of the customer is provided. The system comprises a customer site comprising one or more locations containing one or more pieces of software of the developer, a master key purchased by the customer that specifies the one or more locations on the site of the customer where the software is located wherein the master key is stored at a particular location on the site of the customer. Each piece of software of the developer contains a content key that identifies location of the master key. The system further comprises a user computer comprising means for determining if the execution of the piece of software downloaded from the customer's site is authorized by the developer wherein the determining means comprises means for downloading the piece of software from the customer's site, means for determining the location of the master key based on the content key in the piece of software, means for downloading the master key from the determined location and means for comparing the locations contained in the master key to the location of the piece of software to determine if the piece of software is accessible by the user computer.

Brief Description of the Drawings

[0009]

Figure 1 is a block diagram illustrating a software authorization system in accordance with the invention;

Figure 2 is a block diagram illustrating an example of the customer's creation tool in accordance with the invention;

Figure 3 is a block diagram illustrating an example of the software authorization in accordance with the invention;

Figure 4 illustrates an example of the software/content authorization in accordance with the invention;

Figure 5 illustrates another example of the software/content authorization in accordance with the invention;

Figure 6 illustrates another example of the software/content authorization in accordance with the invention;

Figure 7 is a diagram illustrating a master key in accordance with the invention;

Figure 8 is a flowchart illustrating a method for creating authorized software/content files in accordance with the invention; and

Figure 9 is a flowchart illustrating a method for executing the authorized software/content files in accordance with the invention.

Detailed Description of a Preferred Embodiment

[0010] The invention is particularly applicable to a Web-based content file/rich media asset authorization system and method and it is in this context that the invention will be described. It will be appreciated, however, that the system and method in accordance with the invention has greater utility, such as to other types of software files. The system may also be implemented using a variety of different communications mediums and systems.

[0011] Figure 1 is a block diagram illustrating a software authorization system 30 in accordance with the invention. The system may include a developer's site 32 that may be a Web server containing pieces of software that may be used by a customer to generate/store various software or content. For example, the pieces of software may include software tools, such as a creator 34, which permits a customer (also referred to as an author herein) to create one or more content files 36 (also known as rich media assets) on a customer site 38. The content files may be, for example, a file containing media data which may be stored on a Web server 38 and then displayed to users of customer's Web server when the content file is downloaded to a user's computer. The developer's site 32 may also include a registry 40 that permits the developer to track the licenses provided to the one or more customers as described below in more detail. The developer's site 32 may communicate the various pieces of software, such as the creator 34, to the customer's site 38 after the customer has executed an appropriate license agreement. In the example shown, the software may be the creator 34.

[0012] When the customer executes a license agreement, the customer may specify a location on the site where a master key in accordance with the invention may be stored so that each content file created by the creator 34 may be directed to that location to locate the master key. The location of the master key may be known as the master key uniform resource locator (URL). The customer operating the customer's site may use the creator 34 to create the one or more content files 36. As each content file is created on the customer site having a particular master key, the creator 34 may embed a content key in the content file that specifies the location of the master key URL that may then be used for authorization purposes as described below. The customer's site 38 may also include an administrator 42 which controls the access to the content files in accordance with the invention. In a preferred embodiment, the administrator may be embedded within the creator 34. As described below in more detail, the customer may order a master key with a predetermined number of authorized Web pages or domain names so that the created content files may be stored on the authorized Web pages or domain names. The authorized content files may then be downloaded to the users of the customer's site. In accordance with the invention, only content files embedded in the authorized Web pages or domain names may be displayed or executed on the users' computers.

[0013] One or more users 44 (User #1 - User #N) may access to the customer's site 38 by a communications network 46, such as the Internet or the World Wide Web, so that each user may access the content files embedded in the Web pages of the customer's site and download the content files. Each user computer may communicate with the customer's site using a well known communications protocol, such as the hypertext transfer protocol (HTTP) or the file transfer protocol (FTP). Once the user has downloaded the content files, the user may execute or display the content files using another piece of software. For example, the user may download a free software application 46, known as a player software application, which interprets the content files and displays a three dimensional animated character on the user's computer provided that the customer is authorized to distribute the content files. If the content file has not been authorized, the user may see an error message or may see the content with a watermark which identifies the content file as being free and not authorized. Once the content file becomes authorized, the watermark may disappear so that the user may view the content without the watermark. Now, an example of the creator application in accordance with the invention will be described.

[0014] Figure 2 is a block diagram illustrating an example of the customer's creation tool 34 in accordance with the invention that may be used by the customer to generate authorized content files. In this example, the creator 34 may be provided free to the customer by the developer and may permit the customer to develop and create content files. In more detail, the creator 34 may be a Web authoring tool that is executed by the CPU of the customer's computer, that supports various output formats (DXF, VRML and 3D Studio files) and that generates a rich media asset 50. In a preferred embodiment, the creator 34 may be completely integrated with a Web page using hypertext markup language (HTML) and JavaScripts. In this example, the rich media asset may be a content file containing information about a three dimensional animated character which may be animated on a user's computer. The rich media asset in this example may include a geometry portion 52, an audio portion 54, a behavior portion 56 and a watermark portion 58. The geometry portion 52 may contain a geometrical description of the three dimensional animated character and the audio portion 54 may contain audio track data which may be synchronized to the movement of the three dimensional animated character. The behavior portion 56 may contain information about the movements and actions of the three dimensional animated character and the watermark portion 58 may contain the watermark which is displayed with the three dimensional animated character file unless the rich media asset is downloaded from an authorized Web page or domain name. Now, an example of the authorization system will be described.

[0015] Figure 3 is a block diagram illustrating an example of the software authorization system 30 in accordance with the invention. As described above, the developer's site 32, the customer's site 38 and the user's computer 44 are shown connected to each other. The developer's site 32 may include the registry 40 which receives license requests from the customer and generates the master keys for customers (including the location of the master key on the customer's site). In particular, each customer may register to use the rich media assets it generates using the creator application on one or more URL addresses (Web pages) within a domain name by executing the licensing agreement and agreeing to pay the license fees. The master key generated by the registry may be received by the administrator 42 on the customer's site 38. As the customer generates rich media assets using the creator 34, the customer, using the administrator 42, may plug the URL addresses where Web pages that embed the rich media assets are located into the master key to generate a Web master key. The customer's site 38 may also store the free player software application 46 which may be used by user's computers 44 to display the rich media asset. If the master key matches the content key stored in the rich media asset, then the watermark is not shown to the user otherwise the user views the watermark that indicates that the rich media asset is not properly licensed and that obstructs the display of the rich media asset or views an error message.

[0016] The user's computer 44 may include the player application 46 downloaded from the customer's site and a browser application 60 from communicating with the customer's site. The browser application may be any typical browser application. In a preferred embodiment, the player application may be a plug-in to the browser application. When the user downloads a rich media asset from the customer, the player application determines if the rich media asset is authorized and either displays the watermark or an error message if the rich media asset is not authorized or display the rich media asset if it is authorized as described below in more detail. Now, several examples of customer sites with authorized content/software will be described.

[0017] Figure 4 illustrates an example of the software/content on a customer's site in accordance with the invention. In this example, the rich media asset may be licensed to a unique domain name (as specified by the customer) which permits changing content to be contained on a predetermined number of Web pages (addressed by unique URL's). The content in this example may include animated talking spokesman for a product, digital guides and animated on-line personalities. In this example, the content may be displayed in a pop-up window 70 which pops up in front of a Web page window 72, in a window 74 within the Web page 72 or in a window within a frame 76 of the Web page 72. Each of the windows 70, 74, 76 may be counted as a single authorized use of the content so that the example has three authorized uses. Now, another example of a customer site with authorized content will be described.

[0018] Figure 5 illustrates another example of the software/content authorization in accordance with the invention. In this example, one or more links 80-84 to the licensed content may be contained in a domain name page 86 with a unique URL. In particular, the page 86 may contain a selection of products wherein each product may be animated using a rich media asset. The links 80- 84 on the page 86 may transfer the user to one or more separate Web pages 88, 90, 92 which contain the animated product selected by the user. In this example, the rich media asset may include interactive, animated products that demonstrate themselves, interactive advertising or original content syndicated from a single source. Now, another example of a customer's site with authorized content will be described.

[0019] Figure 6 illustrates another example of the software/content authorization in accordance with the invention wherein a similar or identical rich media asset 100 may be displayed on one or more different domain names or URL's 102, 104, 106. For example, the same content may be syndicated to a predetermined number of unique domain names or URL's. An example of the content may be a interstitial banner advertisement which may be displayed on a plurality of different Web pages. Each URL or domain name may be an authorized use of the content file. Now, an example of the master key in accordance with the invention will be described.

[0020] Figure 7 is a diagram illustrating an example of a screen for modifying a master key 108 in accordance with the invention which permits the developer to receive its compensation for execution or display of the content files downloaded from the customer's site. The master key is very dynamic so that it can be used for a variety of different licensing schemes. The master key contains data specified by the developer at the time of purchase of the license (that cannot be modified by the customer because it is encrypted) and data that is modifiable by the customer in order to authorize specific Web pages, URL addresses and domain names. The screen permits a master key Web URL 109 to be specified by the developer based on information provided to the developer by the customer. The master key Web URL may not be modified by the customer. Once the master key Web URL is specified in the master key, all content files created using the creator application on the customer's computer will contain a content key which contains the master key Web URL so that the player may determine if the content is authorized. A checkbox 110 permits the customer to specify that content files within the same domain as the master key may be displayed even if the actual URL's do not appear on the authorized Web page list in the master key. These content files will be displayed with a watermark indicating they were not explicitly authorized.

[0021] A second checkbox 111 permits the customer to specify that the player application may display the content file from any Web page if the content file is in the player's file system domain (e.g., the URL starts with "file://"). These check boxes are provided as a convenience for the customer to take advantage of during the development and testing of the content before they know the intended URL's. They are not part of the normal use for production assets.

[0022] A listing 112, that may be modified by the customer, permits the customer to specify the URL's that contain authorized content files as a list of Web page authorization slots. The number of Web page authorization slots and the expiration date for each slot is determined by the developer based on the type of license paid for by the customer. For example, a typical purchase option may be to buy 10 slots that are each good for one year from the purchase date (June 7, 2000 in this example since the master key was purchased on June 7, 1999), but any other purchase option is also possible. The customer may then fill in the URL's with the content files into the list. Each URL identifies a Web (HTML) page that is authorized to display the content files that are linked to this master key by the content key. In this example, the customer has specified two URL's with authorized content files. In the third slot shown in Figure 7, the customer has specified a partial feature (only if the partial feature is purchased by the customer) that authorizes any Web pages in the domain (http://www.pulse3d.com/ in this example) to be authorized to contain a content file. The master key thus permits the developer to provide one or more different licensing options to a customer which may be specified using the encrypted master key. Now, a method for generating an authorized rich media asset in accordance with the invention will be described.

[0023] Figure 8 is a flowchart illustrating a method 116 for creating authorized software/content files in accordance with the invention. In step 118, the customer may purchase a master key from the developer which permits a predetermined number of different URL's to store the rich media asset. The actual number of URL's authorized by the master key may be adjusted depending on the licensing fee paid by the customer. For example, the customer may buy a master key that authorizes 10 URL's or a master key that authorized 100 URL's. Thus, the master key may be easily scaled to accommodate the growth of the customer. To purchase the master key, the customer provides the developer with the license fee, a customer identifier, a master key URL and an executed license agreement. The master key URL is the location on the customer's Web server where the master key is located. The master key delivered to the customer may be an encrypted file that identifies the customer identifier, the master key URL and the number of authorized Web pages along with their expiration dates, and whether the customer has purchased the partial URL option.

[0024] In step 120, the customer may develop rich media assets using the developer's free creator software application. The creator software application may generate a content file containing the rich media asset along with a content key which identifies the master key URL. The content key may also contain information identifying and crediting the author of the rich media asset. The content files generated by the creator may be encrypted so that the content key cannot be changed by the customer or any other party. In step 122, the customer may place/store each rich media asset on a particular Web page that has a unique URL and that will invoke the player plug-in in the user's computer to display the rich media asset. Next, the customer may enter the URL's of the Web pages which contain the rich media assets into the master key using the administrator application in step 124. The URL's specified in the master key now have authorized rich media assets. The administrator may convert the master key with the URL's into a master Web key. The customer may then place the master Web key on the Web server at the location identified by the master key URL (previously specified in the original purchase of the master key) in step 126 The rich media assets contained on the URL's identified in the master Web key are now authorized rich media assets so that, when the user attempts to view the rich media assets on those Web pages, the user sees the rich media asset and not an error message or a watermark. Now, a method for a user to display the content/software created using the developer's software will be described.

[0025] Figure 9 is a flowchart illustrating a method 130 for executing the authorized software/content files in accordance with the invention. This method assumes that the user already has downloaded the player application necessary to view the content or software. If the user has not previously used the player application, it may be downloaded free from the customer's site and plugged into the user's browser application. In step 132, the user may view the customer's Web page (using the URL) which contains software or content created by the developer's software. In step 134, the user may download the software or content from the Web page using a well known transfer protocol, such as the hypertext transfer protocol (HTTP) to a location locatable by the player plug-in. After the software or content is downloaded, the player plug-in may review the content key in the downloaded content or software and determine if a master URL is present in step 135. If the master URL is not present, then the player plug-in may execute or display the downloaded content/software with a watermark indicating that the content/software was created without a license. If the master URL is present in the content key, the player plug-in may attempt to download the master Web key and determine if the master Web key is successfully downloaded in step 136.

[0026] The player plug-in may display an error message to the user in step 138 if the master key was not found indicating that the downloaded content/software cannot be validated. If the master key was properly downloaded, then the player plug-in may determine if the master key authorizes the URL of the Web page containing downloaded software or content in step 142. If the URL is authorized by the master key, the player plug-in displays or executes the software or content in step 144. If the content/software is not from an authorized Web site, the player plug-in may determine if the domain of the site is authorized in step 148. If the domain name is authorized, the player plug-in may play/execute the software/content with a watermark in step 133. If the domain is not authorized, the player plug-in may determine if the downloaded content/software being executed/displayed is already resident on the user's persistent storage in step 148 and may display/execute the software content with the watermark in step 133. If the software/content is not already on the persistent storage device of the user, the player plug-in may generate an error message in step 150 indicating that the downloaded software/content is not authorized and therefore may not be displayed or executed by the user. This method may be repeated each time a user wishes to display or execute software or content controlled by the software authorization system in accordance with the invention.

[0027] In summary, user access to the content or software developed by the developer's software in accordance with the invention is controlled by the comparison of the content key in the software or content created by the customer using the developer's software and the master key of the customer. Thus, the system and method permits the developer to control access to the content or software created by the developer's software without a hardware dongle or a piece of software executing on the customer's site. At the same time, the system ensures that the developer is receiving the proper amount of money for the generation of the software or content using the developer's software.

[0028] While the foregoing has been with reference to a particular embodiment of the invention, it will be appreciated by those skilled in the art that changes in this embodiment may be made without departing from the principles and spirit of the invention.

Claims

1. A system for controlling the execution or display of an asset on a customer's site, the asset being developed using a developer's software, the system comprising:

    a customer site comprising one or more locations containing one or more assets, a master key purchased by the customer from the developer that specifies the one or more locations on the site of the customer where the software is located wherein the master key is stored at a particular location on the site of the customer, each asset containing a content key that identifies the location of the master key; and
    a user computer comprising means for determining if the execution or display of the asset downloaded from the customer's site is authorized by the developer, the determining means comprising means for downloading the asset from the customer's site, means for determining the location of the master key based on the content key in the asset, means for downloading the master key from the determined location on the customer's site and means for comparing the locations contained in the master key to the location of the asset to determine if the asset is accessible by the user computer.

2. The system of Claim 1, wherein the location of each of the one or more assets comprises a Web page having a unique URL.

3. The system of Claim 1, wherein the locations of the one or more assets comprises a domain name.

4. The system of Claim 1, wherein the master key and the content key are encrypted.

5. The system of Claim 1, wherein the asset comprises a rich media asset containing information about an animated character.

6. The system of Claim 2, wherein the master key further comprises a customer identification number, a URL of the master key and a listing of the URL's of the Web pages authorized by the customer.

7. The system of Claim 6, wherein the master key further comprises, for each URL, a time period during which the Web page is authorized to be displayed to the user.

8. The system of Claim 6, wherein the user computer further comprises means for generating an error message if the asset is not authorized by the master key and means for generating a watermark covering the asset if the domain name is authorized, but the URL is not authorized.

9. The system of Claim 1, wherein the customer site further comprises means for adding more URL's into the master key to authorize more locations.

10. The system of Claim 1, wherein the customer site further comprises means for creating the asset comprising means for embedding the content key into the asset when the asset is created.

11. A device for controlling the execution or display of an asset downloaded from a customer's site , the asset being developed using a developer's software, the device comprising:

    means for downloading the asset from a customer's site wherein the customer site comprises one or more locations containing one or more assets, a master key purchased by the customer from the developer that specifies the one or more locations on the site of the customer where the software is located wherein the master key is stored at a particular location on the site of the customer, each asset containing a content key that identifies the location of the master key;
    means for determining if the execution or display of the asset downloaded from the customer's site is authorized by the developer, the determining means comprising means for determining the location of the master key based on the content key in the asset, means for downloading the master key from the determined location on the customer's site and means for comparing the locations contained in the master key to the location of the asset to determine if the asset is accessible by the user computer; and
    means for displaying the asset if the asset is authorized.

12. The device of Claim 11, wherein the location of each of the one or more assets comprises a Web page having a unique URL.

13. The device of Claim 11, wherein the locations of the one or more assets comprises a domain name.

14. The device of Claim 11, wherein the master key and the content key are encrypted.

15. The device of Claim 11, wherein the asset comprises a rich media asset containing information about an animated character.

16. The device of Claim 12, wherein the master key further comprises a customer identification number, a URL of the master key and a listing of the URL's of the Web pages authorized by the customer.

17. The device of Claim 16, wherein the master key further comprises, for each URL, a time period during which the Web page is authorized to be displayed to the user.

18. The device of Claim 16 further comprising means for generating an error message if the asset is not authorized by the master key and means for generating a watermark covering the asset if the domain name is authorized, but the URL is not authorized.

19. The device of Claim 11 further comprising means for adding more URL's into the master key to authorize more locations.

20. A method for controlling the execution or display of an asset on a customer's site, the asset being developed using a developer's software, the method comprising:

downloading an asset from a customer site comprising one or more locations containing one or more assets, a master key purchased by the customer from the developer that specifies the one or more locations on the site of the customer where the software is located wherein the master key is stored at a particular location on the site of the customer, each asset containing a content key that identifies the location of the master key;
determining if the execution or display of the asset downloaded from the customer's site is authorized by the developer, the determining comprising determining the location of the master key based on the content key in the asset, downloading the master key from the determined location on the customer's site and comparing the locations contained in the master key to the location of the asset to determine if the asset is accessible by the user computer.

21. The method of Claim 20, wherein the location of each of the one or more assets comprises a Web page having a unique URL.

22. The method of Claim 20, wherein the locations of the one or more assets comprises a domain name.

23. The method of Claim 20, wherein the master key and the content key are encrypted.

24. The method of Claim 20, wherein the asset comprises a rich media asset containing information about an animated character.

25. The method of Claim 21, wherein the master key further comprises a customer identification number, a URL of the master key and a listing of the URL's of the Web pages authorized by the customer.

26. The method of Claim 25, wherein the master key further comprises, for each URL, a time period during which the Web page is authorized to be displayed to the user.

27. The method of Claim 25 further comprising generating an error message if the asset is not authorized by the master key and generating a watermark covering the asset if the domain name is authorized, but the URL is not authorized.

28. The method of Claim 20 further comprising adding more URL's into the master key to authorize more locations.

29. The method of Claim 20 further comprising creating the asset comprising embedding the content key into the asset when the asset is created.

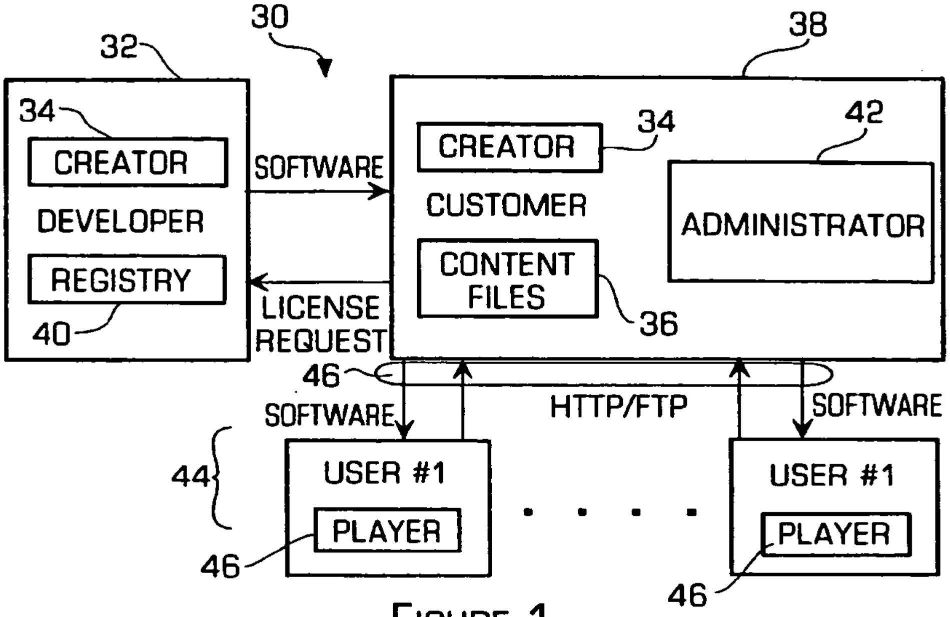


FIGURE 1

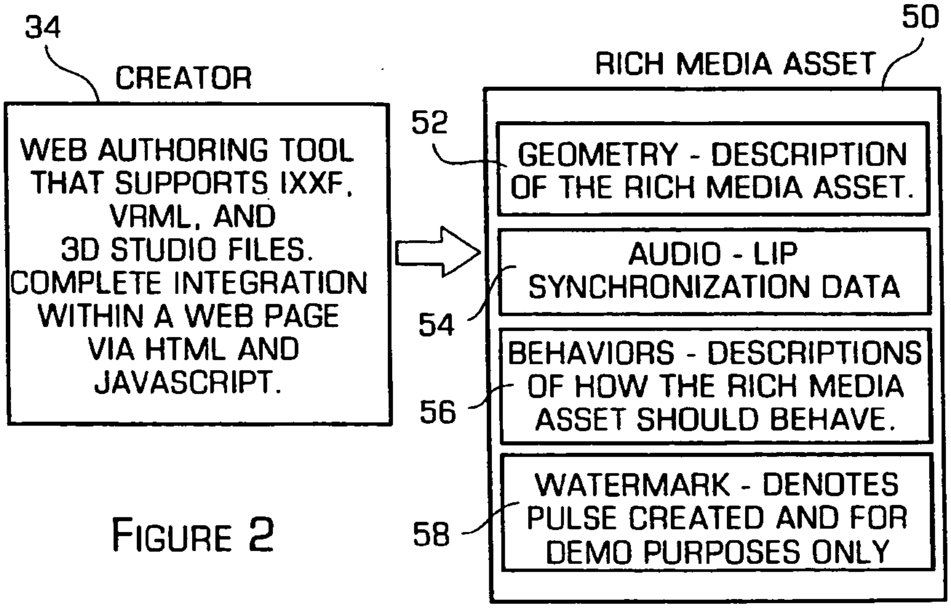

34
CREATOR
WEB AUTHORING TOOL THAT SUPPORTS IXXF, VRML, AND 3D STUDIO FILES. COMPLETE INTEGRATION WITHIN A WEB PAGE VIA HTML AND JAVASCRIPT.
50
RICH MEDIA ASSET
52
GEOMETRY - DESCRIPTION OF THE RICH MEDIA ASSET.
AUDIO - LIP SYNCHRONIZATION DATA
54
BEHAVIORS - DESCRIPTIONS OF HOW THE RICH MEDIA ASSET SHOULD BEHAVE.
56
WATERMARK - DENOTES PULSE CREATED AND FOR DEMO PURPOSES ONLY
58

FIGURE 2

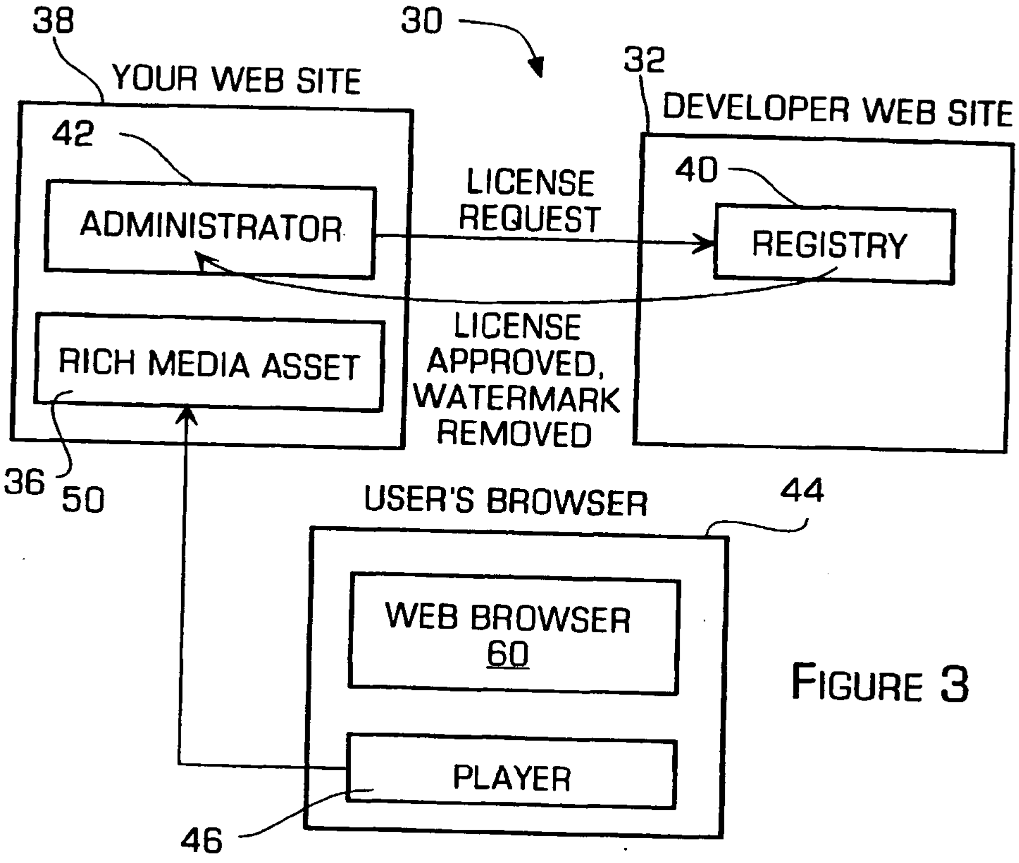


FIGURE 3

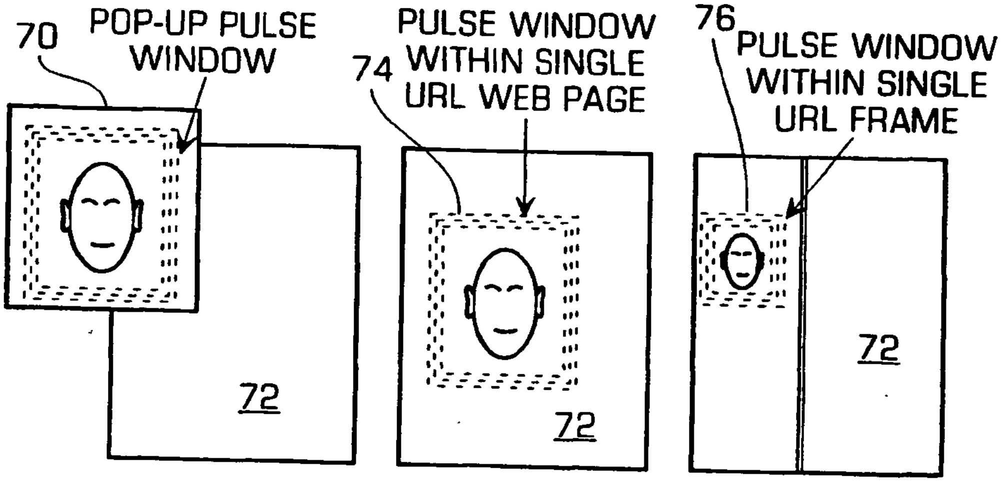

70
POP-UP PULSE WINDOW
72
PULSE WINDOW WITHIN SINGLE URL WEB PAGE
74
72
76
PULSE WINDOW WITHIN SINGLE URL FRAME
72

FIGURE 4

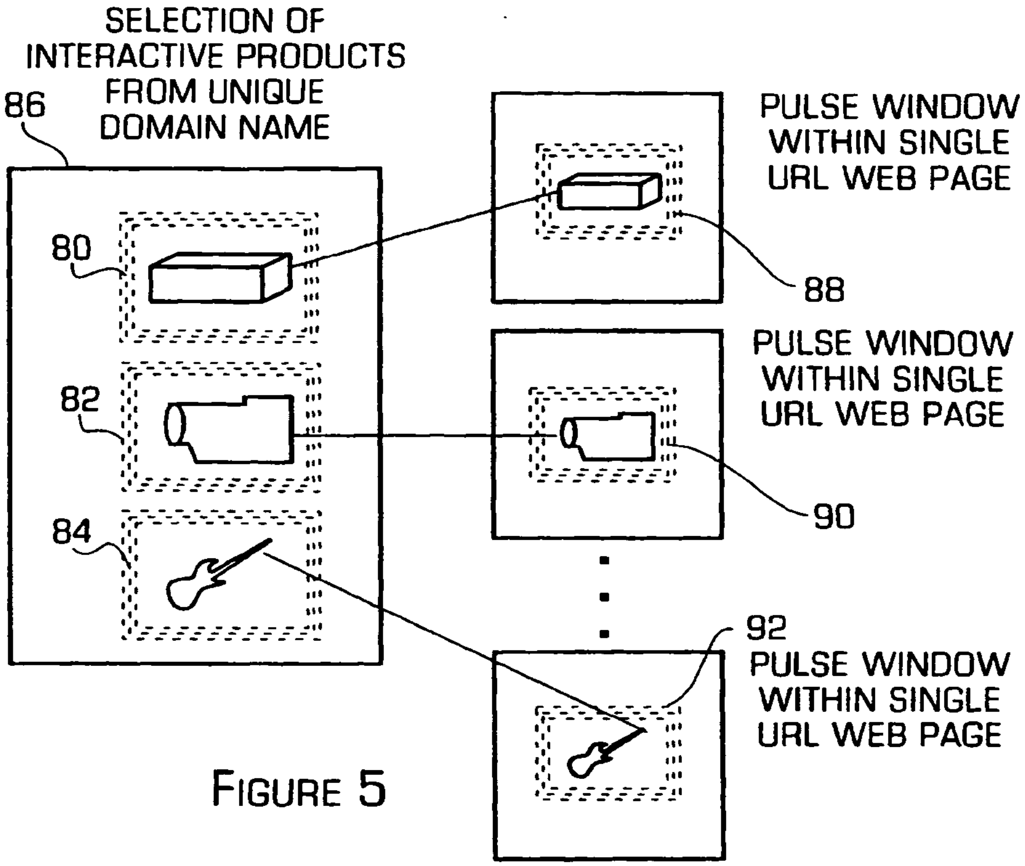

SELECTION OF INTERACTIVE PRODUCTS FROM UNIQUE DOMAIN NAME
86
80
82
84
PULSE WINDOW WITHIN SINGLE URL WEB PAGE
88
PULSE WINDOW WITHIN SINGLE URL WEB PAGE
90
92
PULSE WINDOW WITHIN SINGLE URL WEB PAGE

FIGURE 5

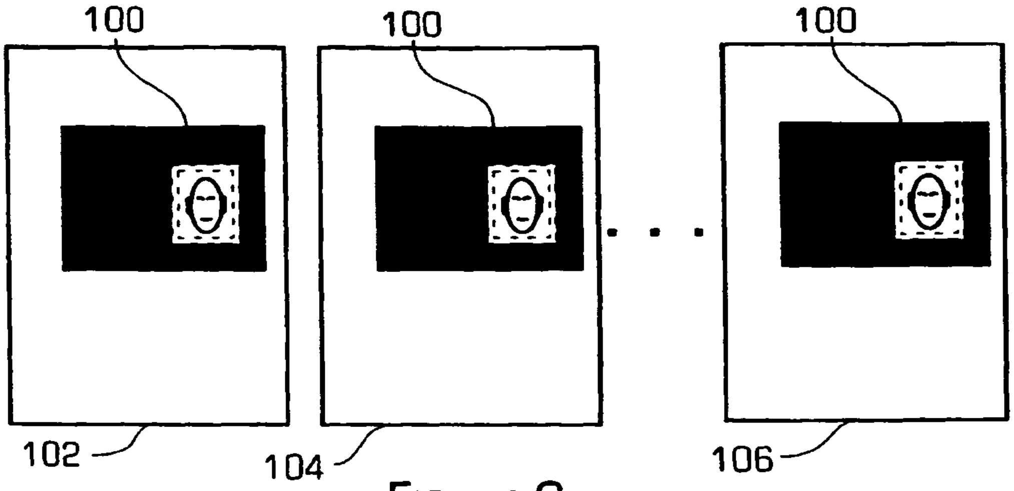
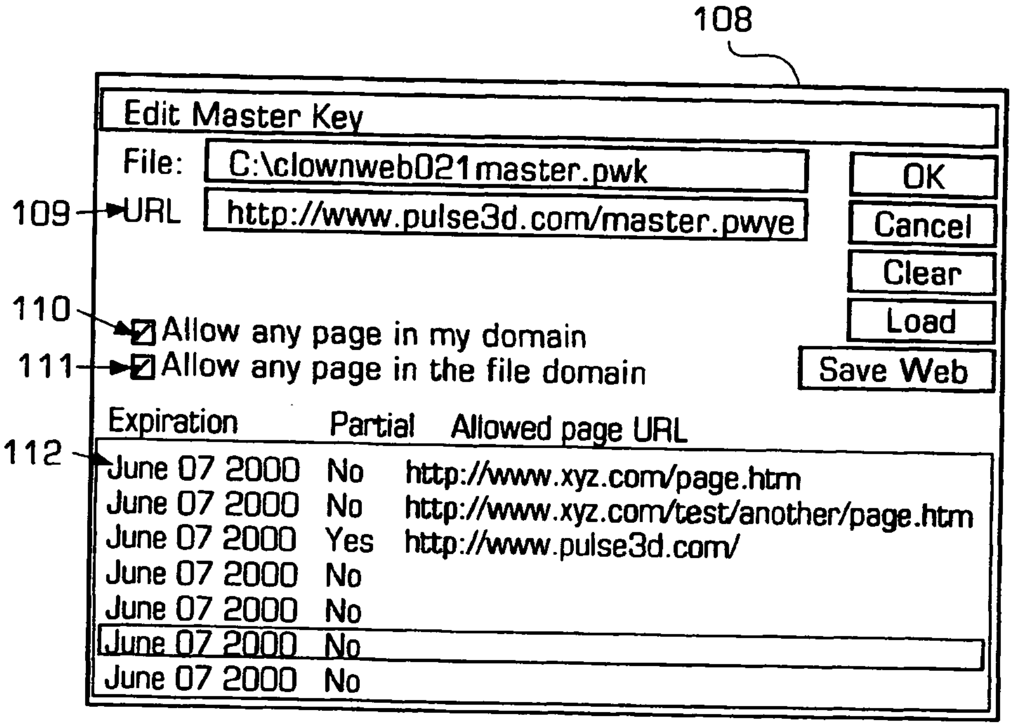


FIGURE 6



Edit Master Key

File: C:\clownweb021master.pwk

URL http://www.pulse3d.com/master.pwye

☑ Allow any page in my domain

☑ Allow any page in the file domain

Expiration	Partial	Allowed page URL
June 07 2000	No	http://www.xyz.com/page.htm
June 07 2000	No	http://www.xyz.com/test/another/page.htm
June 07 2000	Yes	http://www.pulse3d.com/
June 07 2000	No	
June 07 2000	No	
June 07 2000	No	
June 07 2000	No	

FIGURE 7

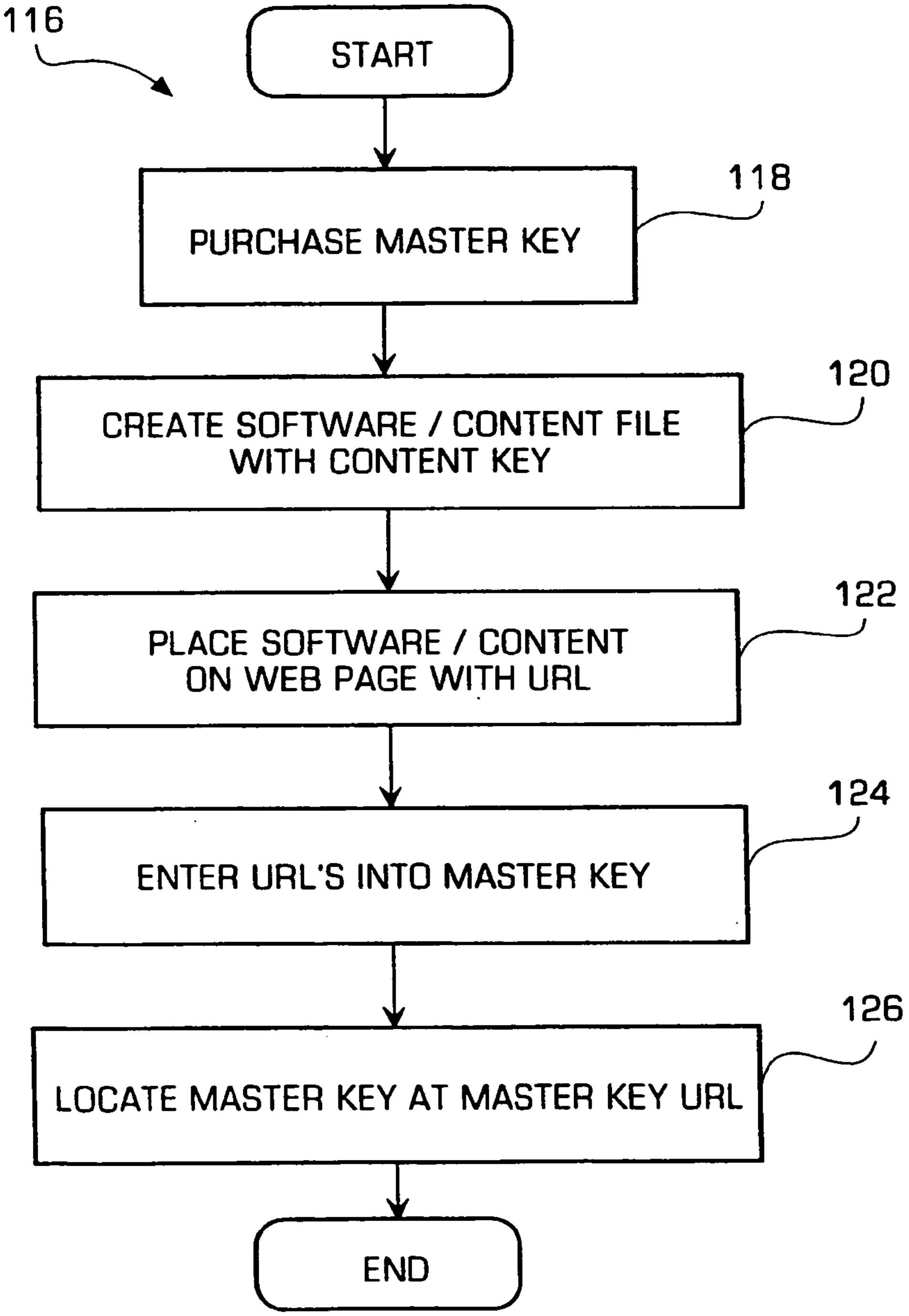

116
START
118
PURCHASE MASTER KEY
120
CREATE SOFTWARE / CONTENT FILE WITH CONTENT KEY
122
PLACE SOFTWARE / CONTENT ON WEB PAGE WITH URL
124
ENTER URL'S INTO MASTER KEY
126
LOCATE MASTER KEY AT MASTER KEY URL
END

FIGURE 8

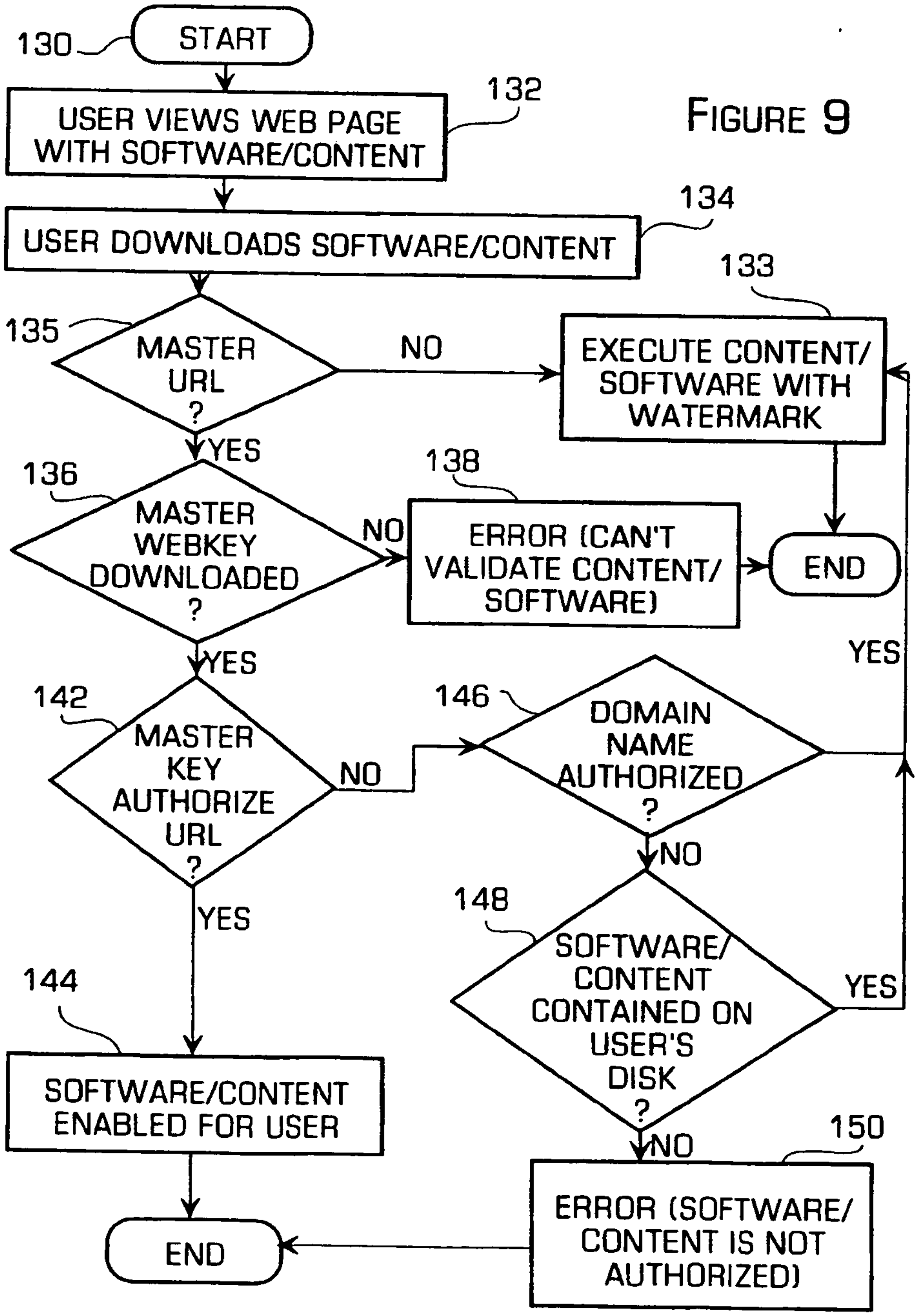


FIGURE 9
130
START
132
USER VIEWS WEB PAGE WITH SOFTWARE/CONTENT
134
USER DOWNLOADS SOFTWARE/CONTENT
133
135
MASTER URL ?
NO
EXECUTE CONTENT/ SOFTWARE WITH WATERMARK
YES
136
MASTER WEBKEY DOWNLOADED ?
138
NO
ERROR (CAN'T VALIDATE CONTENT/ SOFTWARE)
END
YES
YES
142
MASTER KEY AUTHORIZE URL ?
NO
146
DOMAIN NAME AUTHORIZED ?
NO
YES
148
SOFTWARE/ CONTENT CONTAINED ON USER'S DISK ?
YES
144
SOFTWARE/CONTENT ENABLED FOR USER
NO
150
ERROR (SOFTWARE/ CONTENT IS NOT AUTHORIZED)
END

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 10 9236

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	WO 98 25373 A (INTELLECTUAL PROTOCOLS L L C) 11 June 1998 (1998-06-11) * page 13, line 14 - page 15, line 18 * * page 19, line 22 - page 21, line 3 * * page 23, line 16 - page 25, line 18 *	1-5, 9-15, 19-24, 28,29	G06F1/00
A	US 5 319 705 A (HALTER BERNARD J ET AL) 7 June 1994 (1994-06-07) * abstract; figure 3 * * column 2, line 10 - last line * * column 4, line 23 - column 6, line 24 *	1,4-6, 11, 14-16, 20,23-25	
A	WO 98 45768 A (NORTHERN TELECOM LTD) 15 October 1998 (1998-10-15) * abstract; figures 3B,5 * * page 20, line 26 - page 23, line 14 *	1,4,10, 11,14, 20,29	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G06F
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	13 September 2000	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 10 9236

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

13-09-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9825373 A	11-06-1998	NONE	
US 5319705 A	07-06-1994	JP 2996331 B JP 7093148 A	27-12-1999 07-04-1995
WO 9845768 A	15-10-1998	US 6108420 A AU 6492198 A CN 1255209 T EP 0974084 A	22-08-2000 30-10-1998 31-05-2000 26-01-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 715 245 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.06.1996 Bulletin 1996/23

(51) Int Cl.^{6}: G06F 1/00

(21) Application number: 95308420.9

(22) Date of filing: 23.11.1995

(84) Designated Contracting States:
DE FR GB

(30) Priority: 23.11.1994 US 344042

(71) Applicant: XEROX CORPORATION
Rochester New York 14644 (US)

(72) Inventors:
- Stefik, Mark J.
Woodside, California 94062 (US)
- Casey, Michalene M.
Morgan Hill, California 95037 (US)

(74) Representative: Goode, Ian Roy
Rank Xerox Ltd
Patent Department
Parkway
Marlow Buckinghamshire SL7 1YL (GB)

(54) System for controlling the distribution and use of digital works

(57) A system for controlling use and distribution of digital works, in which the owner of a digital work (101) attaches usage rights (102) to that work. Usage rights are granted by the "owner" of a digital work to "buyers" of the digital work. The usage rights define how a digital work may be used and further distributed by the buyer. Each right has associated with it certain optional specifications which outline the conditions and fees upon which the right may be exercised. Digital works are stored in a repository. A repository will process each request (103,104) to access a digital work by examining the corresponding usage rights (105). Digital work playback devices, coupled to the repository containing the work, are used to play, display or print the work. Access to digital works for the purposes of transporting between repositories (e.g. copying, borrowing or transfer) is carried out using a digital work transport protocol. Access to digital works for the purposes of replay by a digital work playback device(e.g. printing, displaying or executing) is carried out using a digital work playback protocol. Access is denied (106) or granted (107) depending whether the requesting repository has the required usage rights.

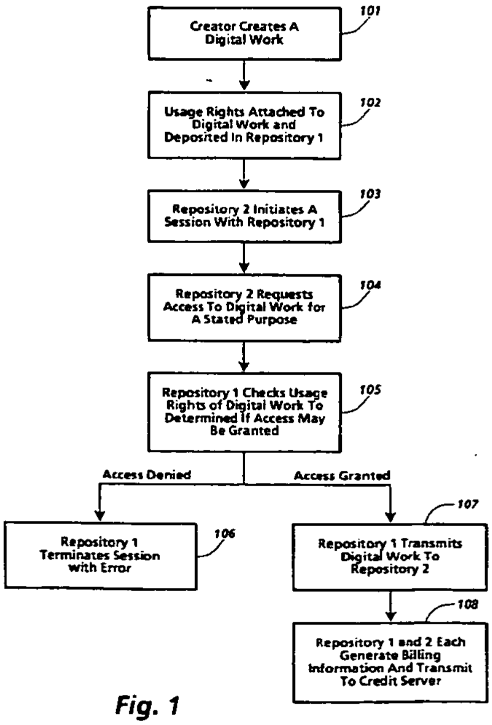

Creator Creates A Digital Work
101
Usage Rights Attached To Digital Work and Deposited In Repository 1
102
Repository 2 Initiates A Session With Repository 1
103
Repository 2 Requests Access To Digital Work for A Stated Purpose
104
Repository 1 Checks Usage Rights of Digital Work To Determined If Access May Be Granted
105
Access Denied
Access Granted
Repository 1 Terminates Session with Error
106
Repository 1 Transmits Digital Work To Repository 2
107
Repository 1 and 2 Each Generate Billing Information And Transmit To Credit Server
108

Fig. 1

EP 0 715 245 A1

Printed by Jouve, 75001 PARIS (FR)

Description

The present invention relates to the field of distribution and usage rights enforcement for digitally encoded works.

A fundamental issue facing the publishing and information industries as they consider electronic publishing is how to prevent the unauthorized and unaccounted distribution or usage of electronically published materials. Electronically published materials are typically distributed in a digital form and recreated on a computer based system having the capability to recreate the materials. Audio and video recordings, software, books and multimedia works are all being electronically published. Companies in these industries receive royalties for each accounted for delivery of the materials, e.g. the sale of an audio CD at a retail outlet. Any unaccounted distribution of a work results in an unpaid royalty (e.g. copying the audio recording CD to another digital medium.)

The ease in which electronically published works can be "perfectly" reproduced and distributed is a major concern. The transmission of digital works over networks is commonplace. One such widely used network is the Internet. The Internet is a widespread network facility by which computer users in many universities, corporations and government entities communicate and trade ideas and information. Computer bulletin boards found on the Internet and commercial networks such as CompuServ and Prodigy allow for the posting and retrieving of digital information. Information services such as Dialog and LEXIS/NEXIS provide databases of current information on a wide variety of topics. Another factor which will exacerbate the situation is the development and expansion of the National Information Infrastructure (the NII). It is anticipated that, as the NII grows, the transmission of digital works over networks will increase many times over. It would be desirable to utilize the NII for distribution of digital works without the fear of widespread unauthorized copying

The most straightforward way to curb unaccounted distribution is to prevent unauthorized copying and transmission. For existing materials that are distributed in digital form, various safeguards are used. In the case of software, copy protection schemes which limit the number of copies that can be made or which corrupt the output when copying is detected have been employed. Another scheme causes software to become disabled after a predetermined period of time has lapsed A technique used for workstation based software is to require that a special hardware device must be present on the workstation in order for the software to run, e.g., see US-A-4,932,054 entitled "Method and Apparatus for Protecting Computer Software Utilizing Coded Filter Network in Conjunction with an Active Coded Hardware Device. " Such devices are provided with the software and are commonly referred to as dongles.

Yet another scheme is to distribute software, but which requires a "key" to enable its use. This is employed in distribution schemes where "demos" of the software are provided on a medium along with the entire product. The demos can be freely used, but in order to use the actual product, the key must be purchased. These schemes do not hinder copying of the software once the key is initially purchased.

It is an object of the present invention to provide an improved system and method for controlling the use and distribution of digital works.

The invention accordingly provides a system and method as claimed in the accompanying claims.

A system for controlling use and distribution of digital works is disclosed. A digital work is any written, aural, graphical or video based work including computer programs that has been translated to or created in a digital form, and which can be recreated using suitable rendering means such as software programs. The present invention allows the owner of a digital work to attach usage rights to the work. The usage rights for the work define how it may be used and distributed. Digital works and their usage rights are stored in a secure repository. Digital works may only be accessed by other secure repositories.

Usage rights for a digital work are embodied in a flexible and extensible usage rights grammar. Conceptually, a right in the usage rights grammar is a label attached to a predetermined behavior and conditions to exercising the right. For example, a COPY right denotes that a copy of the digital work may be made. A condition to exercising the right is the requester must pass certain security criteria. Conditions may also be attached to limit the right itself. For example, a LOAN right may be defined so as to limit the duration of which a work may be LOANed. Conditions may also include requirements that fees be paid.

A repository is comprised of a storage means for storing a digital work and its attached usage rights, an external interface for receiving and transmitting data, a processor and a clock. A repository has two primary operating modes, a server mode and a requester mode. When operating in a server mode, the repository is responding to requests to access digital works. When operating in requester mode, the repository is requesting access to a digital work.

Generally, a repository will process each request to access a digital work by examining the work's usage rights. For example, in a request to make a copy of a digital work, the digital work is examined to see if rights have been granted which would allow copies to be given out. If such a right has been granted, then conditions to exercise of the right are checked (e g. a right to make 2 copies). If conditions associated with the right are satisfied, the copy can be made. Before transporting the digital work, any specified changes to the set of usage rights in the copy are attached to the copy of the digital work.

Repositories communicate utilizing a set of repository transactions. The repository transactions embody a set of protocols for establishing secure sessions connections between repositories, and for processing access requests to the digital works.

Digital works are recreated on rendering systems. A rendering system is comprised of at least a rendering repository and a rendering device (e.g. a printer, display or audio system.) Rendering systems are internally secure. Access to digital works not contained within the rendering repository is accomplished via repository transactions with an external repository containing the desired digital work.

A system and method in accordance with the invention will now be described, by way of example, with reference to the accompanying drawings, in which:-

Figure 1 is a flowchart illustrating a simple instantiation of the operation of the currently preferred embodiment of the present invention.

Figure 2 is a block diagram illustrating the various repository types and the repository transaction flow between them in the currently preferred embodiment of the present invention.

Figure 3 is a block diagram of a repository coupled with a credit server in the currently preferred embodiment of the present invention.

Figures 4a and 4b are examples of rendering systems as may be utilized in the currently preferred embodiment of the present invention.

Figure 5 illustrates a contents file layout for a digital work as may be utilized in the currently preferred embodiment of the present invention.

Figure 6 illustrates a contents file layout for an individual digital work of the digital work of Figure 5 as may be utilized in the currently preferred embodiment of the present invention.

Figure 7 illustrates the components of a description block of the currently preferred embodiment of the present invention.

Figure 8 illustrates a description tree for the contents file layout of the digital work illustrated in Figure 5.

Figure 9 illustrates a portion of a description tree corresponding to the individual digital work illustrated in Figure 6.

Figure 10 illustrates a layout for the rights portion of a description block as may be utilized in the currently preferred embodiment of the present invention.

Figure 11 is a description tree wherein certain d-blocks have PRINT usage rights and is used to illustrate "strict" and "lenient" rules for resolving usage rights conflicts.

Figure 12 is a block diagram of the hardware components of a repository as are utilized in the currently preferred embodiment of the present invention.

Figure 13 is a block diagram of the functional (logical) components of a repository as are utilized in the currently preferred embodiment of the present invention.

Figure 14 is diagram illustrating the basic components of a usage right in the currently preferred embodiment of the present invention.

Figure 15 lists the usage rights grammar of the currently preferred embodiment of the present invention.

Figure 16 is a flowchart illustrating the steps of certificate delivery, hotlist checking and performance testing as performed in a registration transaction as may be performed in the currently preferred embodiment of the present invention.

Figure 17 is a flowchart illustrating the steps of session information exchange and clock synchronization as may be performed in the currently preferred embodiment of the present invention, after each repository in the registration transaction has successfully completed the steps described in Figure 16.

Figure 18 is a flowchart illustrating the basic flow for a usage transaction, including the common opening and closing step, as may be performed in the currently preferred embodiment of the present invention.

Figure 19 is a state diagram of server and client repositories in accordance with a transport protocol followed when moving a digital work from the server to the client repositories, as may be performed in the currently preferred embodiment of the present invention.

OVERVIEW

A system for controlling use and distribution of digital works is disclosed. The present invention is directed to supporting commercial transactions involving digital works.

Herein the terms "digital work", "work" and "content" refer to any work that has been reduced to a digital representation. This would include any audio, video, text, or multimedia work and any accompanying interpreter (e.g. software) that may be required for recreating the work. The term composite work refers to a digital work comprised of a collection of other digital works. The term "usage rights" or "rights" is a term which refers to rights granted to a recipient of a digital work. Generally, these rights define how a digital work can be used and if it can be further distributed. Each usage right may have one or more specified conditions which must be satisfied before the right may be exercised.

Figure 1 is a high level flowchart omitting various details but which demonstrates the basic operation of the present invention. Referring to Figure 1, a creator creates a digital work, step 101. The creator will then determine appropriate usage rights and fees, attach them to the digital work, and store them in Repository 1, step 102. The determination of appropriate usage rights and fees will depend on various economic factors. The digital work remains securely in Repository 1 until a request for access is received. The request for access begins with a session initiation by another repository. Here a Repository 2 initiates a session with Repository 1, step 103. As will be described in greater detail below, this session initiation includes steps which helps to insure that the respective repositories are trustworthy. Assuming that a session can be established, Repository 2 may then request access to the Digital Work for a stated purpose, step 104. The purpose may be, for example, to print the digital work or to obtain a copy of the digital work. The purpose will correspond to a specific usage right. In any event, Repository 1 checks the usage rights associated with the digital work to determine if the access to the digital work may be granted, step 105. The check of the usage rights essentially involves a determination of whether a right associated with the access request has been attached to the digital work and if all conditions associated with the right are satisfied. If the access is denied, repository 1 terminates the session with an error message, step 106. If access is granted, repository 1 transmits the digital work to repository 2, step 107. Once the digital work has been transmitted to repository 2, repository 1 and 2 each generate billing information for the access which is transmitted to a credit server, step 108. Such double billing reporting is done to insure against attempts to circumvent the billing process.

Figure 2 illustrates the basic interactions between repository types in the present invention. As will become apparent from Figure 2, the various repository types will serve different functions. It is fundamental that repositories will share a core set of functionality which will enable secure and trusted communications. Referring to Figure 2, a repository 201 represents the general instance of a repository. The repository 201 has two modes of operation; a server mode and a requester mode. When in the server mode, the repository will be receiving and processing access requests to digital works. When in the requester mode, the repository will be initiating requests to access digital works. Repository 201 is general in the sense that its primary purpose is as an exchange medium for digital works. During the course of operation, the repository 201 may communicate with a plurality of other repositories, namely authorization repository 202, rendering repository 203 and master repository 204. Communication between repositories occurs utilizing a repository transaction protocol 205.

Communication with an authorization repository 202 may occur when a digital work being accessed has a condition requiring an authorization. Conceptually, an authorization is a digital certificate such that possession of the certificate is required to gain access to the digital work. An authorization is itself a digital work that can be moved between repositories and subjected to fees and usage rights conditions. An authorization may be required by both repositories involved in an access to a digital work.

Communication with a rendering repository 203 occurs in connection with the rendering of a digital work. As will be described in greater detail below, a rendering repository is coupled with a rendering device (e.g. a printer device) to comprise a rendering system.

Communication with a master repository 205 occurs in connection with obtaining an identification certificate. Identification certificates are the means by which a repository is identified as "trustworthy". The use of identification certificates is described below with respect to the registration transaction.

Figure 3 illustrates the repository 201 coupled to a credit server 301. The credit server 301 is a device which accumulates billing information for the repository 201. The credit server 301 communicates with repository 201 via billing transactions 302 to record billing transactions. Billing transactions are reported to a billing clearinghouse 303 by the credit server 301 on a periodic basis. The credit server 301 communicates to the billing clearinghouse 303 via clearinghouse transactions 304. The clearinghouse transactions 304 enable a secure and encrypted transmission of information to the billing clearinghouse 303.

RENDERING SYSTEMS

A rendering system is generally defined as a system comprising a repository and a rendering device which can render a digital work into its desired form. Examples of a rendering system may be a computer system, a digital audio system, or a printer. A rendering system has the same security features as a repository. The coupling of a rendering repository with the rendering device may occur in a manner suitable for the type of rendering device.

Figure 4a illustrates a printer as an example of a rendering system. Referring to Figure 4, printer system 401 has contained therein a printer repository 402 and a print device 403. It should be noted that the the dashed line defining printer system 401 defines a secure system boundary. Communications within the boundary are assumed to be secure. Depending on the security level, the boundary also represents a barrier intended to provide physical integrity. The printer repository 402 is an instantiation of the rendering repository 205 of Figure 2. The printer repository 402 will in some instances contain an ephemeral copy of a digital work which remains until it is printed out by the print engine 403. In other instances, the printer repository 402 may contain digital works such as fonts, which will remain and can be billed based on use. This design assures that all communication lines between printers and printing devices are encrypted, unless they are within a physically secure boundary. This design feature eliminates a potential "fault" point through which the digital work could be improperly obtained. The printer device 403 represents the printer components used to create the printed output.

Also illustrated in Figure 4a is the repository 404. The repository 404 is coupled to the printer repository 402. The repository 404 represents an external repository which contains digital works.

Figure 4b is an example of a computer system as a rendering system. A computer system may constitute a "multi-function" device since it may execute digital works (e.g. software programs) and display digital works (e.g. a digitized photograph). Logically, each rendering device can be viewed as having its own repository, although only one physical repository is needed. Referring to Figure 4b, a computer system 410 has contained therein a display/execution repository 411. The display/execution repository 411 is coupled to display device, 412 and execution device 413. The dashed box surrounding the computer system 410 represents a security boundary within which communications are assumed to be secure. The display/execution repository 411 is further coupled to a credit server 414 to report any fees to be billed for access to a digital work and a repository 415 for accessing digital works stored therein.

STRUCTURE OF DIGITAL WORKS

Usage rights are attached directly to digital works. Thus, it is important to understand the structure of a digital work. The structure of a digital work, in particular composite digital works, may be naturally organized into an acyclic structure such as a hierarchy. For example, a magazine has various articles and photographs which may have been created and are owned by different persons. Each of the articles and photographs may represent a node in a hierarchical structure. Consequently, controls, i.e. usage rights, may be placed on each node by the creator. By enabling control and fee billing to be associated with each node, a creator of a work can be assured that the rights and fees are not circumvented.

In the currently preferred embodiment, the file information for a digital work is divided into two files: a "contents" file and a "description tree" file. From the perspective of a repository, the "contents" file is a stream of addressable bytes whose format depends completely on the interpreter used to play, display or print the digital work. The description tree file makes it possible to examine the rights and fees for a work without reference to the content of the digital work. It should be noted that the term description tree as used herein refers to any type of acyclic structure used to represent the relationship between the various components of a digital work.

Figure 5 illustrates the layout of a contents file. Referring to Figure 5, a digital work is comprised of story A 510, advertisement 511, story B 512 and story C 513. It is assumed that the digital work is stored starting at a relative address of 0. Each of the parts of the digital work are stored linearly so that story A 510 is stored at approximately addresses 0-30,000, advertisement 511 at addresses 30,001-40,000, story B 512 at addresses 40,001-60,000 and story C 513 at addresses 60,001-85K. The detail of story A 510 is illustrated in Figure 6. Referring to Figure 6, the story A 510 is further broken down to show text 614 stored at address 0-1500, soldier photo 615 at addresses 1501-10,000, graphics 616 stored at addresses 10,001-25,000 and sidebar 617 stored address 25,001-30,000. Note that the data in the contents file may be compressed (for saving storage) or encrypted (for security).

From Figures 5 and 6 it is readily observed that a digital work can be represented by its component parts as a hierarchy. The description tree for a digital work is comprised of a set of related descriptor blocks (d-blocks). The contents of each d-block is described with respect to Figure 7. Referring to Figure 7, a d-block 700 includes an identifier 701 which is a unique identifier for the work in the repository, a starting address 702 providing the start address of the first byte of the work, a length 703 giving the number of bytes in the work, a rights portion 704 wherein the granted usage rights and their status data are maintained, a parent pointer 705 for pointing to a parent d-block and child pointers 706 for pointing to the child d-blocks. In the currently preferred embodiment, the identifier 701 has two parts. The first part is a unique number assigned to the repository upon manufacture. The second part is a unique number assigned to the work upon creation. The rights portion 704 will contain a data structure, such as a look-up table, wherein the various information associated with a right is maintained. The information required by the respective usage rights is described in more detail below. D-blocks form a strict hierarchy. The top d-block of a work has no parent; all other d-blocks have one parent. The relationship of usage rights between parent and child d-blocks and how conflicts are resolved is described below.

A special type of d-block is a "shell" d-block. A shell d-block adds no new content beyond the content of its parts. A shell d-block is used to add rights and fee information, typically by distributors of digital works.

Figure 8 illustrates a description tree for the digital work of Figure 5. Referring to Figure 8, a top d-block 820 for the digital work points to the various stories and advertisements contained therein. Here, the top d-block 820 points to d-block 821 (representing story A 510), d-block 822 (representing the advertisement 511), d-block 823 (representing story B 512) and and d-block 824 (representing story C 513).

The portion of the description tree for Story A 510 is illustrated in Figure 9. D-block 925 represents text 614, d-block 926 represents photo 615, d-block 927 represents graphics 616 by and d-block 928 represents sidebar 617.

The rights portion 704 of a descriptor block is further illustrated in Figure 10. Figure 10 illustrates a structure which is repeated in the rights portion 704 for each right. Referring to Figure 10, each right will have a right code field 1050 and status information field 1052. The right code field 1050 will contain a unique code assigned to a right. The status information field 1052 will contain information relating to the state of a right and the digital work. Such information is indicated below in Table 1. The rights as stored in the rights portion 704 may typically be in numerical order based on the right code.

TABLE 1

DIGITAL WORK STATE INFORMATION		
Property	**Value**	**Use**
Copies-in-Use	Number	A counter of the number of copies of a work that are in use. Incremented when another copy is used; decremented when use is completed.
Loan-Period	Time-Units	Indicator of the maximum number of time-units that a document can be loaned out
Loaner-Copy	Boolean	Indicator that the current work is a loaned out copy of an authorized digital work.
Remaining-Time	Time-Units	Indicator of the remaining time of use on a metered document right.
Document-Descr	String	A string containing various identifying information about a document. The exact format of this is not specified, but it can include information such as a publisher name, author name, ISBN number, and so on.
Revenue-Owner	RO-Descr	A handle identifying a revenue owner for a digital work. This is used for reporting usage fees.
Publication-Date	Date-Descr	The date that the digital work was published.
History-list	History-Rec	A list of events recording the repostories and dates for operations that copy, transfer, backup, or restore a digital work.

The approach for representing digtal works by separating description data from content assumes that parts of a file are contiguous but takes no position on the actual representation of content. In particular, it is neutral to the question of whether content representation may take an object oriented approach. It would be natural to represent content as objects. In principle, it may be convenient to have content objects that include the billing structure and rights information that is represented in the d-blocks. Such variations in the design of the representation are possible and are viable alternatives but may introduce processing overhead, e.g. the interpretation of the objects.

Digital works are stored in a repository as part of a hierarchical file system. Folders (also termed directories and sub-directories) contain the digital works as well as other folders. Digital works and folders in a folder are ordered in alphabetical order. The digital works are typed to reflect how the files are used. Usage rights can be attached to folders so that the folder itself is treated as a digital work. Access to the folder would then be handled in the same fashion as any other digital work As will be described in more detail below, the contents of the folder are subject to their own rights. Moreover, file management rights may be attached to the folder which define how folder contents can be managed.

ATTACHING USAGE RIGHTS TO A DIGITAL WORK

It is fundamental to the present invention that the usage rights are treated as part of the digital work. As the digital work is distributed, the scope of the granted usage rights will remain the same or may be narrowed. For example, when a digital work is transferred from a document server to a repository, the usage rights may include the right to loan a copy for a predetermined period of time (called the original rights). When the repository loans out a copy of the digital work, the usage rights in the loaner copy (called the next set of rights) could be set to prohibit any further rights to loan out the copy. The basic idea is that one cannot grant more rights than they have.

The attachment of usage rights into a digital work may occur in a variety of ways. If the usage rights will be the same for an entire digital work, they could be attached when the digital work is processed for deposit in the digital work server. In the case of a digital work having different usage rights for the various components, this can be done as the digital work is being created. An authoring tool or digital work assembling tool could be utilized which provides for an automated process of attaching the usage rights.

As will be described below, when a digital work is copied, transferred or loaned, a "next set of rights" can be specified. The"next set of rights" will be attached to the digital work as it is transported.

Resolving Conflicting Rights

Because each part of a digital work may have its own usage rights, there will be instances where the rights of a "contained part" are different from its parent or container part. As a result, conflict rules must be established to dictate when and how a right may be exercised. The hierarchical structure of a digital work facilitates the enforcement of such rules. A "strict" rule would be as follows: a right for a part in a digital work is sanctioned if and only if it is sanctioned for the part, for ancestor d-blocks containing the part and for all descendent d-blocks. By sanctioned, it is meant that (1) each of the respective parts must have the right, and (2) any conditions for exercising the right are satisfied.

It also possible to implement the present invention using a more lenient rule. In the more lenient rule, access to the part may be enabled to the descendent parts which have the right, but access is denied to the descendents which do not.

An example of applying both the strict rule and lenient is illustrated with reference to Figure 11. Referring to Figure 11, a root d-block 1101 has child d-blocks 1102-1105. In this case, root d-block represents a magazine, and each of the child d-blocks 1102-1105 represent articles in the magazine. Suppose that a request is made to PRINT the digital work represented by root d-block 1101 wherein the strict rule is followed. The rights for the root d-block 1101 and child d-blocks 1102-1105 are then examined. Root d-block 1101 and child d-blocks 1102 and 1105 have been granted PRINT rights. Child d-block 1103 has not been granted PRINT rights and child d-block 1104 has PRINT rights conditioned on payment of a usage fee.

Under the strict rule the PRINT right cannot be exercised because the child d-block does not have the PRINT right. Under the lenient rule, the result would be different. The digital works represented by child d-blocks 1102 and 1105 could be printed and the digital work represented by d-block 1104 could be printed so long as the usage fee is paid. Only the digital work represented by d-block 1103 could not be printed. This same result would be accomplished under the strict rule if the requests were directed to each of the individual digital works.

The present invention supports various combinations of allowing and disallowing access. Moreover, as will be described below the usage rights grammar permits the owner of a digital work to specify if constraints may be imposed on the work by a container part The manner in which digital works may be sanctioned because of usage rights conflicts would be implementation specific and would depend on the nature of the digital works.

REPOSITORIES

In the description of Figure 2, it was indicated that repositories come in various forms. All repositories provide a core set of services for the transmission of digital works. The manner in which digital works are exchanged is the basis for all transaction between repositories. The various repository types differ in the ultimate functions that they perform. Repositories may be devices themselves, or they may be incorporated into other systems. An example is the rendering repository 203 of Figure 2.

A repository will have associated with it a repository identifier. Typically, the repository identifier would be a unique number assigned to the repository at the time of manufacture. Each repository will also be classified as being in a particular security class. Certain communications and transactions may be conditioned on a repository being in a particular security class. The various security classes are described in greater detail below.

As a prerequisite to operation, a repository will require possession of an identification certificate. Identification certificates are encrypted to prevent forgery and are issued by a Master repository. A master repository plays the role of an authorization agent to enable repositories to receive digital works. Identification certificates must be updated on a periodic basis. Identification certificates are described in greater detail below with respect to the registration transaction.

A repository has both a hardware and functional embodiment. The functional embodiment is typically software executing on the hardware embodiment. Alternatively, the functional embodiment may be embedded in the hardware embodiment such as an Application Specific Integrated Circuit (ASIC) chip.

The hardware embodiment of a repository will be enclosed in a secure housing which if compromised, may cause the repository to be disabled. The basic components of the hardware embodiment of a repository are described with reference to Figure 12. Referring to Figure 12, a repository is comprised of a processing means 1200, storage system 1207, clock 1205 and external interface 1206. The processing means 1200 is comprised of a processor element 1201 and processor memory 1202. The processing means 1201 provides controller, repository transaction and usage rights transaction functions for the repository. Various functions in the operation of the repository such as decryption and/or decompression of digital works and transaction messages are also performed by the processing means 1200. The processor element 1201 may be a microprocessor or other suitable computing component. The processor memory 1202 would typically be further comprised of Read Only Memories (ROM) and Random Access Memories (RAM). Such memories would contain the software instructions utilized by the processor element 1201 in performing the functions of the repository.

The storage system 1207 is further comprised of descriptor storage 1203 and content storage 1204. The description tree storage 1203 will store the description tree for the digital work and the content storage will store the associated content. The description tree storage 1203 and content storage 1204 need not be of the same type of storage medium, nor are they necessarily on the same physical device. So for example, the descriptor storage 1203 may be stored on a solid state storage (for rapid retrieval of the description tree information), while the content storage 1204 may be on a high capacity storage such as an optical disk.

The clock 1205 is used to time-stamp various time based conditions for usage rights or for metering usage fees which may be associated with the digital works. The clock 1205 will have an uninterruptable power supply, e.g. a battery, in order to maintain the integrity of the time-stamps. The external interface means 1206 provides for the signal connection to other repositories and to a credit server. The external interface means 1206 provides for the exchange of signals via such standard interfaces such as RS-232 or Personal Computer Manufacturers Card Industry Association (PCMCIA) standards, or FDDI. The external interface means 1206 may also provide network connectivity.

The functional embodiment of a repository is described with reference to Figure 13. Referring to Figure 13, the functional embodiment is comprised of an operating system 1301, core repository services 1302, usage transaction handlers 1303, repository specific functions, 1304 and a user interface 1305. The operating system 1301 is specific to the repository and would typically depend on the type of processor being used. The operating system 1301 would also provide the basic services for controlling and interfacing between the basic components of the repository.

The core repository services 1302 comprise a set of functions required by each and every repository. The core repository services 1302 include the session initiation transactions which are defined in greater detail below. This set of services also includes a generic ticket agent which is used to "punch" a digital ticket and a generic authorization server for processing authorization specifications. Digital tickets and authorizations are specific mechanisms for controlling the distribution and use of digital works and are described in more detail below. Note that coupled to the core repository services are a plurality of identification certificates 1306. The identification certificates 1306 are required to enable the use of the repository.

The usage transactions handlers 1303 comprise functionality for processing access requests to digital works and for billing fees based on access. The usage transactions supported will be different for each repository type. For example, it may not be necessary for some repositories to handle access requests for digital works.

The repository specific functionality 1304 comprises functionality that is unique to a repository. For example, the master repository has special functionality for issuing digital certificates and maintaining encryption keys. The repository specific functionality 1304 would include the user interface implementation for the repository.

Repository Security Classes

For some digital works the losses caused by any individual instance of unauthorized copying is insignificant and the chief economic concern lies in assuring the convenience of access and low-overhead billing. In such cases, simple and inexpensive handheld repositories and network-based workstations may be suitable repositories, even though the measures and guarantees of security are modest.

At the other extreme, some digital works such as a digital copy of a first run movie or a bearer bond or stock certificate would be of very high value so that it is prudent to employ caution and fairly elaborate security measures to ensure that they are not copied or forged. A repository suitable for holding such a digital work could have elaborate measures for ensuring physical integrity and for verifying authorization before use.

By arranging a universal protocol, all kinds of repositories can communicate with each other in principle. However, creators of some works will want to specify that their works will only be transferred to repositories whose level of security is high enough. For this reason, document repositories have a ranking system for classes and levels of security. The security classes in the currently preferred embodiment are described in Table 2.

TABLE 2

REPOSITORY SECURITY LEVELS	
Level	Description of Security
0	Open system. Document transmission is unencrypted. No digital certificate is required for identification. The security of the system depends mostly on user honesty, since only modest knowledge may be needed to circumvent the security measures. The repository has no provisions for preventing unauthorized programs from running and accessing or copying files. The system does not prevent the use of removable storage and does not encrypt stored files.
1	Minimal security. Like the previous class except that stored files are minimally encrypted, including ones on removable storage.

TABLE 2 (continued)

REPOSITORY SECURITY LEVELS	
Level	Description of Security
2	Basic security. Like the previous class except that special tools and knowledge are required to compromise the programming, the contents of the repository, or the state of the clock. All digital communications are encrypted. A digital certificate is provided as identification. Medium level encryption is used. Repository identification number is unforgeable.
3	General security. Like the previous class plus the requirement of special tools are needed to compromise the physical integrity of the repository and that modest encryption is used on all transmissions. Password protection is required to use the local user interface. The digital clock system cannot be reset without authorization. No works would be stored on removable storage. When executing works as programs, it runs them in their own address space and does not give them direct access to any file storage or other memory containing system code or works. They can access works only through the transmission transaction protocol.
4	Like the previous class except that high level encryption is used on all communications. Sensors are used to record attempts at physical and electronic tampering. After such tampering, the repository will not perform other transactions until it has reported such tampering to a designated server.
5	Like the previous class except that if the physical or digital attempts at tampering exceed some preset thresholds that threaten the physical integrity of the repository or the integrity of digital and cryptographic barriers, then the repository will save only document description records of history but will erase or destroy any digital identifiers that could be misused if released to an unscrupulous party. It also modifies any certificates of authenticity to indicate that the physical system has been compromised. It also erases the contents of designated documents.
6	Like the previous class except that the repository will attempt wireless communication to report tampering and will employ noisy alarms.
10	This would correspond to a very high level of security. This server would maintain constant communications to remote security systems reporting transactions, sensor readings, and attempts to circumvent security.

The characterization of security levels described in Table 2 is not intended to be fixed. More important is the idea of having different security levels for different repositories. It is anticipated that new security classes and requirements will evolve according to social situations and changes in technology.

Repository User Interface

A user interface is broadly defined as the mechanism by which a user interacts with a repository in order to invoke transactions to gain access to a digital work, or exercise usage rights. As described above, a repository may be embodied in various forms. The user interface for a repository will differ depending on the particular embodiment. The user interface may be a graphical user interface having icons representing the digital works and the various transactions that may be performed. The user interface may be a generated dialog in which a user is prompted for information.

The user interface itself need not be part of the repository. As a repository may be embedded in some other device, the user interface may merely be a part of the device in which the repository is embedded. For example, the repository could be embedded in a "card" that is inserted into an available slot in a computer system. The user interface may be a combination of a display, keyboard, cursor control device and software executing on the computer system.

At a minimum, the user interface must permit a user to input information such as access requests and alpha numeric data and provide feedback as to transaction status. The user interface will then cause the repository to initiate the suitable transactions to service the request. Other facets of a particular user interface will depend on the functionality that a repository will provide.

CREDIT SERVERS

In the present invention, fees may be associated with the exercise of a right. The requirement for payment of fees is described with each version of a usage right in the usage rights language. The recording and reporting of such fees is performed by the credit server. One of the capabilities enabled by associating fees with rights is the possibility of supporting a wide range of charging models. The simplest model, used by conventional software, is that there is a single fee at the time of purchase, after which the purchaser obtains unlimited rights to use the work as often and for as long as he or she wants. Alternative models, include metered use and variable fees. A single work can have different fees for different uses. For example, viewing a photograph on a display could have different fees than making a hardcopy or including it in a newly created work. A key to these alternative charging models is to have a low overhead means of establishing fees and accounting for credit on these transactions.

A credit server is a computational system that reliably authorizes and records these transactions so that fees are billed and paid. The credit server reports fees to a billing clearinghouse. The billing clearinghouse manages the financial transactions as they occur. As a result, bills may be generated and accounts reconciled. Preferably, the credit server would store the fee transactions and periodically communicate via a network with the billing clearinghouse for reconciliation. In such an embodiment, communications with the billing clearinghouse would be encrypted for integrity and security reasons. In another embodiment, the credit server acts as a "debit card" where transactions occur in "real-time" against a user account.

A credit server is comprised of memory, a processing means, a clock, and interface means for coupling to a repository and a financial institution (e.g. a modem). The credit server will also need to have security and authentication functionality. These elements are essentially the same elements as those of a repository. Thus, a single device can be both a repository and a credit server, provided that it has the appropriate processing elements for carrying out the corresponding functions and protocols. Typically, however, a credit server would be a card-sized system in the possession of the owner of the credit. The credit server is coupled to a repository and would interact via financial transactions as described below. Interactions with a financial institution may occur via protocols established by the financial institutions themselves.

In the currently preferred embodiment credit servers associated with both the server and the repository report the financial transaction to the billing clearinghouse. For example, when a digital work is copied by one repository to another for a fee, credit servers coupled to each of the repositories will report the transaction to the billing clearinghouse. This is desirable in that it insures that a transaction will be accounted for in the event of some break in the communication between a credit server and the billing clearinghouse. However, some implementations may embody only a single credit server reporting the transaction to minimize transaction processing at the risk of losing some transactions.

USAGE RIGHTS LANGUAGE

The present invention uses statements in a high level "usage rights language" to define rights associated with digital works and their parts. Usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and also to determine parameters for those transactions. For example, sentences in the language determine whether a given digital work can be copied, when and how it can be used, and what fees (if any) are to be charged for that use. Once the usage rights statements are generated, they are encoded in a suitable form for accessing during the processing of transactions.

Defining usage rights in terms of a language in combination with the hierarchical representation of a digital work enables the support of a wide variety of distribution and fee schemes. An example is the ability to attach multiple versions of a right to a work. So a creator may attach a PRINT right to make 5 copies for $10.00 and a PRINT right to make unlimited copies for $100.00. A purchaser may then choose which option best fits his needs. Another example is that rights and fees are additive. So in the case of a composite work, the rights and fees of each of the components works is used in determining the rights and fees for the work as a whole.

The basic contents of a right are illustrated in Figure 14. Referring to Figure 14, a right 1450 has a transactional component 1451 and a specifications component 1452. A right 1450 has a label (e.g. COPY or PRINT) which indicates the use or distribution privileges that are embodied by the right. The transactional component 1451 corresponds to a particular way in which a digital work may be used or distributed. The transactional component 1451 is typically embodied in software instructions in a repository which implement the use or distribution privileges for the right. The specifications components 1452 are used to specify conditions which must be satisfied prior to the right being exercised or to designate various transaction related parameters. In the currently preferred embodiment, these specifications include copy count 1453, Fees and Incentives 1454, Time 1455, Access and Security 1456 and Control 1457. Each of these specifications will be described in greater detail below with respect to the language grammar elements.

The usage rights language is based on the grammar described below. A grammar is a convenient means for defining valid sequence of symbols for a language. In describing the grammar the notation "[a I b I c] is used to indicate distinct choices among alternatives. In this example, a sentence can have either an "a", "b" or "c". It must include exactly one of them. The braces { } are used to indicate optional items. Note that brackets, bars and braces are used to describe the language of usage rights sentences but do not appear in actual sentences in the language.

In contrast, parentheses are part of the usage rights language. Parentheses are used to group items together in lists. The notation (x*) is used to indicate a variable length list, that is, a list containing one or more items of type x.

The notation (x)* is used to indicate a variable number of lists containing x.

Keywords in the grammar are words followed by colons. Keywords are a common and very special case in the language. They are often used to indicate a single value, typically an identifier. In many cases, the keyword and the parameter are entirely optional. When a keyword is given, it often takes a single identifier as its value. In some cases, the keyword takes a list of identifiers.

In the usage rights language, time is specified in an hours:minutes:seconds (or hh:mm:ss) representation. Time zone indicators, e.g. PDT for Pacific Daylight Time, may also be specified. Dates are represented as year/ month/day (or YYYY/MMM/DD). Note that these time and date representations may specify moments in time or units of time Money units are specified in terms of dollars.

Finally, in the usage rights language, various "things" will need to interact with each other. For example, an instance of a usage right may specify a bank account, a digital ticket, etc.. Such things need to be identified and are specified herein using the suffix "-ID."

The Usage Rights Grammar is listed in its entirety in Figure 15 and is described below.

Grammar element 1501 "**Digital Work Rights: = (Rights*)**" define the digital work rights as a set of rights. The set of rights attached to a digital work define how that digital work may be transferred, used, performed or played. A set of rights will attach to the entire digital work and in the case of compound digital works, each of the components of the digital work. The usage rights of components of a digital may be different.

Grammar element 1502 "**Right : = (Right-Code {Copy-Count} {Control-Spec} {Time-Spec} {Access-Spec} {Fee-Spec})**" enumerates the content of a right. Each usage right must specify a right code. Each right may also optionally specify conditions which must be satisfied before the right can be exercised. These conditions are copy count, control, time, access and fee conditions. In the currently preferred embodiment, for the optional elements, the following defaults apply: copy count equals 1, no time limit on the use of the right, no access tests or a security level required to use the right and no fee is required. These conditions will each be described in greater detail below.

It is important to note that a digital work may have multiple versions of a right, each having the same right code. Thc multiplc vcrsion would provide altemative conditions and fees for accessing the digital work.

Grammar element 1503 "**Right-Code : = Render-Code I Transport-Code I File-Management-Codel Derivative-Works- Code Configuration-Code**" distinguishes each of the specific rights into a particular right type (although each right is identified by distinct right codes). In this way, the grammar provides a catalog of possible rights that can be associated with parts of digital works. In the following, rights are divided into categories for convenience in describing them

Grammar element 1504 "**Render-Code : = [Play: {Player: Player-ID} I Print: {Printer: Printer-ID}]**" lists a category of rights all involving the making of ephemeral, transitory, or non-digital copies of the digital work. After use the copies are erased.

• Play	A process of rendering or performing a digital work on some processor. This includes such things as playing digital movies, playing digital music, playing a video game, running a computer program, or displaying a document on a display.
• Print	To render the work in a medium that is not further protected by usage rights, such as printing on paper.

Grammar element 1505 "**Transport-Code : = [Copy I Transfer I Loan {Remaining-Rights: Next-Set-of-Rights}] {(Next-Copy-Rights: Next-Set of Rights)}**" lists a category of rights involving the making of persistent, usable copies of the digital work on other repositories. The optional Next-Copy-Rights determine the rights on the work after it is transported. If this is not specified, then the rights on the transported copy are the same as on the original. The optional Remaining-Rights specify the rights that remain with a digital work when it is loaned out. If this is not specified, then the default is that no rights can be exercised when it is loaned out.

• Copy	Make a new copy of a work
• Transfer	Moving a work from one repository to another.
• Loan	Temporarily loaning a copy to another repository for a specified period of time.

Grammar element 1506 "**File-Management-Code : = Backup {Back-Up-Copy-Rights: Next-Set -of Rights}I Restore I Delete I Folder I Directory {Name:Hide-Local I Hide - Remote}{Parts:Hide-Local I Hide-Remote}**" lists a category of rights involving operations for file management, such as the making of backup copies to protect the copy owner against catastrophic equipment failure.

Many software licenses and also copyright law give a copy owner the right to make backup copies to protect against catastrophic failure of equipment. However, the making of uncontrolled backup copies is inherently at odds with the ability to control usage, since an uncontrolled backup copy can be kept and then restored even after the authorized copy was sold.

The File management rights enable the making and restoring of backup copies in a way that respects usage rights, honoring the requirements of both the copy owner and the rights grantor and revenue owner. Backup copies of work descriptions (including usage rights and fee data) can be sent under appropriate protocol and usage rights control to other document repositories of sufficiently high security. Further rights permit organization of digital works into folders which themselves are treated as digital works and whose contents may be "hidden" from a party seeking to determine the contents of a repository.

- Backup To make a backup copy of a digital work as protection against media failure.
- Restore To restore a backup copy of a digital work.
- Delete To delete or erase a copy of a digital work.
- Folder To create and name folders, and to move files and folders between folders.
- Directory To hide a folder or its contents.

Grammar element 1507 "**Derivative-Works-Code: [Extract I Embed I Edit {Process: Process-ID}] {Next-Copy-Rights : Next-Set-of Rights}**" lists a category of rights involving the use of a digital work to create new works.

- Extract To remove a portion of a work, for the purposes of creating a new work.
- Embed To include a work in an existing work.
- Edit To alter a digital work by copying, selecting and modifying portions of an existing digital work.

Grammar element 1508 "**Configuration-Code : = Install I Uninstall**" lists a category of rights for installing and uninstalling software on a repository (typically a rendering repository.) This would typically occur for the installation of a new type of player within the rendering repository.

- Install: To install new software on a repository.
- Uninstall: To remove existing software from a repository.

Grammar element 1509 "**Next-Set-of-Rights : = {(Add : Set-Of-Rights)} {(Delete: Set-Of-Rights)} {(Replace: Set-Of-Rights)} {(Keep: Set-Of-Rights)}**" defines how rights are carried forward for a copy of a digital work. If the Next-Copy-Rights is not specified, the rights for the next copy are the same as those of the current copy. Otherwise, the set of rights for the next copy can be specified. Versions of rights after Add: are added to the current set of rights. Rights after Delete: are deleted from the current set of rights. If only right codes are listed after Delete:, then all versions of rights with those codes are deleted. Versions of rights after Replace: subsume all versions of rights of the same type in the current set of rights.

If Remaining-Rights is not specified, then there are no rights for the original after all Loan copies are loaned out. If Remaining-Rights is specified, then the Keep: token can be used to simplify the expression of what rights to keep behind. A list of right codes following keep means that all of the versions of those listed rights are kept in the remaining copy. This specification can be overridden by subsequent Delete: or Replace: specifications.

Copy Count Specification

For various transactions, it may be desirable to provide some limit as to the number of "copies" of the work which may be exercised simultaneously for the right. For example, it may be desirable to limit the number of copies of a digital work that may be loaned out at a time or viewed at a time.

Grammar element 1510 "**Copy-Count : = (Copies: positive-integer I 0 I unlimited)**" provides a condition which defines the number of "copies" of a work subject to the right . A copy count can be 0, a fixed number, or unlimited. The copy-count is associated with each right, as opposed to there being just a single copy-count for the digital work. The Copy-Count for a right is decremented each time that a right is exercised. When the Copy-Count equals zero, the right can no longer be exercised. If the Copy-Count is not specified, the default is one.

Control Specification

Rights and fees depend in general on rights granted by the creator as well as further restrictions imposed by later distributors. Control specifications deal with interactions between the creators and their distributors governing the imposition of further restrictions and fees. For example, a distributor of a digital work may not want an end consumer of a digital work to add fees or otherwise profit by commercially exploiting the purchased digital work.

Grammar element 1511 "**Control-Spec : = (Control: {Restrictable I Unrestrictable} {Unchargeable I Chargeable})**" provides a condition to specify the effect of usage rights and fees of parents on the exercise of the right. A digital work is restrictable if higher level d-blocks can impose further restrictions (time specifications and access specifications) on the right. It is unrestrictable if no further restrictions can be imposed. The default setting is restrictable. A right is unchargeable if no more fees can be imposed on the use of the right. It is chargeable if more fees can be imposed. The default is chargeable.

Time Specification

It is often desirable to assign a start date or specify some duration as to when a right may be exercised. Grammar element 1512 "**Time-Spec : = ({Fixed-Interval I Sliding-Interval I Meter-Time} Until: Expiration-Date)**" provides for specification of time conditions on the exercise of a right. Rights may be granted for a specified time. Different kinds of time specifications are appropriate for different kinds of rights. Some rights may be exercised during a fixed and predetermined duration. Some rights may be exercised for an interval that starts the first time that the right is invoked by some transaction. Some rights may be exercised or are charged according to some kind of metered time, which may be split into separate intervals. For example, a right to view a picture for an hour might be split into six ten minute viewings or four fifteen minute viewings or twenty three minute viewings.

The terms "time" and "date" are used synonymously to refer to a moment in time. There are several kinds of time specifications. Each specification represents some limitation on the times over which the usage right applies. The Expiration-Date specifies the moment at which the usage right ends. For example, if the Expiration-Date is "Jan 1, 1995," then the right ends at the first moment of 1995. If the Expiration-Date is specified as "forever", then the rights are interpreted as continuing without end. If only an expiration date is given, then the right can be exercised as often as desired until the expiration date.

Grammar element 1513 "**Fixed-Interval := From: Start-Time**" is used to define a predetermined interval that runs from the start time to the expiration date.

Grammar element 1514 "**Sliding-Interval : = Interval: Use-Duration**" is used to define an indeterminate (or "open") start time. It sets limits on a continuous period of time over which the contents are accessible. The period starts on the first access and ends after the duration has passed or the expiration date is reached, whichever comes first. For example, if the right gives 10 hours of continuous access, the use-duration would begin when the first access was made and end 10 hours later.

Grammar element 1515 "**Meter-Time: = Time-Remaining: Remaining-Use**" is used to define a "meter time," that is, a measure of the time that the right is actually exercised. It differs from the Sliding-Interval specification in that the time that the digital work is in use need not be continuous. For example, if the rights guarantee three days of access, those days could be spread out over a month. With this specification, the rights can be exercised until the meter time is exhausted or the expiration date is reached, whichever comes first.

Remaining-Use: = Time-Unit
Start-Time: = Time-Unit
Use-Duration: = Time-Unit
All of the time specifications include time-unit specifications in their ultimate instantiation.

Security Class and Authorization Specification

The present invention provides for various security mechanisms to be introduced into a distribution or use scheme. Grammar element 1516 "**Access-Spec : = ({SC: Security-Class} {Authorization: Authorization-ID*} {Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID})**" provides a means for restricting access and transmission. Access specifications can specify a required security class for a repository to exercise a right or a required authorization test that must be satisfied.

The keyword "**SC:**" is used to specify a minimum security level for the repositories involved in the access. If "**SC:** " is not specified, the lowest security level is acceptable.

The optional "**Authorization:**" keyword is used to specify required authorizations on the same repository as the work. The optional "**Other-Authorization:**" keyword is used to specify required authorizations on the other repository in the transaction.

The optional "**Ticket:**" keyword specifies the identity of a ticket required for the transaction. A transaction involving digital tickets must locate an appropriate digital ticket agent who can "punch" or otherwise validate the ticket before the transaction can proceed. Tickets are described in greater detail below.

In a transaction involving a repository and a document server, some usage rights may require that the repository have a particular authorization, that the server have some authorization, or that both repositories have (possibly different) authorizations. Authorizations themselves are digital works (hereinafter referred to as an authorization object) that can be moved between repositories in the same manner as other digital works. Their copying and transferring is subject to the same rights and fees as other digital works. A repository is said to have an authorization if that authorization object is contained within the repository.

In some cases, an authorization may be required from a source other than the document server and repository. An authorization object referenced by an Authorization-ID can contain digital address information to be used to set up a communications link between a repository and the authorization source. These are analogous to phone numbers. For such access tests, the communication would need to be established and authorization obtained before the right could be exercised.

For one-time usage rights, a variant on this scheme is to have a digital ticket. A ticket is presented to a digital ticket agent, whose type is specified on the ticket. In the simplest case, a certified generic ticket agent, available on all repositories, is available to "punch" the ticket. In other cases, the ticket may contain addressing information for locating a "special" ticket agent. Once a ticket has been punched, it cannot be used again for the same kind of transaction (unless it is unpunched or refreshed in the manner described below.) Punching includes marking the ticket with a timestamp of the date and time it was used. Tickets are digital works and can be copied or transferred between repositories according to their usage rights.

In the currently preferred embodiment, a "punched" ticket becomes "unpunched" or "refreshed" when it is copied or extracted. The Copy and Extract operations save the date and time as a property of the digital ticket. When a ticket agent is given a ticket, it can simply check whether the digital copy was made after the last time that it was punched. Of course, the digital ticket must have the copy or extract usage rights attached thereto.

The capability to unpunch a ticket is inportant in the following cases:

- A digital work is circulated at low cost with a limitation that it can be used only once.
- A digital work is circulated with a ticket that can be used once to give discounts on purchases of other works.
- A digital work is circulated with a ticket (included in the purchase price and possibly embedded in the work) that can be used for a future upgrade.

In each of these cases, if a paid copy is made of the digital work (including the ticket) the new owner would expect to get a fresh (unpunched) ticket, whether the copy seller has used the work or not. In contrast, loaning a work or simply transferring it to another repository should not revitalize the ticket.

Usage Fees and Incentives Specification

The billing for use of a digital work is fundamental to a commercial distribution system. Grammar Element 1517 "**Fee-Spec: = {Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec | Markup-Spec**" provides a range of options for billing for the use of digital works.

A key feature of this approach is the development of low-overhead billing for transactions in potentially small amounts. Thus, it becomes feasible to collect fees of only a few cents each for thousands of transactions.

The grammar differentiates between uses where the charge is per use from those where it is metered by the time unit. Transactions can support fees that the user pays for using a digital work as well as incentives paid by the right grantor to users to induce them to use or distribute the digital work.

The optional scheduled discount refers to the rest of the fee specification--discounting it by a percentage over time. If it is not specified, then there is no scheduled discount. Regular fee specifications are constant over time. Scheduled fee specifications give a schedule of dates over which the fee specifications change. Markup specifications are used in d-blocks for adding a percentage to the fees already being charged.

Grammar Element 1518 "**Scheduled-Discount: = (Scheduled-Discount: (Time-Spec Percentage)*)**" A Scheduled-Discount is a essentially a scheduled modifier of any other fee specification for this version of the right of the digital work. (It does not refer to children or parent digital works or to other versions of rights.). It is a list of pairs of times and percentages. The most recent time in the list that has not yet passed at the time of the transaction is the one in effect. The percentage gives the discount percentage. For example, the number 10 refers to a 10% discount.

Grammar Element 1519 "**Regular-Fee-Spec : = ({Fee: | Incentive: } [Per-Use-Spec | Metered-Rate-Spec | Best-Price-Spec | Call-For-Price-Spec] {Min: Money-Unit Per: Time-Spec)(Max: Money-Unit Per: Time-Spec} To: Account-ID)**" provides for several kinds of fee specifications.

Fees are paid by the copy-owner/user to the revenue-owner if Fee: is specified. Incentives are paid by the revenue-owner to the user if Incentive: is specified. If the Min: specification is given, then there is a minimum fee to be charged per time-spec unit for its use. If the Max: specification is given, then there is a maximum fee to be charged per time-spec for its use. When Fee: is specified, Account-ID identifies the account to which the fee is to be paid. When Incentive: is specified, Account-ID identifies the account from which the fee is to be paid.

Grammar element 1520 "**Per-Use-Spec: = Per-Use: Money-unit**" defines a simple fee to be paid every time the right is exercised, regardless of how much time the transaction takes.

Grammar element 1521 **"Metered-Rate-Spec : = Metered: Money-Unit Per: Time-Spec"** defines a metered-rate fee paid according to how long the right is exercised. Thus, the time it takes to complete the transaction determines the fee.

Grammar element 1522 **"Best-Price-Spec := Best-Price: Money-unit Max: Money-unit"** is used to specify a best-price that is determined when the account is settled. This specification is to accommodate special deals, rebates, and pricing that depends on information that is not available to the repository. All fee specifications can be combined with tickets or authorizations that could indicate that the consumer is a wholesaler or that he is a preferred customer, or that the seller be authorized in some way. The amount of money in the Max: field is the maximum amount that the use will cost. This is the amount that is tentatively debited from the credit server. However, when the transaction is ultimately reconciled, any excess amount will be returned to the consumer in a separate transaction.

Grammar element 1523 **"Call-For-Price-Spec:= Call-For-Price"** is similar to a **"Best-Price-Spec"** in that it is intended to accommodate cases where prices are dynamic. **A Call-For-Price Spec** requires a communication with a dealer to determine the price. This option cannot be exercised if the repository cannot communicate with a dealer at the time that the right is exercised. It is based on a secure transaction whereby the dealer names a price to exercise the right and passes along a deal certificate which is referenced or included in the billing process.

Grammar element 1524 **"Scheduled-Fee-Spec: = (Schedule: (Time-Spec Regular-Fee-Spec)*)"** is used to provide a schedule of dates over which the fee specifications change. The fee specification with the most recent date not in the future is the one that is in effect. This is similar to but more general than the scheduled discount. It is more general, because it provides a means to vary the fee agreement for each time period.

Grammar element 1525 **"Markup-Spec: = Markup: percentage To: Account-ID"** is provided for adding a percentage to the fees already being charged. For example, a 5% markup means that a fee of 5% of cumulative fee so far will be allocated to the distributor. A markup specification can be applied to all of the other kinds of fee specifications. It is typically used in a shell provided by a distributor. It refers to fees associated with d-blocks that are parts of the current d-block. This might be a convenient specification for use in taxes, or in distributor overhead.

REPOSITORY TRANSACTIONS

When a user requests access to a digital work, the repository will initiate various transactions. The combination of transactions invoked will depend on the specifications assigned for a usage right. There are three basic types of transactions, Session Initiation Transactions, Financial Transactions and Usage Transactions. Generally, session initiation transactions are initiated first to establish a valid session. When a valid session is established, transactions corresponding to the various usage rights are invoked. Finally, request specific transactions are performed.

Transactions occur between two repositories (one acting as a server), between a repository and a document playback platform (e.g. for executing or viewing), between a repository and a credit server or between a repository and an authorization server. When transactions occur between more than one repository, it is assumed that there is a reliable communication channel between the repositories. For example, this could be a TCP/IP channel or any other commercially available channel that has built-in capabilities for detecting and correcting transmission errors. However, it is not assumed that the communication channel is secure. Provisions for security and privacy are part of the requirements for specifying and implementing repositories and thus form the need for various transactions.

Message Transmission

Transactions require that there be some communication between repositories. Communication between repositories occurs in units termed as messages. Because the communication line is assumed to be unsecure, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.

Key management and security is instrumental in the success of a public key encryption system. In the currently preferred embodiment, one or more master repositories maintain the keys and create the identification certificates used by the repositories.

When a sending repository transmits a message to a receiving repository, the sending repository encrypts all of its data using the public writing key of the receiving repository. The sending repository includes its name, the name of the receiving repository, a session identifier such as a nonce (described below), and a message counter in each message.

In this way, the communication can only be read (to a high probability) by the receiving repository, which holds the private checking key for decryption. The auxiliary data is used to guard against various replay attacks to security. If messages ever arrive with the wrong counter or an old nonce, the repositories can assume that someone is interfering with communication and the transaction terminated.

The respective public keys for the repositories to be used for encryption are obtained in the registration transaction described below.

Session Initiation Transactions

A usage transaction is carried out in a session between repositories. For usage transactions involving more than one repository, or for financial transactions between a repository and a credit server, a registration transaction is performed. A second transaction termed a login transaction, may also be needed to initiate the session. The goal of the registration transaction is to establish a secure channel between two repositories who know each others identities. As it is assumed that the communication channel between the repositories is reliable but not secure, there is a risk that a non-repository may mimic the protocol in order to gain illegitimate access to a repository.

The registration transaction between two repositories is described with respect to Figures 16 and 17. The steps described are from the perspective of a "repository-1" registering its identity with a "repository-2". The registration must be symmetrical so the same set of steps will be repeated for repository-2 registering its identity with repository-1. Referring to Figure 16, repository-1 first generates an encrypted registration identifier, step 1601 and then generates a registration message, step 1602. A registration message is comprised of an identifier of a master repository, the identification certificate for the repository-1 and an encrypted random registration identifier. The identification certificate is encrypted by the master repository in its private key and attests to the fact that the repository (here repository-1) is a bona fide repository. The identification certificate also contains a public key for the repository, the repository security level and a timestamp (indicating a time after which the certificate is no longer valid.) The registration identifier is a number generated by the repository for this registration. The registration identifier is unique to the session and is encrypted in repository-1's private key. The registration identifier is used to improve security of authentication by detecting certain kinds of communications based attacks. Repository-1 then transmits the registration message to repository-2, step 1603.

Upon receiving the registration message, repository-2 determines if it has the needed public key for the master repository, step 1604. If repository-2 does not have the needed public key to decrypt the identification certificate, the registration transaction terminates in an error, step 1618.

Assuming that repository-2 has the proper public key the identification certificate is decrypted, step 1605. Repository-2 saves the encrypted registration identifier, step 1606, and extracts the repository identifier, step 1607. The extracted repository identifier is checked against a "hotlist" of compromised document repositories, step 1608. In the currently preferred embodiment, each repository will contain "hotlists" of compromised repositories. If the repository is on the "hotlist', the registration transaction terminates in an error per step 1618. Repositories can be removed from the hotlist when their certificates expire, so that the list does not need to grow without bound. Also, by keeping a short list of hotlist certificates that it has previously received, a repository can avoid the work of actually going through the list. These lists would be encrypted by a master repository. A minor variation on the approach to improve efficiency would have the repositories first exchange lists of names of hotlist certificates, ultimately exchanging only those lists that they had not previously received. The "hotlists" are maintained and distributed by Master repositories.

Note that rather than terminating in error, the transaction could request that another registration message be sent based on an identification certificate created by another master repository. This may be repeated until a satisfactory identification certificate is found, or it is determined that trust cannot be established.

Assuming that the repository is not on the hotlist, the repository identification needs to be verified. In other words, repository-2 needs to validate that the repository on the other end is really repository-1. This is termed performance testing and is performed in order to avoid invalid access to the repository via a counterfeit repository replaying a recording of a prior session initiation between repository-1 and repository-2. Performance testing is initiated by repository-2 generating a performance message, step 1609. The performance message consists of a nonce, the names of the respective repositories, the time and the registration identifier received from repository-1. A nonce is a generated message based on some random and variable information (e.g. the time or the temperature.) The nonce is used to check whether repository-1 can actually exhibit correct encrypting of a message using the private keys it claims to have, on a message that it has never seen before. The performance message is encrypted using the public key specified in the registration message of repository-1. The performance message is transmitted to repository-1, step 1610, where it is decrypted by repository-1 using its private key, step 1611. Repository-1 then checks to make sure that the names of the two repositories are correct, step 1612, that the time is accurate, step 1613 and that the registration identifier corresponds to the one it sent, step 1614. If any of these tests fails, the transaction is terminated per step 1616. Assuming that the tests are passed, repository-1 transmits the nonce to repository-2 in the clear, step 1615. Repository-2 then compares the received nonce to the original nonce, step 1617. If they are not identical, the registration transaction terminates in an error per step 1618. If they are the same, the registration transaction has successfully completed.

At this point, assuming that the transaction has not terminated, the repositories exchange messages containing session keys to be used in all communications during the session and synchronize their clocks. Figure 17 illustrates the session information exchange and clock synchronization steps (again from the perspective of repository-1.) Referring to Figure 17, repository-1 creates a session key pair, step 1701. A first key is kept private and is used by repository-1 to encrypt messages. The second key is a public key used by repository-2 to decrypt messages. The second key is encrypted using the public key of repository-2, step 1702 and is sent to repository-2, step 1703. Upon receipt, repository-2 decrypts the second key, step 1704. The second key is used to decrypt messages in subsequent communications. When each repository has completed this step, they are both convinced that the other repository is bona fide and that they are communicating with the original. Each repository has given the other a key to be used in decrypting further communications during the session. Since that key is itself transmitted in the public key of the receiving repository only it will be able to decrypt the key which is used to decrypt subsequent messages.

After the session information is exchanged, the repositories must synchronize their clocks. Clock synchronization is used by the repositories to establish an agreed upon time base for the financial records of their mutual transactions. Referring back to Figure 17, repository-2 initiates clock synchronization by generating a time stamp exchange message, step 1705, and transmits it to repository-1, step 1706. Upon receipt, repository-1 generates its own time stamp message, step 1707 and transmits it back to repository-2, step 1708. Repository-2 notes the current time, step 1709 and stores the time received from repository-1, step 1710. The current time is compared to the time received from repository-1, step 1711. The difference is then checked to see if it exceeds a predetermined tolerance (e.g. one minute), step 1712. If it does, repository-2 terminates the transaction as this may indicate tampering with the repository, step 1713. If not repository-2 computes an adjusted time delta, step 1714. The adjusted time delta is the difference between the clock time of repository-2 and the average of the times from repository-1 and repository-2.

To achieve greater accuracy, repository-2 can request the time again up to a fixed number of times (e.g. five times), repeat the clock synchronization steps, and average the results.

A second session initiation transaction is a Login transaction. The Login transaction is used to check the authenticity of a user requesting a transaction. A Login transaction is particularly prudent for the authorization of financial transactions that will be charged to a credit server. The Login transaction involves an interaction between the user at a user interface and the credit server associated with a repository. The information exchanged here is a login string supplied by the repository/credit server to identify itself to the user, and a Personal Identification Number (PIN) provided by the user to identify himself to the credit server. In the event that the user is accessing a credit server on a repository different from the one on which the user interface resides, exchange of the information would be encrypted using the public and private keys of the respective repositories.

Billing Transactions

Billing Transactions are concerned with monetary transactions with a credit server. Billing Transactions are carried out when all other conditions are satisfied and a usage fee is required for granting the request. For the most part, billing transactions are well understood in the state of the art. These transactions are between a repository and a credit server, or between a credit server and a billing clearinghouse. Briefly, the required transactions include the following:

- Registration and LOGIN transactions by which the repository and user establish their bona fides to a credit server. These transactions would be entirely internal in cases where the repository and credit server are implemented as a single system.
- Registration and LOGIN transactions, by which a credit server establishes its bona fides to a billing clearinghouse.
- An Assign-fee transaction to assign a charge. The information in this transaction would include a transaction identifier, the identities of the repositories in the transaction, and a list of charges from the parts of the digital work. If there has been any unusual event in the transaction such as an interruption of communications, that information is included as well.
- A Begin-charges transaction to assign a charge. This transaction is much the same as an assign-fee transaction except that it is used for metered use. It includes the same information as the assign-fee transaction as well as the usage fee information. The credit-server is then responsible for running a clock.
- An End-charges transaction to end a charge for metered use. (In a variation on this approach, the repositories would exchange periodic charge information for each block of time.)
- A report-charges transaction between a personal credit server and a billing clearinghouse. This transaction is invoked at least once per billing period. It is used to pass along information about charges. On debit and credit cards, this transaction would also be used to update balance information and credit limits as needed.

All billing transactions are given a transaction ID and are reported to the credit severs by both the server and the client. This reduces possible loss of billing information if one of the parties to a transaction loses a banking card and provides a check against tampering with the system.

Usage Transactions

After the session initiation transactions have been completed, the usage request may then be processed. To simplify the description of the steps carried out in processing a usage request, the term requester is used to refer to a repository in the requester mode which is initiating a request, and the term server is used to refer to a repository in the server mode and which contains the desired digital work. In many cases such as requests to print or view a work, the requester and server may be the same device and the transactions described in the following would be entirely internal. In such instances, certain transaction steps, such as the registration transaction, need not be performed.

There are some common steps that are part of the semantics of all of the usage rights transactions. These steps are referred to as the common transaction steps. There are two sets -- the "opening" steps and the "closing" steps. For simplicity, these are listed here rather than repeating them in the descriptions of all of the usage rights transactions.

Transactions can refer to a part of a digital work, a complete digital work, or a Digital work containing other digital works. Although not described in detail herein, a transaction may even refer to a folder comprised of a plurality of digital works. The term "work" is used to refer to what ever portion or set of digital works is being accessed.

Many of the steps here involve determining if certain conditions are satisfied. Recall that each usage right may have one or more conditions which must be satisfied before the right can be exercised. Digital works have parts and parts have parts. Different parts can have different rights and fees. Thus, it is necessary to verify that the requirements are met for ALL of the parts that are involved in a transaction For brevity, when reference is made to checking whether the rights exist and conditions for exercising are satisfied, it is meant that all such checking takes place for each of the relevant parts of the work.

Figure 18 illustrates the initial common opening and closing steps for a transaction. At this point it is assumed that registration has occurred and that a "trusted" session is in place. General tests are tests on usage rights associated with the folder containing the work or some containing folder higher in the file system hierarchy. These tests correspond to requirements imposed on the work as a consequence of its being on the particular repository, as opposed to being attached to the work itself. Referring to Figure 18, prior to initiating a usage transaction, the requester performs any general tests that are required before the right associated with the transaction can be exercised, step, 1801. For example, install, uninstall and delete rights may be implemented to require that a requester have an authorization certificate before the right can be exercised. Another example is the requirement that a digital ticket be present and punched before a digital work may be copied to a requester. If any of the general tests fail, the transaction is not initiated, step, 1802. Assuming that such required tests are passed, upon receiving the usage request, the server generates a transaction identifier that is used in records or reports of the transaction, step 1803. The server then checks whether the digital work has been granted the right corresponding to the requested transaction, step 1804. If the digital work has not been granted the right corresponding to the request, the transaction terminates, step 1805. If the digital work has been granted the requested right, the server then determines if the various conditions for exercising the right are satisfied. Time based conditions are examined, step 1806. These conditions are checked by examining the time specification for the the version of the right. If any of the conditions are not satisfied, the transaction terminates per step 1805.

Assuming that the time based conditions are satisfied, the server checks security and access conditions, step 1807. Such security and access conditions are satisfied if: 1) the requester is at the specified security class, or a higher security class, 2) the server satisfies any specified authorization test and 3) the requester satisfies any specified authorization tests and has any required digital tickets. If any of the conditions are not satisfied, the transaction terminates per step 1805.

Assuming that the security and access conditions are all satisfied, the server checks the copy count condition, step 1808. If the copy count equals zero, then the transaction cannot be completed and the transaction terminates per step 1805.

Assuming that the copy count does not equal zero, the server checks if the copies in use for the requested right is greater than or equal to any copy count for the requested right (or relevant parts), step 1809. If the copies in use is greater than or equal to the copy count, this indicates that usage rights for the version of the transaction have been exhausted. Accordingly, the server terminates the transaction, step 1805. If the copy count is less than the copies in use for the transaction the transaction can continue, and the copies in use would be incremented by the number of digital works requested in the transaction, step 1810.

The server then checks if the digital work has a "Loan" access right, step 1811. The "Loan" access right is a special case since remaining rights may be present even though all copies are loaned out. If the digital work has the "Loan" access right, a check is made to see if all copies have been loaned out, step 1812. The number of copies that could be loaned is the sum of the Copy-Counts for all of the versions of the loan right of the digital work. For a composite work, the relevant figure is the minimal such sum of each of the components of the composite work. If all copies have been loaned out, the remaining rights are determined, step 1813. The remaining-rights is determined from the remaining rights specifications from the versions of the Loan right. If there is only one version of the Loan right, then the determination is simple. The remaining rights are the ones specified in that version of the Loan right, or none if Remaining-Rights: is not specified. If there are multiple versions of the Loan right and all copies of all of the versions are loaned out, then the remaining rights is taken as the minimum set (intersection) of remaining rights across all of the versions of the loan right. The server then determines if the requested right is in the set of remaining rights, step 1814. If the requested right is not in the set of remaining rights, the server terminates the transaction, step 1805.

If Loan is not a usage right for the digital work or if all copies have not been loaned out or the requested right is in the set of remaining rights, fee conditions for the right are then checked, step 1815. This will initiate various financial transactions between the repository and associated credit server. Further, any metering of usage of a digital work will commence. If any financial transaction fails, the transaction terminates per step 1805.

It should be noted that the order in which the conditions are checked need not follow the order of steps 1806-1815.

At this point, right specific steps are now performed and are represented here as step 1816. The right specific steps are described in greater detail below.

The common closing transaction steps are now performed. Each of the closing transaction steps are performed by the server after a successful completion of a transaction. Referring back to Figure 18, the copies in use value for the requested right is decremented by the number of copies involved in the transaction, step 1817. Next, if the right had a metered usage fee specification, the server subtracts the elapsed time from the Remaining-Use-Time associated with the right for every part involved in the transaction, step 1818. Finally, if there are fee specifications associated with the right, the server initiates End-Charge financial transaction to confirm billing, step 1819.

Transmission Protocol

An important area to consider is the transmission of the digital work from the server to the requester. The transmission protocol described herein refers to events occurring after a valid session has been created. The transmission protocol must handle the case of disruption in the communications between the repositories. It is assumed that interference such as injecting noise on the communication channel can be detected by the integrity checks (e.g., parity, checksum, etc.) that are built into the transport protocol and are not discussed in detail herein.

The underlying goal in the transmission protocol is to preclude certain failure modes, such as malicious or accidental interference on the communications channel. Suppose, for example, that a user pulls a card with the credit server at a specific time near the end of a transaction. There should not be a vulnerable time at which "pulling the card" causes the repositories to fail to correctly account for the number of copies of the work that have been created. Restated, there should be no time at which a party can break a connection as a means to avoid payment after using a digital work.

If a transaction is interrupted (and fails), both repositories restore the digital works and accounts to their state prior to the failure, modulo records of the failure itself.

Figure 19 is a state diagram showing steps in the process of transmitting information during a transaction. Each box represents a state of a repository in either the server mode (above the central dotted line 1901) or in the requester mode (below the dotted line 1901). Solid arrows stand for transitions between states. Dashed arrows stand for message communications between the repositories. A dashed message arrow pointing to a solid transition arrow is interpreted as meaning that the transition takes place when the message is received. Unlabeled transition arrows take place unconditionally. Other labels on state transition arrows describe conditions that trigger the transition.

Referring now to Figure 19, the server is initially in a state 1902 where a new transaction is initiated via start message 1903. This message includes transaction information including a transaction identifier and a count of the blocks of data to be transferred. The requester, initially in a wait state 1904 then enters a data wait state 1905.

The server enters a data transmit state 1906 and transmits a block of data 1907 and then enters a wait for acknowledgement state 1908. As the data is received, the requester enters a data receive state 1909 and when the data blocks are completely received it enters an acknowledgement state 1910 and transmits an Acknowledgement message 1911 to the server.

If there are more blocks to send, the server waits until receiving an Acknowledgement message from the requester. When an Acknowledgement message is received it sends the next block to the requester and again waits for acknowledgement. The requester also repeats the same cycle of states.

If the server detects a communications failure before sending the last block, it enters a cancellation state 1912 wherein the transaction is cancelled. Similarly, if the requester detects a communications failure before receiving the last block it enters a cancellation state 1913.

If there are no more blocks to send, the server commits to the transaction and waits for the final Acknowledgement in state 1914. If there is a communications failure before the server receives the final Acknowledgement message, it still commits to the transaction but includes a report about the event to its credit server in state 1915. This report serves two purposes. It will help legitimize any claims by a user of having been billed for receiving digital works that were not completely received. Also it helps to identify repositories and communications lines that have suspicious patterns of use and interruption. The server then enters its completion state 1916.

On the requester side, when there are no more blocks to receive, the requester commits to the transaction in state 1917. If the requester detects a communications failure at this state, it reports the failure to its credit server in state 1918, but still commits to the transaction. When it has committed, it sends an acknowledgement message to the server. The server then enters its completion state 1919.

The key property is that both the server and the requester cancel a transaction if it is interrupted before all of the data blocks are delivered, and commits to it if all of the data blocks have been delivered.

There is a possibility that the server will have sent all of the data blocks (and committed) but the requester will not have received all of them and will cancel the transaction. In this case, both repositories will presumably detect a communications failure and report it to their credit server. This case will probably be rare since it depends on very precise timing of the communications failure. The only consequence will be that the user at the requester repository may want to request a refund from the credit services -- and the case for that refund will be documented by reports by both repositories.

To prevent loss of data, the server should not delete any transferred digital work until receiving the final acknowledgement from the requester. But it also should not use the file. A well known way to deal with this situation is called "two-phase commit" or 2PC.

Two-phase commit works as follows. The first phase works the same as the method described above. The server sends all of the data to the requester. Both repositories mark the transaction (and appropriate files) as uncommitted. The server sends a ready-to-commit message to the requester. The requester sends back an acknowledgement. The server then commits and sends the requester a commit message. When the requester receives the commit message, it commits the file.

If there is a communication failure or other crash, the requester must check back with the server to determine the status of the transaction. The server has the last word on this. The requester may have received all of the data, but if it did not get the final message, it has not committed. The server can go ahead and delete files (except for transaction records) once it commits, since the files are known to have been fully transmitted before starting the 2PC cycle.

There are variations known in the art which can be used to achieve the same effect. For example, the server could use an additional level of encryption when transmitting a work to a client. Only after the client sends a message acknowledging receipt does it send the key. The client then agrees to pay for the digital work. The point of this variation is that it provides a clear audit trail that the client received the work. For trusted systems, however, this variation adds a level of encryption for no real gain in accountability.

The transaction for specific usage rights are now discussed.

The Copy Transaction

A Copy transaction is a request to make one or more independent copies of the work with the same or lesser usage rights. Copy differs from the extraction right discussed later in that it refers to entire digital works or entire folders containing digital works. A copy operation cannot be used to remove a portion of a digital work.

- The requester sends the server a message to initiate the Copy Transaction. This message indicates the work to be copied, the version of the copy right to be used for the transaction, the destination address information (location in a folder) for placing the work, the file data for the work (including its size), and the number of copies requested.
- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the client according to the transmission protocol. If a Next-Set-Of-Rights has been provided in the version of the right, those rights are transmitted as the rights for the work. Otherwise, the rights of the original are transmitted. In any event, the Copy-Count field for the copy of the digital work being sent right is set to the number-of-copies requested.
- The requester records the work contents, data, and usage rights and stores the work. It records the date and time that the copy was made in the properties of the digital work.
- The repositories perform the common closing transaction steps.

The Transfer Transaction

A Transfer transaction is a request to move copies of the work with the same or lesser usage rights to another repository. In contrast with a copy transaction, this results in removing the work copies from the server.

- The requester sends the server a message to initiate the Transfer Transaction. This message indicates the work to be transferred, the version of the transfer right to be used in the transaction, the destination address information for placing the work, the file data for the work, and the number of copies involved.

- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the work. Otherwise, the rights of the original are transmitted.

In either case, the Copy-Count field for the transmitted rights are set to the number-of-copies requested.

- The requester records the work contents, data, and usage rights and stores the work.
- The server decrements its copy count by the number of copies involved in the transaction.
- The repositories perform the common closing transaction steps.
- If the number of copies remaining in the server is now zero, it erases the digital work from its memory.

The Loan Transaction

A loan transaction is a mechanism for loaning copies of a digital work. The maximum duration of the loan is determined by an internal parameter of the digital work. Works are automatically returned after a predetermined time period.

- The requester sends the server a message to initiate the Transfer Transaction. This message indicates the work to be loaned, the version of the loan right to be used in the transaction, the destination address information for placing the work, the number of copies involved, the file data for the work, and the period of the loan.
- The server checks the validity of the requested loan period, and ends with an error if the period is not valid. Loans for a loaned copy cannot extend beyond the period of the original loan to the server.
- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the work. Otherwise, the rights of the original are transmitted, as modified to reflect the loan period.
- The requester records the digital work contents, data, usage rights, and loan period and stores the work.
- The server updates the usage rights information in the digital work to reflect the number of copies loaned out.
- The repositories perform the common closing transaction steps.
- The server updates the usage rights data for the digital work. This may preclude use of the work until it is returned from the loan. The user on the requester platform can now use the transferred copies of the digital work. A user accessing the original repository cannot use the digital work , unless there are copies remaining. What happens next depends on the order of events in time.

Case 1. If the time of the loan period is not yet exhausted and the requester sends the repository a Return message.

- The return message includes the requester identification, and the transaction ID.
- The server decrements the copies-in-use field by the number of copies that were returned. (If the number of digital works returned is greater than the number actually borrowed, this is treated as an error.) This step may now make the work available at the server for other users.
- The requester deactivates its copies and removes the contents from its memory.

Case 2. If the time of the loan period is exhausted and the requester has not yet sent a Return message.

- The server decrements the copies-in-use field by the number digital works that were borrowed.
- The requester automatically deactivates its copies of the digital work. It terminates all current uses and erases the digital work copies from memory. One question is why a requester would ever return a work earlier than the period of the loan, since it would be returned automatically anyway. One reason for early return is that there may be a metered fee which determines the cost of the loan. Returning early may reduce that fee.

The Play Transaction

A play transaction is a request to use the contents of a work. Typically, to "play" a work is to send the digital work through some kind of transducer, such as a speaker or a display device. The request implies the intention that the contents will not be communicated digitally to any other system. For example, they will not be sent to a printer, recorded on any digital medium, retained after the transaction or sent to another repository.

This term "play" is natural for examples like playing music, playing a movie, or playing a video game. The general form of play means that a "player" is used to use the digital work. However, the term play covers all media and kinds of recordings. Thus one would "play" a digital work, meaning, to render it for reading, or play a computer program, meaning to execute it. For a digital ticket the player would be a digital ticket agent.

- The requester sends the server a message to initiate the play transaction. This message indicates the work to be played, the version of the play right to be used in the transaction, the identity of the player being used, and the file data for the work.
- The server checks the validity of the player identification and the compatibility of the player identification with the player specification in the right. It ends with an error if these are not satisfactory.
- The repositories perform the common opening transaction steps.
- The server and requester read and write the blocks of data as requested by the player according to the transmission protocol. The requester plays the work contents, using the player.
- When the player is finished, the player and the requester remove the contents from their memory.
- The repositories perform the common closing transaction steps.

The Print Transaction

A Print transaction is a request to obtain the contents of a work for the purpose of rendering them on a "printer." We use the term "printer" to include the common case of writing with ink on paper. However, the key aspect of "printing" in our use of the term is that it makes a copy of the digital work in a place outside of the protection of usage rights. As with all rights, this may require particular authorization certificates.

Once a digital work is printed, the publisher and user are bound by whatever copyright laws are in effect. However, printing moves the contents outside the control of repositories. For example, absent any other enforcement mechanisms, once a digital work is printed on paper, it can be copied on ordinary photocopying machines without intervention by a repository to collect usage fees. If the printer to a digital disk is permitted, then that digital copy is outside of the control of usage rights. Both the creator and the user know this, although the creator does not necessarily give tacit consent to such copying, which may violate copyright laws.

- The requester sends the server a message to initiate a Print transaction. This message indicates the work to be played, the identity of the printer being used, the file data for the work, and the number of copies in the request.
- The server checks the validity of the printer identification and the compatibility of the printer identification with the printer specification in the right. It ends with an error if these are not satisfactory.
- The repositories perform the common opening transaction steps.
- The'server transmits blocks of data according to the transmission protocol.
- The requester prints the work contents, using the printer.
- When the printer is finished, the printer and the requester remove the contents from their memory.
- The repositories perform the common closing transaction steps.

The Backup Transaction

A Backup transaction is a request to make a backup copy of a digital work, as a protection against media failure. In the context of repositories, secure backup copies differ from other copies in three ways: (1) they are made under the control of a Backup transaction rather than a Copy transaction, (2) they do not count as regular copies, and (3) they are not usable as regular copies. Generally, backup copies are encrypted.

Although backup copies may be transferred or copied, depending on their assigned rights, the only way to make them useful for playing, printing or embedding is to restore them.

The output of a Backup operation is both an encrypted data file that contains the contents and description of a work, and a restoration file with an encryption key for restoring the encrypted contents. In many cases, the encrypted data file would have rights for "printing" it to a disk outside of the protection system, relying just on its encryption for security. Such files could be stored anywhere that was physically safe and convenient. The restoration file would be held in the repository. This file is necessary for the restoration of a backup copy. It may have rights for transfer between repositories.

- The requester sends the server a message to initiate a backup transaction. This message indicates the work to be backed up, the version of the backup right to be used in the transaction, the destination address information for placing the backup copy, the file data for the work.
- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester. If a Next-Set-Of-Rights has been provided,

those rights are transmitted as the rights for the work. Otherwise, a set of default rights for backup files of the original are transmitted by the server.

- The requester records the work contents, data, and usage rights. It then creates a one-time key and encrypts the contents file. It saves the key information in a restoration file.
- The repositories perform the common closing transaction steps.

In some cases, it is convenient to be able to archive the large, encrypted contents file to secure offline storage, such as a magneto-optical storage system or magnetic tape. This creation of a non-repository archive file is as secure as the encryption process. Such non-repository archive storage is considered a form of "printing" and is controlled by a print right with a specified "archive-printer." An archive-printer device is programmed to save the encrypted contents file (but not the description file) offline in such a way that it can be retrieved.

The Restore Transaction

A Restore transaction is a request to convert an encrypted backup copy of a digital work into a usable copy. A restore operation is intended to be used to compensate for catastrophic media failure. Like all usage rights, restoration rights can include fees and access tests including authorization checks.

- The requester sends the server a message to initiate a Restore transaction. This message indicates the work to be restored. the version of the restore right for the transaction, the destination address information for placing the work, and the file data for the work.
- The server verifies that the contents file is available (i.e. a digital work corresponding to the request has been backed-up) If it is not. it ends the transaction with an error.
- The repositories perform the common opening transaction steps.
- The server retrieves the key from the restoration file. It decrypts the work contents, data, and usage rights.
- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the work. Otherwise, a set of default rights for backup files of the original are transmitted by the server.
- The requester stores the digital work.
- The repositories perform the common closing transaction steps.

The Delete Transaction

A Delete transaction deletes a digital work or a number of copies of a digital work from a repository. Practically all digital works would have delete rights.

- The requester sends the server a message to initiate a delete transaction. This message indicates the work to be deleted, the version of the delete right for the transaction.
- The repositories perform the common opening transaction steps.
- The server deletes the file, erasing it from the file system.
- The repositories perform the common closing transaction steps.

The Directory Transaction

A Directory transaction is a request for information about folders, digital works, and their parts. This amounts to roughly the same idea as protection codes in a conventional file system like TENEX, except that it is generalized to the full power of the access specifications of the usage rights language.

The Directory transaction has the important role of passing along descriptions of the rights and fees associated with a digital work. When a user wants to exercise a right, the user interface of his repository implicitly makes a directory request to determine the versions of the right that are available. Typically these are presented to the user -- such as with different choices of billing for exercising a right. Thus, many directory transactions are invisible to the user and are exercised as part of the normal process of exercising all rights.

- The requester sends the server a message to initiate a Directory transaction. This message indicates the file or folder that is the root of the directory request and the version of the directory right used for the transaction.
- The server verifies that the information is accessible to the requester. In particular, it does not return the names of any files that have a HIDE-NAME status in their directory specifications, and it does not return the parts of any folders or files that have HIDE-PARTS in their specification. If the information is not accessible, the server ends

the transaction with an error.

- The repositories perform the common opening transaction steps.
- The server sends the requested data to the requester according to the transmission protocol.
- The requester records the data.
- The repositories perform the common closing transaction steps.

The Folder Transaction

A Folder transaction is a request to create or rename a folder, or to move a work between folders. Together with Directory rights, Folder rights control the degree to which organization of a repository can be accessed or modified from another repository.

- The requester sends the server a message to initiate a Folder transaction. This message indicates the folder that is the root of the folder request, the version of the folder right for the transaction, an operation, and data. The operation can be one of create, rename, and move file. The data are the specifications required for the operation, such as a specification of a folder or digital work and a name.
- The repositories perform the common opening transaction steps.
- The server performs the requested operation -- creating a folder, renaming a folder, or moving a work between folders.
- The repositories perform the common closing transaction steps.

The Extract Transaction

A extract transaction is a request to copy a part of a digital work and to create a new work containing it. The extraction operation differs from copying in that it can be used to separate a part of a digital work from d-blocks or shells that place additional restrictions or fees on it. The extraction operation differs from the edit operation in that it does not change the contents of a work, only its embedding in d-blocks. Extraction creates a new digital work.

- The requester sends the server a message to initiate an Extract transaction. This message indicates the part of the work to be extracted, the version of the extract right to be used in the transaction, the destination address information for placing the part as a new work, the file data for the work, and the number of copies involved.
- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the new work. Otherwise, the rights of the original are transmitted. The Copy-Count field for this right is set to the number-of-copies requested.
- The requester records the contents, data, and usage rights and stores the work. It records the date and time that new work was made in the properties of the work.
- The repositories perform the common closing transaction steps.

The Embed Transaction

An embed transaction is a request to make a digital work become a part of another digital work or to add a shell d-block to enable the adding of fees by a distributor of the work.

- The requester sends the server a message to initiate an Embed transaction. This message indicates the work to be embedded, the version of the embed right to be used in the transaction, the destination address information for placing the part as a a work, the file data for the work, and the number of copies involved.
- The server checks the control specifications for all of the rights in the part and the destination. If they are incompatible, the server ends the transaction with an error.
- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the new work. Otherwise, the rights of the original are transmitted. The Copy-Count field for this right is set to the number-of-copies requested.
- The requester records the contents, data, and usage rights and embeds the work in the destination file.
- The repositories perform the common closing transaction steps.

The Edit Transaction

An Edit transaction is a request to make a new digital work by copying, selecting and modifying portions of an existing digital work. This operation can actually change the contents of a digital work. The kinds of changes that are permitted depend on the process being used. Like the extraction operation, edit operates on portions of a digital work. In contrast with the extract operation, edit does not affect the rights or location of the work. It only changes the contents. The kinds of changes permitted are determined by the type specification of the processor specified in the rights. In the currently preferred embodiment, an edit transaction changes the work itself and does not make a new work. However, it would be a reasonable variation to cause a new copy of the work to be made.

- The requester sends the server a message to initiate an Edit transaction. This message indicates the work to be edited, the version of the edit right to be used in the transaction, the file data for the work (including its size), the process-ID for the process, and the number of copies involved.
- The server checks the compatibility of the process-ID to be used by the requester against any process-ID specification in the right. If they are incompatible, it ends the transaction with an error.
- The repositories perform the common opening transaction steps.
- The requester uses the process to change the contents of the digital work as desired. (For example, it can select and duplicate parts of it; combine it with other information; or compute functions based on the information. This can amount to editing text, music, or pictures or taking whatever other steps are useful in creating a derivative work.)
- The repositories perform the common closing transaction steps.

The edit transaction is used to cover a wide range of kinds of works. The category describes a process that takes as its input any portion of a digital work and then modifies the input in some way. For example, for text, a process for editing the text would require edit rights. A process for "summarizing" or counting words in the text would also be considered editing. For a music file, processing could involve changing the pitch or tempo, or adding reverberations, or any other audio effect. For digital video works, anything which alters the image would require edit rights. Examples would be colorizing, scaling, extracting still photos, selecting and combining frames into story boards, sharpening with signal processing, and so on.

Some creators may want to protect the authenticity of their works by limiting the kinds of processes that can be performed on them. If there are no edit rights, then no processing is allowed at all. A processor identifier can be included to specify what kind of process is allowed. If no process identifier is specified, then arbitrary processors can be used. For an example of a specific process, a photographer may want to allow use of his photograph but may not want it to be colorized. A musician may want to allow extraction of portions of his work but not changing of the tonality.

Authorization Transactions

There are many ways that authorization transactions can be defined. In the following, our preferred way is to simply define them in terms of other transactions that we already need for repositories. Thus, it is convenient sometimes to speak of "authorization transactions," but they are actually made up of other transactions that repositories already have.

A usage right can specify an authorization-ID, which identifies an authorization object (a digital work in a file of a standard format) that the repository must have and which it must process. The authorization is given to the generic authorization (or ticket) server of the repository which begins to interpret the authorization.

As described earlier, the authorization contains a server identifier, which may just be the generic authorization server or it may be another server. When a remote authorization server is required, it must contain a digital address. It may also contain a digital certificate.

If a remote authorization server is required, then the authorization process first performs the following steps:

- The generic authorization server attempts to set up the communications channel. (If the channel cannot be set up, then authorization fails with an error.)
- When the channel is set up, it performs a registration process with the remote repository. (If registration fails, then the authorization fails with an error.)
- When registration is complete, the generic authorization server invokes a "Play" transaction with the remote repository, supplying the authorization document as the digital work to be played, and the remote authorization server (a program) as the "player." (If the player cannot be found or has some other error, then the authorization fails with an error.)
- The authorization server then "plays" the authorization. This involves decrypting it using either the public key of the master repository that issued the certificate or the session key from the repository that transmitted it. The authorization server then performs various tests. These tests vary according to the authorization server. They

include such steps as checking issue and validity dates of the authorization and checking any hot-lists of known invalid authorizations. The authorization server may require carrying out any other transactions on the repository as well, such as checking directories, getting some person to supply a password, or playing some other digital work. It may also invoke some special process for checking information about locations or recent events. The "script" for such steps is contained within the authorization server.

- If all of the required steps are completed satisfactorily, the authorization server completes the transaction normally, signaling that authorization is granted.

The Install Transaction

An Install transaction is a request to install a digital work as runnable software on a repository. In a typical case, the requester repository is a rendering repository and the software would be a new kind or new version of a player. Also in a typical case, the software would be copied to file system of the requester repository before it is installed.

- The requester sends the server an Install message. This message indicates the work to be installed, the version of the Install right being invoked, and the file data for the work (including its size).
- The repositories perform the common opening transaction steps.
- The requester extracts a copy of the digital certificate for the software. If the certificate cannot be found or the master repository for the certificate is not known to the requester, the transaction ends with an error.
- The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step certifies the software.)
- The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)
- The requester retrieves the instructions in the compatibility-checking script and follows them. If the software is not compatible with the repository, the installation transaction ends with an error. (This step checks platform compatibility.)
- The requester retrieves the instructions in the installation script and follows them. If there is an error in this process (such as insufficient resources), then the transaction ends with an error. Note that the installation process puts the runnable software in a place in the repository where it is no longer accessible as a work for exercising any usage rights other than the execution of the software as part of repository operations in carrying out other transactions.
- The repositories perform the common closing transaction steps.

The Uninstall Transaction

An Uninstall transaction is a request to remove software from a repository. Since uncontrolled or incorrect removal of software from a repository could compromise its behavioral integrity, this step is controlled.

- The requester sends the server an Uninstall message. This message indicates the work to be uninstalled, the version of the Uninstall right being invoked, and the file data for the work (including its size).
- The repositories perform the common opening transaction steps.
- The requester extracts a copy of the digital certificate for the software. If the certificate cannot be found or the master repository for the certificate is not known to the requester, the transaction ends with an error.
- The requester checks whether the software is installed. If the software is not installed, the transaction ends with an error.
- The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step authenticates the certification of the software, including the script for uninstalling it.)
- The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)
- The requester retrieves the instructions in the uninstallation script and follows them. If there is an error in this process (such as insufficient resources), then the transaction ends with an error.
- The repositories perform the common closing transaction steps.

Claims

1. A system for secure distribution and control of digital works between repositories comprising:

   means for creating usage rights, each instance of a usage right representing a specific instance of how a digital work may be used or distributed;
   means for attaching a created set of usage rights to a digital work;
   a communications medium for coupling repositories to enable exchange of repository transaction messages;
   a plurality of general repositories for storing and securely exchanging digital works with attached usage rights, each of said general repositories comprising:
   a storage means for storing digital works and their attached usage rights;
   an identification certificate for indicating that the associated general repository is secure;
   an external interface for removably coupling to said communications medium;
   a session initiation transaction processing means for establishing a secure and trusted session with another repository, said session initiation transaction processing means using said identification certificate;
   a usage transaction processing means having a requester mode of operation for generating usage repository transaction messages to request access to digital works stored in another general repository, said usage repository transaction message specifying a usage right, said usage transaction processing means further having a server mode of operation for determining if a request for access to a digital work stored in said storage means may be granted, said request being granted only if the usage right specified in said request is attached to said digital work; and
   an input means coupled to said usage transaction processing means for enabling user created signals to cause generation of a usage repository transaction message to request access to digital works.

2. The system as recited in Claim 1 further comprising a rendering system, said rendering system comprising:

   a rendering repository for securely accessing digital works from a general repository, said rendering repository comprising;
   a storage means for storing digital works and their attached usage rights;
   an identification certificate, said identification certificate for indicating that the rendering repository is secure;
   an external interface for removably coupling to said communications medium;
   a session initiation transaction processing means for establishing a secure and trusted session with a general repository, said session initiation transaction processing means using said identification certificate;
   a usage transaction processing means for generating usage repository transaction messages to request access to digital works stored in a general repository, said usage repository transaction message specifying a usage right;
   an input means coupled to said usage transaction processing means for enabling user created signals to cause generation of usage repository transaction messages to request access to digital works;
   a rendering device for rendering digital works.

3. The system as recited in Claim 1 wherein said means for creating usage rights is further for the specification of different sets of usage rights to be attached to digital works when a corresponding usage right is exercised.

4. The system as recited in Claim 1 wherein said usage rights grammar further defines means for specifying conditions which must be satisfied before a usage right may be exercised and said usage transaction processing means in said server mode is further comprised of means for determining if specified conditions for a usage right are satisfied before access is granted.

5. The system as recited in Claim 1 wherein a first usage right enables copying of a digital work and specification of a revenue owner who is paid a fee whenever a copy of said digital work is made.

6. A method for controlling distribution and use of digital works comprising the steps of:

   a) attaching a set of usage rights to a digital work, each of said usage rights defining a specific instance of how a digital work may be used or distributed, said usage right specifying one or more conditions which must be satisfied in order for said usage right to be exercised and a next set of usage rights to be attached to a distributed digital work;
   b) storing said digital work and its attached usage rights in a first repository;

c) a second repository initiating a request to access said digital work in said first repository, said request identifying a usage right representing how said second repository desires to use said digital work;
d) said first repository receiving said request from said second repository;
e) said first repository determining if the identified usage right is attached to said digital work;
f) said first repository denying access to said digital work if said identified usage right is not attached to said digital work;
g) if said identified usage right is attached to said digital work, said first repository determining if conditions specified by said usage right are satisfied;
h) if said conditions are not satisfied, said first repository denying access to said digital work;
i) if said conditions are satisfied, said first repository attaching a next set of usage rights to said digital work, said next set of usage rights specifying how said second repository may use and distribute said digital work; and
j) said first repository transmitting said digital work and said attached next set of usage rights to said second repository.

7. The method as recited in Claim 6 wherein said step of a second repository initiating a request to access said digital work in said first repository is further comprised of the steps of:

c1) said second repository initiating establishment of a trusted session with said first repository;
c2) said first repository performing a set of registration transaction steps with said second repository, successful completion of said set of registration transaction steps indicating that said first repository is a trusted repository;
c3) said second repository performing said set of registration transaction steps with said first repository, successful completion of said set of registration transaction steps indicating that said second repository is a trusted repository;
c4) if said first repository and said second repository each successfully complete said set of registration steps, said first and second repository exchanging session encryption and decryption keys for secure transmission of subsequent communications between said first and second repository; and
c5) if said first repository or said second repository cannot successfully complete said set of registration transaction steps, terminating said session.

8. A system for controlling distribution and use of digital works comprising:

means for attaching usage rights to said digital work, said usage rights indicating how a recipient may use and and subsequently distribute said digital work;
a communications medium for coupling repositories to enable distribution of digital works;
a plurality of repositories for managing exchange of digital works based on usage rights attached to said digital works, each of said plurality of repositories comprising:
a storage means for storing digital works and their attached usage rights:
a processor operating responsive to coded instructions;
a memory means coupled to said processor for storing coded instruction to enable said processor to operate in a first server mode for processing access requests to digital works and for attaching usage rights to digital works when transmitted to another of said plurality of repositories, a second requester mode for initiating requests to access digital works, and a session initiation mode for establishing a trusted session with another of said plurality of repositories over said communications medium;
a clock;
a repository interface for coupling to said communications medium.

9. The system as recited in Claim 8 further comprising a plurality of rendering systems for rendering of digital works, each of said rendering systems comprising:

a repository for secure receipt of a digital work; and
a rendering device having means for converting digital works to signals suitable for rendering of said digital works.

10. A method for secure access of digital works stored on a server repository, said digital works having associated therewith one or more usage rights for specifying how said digital work may be used or distributed, said method comprising the steps of:

a) a requesting repository performing a first registration transaction with a server repository, said first registration transaction for establishing to said server repository that said requesting repository is trustworthy;

b) concurrently with step a), said server repository responding with a second registration transaction, said second registration transaction for establishing to said requesting repository that said server repository is trustworthy;

c) if either said first registration transaction or said second registration transaction fails, said server repository denying access to said digital work;

d) if said first registration transaction and said second registration transaction are successful, said requesting repository initiating a usage transaction with respect to a digital work stored in said server repository, said usage transaction indicating a request to access a digital work and specifying a particular usage right;

e) determining if said usage transaction may be completed by comparing said particular usage right specified in said usage transaction and usage rights associated with said digital work;

f) if said particular usage right is not one of said usage rights associated with said digital work, denying access to said digital work; and

g) if said particular usage right is one of said usage rights associated with said digital work, granting access to said digital work and performing usage transaction steps associated with said particular usage right.

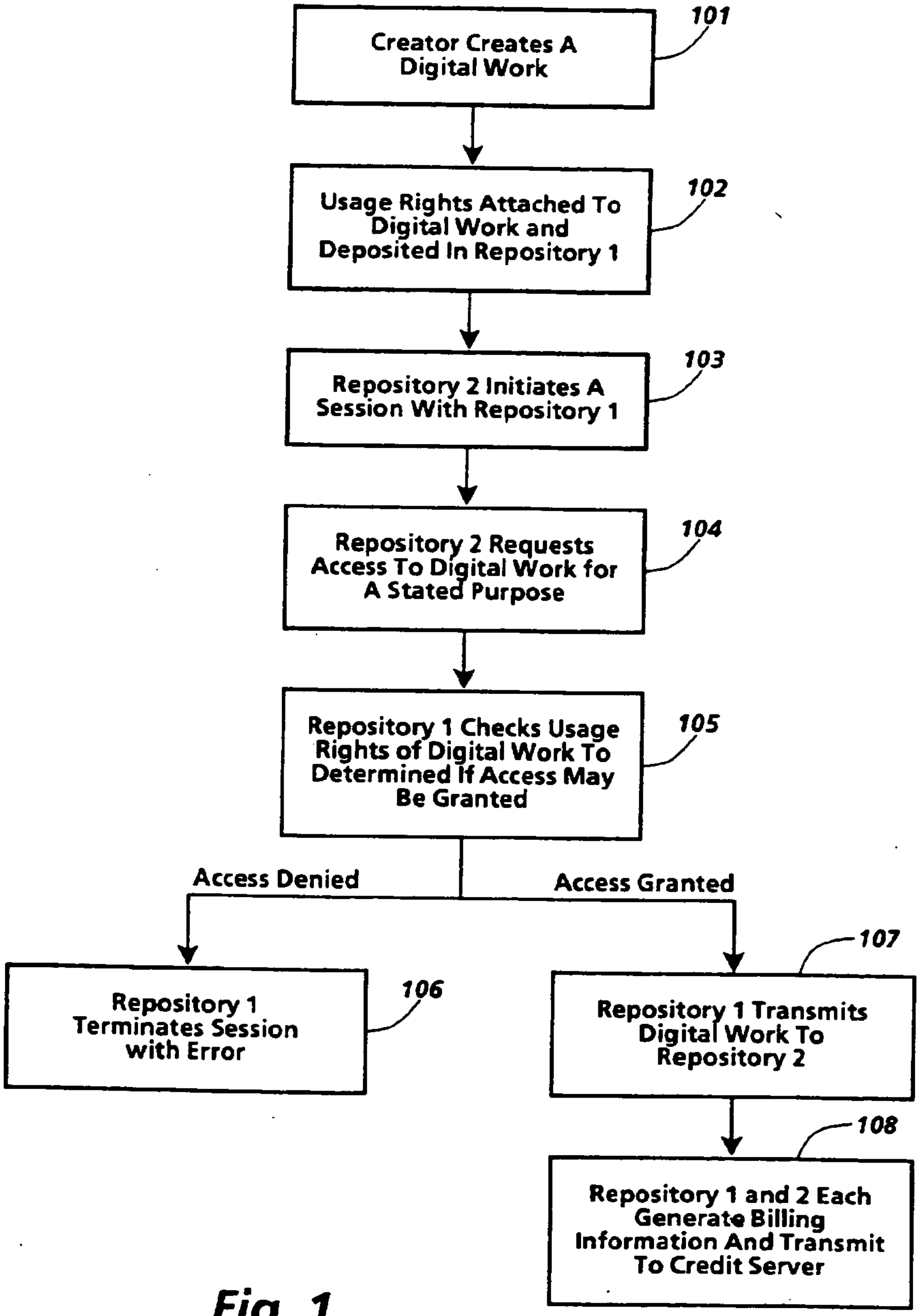

Creator Creates A Digital Work
101
Usage Rights Attached To Digital Work and Deposited In Repository 1
102
Repository 2 Initiates A Session With Repository 1
103
Repository 2 Requests Access To Digital Work for A Stated Purpose
104
Repository 1 Checks Usage Rights of Digital Work To Determined If Access May Be Granted
105
Access Denied
Access Granted
Repository 1 Terminates Session with Error
106
107
Repository 1 Transmits Digital Work To Repository 2
108
Repository 1 and 2 Each Generate Billing Information And Transmit To Credit Server

Fig. 1

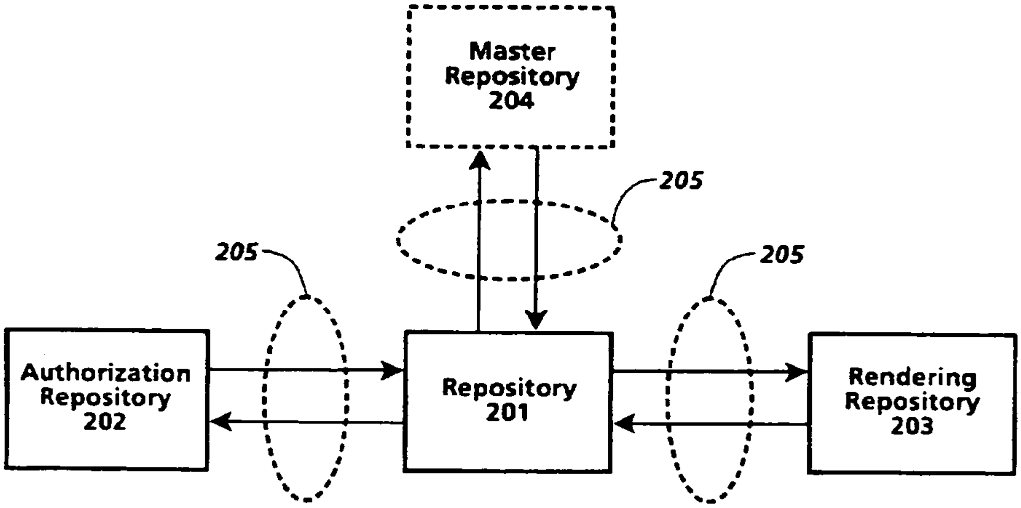

Master Repository 204
205
205
205
Authorization Repository 202
Repository 201
Rendering Repository 203

Fig. 2

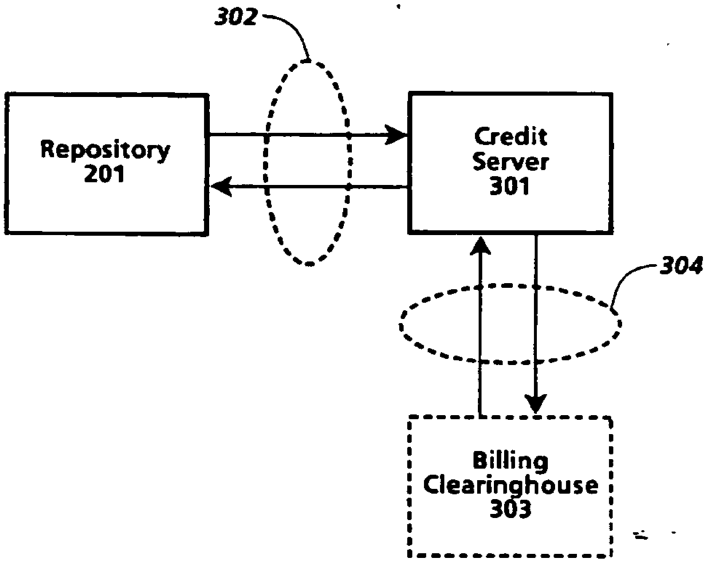

302
Repository 201
Credit Server 301
304
Billing Clearinghouse 303

Fig. 3

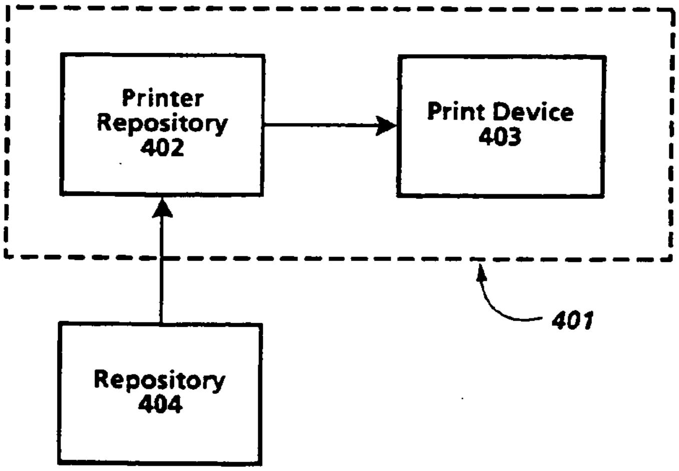

Printer Repository 402
Print Device 403
401
Repository 404

Fig. 4a

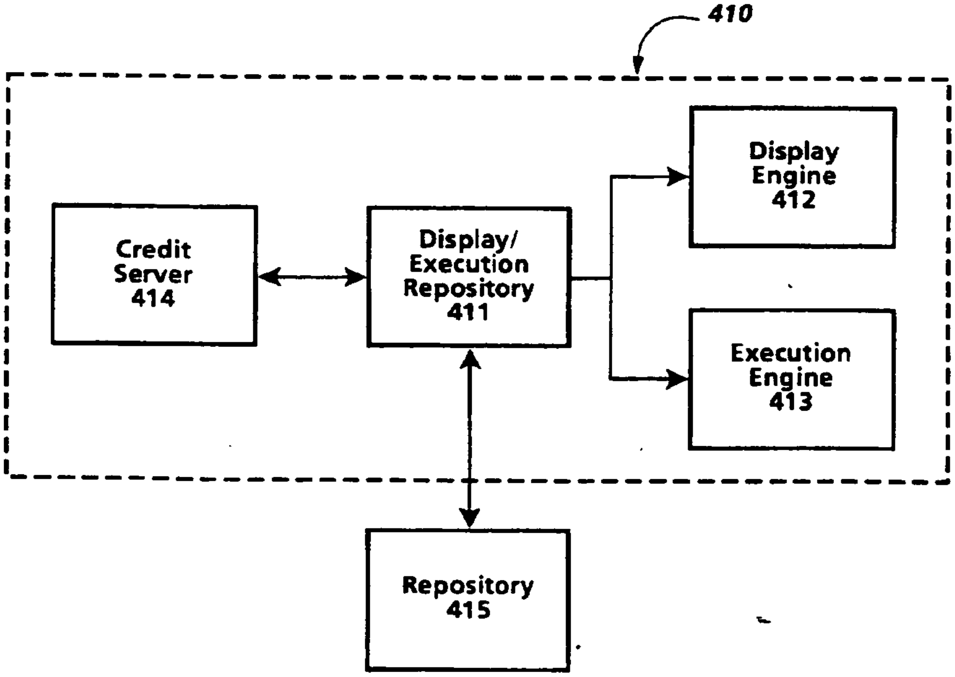

410
Credit Server 414
Display/ Execution Repository 411
Display Engine 412
Execution Engine 413
Repository 415

Fig. 4b

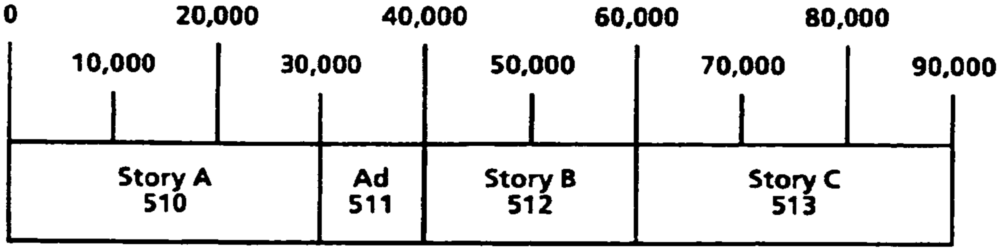

0
20,000
40,000
60,000
80,000
10,000
30,000
50,000
70,000
90,000
Story A
510
Ad
511
Story B
512
Story C
513

Fig. 5

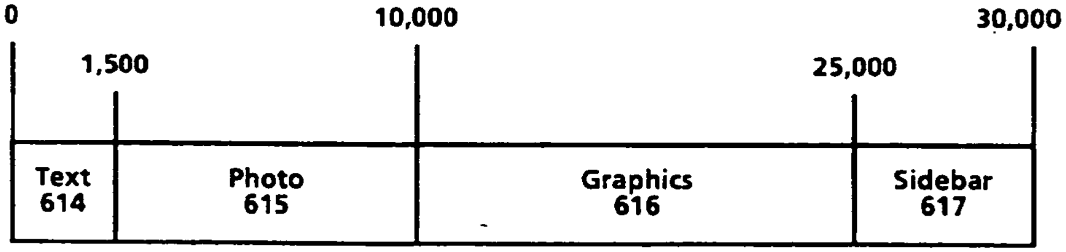

0
10,000
30,000
1,500
25,000
Text
614
Photo
615
Graphics
616
Sidebar
617

Fig. 6

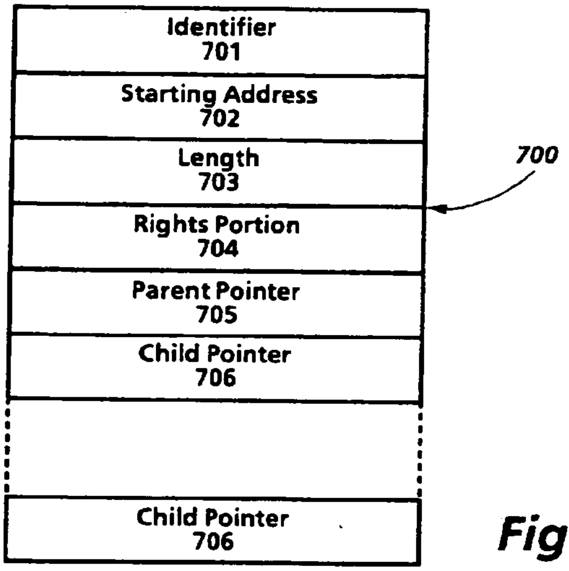


Fig. 7

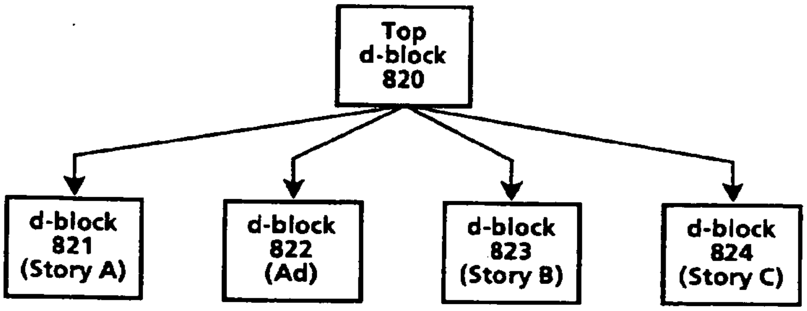


Fig. 8

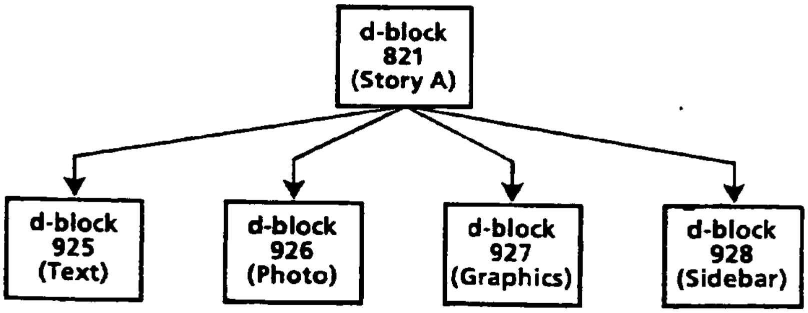


Fig. 9

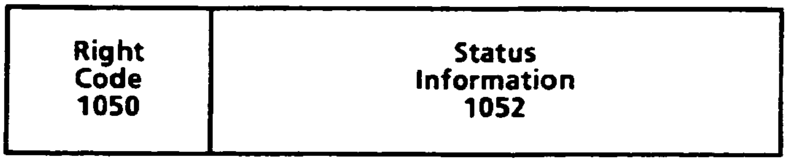

Right
Code
1050
Status
Information
1052

Fig.10

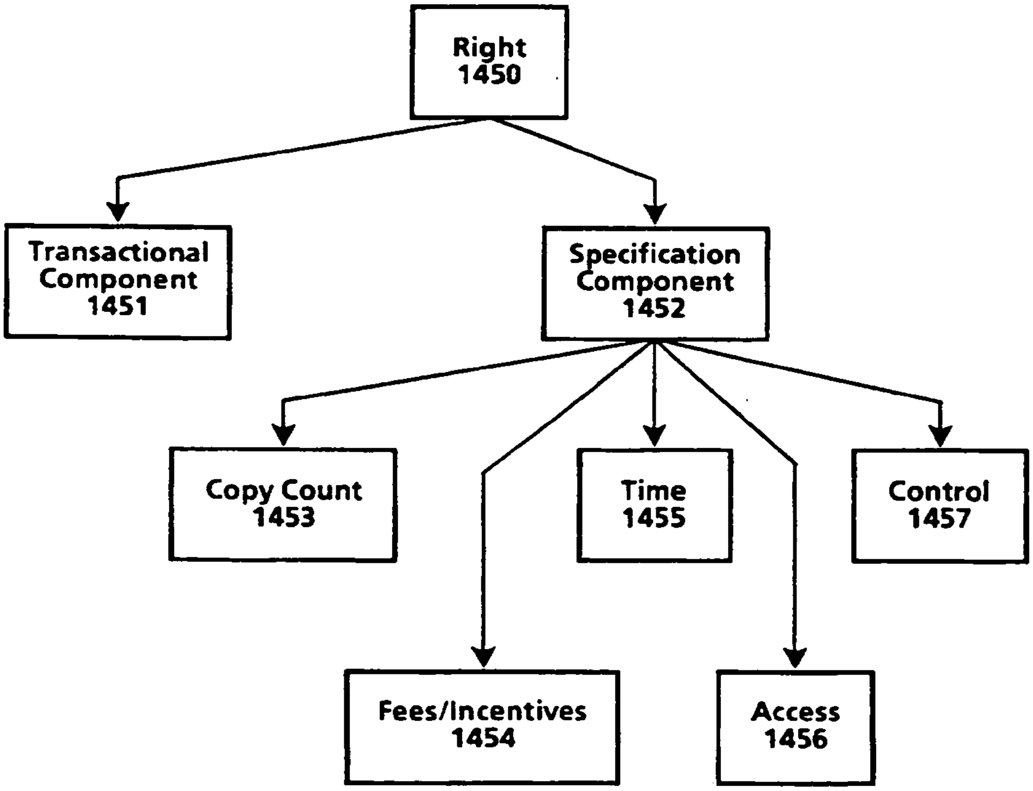

Right
1450
Transactional
Component
1451
Specification
Component
1452
Copy Count
1453
Time
1455
Control
1457
Fees/Incentives
1454
Access
1456

Fig.14

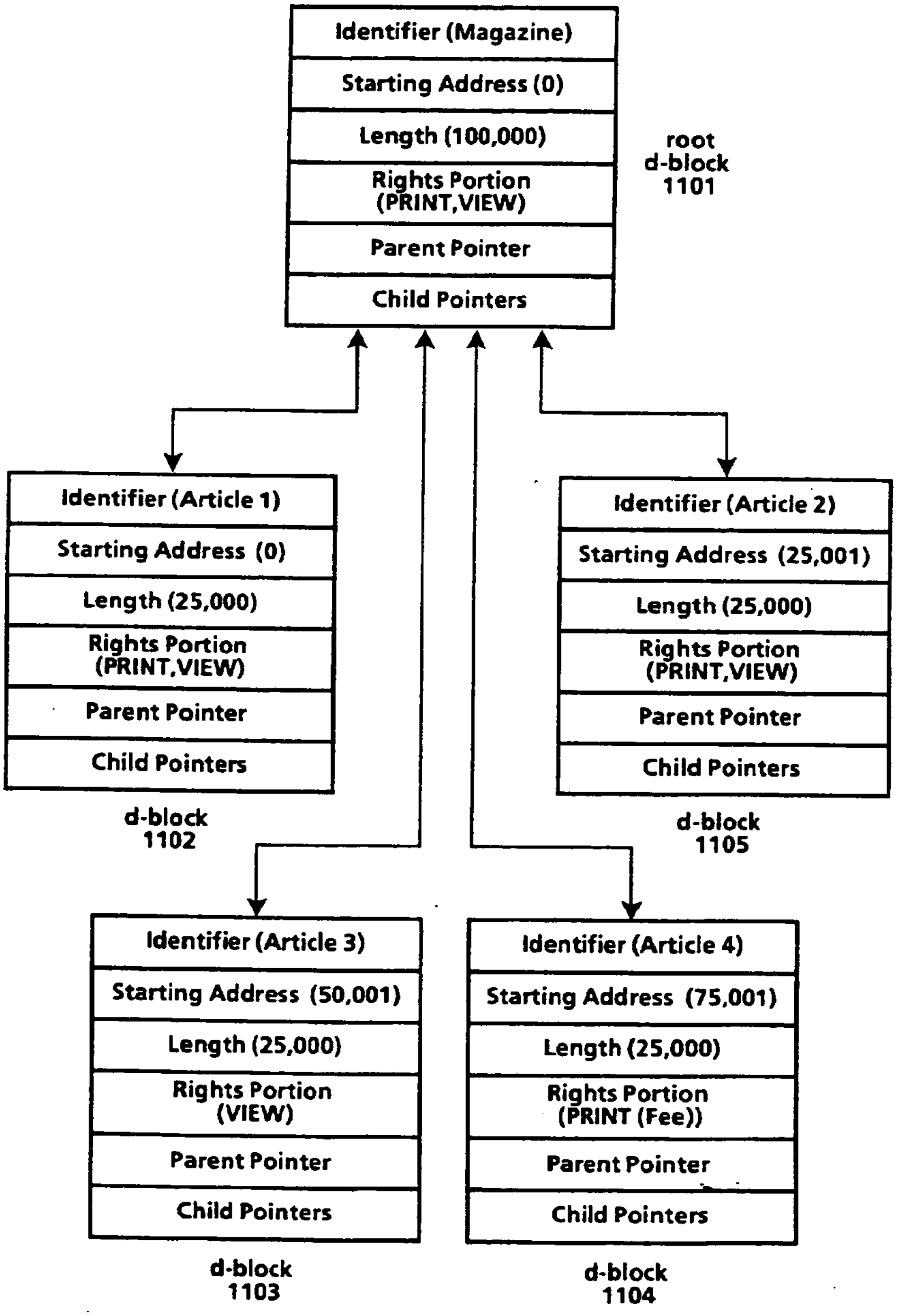

Identifier (Magazine)
Starting Address (0)
Length (100,000)
Rights Portion (PRINT,VIEW)
Parent Pointer
Child Pointers
root d-block 1101
Identifier (Article 1)
Starting Address (0)
Length (25,000)
Rights Portion (PRINT,VIEW)
Parent Pointer
Child Pointers
d-block 1102
Identifier (Article 2)
Starting Address (25,001)
Length (25,000)
Rights Portion (PRINT,VIEW)
Parent Pointer
Child Pointers
d-block 1105
Identifier (Article 3)
Starting Address (50,001)
Length (25,000)
Rights Portion (VIEW)
Parent Pointer
Child Pointers
d-block 1103
Identifier (Article 4)
Starting Address (75,001)
Length (25,000)
Rights Portion (PRINT (Fee))
Parent Pointer
Child Pointers
d-block 1104

Fig.11

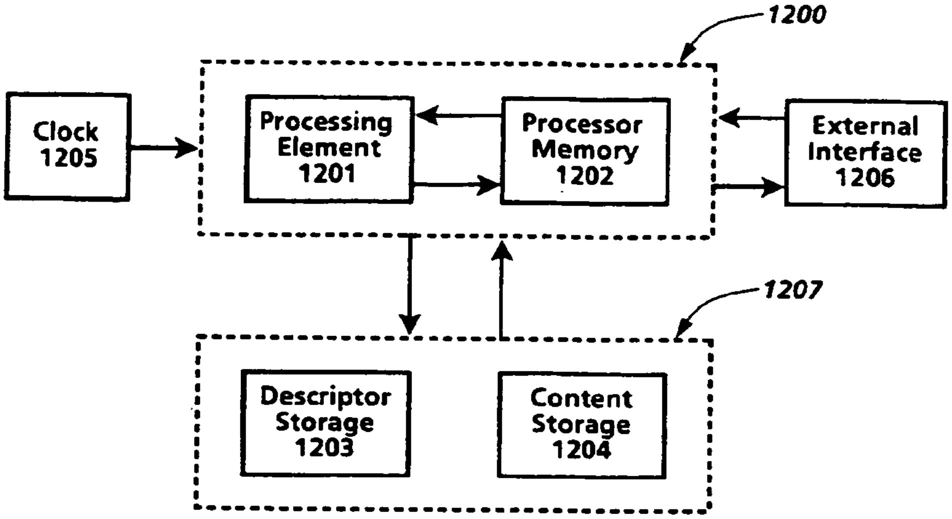

1200
Clock
1205
Processing
Element
1201
Processor
Memory
1202
External
Interface
1206
1207
Descriptor
Storage
1203
Content
Storage
1204

Fig. 12

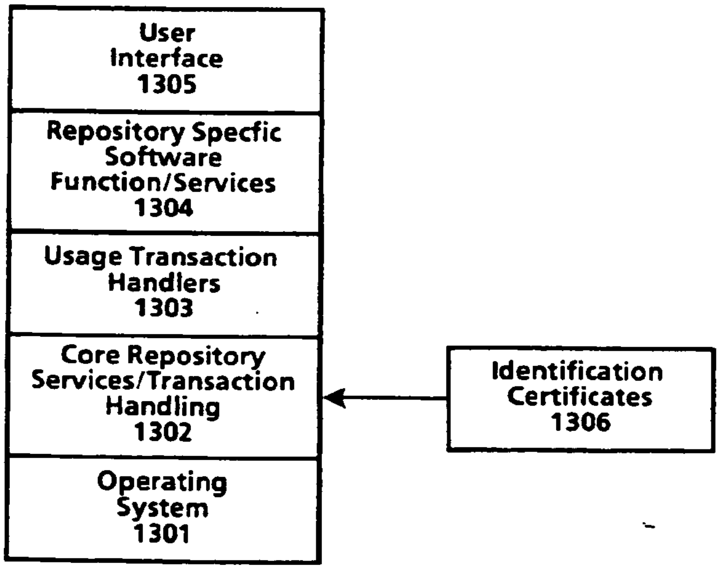

User
Interface
1305
Repository Specfic
Software
Function/Services
1304
Usage Transaction
Handlers
1303
Core Repository
Services/Transaction
Handling
1302
Operating
System
1301
Identification
Certificates
1306

Fig. 13

```
1501—Digital Work Rights:= (Rights*)
 1502—Right := (Right-Code {Copy-Count} {Control-Spec} {Time-Spec }
        {Access-Spec} {Fee-Spec})
    1503—Right-Code := Render-Code | Transport-Code | File-Management-
          Code| Derivative-Works- Code | Configuration-Code
       1504—Render-Code := [ Play : {Player: Player-ID} | Print:  {Printer: Printer-ID}]
       1505—Transport-Code := [Copy | Transfer | Loan {Remaining-Rights:
             Next-Set-of-Rights}]{(Next-Copy-Rights: Next-Set-of-Rights)}
       1506—File-Management-Code     := Backup {Back-Up-Copy-Rights:
                                        Next-Set-of-Rights} | Restore | Delete | Folder
                                        | Directory {Name: Hide-Local | Hide-Remote}
                                        {Parts: Hide-Local | Hide-Remote}
       1507—Derivative-Works-Code :=   [Extract | Embed | Edit{Process:
                                          Process-ID}] {Next-Copy-Rights :
                                          Next-Set-of Rights}
       1508—Configuration-Code := Install | Uninstall
       1509—Next-Set-of-Rights := {(Add: Set-Of-Rights)} {(Delete:
             Set-Of-Rights)} {(Replace: Set-Of-Rights )}{(Keep: Set-Of-Rights )}
1510—Copy-Count := (Copies:positive-integer | 0 | Unlimited)
1511— Control-Spec := (Control: {Restrictable | Unrestrictable}
                        {Unchargeable | Chargeable})
1512—Time-Spec := ({Fixed-Interval  | Sliding-Interval | Meter-Time}
                    Until: Expiration-Date)
   1513— Fixed-Interval := From: Start-Time
   1514—Sliding-Interval := Interval: Use-Duration
   1515—Meter-Time:= Time-Remaining: Remaining-Use
1516— Access-Spec := ({SC: Security-Class} {Authorization: Authorization-ID*}
        {Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID})
1517— Fee-Spec:= {Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec |
                   Markup-Spec
   1518—Scheduled-Discount:= Scheduled-Discount: (Scheduled-Discount:
                                (Time-Spec Percentage)*)
   1519—Regular-Fee-Spec := ({Fee:  | Incentive: } [Per-Use-Spec | Metered-Rate-
                              Spec | Best-Price-Spec | Call-For-Price-Spec]
                              {Min: Money-Unit Per: Time-Spec}{Max:
                              Money-Unit Per: Time-Spec} To: Account-ID)
      1520—Per-Use-Spec:= Per-Use: Money-unit
      1521—Metered-Rate-Spec := Metered: Money-Unit Per: Time-Spec
      1522—Best-Price-Spec := Best-Price: Money-unit Max: Money-unit
      1523—Call-For-Price-Spec := Call-For -Price
   1524—Scheduled-Fee-Spec:= (Schedule: (Time-Spec Regular-Fee-Spec)* )
   1525—Markup-Spec:= Markup: percentage To: Account-ID
```

Fig.15

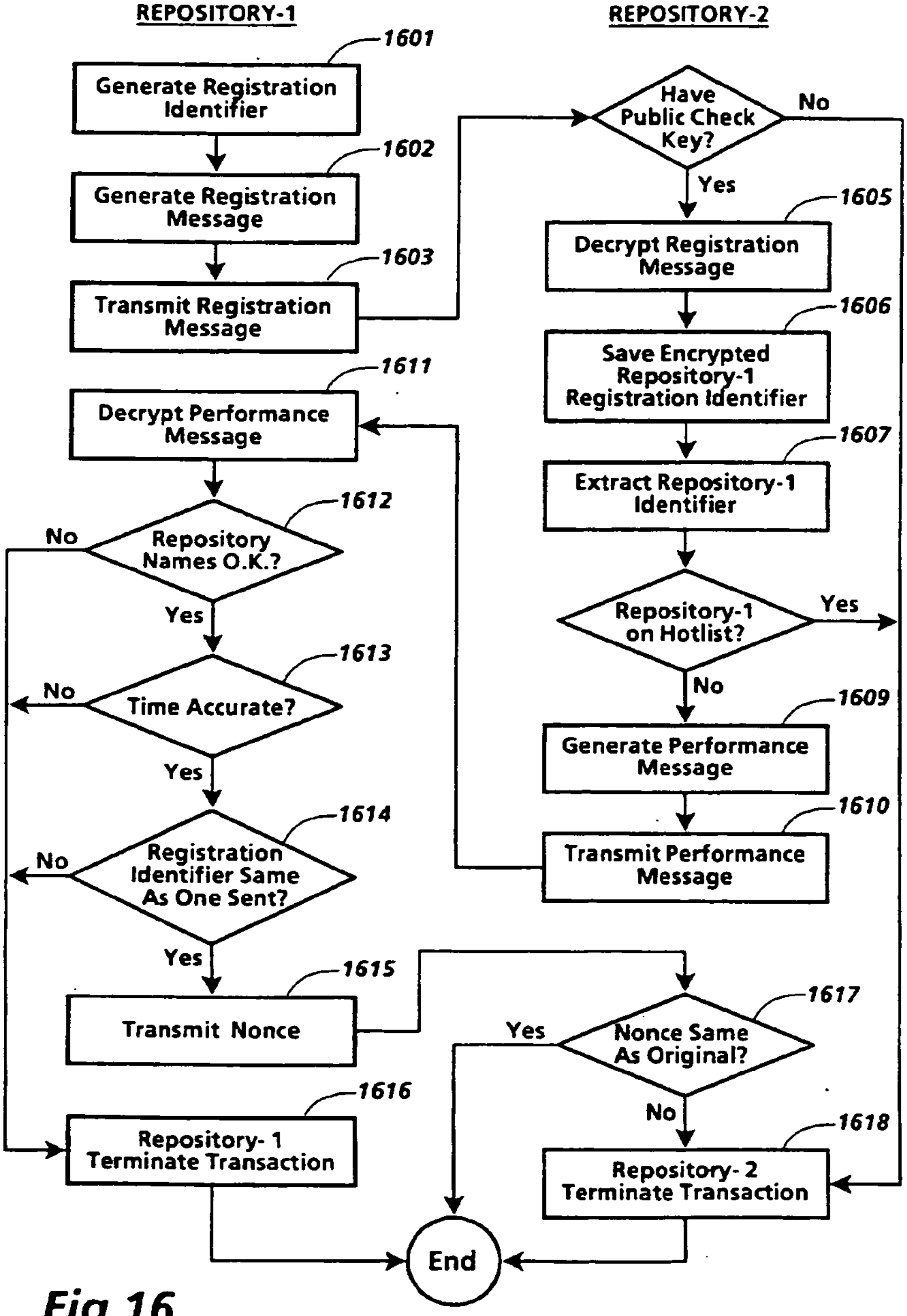

REPOSITORY-1
REPOSITORY-2
1601
Generate Registration Identifier
1602
Generate Registration Message
1603
Transmit Registration Message
Have Public Check Key?
No
Yes
1605
Decrypt Registration Message
1606
Save Encrypted Repository-1 Registration Identifier
1607
Extract Repository-1 Identifier
Repository-1 on Hotlist?
Yes
No
1609
Generate Performance Message
1610
Transmit Performance Message
1611
Decrypt Performance Message
1612
Repository Names O.K.?
No
Yes
1613
Time Accurate?
No
Yes
1614
Registration Identifier Same As One Sent?
No
Yes
1615
Transmit Nonce
1617
Nonce Same As Original?
Yes
No
1616
Repository- 1 Terminate Transaction
1618
Repository- 2 Terminate Transaction
End

Fig.16

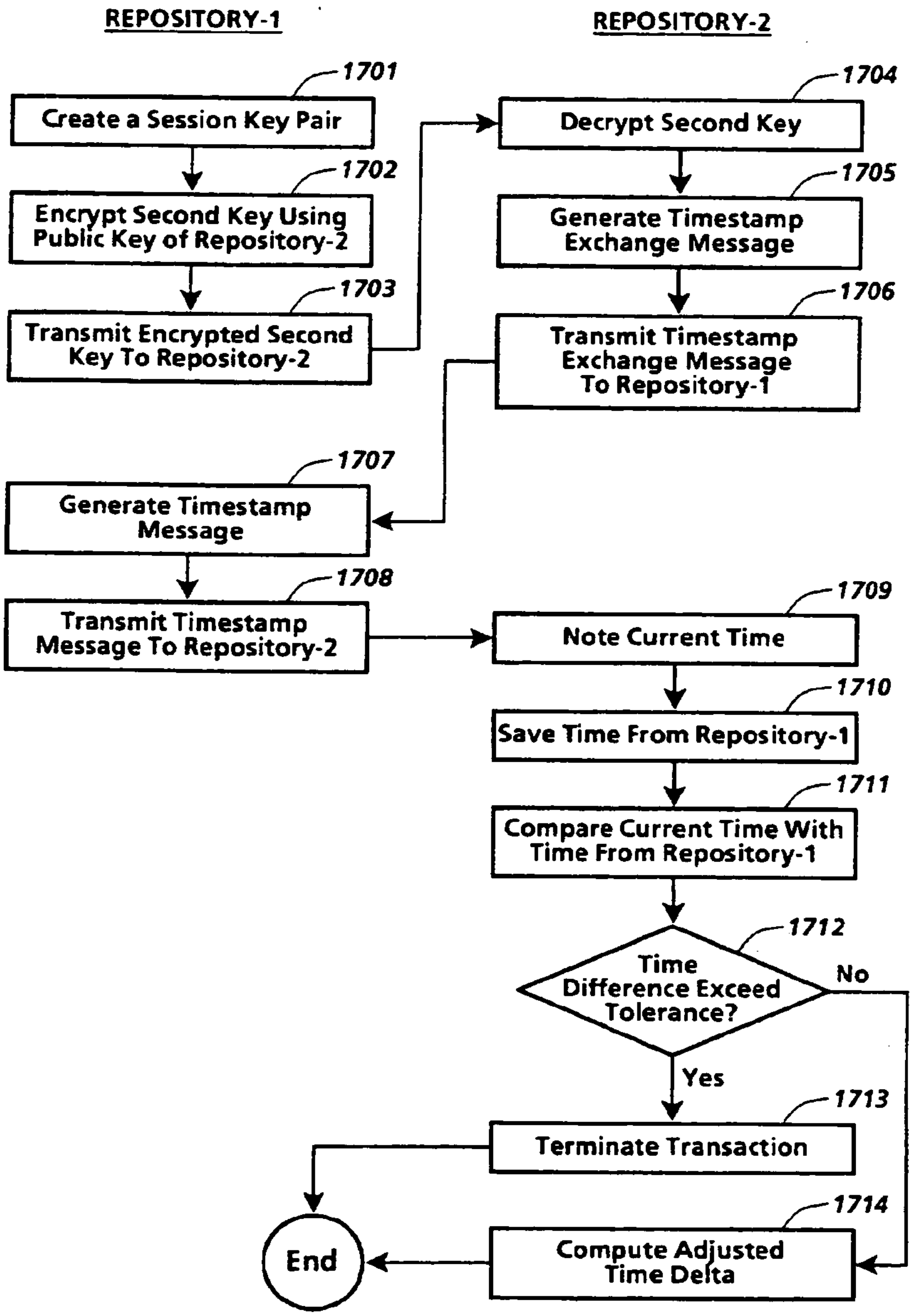

REPOSITORY-1
REPOSITORY-2
1701
Create a Session Key Pair
1702
Encrypt Second Key Using Public Key of Repository-2
1703
Transmit Encrypted Second Key To Repository-2
1704
Decrypt Second Key
1705
Generate Timestamp Exchange Message
1706
Transmit Timestamp Exchange Message To Repository-1
1707
Generate Timestamp Message
1708
Transmit Timestamp Message To Repository-2
1709
Note Current Time
1710
Save Time From Repository-1
1711
Compare Current Time With Time From Repository-1
1712
Time Difference Exceed Tolerance?
No
Yes
1713
Terminate Transaction
1714
Compute Adjusted Time Delta
End

Fig.17

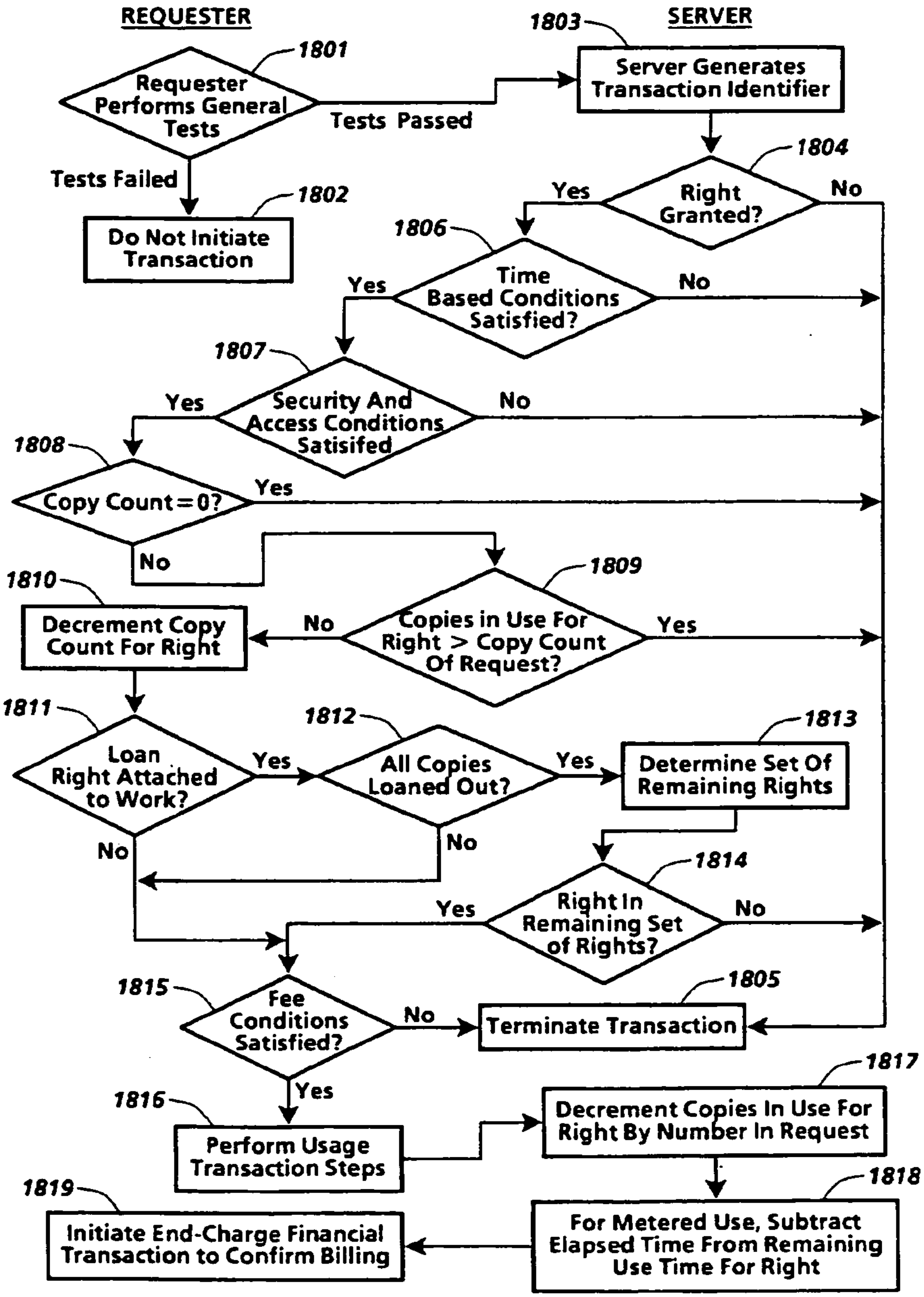

REQUESTER
SERVER
1801
Requester Performs General Tests
Tests Passed
Tests Failed
1802
Do Not Initiate Transaction
1803
Server Generates Transaction Identifier
1804
Right Granted?
Yes
No
1806
Time Based Conditions Satisfied?
Yes
No
1807
Security And Access Conditions Satisifed
Yes
No
1808
Copy Count=0?
Yes
No
1809
Copies in Use For Right > Copy Count Of Request?
No
Yes
1810
Decrement Copy Count For Right
1811
Loan Right Attached to Work?
Yes
No
1812
All Copies Loaned Out?
Yes
No
1813
Determine Set Of Remaining Rights
1814
Right In Remaining Set of Rights?
Yes
No
1815
Fee Conditions Satisfied?
No
Yes
1805
Terminate Transaction
1816
Perform Usage Transaction Steps
1817
Decrement Copies In Use For Right By Number In Request
1818
For Metered Use, Subtract Elapsed Time From Remaining Use Time For Right
1819
Initiate End-Charge Financial Transaction to Confirm Billing

Fig.18

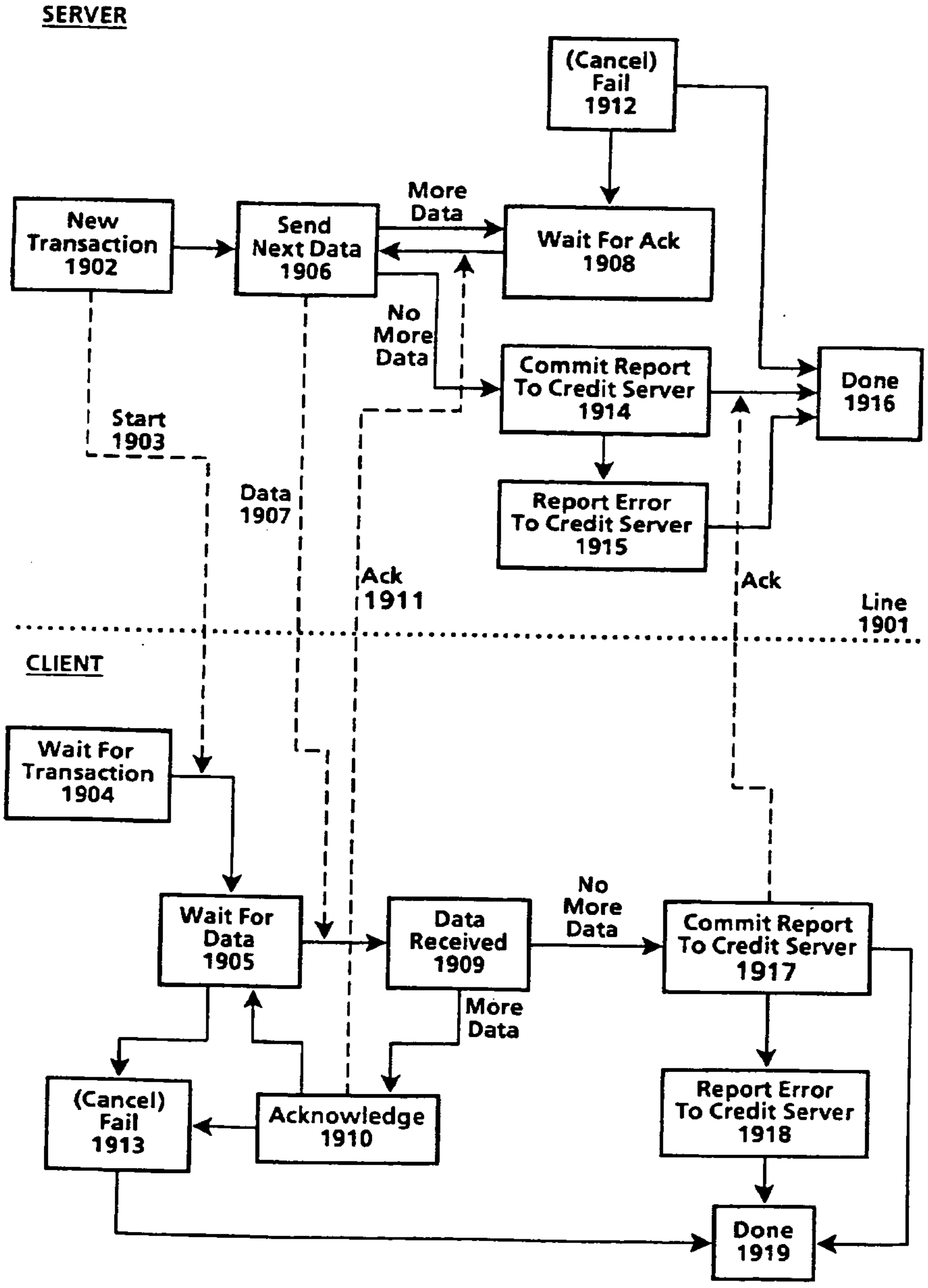

SERVER
(Cancel) Fail 1912
New Transaction 1902
Send Next Data 1906
More Data
Wait For Ack 1908
No More Data
Commit Report To Credit Server 1914
Done 1916
Start 1903
Data 1907
Report Error To Credit Server 1915
Ack 1911
Ack
Line 1901
CLIENT
Wait For Transaction 1904
Wait For Data 1905
Data Received 1909
No More Data
Commit Report To Credit Server 1917
More Data
(Cancel) Fail 1913
Acknowledge 1910
Report Error To Credit Server 1918
Done 1919

Fig.19

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 30 8420

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	WO-A-92 20022 (DIGITAL EQUIPMENT CORP.) * page 45, line 10 - page 64, line 17 * ---	1,6,8,10	G06F1/00
A	GB-A-2 236 604 (SUN MICROSYSTEMS INC) * page 9, line 11 - page 20, line 15 * ---	1,6,8,10	
A	US-A-5 291 596 (MITA) * the whole document * -----	1,6,8,10	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	1 April 1996	Moens, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/05229 A2

(51) International Patent Classification⁷: G07F 17/32

(21) International Application Number: PCT/US01/21260

(22) International Filing Date: 5 July 2001 (05.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/614.846 12 July 2000 (12.07.2000) US

(71) Applicant: **ONLINE GAMES LLC** [US/US]; 661 Hillside Road. P.O. Box 889. Pelham Manor, NY 10803 (US).

(72) Inventors: **FESJIAN, Robert, A.**; 660 Colonial Avenue, Pelham Manor. NY 10803 (US). **GUARNIERI, Jack**; 31 Danielle Court. Jackson. NJ 08527 (US).

(74) Agent: **MAHON, James, V.**: Clifford Chance Rogers & Wells LLP. 200 Park Avenue, New York, NY 10166 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ; LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VIDEO GAME SYSTEM

(57) **Abstract:** A computer-implemented method of communicating gaming data. The method includes receiving game software at a game console from a server, executing the game software at the game console to enable game play, and generating billing information at the game console in response to game play.

VIDEO GAME SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Serial No. 09/614,846, filed July 12, 2000.

BACKGROUND OF THE INVENTION

Computer game software is often distributed to a user on a fixed media, such as read-only memory (ROM) cartridge, a CD-ROM, or other fixed memory media. Game software used for home gaming systems typically has a high purchase cost, but may be used on an unlimited use basis. This purchase model is advantageous where a consumer anticipates playing a game frequently. However, where the consumer has less interest in a particular game, or anticipates infrequent use, the consumer may forego the purchase of the game. As a result, the game manufacturer receives no revenue and the consumer may obtain less use of his or her game console. In the case of arcade (i.e., commercial) gaming systems, game consoles may have a fixed software program that cannot easily be changed. As a gaming console ages, and its game software falls out of favor, revenue from that game console may decline. Enabling the game console software to be easily changed would be advantageous. Consequently new means of distributing game software are desired

SUMMARY OF THE INVENTION

In general, in one aspect, the invention features a computer-implemented method of communicating gaming data. The method includes receiving game software at a game console from a server, executing the game software at the game console to enable game play, and generating billing information at the game console in response to game play.

Implementations may include one or more of the following features. Received game software can be stored (permanently or temporarily) in a memory at the game console. The game software received from the server can include code that configures the game console to perform processing such as receiving player input and rendering output images, or can include a digital certificate or other "key" code to enable software resident at the game console to be executed. Billing information can be generated at the start of a game, as game features (e.g., skill levels) are accessed during game play, and at other times. A game console may offer multiple different games that are user-selectable, and the available games may be determined based on a usage pattern tracked at the server. Usage patterns, as well as other data, can be maintained in a player profile that is stored at the server and updated in response to game play. The player profiles can be accessed from one or more game consoles that are connected to the game server. In a commercial game console implementation, the video game console may include a coin or bill collector, a credit or debit card reader, or other device to receive a monetary payment (e.g., a token, a coin, a monetary note, debit account information, or credit account).

Implementations may include one or more of the following advantages. A video game architecture may provide automated downloading of game software from a central software repository, thereby facilitating purchase and distribution of game software. The downloaded game software may be received at a game server on a trial-bases (i.e., with particular features disabled or accessible for a limited number of plays), a player may thereafter make a payment to receive a fully or permanently enabled version of the game software. Improvements in game software licensing can be achieved by allowing a manufacturer to implement per-use charges and to vary licensing charges.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a networked game system.

Fig. 2 is a block diagram of a game console.

Fig. 3 is a block diagram of a game server.

Figs. 4A and 4B are flowcharts showing exemplary game console and game server operations.

Fig. 5 is an information flow diagram.

Figs. 6A and 6B are flowcharts of game unit purchase and resale operations.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 shows a networked game system 100 that includes video game consoles 111-113 and game server 130. The game consoles and game server each include a data network interface that lets the game consoles and game server exchange data over a network 150. In the system 100, game software can be downloaded from the game server to the game consoles to update features of the game consoles and to configure the game consoles to play new games. In addition, the game consoles and game server can exchange billing, game usage, player statistical data, and other types of data. Data sent from the game consoles to the game server can be used to bill for game usage, to track player skill levels and achievements, to record statistics, and for other purposes. In some implementations, the game consoles also may directly exchange data with each other through the network 150 or may indirectly exchange data using data relay services provided by the game server 130 or other network equipment. Data exchanged between the game consoles may be used, among other things, to play and synchronize multi-player games.

Fig. 2 shows a block diagram of a game console 200. The game console 200 may be a consumer video game consoles (such as a Sony Playstation®, Nintendo 64® or a Sega Dreamcast® video game consoles), a personal computers, a coin-operated game (such as amusement center video game machine), or other software-controlled gaming devices. The game console includes a joystick, keyboard, mouse and/or other input device 210 coupled to a processing unit 200. The processing unit 200 includes a software controlled processor and its associated support circuitry (such as RAM memory, hard disk data storage, and/or ROM memory) 201, a video display controller 202, and a network interface 203. The network interface 203 may be a modem, digital subscriber line interface, wireless network interface, local area network interface, or other device allowing data to be transmitted and received on the network 150

Fig. 3 shows a block diagram of a game server 130. The game server 130 includes a network interface 301, a processing server 302, a database 303. Components 301-304 may be implemented using industry-standard computer hardware and software and may be implemented as components of a single computer or may be distributed among one or more servers. For example, the processing server 302 may be a computer executing a Microsoft Windows NT®, SUN Solaris®, LINUX, or other UNIX-based operating system, and the database 303 may consist of files stored on that server's hard disk drive. All or part of the database 303 also can be distributed on separate database servers and systems. For example, the database 303 may reside at a server executing relational database management software and/or at a web server that returns data in response to hypertext transfer protocol (HTTP) requests. Database 303 can store data and software programs that can be sent (downloaded) to the game consoles 111-113, and can also store statistical data, game, and player information received from the game consoles.

Implementations of the system 100 can provide, among other things, on-demand and/or periodic distribution of game software to game consoles, game usage billing, game access control, and player information storage and distribution. Fig. 4A is a flow chart showing operation of an implementation of a game console and Fig. 4B is a flow chart showing operation of an implementation of a game server. The operations shown in Figs. 4A and 4B include player identification, game access control, distribution of software, management of billing information, and storing player statistics. Fig. 5 is a data flow diagram showing exchange of data between a game console and a game server during the operation shown in Figs. 4A and 4B. It is noted that in different implementations of the system 100, the operations shown in Figs. 4A and 4B may be augmented, performed in a different order, and/or one or more of the operations may be eliminated. For example, an implementation may eliminate player identification 401 and storage of player statistics. An exemplary operation of the system 100 will now be described.

Referring to Figs. 4A, 4B and 5, operation of a game console and game server can include initialization stages 401, 460-462 in which the game console and server exchange data needed for the operation of the game console. Initialization may begin with an initialization request message 501 sent from the game console to the game server (step 401). The initialization request message may include game console identification (ID) information that describes capabilities of the game console. As an example, the game console ID can include one or more codes that identify the game console manufacturer, model, processing capabilities, available controller types 210, resident software versions, and other capabilities. The game server receives the initialization message (step 451) and may processes the message using an initialization routine 460-462 that includes querying database 303 to retrieve console initialization data (step 460), performing initial processing on that data (step 461) and returning response data (step 462) in a message 502 to the game console. The data in the message 502 can include a listing of games available for download from the server, game console configuration parameters, software, and/or other data.

After the game console has been initialized 401, the game console may execute a customization routine 402-404 whereby the operation of the game console is customized for a particular player. This player-specific customization may include customizing game operation, controlling access to different games, storing and retrieving data and statistics, retrieving list of frequently or recently played games, enabling resumption of an interrupted game, and/or other personalized operations. The customization routine begins with the entry of a player identifier (ID) using an input device 210 (step 402). The player identifier 402 may be a login name and password, a set of initials, an account code, or other data identifying a particular player. In some implementations, the player ID may be stored on a bar coded, magnetic stripe, or other data storage card and entered into the console using a card reader.

For example, an arcade could distribute "frequent customer" cards storing player IDs to its customers.

After receiving the player ID, the game console sends a player data request message 503 containing a player ID to the game server (step 403). The game server uses parameters in the request message (e.g., the player ID) to query the database 303 and retrieve player-specific configuration information (step 480). The player-specific configuration information may include player statistics, a list of games available to the player, a list of restricted games, game status information, permission levels, and game software. The server returns the player-specific configuration information in a response message 504 sent to the game console (steps 481). The response message 504 is then processed at the game console (step 404) to configure the game console for the player. Configuration (step 404) may include, e.g., determining and displaying games available to the player, customizing game options, and allowing game play to continue from a previous point.

Some game consoles can be used to play different types of games. In such game consoles, a listing of the available games may be presented to the player, and the desired game selected using an input device 210 (step 405). The available games may be determined from the console initialization data 502, from player-specific configuration information 504 received by the game console, and/or from a list of game identifies stored at the console. The player-specific information 504 may enumerate the available games and/or may contain data used to determine a subset of available games that the particular player is permitted to access. The information 504 may include access control data that modifies a list of games returned in the console initialization data 502. Modification of the list of games may include blocking categories of games, such as violent games.

After the desired game or game option has been selected (step 405), the game console may perform a software download process (step 406) to obtain needed software from the game server. The download process (step 406) includes sending a request message 507 to the game server to request the needed software. In response, the server retrieves the software from its database 303 and sends it in a message 508 to the game console (steps 451, 475-476). Software downloaded to the game console may be stored in persistent memory (e.g., on a hard disk drive) for future access. In such cases, the game console may perform a check of its local storage space prior to downloading. In some implementations, available game software may have been previously stored at the game console (e.g., at game console manufacturing time) and, rather than actual software code being sent in the message 508, the "software code" may be an authorization code (e.g., a digital certificate) that enables access to the previously stored software.

The game console can then begin game play (step 408).In some implementations, a payment may be collected and/or payment information processed (step 407) prior to game play (step 408). Payment processing (406) may be required where, for example, a charge is associated with downloading of software (step 406). Payment processing (406) may also be required where a payment must be made each time a game is played (a game play payment). The amount of the payment may be variable and may depend on the software downloaded, the game selected, or other factors.

Payments can be made by depositing coins or bills into a money collection device at the game console (e.g., an arcade machine's coin slot or bill collector), or by deducting a payment from an account managed by the game server (a "player's account"). The player's account can be implemented using data stored in the database 303 to track payment credits ("game units") earned or purchased by the player. Each game unit can represent a fixed sum of money (e.g., "25 cents"), a fixed or variable period of game play (e.g., five minutes of play or three levels of game play), or may be an arbitrary value (e.g., "thirty units"). The player may establish the player's account by inputting information such as the player's name and a credit card number at an input screen displayed by the game console, using a separate web-based interface to the game server 130, using a phone call to an operator or manager of the system 100, using a card swipe machine (i.e., a smartcard or magnetic stripe card reader), or by other means. The game server 130 can exchange data with a credit processing system 114 in order to process credit card information or other financial information used in establishing the player's account.

To make a payment using game units in a player's account, the game console sends a billing message 505 or 509 to the game server from the game console. Billing message 505 may be a message requesting payment prior to a software download (406) and billing message 509 may be a message requesting payment prior to beginning game play (408). A billing message may identify a requested payment (e.g., a number of game units) and a player ID, account ID or other data that can be used to identify the player's account. The requested payment may differ depending on the software being downloaded or the game selected for play. For example, popular games may require a higher number of game units to play. The game server processes a billing message by querying database 303 to access the player's account information (step 470), determining whether the requested payment can be made (step 471), deducting the requested payment from the player's account (step 472), and sending a payment approval or denial message (504 or 508) to the game console (step 473). The payment approval message may indicate the number of game units that have been approved.

In some implementations, the player's account can be automatically established in the course of playing a game. For example, during game play, a player can accumulate game units by playing a certain number of games, by earning a high score, or by completing certain tasks or demonstrating skill in a game. When the game has ended, a message can be sent to the game server 511 containing a player ID and the number of game units earned. The game server may then automatically check to determine if an account is associated with the player ID and credit that account if one exists, or, if such an account does not exist, the game server can establish a new player's account and credit it with the earned game units. Thereafter, the stored game units can be accessed by the player to play additional games.

Additional payment processing (step 409) may occur during game play (step 408). Payment processing 409 may include periodic messages to deduct game units from the player's account. Iin a game billed on a duration-of-play basis, payment processing 409 can automatically send messages to deduct additional game units from a player's account after pre-set periods of game play. Payment processing 409 also can occur when special features of a game are accessed. For example, game units may be deducted from a player's account to obtain game hints, to access advanced game levels, to access special game features, or to play a multi-player game with other players (game consoles) connected to the network 150.

After a game has been completed, the game console can send game result data 511 to the game server (step 410). The game result data can include the player's score, time to complete the game, the point at which the game was stopped, the player's rating of the game, and other information. The game result data can be stored (step 485) by the game server and used to customize subsequent operation of the game console, to track the player's skill level, to identify a point at which to resume a game, and/or to track usage patterns. For example, the game server may use usage pattern data to determine new games that a player might be interested in. The player may be advised of such games in the response message 504 sent to the game console as part of the player customization process.

In some implementations, game consoles 111-113 can exchange data with each other as well as with the game server 130 to allow for multi-player games or for games played against an automated opponent. Players may be able to select partners for multi-player games based on the skill levels of the potential partners (which may be determined by result data 511 associated with the potential partners). Statistical information about players may be used by the game server to determine appropriate player matches for multi-player games. For example, player ranking statistics may be used to automatically pair players for a chess game.

In a commercial implementation, the system 100 can be used to invoice a commercial establishment for use of arcade game machines. For example, an arcade owner may purchase a fixed number of game units from a game console manufacturer or software provider using payment processing features implemented in game consoles 111-113 and the game server 130. These units may be purchases as-needed (i.e., immediately before a game is played) or pre-purchased in bulk The owner may then re-sell the purchased game units to patrons. Figs. 6A and 6B show processes that can be implemented to allowing game unit purchase and reselling. Fig. 6A shows a process whereby game units can be purchased by an establishment and Fig. 6B shows the treatment of those game units when a game is played.

Referring to Fig. 6A, game units can be purchased by initiating (step 601) a game unit loading and purchasing process. The process (601) may be initiated by entering a code at an input device 210, by depressing a hidden switch to initiate the loading and purchasing process, or by other means. The game console can then collect purchasing account information, such as a credit card number or other account identifier (step 602). The purchasing account information is then sent to the game server (step 603). The purchasing account information can be sent in a billing message similar to billing messages 505 and 509. After receiving the account information, the game server allocates game units and sends a response message to the game console indicating the number of game units allocated. The response message can be sent and processed similar to a response messages 506 and 510. Data in the response message can be encrypted and/or digitally signed to prevent forgery or alteration of the response message and the allocated game units value. After receiving the response message (and, if necessary, decrypting it or verifying its digital signature), the game console adds the allocated game units indicated in the response message to any previously allocated, unused game units. The resultant available game units value may be stored in an encrypted form at the game console and the available game units can be re-sold to players. Game units can also be stored at a server. The game server may subsequently send a bill to the owner or may exchange data with a credit processing system 114 to automatically bill the owner.

The available game units at a game console can then be re-sold to players. For example, game units purchased for $0.15 by an arcade owner may be sold to players for $0.25. Referring to Fig. 6B, game unit re-sale may be initiated when a player deposits money (step 610) in a game console's coin or bill collector and depresses "start" button on the game console (step 611). After the "start" button is pressed, the game console determines if there are any available (unused) game units remaining and, if so, deducts from the available game units a number of game units required for play (step 612). The game may then be played by the player (step 613). If game units are unavailable, the game console may display a message indicating that the owner should perform the unit loading and purchasing operation (Fig. 6A).

In some implementations, both consumer-type game consoles and commercial-type game consoles may operate on the same network 150 and may communicate with the same game server 130. Such a system could provide a roaming configuration and payment capability allowing the player customization data, player statistics, and billing information to be used at a variety of machine types and locations.

The data exchanges through network 150 may be transmitted over data exchange systems that include circuit-switched and/or packet-switched technologies. Circuit-switched connection technologies include the use of modems and/or digital subscriber line interfaces to communicate over analog or digital phone connections. Packet-switched connection technologies include the use of packet switching through the Internet, a local area network, or other type of network 150. In some cases, a circuit-switched connection may be used to connect to a modem bank which provides an interface to a packet switching network. Other types of network configurations and data exchange technologies also may be used.

The invention may be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Apparatus of the invention may be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention may be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output. The invention may advantageously be implemented in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. Each computer program may be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language if desired; and in any case, the language may be a compiled or interpreted language. Suitable processors include, by way of example, both general and special purpose microprocessors. Generally, a processor will receive instructions and data from a read-only memory and/or a random access memory. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of nonvolatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; DVD-RW, DVD-ROM, CD-RW and CD-ROM disks. Any of the foregoing may be supplemented by, or incorporated in, specially-designed ASICs (application-specific integrated circuits). Messages exchanged between the game console and game server may use a variety of different protocols. For example, proprietary protocols, TCP/IP, FTP, HTTP, NFS, SMTP and other data transfer protocols may be used in different implementations.

A number of embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. For example, gaming devices can include non-video devices. Exemplary non-video gaming devices can include a pinball machine in which a software controlled processor controls the action of bumpers, flippers, targets, and scoring. In such a pinball machine, software can be downloaded from server 130 to make the pinball game more challenging by changing the score for various targets, or to make the game easier by increasing points awarded for hitting various targets with the pinball. The data messages shown in Fig. 5 may be sent in a different order.

Accordingly, other embodiments are within the scope of the following claims.

WHAT IS CLAIMED IS:

1. A computer-implemented method of communicating gaming data comprising:
receiving game software code at a game console from a server, the game console and the server being operatively connected by a network;
processing the game software code at the game console to enable game play; and
generating billing information at the game console in response to game play.

2. The method of claim 1 further comprising storing the received game software code in a memory at the game console.

3. The method of claim 1 wherein processing the game software code comprises processing software instructions configuring the game console to enable game play by:
receiving player input at an input device;
rendering an output image in response to the player input; and
displaying the output image on a video display device.

4. The method of claim 1 wherein generating billing information in response to game play comprises generating billing information in response to a request to start a game.

5. The method of claim 1 wherein generating billing information in response to game play comprises generating the billing information in response to a game feature accessed during game play.

6. The method of claim 5 wherein the game play feature comprises a skill level associated with a game.

7. The method of claim 1 further comprising:
identifying a plurality of available games;
receiving an input selecting one of the available games;
and wherein the game software code comprises software implementing the selected game.

8. The method of claim 7 further comprising tracking a game usage pattern, and wherein displaying the plurality of available games comprises displaying based on the usage pattern.

9. The method of claim 1 wherein the video game console is a commercial video game console enabling video game play upon receipt of a monetary payment.

10. The method of claim 9 wherein the monetary payment is selected from the group consisting of a token, a coin, a monetary note, debit account information, and credit account information.

11. The method of claim 1 further comprising receiving a payment for a purchase of a unit of game time.

12. The method of claim 11 wherein the unit of game time represents a fixed period of game play, the fixed period being dependent on a one of a plurality of games selected by a user of the game console.

13. The method of claim 1 further comprising:
permanently storing the downloaded game software code on a storage media at the client computer.

14. The method of claim 1 wherein a plurality of other game consoles are operatively connected by the network to the game server and wherein the method further comprises:

updating a player profile at the server in response to game play at the game console; and

accessing the player profile to configure one of the other game consoles.

15. The method of claim 1 wherein the game software code comprises a digital certificate and processing the game software code comprises processing to determine authorization to execute software instructions locally stored at the game console.

16. A gaming system comprising:

a game server comprising a network interface operatively coupling the server to a plurality of game consoles;

a game database coupled to the game server and comprising a plurality of downloadable games; and

at memory coupled to the game server and comprising instructions to configure the game server to:

receive a game request from one of the game consoles,

process the game request to select one of the downloadable games,

send the selected one of the downloadable games to the one of the game consoles, and

receive billing information generated at the game console in response to execution of the one of the downloadable games.

17. The system of claim 16 wherein each of the downloadable games comprising game console executable software code

18. The system of claim 16 wherein the instructions further comprising instructions to configure the server to:

receive billing information generated at the one of the game consoles during an execution of the one of the games; and

send an message to authorize a continuation of execution of the one of the games.

19. The system of claim 18 wherein the billing information comprises a credit check message and the message to authorize comprises a message indicating a sufficient user credit in an account maintained by the server.

20. The system of claim 16 wherein the game software code comprises software implementing the selected game and the instructions further comprising instructions to configure the server to:

identifying a plurality of available games; and

receiving an input selecting one of the available games.

21. The system of claim 16 wherein the instructions further comprising instructions to configure the server to:

track a game usage pattern and store the game usage pattern in a user profile.

22. The system of claim 16 wherein the instructions further comprising instructions to configure the server to:

receive a game console identifier specifying an execution environment characteristics of the one of the game consoles.

23. The system of claim 22 wherein the execution environment characteristics comprises an available memory level.

24. The system of claim 23 wherein the execution environment characteristic comprises a game console software capability identifier.

25. The system of claim 1 wherein a plurality of other game consoles are operatively connected by the network to the game server and wherein the method further comprises:

updating a player profile at the server in response to game play at the game console; and

accessing the player profile to configure one of the other game consoles.

26. The system of claim 17 wherein the game software code comprises a digital certificate to authorize execution of game software locally stored at a game console.

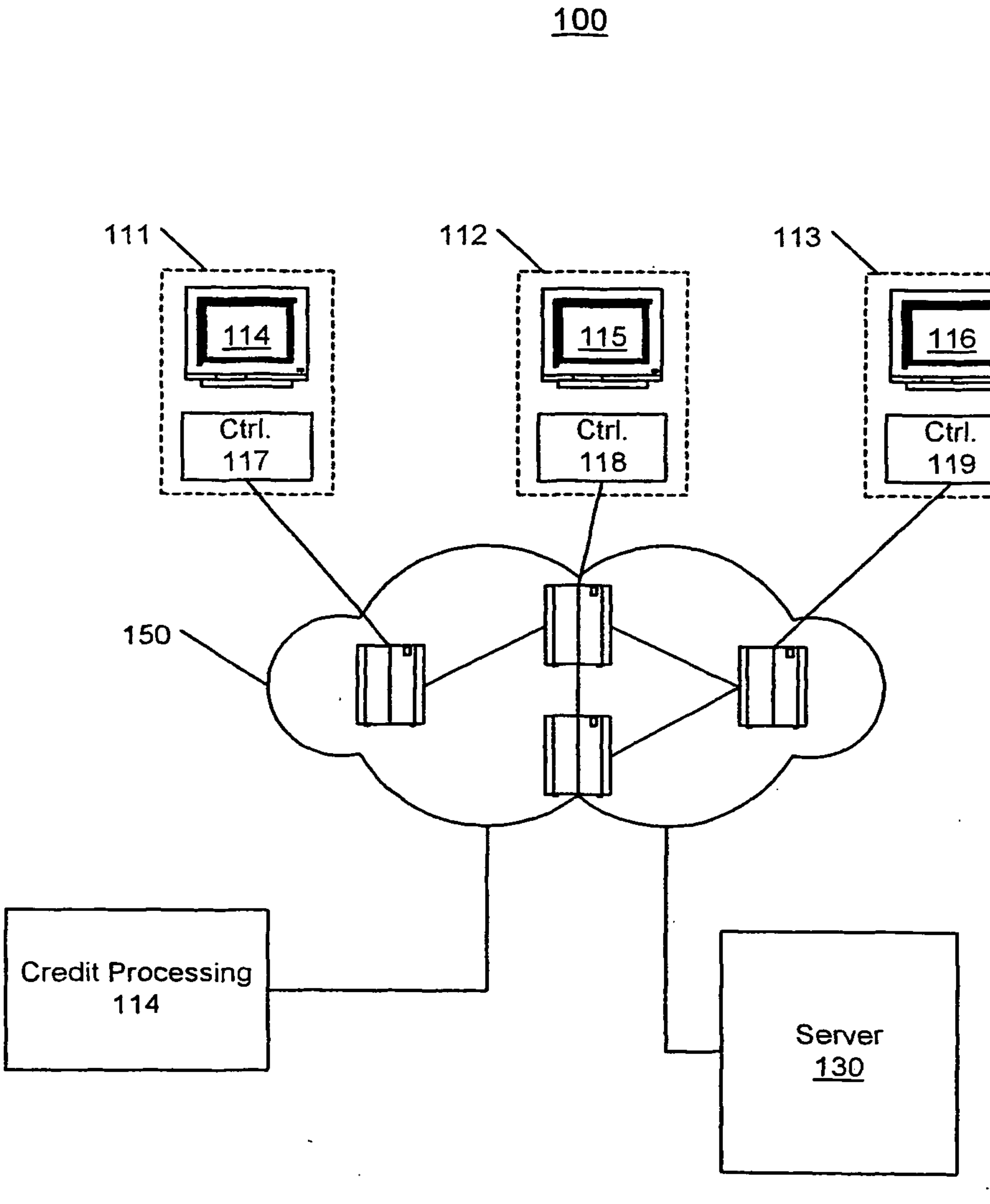

100
111
112
113
114
115
116
Ctrl.
117
Ctrl.
118
Ctrl.
119
150
Credit Processing
114
Server
130

Fig. 1

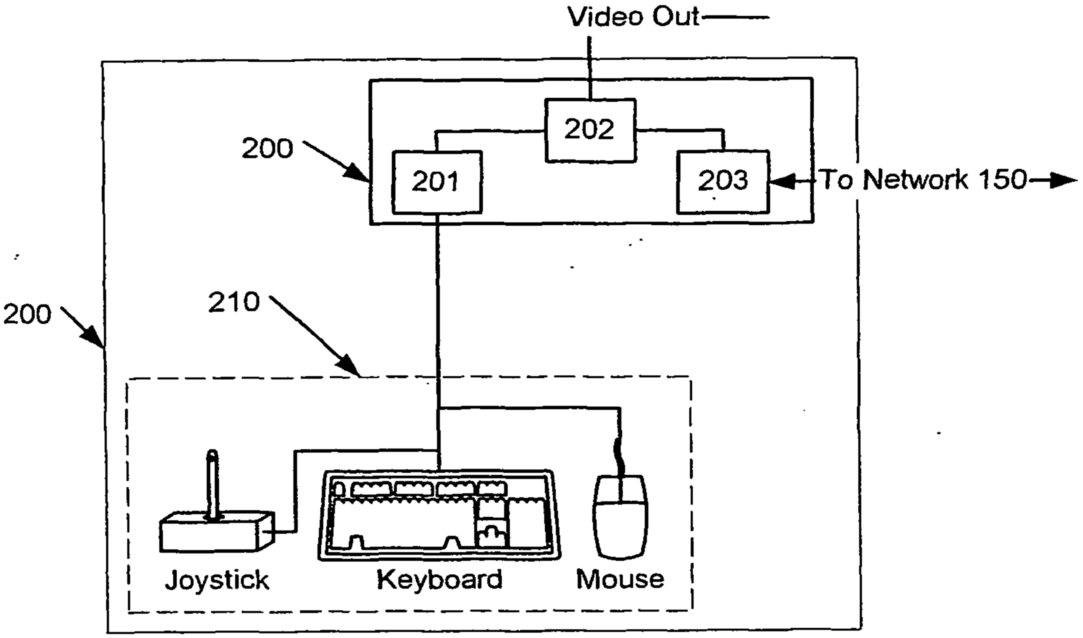

Video Out
200
202
201
203
To Network 150
200
210
Joystick
Keyboard
Mouse

Fig. 2

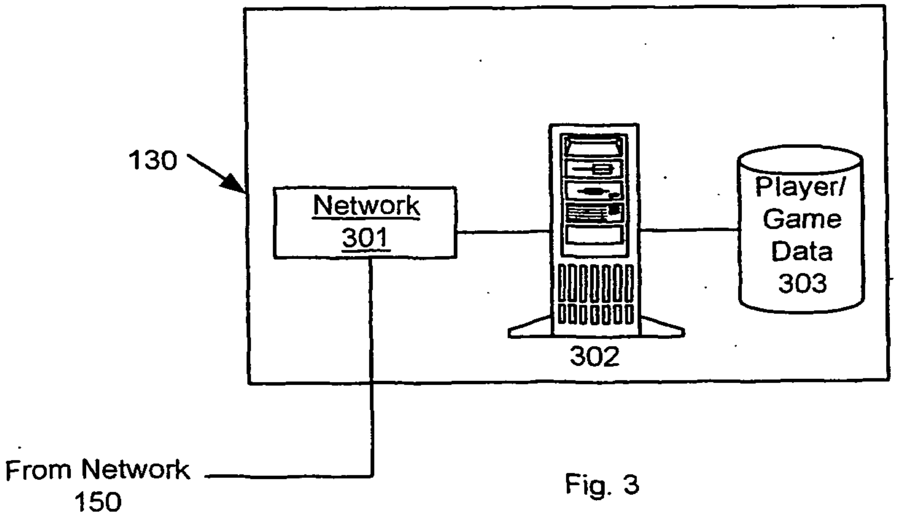

130
Network
301
Player/
Game
Data
303
302
From Network
150

Fig. 3

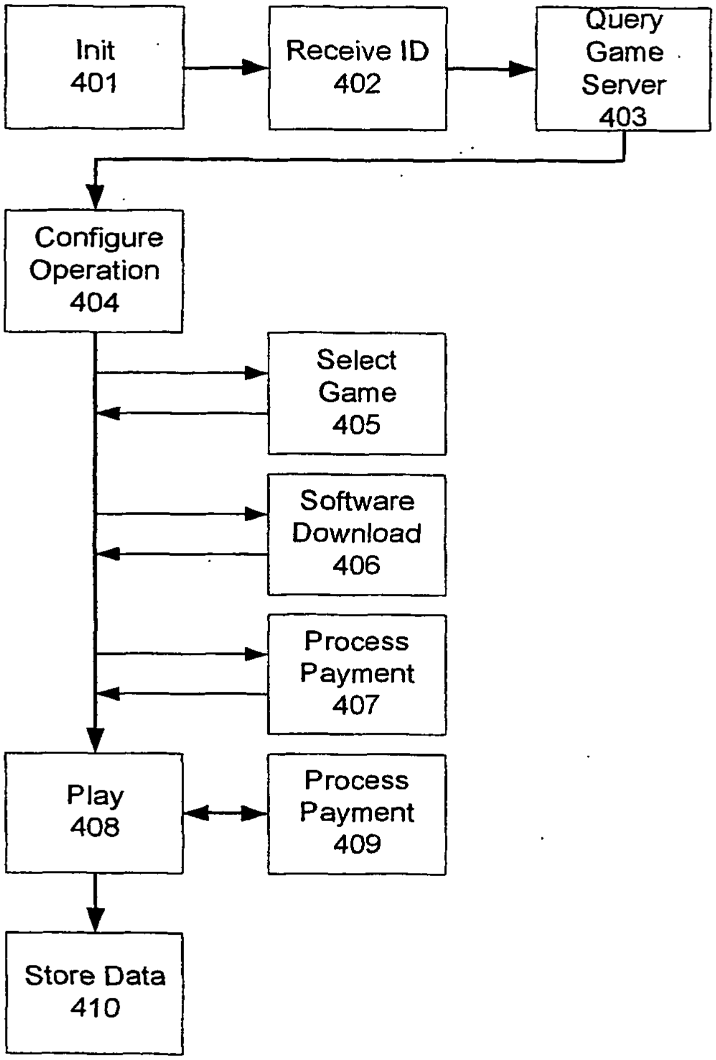

Init
401
Receive ID
402
Query
Game
Server
403
Configure
Operation
404
Select
Game
405
Software
Download
406
Process
Payment
407
Play
408
Process
Payment
409
Store Data
410

Fig. 4A

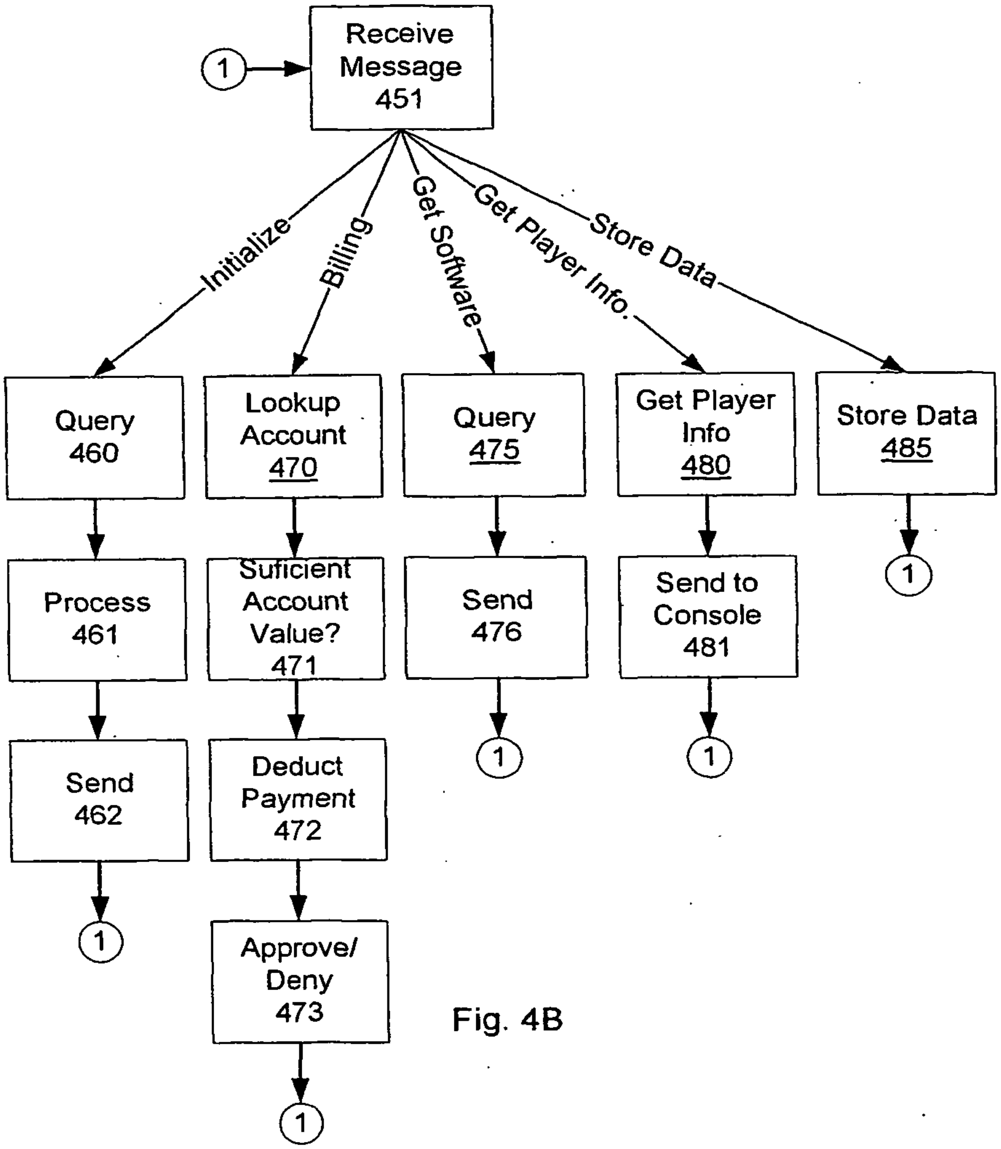

1
Receive Message 451
Initialize
Billing
Get Software
Get Player Info.
Store Data
Query 460
Lookup Account 470
Query 475
Get Player Info 480
Store Data 485
Process 461
Suficient Account Value? 471
Send 476
Send to Console 481
1
Send 462
Deduct Payment 472
1
1
1
Approve/ Deny 473
1

Fig. 4B

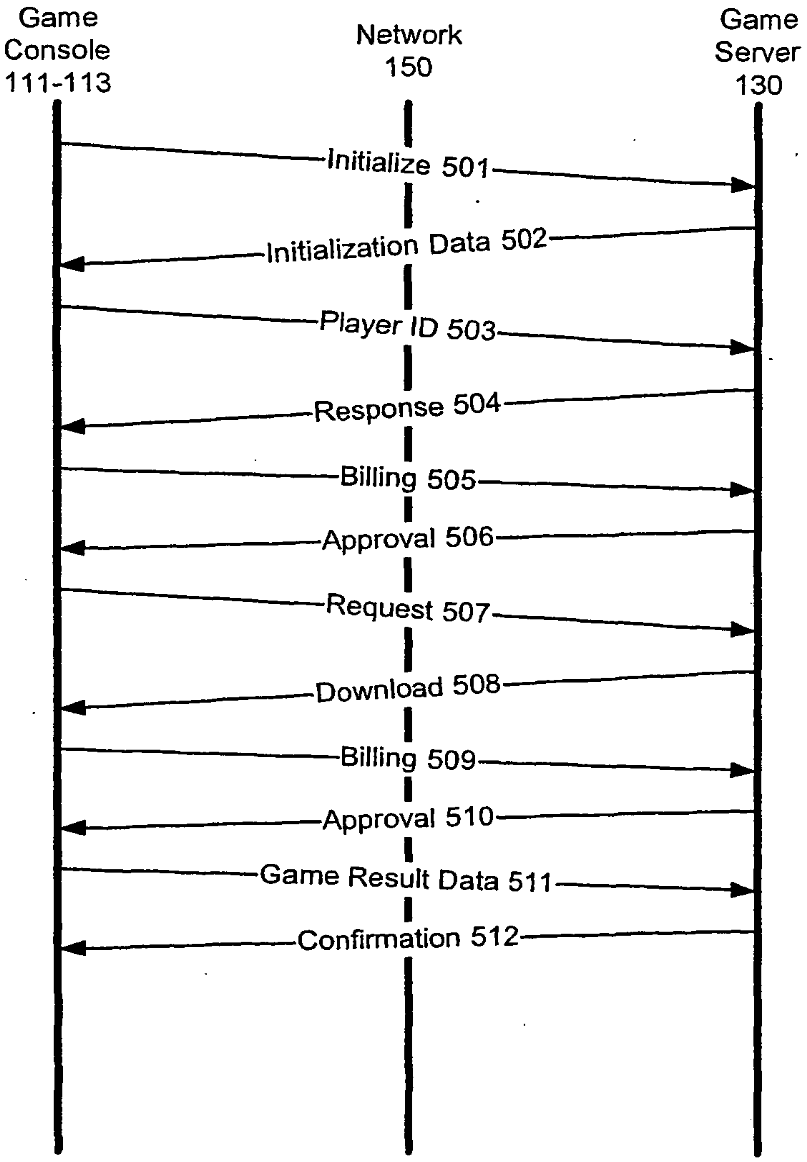

Game Console 111-113
Network 150
Game Server 130
Initialize 501
Initialization Data 502
Player ID 503
Response 504
Billing 505
Approval 506
Request 507
Download 508
Billing 509
Approval 510
Game Result Data 511
Confirmation 512

Fig. 5

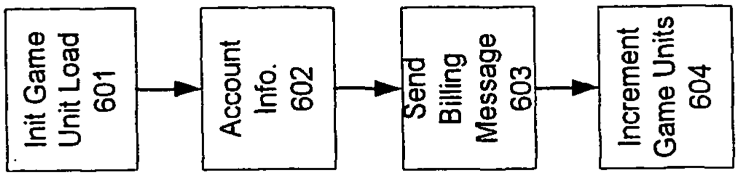

Init Game Unit Load 601
Account Info. 602
Send Billing Message 603
Increment Game Units 604

Fig. 6A

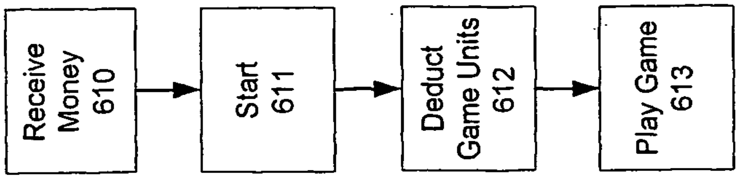

Receive Money 610
Start 611
Deduct Game Units 612
Play Game 613

Fig. 6B

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/005229 A3

(51) International Patent Classification⁷: G07F 17/32

(21) International Application Number: PCT/US01/21260

(22) International Filing Date: 5 July 2001 (05.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/614,846 12 July 2000 (12.07.2000) US

(71) Applicant: ONLINE GAMES LLC [US/US]; 661 Hillside Road, P.O. Box 889, Pelham Manor, NY 10803 (US).

(72) Inventors: FESJIAN, Robert, A.; 660 Colonial Avenue, Pelham Manor, NY 10803 (US). GUARNIERI, Jack; 31 Danielle Court, Jackson, NJ 08527 (US).

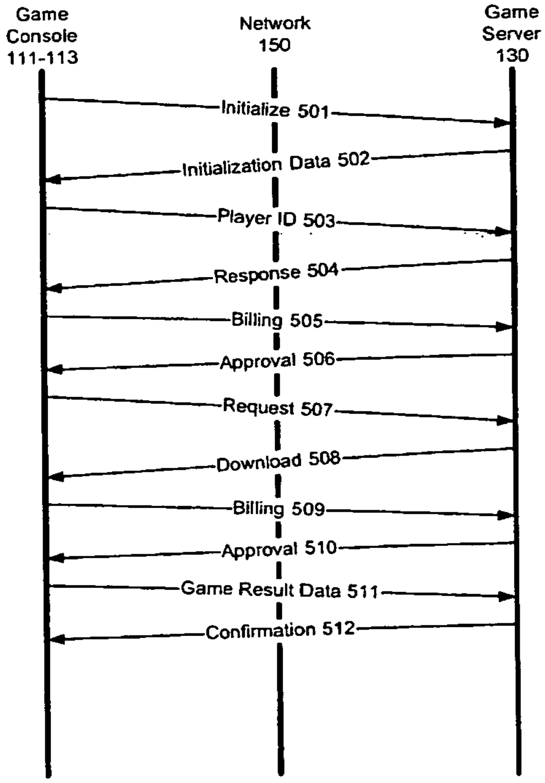
(74) Agent: MAHON, James, V.; Clifford Chance Rogers & Wells LLP, 200 Park Avenue, New York, NY 10166 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: COMMUNICATION OF DATA IN A GAME SYSTEM



(57) Abstract: A computer-implemented method of communicating gaming data. The method includes receiving game software at a game console from a server, executing the game software at the game console to enable game play, and generating billing information at the game console in response to game play.

WO 02/005229 A3

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 3 October 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/21260

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F17/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 556 840 A (RICOS KK) 25 August 1993 (1993-08-25) column 11, line 27 -column 14, line 33 abstract; claim 10 ---	1-26
X	DE 197 30 002 A (NSM AG) 14 January 1999 (1999-01-14) column 1, line 56 -column 3, line 37 abstract; figure ---	1-26
A	DE 195 16 681 A (NSM AG) 1 August 1996 (1996-08-01) column 2, line 39 -column 4, line 28 abstract; claims 1,4,6,7,16; figures ---	1-26
A	US 4 335 809 A (WAIN JOHN L) 22 June 1982 (1982-06-22) column 2, line 57 -column 3, line 53 -----	1-26

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 16 July 2002	Date of mailing of the international search report 23/07/2002
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Reule, D

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/21260

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0556840 A	25-08-1993	JP 5228259 A	07-09-1993
		JP 5237265 A	17-09-1993
		JP 5324509 A	07-12-1993
		JP 3268838 B2	25-03-2002
		JP 6044269 A	18-02-1994
		JP 3268839 B2	25-03-2002
		JP 6044159 A	18-02-1994
		JP 6044160 A	18-02-1994
		AU 672770 B2	17-10-1996
		AU 3312193 A	19-08-1993
		CA 2089774 A1	19-08-1993
		CN 1076537 A ,B	22-09-1993
		DE 69329160 D1	14-09-2000
		DE 69329160 T2	11-01-2001
		EP 0556840 A2	25-08-1993
		EP 0962900 A2	08-12-1999
		ES 2148187 T3	16-10-2000
		US 5547202 A	20-08-1996
DE 19730002 A	14-01-1999	DE 19730002 A1	14-01-1999
		WO 9902230 A1	21-01-1999
DE 19516681 A	01-08-1996	DE 19516681 A1	01-08-1996
		WO 9623288 A1	01-08-1996
		EP 0806023 A1	12-11-1997
US 4335809 A	22-06-1982	AT 35470 T	15-07-1988
		DE 3072104 D1	04-08-1988
		EP 0015081 A1	03-09-1980
		ES 488540 D0	16-12-1980
		ES 8101795 A1	16-03-1981
		GB 2042234 A ,B	17-09-1980

#7
1-2-04

Electronic Filing System (EFS) Data
Electronic Patent Application Submission
USPTO Use Only

EFS ID:	47972
Application ID:	10116424
Title of Invention:	SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT
First Named Inventor:	BINH NGUYEN
Domestic/Foreign Application:	Domestic Application
Filing Date:	2003-09-18
Effective Receipt Date:	2003-09-18
Submission Type:	Information Disclosure Statement
Filing Type:	
Confirmation number:	3186
Attorney Docket Number:	IGT1P034X1

Total Fees Authorized:

Digital Certificate Holder: cn=David P. Olynick,ou=Registered Attorneys,ou=Patent and Trademark Office,ou=Department of Commerce,o=U.S. Government,c=US
Certificate Message Digest: 93b871b1a87cf8c24a4cd58222ce234fe66b6c8c

TRANSMITTAL

Electronic Version v1.1
Stylesheet Version v1.1.0

Title of Invention	SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Application Number: 10/116424
Date: 2003-09-18
First Named Applicant: Mr. BINH T. NGUYEN

Confirmation Number: 3186
Attorney Docket Number: IGT1P034X1

I hereby certify that the use of this system is for OFFICIAL correspondence between patent applicants or their representatives and the USPTO. Fraudulent or other use besides the filing of official correspondence by authorized parties is strictly prohibited, and subject to a fine and/or imprisonment under applicable law.

I, the undersigned, certify that I have viewed a display of document(s) being electronically submitted to the United States Patent and Trademark Office, using either the USPTO provided style sheet or software, and that this is the document(s) I intend for initiation or further prosecution of a patent application noted in the submission. This document(s) will become part of the official electronic record at the USPTO.

Submitted by:	Elec. Sign.	Sign. Capacity
Mr. DAVID P. OLYNICK Registered Number: 48,615	David P. Olynick	Agent

Documents being submitted	Files
us-ids	IGT1P034X1-usidst.xml us-ids.dtd us-ids.xsl

Comments

ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18
Stylesheet Version v18.0

Title of Invention	SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Application Number:	10/116424
Confirmation Number:	3186
First Named Applicant:	BINH NGUYEN
Attorney Docket Number:	IGT1P034X1
Art Unit:	3711
Search string:	(6165072 or 6508709).pn.

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	6165072	2000-12-26	Davis et al.		463	29
	2	6508709	2003-01-21	Karmarkar		463	43

Signature

Examiner Name	Date

#8
GP
01-12-04
2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Binh T. Nguyen, et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277 CIP

Examiner: Ayaz R. Sheikh

Group: 2131

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on December 29, 2003 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Tomika Thomas
Tomika Thomas

INFORMATION DISCLOSURE STATEMENT 37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure

Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 778
Berkeley, CA 94704-0778
(510) 843-6200

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277 CIP **Applicant:** Binh T. Nguyen, et al. **Filing Date** April 3, 2002	**Application No.:** 10/116,424 **Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	2002/0045477	04/18/2002	Dabrowski	463	29	08/27/2001
	A2	2002/0071557	06/13/2002	Nguyen	380	251	12/07/2000

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	B1	EP 0744786	27.11.1996	EP			X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 744 786 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.11.1996 Bulletin 1996/48

(51) Int. Cl.⁶: H01Q 1/22, G07F 17/34,
H04B 7/00

(21) Application number: 96107290.7

(22) Date of filing: 08.05.1996

(84) Designated Contracting States:
BE DE ES FR GB GR IT NL SE

(30) Priority: 24.05.1995 US 449349

(71) Applicant: International Game Technology
Reno, Nevada 89502 (US)

(72) Inventors:
- Hoorn, Dennis W.
Sparks, Nevada 89436 (US)
- Loar, David W.
Reno, Nevada 89509 (US)
- Adams, Roy E.
Reno, Nevada 89503 (US)

(74) Representative: Finsterwald, Manfred, Dipl.-Ing.,
Dipl.-Wirtsch.-Ing. et al
Manitz, Finsterwald & Partner
Robert-Koch-Strasse 1
80538 München (DE)

(54) Candle antenna

(57) An antenna (120) for a wireless network is disclosed. The network includes multiple gaming machines such as slot machines or video poker machines located in an establishment. These machines communicate certain playing data (coin-in, coin-out data, etc.) to a central computer over the wireless network. Antennas for the gaming machines are located in a conventional candle (120) on top of the gaming machine. Such candles typically contain one or more lights which when illuminated indicate a certain event such as a jackpot being hit. The disclosed antenna (202) is unobtrusively located within a conventional candle structure so that from its exterior. The candle antenna appears to be a normal candle of the type typically used on gaming machines. However, interior to the candle antenna is an antenna capable of sending and receiving signals of a particular radio frequency band, via a wireless LAN.

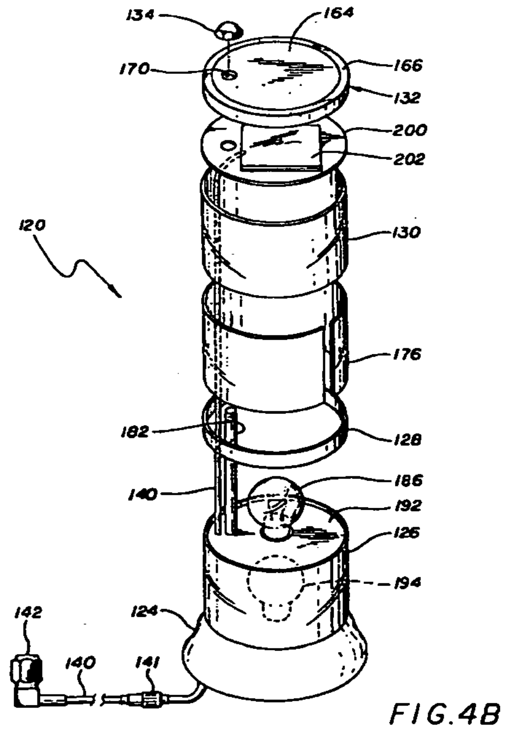


FIG.4B

Printed by Rank Xerox (UK) Business Services
2.13.8/3.4

Description

BACKGROUND OF THE INVENTION

Casinos derive much of their revenue from gaming machines such as slot machines, video poker machines, etc. Increasingly, casinos have come to rely on local area networks (or "LANs") for monitoring the activity of their various machines. With a LAN, the casino operator can easily tally the coin-in, coin-out, and other data associated with each gaming machine. In addition, the LANs of multiple casinos can communicate among themselves via a wide area network (or "WAN") to share information for various purposes. One such application of a WAN is in progressive games which allow jackpots from multiple machines in multiple locations to grow as one large jackpot. Thus, a player could win a potentially huge jackpot by playing a small denomination machine, e.g., a player could win one million dollars or more by playing a quarter (25 cent) slot machine, or as much as 8 to 9 million dollars by playing a dollar machine.

To maximize customer appeal, casino operators periodically move their various gaming machines to new locations within their establishments. Unfortunately, such moves can be difficult, time consuming, and expensive. This is particularly true for casinos in which the gaming machines are connected on a LAN. In such cases, many or all of the wire connections among the machines must be pulled out and replaced during each move. In fact, reconfiguring the wires is often the most expensive part of a move.

To simplify the moving procedure, it has been proposed to employ a "wireless" LAN in which each gaming machine includes a radio transceiver for communicating with a base station radio. The base station radio, in turn, communicates data from the gaming machines to a central host computer (sometimes referred to as a "server"). When it comes time to rearrange the floor layout of the gaming machines connected over a wireless LAN, the move can be made with comparative ease, as no wires need to be disconnected, reconnected, etc.

All wireless transceivers require an antenna to send and receive radio frequency signals. In the proposed wireless LANs for casinos, each gaming machine would have its own transceiver and associated antenna. Such antennas must be mounted in locations were they can send and receive radio signals unimpeded by structures which would absorb such signals. Thus, a machine antenna must not be blocked by a conductive structure in its "line of sight" with a radio base station's antenna. Being aware of this basic requirement, one might assume that an antenna should be placed on the exterior of a gaming machine at a location facing toward the base station's antenna.

Unfortunately, some gaming machine users can be expected to tamper with or destroy new structures prominently featured on the gaming machine exterior. Some users would likely try to defeat the new system by interfering with the transmission or reception of radio signals. Other users may be afraid to use a particular machine if it has a feature which is unfamiliar to them.

Thus, it would be desirable to have a new gaming machine design adapted to handle wireless transmission, but at the same time not encourage some users to tamper or discourage other users from playing.

SUMMARY OF THE INVENTION

The present invention provides an antenna located within a gaming machine's candle. Such antennas are referred to herein as "candle antennas." As is known to those of skill in the art, candles are prominent structures employed on top of gaming machines to signal certain predesignated events such as hitting a jackpot. Specifically, the candle typically includes one or more light sources which, when illuminated, signify to those in the casino that one of the predesignated events has occurred. The candle antenna of this invention appears from its exterior to be a normal candle of the type typically used on gaming machines. However, interior to the candle antenna is an antenna capable of sending and receiving signals in a particular radio frequency band. Because the candle antenna appears to be a normal candle, players will not, it is expected, recognize that the gaming machine is actually sending and receiving data over a wireless modem.

In one aspect, the present invention provides a candle antenna assembly which can be characterized by the following elements: (1) a substantially hollow candle housing which is at least partially transparent to light; (2) a first light source within the candle housing (typically two or more light sources are used in a candle); and (3) an antenna within the candle housing. Preferably, the antenna is mounted on a ground plane which is positioned above the first light source (at least when the candle housing is mounted in its normal position on top of a gaming machine). Thus, when the gaming machine is operating, the antenna will be located near the top of the candle structure where it can send radio frequency signals to "higher" locations within the casino. Such locations might include the casino ceiling, where an antenna for a base station is preferably located. In such cases, signals generally can be sent unobstructed between the gaming machine's candle antenna and the central computer's antenna. To further ensure that the candle antenna will be able to send and receive signals regardless of where it is located on the casino floor, the antennas used in this invention preferably have a substantially hemispherical intensity distribution (directed above the gaming machine).

Conventional candles also include vertical rods within their housings. Such rods serve various functions such as aligning the "caps" provided on top of candles. In the present invention, the rod has an additional function: to support the ground plane on which an antenna is mounted. Further in this invention, the rod may be used to hide a conductive line (e.g., coaxial cable) coupled to the antenna and extending downward within the candle housing. This is accomplished by stringing the conductive line so that it is substantially parallel with the rod, and it is positioned along a line of sight defined between rod and the first light source. A conductive line so positioned will not cast a shadow appearing any differently than a shadow cast by a rod in a conventional candle.

In another aspect, the present invention provides an entire wireless system in a establishment. The system may be defined to include the following: (1) a plurality of gaming machines, each including (a) a machine chassis having an upper surface, (b) a candle mounted on the machine chassis upper surface, (c) an antenna located within the candle, and (d) a first transceiver electrically coupled to the antenna; (2) a host computer programmed to process data from the plurality of gaming machines; and (3) a second transceiver (sometimes referred to as a "base station" herein) electrically coupled to the host computer, wherein the plurality of gaming machines and the host computer together form part of a LAN. By way of example, an antenna for the host computer is located in the ceiling of the establishment. Preferably, the transceivers of the wireless system communicate via radio frequency signals on an ISM band; most preferably, the band is between about 2.4 and 2.48 GHz. Further, the transceivers preferably are adapted to send and receive spread spectrum signals.

Yet another aspect of the present invention is a method of communicating over a wireless LAN connecting a plurality of gaming machines and a host computer. The method may be characterized as including the following steps: (1) generating playing data at one of the plurality of gaming machines; and (2) transmitting that data through a candle antenna (as defined above) on the gaming machine generating the playing data. The playing data may be any form of data associated with a gaming machine including various playing statistics, status messages, alarm conditions, etc. The method will, of course, also include a step of receiving the playing data at a transceiver associated with the host computer. The method will still further include a step of sending data from the transceiver associated with the host computer to the candle antenna(s) of a specified gaming machine(s).

These and other features of the present invention will be presented in more detail in the following detailed description of the invention and the associated figures.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing the principle elements of a wireless communications system in which a candle antenna of the present invention may be employed.

Fig. 2 is a block diagram of a wireless modem which may be used with a candle antenna in preferred embodiments of the present invention.

Fig. 3 is perspective view of a gaming machine including a candle antenna in accordance with a preferred embodiment of this invention.

Fig. 4A is an illustration of a candle antenna (separated from a gaming machine).

Fig. 4B is an exploded view of a candle antenna in accordance with a preferred embodiment of the present invention.

Fig. 4C is a side view of a candle antenna constructed in accordance with an alternative embodiment of the present invention.

Fig. 4D is a top view of the candle antenna depicted in Fig. 4C.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 is a block diagram showing some elements of a wireless system suitable for use with candle antennas of the present invention. The wireless system 10 includes a host computer (or "server") 8 which communicates with primary and secondary radio base station radios 12 and 14 respectively over a line 6. The secondary base station 14 is a redundant station used to back up the primary base station 12 should it go down. Both base stations 12 and 14 include low profile antennas: antenna 16 for the primary station and antenna 18 for the secondary base station. The base stations send and receive radio frequency signals to a plurality of gaming machines 20, 22, 24, and 26. These machines, in turn, send and receive radio frequency signals through antennas 50, 52, 54, and 56 which are attached to electronic gaming machine components 30, 32, 34, and 36 through transceivers 40, 42, 44, and 46. Although only four gaming machines have been shown in this example, many more, may be employed in a given casino (e.g., up to 100 or more per base station radio).

The host computer 8 may be any of a variety of commercially available computer systems. Such machines include, but are not limited to, DEC VAX, IBM AS 400 or PC compatibles. The central computer system can, also, include multiple work stations, terminals, disk drives with fixed and/or removable media all connected over a communication network consistent with industry standards (Token Ring, Ethernet, etc.). Typically, the host computer 8 will be provided with a front end controller (not shown) which is able to handle data concurrently provided through multiple ports.

Fig. 2 is a block diagram depicting a preferred wireless modem for use with a candle antenna of the present invention. As shown, a wireless modem 75 couples a gaming machine 78 with a candle antenna 72. The wireless modem 75 includes a UHF transceiver 80, coupled to a processor core 82 which is, in turn, connected to a communications interface 84. As shown, the candle antenna 72 is directly coupled to UHF transceiver 80, and the game machine 78 is directly coupled to communications interface 84. These elements are realized by good design practice consistent with electrical engineers skilled in the art utilizing selected, commercially available, standard integrated circuits and discrete components appropriate for product requirements and specifications.

Although the details are not shown, the primary and secondary base station radios 12 and 14 each also include a communications interface, a processor core, and a UHF transceiver (which is connected to the associated low profile antenna (16 or 18)). In addition, the base stations 12 and 14 will include a switch used to select one of the two stations as the current designated station (i.e., the station handling communications with the gaming machines on the wireless network). The modems employed in the primary and secondary base stations 12 and 14 as well as the gaming machines perform error checks on the data to ensure that it was received correctly before communicating that data to host computer 8 or the gaming machines 20, 22, 24, or 26.

Preferably, the antennas 16 and 18 are located in the ceiling of an establishment in which the gaming machines 20, 22, 24, and 26 are located. This allows radio frequency signals to be communicated between the gaming machines and the base station radios substantially unimpeded. Preferably, the base station antennas will be provided in the ceiling such that they are not prominently displayed, and preferably not noticeable to the users of the gaming machines.

Fig. 3 is an illustration of a gaming machine 90 having a candle antenna 102 provided thereon. As shown, the gaming machine 90 includes a machine chassis 92, various game play option buttons 98, a game play lever 96, and a display 100. It is important to note the candle antenna 102 is located on top of the gaming machine chassis 92 in the same location and orientation as a conventional candle (without an antenna). Further, the candle antenna has the same external appearance as a conventional candle. However, unlike a conventional candle, the candle antenna 102 includes an antenna (not shown) disposed in its interior -- which is invisible to a gaming machine player.

To play gaming machine 90, a player inserts coins or tokens through a slot 106, activates the machine by pulling the lever 96, pushing buttons 98, or taking some other action. The player then observes the indicators in display 100 to determine if he or she has obtained a winning combination. If so, the display 100 may indicate the amount won. Simultaneously, any winnings will be dropped into a tray 94. At various stages during this procedure, the candle antenna 102 may be active. For example, if a player does win, a coin hopper in gaming machine 90 may have to be refilled. In this case, a candle light of a particular color will be illuminated. This is an example of a traditional use of a candle. In addition, each coin that enters through slot 106 or leaves through tray 94 will be tallied by machine 90. This tally is periodically communicated via the antenna to a central computer or server in the establishment. This, of course, is an example of a non-traditional use of a candle -- and one in accordance with the present invention.

It should be recognized that the candle antennas of the present invention may be used with any conventional gaming machine that employs a candle. Exemplary manufactures of such gaming machines include International Game Technology, of Reno, Nevada and Bally Gaming, Inc. of Las Vagas, Nevada. Candles provided on the gaming machines of such vendors typically include two light sources, although some candles may have 1, 3, or 4 light sources. Each such light source is located in a different vertical position and has a different associated color band. This allows the gaming machine to display messages coded by different colors. For example, a yellow light might indicate that a coin hopper is empty and requires the service of an employee in charge of restocking the hopper, and a white color light might indicate an alarm condition such as a machine door being open.

Fig. 4A is a side exterior view of a candle antenna of the present invention. The candle antenna 120 includes a base 124 adapted to be mounted on gaming machine chassis 92. The base 124 is also adapted to receive a cylindrical sleeve 126 which transmits light of a particular color from a first light source (not shown) disposed within a lower region of candle antenna 120. A divider ring 128 separates the lower cylindrical sleeve 126 from an upper cylindrical sleeve 130. The upper cylindrical sleeve transmits light of a color which is different from that of the light transmitted by lower cylindrical sleeve 126. The upper cylindrical sleeve 130 also serves as a housing for a second light source (not shown) vertically displaced above the first light source provided within lower cylindrical sleeve 126. A cap 132 is provided on top of upper cylindrical sleeve 130. The cap is held in place on top of candle antenna 120 by a nut 134 which is screwed onto a threaded vertical rod (not shown) which spans the interior of candle antenna 120.

Various electrical connections are provided from candle antenna 120. These include a chassis ground strap 136 which is adapted to be electrically coupled to the metal game chassis 92. In addition, a light harness 138 is provided with an appropriate connector 139 to connect to a power source in the gaming machine and thereby provide the voltage necessary to illuminate the first and second light sources. Finally, a flexible coaxial radio frequency cable 140 is provided within the interior of candle antenna 120 and connected to an antenna (not shown). Coaxial cable 140 is terminated with a radio frequency male connector 142 (or other appropriate connector).

Fig. 4B is an exploded view of the candle antenna 120 shown in Fig. 4A. The displayed candle antenna 120 is a "two-stage" candle having a bottom stage with a first light source 194 and top stage with a second light source 186. The candle antenna 120 is designed so that when the first light source is illuminated, the bottom stage appears lighted and when the second light source is illuminated, the top stage appears lighted.

The candle antenna 120 includes base 124 which, as explained, is designed to be mounted on the top of a gaming machine -- typically by one or more bolts or screws. In addition, it will include provisions for passing the various conductive lines from light sources, an antenna, etc. into the gaming machine. The top of base 124 is sized to receive cylindrical sleeve 126 which forms the candle's outer wall for the first stage. Cylindrical sleeve 126 is preferably made from a plastic such as an uncolored acrylic. Typically, an inner circumferential surface of sleeve 126 will be lined with a flexible colored insert so that when light is emanating from the first stage, it has a specified color. In an alternative embodiment, the same effect can be achieved with a sleeve made from a colored translucent plastic (without resorting to the use of a colored insert). A first light source 194, which is preferably an electric light bulb, is mounted in the base 124 so that when it is illuminated, the bottom stage (through cylindrical sleeve 126) glows to indicate a particular event.

An opaque circular support 192 is provided on top of the first cylindrical sleeve 126 and serves as a support for a second light source 186. In addition, opaque support 192 prevents light from bleeding between the first and second stages. This ensures that when only one of the first or second light sources is illuminated, only the stage associated with that light source will appear to be emanating light. A divider ring 128 rests on top of the plastic cylindrical sleeve 126 and supports a second cylindrical sleeve 130 which defines the upper stage. Typically, the divider ring will be made from a plastic material having a decorative coating, such as a chrome coating. Further, the divider ring 128 will be open in the middle so that it can rest on top of sleeve 126 without contacting the second light source 186. It should be noted, that like the first light source 194, second light source 186 is preferably an electric light bulb.

The top stage of candle antenna 120 is defined by the second cylindrical sleeve 130 which totally encloses second light source 186. Preferably, the sleeve 130 is made from a transparent plastic and is lined with a flexible color plastic insert 176. Of course, the plastic sleeve itself could be made from a colored opaque material. Regardless of the means by which the top and bottom stages are colored, the particular colors of the top and bottom stages will generally be different and chosen according to a casino operator's preference. As explained above, illumination of each stage of a candle has a particular meaning to casino operators.

A vertical conductive rod 182 (typically a brass rod) is mounted in base 124 and spans the height of the candle antenna. The opaque circular support 192 will have an appropriately located hole to allow rod 182 to pass through it. At the top of rod 182, a nut 134 is provided to hold the various components of the candle antenna together. In conventional candles, as well as the candle antennas of this invention, the rod serves as a conductive path to ground (through ground line 136) for static discharges applied to the candle. It has been observed that some individuals have attempted to defeat security mechanisms in gaming machines by applying strong static discharges to candles and other gaming machine componentry.

A conductive ground plane 200 is mounted in electrical contact with conductive rod 182 near the top of rod 182. Preferably, ground plane 200 will be circular and sized to snugly fit within second clear plastic sleeve 130. An antenna 202 is mounted (preferably by soldering) on ground plane 200 and has an associated coaxial cable 140. Cable 140 extends downward from antenna 202 through the candle antenna 120 and out through base 124. As mentioned above, the coaxial cable 140 will be terminated with an RF male connector 142 which connects to a wireless modem in the gaming machine itself.

Preferably, an appropriate RF connector 141 is attached to the antenna 202 so that coaxial cable 140 can be disconnected from the antenna. This allows damaged antennas to be easily replaced like light bulbs. Further, it allows different types of antennas to be installed to provide additional isolation between base station cells (assuming that there are multiple base stations in the same casino). This second point is important if the gaming machine is to be moved about in a large casino where isolation between base stations relies, at least in part, on polarization of electromagnetic signals. The type of antennas used to transmit electromagnetic energy will have either a left hand or right hand circular polarization. Signals with left hand circular polarization are not easily received by antennas designed to receive signals with right had circular polarization -- and vice-versa. Thus, by providing some casino gaming machines with one type of antenna and other gaming machines with another type of antenna, good isolation between base station cells can be obtained.

A cap 132 is provided at the top of candle antenna 120. Cap 132 includes a small hole 170 through which the rod 182 passes. A nut 134 is positioned above cap 132 and screws down onto rod 182 to hold the whole candle antenna assembly together. Cap 132 is preferable made from a plastic material that includes a decorative chrome coating 166 along its outer perimeter. However, cap 132 should also have a central region 164 (disposed above antenna 202) which is non-conductive. This allows radio frequency signals to freely pass to and from antenna 202.

It should be noted that in most regards candle antenna 120 appears to a gaming machine user to be identical to a conventional candle (i.e., one which is not used for wireless communication). One difference, however, is the lack of a conductive chrome coating in region 164 of cap 132. However, because the eye level of a gaming machine user is below the candle, the user should not notice this difference. To the extent that the user can see cap 132, he or she will note that it has a reflective chrome coating 166 like a conventional candle. Further, ground plane 200 will prevent light from top light source 186 from passing through the top candle antenna 120. Thus, no additional illumination from the top of the candle should be observable.

In preferred embodiments, coaxial cable 140 is positioned along a line of sight between rod 182 and light sources 186 and 194. Thus, coaxial cable 140 will not cast a shadow which is distinct from a shadow cast by rod 182. This further camouflages the presence of antenna 202. Preferably, the coaxial cable 140 is aligned so that it will be directly in front of the conductive rod (i.e., upstream from the rod in the line of sight with the light sources). A shadow cast by the cable should be coextensive with a shadow cast by the conductive rod.

In general, the ground plane 200 is provided between the antenna 202 and the interior of the candle so that the other components of the candle have no effect on the radiation pattern of the antenna. Antennas from various vendors can be used with the present invention. However, in general, the antenna should have a symmetric radiation pattern which is hemispherical and directed above a horizontal plane defined by the ground plane. Because the gaming machines used with the present invention may be moved to various positions within an establishment (e.g., a casino), a hemispherical radiation pattern ensures communication with base station radios installed at a central location in the establishment. Preferably, that location is a ceiling.

The antenna may be one of the various commercially available antennas which meet the size and radiation frequency requirements of this invention. For example, the antenna 202 may be a patch antenna, a helical antenna, a linear antenna, etc. Suitable antennas may be obtained from Micropulse, Inc. of Camarillo, California or from M/A-COM, Inc. of Lowell, Mass. The antenna 202 may be customized to the extent that it is integrated with, and attached to circular ground plane 200 which is designated to attach to the conductive rod 182 and accommodate a mechanical strain-relief feature for the coaxial cable. In an alternative embodiment, the antenna used in the candle is chosen to have a ground plane incorporated in the antenna itself, and have no separate ground plane 200.

Preferably, a candle antenna of this invention employs a radio frequency band that does not require a Federal Communications Commission ("FCC") site license in the United States. Thus, the band should be an Industrial, Scientific, and Medical band ("ISM") meeting the FCC restrictions on effective radiated power. In addition, the system should employ a spread spectrum broadcasting technique. Various "non-license" bands in the United States are available from the FCC including 902 to 928 MHz, 2.4 to 2.4835 GHz, and 5.6 to 5.7 GHz as specified in FCC regulation § 15.247. Preferably, for this invention, the 2.4 to 2.4835 GHz band will be employed. This band is reasonably far removed from heavily used bands such as cellular radio and cellular telephone bands (unlike the 902-928 MHz band). Further, the componentry required for this band is less expensive than that required for higher frequency bands such as the 5.6-5.7 GHz band. In general, the expense of radio equipment is nearly directly proportional to its band frequency. It should be understood that this application discusses frequency ranges as specified in by the FCC for the Untied States. Operation in different frequency ranges may be preferred in areas outside the United States.

An alternative embodiment of the present invention is illustrated in Figs 4C (side view) and 4D (top view). The candle antenna 200 of this embodiment includes first and second light bulbs 202 and 204 mounted on first and second lamp holders 206 and 208 and first and second lamp mounting tabs 212 and 214. The lamp mounting tabs are supported on and affixed to support post 216 which corresponds to conductive rod 182 in the embodiment of Fig. 4B. The support post 216 also supports on antenna assembly 220 which is preferably ceramic disk that includes a conductive ground plane 222. The circuitry for the antenna is provided on a conductive region 224 which is electronically coupled to a coaxial cable 226 via a connector 228. As illustrated, this embodiment does not require separate ground plane an antenna elements. Often the antenna is supplied by vendors in this format. In a preferred embodiment, the antenna assembly is affixed to a lid (not shown) by an adhesive such as double sided tape. The adhesive is provided on the top surface of the antenna assembly 220 on the region surrounding the conductive region 224. In an alternative embodiment, the antenna is provided on top of a candle's lid.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, although the specification has described a cylindrical candle antenna, other shapes may be used as well. For example, a pyramidal or rectangular candle antenna may also be used. In addition, the reader will understand that the wireless modem associated with a gaming machine as describe herein can be located most anywhere within the gaming machine, and, in some embodiments, may even form part of the candle antenna itself.

Claims

1. A candle antenna assembly comprising:

   a substantially hollow candle housing which is at least partially transparent to light;
   a first light source disposed within said candle housing; and
   an antenna disposed within said candle housing.

2. The candle antenna of claim 1 wherein said antenna is positioned above the first light source.

3. The candle antenna of claim 1 further comprising a ground plane having a top surface on which said antenna is mounted.

4. The candle antenna of claim 1 wherein the antenna is affixed to a lid on top of the candle housing.

5. The candle antenna of claim 1 further comprising a rod within the candle housing which is oriented in a substantially vertical direction.

6. The candle antenna of claim 5 wherein the antenna is supported by said rod such that the antenna is oriented substantially horizontally.

7. The candle antenna of claim 5 wherein said antenna is coupled to a conductive line extending within said housing substantially in parallel with said rod.

8. The candle antenna of claim 7 wherein said conductive line is positioned along a line of sight defined by said rod with respect to said first light source such that when said first light source is illuminated, said conductive line casts no shadow beyond that shadow cast by said rod or casts a shadow that is substantially coextensive with any shadow that would be cast by the rod if the conductive line was not in place.

9. The candle antenna of claim 1 wherein said antenna transmits and receives radio frequency signals in a substantially hemispherical intensity distribution.

10. The candle antenna of claim 9 wherein said antenna is horizontally oriented within said candle housing, wherein said hemispherical intensity distribution is defined above a horizontal plane defined by the antenna.

11. The candle antenna of claim 1 further comprising a second light source also disposed within said candle housing, said second light source being vertically displaced from said first light source.

12. The candle antenna of claim 11 further comprising an opaque divider separating the first light source form the second light source such that when one of said light sources is illuminated, light from that source is substantially prevented from bleeding through to the other light source.

13. The candle antenna of claim 1 further comprising a transceiver which sends and receives spread spectrum signals.

14. The candle antenna of claim 13 wherein the transceiver sends and receives signals on an unlicensed radio frequency band.

15. The candle antenna of claim 1 further comprising a cap located on said candle housing and above the antenna, wherein the cap includes a nonconductive region which allows transmission of radio frequency signals to and from said antenna.

16. A gaming machine comprising:

a machine chassis having an upper surface and
a candle antenna mounted on said machine chassis upper surface, said candle antenna including
a substantially hollow candle housing which is at least partially transparent to light,
a first light source disposed within said candle housing.
an antenna disposed within said candle housing.

17. The gaming machine of claim 16 further comprising a ground plane disposed within said candle housing and having a top surface on which the antenna is mounted.

18. The gaming machine of claim 16 further comprising a rod disposed within the candle housing and oriented substantially vertically, wherein the antenna is supported by the rod such that the antenna is oriented substantially horizontally.

19. The gaming machine of claim 18 further comprising a transceiver, wherein said antenna is coupled to a conductive line extending within said housing substantially in parallel with said rod and into the gaming machine chassis where it is electrically coupled to the transceiver.

20. The gaming machine of claim 16 further comprising a second light source also disposed within the candle housing.

21. The gaming machine of claim 20 further comprising an opaque divider separating the first light source from the second light source such that when one of the lights sources is illuminated, light from that source is substantially prevented from bleeding through to the other light source.

22. The gaming machine of claim 16 further comprising a cap located on top of said candle housing and above the antenna, wherein the cap has a nonconductive region which allows transmission of radio frequency signals.

23. A communication system in an establishment, the system comprising:

a plurality of gaming machines, at least one of the plurality of gaming machines which includes
a machine chassis having an upper surface,
a candle mounted on said machine chassis upper surface,
an antenna disposed within the candle, and
a first transceiver electrically coupled to said antenna;
a host computer programmed to process data from said at least one of the plurality of gaming machines; and
a second transceiver electrically coupled to said host computer, wherein the at least one of the plurality of gaming machines and the host computer form part of a LAN.

24. The system of claim 23 wherein said host computer is part of a WAN.

25. The system of claim 23 wherein the transceivers communicate via radio frequency signals on an unlicensed band.

26. The system of claim 23 wherein said first and second transceivers are adapted to send and receive spread spectrum signals.

27. The system of claim 23 wherein said antenna transmits and receives radio frequency signals over a substantially hemispherical intensity distribution.

28. The system of claim 27 wherein said second transceiver is provided with a second antenna located proximate to a ceiling of said establishment.

29. A method of communicating over a wireless LAN having a plurality of gaming machines and a host computer programmed to process data from said plurality of gaming machines, the method comprising the following steps:

generating playing data at one of said plurality of gaming machines; and
transmitting said data through an antenna on one of said gaming machines, the antenna being located within a candle disposed on the one gaming machine, wherein, the data is transmitted in a frequency range for which a transceiver associated with the host computer is tuned.

30. The method of claim 29 wherein the playing data is transmitted through an antenna disposed within the candle.

31. The method of claim 29 wherein the playing data is transmitted from the antenna in signals having a substantially hemispherical intensity distribution above a horizontal plane at the location of the antenna

32. The method of claim 29 wherein the playing data is transmitted from the antenna in radio frequency signals on an unlicensed frequency band.

33. The method of claim 29 further comprising a step of receiving said playing data at said transceiver associated with the host computer.

34. The method of claim 33 further comprising a step of sending data from said transceiver associated with the host computer to said antenna disposed within the candle.

FIG. 1

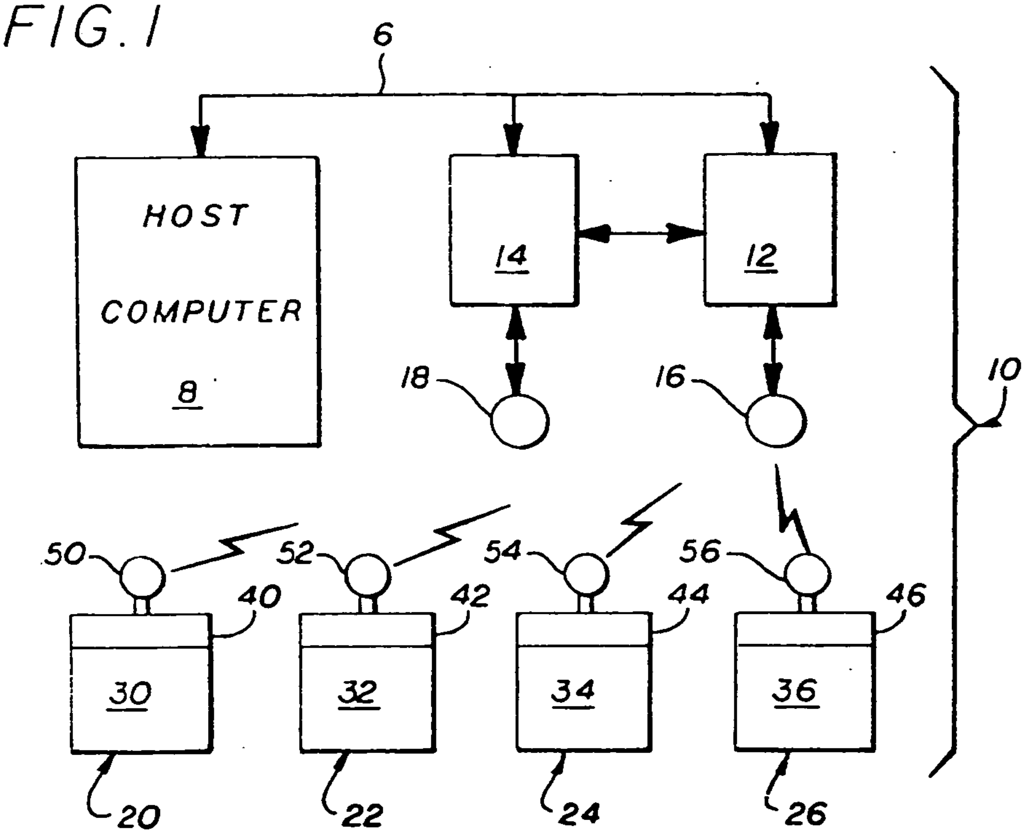
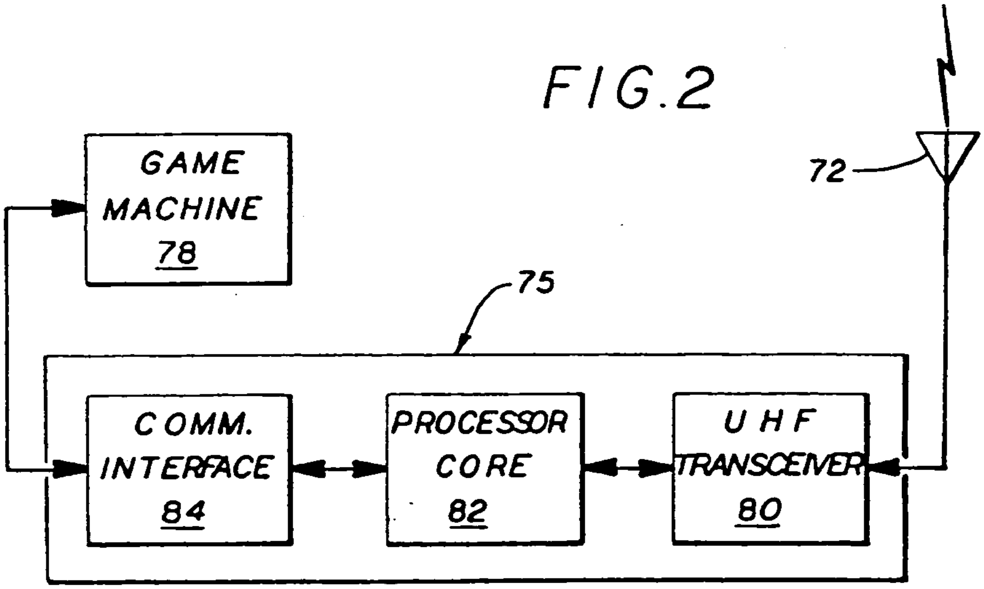

6
HOST
COMPUTER
8
14
12
18
16
10
50
52
54
56
40
42
44
46
30
32
34
36
20
22
24
26

FIG. 2


GAME
MACHINE
78
72
75
COMM.
INTERFACE
84
PROCESSOR
CORE
82
U H F
TRANSCEIVER
80

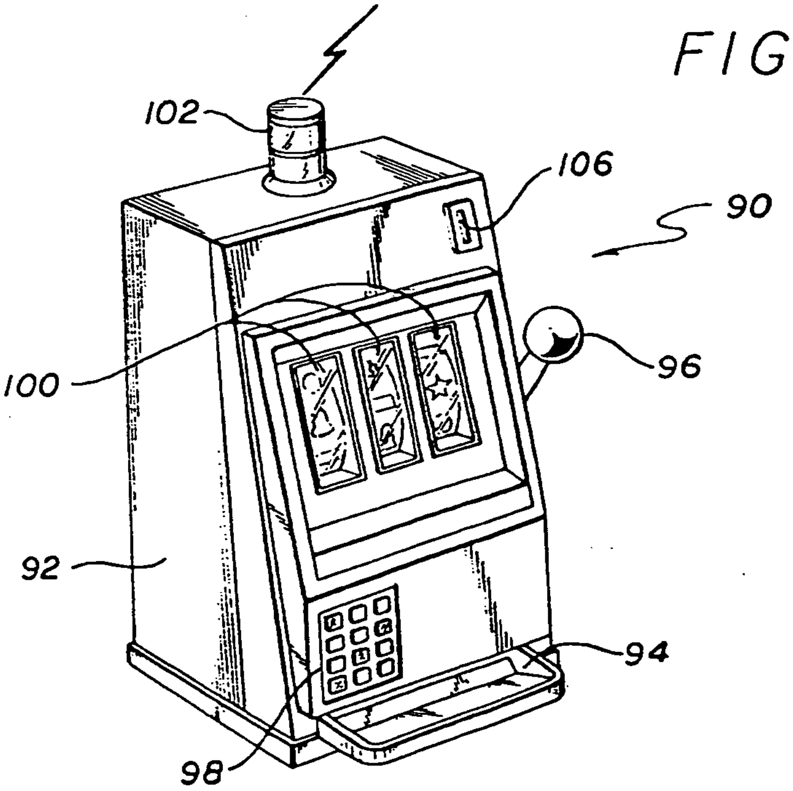

102
106
90
100
96
92
94
98

FIG. 3

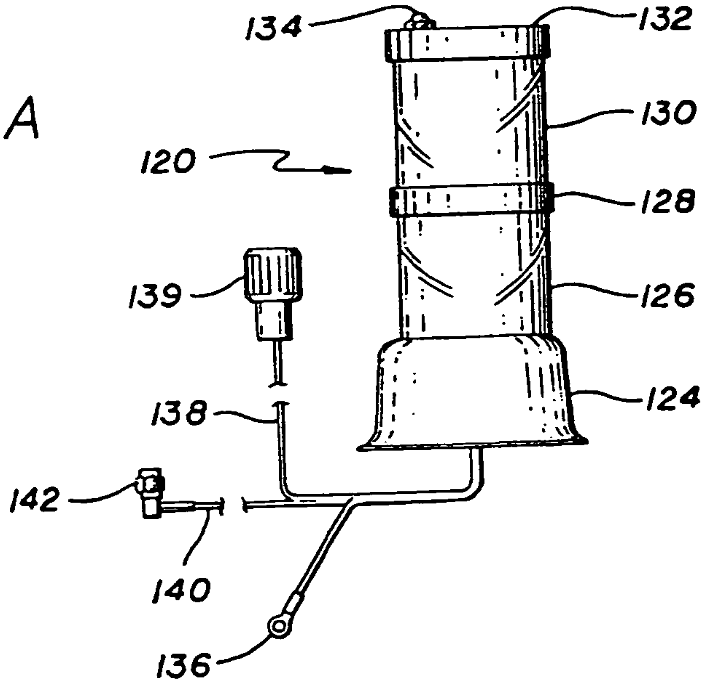

134
132
130
120
128
139
126
138
124
142
140
136

FIG. 4A

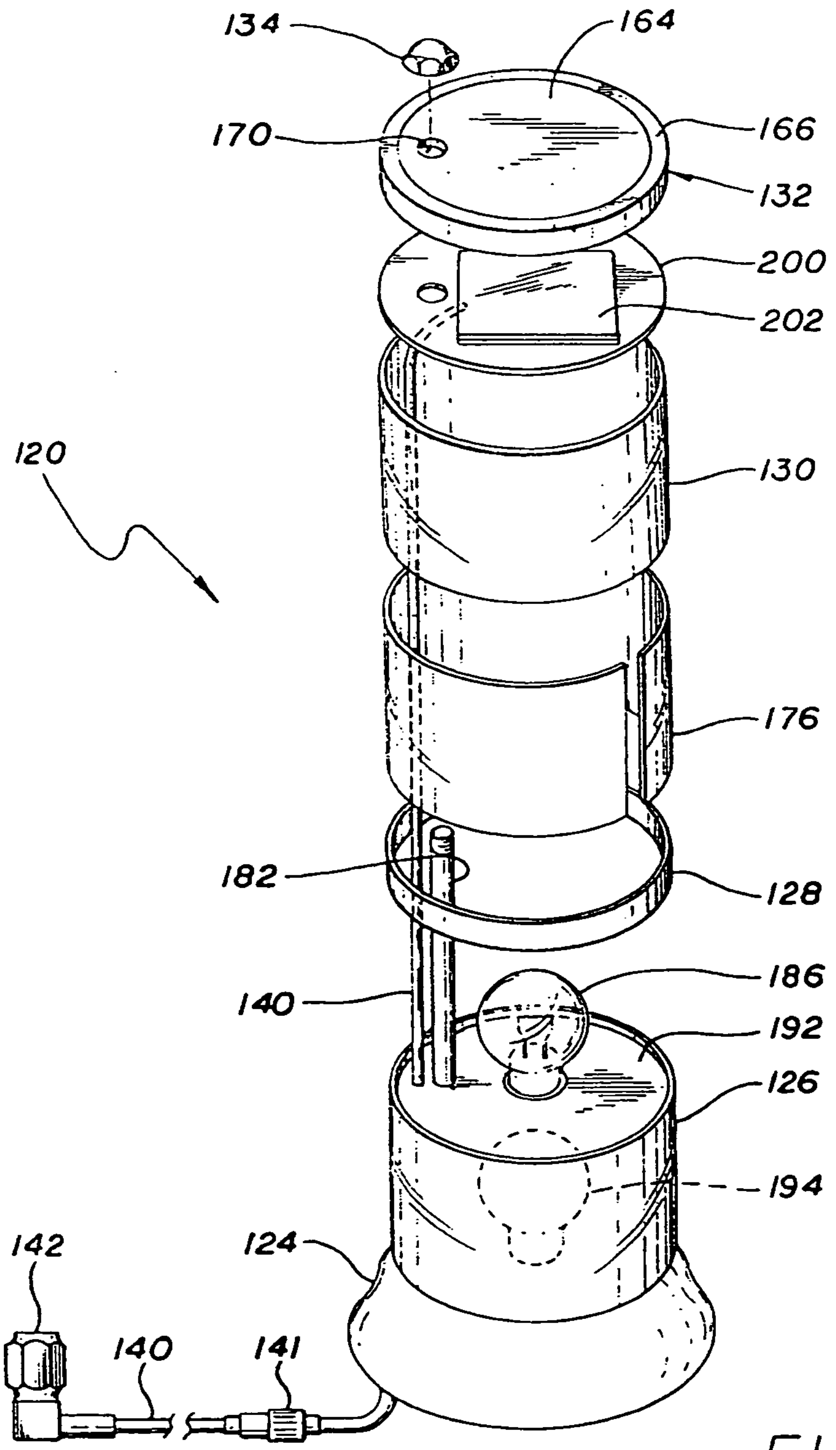
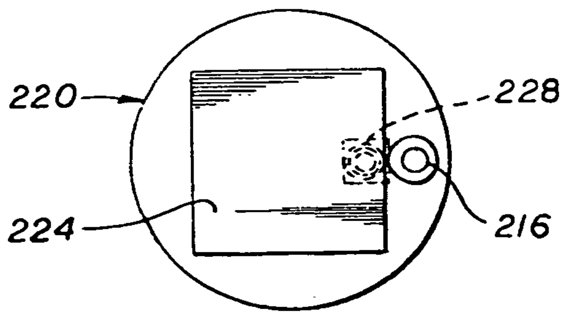

134
164
170
166
132
200
202
120
130
176
182
128
140
186
192
126
194
124
142
140
141

FIG.4B

FIG.4D



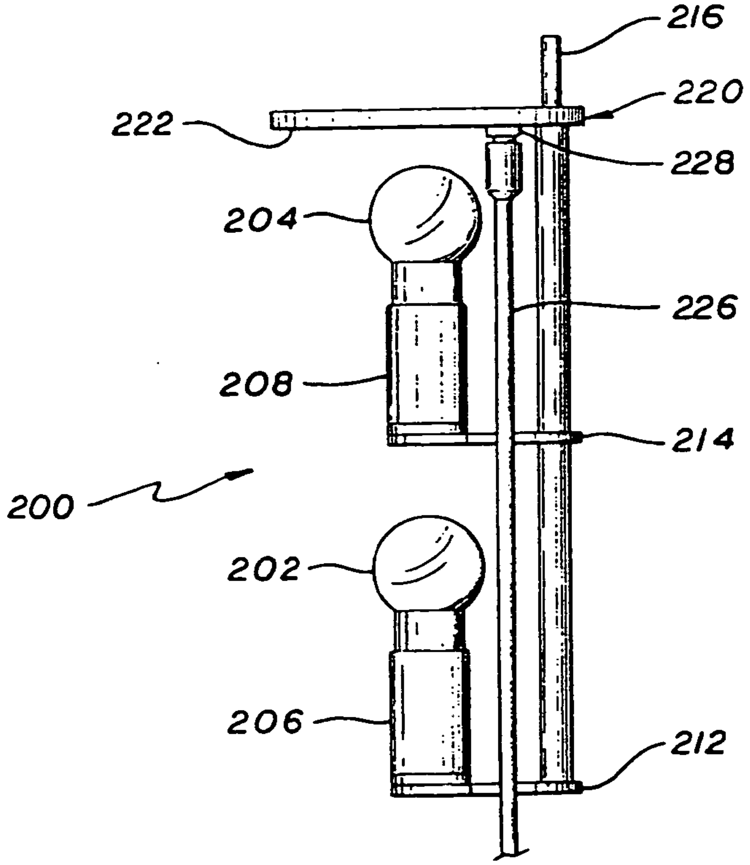


FIG.4C

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 10 7290

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	GB-A-2 256 750 (MARCONI GEC LTD) 16 December 1992	1-12,15	H01Q1/22 G07F17/34 H04B7/00
Y	* page 2 - page 3 *	13,14, 16-22	

X	PATENT ABSTRACTS OF JAPAN vol. 015, no. 026 (E-1025), 22 January 1991 & JP-A-02 270403 (NISSAN MOTOR CO LTD), 5 November 1990, * abstract *	1-12,15	
Y		13,14, 16-22	

Y	US-A-4 099 722 (RODESCH DALE F ET AL) 11 July 1978 * column 3, line 1 * * column 4, line 11-12 * * column 4, line 25-26 *	16-34	
	---		TECHNICAL FIELDS SEARCHED (Int.Cl.6)
Y	US-A-5 251 738 (DABROWSKI STANLEY P) 12 October 1993 * column 4, line 14-18 * * column 6, line 28-31 *	16-34	H01Q G07F H04B

Y	US-A-5 252 979 (NYSEN PAUL A) 12 October 1993 * column 4, line 28 - column 5, line 62 * * column 7, line 46 - column 8, line 2 *	23-25, 27-34	

Y	US-A-5 046 066 (MESSENGER STEVEN) 3 September 1991 * column 2, line 68 - column 3, line 15 * * column 12, line 32-43 *	13, 23-27, 29-34	
	--- -/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	7 August 1996	McLean, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 10 7290

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	PATENT ABSTRACTS OF JAPAN vol. 017, no. 283 (E-1373), 31 May 1993 & JP-A-05 014349 (MURATA MACH LTD), 22 January 1993, * abstract * ---	23-25, 28-34	
Y	DE-A-43 23 144 (DIEHL GMBH & CO) 19 January 1995 * column 2, line 56-60 * -----	14,25,32	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	7 August 1996	McLean, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

3711 #10
SP
3-04-04
2131

N THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Binh T. Nguyen

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VITURAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277 CIP

Examiner: Not yet assigned

Group: 3711

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on February 13, 2004 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Tomika Thomas
Tomika Thomas

INFORMATION DISCLOSURE STATEMENT
37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure

Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48, 615

P.O. Box 778
Berkeley, CA 94704-0778
(510) 843-6200

Form 1449 (Modified)	**Atty Docket No.** IGT1P034X1/P-277 CIP	**Application No.:** 10/116,424
Information Disclosure Statement By Applicant	**Applicant:** Binh T. Nguyen	
(Use Several Sheets if Necessary)	**Filing Date** April 3, 2002	**Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	1A	5,970,143	10/19/1999	Schneier, *et al.*			08/08/1996

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

3711

N THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Binh T. Nguyen

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VITURAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277 CIP

Examiner: Not yet assigned

Group: 3711

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on April 14, 2005 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Tomika Thomas
Tomika Thomas

INFORMATION DISCLOSURE STATEMENT
37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO Form 1449, copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure

Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48, 615

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100, ext. 231

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277 CIP **Applicant:** Binh T. Nguyen, *et al.* **Filing Date** April 3, 2002	**Application No.:** 10/116,424 **Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	5,970,143	10/19/1999	Schneier			08/08/1996
	A2	5,421,009	05/30/1995	Stephen M. Platt			12/22/1993
	A3	5,759,102	06/02/1998	Pease, *et al.*			02/12/1996
	A4	5,905,523	05/18/1999	Woodfield, *et al.*			06/28/1996
	A5	6,029,046	02/22/2000	Khan, *et al.*			12/01/1995
	A6	6,104,815	08/15/2000	Alcorn, *et al.*			01/09/1998
	A7	5,870,723	02/09/1999	Pare, Jr. *et al.*			08/29/1996
	A8	5,654,746	08/05/1997	McMullan, Jr. *et al.*			12/01/1994
	A9	5,136,644	08/04/1992	Audebert, *et al.*			09/19/1989
	A10	5,845,090	12/01/1998	Theodore Joseph Collins, *et al.*			09/30/1996
	A11	6,317,827	11/13/2001	Cooper			08/16/1996
	A12	6,047,128	04/042000	Zander			12/09/1997
	A13	5,896,566	04/20/1999	Averbuch, *et al.*			07/28/1995
	A14	5,848,064	12/08/1998	Cowan			08/07/1996
	A15	6,154,878	11/28/2000	Saboff			07/21/1998
	A16	6,006,034	12/21/1999	Heath, *et al.*			09/05/1996
	A17	5,845,077	12/01/1998	Fawcett			11/27/1995
	A18	5,715,462	02/03/1998	Iwamoto, *et al.*			02/27/1995
	A19	5,473,772	12/05/1995	Halliwell, *et al.*			09/02/1993
	A20	5,155,837	10/13/1992	Liu, *et al.*			03/02/1989
	A21	5,410,703	04/25/1995	Nilsson, *et al.*			07/01/1992
	A22	5,421,017	05/30/1995	Scholz, *et al.*			01/14/1994
	A23	5,682,533	10/28/1997	Siljestroemer			09/27/1994
	A24	5,885,158	03/23/1999	Torango, *et al.*			09/10/1996
	A25	2002/0137217	09/26/2002	Rowe			12/21/2000
	A26	2003/0064771	04/03/2003	Morrow, *et al.*			09/28/2001
	A27	2003/0188306	10/02/2003	Harris, *et al.*			03/26/2003
	A28	5,643,086	07/01/1997	Alcorn, *et al.*			06/29/1995
	A29	5,555,418	09/10/1996	Nilsson, et al.			01/30/1995

Examiner	**Date Considered**

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified)	**Atty Docket No.**	**Application No.:**
	IGT1P034X1/P-277 CIP	10/116,424
Information Disclosure	**Applicant:**	
Statement By Applicant	Binh T. Nguyen, *et al.*	
	Filing Date	**Group**
(Use Several Sheets if Necessary)	April 3, 2002	3711

Foreign Patent or Published Foreign Patent Application

Examiner Initial	**No.**	**Document No.**	**Publication Date**	**Country or Patent Office**	**Class**	**Sub-class**	**Translation**	
							Yes	**No**
	B1	EP 0841 615	05/13/1998	EPO			X	
	B2	EP 0 706 275	04/10/1996	EPO			X	
	B3	EP 0 905 614	03/31/1999	EPO			X	
	B4	0 689 325	06/20/1995	EPO			X	
	B5	WO 01/20424 A2	22/03/2001	PCT			X	
	B6	EP 1 004 970	31/05/2000	EPO			X	

Other Documents

Examiner Initial	**No.**	**Author, Title, Date, Place (e.g. Journal) of Publication**
	C1	Hiroaki Higaki, 8 page document entitled "Group Communication Algorithm for Dynamically Updating in Distributed Systems" Copyright 1994 IEEE International Conference On Parallel and Distributed Systems (pages 56 – 62) 08-8186-655-6/94, higaki@sdesun.slab.ntt.jp
	C2	Steffen Hauptmann, *et al.*, 12 page document entitled "On-line Maintenance With On-The-Fly Software Replacement" Copyright 1996 IEEE Proceedings, Third International Conference On Configurable Distributed Systems, (pages 70 – 80) 0-8186-7395-8/96
	C3	Hiroaki Higaki, 9 page document entitled "Extended Group Communication Algorithm For Updating Distributed Programs" Copyright 1996, IEEE, International Conference ON Parallel and Distributed Systems, 0-8186-7267-6/96, , hig@takilab.k.dendai.as.jp

Examiner	**Date Considered**

xaminer: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 841 615 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.05.1998 Bulletin 1998/20

(51) Int. Cl.^{6}: **G06F 9/445**, G06F 9/44

(21) Application number: 97307138.4

(22) Date of filing: 15.09.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: 08.11.1996 GB 9623298

(71) Applicant:
INTERNATIONAL COMPUTERS LIMITED
Putney, London, SW15 1SW (GB)

(72) Inventor: Rowley, David John
Warrington, Cheshire WA4 5HZ (GB)

(74) Representative:
Guyatt, Derek Charles
Intellectual Property Department
International Computers Limited
Cavendish Road
Stevenage, Herts, SG1 2DY (GB)

(54) Updating mechanism for software

(57) A computer has a memory storing a number of software applications, and a registration file, indicating which application versions are currently installed in the memory. A software update mechanism in the computer accesses a remote file server to obtain a release file containing a list of software applications available from the remote server, and compares the release file with the registration file to determine which of the installed applications have upgrades available. When a user selects an application for upgrading, and the update mechanism accesses the remote file server to obtain a manifest file containing details of the application files required to form an updated version of this applications. The manifest file is used to determine which of the required application files are already available in the computer; and only those application files that are not already available in the computer are accessed and installed in the memory.

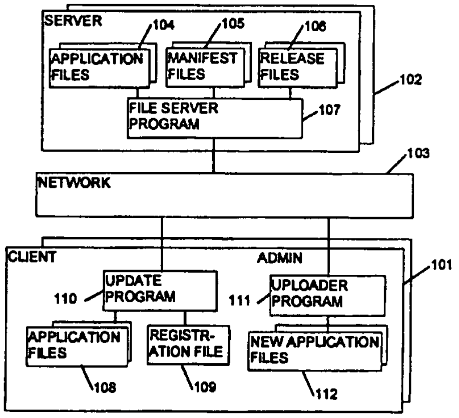


FIG. 1

Printed by Xerox (UK) Business Services
2.16.2/3.4

Description

Background to the Invention

This invention relates to an updating mechanism for software applications.

The invention is concerned with the problem of updating a number of software applications installed in a number of client computers. Conventionally, this is done by distributing the update information on media such as floppy disks or CD-ROMs. It is also possible for users to download required updates over a network from a file server, for example using a standard file transfer protocol such as ftp.

Problems with these existing methods of updating software applications are that they are inconvenient for the user, requiring the user to perform actions to obtain the necessary update information and to install it on the user's computer, and that the administrative function does not know whether the update has been done. The object of the present invention is to provide a more convenient and user-friendly mechanism for performing updates.

Summary of the Invention

According to the invention a computer comprises a memory storing a plurality of software applications and storing a registration file, indicating which applications are currently installed in said memory and their version details, the computer also including a software update mechanism comprising:

(a) means for accessing a remote file server to obtain a release file containing a list of software applications available from the remote server and their current version details;
(b) means for comparing said release file with said registration file to determine which of the installed applications have upgrades available;
(c) user interface means for allowing a user to select at least one of said applications for upgrading;
(d) means for accessing the remote file server to obtain a manifest file containing details of the application files required to form an updated version of the selected application;
(e) means for using the manifest file to determine which of said application files are already available in the computer; and
(f) means for accessing the remote file server to retrieve those application files that are not already available in the computer, and installing those files in the memory.

Brief Description of the Drawings

Figure 1 is a block diagram of a computer network, including a number of clients and servers.

Figure 2 is a flow chart of an uploader program.

Figures 3A and 3B are flow charts of an update program.

Figures 4 to 8 show screen displays used by the uploader program.

Figure 9 shows a screen display used by the update program.

Description of an Embodiment of the Invention

One embodiment of the invention will now be described by way of example with reference to the accompanying drawings.

Figure 1 shows a computer network comprising a number of client computers 101 and a number of server computers 102, interconnected by a network 103. The computers 101, 102 may for example be standard personal computers (PCs) running under the Microsoft Windows operating system. The network 103 may employ a conventional transport protocol, such as TCP/IP.

Each file server 102 stores a number of application files 104, forming a number of software applications. Normally, each application consists of several application files. The application files are stored in compressed form, using any standard data compression technique.

Conveniently, the server has a number of application directories, one for each application. Each of these directories has a number of sub-directories, which hold the new or amended application files for different versions of the application. Typically, one of these versions is an installer version of the application, while the other versions are non-installers. An installer is an executable program which, when run on a client machine, sets up the correct environment for the application. Normally, the first release of an application is an installer, and subsequent releases are non-installers.

Each file server also stores a number of manifest files 105, one for each version of each application stored on the server. These manifest files are stored in the relevant sub-directories, and each has a name constructed from the name and release number of the application to which it relates. Each manifest file contains a list of the application files that make up the particular version of the application. For each application file, it contains the following parameters:

- The filename of the application file.
- The version number of the application file.
- The target directory into which the application file should be installed.
- Date and time of issue.
- File size and compressed file size.
- An action parameter which indicates whether the file is to be installed, to be deleted, or to be executed on download.
- A flag which indicates access permissions of the

file, e.g. read only.

- A cyclic redundancy checksum (CRC).

Additionally, each server stores one or two release files 106 containing a list of all the applications available on the server. For each application, a release file contains the following parameters:

- The name of the application, i.e. a short identifying name for the application.
- The version number of the application.
- The application title, i.e. an identifier by which it is known to the user. (Note that the application title is distinct from the application name).
- A parameter which specifies a linkage between this application and another application, such that any upgrade to this application will automatically cause the other application to be upgraded.
- A list of user names indicating which users are permitted to download the application. If no user names are specified, any user is permitted to download the application.
- A parameter which specifies whether the version number should be displayed to the user as a date.
- The status of the application.

A release file may be in one of two states: live or deferred. When the release file is in the live state, it is visible to the software updating mechanism; otherwise it is invisible. At any point in time on a server, there will be either:

(a) one live release file and no (i.e. an empty) deferred release file; or
(b) one live release file and one deferred release file.

Each server computer includes a standard file server program 107, which can supply (to the update program) or receive (from the uploader program) files over the network on request to or from any of the client computers, using a standard file transfer protocol such as ftp.

Each of the client computers 101 stores a number of software applications, each consisting of a number of application files 108. Each client also stores a registration file 109 containing a list of all the applications currently installed on the client which are to be maintained by a software updating mechanism. For each application, the registration file contains the following parameters:

- The application name.
- The latest version number installed on the client.
- The application title.
- The directory in which the application is installed.

In general, the applications currently installed on any given client will be a subset of the applications available on the servers, and may not be the most up-to-date versions of those applications.

Each client computer includes an update program 110, which provides a mechanism for updating the software applications installed on that computer, and for installing new applications if required.

The system also includes an uploader program 111, which provides a mechanism for uploading a new or updated version of an application onto the servers. In Figure 1, the uploader program 111 is shown as resident on one of the client computers 101. Alternatively, the uploader may reside on a different computer, such as one of the servers, or on a separate system administration computer. The new or updated application comprises a set of new application files 112, accessible to the computer in which the uploader resides.

Uploader program

Figure 2 shows the operation of the uploader program 111. This program is used by a system administrator when it is desired to upload a new or updated version of a software application onto the servers. The uploader is conveniently a Microsoft Windows program.

(Step 201) The uploader first displays a main screen, as shown in Figure 4, which allows the administrator to specify which of the servers 102 is to act as a source server for obtaining a release file. The administrator can also specify the file transfer protocol to be used, for example ftp. This main screen is displayed throughout the uploader session, and plots the progress of the session,

The administrator can also specify, by way of message boxes, whether the new or updated application is an installer or a non-installer, and whether a deferred or live release file is to be used as a source. Of course, the second question is only asked if there is a non-empty deferred release file in existence at that time. If not, then the live release file is used as source by default. When a release file is made live, the deferred release file is emptied, i.e. it effectively does not exist.

(Step 202) Selecting the "Start" button from the main screen causes the uploader to contact the specified source server and to check whether the chosen release file is available.

(Step 203) If the chosen release file is not available, the uploader asks if a new uploader environment is to be created in the source server. If so, it then sets up a new skeleton directory structure and empty release files (live and deferred), and then exits.

(Step 204) Assuming that the chosen release file is available, the uploader fetches this file from the source server.

(Step 205) The uploader then displays a "Select New Release" screen, as shown in Figure 5. This screen allows the administrator to select either a "Base on Existing Application" option or a "New Application" option.

If the "Base on Existing Application" option is selected, the uploader displays a list of the existing software applications, along with their version numbers, derived from the chosen release file. The administrator can then select one of these existing applications and enter a new version number. If the "New Application" option is selected, the administrator can enter a new name ("Moniker") and a version number for the new application.

If an "Edit Release Details" button is selected, the uploader proceeds to Step 206 below. If an "OK" button is selected, the uploader proceeds to Step 209.

(Step 206) If the "Edit Release Details" button is selected, the uploader displays a screen as shown in Figure 6, which allows the administrator to update an entry in the release file, or to create a new entry. This screen includes the following text input boxes:

"Title" - the application title.
"DependsUpon" - this specifies a linkage between this application and another application.
"UserName" - a list of user names indicating which users are permitted to download the application.
"DisplayAsDate" - a parameter specifying whether the version number should be displayed to the user as a date.
"Status" - the status of the application.

Selection of a "Select Target Servers" button causes the uploader to proceed to Step 207 below. Selection of an "OK" button causes the uploader to proceed to Step 208, provided that at least one target server has been selected; if not it displays a warning message that no target server has been selected.

(Step 207) If the "Select Target Servers" button is selected, the uploader displays a screen as shown in Figure 7, which allows the administrator to select one or more servers as target servers, to receive the updated release file. Selecting the "OK" button on this screen causes the uploader to return to Step 206.

(Step 208) The uploader writes the updated release file to each of the selected target servers for an existing application. This allows a system administrator to only update these release fields on the servers without going through a full uploader session or even creating a new release version of the application. However, for a new application, the uploader does not update the release file with the new release fields and write it to the servers until an actual release exists on the servers at step 212.

(Step 209) The uploader contacts the source server to obtain the manifest file for the selected application.

(Step 210) The uploader then displays a screen as shown in Figure 8, showing the contents of the manifest file. This file can then be edited by the administrator, so as to create a new manifest file for the new or updated application. This may involve, for example, adding new directories or files, removing files, marking existing files for deletion on download, marking files for execution on download, and editing other file details (e.g. marking the file read only). This is done through menu commands.

(Step 211) The uploader can then display a screen as shown in Figure 7 through a menu command if not done at step 207, allowing the administrator to select one or more servers as target servers, or to modify any existing selection done at step 207.

(Step 212) By choosing the appropriate menu command, the system administrator can then cause the uploader to write the updated release file, the new manifest file and all the new application files 112 to each of the selected target servers. The updated release file may be written in either a deferred or live state. If it is written in the live state, then any existing deferred release file is emptied.

Optionally, the updated release file may be sorted into a user-defined order before it is written (which is the order displayed in Figure 9). Also optionally, the uploader may tidy the filestore on each target server after performing the writes.

(Step 213) The uploader also saves the previous version number of the application and, optionally, prints out the release files.

(Step 214) The uploader then asks the administrator whether the release is to be repeated to new or failed servers. If so, the uploader returns to Step 211; otherwise it exits.

Update program

Figures 3A and 3B show the operation of the update program 110. This program can be run at any time on request by a user. Conveniently, it is a Microsoft Windows program.

(Step 301) Referring to Figure 3A, the update program first contacts one of the servers 102, by way of the network 103, to obtain the live release file from that server.

(Step 302) The update program then compares this release file with its locally held registration file 109, to identify which of the currently installed applications have more recent versions available. It also identifies any new application installers in the release file for applications that are not installed locally on the client.

The update program then displays a screen, as shown in Figure 9, which allows the user to select either an "Updates" option or a "New Release" option. If the user selects the "Updates" option, the update program proceeds to step 303 in Figure 3A. Alternatively, if the user selects the "New Release" option, the update program proceeds to step 310 in Figure 3B (see below).

(Step 303) If the user selects the "Updates" option, a list of the titles and versions of currently installed applications is displayed, as shown in Figure 9. The display indicates which, if any, of the applications have more recent versions available. As an example, Figure 9 shows that the installed application "Peripheral Products Binder [1/10/96]" is up-to-date, while the installed application "Networking Binder [1/9/96]" has a more recent version available. The user may select from this list one or more (or all) of the applications for which a more recent version is available. Selection of an application will automatically cause any dependent applications to be selected.

If there is a more recent version available of the update program itself, this is automatically selected. Hence, every time the update program runs it will update itself if necessary.

If the user selects the "OK" button on this screen, the program proceeds to Step 304 below. Alternatively, the user may simply exit from the program without performing any updates by selecting the "Cancel" button.

(Step 304) Assuming the "OK" button was selected in step 303, the update program contacts the server 102 to obtain the manifest file for the first (or only) of the selected applications.

(Step 305) The update program then determines differences between files installed on the client computer and those listed in the manifest file. For each application file listed in the manifest file, a check is made to determine whether the specified file is already present in the specified directory in the client by using CRC checks. If not, the program contacts the server 102, to retrieve the required application file. The retrieved file is expanded, and then checked for file-transfer corruption, using the CRC checksum. All the application files are read into a temporary directory on the client computer.

Thus, it can be seen that the update program does not fetch any application file if the required version of that file is already installed in the required directory, thereby eliminating unnecessary traffic over the network.

(Step 306) When all the files listed in the manifest file have been correctly retrieved, the installation actions are implemented as follows. Any files marked for deletion are deleted from the client computer, files marked for execution are executed and files marked for installation are installed into the specified directories in the client, provided the file version is more advanced than that of the existing file. Hence then any existing files with the same names in the directories will be overwritten.

If, on the other hand, some of the file transfers failed, none of the files are installed. Instead, a message is displayed, giving the user the option of either cancelling the update, or making another attempt to access the files.

(Step 307) If all the required applications have now been updated, the update program proceeds to Step 308. Otherwise it returns to Step 304 above to get the manifest file for the next required application to be updated.

(Step 308) Before exiting, the update program allows the user to return feedback (i.e. comments on the update program or the other applications the user is downloading and using) to a central server. The program also automatically returns statistics to the central server, showing who the user is and what has been downloaded. The central server maintains a table based on these statistics, allowing the system administrator to check whether each user is using the latest versions of the software applications.

Referring now to Figure 3B, if the user selects the "New Release" option from the screen shown in Figure 9, the update program proceeds as follows.

(Step 310) A list of newly released application installers, for applications not currently installed on this client, is displayed. The user may select only one of the application installers from this list.

If the user selects the "OK" button on this screen, the program proceeds to Step 311 below. Alternatively, the user may simply exit from the program without performing any updates by selecting the "Cancel" button.

(Step 311) If the "OK" button was selected in step 310, the update program contacts the server 102 to obtain the manifest file for the selected application installer.

(Step 312) A check is then made to determine whether the specified installer file is already present in the specified directory in the client by using CRC checks. If not, the program contacts the server 102, to retrieve the required installer file. The retrieved file is expanded, and then checked for file-transfer corruption, using the CRC checksum. The installer file is read into the temporary directory, and remains there for subsequent execution.

(Step 313) The update program returns statistics on the installation to the central server.

(Step 314) The update program then displays a message box, asking whether the user wishes to execute the installer now.

(Step 315) If the user selects "Yes" from this message box, the update program exits and enters the installer.

The update program logs its actions, so that in the event of a failure, such as a communications failure, it can restart from the point where the last file was correctly received.

It should be noted that the software update mechanism and the uploading mechanism described above do not require any special-purpose software resident on the servers. The servers run standard file server programs, and all the intelligence for the software update mechanism and the uploading mechanism resides solely in the update program and the uploader program.

Some possible modifications

It will be appreciated that many modifications may be made to the system described above without departing from the scope of the present invention. For example, the system may be adapted to different operating systems and transport protocols.

Claims

1. A computer comprising a memory storing a plurality of software applications and storing a registration file, indicating which applications are currently installed in said memory and their version details, the computer also including a software update mechanism comprising:

   (a) means for accessing a remote file server to obtain a release file containing a list of software applications available from the remote server and their current version details;
   (b) means for comparing said release file with said registration file to determine which of the installed applications have upgrades available;
   (c) user interface means for allowing a user to select at least one of said applications for upgrading;
   (d) means for accessing the remote file server to obtain a manifest file containing details of the application files required to form an updated version of the selected application;
   (e) means for using the manifest file to determine which of said application files are already available in the computer; and
   (f) means for accessing the remote file server to retrieve those application files that are not already available in the computer, and installing those files in the memory.

2. A computer according to Claim 1 wherein said manifest file also includes details of application files required to be deleted or executed in order to form the updated version of said selected application.

3. A computer according to Claim 1 or 2, wherein said release file includes at least one parameter specifying a linkage between a first application and a second application, and wherein said user interface means automatically selects said second application for upgrading whenever said first application is selected for upgrading.

4. A computer according to any preceding claim, wherein said software update mechanism comprises an update program, and wherein said user interface means automatically selects the update program for upgrading whenever one of said applications is selected for upgrading.

5. A computer according to any preceding claim including means for using a checksum to check said application files when retrieved from said remote file server and for allowing the retrieved files to be installed only if the check is satisfactory.

6. A computer according to any preceding claim, further comprising:

   (a) means for comparing said release file with said registration file to identify available new installer versions of applications;
   (b) user interface means for allowing a user to select one of said installer versions;
   (c) means for accessing the remote file server to obtain a manifest file containing details of the installer files associated with said one of said installer versions;
   (d) means for using the manifest file to determine which of said installer files are already available in said memory means; and
   (e) means for retrieving those installer files that are not already available in said memory means from the remote file server, and executing those files.

7. A computer network comprising a plurality of server computers and a plurality of client computers, wherein each of the client computers comprises:

   (a) memory means for storing a plurality of software applications, and for storing a registration file, indicating which applications are currently installed in the memory means and their version details;
   (b) means for accessing one of said server computers to obtain a release file containing a list of software applications available from said server computer and their current version details;
   (c) means for comparing said release file with said registration file to determine which of the installed applications have upgrades available;
   (d) user interface means for allowing a user to select at least one of said applications for upgrading;
   (e) means for accessing said server computer to obtain a manifest file containing details of the application files required to form an updated version of the selected application;
   (f) means for using the manifest file to determine which of said application files are already available in said memory means; and
   (g) means for accessing said server computer to retrieve those application files that are not already available in said memory means, and installing those files in said memory means.

8. A computer network according to Claim 7 wherein at least one of said computers includes an uploader mechanism comprising:

   (a) means for accessing one of said server computers to obtain a manifest file containing details of the application files forming a current version of a particular application;

(b) means for editing the manifest file to form a new manifest file for a new or updated application;

(c) means for writing the new manifest file, along with application files for the new or updated application, into one or more of the server computers.

9. A computer network according to Claim 7 or 8 wherein at least one of said servers includes means for maintaining statistics on which applications have been downloaded by which users.

10. A method of updating software in a computer, the method comprising:

(a) storing a registration file, indicating which applications are currently installed in the computer and their version details;

(b) accessing a remote file server to obtain a release file containing a list of software applications available from the remote server and their current version details;

(c) comparing said release file with said registration file to determine which of the installed applications have upgrades available;

(d) allowing a user to select at least one of said applications for upgrading;

(e) accessing the remote file server to obtain a manifest file containing details of the application files required to form an updated version of the selected application;

(f) using the manifest file to determine which of the required application files are already available in the computer; and

(g) accessing the remote file server to retrieve those application files that are not already available in the computer, and installing those files in the computer.

11. A method according to Claim 10, including the further step of deleting or executing further application files as specified in said manifest file.

12. A method according to Claim 10 or 11, wherein said release file includes at least one parameter specifying a linkage between a first application and a second application, and including the further step of automatically selecting said second application for upgrading whenever said first application is selected for upgrading.

13. A method according to any one of Claims 10 to 12, including the further step of automatically selecting an update program for upgrading whenever one of said applications is selected for upgrading.

14. A method according to any one of Claims 10 to 13 including the further step of using a checksum to check said application files when retrieved from said remote file server, and allowing the retrieved files to be installed only if the check is satisfactory.

15. A method according to any one of Claims 10 to 14, including the further steps:

(a) comparing said release file with said registration file to identify available new installer versions of applications;

(b) allowing a user to select one of said installer versions;

(c) accessing the remote file server to obtain a manifest file containing details of the installer files associated with said one of said installer versions;

(d) using the manifest file to determine which of said installer files are already available in said memory means; and

(e) retrieving those installer files that are not already available in said memory means from the remote file server, and executing those files.

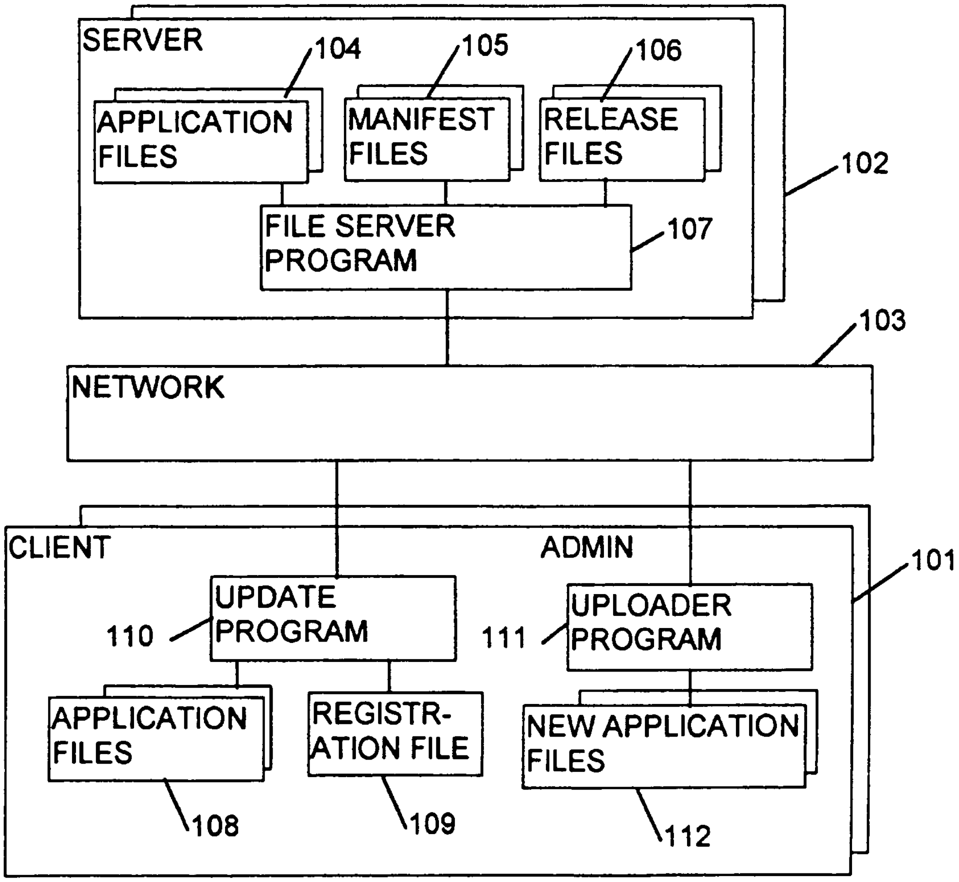

SERVER
104
105
106
APPLICATION FILES
MANIFEST FILES
RELEASE FILES
102
FILE SERVER PROGRAM
107
103
NETWORK
CLIENT
ADMIN
101
UPDATE PROGRAM
110
111
UPLOADER PROGRAM
APPLICATION FILES
REGISTR-ATION FILE
NEW APPLICATION FILES
108
109
112

FIG. 1

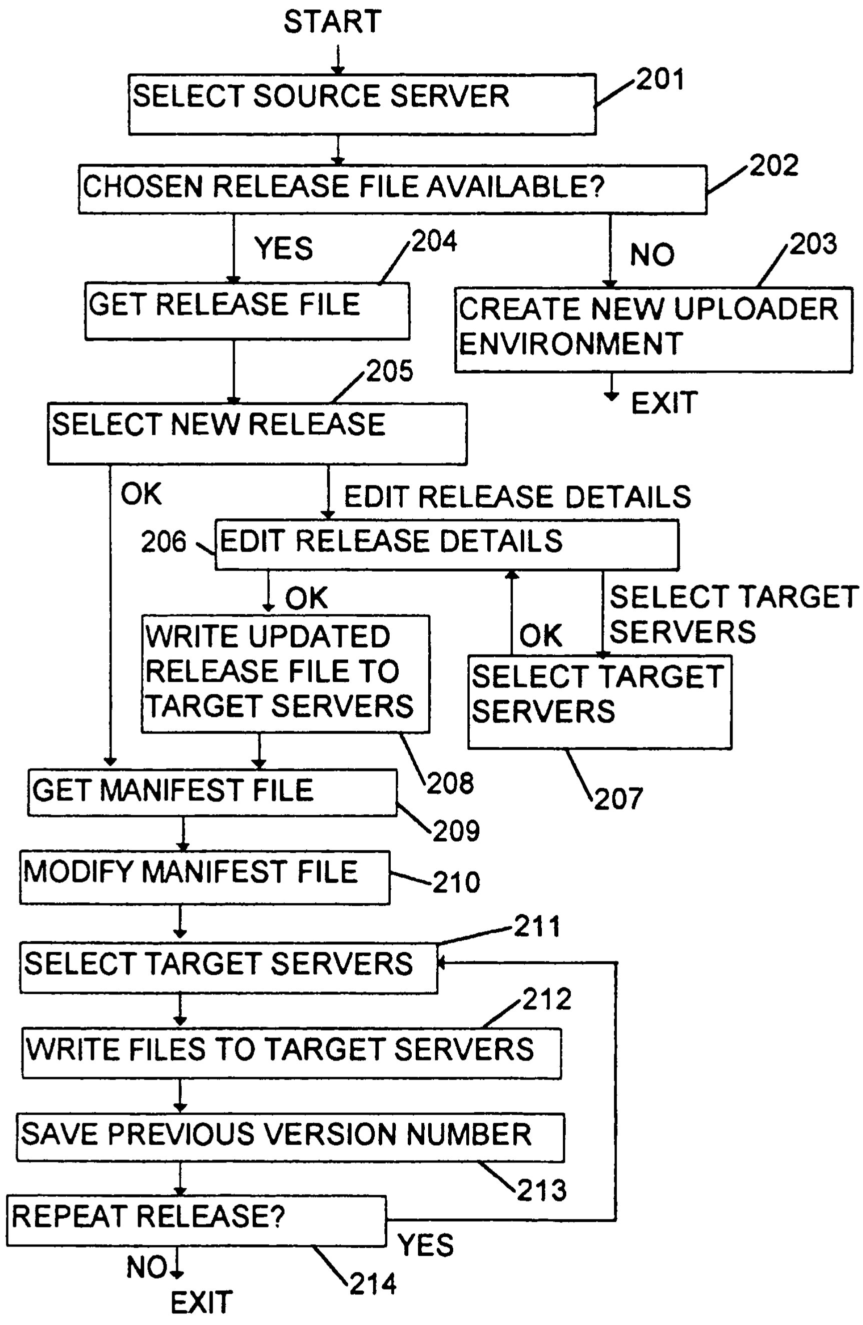

START
SELECT SOURCE SERVER
201
CHOSEN RELEASE FILE AVAILABLE?
202
YES
204
NO
203
GET RELEASE FILE
CREATE NEW UPLOADER ENVIRONMENT
EXIT
205
SELECT NEW RELEASE
OK
EDIT RELEASE DETAILS
206
EDIT RELEASE DETAILS
OK
SELECT TARGET SERVERS
WRITE UPDATED RELEASE FILE TO TARGET SERVERS
OK
SELECT TARGET SERVERS
208
207
GET MANIFEST FILE
209
MODIFY MANIFEST FILE
210
211
SELECT TARGET SERVERS
212
WRITE FILES TO TARGET SERVERS
SAVE PREVIOUS VERSION NUMBER
213
REPEAT RELEASE?
YES
NO
EXIT
214

FIG. 2

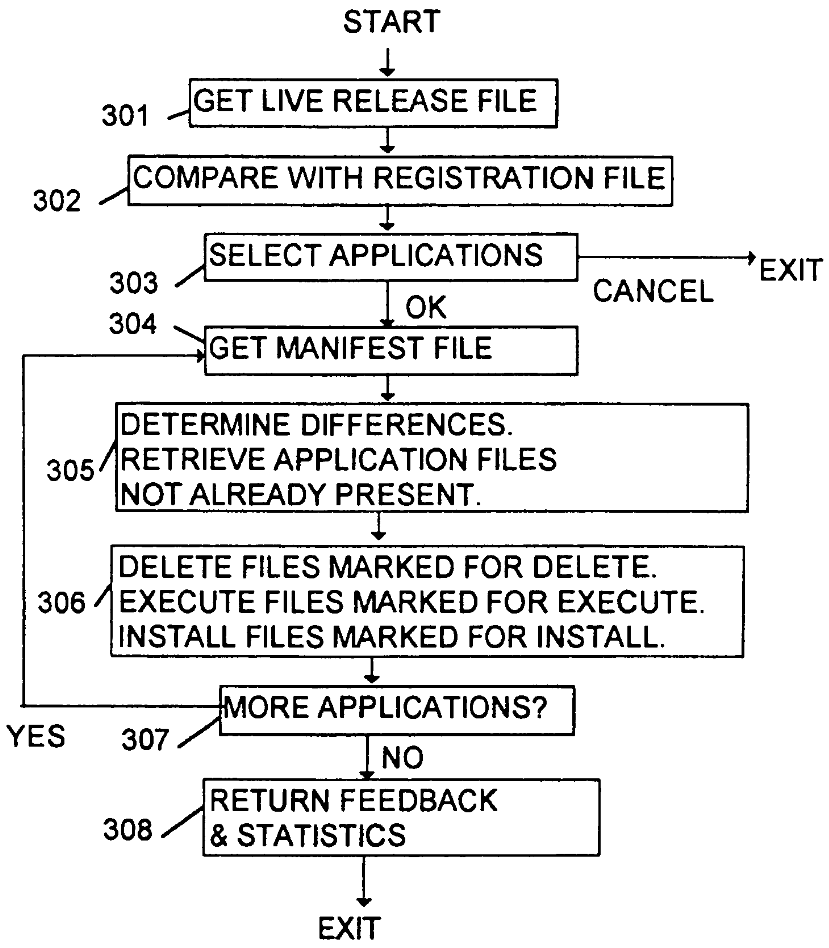

START
301
GET LIVE RELEASE FILE
302
COMPARE WITH REGISTRATION FILE
303
SELECT APPLICATIONS
CANCEL
EXIT
OK
304
GET MANIFEST FILE
305
DETERMINE DIFFERENCES.
RETRIEVE APPLICATION FILES
NOT ALREADY PRESENT.
306
DELETE FILES MARKED FOR DELETE.
EXECUTE FILES MARKED FOR EXECUTE.
INSTALL FILES MARKED FOR INSTALL.
MORE APPLICATIONS?
YES
307
NO
308
RETURN FEEDBACK
& STATISTICS
EXIT

FIG. 3A

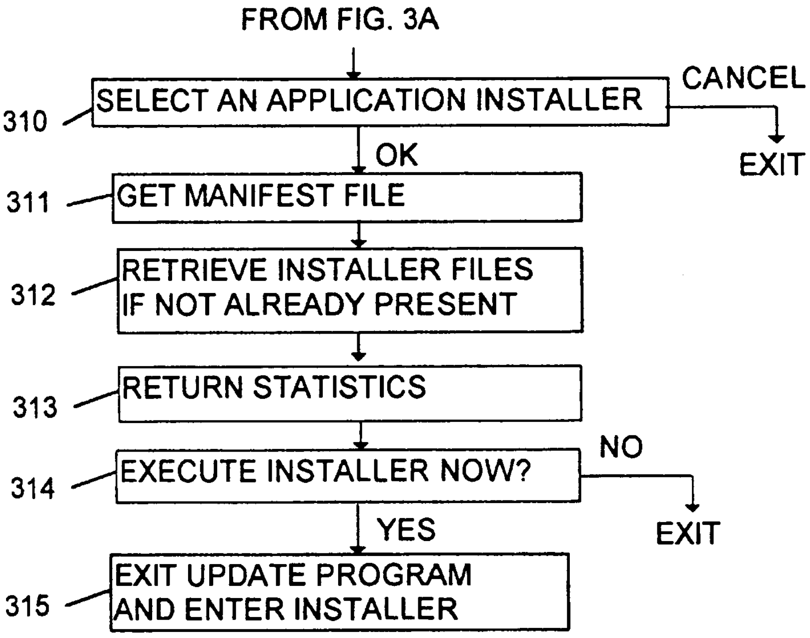
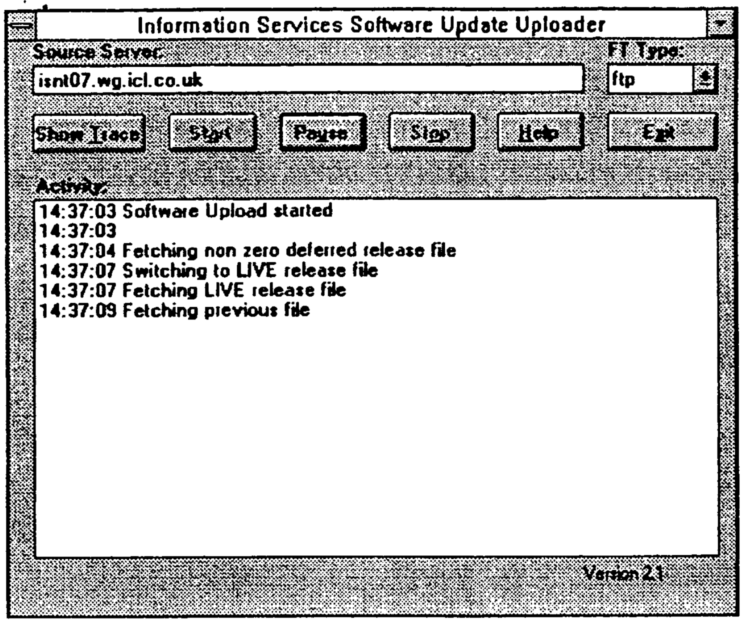

FROM FIG. 3A
310
SELECT AN APPLICATION INSTALLER
CANCEL
EXIT
OK
311
GET MANIFEST FILE
312
RETRIEVE INSTALLER FILES
IF NOT ALREADY PRESENT
313
RETURN STATISTICS
314
EXECUTE INSTALLER NOW?
NO
EXIT
YES
315
EXIT UPDATE PROGRAM
AND ENTER INSTALLER

FIG. 3B



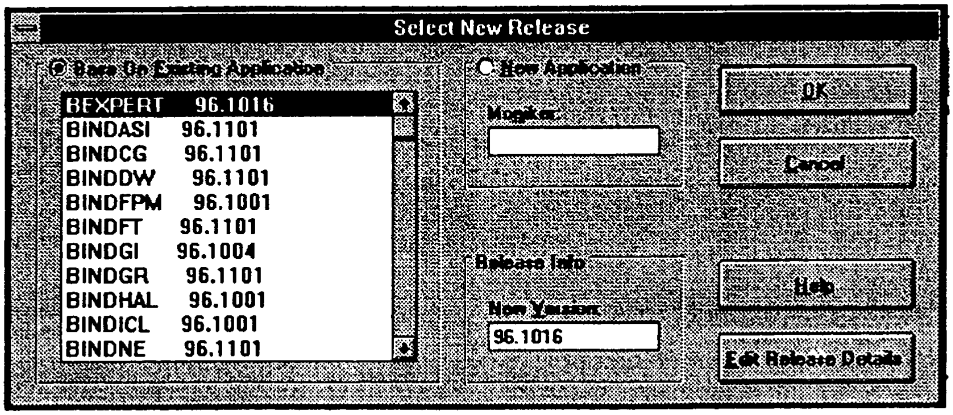
Source Server: isnt07.wg.icl.co.uk

FT Type: ftp

Activity:

```
14:37:03 Software Upload started
14:37:03
14:37:04 Fetching non zero deferred release file
14:37:07 Switching to LIVE release file
14:37:07 Fetching LIVE release file
14:37:09 Fetching previous file
```

FIG. 4



● Base On Existing Application

```
BEXPERT    96.1016
BINDASI    96.1101
BINDCG     96.1101
BINDDW     96.1101
BINDFPM    96.1001
BINDFT     96.1101
BINDGI     96.1004
BINDGR     96.1101
BINDHAL    96.1001
BINDICL    96.1001
BINDNE     96.1101
```

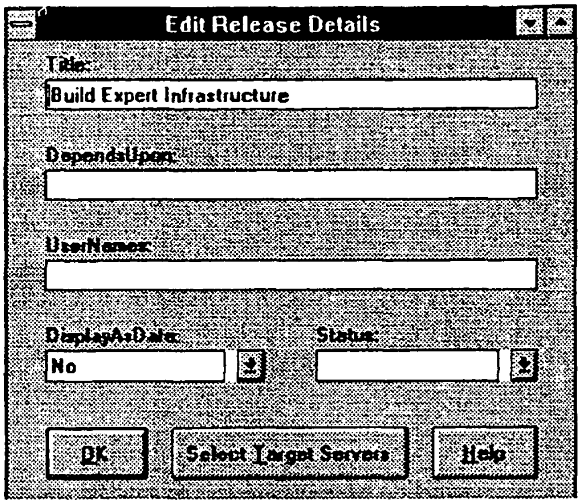
○ New Application

Moniker:

Release Info

New Version: 96.1016

FIG. 5



Edit Release Details

Title: Build Expert Infrastructure

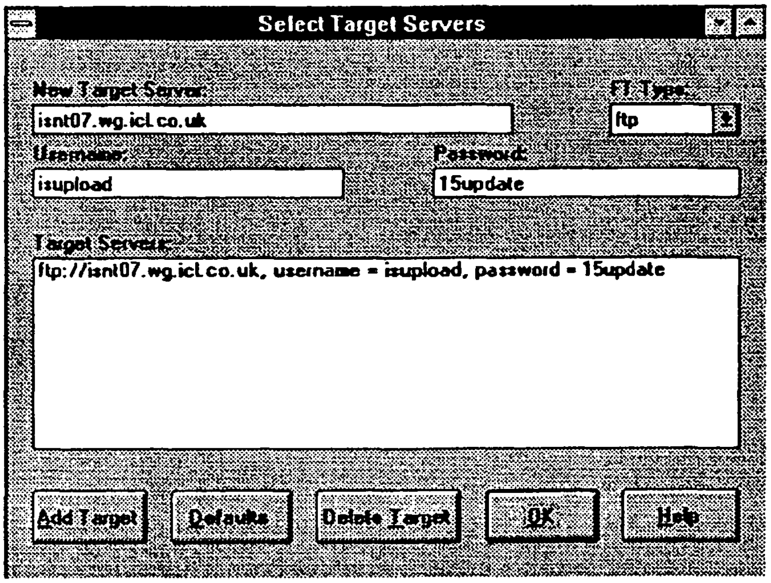
DependsUpon:

UserNames:

DisplayAsDate: No

Status:

FIG. 6



Select Target Servers

New Target Server: isnt07.wg.icl.co.uk

FT Type: ftp

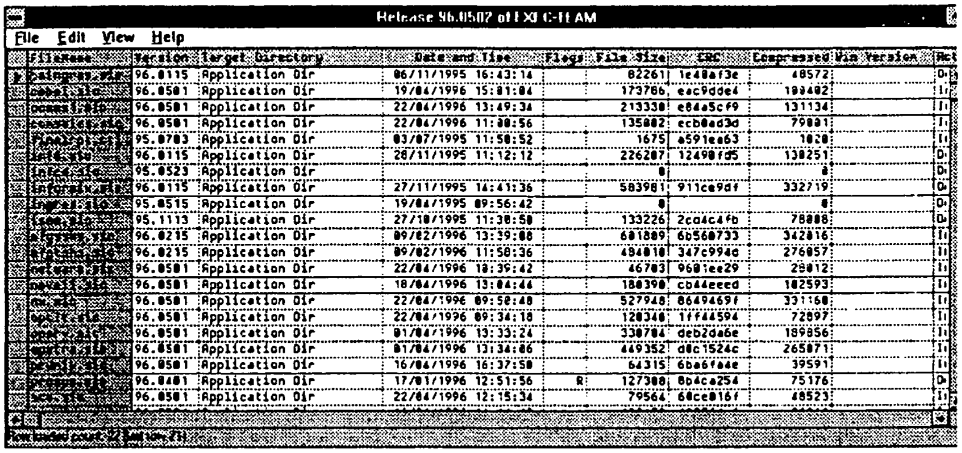
Username: isupload

Password: 15update

Target Servers:

ftp://isnt07.wg.icl.co.uk, username = isupload, password = 15update

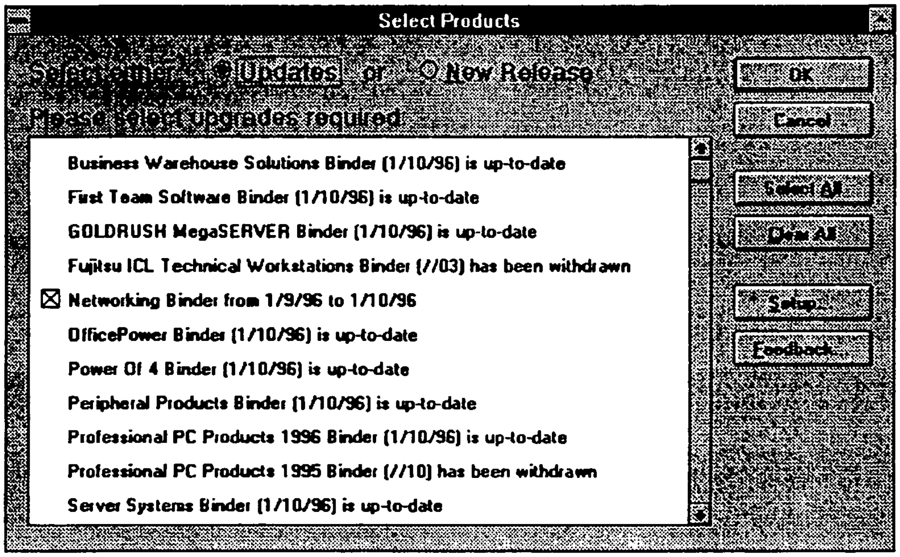
FIG. 7



Release 96.0507 of [illegible] AM

FileName	Version	Target Directory	Date and Time	Flags	File Size	CRC	Compressed	Win Version	Act
[illegible]	96.0115	Application Dir	06/11/1995 16:43:14		82261	1e40af3e	48572		D
[illegible]	96.0501	Application Dir	19/04/1996 15:01:04		173786	eac9dde4	100402		I
[illegible]	96.0501	Application Dir	22/04/1996 13:49:34		213330	e84a5cf9	131134		I
[illegible]	96.0501	Application Dir	22/04/1996 11:00:56		135002	ecb0ad3d	79001		I
[illegible]	95.0703	Application Dir	03/07/1995 11:50:52		1675	a591ea63	1020		I
[illegible]	96.0115	Application Dir	28/11/1995 11:12:12		226207	12490fd5	130251		D
[illegible]	95.0523	Application Dir			0		0		D
[illegible]	96.0115	Application Dir	27/11/1995 14:41:36		583981	911ce9df	332719		D
[illegible]	95.0515	Application Dir	19/04/1995 09:56:42		0		0		D
[illegible]	95.1113	Application Dir	27/10/1995 11:30:50		133226	2ca4c4fb	78008		D
[illegible]	96.0215	Application Dir	09/02/1996 13:39:08		601809	6b560733	342016		I
[illegible]	96.0215	Application Dir	09/02/1996 11:58:36		484010	347c994c	276057		I
[illegible]	96.0501	Application Dir	22/04/1996 10:39:42		46703	960iee29	28012		I
[illegible]	96.0501	Application Dir	18/04/1996 13:04:44		180390	cb44eeed	102593		I
[illegible]	96.0501	Application Dir	22/04/1996 09:50:40		527948	8649469f	331160		I
[illegible]	96.0501	Application Dir	22/04/1996 09:34:18		120340	1ff44594	72897		I
[illegible]	96.0501	Application Dir	01/04/1996 13:33:24		330704	deb2da6e	189056		I
[illegible]	96.0501	Application Dir	01/04/1996 13:34:06		449352	d0c1524c	265071		I
[illegible]	96.0501	Application Dir	16/04/1996 16:37:50		64315	6ba6fa4e	39591		I
[illegible]	96.0401	Application Dir	17/01/1996 12:51:56	R	127308	8b4ca254	75176		D
[illegible]	96.0501	Application Dir	22/04/1996 12:15:34		79564	60ce016f	48523		I

FIG. 8



Select Products

Select either: ● Updates or ○ New Release

Please select upgrades required

Business Warehouse Solutions Binder (1/10/96) is up-to-date

First Team Software Binder (1/10/96) is up-to-date

GOLDRUSH MegaSERVER Binder (1/10/96) is up-to-date

Fujitsu ICL Technical Workstations Binder (//03) has been withdrawn

☒ Networking Binder from 1/9/96 to 1/10/96

OfficePower Binder (1/10/96) is up-to-date

Power Of 4 Binder (1/10/96) is up-to-date

Peripheral Products Binder (1/10/96) is up-to-date

Professional PC Products 1996 Binder (1/10/96) is up-to-date

Professional PC Products 1995 Binder (//10) has been withdrawn

Server Systems Binder (1/10/96) is up-to-date

FIG. 9

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 905 614 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
08.12.2004 Bulletin 2004/50

(51) Int Cl.⁷: **G06F 9/445**

(21) Application number: **98118326.2**

(22) Date of filing: **28.09.1998**

(54) **Processing apparatus and an operation control information update system employing the processing apparatus**

Verarbeitungsanordnung und System zur Aktualisierung von Betriebssteuerungsinformationen unter Verwendung der Verarbeitungsanordnung

Dispositif de traitement et système de mise à jour des données de commande de fonctionnement en utilisant le dispositif de traitement

(84) Designated Contracting States:
DE FR GB

(30) Priority: **26.09.1997 JP 26253297**

(43) Date of publication of application:
31.03.1999 Bulletin 1999/13

(73) Proprietor: **Noritsu Koki Co., Ltd.**
Wakayama-shi, Wakayama-ken 640-8550 (JP)

(72) Inventor: **Masuda, Takeshi**
Wakayama-shi, Wakayama-ken (JP)

(74) Representative: **Müller-Boré & Partner**
Patentanwälte
Grafinger Strasse 2
81671 München (DE)

(56) References cited:
EP-A- 0 489 204
EP-A- 0 703 531
GB-A- 2 227 584

EP 0 905 614 B1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION AND RELATED ART STATEMENT

[0001] The present invention relates to a processing apparatus which performs a specified operation in accordance with operation control information, such as a processing program and data. stored in a memory as well as to an operation control information update system employing the processing apparatus.

[0002] The use of photographic processing machines in which film images, for instance, are automatically printed on photographic printing paper is widespread in recent years. In this kind of photographic processing machine, operational processes of individual processing segments, such as an exposure processor and a development processor, are controlled based on a processing program and data (hereinafter referred to as operation control information) which are stored in a memory in carrying out exposure, development and other processing steps. The operation control information stored in the memory is updated when the processing program has been upgraded or when the need arises to do so for other reasons whatsoever. Conventionally, when the need arises to update the operation control information, service personnel visit each of their customers carrying a floppy disk on which an upgrade version of the operation control information is written, load the disk in a floppy disk drive of the photographic processing machine, and update the previously stored operation control information overwriting it with the new operation control information read out from the disk.

[0003] One problem of this conventional method is that the customers can not use their photographic processing machines while the operation control information including the processing program and data is being updated. It has therefore been necessary for the service personnel to visit their customers during time periods specified by the individual customers, and this has considerably decreased labor efficiency in updating the operation control information. Another problem is that locations of the customers are usually distant from one another, making it necessary for the service personnel to spend much time in moving from one customer to another. Accordingly, the number of machines handled by the service personnel in a given period of time is limited. This also has contributed to deterioration of labor efficiency in updating the operation control information. Such problems would be encountered not only with the photographic processing machines but with other processing apparatus which perform a specified operation in accordance with operation control information stored in a memory.

[0004] As a further example, EP-A-0 489 204 relates to a data storage device, which can be re-programmed with new program codes, comprising input/output means, media read/write means, a data buffer and control and processing means, which are connected to the input/output means, the data buffer and the read/write means, and operative to control the transfer of data via said data buffer between the input/output means and the read/write means and to process said data, said data control and processing means including a nonvolatile memory for holding a program code and a program-controlled processor operative to execute said program code.

SUMMARY OF THE INVENTION

[0005] It is an object of the invention to provide a processing apparatus which makes it possible to update operation control information stored in a memory in an efficient manner and an operation control information update system employing such processing apparatus.

[0006] The present invention is defined in the appended claims.

[0007] According to one important aspect of the invention, a processing apparatus comprises an apparatus controller which includes a control information memory for storing operation control information, enabling the processing apparatus to perform a specified operation and an information controller which includes an update information memory for holding operation control information transmitted from a control center and an information updater for updating the operation control information currently stored in the control information memory by transferring the operation control information held in the update information memory to the control information memory.

[0008] In the processing apparatus thus constructed, the operation control information including a processing program and associated data received from the control center is temporarily stored in the update information memory of the information controller. The operation control information thus stored in the update information memory is transferred to the control information memory of the apparatus controller by the information updater to thereby update the operation control information previously stored in the control information memory.

[0009] According to another aspect of the invention, the information updater may be set to transfer the operation control information taken into the update information memory to the control information memory on condition that transmission of the operation control information from the control center has been completed.

[0010] In this construction, the information updater begins to transfer the operation control information taken into the update information memory at the end of transmission from the control center. The expression "end of transmission" above does not necessarily refer to the completion of transmitting the whole operation control information, but it implies a situation in which a certain amount of information that corresponds to the storage capacity of the update information memory, or any predefined amount of information, has just been transmitted. In this latter case, when transmission of the predefined amount, or portion, of the operation control information has been completed, that portion of the operation control information is transferred to the control information memory and, then, each successive portion of the operation control information is taken into the update information memory and transferred to the control information memory until the whole operation control information is transferred to the control information memory.

[0011] According to still another aspect of the invention, the information updater may be set to transfer the operation control information taken into the update information memory to the control information memory on condition that a prescribed prerequisite for information updating has been satisfied.

[0012] With this arrangement, the operation control information taken into the update information memory is transferred to only when the prescribed prerequisite for information updating has been satisfied.

[0013] According to yet another aspect of the invention, the processing apparatus may further comprise a power supply for providing electric power to the processing apparatus and the aforementioned prerequisite for information updating is that the power supply has been activated.

[0014] In this construction, the information updater begins to transfer the operation control information taken into the update information memory to the control information memory when the power supply which provides electric power to the whole processing apparatus has been activated by turning on a power switch of the processing apparatus, or when processing apparatus has been started up.

[0015] According to a further aspect of the invention, the aforementioned prerequisite for information updating may be a transfer command given by an operator. With this arrangement, the information updater begins to transfer the operation control information taken into the update information memory to the control information memory when the operator gives a transfer command by turning on a transfer start switch, for example.

[0016] According to a still further aspect of the invention, the processing apparatus may further comprise a writing device for writing operation control information on an external storage medium loaded in the processing apparatus and the aforementioned prerequisite for information updating is that the writing device has become ready to write on the external storage medium.

[0017] In this construction, the information updater begins to transfer the operation control information taken into the update information memory to the control information memory when an external storage medium, such as a floppy disk, has been loaded and the writing device has become ready to write on the external storage medium. The operation control information thus updated is copied onto the external storage medium.

[0018] According to a further aspect of the invention, the aforementioned prerequisite for information updating may be that the operation control information is not stored in the control information memory.

[0019] In this arrangement, the information updater begins to transfer the operation control information taken into the update information memory to the control information memory in response to an information request signal, for instance, which would be generated when the control information memory been replaced and it does not store the correct operation control information, or any operation control information at all, necessary for controlling the processing apparatus.

[0020] According to a further aspect of the invention, the processing apparatus may further comprise a display unit for displaying information on the operation control information taken into the update information memory. In this construction, information on the operation control information received from the control center, such as changes to the existing operation control information, is displayed on the display unit. This allows the operator to decide whether or not to update the operation control information after verifying the contents of changes displayed on the display unit.

[0021] According to a still further aspect of the invention, the processing apparatus may further comprise an update enabling device for enabling transfer of the operation control information taken into the update information memory and displayed on the display unit to the control information memory.

[0022] In this arrangement, the operation control information taken into the update information memory is transferred to the control information memory only when the update enabling device has been operated. This allows the operator to update the operation control information only when he, or she. thinks it is necessary to do so after verifying the contents of changes to the current operation control information displayed on the display unit.

[0023] According to another important aspect of the invention, an operation control information update system comprises an operation control information transmitting apparatus for transmitting an operation control information; and a processing apparatus for receiving the operation control information from the operation control information transmitting apparatus. The processing apparatus includes an apparatus controller and an information controller. The apparatus controller has a control information memory for storing the operation control information, enabling the processing apparatus to perform a specified operation and the information controller having an update information memory for holding the operation control information transmitted from the operation control information transmitting apparatus and an information updater for updating the operation control information currently stored in the control information memory by transferring the operation control information held in the update information memory to the control information memory.

[0024] In this arrangement, the operation control information including a processing program and associated data. for instance, is transmitted from the operation control information transmitting apparatus and received by the processing apparatus. The operation control information received by the processing apparatus is once stored in the update information memory of the information controller and transferred to the control information memory of the apparatus controller to thereby update the operation control information previously stored in the control information memory.

[0025] It will be appreciated that the invention permits efficient updating of the operation control information stored in the control information memory.

[0026] These and other objects, features and advantages of the invention will be more fully understood upon reading the following detailed description in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027]

FIG. 1 is a block diagram generally showing the configuration of an operation control information update system employing a processing apparatus according to a first embodiment of the invention;

FIG. 2 is a flowchart depicting the operation of the processing apparatus employed in the operation control information update system of FIG. 1;

FIG. 3 is a block diagram showing part of an operation control information update system employing a processing apparatus according to a second embodiment of the invention;

FIG. 4 is a flowchart depicting the operation of the processing apparatus employed in the operation control information update system of FIG. 3;

FIG. 5 is a block diagram showing part of an operation control information update system employing a processing apparatus according to a third embodiment of the invention:

FIG. 6 is a flowchart depicting the operation of the processing apparatus employed in the operation control information update system of FIG. 5;

FIG. 7 is a block diagram showing part of an operation control information update system employing a processing apparatus according to a fourth embodiment of the invention:

FIG. 8 is a flowchart depicting the operation of the processing apparatus employed in the operation control information update system of FIG. 7;

FIG. 9 is a block diagram showing part of an operation control information update system employing a processing apparatus according to a fifth embodiment of the invention: and

FIG. 10 is a flowchart depicting the operation of the processing apparatus employed in the operation control information update system of FIG. 9.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS OF THE INVENTION

[0028] FIG. 1 is a diagram generally showing the configuration of an operation control information update system 10 employing a processing apparatus according to a first embodiment of the invention. The operation control information update system 10 of this embodiment is constructed such that operation control information including a processing program and associated data can be transmitted from a system control center to the processing apparatus through a communication line and loaded into the processing apparatus, automatically updating existing operation control information when the processing apparatus is not operated, during nighttime hours, for example.

[0029] Specifically, the operation control information update system 10 comprises an operation control information transmitting apparatus 20, such as a personal computer. provided in the system control center and a photographic processing machine 30 which serves as a receiving station that is connected to the operation control information transmitting apparatus 20 by a communication line TL and provided in a photographic processing shop, for instance.

[0030] The operation control information transmitting apparatus 20 comprises a control unit 21, a display unit 22 including a cathode ray tube (hereinafter referred to as CRT) for instance, a keyboard 23 and a modem 24. The operation control information transmitting apparatus 20 thus constructed transmits an upgrade version of operation control information, which differs from the currently used operation control information, to the operation control information transmitting apparatus 20 for updating the operation control information previously stored in control information memories of a machine control block 32.

[0031] The control unit 21 includes a data reading device 211 for reading data stored on an external storage medium, such as a floppy disk, a data processor 212 which performs a specified signal processing operation on the data read out by the data reading device 211, a data storage 213 for storing data obtained through the signal processing operation performed by the data processor 212 or entered through the keyboard 23, and a controller 214 for controlling overall operation of the operation control information transmitting apparatus 20.

[0032] The display unit 22 displays the contents of data transmission condition settings and a message to be transmitted to the photographic processing machine 30 while the keyboard 23 permits entry of various data including the data transmission conditions and message to be transmitted to the photographic processing machine 30. The modem 24 converts data from digital form to analog form, and vice versa. More specifically, the modem 24 converts digital data stored in the controller 214 into analog data. and analog data transmitted from the photographic processing machine 30 into digital data.

[0033] The photographic processing machine 30 comprises an exposure processor and a development processor which are not illustrated. Photographic printing paper is exposed with images recorded on a film. for instance, in the exposure processor and the exposed photographic printing paper is developed in the development processor. The photographic processing machine 30 further comprises the aforementioned machine control block 32 and an information control block 34 and is connected to the operation control information transmitting apparatus 20 via an external modem 36.

[0034] The machine control block 32 controls operational processes of individual processing segments including the aforementioned exposure processor and the development processor. In this embodiment, the machine control block 32 includes a first controller 321a and a second controller 321b. The first and second controllers 321a, 321b each include a central processing unit (hereinafter referred to as CPU) 322 which performs a specified processing operation, an electrically erasable programmable read-only memory (hereinafter referred to as EEPROM) 323 which constitutes a control information memory for storing a specific processing program, and a random-access memory (hereinafter referred to as RAM) 324 for temporarily storing processing data. Each EEPROM 323 is a read-only memory of which contents can be electrically rewritten. As shown in FIG. 1, a display device 326 for displaying the contents of the operation control information and processing condition settings stored in the EEPROMs 323, an input device 327, such as a keyboard, and a power switch 381 used for turning on and off a power supply 38 which supplies electric power to the exposure processor and other processing segments are connected to the first controller 321a. The CPU 322 of the first controller 321a incorporates the function of a power-off signal transmitter 322a which transmits a power-off signal when the power switch 381 is turned off.

[0035] The information control block 34 once stores the operation control information transmitted from the operation control information transmitting apparatus 20 and transfers it to the machine control block 32. To perform this function, the information control block 34 includes a CPU 341 which performs a specified processing operation, an EEPROM 342 storing a specific processing program, and a RAM 343 which constitutes an information memory for temporarily storing the operation control information received from the operation control information transmitting apparatus 20.

[0036] A display device 344 for displaying messages concerning the operation control information stored in the RAM 343, such as changes from the previous version of the operation control information, are connected to the information control block 34. The CPU 341 incorporates several functional elements including a memory controller 341a which causes the RAM 343 to temporarily store the operation control information when it has been received from the operation control information transmitting apparatus 20, a power-off signal receiver 341b which receives the power-off signal fed from the power-off signal transmitter 322a, a power-off status discriminator 341c which judges whether the photographic processing machine 30 is in an operating or non-operating condition (that is. whether the power-off signal transmitted by the power-off signal transmitter 322a has been received), and an information updater 341d which transfers the operation control information written in the RAM 343 to the EEPROMs 323 of the machine control block 32 and updates the operation control information stored in the EEPROMs 323.

[0037] The memory controller 341a functions also as an information discriminator for sensing whether the operation control information has been written into the RAM 343, while the information updater 341d functions also as a data transfer controller for issuing a command to transfer the operation control information written in the RAM 343 to the EEPROMs 323 of the machine control block 32 as well as an immediate update discriminator for judging whether an immediate update request requiring immediate updating of the operation control information is present.

[0038] The EEPROM 342 is, like the EEPROMs 323 of the machine control block 32, a read-only memory of which contents can be electrically rewritten. The RAM 343 has a first storage area for temporarily storing the processing program to be written into the EEPROMs 323 of the machine control block 32, a second storage area for temporarily storing data to be written into the EEPROMs 323 of the machine control block 32, a third storage area for temporarily storing the processing program to be written into the EEPROM 342 of the information control block 34, and a fourth storage area for temporarily storing data.

[0039] The modem 36 converts data from digital form to analog form, and vice versa. More specifically, the modem 36 converts analog data transmitted from the operation control information transmitting apparatus 20 into digital data. and digital data to be transmitted to the operation control information transmitting apparatus 20 into analog data.

[0040] Operation of the operation control information update system 10 thus constructed is now described with reference to the flowchart of FIG. 2.

[0041] When the power switch 381 connected to the power supply 38 is turned off at the end of working hours, for instance, the power-off signal transmitter 322a transmits a power-off signal to the information control block 34. The power-off signal is received by the power-off signal receiver 341b of the information control block 34 and stored in the RAM 343 and. then. the photographic processing machine 30 is set to a ready-to-receive state waiting for any incoming data with a night-time timer working.

[0042] Referring to FIG. 2, it is judged whether any operation control information transmitted from the operation control information transmitting apparatus 20 in the system control center has been written into the RAM 343 of the information control block 34 (step S1). If it is judged that the operation control information has been written into the RAM 343 (Yes in step S1), a further judgment is made as to whether the photographic processing machine 30 is in a power-off state (step S3). This judgment is intended to ensure that the operation control information is updated only if the photographic processing machine 30 is in its non-operating condition, because normal processing operation of the photographic processing machine 30 will be disturbed if the operation control information already existing in the machine control block 32 is updated while the photographic processing machine 30 is being operated.

[0043] If it is judged that the photographic processing machine 30 is in the power-off state (Yes in step S3), it is further judged whether an immediate update request requiring immediate updating of the operation control information is present (step S5). If the judgment result is in the affirmative (Yes in step S5), the operation control information written in the RAM 343 is transferred to the individual EEPROMs 323 of the machine control block 32 immediately when transmission from the operation control information transmitting apparatus 20 has been completed (step S7).

[0044] The aforementioned immediate update request may be given in the form of a command transmitted from the operation control information transmitting apparatus 20 as part of the operation control information. Alternatively, the processing program stored in the EEPROM 342 of the information control block 34 may contain a routine to issue a similar command which causes the information updater 341d to transfer the operation control information immediately at the end of transmission from the operation control information transmitting apparatus 20 has been completed.

[0045] The expression "end of transmission" used above does not necessarily refer to the completion of transmitting the whole operation control information. It should be understood that the expression also implies a situation in which a certain amount of information that corresponds to the storage capacity of the RAM 343, or any predefined amount of information, has just been transmitted. In this latter case, when transmission of the predefined amount, or portion, of the operation control information has been completed, that portion of the operation control information is transferred to the EEPROMs 323 and, then, each successive portion of the operation control information is taken into the RAM 343 and transferred to the EEPROMs 323 until the whole operation control information is transferred to the EEPROMs 323.

[0046] It is possible to update the operation control information stored in the EEPROMs 323 of the machine control block 32 in an efficient manner in the operation control information update system 10 of the first embodiment described above since the current operation control information is updated by transmitting the upgrade version of the operation control information from the system control center to the photographic processing machine 30 as described above. When the operation control information previously stored in the EEPROMs 323 of the machine control block 32 has been updated in this way. operation of the photographic processing machine 30 is controlled in accordance with the upgrade version of the operation control information.

[0047] It would be recognized from the foregoing discussion that the above-described first embodiment permits automatic updating of the operation control information after the power switch 381 has been turned off. The embodiment may be varied such that the operation control information is updated only when it is necessary to do so. This will be achieved by providing an update enabling device including an enable switch which enables transfer of the upgrade version of the operation control information stored in the RAM 343 on the input device 327, for example. This arrangement would allow an operator of the photographic processing machine 30 to verify the contents of changes to the current operation control information by displaying the same on the display device 344 of the information control block 34 and press the enable switch only when it is considered necessary to update the operation control information.

[0048] The above-described first embodiment may be varied such that various data stored in the EEPROMs 323 and the RAMs 324 of the first and second controllers 321a, 321b of the machine control block 32 are transferred to and stored in the RAM 343 of the information control block 34 when the power switch 381 is turned off, for example. This varied form of the first embodiment makes it possible to restore the photographic processing machine 30 to its original condition in case information stored in photographic processing machine 30 is destroyed by an operational error. This variation may be applied to other embodiments of the invention which will be described later.

[0049] Although the operation control information is transmitted from the operation control information transmitting apparatus 20 to the photographic processing machine 30 through the communication line TL in the above-described first embodiment, the information may be transmitted through a radio communication link. In this varied form of the first embodiment, the operation control information transmitting apparatus 20 and the photographic processing machine 30 are provided with their respective radio communications terminals. This variation is applicable also to the other embodiments to be described later.

[0050] The aforementioned first embodiment may be varied such that the operation control information is compressed in the operation control information transmitting apparatus 20 before it is transmitted to the photographic processing machine 30. This will make it possible to decrease the storage capacity of the RAM 343 of the information control block 34 and the time required for transmitting the operation control information. This variation is applicable also to the other embodiments to be described later. When the operation control information is compressed in the operation control information transmitting apparatus 20, the photographic processing machine 30 should be provided with means for expanding the compressed operation control information once stored in the RAM 343 when the operation control information is transferred to the machine control block 32.

[0051] The aforementioned first embodiment may also be varied such that the processing program stored in the EEPROM 342 of the information control block 34 is also updated. While the machine control block 32 of the first embodiment includes the first controller 321a and the second controller 321b, it may becomes necessary to update the processing program stored in the EEPROM 342 if the number of controllers incorporated in the machine control block 32 increases. In such a case. it would be possible to update the processing program stored in the EEPROM 342 in a manner similar to the updating of the operation control information for the machine control block 32. This variation is applicable also to the other embodiments to be described later.

[0052] FIG. 3 is a block diagram showing part of an operation control information update system 50 employing a processing apparatus (photographic processing machine 30) according to a second embodiment of the invention, in which elements identical or equivalent to those included in the operation control information update system 10 of the first embodiment are designated by the same reference numerals and a detailed description of such elements is omitted.

[0053] What is characteristic of the operation control information update system 50 of the second embodiment is that the operation control information is updated by transferring its upgrade version which has been transmitted from the system control center and stored in a RAM 343 of an information control block 34 to a machine control block 32 when the photographic processing machine 30 is started from its non-operating condition by turning on a power switch 381 of a power supply 38.

[0054] In this operation control information update system 50, a CPU 322 of a first controller 321a incorporates, besides the function of the earlier-described power-off signal transmitter 322a, additional functional elements including a power-on signal transmitter 322b which transmits a power-on signal when the power switch 381 is turned on, and a transfer enable signal transmitter 322c which transmits a transfer enable signal for enabling transfer of the operation control information from the information control block 34 to the machine control block 32 when a particular key of an input device 327 is pressed.

[0055] On the other hand, a CPU 341 of the information control block 34 incorporates, besides the functions of the earlier-described memory controller 341a, power-off signal receiver 341b. power-off status discriminator 341c and information updater 341d. some additional functional elements including a power-on signal receiver 341f which receives the power-on signal fed from the power-off signal transmitter 322b, a power-on signal discriminator 341g which judges whether the power-on signal transmitted by the power-off signal transmitter 322b has been received, a transfer enable signal receiver 341h which receives the transfer enable signal fed from the transfer enable signal transmitter 322c, and a transfer enable discriminator 341i which judges whether the transfer enable signal has been received.

[0056] Operation of the operation control information update system 50 thus constructed is now described with reference to the flowchart of FIG. 4.

[0057] When the power switch 381 connected to the power supply 38 is turned off at the end of working hours, for instance, the photographic processing machine 30 is set to a ready-to-receive state waiting for any incoming data with a nighttime timer working in the same way as the first embodiment.

[0058] Referring to FIG. 4, it is judged whether any operation control information transmitted from the operation control information transmitting apparatus 20 in the system control center has been written into the RAM 343 of the information control block 34 (step S11). If it is judged that the operation control information has been written into the RAM 343 (Yes in step S11), a further judgment is made as to whether the photographic processing machine 30 is in a power-off state (step S13). This step is intended to ensure that the operation control information is not inadvertently updated while the photographic processing machine 30 is being operated.

[0059] If it is judged that the photographic processing machine 30 is in the power-off state (Yes in step S13), it is further judged whether the power switch 381 has been turned on (step S15). If it is judged that the power switch 381 has been turned on (Yes in step S15), a message concerning the operation control information written in the RAM 343, such as changes from the previous version of the operation control information, is displayed on a display device 344 (step S17).

[0060] Next, it is judged whether the transfer enable signal has been transmitted (step S19). The transfer enable signal is generated when the operator, who has decided to update the operation control information after verifying the message displayed on the display device 344, presses a specified key of the input device 327. If it is judged that transfer of the operation control information has been enabled (Yes in step S19), the operation control information written in the RAM 343 is transferred to individual EEPROMs 323 of the machine control block 32 (step S21).

[0061] It is possible to update the operation control information stored in the EEPROMs 323 of the machine control block 32 in an efficient manner in the operation control information update system 50 of the second embodiment described above since the existing operation control information is updated by transmitting the upgrade version of the operation control information from the system control center to the photographic processing machine 30 in a manner similar to the first embodiment. In this embodiment, the operator can choose not to update the operation control information if he. or she, thinks it is not necessary to do so. This is because the operator enables transfer of the new operation control information after verifying the contents of changes to the existing operation control information displayed on the display device 344.

[0062] Although the operation flow of the second embodiment described above includes the step of judging the photographic processing machine 30 is in its non-operating condition, this step is not necessarily required. Further, although the display device 344 is made operational after the power switch 381 has been turned on in this embodiment, it may be varied such that the display device 344 is powered on immediately when transmission the operation control information from the operation control information transmitting apparatus 20 has been completed, for example. These variations are applicable to the later-described embodiments as well.

[0063] FIG. 5 is a block diagram showing part of an operation control information update system 60 employing a processing apparatus (photographic processing machine 30) according to a third embodiment of the invention, in which elements identical or equivalent to those included in the operation control information update system 10 of the first embodiment are designated by the same reference numerals and a detailed description of such elements is omitted.

[0064] What is characteristic of the operation control information update system 60 of the second embodiment is that the operation control information is updated by transferring its upgrade version which has been stored in a RAM 343 of an information control block 34 to a machine control block 32 when the operator gives an instruction to start transfer of the information by pressing a particular key of an input device 327, for example.

[0065] In this operation control information update system 60. a CPU 322 of a first controller 321a incorporates, besides the functions of the earlier-described power-off signal transmitter 322a and transfer enable signal transmitter 322c, an additional function as a transfer command signal transmitter 322d which transmits a transfer command signal requesting a transfer of the operation control information from the information control block 34 to the machine control block 32 when a particular key of the input device 327 is pressed.

[0066] On the other hand. a CPU 341 of the information control block 34 incorporates, besides the functions of the earlier-described memory controller 341a. power-off signal receiver 341b. power-off status discriminator 341c. information updater 341d. transfer enable signal receiver 341h and transfer enable discriminator 341i, additional functions as a transfer command signal receiver 341j which receives the transfer command signal fed from the transfer command signal transmitter 322d and as a transfer command discriminator 341k which judges whether the transfer command signal has been received.

[0067] Operation of the operation control information update system 60 thus constructed is now described with reference to the flowchart of FIG. 6. When a power switch 381 connected to the power supply 38 is turned off at the end of working hours, for instance, the photographic processing machine 30 is set to a ready-to-receive state waiting for any incoming data with a night-time timer working in the same way as the first embodiment.

[0068] Referring to FIG. 6. it is judged whether any operation control information transmitted from the operation control information transmitting apparatus 20 in the system control center has been written into the RAM 343 of the information control block 34 (step S31). If it is judged that the operation control information has been written into the RAM 343 (Yes in step S31), a further judgment is made as to whether the photographic processing machine 30 is in a power-off state (step S33). This step is intended to ensure that the operation control information is not inadvertently updated while the photographic processing machine 30 is being operated.

[0069] If it is judged that the photographic processing machine 30 is in the power-off state (Yes in step S33), it is further judged whether a transfer command has been issued (step S35). The transfer command is generated when the operator presses a specified key of the input device 327. Alternatively, a transfer command may be entered by selecting "TRANSFER" on a menu displayed on a display device 326, for example. If it is judged that the transfer command has been issued (Yes in step S35), a message concerning the operation control information written in the RAM 343, such as changes from the previous version of the operation control information, is displayed on a display device 344 (step S37).

[0070] Next. it is judged whether the transfer enable signal has been transmitted (step S39). The transfer enable signal is generated when the operator, who has decided to update the operation control information after verifying the message displayed on the display device 344, presses a specified key of the input device 327. If it is judged that transfer of the operation control information has been enabled (Yes in step S39), the operation control information written in the RAM 343 is transferred to individual EEPROMs 323 of the machine control block 32 (step S41).

[0071] It is possible to update the operation control information stored in the EEPROMs 323 of the machine control block 32 in an efficient manner in the operation control information update system 60 of the third embodiment described above since the existing operation control information is updated by transmitting the upgrade version of the operation control information from the system control center to the photographic processing machine 30 in a manner similar to the first embodiment. Further, the operation control information can be updated whenever it is convenient, because the operation control information stored in the RAM 343 of the information control block 34 is transferred to the individual EEPROMs 323 when the operator give a transfer command by pressing a specified key of the input device 327. Moreover, the operator can choose not to update the operation control information if he. or she, thinks it is not necessary to do so. This is because the operator enables transfer of the new operation control information after verifying the contents of changes to the existing operation control information displayed on the display device 344.

[0072] FIG. 7 is a block diagram showing part of an operation control information update system 70 employing a processing apparatus (photographic processing machine 30) according to a fourth embodiment of the invention, in which elements identical or equivalent to those included in the operation control information update system 10 of the first embodiment are designated by the same reference numerals and a detailed description of such elements is omitted.

[0073] What is characteristic of the operation control information update system 70 of the fourth embodiment is that the operation control information is updated by transferring its upgrade version which has been stored in a RAM 343 of an information control block 34 to a machine control block 32 when the operation control information stored in the RAM 343 is copied onto an external storage medium, such as a floppy disk. The photographic processing machine 30 of this operation control information update system 70 is so constructed that an external storage medium like a floppy disk can be loaded into a first controller 321a of the machine control block 32 and a writing device 328 for recording information on the external storage medium is connected to the first controller 321a. A CPU 322 of the first controller 321a incorporates, besides the function of the earlier-described transfer enable signal transmitter 322c, an additional function as a storage medium mount signal transmitter 322e which transmits a storage medium mount signal requesting a transfer of the operation control information from the information control block 34 to the machine control block 32 when the external storage medium has been loaded into the writing device 328.

[0074] On the other hand, a CPU 341 of the information control block 34 incorporates, besides the functions of the earlier-described memory controller 341a. information updater 341d. transfer enable signal receiver 341h and transfer enable discriminator 341i. additional functions as a storage medium mount signal receiver 341m which receives the storage medium mount signal fed from the storage medium mount signal transmitter 322e and as a storage medium sensor 341n which judges whether the storage medium mount signal has been received.

[0075] Operation of the operation control information update system 70 thus constructed is now described with reference to the flowchart of FIG. 8.

[0076] First, it is judged whether any operation control information transmitted from the operation control information transmitting apparatus 20 in the system control center has been written into the RAM 343 of the information control block 34 (step S51). If it is judged that the operation control information has been written into the RAM 343 (Yes in step S51), a further judgment is made as to whether an external storage medium has been loaded into the writing device 328 (step S53). If it is judged that the external storage medium has been loaded into the writing device 328 (Yes in step S53), a message concerning the operation control information written in the RAM 343, such as changes from the previous version of the operation control information, is displayed on a display device 344 (step S55).

[0077] Next, it is judged whether the transfer enable signal has been transmitted (step S57). The transfer enable signal is generated when the operator, who has decided to update the operation control information after verifying the message displayed on the display device 344, presses a specified key of an input device 327. If it is judged that transfer of the operation control information has been enabled (Yes in step S57), the operation control information written in the RAM 343 is transferred to individual EEPROMs 323 of the machine control block 32 (step S59). In this embodiment, the updated operation control information in the EEPROMs 323 is copied onto the external storage medium after the operation control information in the individual EEPROMs 323 has been updated. As an alternative, the operation control information may be copied onto the external storage medium at the same time as the operation control information is transferred to the EEPROMs 323. The external storage medium on which the updated operation control information has been written is used for updating the operation control information stored in the machine control block 32 of other photographic processing machines, for instance.

[0078] It is possible to update the operation control information stored in the EEPROMs 323 of the machine control block 32 in an efficient manner in the operation control information update system 70 of the fourth embodiment described above since the existing operation control information is updated by transmitting the upgrade version of the operation control information from the system control center to the photographic processing machine 30 in a manner similar to the first embodiment. Further, the operation control information can be updated whenever it is convenient, because the operation control information stored in the RAM 343 of the information control block 34 is transferred to the individual EEPROMs 323 when the operation control information is copied onto the external storage medium. Moreover, the operator can choose not to update the operation control information if he, or she, thinks it is not necessary to do so. This is because the operator enables transfer of the new operation control information after verifying the contents of changes to the existing operation control information displayed on the display device 344.

[0079] Although the writing device 328 is connected to the first controller 321a in the fourth embodiment described above, it may be connected to the information control block 34.

[0080] FIG. 9 is a block diagram showing part of an operation control information update system 80 employing a processing apparatus (photographic processing machine 30) according to a fifth embodiment of the invention, in which elements identical or equivalent to those included in the operation control information update system 10 of the first embodiment are designated by the same reference numerals and a detailed description of such elements is omitted.

[0081] What is characteristic of the operation control information update system 80 of the fifth embodiment is that the operation control information is loaded into individual EEPROMs 323 by transferring the same which has been stored in a RAM 343 of an information control block 34 to a machine control block 32 in cases where one or both of the EEPROMs 323 have been replaced, for instance, and the EEPROMs 323 do not store the correct operation control information, or any operation control information at all, necessary for controlling the photographic processing machine 30.

[0082] In this operation control information update system 80 a CPU 322 of a first controller 321a incorporates, besides the function of the earlier-described transfer enable signal transmitter 322c, additional functional elements including an information verifier 322f which ascertains whether or not the appropriate operation control information is stored in the EEPROMs 323 of the machine control block 32, and an information request signal transmitter 322g which transmits an information request signal requesting the operation control information when it is not stored in the EEPROMs 323.

[0083] On the other hand, a CPU 341 of the information control block 34 incorporates, besides the functions of the earlier-described memory controller 341a, information updater 341d, transfer enable signal receiver 341h and transfer enable discriminator 341i, additional functions as an information request signal receiver 341p which receives the information request signal fed from the information request signal transmitter 322g and as an information request signal discriminator 341q which judges whether the information request signal has been received.

[0084] Operation of the operation control information update system 80 thus constructed is now described with reference to the flowchart of FIG. 10.

[0085] First, it is judged whether any operation control information transmitted from the operation control information transmitting apparatus 20 in the system control center has been written into the RAM 343 of the information control block 34 (step S71). If it is judged that the operation control information has been written into the RAM 343 (Yes in step S71), a further judgment is made as to whether the operation control information is absent or destroyed in the EEPROMs 323 of the machine control block 32 (step S73). If it is judged that the operation control information is absent or destroyed in the EEPROMs 323 (Yes in step S73), a message concerning the operation control information written in the RAM 343, such as changes from the previous version of the operation control information, is displayed on a display device 344 (step S75).

[0086] Next, it is judged whether the transfer enable signal has been transmitted (step S77). The transfer enable signal is generated when the operator, who has decided to load or update the operation control information after verifying the message displayed on the display device 344, presses a specified key of an input device 327. If it is judged that transfer of the operation control information has been enabled (Yes in step S77), the operation control information written in the RAM 343 is transferred to the individual EEPROMs 323 of the machine control block 32 (step S79).

[0087] It is possible to update the operation control information in the EEPROMs 323 of the machine control block 32 in an efficient manner in the operation control information update system 80 of the fifth embodiment described above since the operation control information is updated by transmitting it from the system control center to the photographic processing machine 30 in a manner similar to the first embodiment. Furthermore, the operator can choose not to update the operation control information if he, or she, thinks it is not necessary to do so. This is because the operator enables transfer of the new operation control information after verifying the contents of changes to the existing operation control information displayed on the display device 344.

[0088] Although the processing apparatus is the photographic processing machine 30 in the foregoing embodiments, the invention is applicable to any processing apparatus if it is of a type performs a specified operation in accordance with the operation control information stored in the EEPROMs 323 of the machine control block 32. The processing apparatus of any of the foregoing embodiments may be modified such that the processing apparatus further comprises means for mode selection and has the capability to perform all the functions included in the first to fifth embodiments. thereby allowing the operator to select a desired function on a menu presented on the display device 326.

[0089] Although various signals are transmitted from the machine control block 32 and received by the information control block 34 in any of the foregoing embodiments, it is possible to modify their system construction in such a manner that flags are set in the machine control block 32 and the machine control block 32 reads such flags.

[0090] Although updating of the operation control information is permitted when the power supply 38 has been turned on, when the operator has given a transfer command, and when an external storage medium has been loaded into the writing device 328 in the second to fourth embodiments described above, respectively, these embodiments may be modified to permit the updating when some other operation has been accomplished.

[0091] Although the present invention has been fully described by way of example with reference to the accompanying drawings, it is to be understood that various changes and modifications will be apparent to those skilled in the art. Therefore, unless otherwise such changes and modifications depart from the scope of the present invention defined in the claims they should be considered as being included therein.

Claims

1. A processing apparatus (30) comprising:

   an apparatus controller (32) including a control information memory (323) for storing operation control information, enabling the processing apparatus (30) to perform a specified operation; and
   an information controller (34) including:

      an update information memory (343) for holding operation control information transmitted from a control center (20) and an information updater (341) or updating the operation control information currently stored in the control information memory (323) by transferring the operation control information held in the update information memory (343) to the control information memory (323), **characterized in that**

   the information controller (34) is adapted to detect whether the apparatus controller (32) is in a power-off state or not (S3, S13, S33) and, after having received the operation control information, adapted to control the transmission of the operation control information to the apparatus controller (32) while the apparatus controller is in the power-off state.

2. The processing apparatus according to claim 1, **characterized in that** the information updater (341) transfers the operation control information held in the update information memory (343) to the control information memory (323) on condition that transmission of the operation control information from the control center (20) has been completed.

3. The processing apparatus according to claim 1, **characterized in that** the information updater (341) transfers the operation control information held in the update information memory (343) to the control information memory (323) on condition that a prerequisite for information updating have been satisfied.

4. The processing apparatus according to claim 3, further comprising a power supply for providing electric power to the processing apparatus (30) and the prerequisite for information updating is that the power supply has been activated.

5. The processing apparatus according to claim 3, **characterized in that** the prerequisite for information updating is a presence of a transfer command given by an operator.

6. The processing apparatus according to claim 3, further comprising a writing device for writing operation control information on an external storage medium loaded in the processing apparatus (30) and the prerequisite for information updating is that the writing device has become ready to write on the external storage medium.

7. The processing apparatus according to claim 3, **characterized in that** the prerequisite for information updating is that the operation control information is not stored in the control information memory (323).

8. The processing apparatus according to one of claims 1 through 7, further comprising a display unit (22) for displaying information on the operation control information held in the update information memory (343).

9. The processing apparatus according to claim 8, further comprising an update enabling device for enabling transfer of the operation control information held in the update information memory (343) and displayed on the display unit (22) to the control information memory (323).

10. An operation control information update system comprising an operation control information transmitting apparatus for transmitting an operation control information and a processing apparatus according to one of claims 1 through 9 for receiving the operation control information.

11. The processing apparatus (30) according to claim 1, **characterized in that** the apparatus controller (32) is adapted to transmit a power-off signal to the information controller (34) and to be set to a ready-to-receive state, and the power off signal is stored in the information controller.

Patentansprüche

1. Verarbeitungsanordnung bzw. -gerät (30), umfassend:

    eine Geräte- bzw. Anordnungssteuerung bzw. -regelung (32), beinhaltend einen Steuer- bzw. Regelinformationsspeicher (323), um Betriebssteuer- bzw. - regelinformation zu speichern, die es der Verarbeitungsanordnung (30) ermöglicht, eine bestimmte Tätigkeit auszuführen; und
    eine Informations-Steuer- bzw. -Regeleinrichtung (34), beinhaltend:
    einen Aktualisierungsinformationsspeicher (343), um Betriebssteuer - bzw. - regelinformation zu halten, die von einem Steuer- bzw. Regelzentrum (20) übertragen ist, und
    eine Informationsaktualisierungseinrichtung (341), um die Betriebssteuer - bzw. - regelinformation zu aktualisieren, die gegenwärtig in dem Steuer- bzw. Regelinformationsspeicher (323) gespeichert ist, indem die Betriebssteuer- bzw. -regelinformation, die in dem Aktualisierungsinformationsspeicher (343) gehalten ist, auf den Steuer- bzw. Regelinformationsspeicher (323) übertragen wird, **dadurch gekennzeichnet, daß**
    die Informations-Steuer- bzw. -Regeleinheit (34) adaptiert ist, um zu detektieren, ob die Anordnungssteuer- bzw. -regeleinheit (32) in einem Leistung-Aus-Zustand ist oder nicht (S3, S13, S33), und nachdem sie die Betriebssteuer- bzw -regelinformation erhalten hat, adaptiert ist, um die Übertragung der Betriebssteuer- bzw. -regelinformation zu der Anordnungssteuer- bzw. -regeleinrichtung (32) zu steuern bzw. zu regeln. während die Anordnungssteuer- bzw. -regeleinrichtung in dem Leistung-Aus-Zustand ist.

2. Verarbeitungsanordnung nach Anspruch 1, **dadurch gekennzeichnet, daß** die Informationsaktualisierungseinrichtung (341) die Betriebssteuer- bzw. - regelinformation, die in dem Aktualisierungsinformationsspeicher (343) gehalten ist, zu dem Steuer- bzw. Regelinformationsspeicher (323) unter der Bedingung überträgt, daß eine Übertragung der Betriebssteuer- bzw. -regelinformation von dem Steuer- bzw. Regelzentrum (20) vervollständigt wurde.

3. Verarbeitungsanordnung nach Anspruch 1, **dadurch gekennzeichnet, daß** die Informationsaktualisierungseinrichtung (341) die Betriebssteuer- bzw. - regelinformation, die in dem Aktualisierungsinformationsspeicher (343) gehalten ist, zu dem Steuer- bzw. Regelinformationsspeicher (323) unter der Bedingung überträgt, daß ein Vorerfordernis für ein Aktualisieren von Information erfüllt wurde.

4. Verarbeitungsanordnung nach Anspruch 3, weiterhin umfassend eine Leistungszufuhr für ein Bereitstellen von elektrischer Leistung zu der Verarbeitungsanordnung (30), und wobei das Vorerfordemis für eine Informationsaktualisierung ist, daß die Leistungszufuhr aktiviert wurde.

5. Verarbeitungsanordnung nach Anspruch 3, **dadurch gekennzeichnet, daß** das Vorerfordemis für eine Informationsaktualisierung eine Anwesenheit eines Übertragungsbefehls ist, der durch einen Betätiger gegeben ist.

6. Verarbeitungsanordnung nach Anspruch 3, weiterhin umfassend eine Schreibvorrichtung zum Schreiben von Betriebssteuer- bzw. -regelinformation auf einem externen Speichermedium, das in die Verarbeitungsvorrichtung (30) geladen ist, und wobei das Vorerfordernis für eine Informationsaktualisierung ist, daß die Schreibvorrichtung für ein Schreiben auf dem externen Speichermedium bereit ist.

7. Verarbeitungsanordnung nach Anspruch 3, **dadurch gekennzeichnet, daß** das Vorerfordernis für eine Informationsaktualisierung ist, daß die Betriebssteuer- bzw. -regelinformation nicht in dem Steuer- bzw. Regelinformationsspeicher (323) gespeichert ist.

8. Verarbeitungsanordnung nach einem der Ansprüche 1 bis 7, weiterhin umfassend eine Anzeigeeinheit (22) zum Anzeigen von Information auf der Betriebssteuer- bzw. -regelinformation, die in dem Aktualisierungsinformationsspeicher (343) gehalten ist.

9. Verarbeitungsanordnung nach Anspruch 8, weiterhin umfassend eine Aktualisierungsedaubnisvorrichtung zum Erlauben eines Transfers der Betriebssteuer- bzw. -regelinformation, die in dem Aktualisierungsinformationsspeicher (343) gehalten ist und auf der Anzeigeeinheit (22) angezeigt ist, zu dem Steuer- bzw. Regelinformationsspeicher (323).

10. Betriebssteuer- bzw. -regelinformations-Aktualisierungssystem, umfassend eine Betriebssteuer- bzw. -regelinformationsübertragungsanordnung zum Übertragen einer Betätigungssteuer- bzw. -regelinformation und eine Verarbeitungsanordnung nach einem der Ansprüche 1 bis 9, um die Betriebssteuer- bzw. -regelinformation zu erhalten.

11. Verarbeitungsanordnung (30) nach Anspruch 1, **da-**

durch gekennzeichnet, daß die Gerätesteuer- bzw. -regeleinrichtung (32) adaptiert ist, um ein Leistung-Aus-Signal zu der Informationssteuer- bzw. -regeleinrichtung (34) zu übertragen und auf einen empfangsbereiten Zustand gesetzt bzw. eingestellt zu sein, und daß das Leistung-Aus-Signal in der Informationssteuer- bzw. -regeleinrichtung gespeichert ist.

Revendications

1. Un dispositif de traitement (30) comprenant :

   un contrôleur du dispositif (32) comprenant une mémoire de données de commande (323) pour stocker des données de commande de fonctionnement, permettant au dispositif de traitement (30) d'effectuer une opération spécifiée ; et
   un contrôleur de données (34) comprenant :

   une mémoire de données de mise à jour (343) pour contenir des données de commande de fonctionnement transmises depuis un centre de commande (20), et
   un système de mise à jour de données (341) pour la mise à jour des données de commande de fonctionnement stockées à cet instant dans la mémoire de données de commande (323) en transférant les données de commande de fonctionnement contenues dans la mémoire de données de mise à jour (343) vers la mémoire de données de commande (323), **caractérisé en ce que**
   le contrôleur de données (34) est adapté pour détecter si le contrôleur du dispositif (32) est ou non en état hors tension (S3, S13, S33), et est adapté, après réception des données de commande de fonctionnement, pour commander la transmission des données de commande de fonctionnement au contrôleur du dispositif (32) pendant que le contrôleur du dispositif est dans l'état hors tension.

2. Le dispositif de traitement selon la revendication 1, **caractérisé en ce que** le système de mise à jour de données (341) transfère les données de commande de fonctionnement contenues dans la mémoire de données de mise à jour (343) vers la mémoire de données de commande (323), à condition que soit terminée la transmission des données de commande de fonctionnement depuis le centre de commande (20).

3. Le dispositif de traitement selon la revendication 1, **caractérisé en ce que** le système de mise à jour de données (341) transfère les données de commande de fonctionnement contenues dans la mémoire de données de mise à jour (343) vers la mémoire de données de commande (323), à condition qu'un pré-requis pour la mise à jour des données ait été satisfait.

4. Le dispositif de traitement selon la revendication 3, comprenant en outre une alimentation électrique pour fournir de l'énergie électrique au dispositif de traitement (30), et le pré-requis pour la mise à jour des données est que l'alimentation électrique ait été activée.

5. Le dispositif de traitement selon la revendication 3, **caractérisé en ce que** le pré-requis pour la mise à jour des données est l'existence d'un ordre de transfert donné par un opérateur.

6. Le dispositif de traitement selon la revendication 3, comprenant en outre un périphérique d'écriture pour écrire des données de commande de fonctionnement sur un support de stockage externe chargé dans le dispositif de traitement (30), et le pré-requis pour la mise à jour des données est que le périphérique d'écriture soit devenu prêt à écrire sur le support de stockage externe.

7. Le dispositif de traitement selon la revendication 3, **caractérisé en ce que** le pré-requis pour la mise à jour des données est que les données de commande de fonctionnement ne soient pas stockées dans la mémoire de données de commande (323).

8. Le dispositif de traitement selon l'une des revendications 1 à 7, comprenant en outre un écran de visualisation (22) pour afficher les informations sur les données de commande de fonctionnement contenues dans la mémoire de données de mise à jour (343).

9. Le dispositif de traitement selon la revendication 8, comprenant en outre un périphérique d'activation des mises à jour pour activer le transfert, vers la mémoire de données de commande (323), des données de commande de fonctionnement contenues dans la mémoire de données de mise à jour (343) et affichées sur l'écran de visualisation (22).

10. Un système de mise à jour de données de commande de fonctionnement comprenant un dispositif de transmission des données de commande de fonctionnement pour transmettre une donnée de commande de fonctionnement, et un dispositif de traitement selon l'une quelconque des revendications 1 à 9 pour recevoir les données de commande de fonctionnement.

11. Le dispositif de traitement (30) selon la revendication 1, **caractérisé en ce que** le contrôleur du dispositif (32) est adapté pour transmettre un signal de mise hors tension au contrôleur de données (34) et pour être placé dans un état « prêt à recevoir », le signal de mise hors tension étant stocké dans le contrôleur de données.

FIG.1

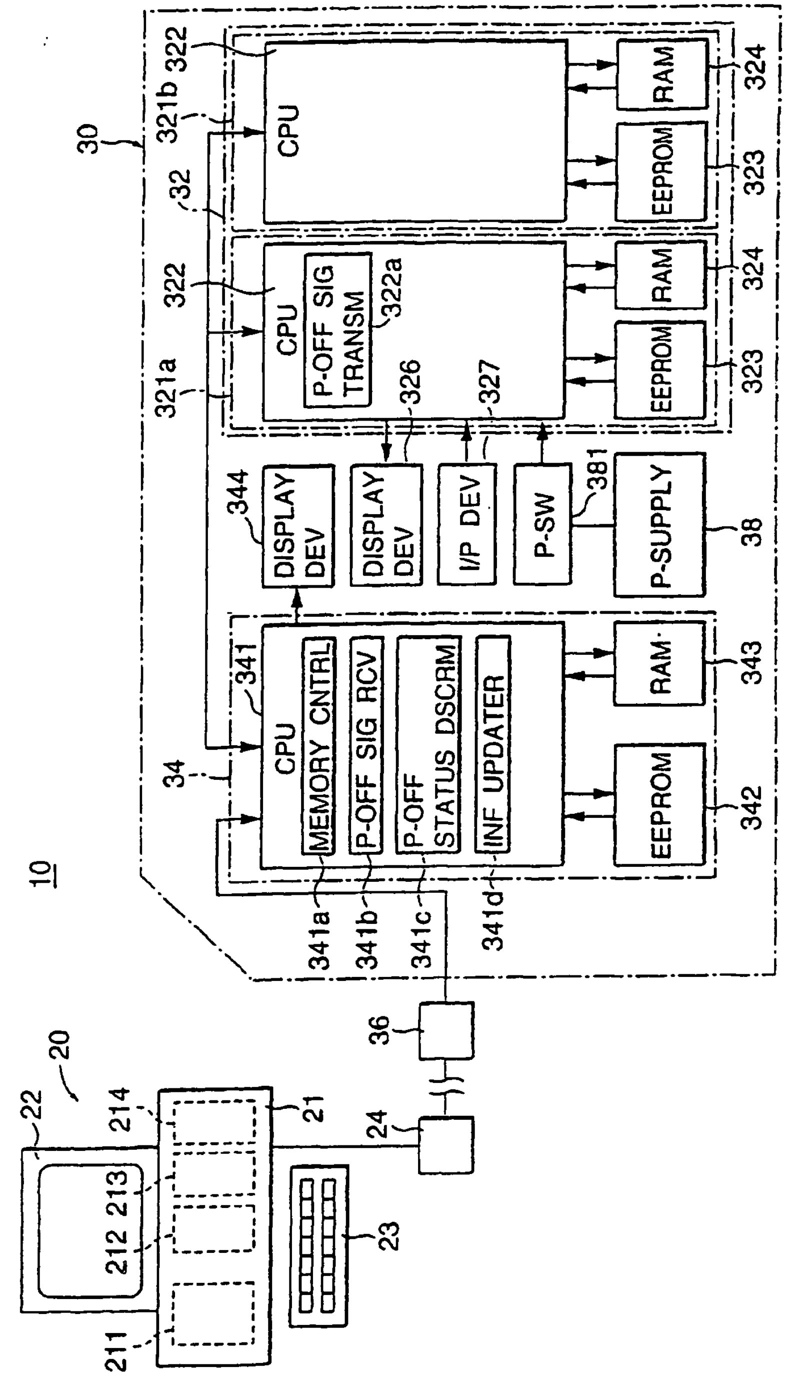

10
30
32
321a
321b
322
CPU
P-OFF SIG TRANSM
322a
326
327
EEPROM
RAM
323
324
CPU
EEPROM
RAM
323
324
344
DISPLAY DEV
DISPLAY DEV
I/P DEV
P-SW
381
P-SUPPLY
38
34
341
CPU
MEMORY CNTRL
P-OFF SIG RCV
P-OFF STATUS DSCRM
INF UPDATER
RAM
343
EEPROM
342
341a
341b
341c
341d
36
24
20
21
22
211
212
213
214
23

FIG.2

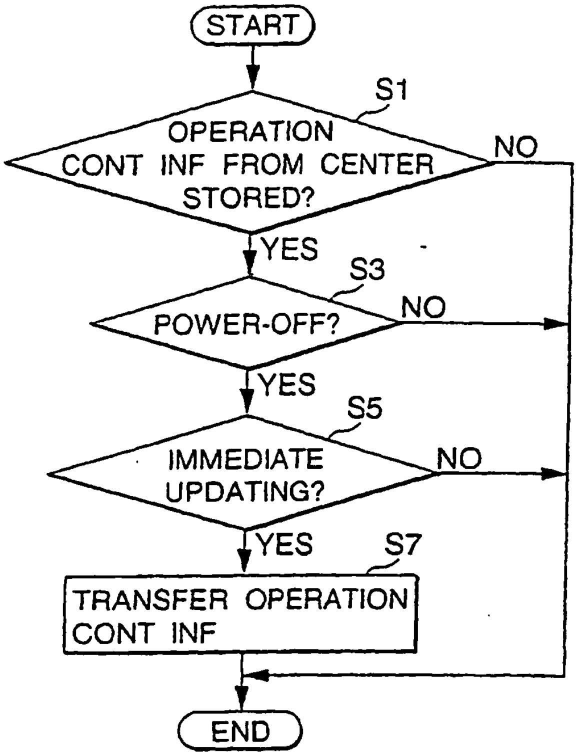

START
S1
OPERATION CONT INF FROM CENTER STORED?
NO
YES
S3
POWER-OFF?
NO
YES
S5
IMMEDIATE UPDATING?
NO
YES
S7
TRANSFER OPERATION CONT INF
END

FIG.3

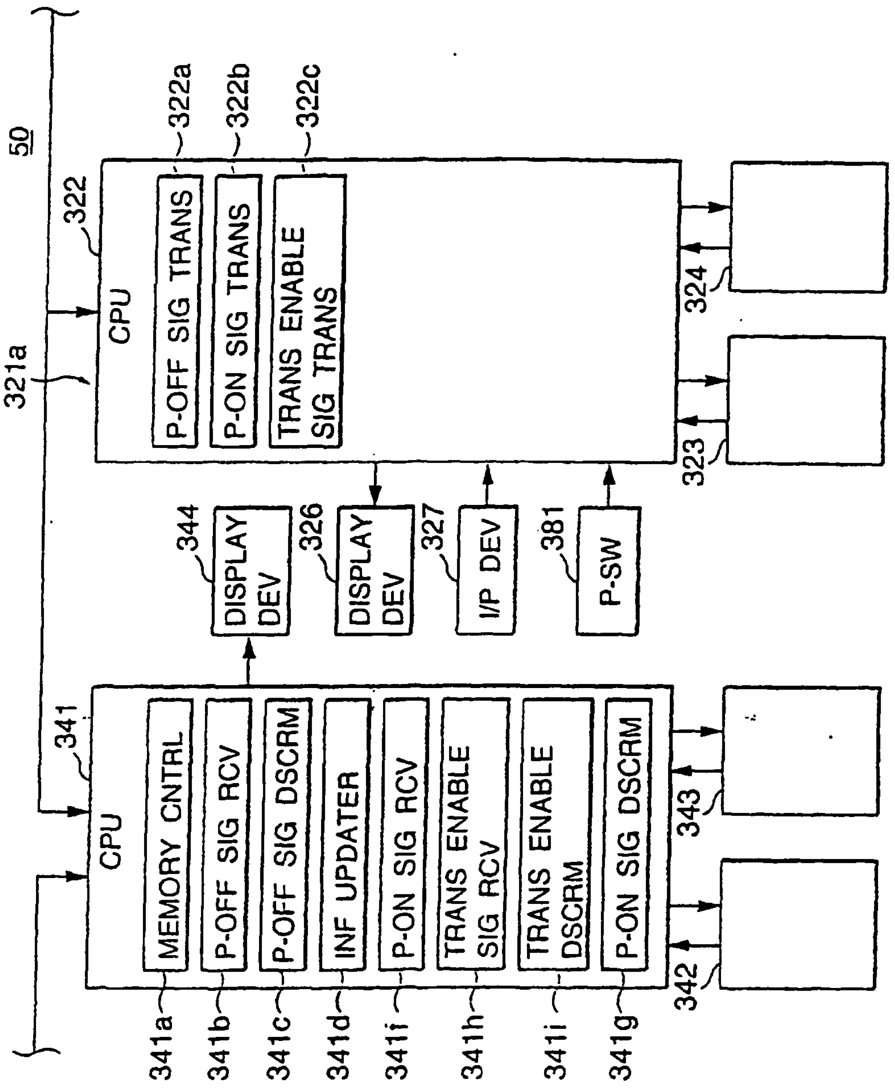

50
321a
322
CPU
P-OFF SIG TRANS
P-ON SIG TRANS
TRANS ENABLE SIG TRANS
322a
322b
322c
323
324
344
DISPLAY DEV
326
DISPLAY DEV
327
I/P DEV
381
P-SW
341
CPU
MEMORY CNTRL
P-OFF SIG RCV
P-OFF SIG DSCRM
INF UPDATER
P-ON SIG RCV
TRANS ENABLE SIG RCV
TRANS ENABLE DSCRM
P-ON SIG DSCRM
341a
341b
341c
341d
341f
341h
341i
341g
342
343

FIG.4

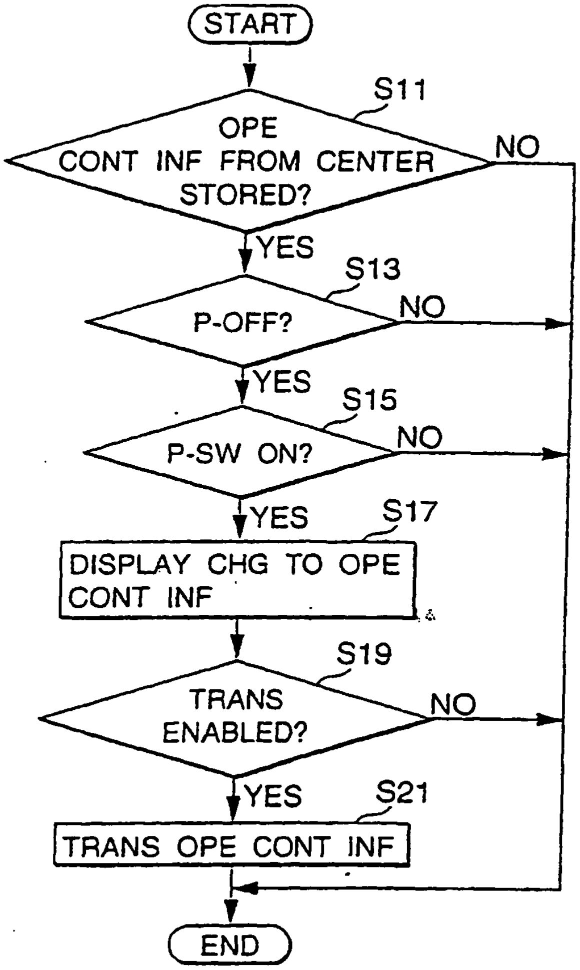

START
S11
OPE CONT INF FROM CENTER STORED?
NO
YES
S13
P-OFF?
NO
YES
S15
P-SW ON?
NO
YES
S17
DISPLAY CHG TO OPE CONT INF
S19
TRANS ENABLED?
NO
YES
S21
TRANS OPE CONT INF
END

FIG.5

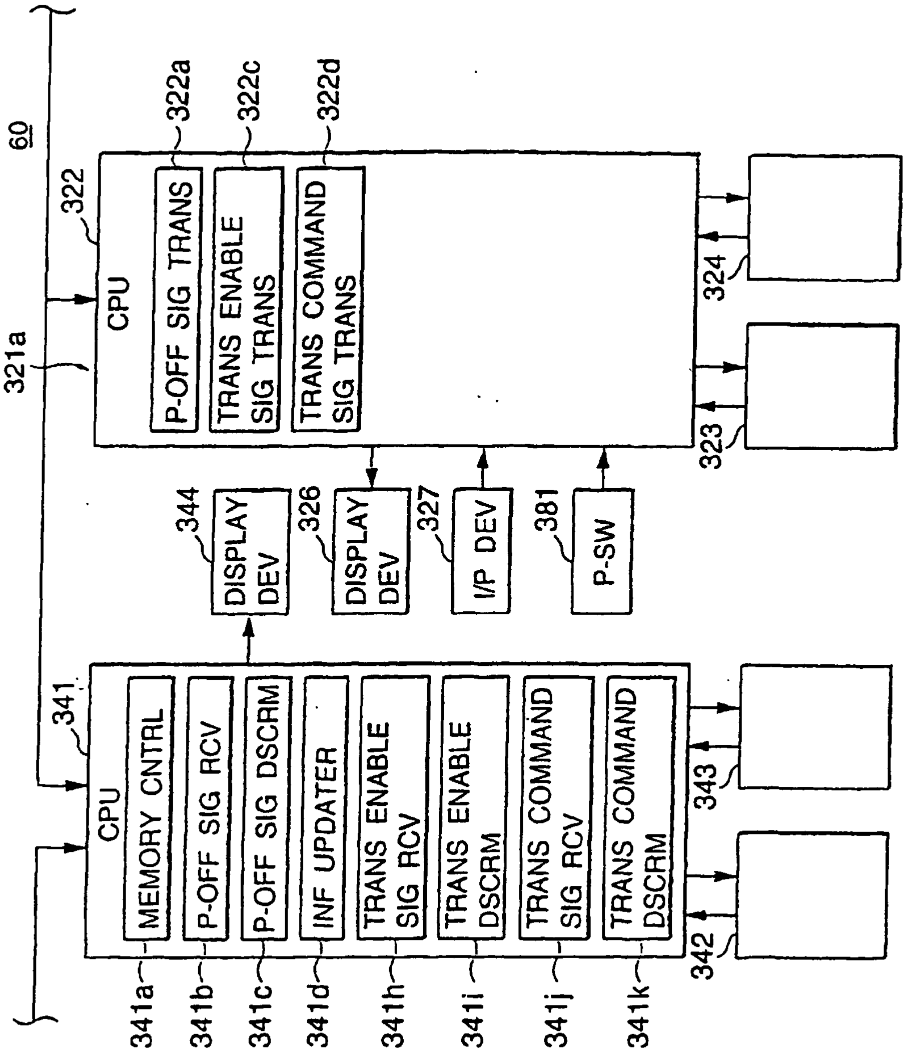

60
321a
322
CPU
P-OFF SIG TRANS
TRANS ENABLE SIG TRANS
TRANS COMMAND SIG TRANS
322a
322c
322d
323
324
344
DISPLAY DEV
326
DISPLAY DEV
327
I/P DEV
381
P-SW
341
CPU
MEMORY CNTRL
P-OFF SIG RCV
P-OFF SIG DSCRM
INF UPDATER
TRANS ENABLE SIG RCV
TRANS ENABLE DSCRM
TRANS COMMAND SIG RCV
TRANS COMMAND DSCRM
341a
341b
341c
341d
341h
341i
341j
341k
342
343

FIG.6

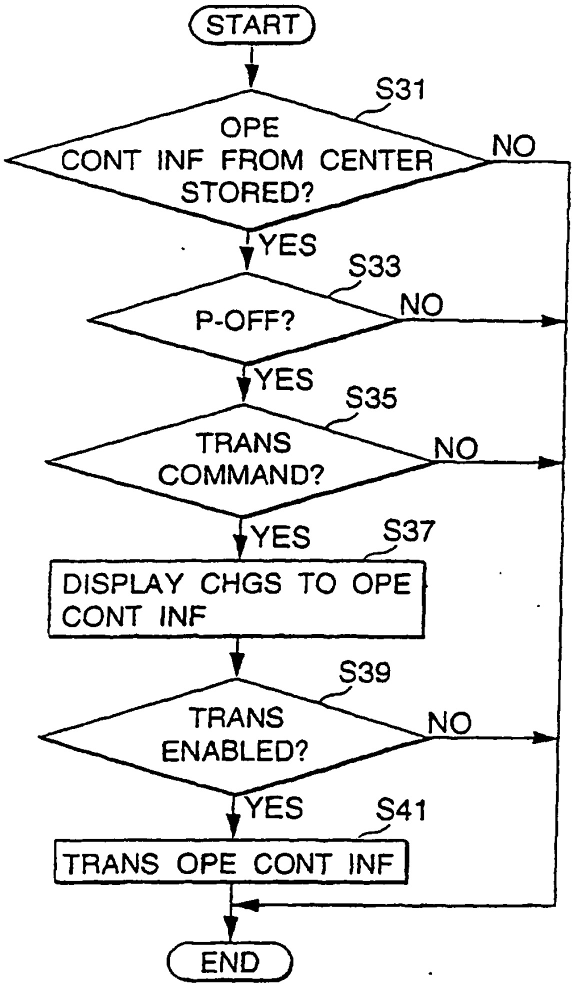

START
S31
OPE CONT INF FROM CENTER STORED?
NO
YES
S33
P-OFF?
NO
YES
S35
TRANS COMMAND?
NO
YES
S37
DISPLAY CHGS TO OPE CONT INF
S39
TRANS ENABLED?
NO
YES
S41
TRANS OPE CONT INF
END

FIG.7

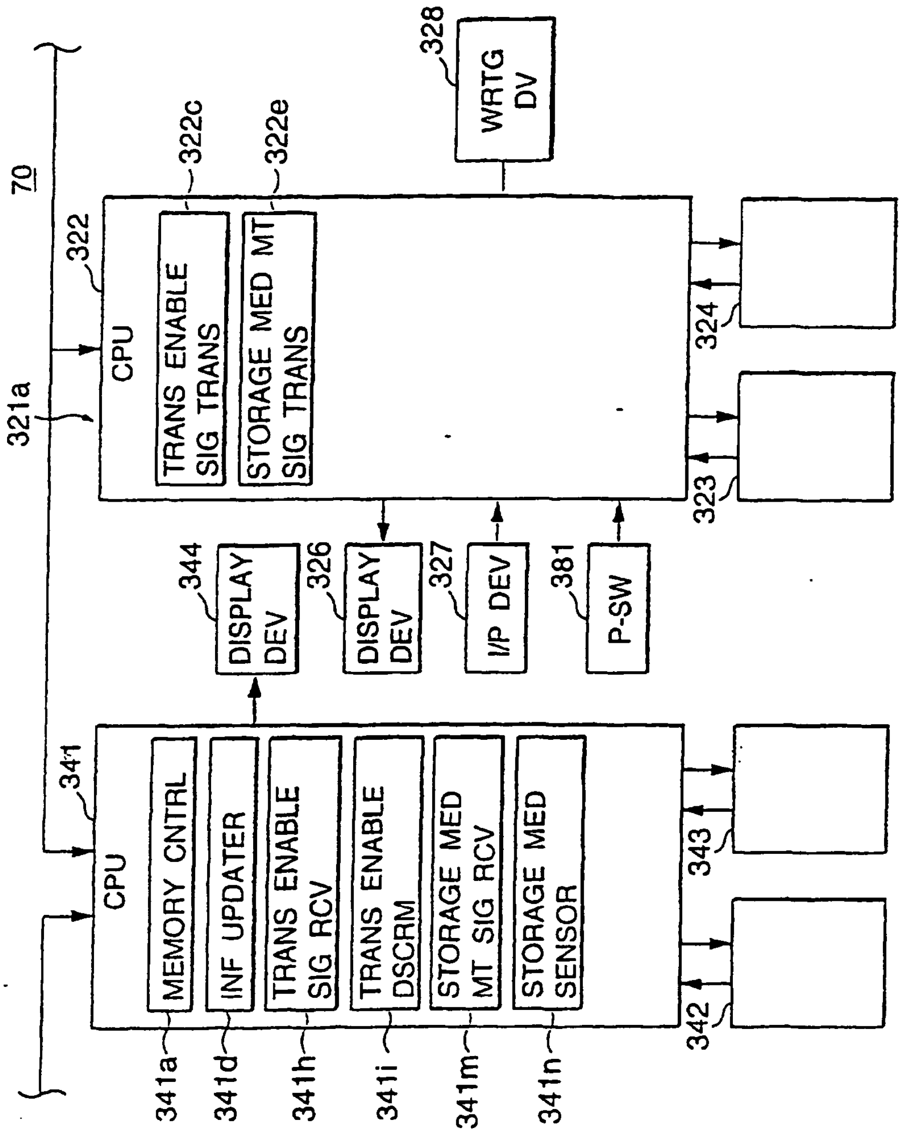

70
321a
322
CPU
TRANS ENABLE SIG TRANS
322c
STORAGE MED MT SIG TRANS
322e
WRTG DV
328
323
324
344
DISPLAY DEV
326
DISPLAY DEV
327
I/P DEV
381
P-SW
341
CPU
MEMORY CNTRL
INF UPDATER
TRANS ENABLE SIG RCV
TRANS ENABLE DSCRM
STORAGE MED MT SIG RCV
STORAGE MED SENSOR
341a
341d
341h
341i
341m
341n
342
343

FIG.8

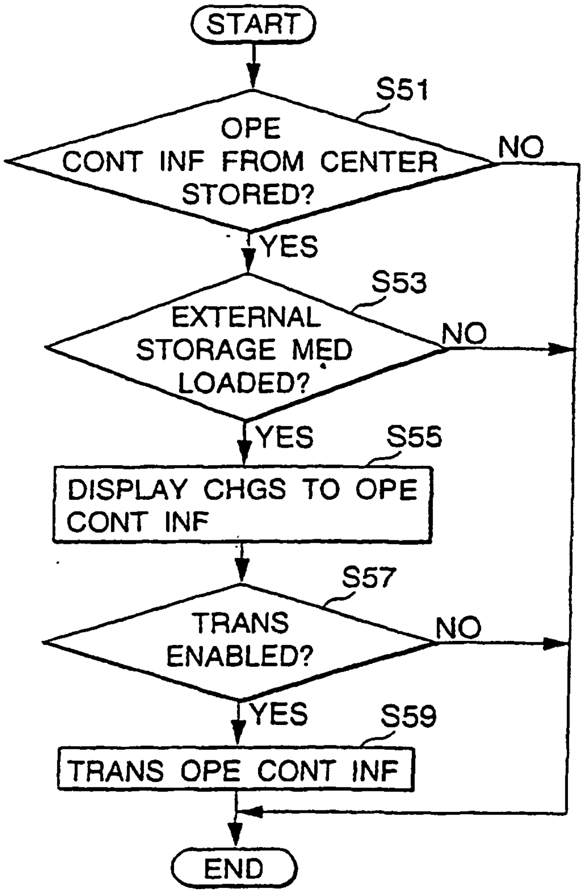

START
S51
OPE CONT INF FROM CENTER STORED?
NO
YES
S53
EXTERNAL STORAGE MED LOADED?
NO
YES
S55
DISPLAY CHGS TO OPE CONT INF
S57
TRANS ENABLED?
NO
YES
S59
TRANS OPE CONT INF
END

FIG.9

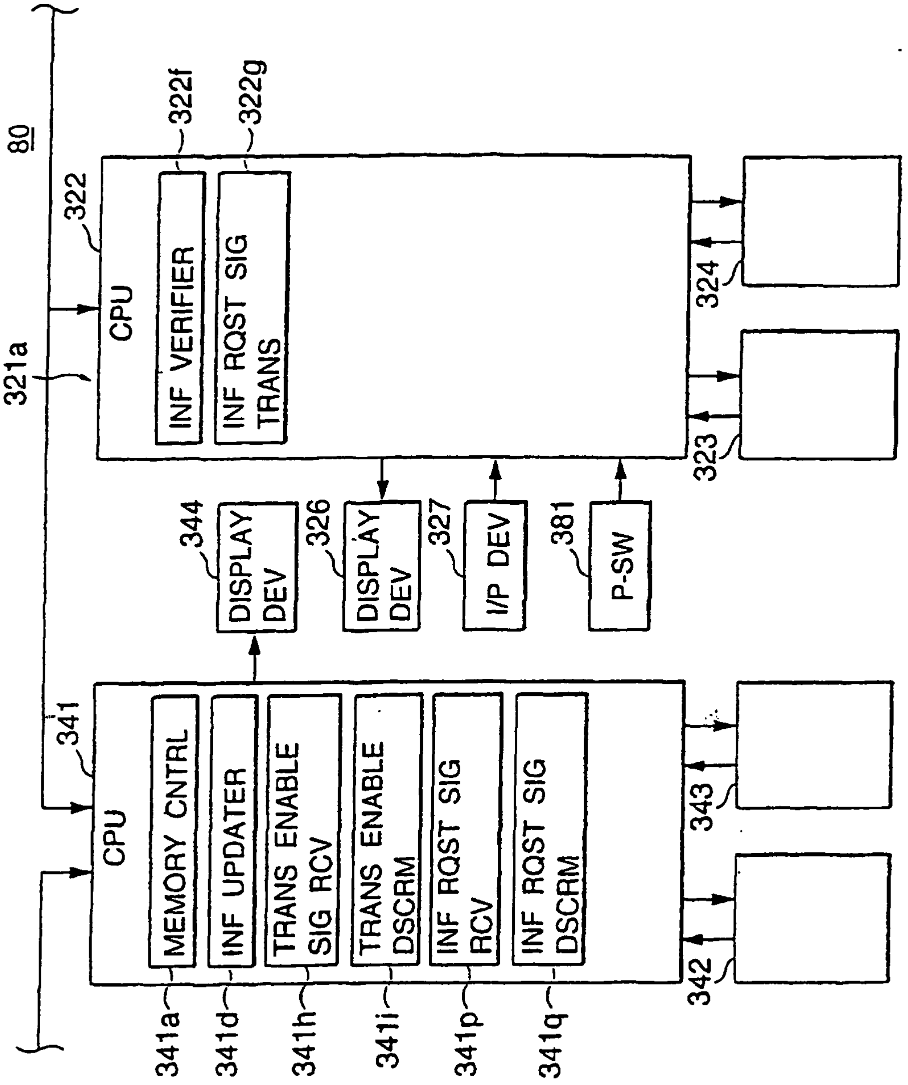
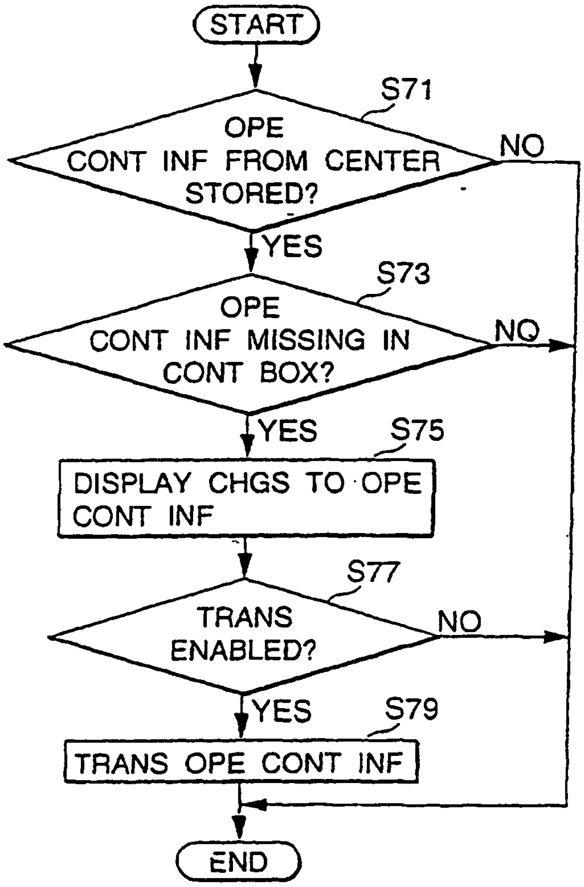

80
321a
322
CPU
INF VERIFIER
322f
INF RQST SIG TRANS
322g
323
324
344
DISPLAY DEV
326
DISPLAY DEV
327
I/P DEV
381
P-SW
341
CPU
MEMORY CNTRL
INF UPDATER
TRANS ENABLE SIG RCV
TRANS ENABLE DSCRM
INF RQST SIG RCV
INF RQST SIG DSCRM
341a
341d
341h
341i
341p
341q
342
343

FIG.10


START
S71
OPE
CONT INF FROM CENTER
STORED?
NO
YES
S73
OPE
CONT INF MISSING IN
CONT BOX?
NO
YES
S75
DISPLAY CHGS TO OPE
CONT INF
S77
TRANS
ENABLED?
NO
YES
S79
TRANS OPE CONT INF
END

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☑ BLACK BORDERS

☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

□ FADED TEXT OR DRAWING

□ BLURRED OR ILLEGIBLE TEXT OR DRAWING

□ SKEWED/SLANTED IMAGES

□ COLOR OR BLACK AND WHITE PHOTOGRAPHS

□ GRAY SCALE DOCUMENTS

☑ LINES OR MARKS ON ORIGINAL DOCUMENT

☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

□ OTHER: ______________________________

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2001 (22.03.2001)

PCT

(10) International Publication Number
WO 01/20424 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number: PCT/US00/15078

(22) International Filing Date: 1 June 2000 (01.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/137,352 3 June 1999 (03.06.1999) US

(71) Applicant: **ANCHOR GAMING** [US/US]; 2311 South 7th Avenue, Bozeman, MT 59715 (US).

(72) Inventors: **HARRIS, David**; 9690 Forest Creek Drive, Bozeman, MT 59718 (US). **KOURY, Mitchell, William**; 622 South 15th, Bozeman, MT 59715 (US). **MOODY, William, J.**; 601 MacGregor Road, Belgrade, MT 59714 (US). **BOLTON, Paul, W.**; 410 Morroco, Bozeman, MT 59715 (US). **AMICUCCI, Phillip, Louis**; P.O. Box 1147, Three Forks, MT 59752 (US). **WALL, Robert, Lyle**; 222 Westridge Drive, Bozeman, MT 59715 (US). **SWENSON, Charles, Glen**; 101 Churn Road, Bozeman, MT 59715 (US).

(74) Agents: **KIRCHER, William, B.** et al.; Shook, Hardy & Bacon L.L.P., One Kansas City Place, 1200 Main Street, Kansas City, MO 64105-2118 (US).

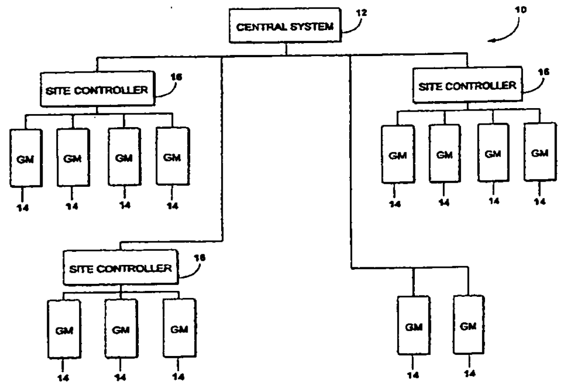
(81) Designated States *(national)*: AU, CA, PL.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND DEVICE FOR IMPLEMENTING A DOWNLOADABLE SOFTWARE DELIVERY SYSTEM



(57) Abstract: A method and device implementing a downloadable operatively connected to a plurality of gaming machines either by a direct communications link or through the use of one or more site controllers or PCs. Each gaming machine and site controller or PC contains two executable spaces, one of which typically contains the software image currently being implemented by the device. The other executable space is designated to receive from the central system a new software image that will be utilized by the device. The central system transfers a new image to be executed, via packet encrypted communications, to a networked device which stores the image in an executable space, while continuing to run the currently designated image. Upon instruction from the central system, the device switches over to the new image, allowing one or more machines to implement a software upgrade on a continuous basis.

WO 01/20424 A2

METHOD AND DEVICE FOR IMPLEMENTING A DOWNLOADABLE SOFTWARE DELIVERY SYSTEM

TECHNICAL FIELD

In general, this invention relates to a downloadable software system, and more particularly, to a method and device implementing a downloadable software system for an electronic gaming machine communications network.

BACKGROUND OF THE INVENTION

In general, conventional gaming machine networks typically include a central system operatively connected to one or more individual gaming machines via intermediate communication site controllers. Although the gaming machines communicate with the central system, each gaming machine or site controller contains a central chipset which locally stores the computer code to be is executed by the device to perform gaming related functions. These chipsets typically consist of electronic programmable read only memory (EPROM) which permanently store the computer code. EPROM chipsets are conventionally preferred because the electronic memory can be controlled in a secured manner without giving unauthorized access to the gaming machine code. For example, in the event the computer code needs to be upgraded, service personnel are required to manually change the chipset for each gaming machine and/or site controller.

Because a service technician must perform the same operation for each machine or controller, the current method of upgrading gaming machine/site controller or PC software typically takes a long time to accomplish at a substantial cost, including the cost of the technician time and the cost of a new chipset for each machine.

Accordingly, there is a need for a system which can upgrade computer code within a networked device without requiring a manual change in the device components or requiring a high cost of implementation.

SUMMARY OF THE INVENTION

Generally described, a gaming machine system is provided. The gaming machine system includes a central system and one or more gaming devices having at least one storage component operable to receive an executable software image and in communication with the central system. Additionally, the gaming device receives the software image from the central system.

In another aspect of the present invention, a method in a computer system for implementing a gaming machine system including a central system in communication with one or more gaming devices is provided. In accordance with the method, a software image to be downloaded to the one or more gaming devices is obtained. The software image is downloaded to a selected group of the one or more gaming devices.

In a further aspect of the present invention, a method is a computer system for implementing a download of a software image is provided. In accordance with the method, a central process obtains a software image to be downloaded and transfers the software image to one or more device processes. The one or more device processes receives and stores the software image. At least one of the one or more device processes executes the software image.

In yet another aspect of the present invention, a gaming machine system is provided. The gaming machine system includes a central system and one or more gaming devices having storage means for receiving an executable software image. The one or more gaming devices are in communication with the central system. Additionally, the gaming machine system includes downloading means for transferring the software image from the central system to the one or more gaming devices.

A method and device implementing a downloadable software delivery system for an electronic gaming machine communications network is provided. A central system is operatively connected to a plurality of gaming machines either by a direct communications link or through the use of one or more site controllers. In this regard, it is contemplated that a PC or suitable computing device could be substituted for a site controller and that the downloadable software delivery still be effected. Each gaming machine and site controller or PC contains two executable spaces, one of which typically contains the software image currently being implemented by the device. The other executable space is designated to receive from the central system a new software image that will be utilized by the device. The central system transfers a new image to be executed, via packet encrypted communications, to a networked device which stores the image in an executable space, while continuing to run the currently designated image. Upon instruction from the central system, the device switches over to the new image, allowing one or more machines to implement a software upgrade on a continuous basis.

BRIEF DESCRIPTION OF THE DRAWING

The present invention is described in detail below with reference to the attached figures, wherein:

FIG. 1 is a block diagram of a gaming machine network utilized in accordance with the present invention;

FIG. 2 is a block diagram illustrative of various device components utilized in accordance with the present invention;

FIGS. 3A, 3B & 3C are flow diagrams illustrative of a software image transfer method utilizing random key encryption in accordance with the present invention;

FIGS. 4A & 4B are flow diagrams illustrative of an image transfer error checking and bypass process in accordance with the present invention;

FIG. 5 is a flow diagram illustrative of a software image transfer method to a gaming machine in accordance with the present invention; and

FIG. 6 is a block diagram illustrative of a software image parsing embodiment in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In essence, the present invention enables a central system operatively connected to a plurality of gaming machines and site controllers (or PCs) to upgrade one or more software images via a communications link without requiring a manual change of the device chipset.

FIG. 1 is block diagram illustrative of a gaming machine network operable to be utilized by the present invention, designated generally by the reference numeral 10. Generally, the gaming machine network 10 includes a central system 12 operatively connected to a number of gaming machines 14 either by a direct communication link to each individual machine 14 or indirectly through the one or more site controllers or PC 's 16. The connectivity of the central system 12 to the gaming machines 14 can include continuous, on-line communication systems, including local area networks and/or wide area networks, or may be periodic, dial up semi-continuous communications. Because many gaming machine network currently utilize some type of communication network, the present invention preferably utilizes the preestablished communication system between the central system and the gaming machines such as through telephone, cable, radio or satellite links. However, a dedicated software delivery communication network may also be implemented and is considered to be within the scope of the present invention.

FIG. 2 is a block diagram illustrative of some of the components common to the gaming machines 14, site controllers 16 or other networked device (FIG. 1), generally referred to as a device 18, utilized in the present invention. Each device 18 preferably contains a processor 20, a memory 22, a communications input/output 24, such as a modem or network card, and at least two executable spaces 26. As would be readily understood by one skilled in the relevant art, the processor 20, memory 22 and communications input/output 24 includes any variety of component generally utilized in the implementation of the device. Moreover, in one embodiment, one or more of the executable spaces 26 are FLASH ROM. However, as would be readily understood, the executable spaces 26 may include DVD, CD-ROM, battery backed RAM or any other nonvolatile memory storage device.

Preferably, one executable space 26 is typically designated to store the software code, or image, currently being executed by the device 18. The other executable space is typically designated to receive a new image transferred by the central system. As would be understood, although the two executable spaces are preferably separate, the same effect is accomplished through the use of a single, larger executable space. In this embodiment, each device uses a portion of the executable space 26 to assist in receiving and storing incoming images from the central system.

As an alternative embodiment, the present invention may also be implemented with one executable space and sufficient other memory, which can include memory 22, to temporarily store a downloaded image. In this embodiment, the image would be downloaded to the temporary memory and then transferred to the more permanent executable space 26.

Generally, the present invention facilitates the implementation and replacement of a software image on a device in a gaming machine network by allowing the transmittal of a new image to a device while the device continues to execute and/or process a previous software image. Additionally, because the present invention may utilize one or more existing communication lines, the transfer of a new image can include various security and error checking features to ensure and preserve the secured character of the executable code.

FIGS. 3A, 3B & 3C are flow diagrams of an image downloading process utilizing a random key encryption in accordance with the present invention. With reference to FIG. 3A, at S28, the desired image to be downloaded is created, and loaded into the central system. Preferably, the operating system of the central system provides a user interface, such as a graphical user interface, that allows a user to download the image to the central system's memory. Additionally, the user interface can include prompts for a user to enter additional information needed for the downloading process including download time information, download windows and version numbers. As would be understood, depending on the function of the image being downloaded, the additional information needed to complete the download will vary.

Once the image has been downloaded to the central system, the user selects which devices are to receive the image. The user selection can include all of the devices or subsets of devices. Preferably, the central system includes some form of error checking that ensures that the designated device is compatible with the image to be downloaded. At S30, the central system generates a random encryption key for each device designated to receive the image and encrypts the image with each of the random keys at S32. The random keys and encrypted images are stored in the central system memory. Additionally, the central system stores a completed, unencrypted version of the image in memory to use a signature for verification that the download is complete.

Generally, the function of a site controller (or PC) download differs from the function of the gaming machine download. Accordingly, at S34 a determination of whether the download is for a site controller is made. With reference to FIGS. 3A & 3B, if at S34 the desired image is designated to be downloaded to a site controller or PC, the random keys used to encrypt the image are themselves encrypted with a general encryption key and sent to the site controller at S36. At S38, the site controller or PC decrypts the random keys and stores the keys in a memory, such as memory 22 (FIG. 2). The central system then sends the random key encrypted message to the site controller at S40. Once the download is complete, the central system sends additional instructions to the site controller such as to decrypt the image with the stored random keys or to store the image into its second executable space.

With reference to FIGS. 3A & 3C, if at S34, the desired image is designated to be downloaded to a gaming machine or other device, the central system sends the encrypted message to the site controller (or PC) associated with the particular gaming machine at S44, preferably in a manner as described above in steps S36-S42. At S46, the central system sends the site controller a list of the gaming machines to receive the image and their preassigned general encryption keys, which are encrypted with a key known to the gaming machine. At S48, the site controller transfers the encryption keys to the gaming machine, which decrypts and stores the random keys in memory. The site controller then sends the random key encrypted image to the gaming machine at S50. Once the download is complete, the central system instructs the gaming machine, via the site controller, to prepare and store the image into its second executable space at S54.

With reference to FIGS. 4A & 4B, the present invention implements a bypass and error checking function between the central system and the site controller or PC. Because the site controller can be associated with a number of gaming machines or other devices, once the site controller stores the image into its executable space, it does not need to reexecute the downloading step for each subsequent transfer to a gaming machine. With reference to FIG. 4A, the central system begins the download process each time an image is to be transferred to a device as illustrated at S56. At S58, the central system checks whether a downloaded image has already been stored in the site controller's executable space. If so, at S60, the central system verifies that the signature of the image loaded on the site controller is correct and the transfer is complete at S72. With reference to FIGS. 4A & 4B if an image is not present in the site controller's executable space at S58 or if the signature does not match at S60, the central system sends the image via packets to the site controller or PC at S62.

Preferably, the central system relies on package acknowledge signals from the site controller to ensure that each individual packet is received by the site controller. Accordingly, at S64, the central system determines whether all the packets have been received. If one or more package acknowledge signals are not received, the transfer is incomplete at S70. At this point, the central system may resend the individual packets not received or may attempt to resend the entire image. Alternatively, the central system may just declare the transfer a failure.

If the packets are received and acknowledged at S64, the central system completes the transfer at S66. At S68, the central system requests a signature of the image from the site controller to verify a proper transmission and decryption. With reference to FIGS. 4A & 4B, if the signature is a match, the download is a success at S72 and the site controller implements any downloading instruction. If the signature is not a match, the transfer is incomplete at S70.

With reference to FIG. 5, the present invention also implements an error transfer method for the downloading of an image from the site controller to the gaming machine. Upon receiving and storing the downloaded image in memory, the site controller (or PC) begins the download to the gaming machine at S74. Preferably as illustrated in FIG. 6, the software image 86 is organized into one or more frames 88 which are further organized into one ore more blocks 92 per frame. Each of the blocks 92 can then be transferred as individual communication packets. During the download process, site controller transfers all packets that make up the frame with reference again to FIG. 5, at the end of the transfer frame the site controller requests an acknowledgment from the gaming machine at S70.

If the gaming machine did not receive some portion of the frame, the transfer is incomplete at S82. The site controller preferably resends only those packets which are incomplete. Alternatively, the entire image may be resent or the transfer may be declared a failure. Accordingly, the gaming machine does not need to acknowledge receipt of each packet. As would be understood, however, alternative methods of grouping and sending the software image would be considered within the scope of the present invention.

Upon the transfer of the entire image to the gaming machine at S78, the central system requests an image signature to verify the transfer was successful at S80. If the signature is a match, the transfer is successful at S84. If the image is not a match, the image is incomplete at S82.

The above-described transfer protocols have been incorporated with reference to two separate encryption methods. As would be understood, a system implementing only a portion, different or no encryption methods would be considered within the scope of the present invention.

Once the image has been successfully transferred to the device, the image can be executed. Preferably, the central system sends a command to the device to begin using the new image in the executable space. This command typically includes separate instructions for configuring the system to accommodate the new image and preventing the future play of the current image while the switch is occurring. Upon the completion of the command, the device begins executing the new image and the switch is complete.

Because the device contains at least two separate executable spaces, the old image previously being executed remains in the device executable space after the switch is complete. In the event that the new image is corrupt or not functioning properly, the central system can execute a command to revert to the old image if it is still available and intact.

Although the devices specifically referenced in the present application refer solely to gaming machines or site controllers or PCs, the present invention allows images to be transferred to any device that is configured to receive an image. Such devices could include peripheral devices such as printers and bill acceptors or other intermediate communications devices. As would be understood, the images associated with each device would vary with the type of device and its function in the system.

In the foregoing specification, the present invention has been described with reference to the specific exemplary embodiments thereof. It will be apparent to those skilled in the art that a person understanding this invention may conceive of changes or other embodiments or variations, which utilize the principals of this invention without departing from the broader scope of the invention.

What is claimed:

1. A gaming machine system comprising: a central system; and one or more gaming devices having at least one storage component operable to receive an executable software image, wherein the one or more gaming devices are in communication with the central system; wherein the gaming device receives the software image from the central system.

2. The gaming machine system as recited in claim 1, wherein the central system includes a user interface for accepting the software image to be downloaded to the one or more gaming devices.

3. The gaming machine system as recited in claim 1, wherein the central system is in communication with the one or more gaming devices via a dedicated, continuous communication network.

4. The gaming machine system as recited in claim 1, wherein the central system is in communication with the one or more gaming devices via a nondedicated communication network.

5. The gaming machine system as recited in claim 1, wherein the central system is remote from at least one of the one or more gaming devices.

6. The gaming machine system as recited in claim 1, wherein the one or more gaming devices include at least one gaming machine.

7. The gaming machine system as recited in claim 1, wherein the one or more gaming devices include at least one site controller or PC.

8. The gaming machine system as recited in claim 1, wherein the at least one storage component of the one or more gaming devices includes a first executable space for storing an image currently being implemented by the gaming device and a second executable space operable to receive the software image to be downloaded.

9. The gaming machine system as recited in claim 8, wherein two or more the executable spaces are flash read only memory.

10. A method in a computer system for implementing a gaming machine system including a central system in communication with one or more gaming devices, the method comprising: obtaining a software image to be downloaded to the one or more gaming devices; and downloading the software image to a selected group of the one or more gaming devices.

11. The method as recited in claim 10, wherein the obtaining step includes providing one or more user interfaces for receiving the software image from a user.

12. The method as recited in claim 11, wherein the downloading step further comprises: encrypting the software image with a random key; and transferring the encrypted software image to the selected group of the one or more gaming devices.

13. The method as recited in claim 12, wherein the downloading step further comprises: encrypting the random key with a general encryption key; and transferring the encrypted key to the selected group of the one or more gaming devices.

14. The method as recited in claim 12, where each gaming device within the selected group of the one or more gaming devices corresponds to a different random key.

15. The method as recited in claim 10, further comprising issuing to the selected group of the one or more gaming devices instructions to begin executing the downloaded software image.

16. The method as recited in claim 10, wherein the one or more gaming devices include at least one site controller or PC and at least one gaming

machine, wherein the downloading step includes transferring the software image and an instruction to download the image to the gaming machine to the site controller or PC.

17. The method as recited in claim 16, wherein the download step further comprises: detecting whether the site controller or PC contains a copy of the image to be downloaded to the gaming machine; and if the copy is a valid image, canceling the download of the software image.

18. The method as recited in claim 10 further comprising issuing to the selected group of the one or more gaming devices instructions to cease executing the downloaded software image and revert back to a previous image.

19. A computer-readable medium having computer-executable instruction for performing the steps recited in claim 10.

20. A computer system having a processor, a memory and an operating environment, the computer system operable to perform the steps recited in claim 10.

21. A method in a computer system for implementing a download of a software image, the method comprising: obtaining, by a central process, a software image to be downloaded; transferring, by the central process, the software image to one or more device processes; receiving, by the one or more device processes, the software image; storing, by the one or more device processes, the software image; and executing, by at least one of the one or more device processes, the software image.

22. The method as recited in claim 21, further comprising: encrypting, by the central process, the software image; and decrypting, by the one or more device process, the software image.

23. The method as recited in claim 21 further comprising issuing, by the central process, a command to begin executing the downloaded software image.

24. The method as recited in claim 21 further comprising issuing, by the central process, a command to cease executing the downloaded software image and begin executing a previous software image.

25. The method as recited in claim 21, wherein the transferring step includes: transferring, by the central process, the software image to a site controller process; receiving, by the site controller process, the software image; and transferring, by the site controller process, the software image to a gaming machine process.

26. The method as recited in claim 25, further comprising canceling, by the central process, the software image download if the site controller already has a copy of the software image.

27. A computer-readable medium having computer-executable instructions operable for performing the steps recited in claim 21.

28. A computer system having a processor, a memory and an operating system, the computer system operable to perform the steps recited in claim 21.

29. A gaming machine system comprising: a central system; one or more gaming devices having storage means for receiving an executable software image, wherein the one or more gaming devices are in communication with the central system; and downloading means for transferring the software image from the central system to the one or more gaming devices.

30. The gaming machine system as recited in claim 29, wherein the central system includes interface means for accepting the software image to be downloaded to the one or more gaming devices.

31. The gaming machine system as recited in claim 29, wherein the storage means include flash read only memory.

32. The gaming machine system as recited in claim 31, wherein the storage means include two separate flash read only memory components.

33. The gaming machine system as recited in claim 29, wherein the one or more gaming devices include at least one gaming machine.

34. The gaming machine system as recited in claim 29, wherein the one or more gaming devices include at least one site controller or compatible computing device.

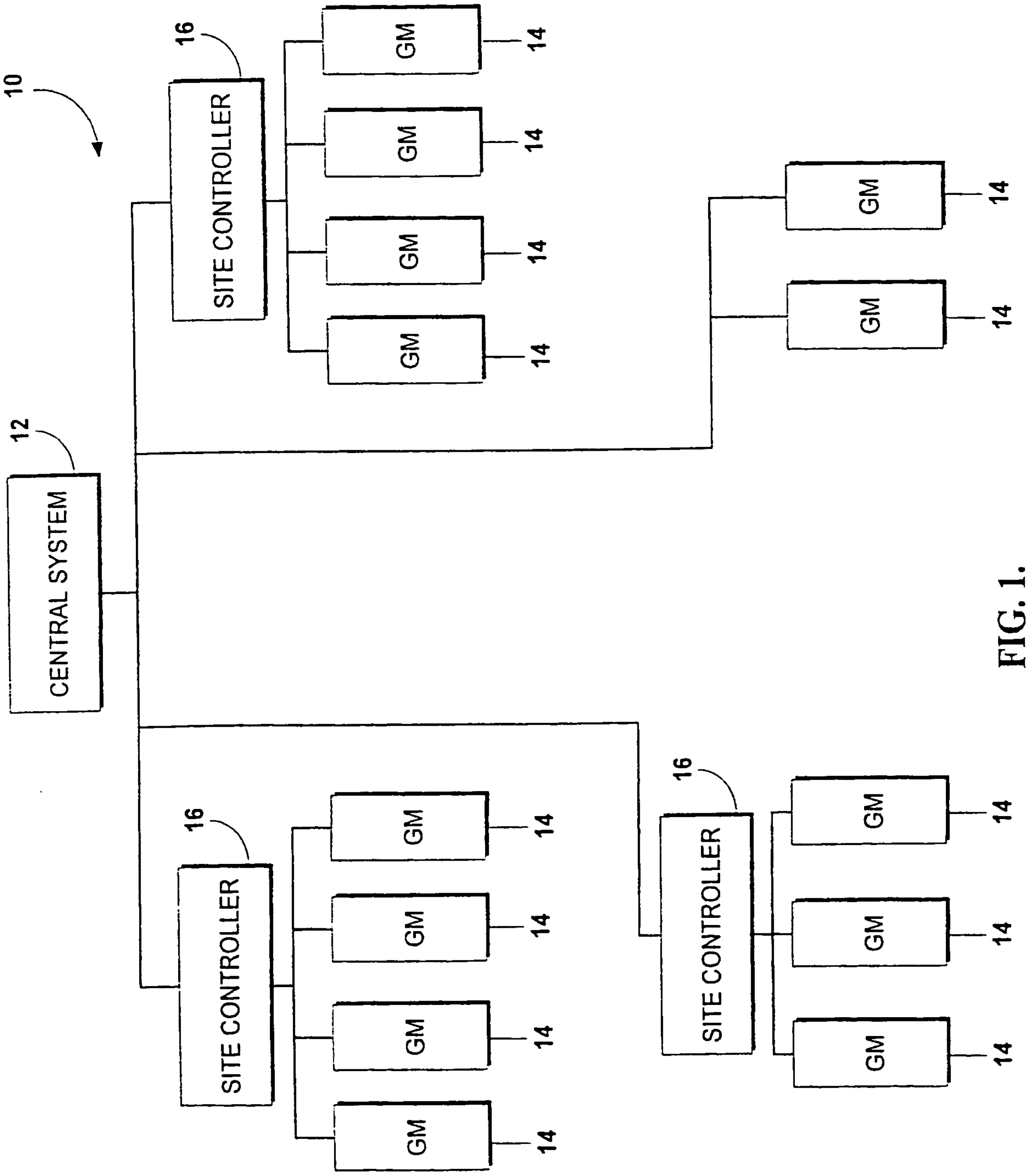

10
12
CENTRAL SYSTEM
16
SITE CONTROLLER
16
SITE CONTROLLER
16
SITE CONTROLLER
GM
14

FIG. 1.

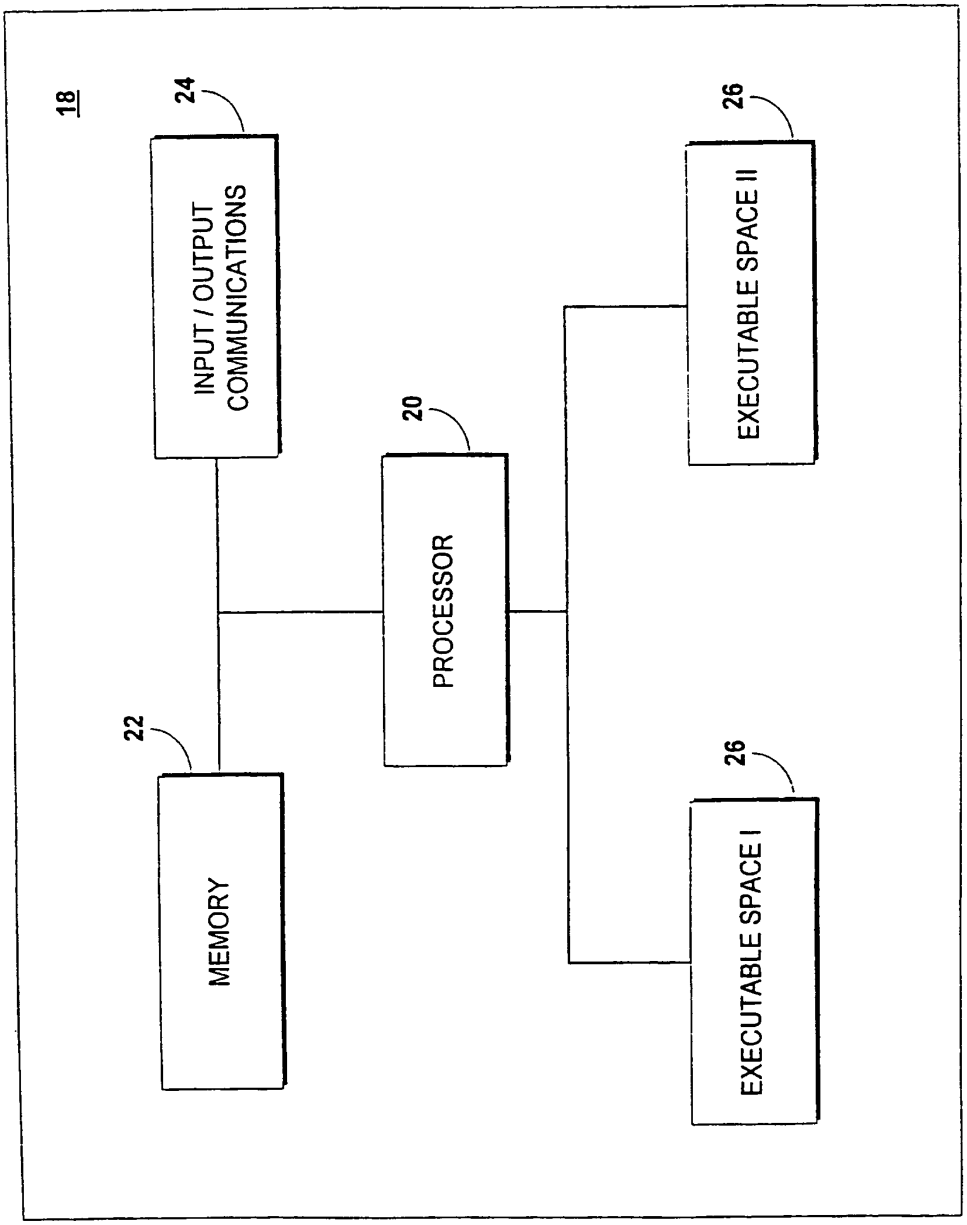

18
24
INPUT / OUTPUT COMMUNICATIONS
20
PROCESSOR
22
MEMORY
26
EXECUTABLE SPACE II
26
EXECUTABLE SPACE I

FIG. 2.

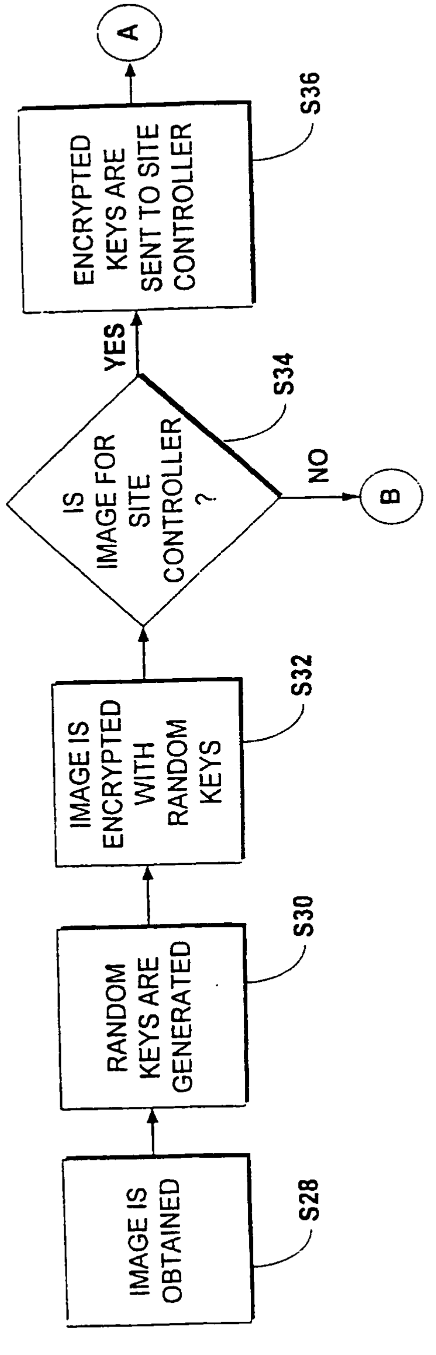


IMAGE IS OBTAINED
S28
RANDOM KEYS ARE GENERATED
S30
IMAGE IS ENCRYPTED WITH RANDOM KEYS
S32
IS IMAGE FOR SITE CONTROLLER ?
S34
YES
NO
B
ENCRYPTED KEYS ARE SENT TO SITE CONTROLLER
S36
A

FIG. 3A.

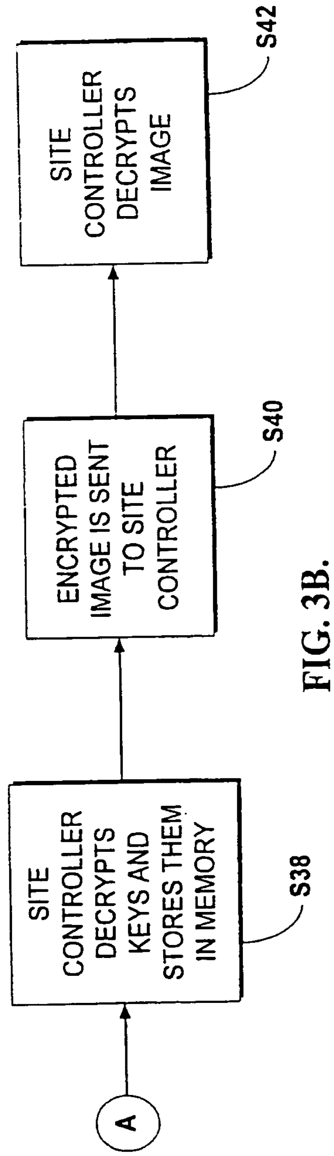

A
SITE CONTROLLER DECRYPTS KEYS AND STORES THEM IN MEMORY
S38
ENCRYPTED IMAGE IS SENT TO SITE CONTROLLER
S40
SITE CONTROLLER DECRYPTS IMAGE
S42

FIG. 3B.

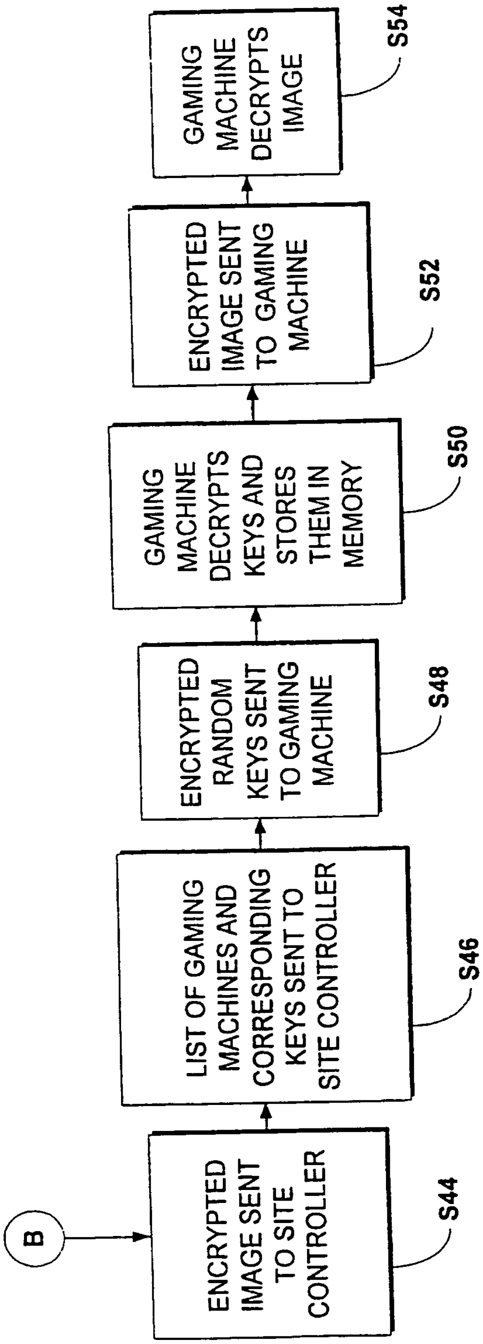

B
ENCRYPTED IMAGE SENT TO SITE CONTROLLER
S44
LIST OF GAMING MACHINES AND CORRESPONDING KEYS SENT TO SITE CONTROLLER
S46
ENCRYPTED RANDOM KEYS SENT TO GAMING MACHINE
S48
GAMING MACHINE DECRYPTS KEYS AND STORES THEM IN MEMORY
S50
ENCRYPTED IMAGE SENT TO GAMING MACHINE
S52
GAMING MACHINE DECRYPTS IMAGE
S54

FIG. 3C.

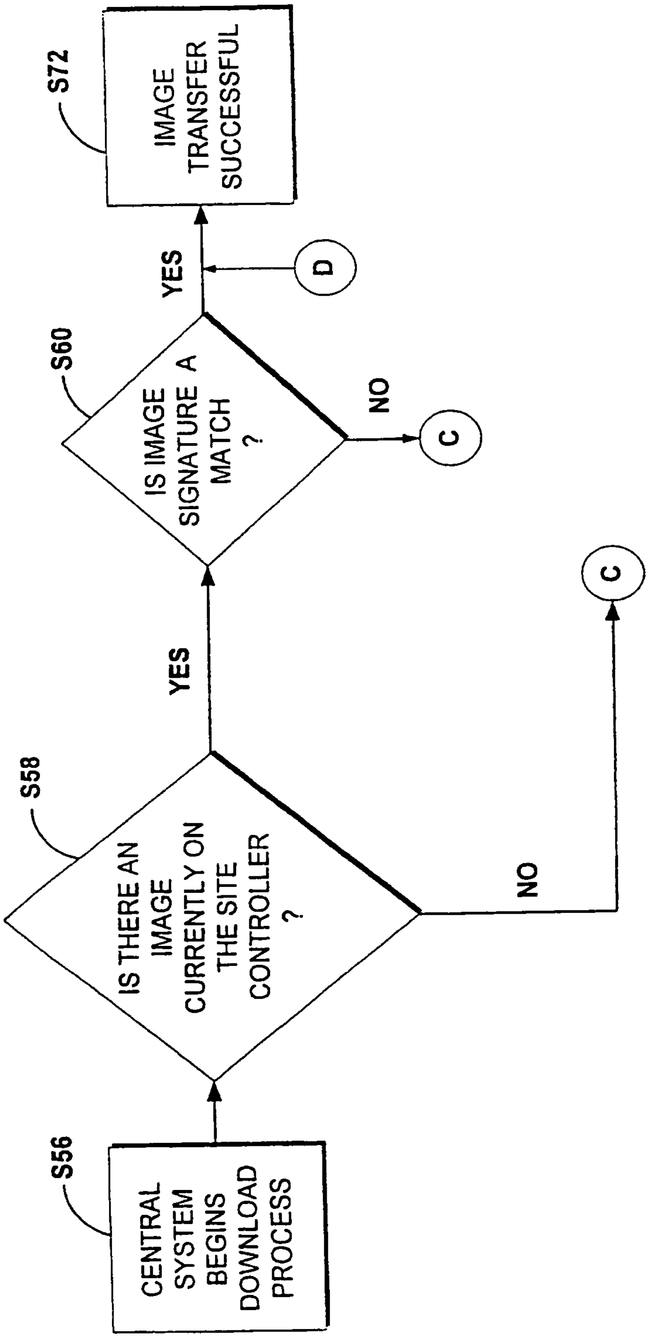

S56
CENTRAL SYSTEM BEGINS DOWNLOAD PROCESS
S58
IS THERE AN IMAGE CURRENTLY ON THE SITE CONTROLLER ?
YES
NO
C
S60
IS IMAGE SIGNATURE A MATCH ?
YES
NO
C
D
S72
IMAGE TRANSFER SUCCESSFUL

FIG. 4A.

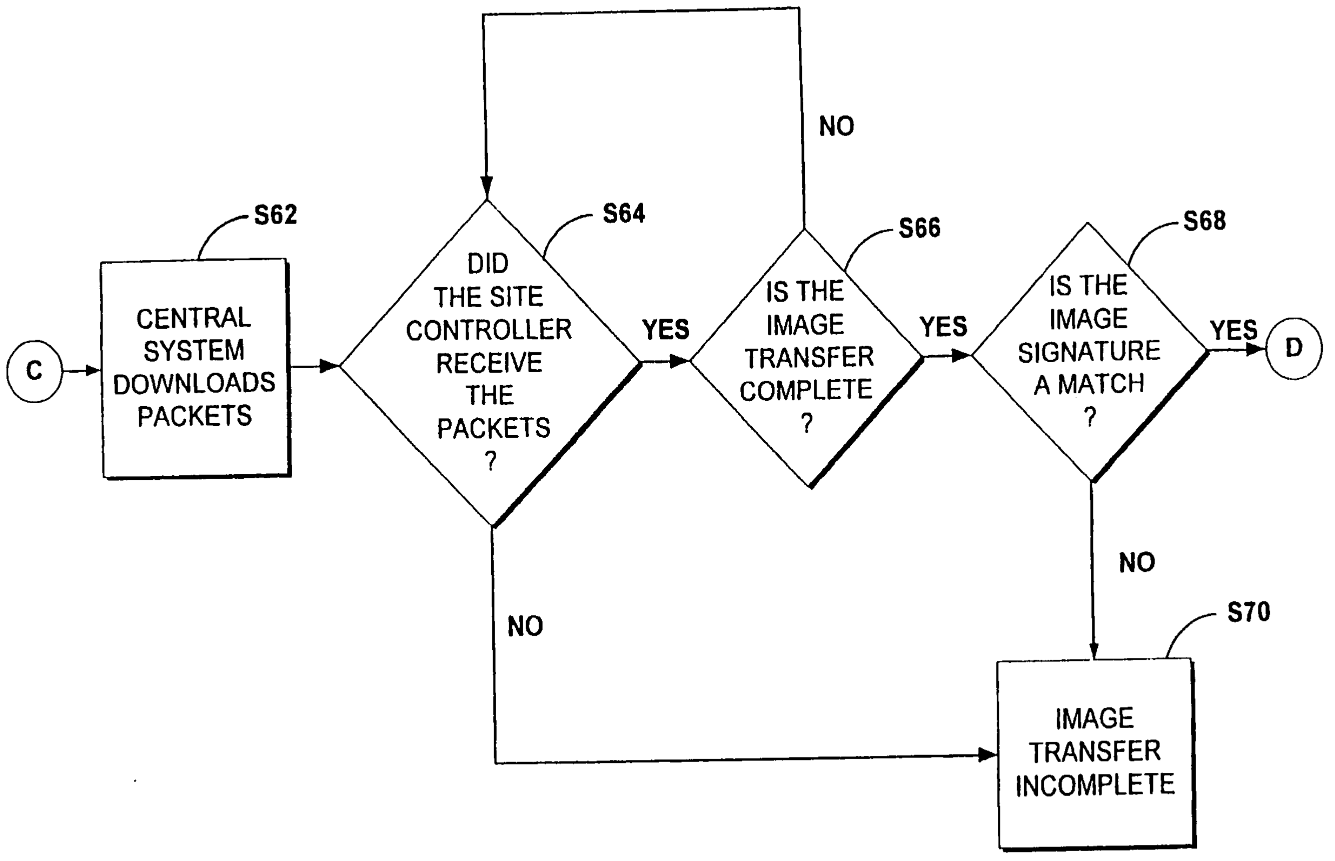

S62
C
CENTRAL SYSTEM DOWNLOADS PACKETS
S64
DID THE SITE CONTROLLER RECEIVE THE PACKETS ?
YES
NO
S66
IS THE IMAGE TRANSFER COMPLETE ?
YES
NO
S68
IS THE IMAGE SIGNATURE A MATCH ?
YES
D
NO
S70
IMAGE TRANSFER INCOMPLETE

FIG. 4B.

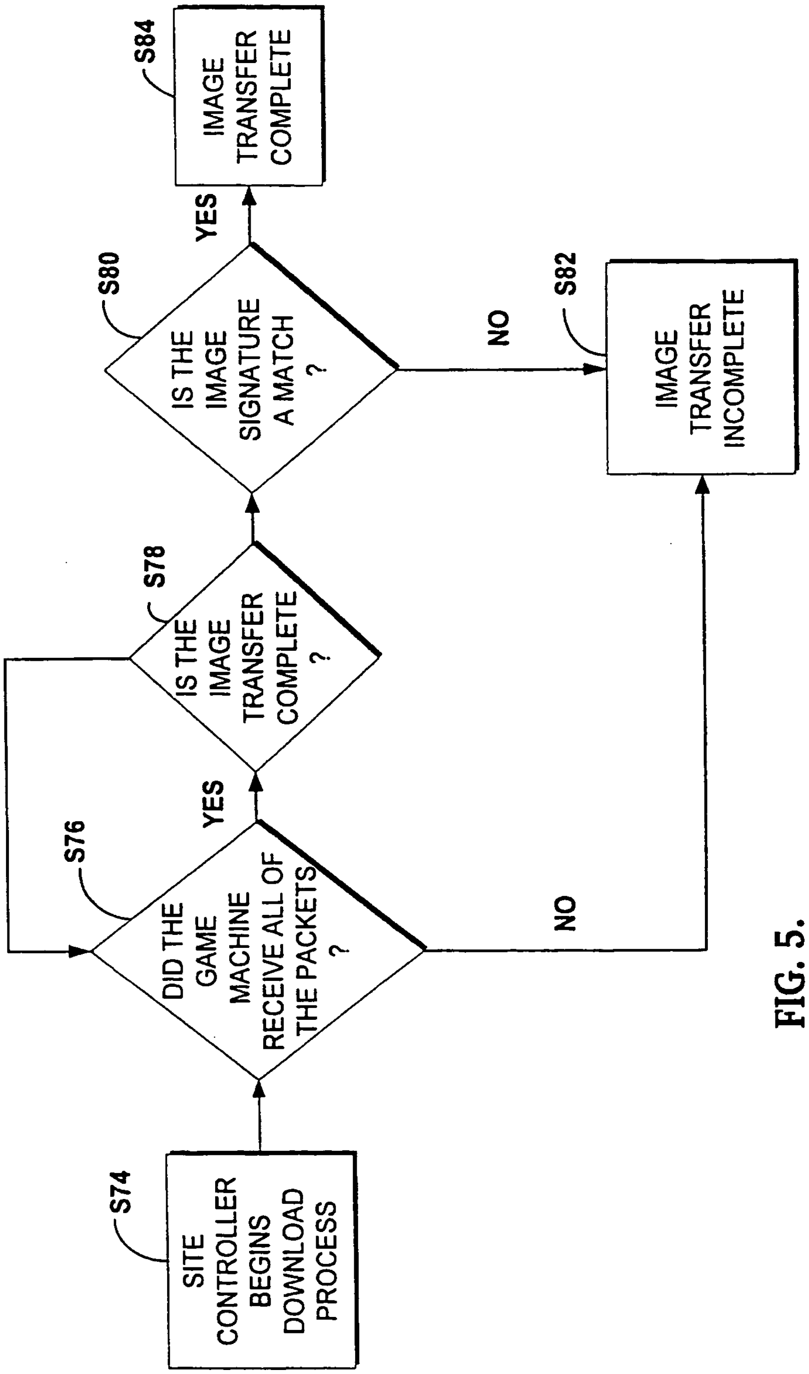

S74
SITE CONTROLLER BEGINS DOWNLOAD PROCESS
S76
DID THE GAME MACHINE RECEIVE ALL OF THE PACKETS ?
YES
NO
S78
IS THE IMAGE TRANSFER COMPLETE ?
S80
IS THE IMAGE SIGNATURE A MATCH ?
YES
NO
S84
IMAGE TRANSFER COMPLETE
S82
IMAGE TRANSFER INCOMPLETE

FIG. 5.

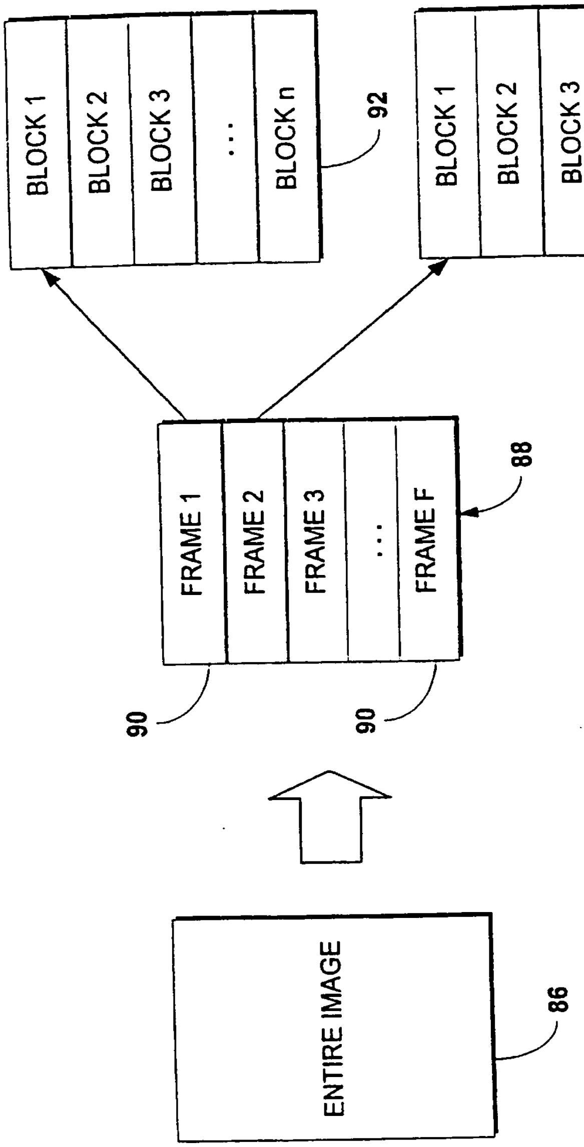

BLOCK 1
BLOCK 2
BLOCK 3
...
BLOCK n
92
BLOCK 1
BLOCK 2
BLOCK 3
...
BLOCK n
92
FRAME 1
FRAME 2
FRAME 3
...
FRAME F
88
90
90
ENTIRE IMAGE
86

FIG. 6.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☑ BLACK BORDERS

☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

□ FADED TEXT OR DRAWING

□ BLURRED OR ILLEGIBLE TEXT OR DRAWING

□ SKEWED/SLANTED IMAGES

□ COLOR OR BLACK AND WHITE PHOTOGRAPHS

□ GRAY SCALE DOCUMENTS

☑ LINES OR MARKS ON ORIGINAL DOCUMENT

☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

□ OTHER: ______________________________

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 706 275 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.04.1996 Bulletin 1996/15

(51) Int. Cl.^{6}: H04L 9/32, H04L 9/30

(21) Application number: 95113153.1

(22) Date of filing: 22.08.1995

(84) Designated Contracting States:
DE FR GB

(30) Priority: 15.09.1994 US 306741

(71) Applicant: International Business Machines Corporation
Armonk, N.Y. 10504 (US)

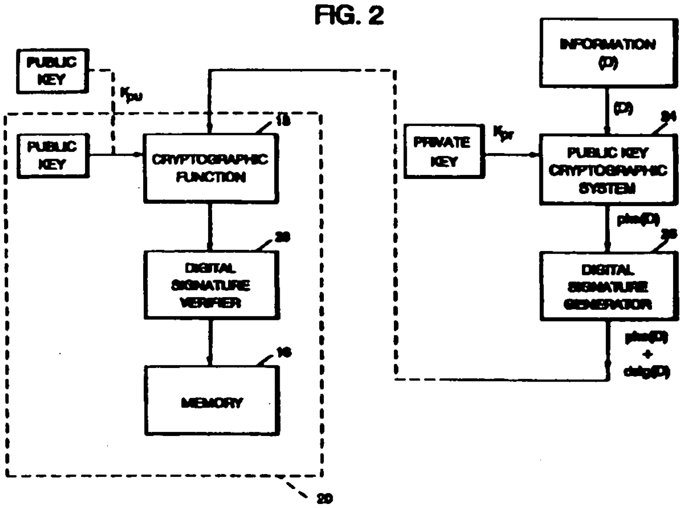
(72) Inventor: Arnold, Todd Weston
Charlotte, NC 28262 (US)

(74) Representative: Rach, Werner, Dr.
IBM Deutschland
Informationssysteme GmbH,
Patentwesen und Urheberrecht
D-70548 Stuttgart (DE)

(54) System and method for secure storage and distribution of data using digital signatures

(57) The present invention overcomes the disadvantages and limitations of the related art by providing an apparatus and method for secure distribution of software, software updates, and configuration data. Cryptography is used to protect software or data updates sent to computer products or peripherals using non-secure distribution channels. In the preferred embodiment, the contents of the data cannot be read by anyone who obtains the data, and the data will not be accepted unless it is unmodified and originated with the valid source for such data.

FIG. 2



Printed by Rank Xerox (UK) Business Services
2.10.4/3.4

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an apparatus and method for secure distribution of data. More particularly, the present invention relates to an apparatus and method for secure distribution of software, software updates, and configuration data.

2. Description of Related Art

In today's business environment, data is one of the most valuable resources required for maintaining a competitive edge. As a result, businesses must often be able to maintain data confidentiality, readily determine the authenticity of data, and closely control access to data. As used herein, the term "data" means a representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automatic means, including, but not limited to, software, software updates, and configuration data.

Data systems commonly consist of many types and sizes of computer systems that are interconnected through many different electronic data networks. It is now common for an organization to interconnect its data systems with systems that belong to customers, vendors, and competitors. Larger organizations might include international operations, or they might provide continual services. For purposes herein, "computer" includes a device capable of performing the functions of a Turing Machine, including a microcomputer, minicomputer, or mainframe computer. A Turing Machine is a well-known computer science concept and is explained in Encyclopedia of Computer Science, Ed. Anthony Ralston, ISBN 0-88405-321-0, which is specifically incorporated herein by reference. "Memory" includes a device or devices for storing data for use by a computer, including electronic, magnetic, and electro-magnetic memory.

A combination of elements must work together to achieve a more secure environment. A security policy, based on an appraisal of the value of the data and potential threats to that data, provides the foundation for a secure environment.

Security functions can be categorized as follows:

- Identification and authentication. Identifies users to the system and provides proof that they are who they claim to be.
- Access control. Determines which users can access which resources.
- Data confidentiality. Protects an organization's sensitive data from unauthorized disclosure.
- Data integrity. Ensures that data is in its original form and that it has not been altered.
- Security management. Administers, controls, and reviews a business, security policy.
- Nonrepudiation. Assures that the message was sent by the appropriate individual.

Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data confidential and for verifying data integrity. Cryptography: A Guide for the Design and Implementation of Secure Systems, by Carl H. Meyer and Stephen M. Matyas, ISBN 0-471-04892-5, John Wiley & Sons, Inc. (1982), is a classic text on the design and implementation of cryptographic systems, which is specifically incorporated herein by reference.

For commercial business applications, the cryptographic process known as the Data Encryption Algorithm (DEA) has been widely adopted. The Data Encryption Standard (DES), as well as other documents, defines how to use the DEA to encipher data. Federal Information Processing Standards Publication 46, which defines DES, is reprinted in the Meyer & Matyas text. Many other processes for concealing data, such as protection of passwords and personal identification numbers (PINs), are based on the DES process. The DES algorithm uses a key to vary the way that the algorithm processes the data. A DES key is a very small piece of data (56 bits) that is normally retained in 8 bytes. The same key is used to transform the original data (plaintext) to its disguised, enciphered form (ciphertext) and to return it to its plaintext form. Because the DES algorithm is common knowledge, one must keep the key secret to make the data confidential; otherwise, someone who has the key that one used to encipher the data would be able to decipher the data. Key management refers to the procedures that are used to keep keys secret.

To confirm the integrity of data, one can use the DES algorithm to compute a message authentication code (MAC). Used in this way the DES algorithm is a powerful tool; it is almost impossible to meaningfully modify the data and still have it produce the same MAC for a given key. The standardized approaches authenticate data such as financial transactions, passwords, and computer programs.

After the MAC has been computed, it is sent with data. To authenticate the data, the system uses the DES algorithm to recompute the MAC; the system then compares this result with the MAC that was sent with the data. Someone could, of course, change both the data and the MAC; therefore, the key that is used to compute the MAC must be kept secret between the MAC's originator and the MAC's authenticator.

An alternative approach to data integrity checking uses a standard key value and multiple iterations of the DES algorithm to generate a modification detection code (MDC). In this approach to data integrity checking, the MDC must be received from a trustedsource. The person who wants to authenticate the data recomputes the MDC and compares the result with the MDC that was sent with the data.

Because the DES algorithm has been used for many years, its strength has been well demonstrated. Both software and specialized hardware can implement the DES algorithm. A hardware solution is often desirable for the following reasons:

- the algorithm requires many computer instructions to be processed
- the keys must be protected so that they can remain secret
- performance can be improved

If a data security threat comes from an external source, a software implementation of the cryptographic algorithm might be sufficient; unfortunately, however, much fraud originates with individuals within an organization (insiders). As a result, specialized cryptographic hardware can be required to protect against both insider and outsider data security threats. Well-designed hardware can do the following:

- ensure the security of cryptographic keys
- ensure the integrity of the cryptographic processes
- limit the key-management activities to a well-defined and carefully controllable set of services

The DES algorithm, which has been proven to be efficient and strong, is widely known; however the keys must normally remain secret. Because the same key is used both to encipher the data and to decipher the data, the process is said to be symmetric; it uses a symmetric key.

In another type of cryptographic process, an asymmetric process, one key is used to encipher the data, while a different but corresponding key is used to decipher the data to its original form. A system that uses this type of process is known as a public-key system. The key that is used to encipher the data is widely known, but the corresponding key for deciphering the data is secret. For example, many people who know a person's public key can send enciphered data to that person confidentially, knowing that only that person should possess the secret key for deciphering the data. Public-key cryptographic algorithms have been incorporated into processes for simplifying the distribution of secret keys and for assuring data integrity, including providing nonrepudiation by using digital signatures. Public-key and digital signature techniques are discussed in more detail the Meyer & Matyas text.

Public-key algorithms (e.g., RSA algorithm, by R. Rivest, A. Shamir, and L. Adleman) use a relatively large key and use even more computer time than the DES algorithm. The use of a public-key system is, therefore, often restricted to situations in which the characteristics of the public-key algorithms have special value.

In both the DES and RSA algorithms, no practical means exists to identically cipher data without knowing the cryptographic key; therefore, keeping a key secret at a cryptographic node is essential. In real systems, however, this often does not provide sufficient protection. If adversaries have access to the cryptographic process and to certain protected keys, they could possibly misuse the keys and eventually compromise the system. A carefully devised set of processes must be in place to protect and distribute cryptographic keys in a secure manner.

Access control protects data by allowing only persons or programs with a legitimate need to access system resources, such as a file, selected records or fields in a file, a hardware device, or the computing capability of the system. Access control uses the following services:

- Identification and verification. Identification is the ability to use a unique name, label, or other reference to identify each user or program to the system. Verification is the ability to provide proof that users and programs are who and what they claim to be. (Verification is also known as "authentication".)

- Authorization. Authorization is the process whereby users or programs are restricted to specific resources, such as data sets, programs, or transactions. (Authorization is also known as "access control".)

- Enforcement. Enforcement is a subsystem process of verifying the requester's authorization.

In systems that consist of multiple computers, it is increasingly necessary for persons or programs at one system to be able to convince persons or programs at another system that they are entitled to receive service. Common solutions to this problem involve the following:

- using local access controls

- using cryptographic processing to ensure the authenticity of a process

- ensuring that the authorization information is confidential

Many computer products and peripherals now have their own intelligence, separate from the computer itself, in the form of integrated microprocessors. These microprocessors use stored programs to provide some part of the device's function.

For example, the IBM 4755 Cryptographic Adapter is a device which includes a microprocessor, memory, and programming logic mounted on a printed circuit board. Functions are housed within a tamper-resistant module, or secured area, for protection, such as that discussed more fully in U.S. Pat. No. 5,027,397, which is specifically incorporated herein by reference. The IBM 4755 is a component of the IBM Transaction Security System, discussed in the IBM publication entitled "Transaction Security System: General Information Manual and Planning Guide" (GA34-2137-0), U.S. Pat. No. 5,048,085, and U.S. Pat. No. 5,148,481, which are specifically incorporated herein by reference.

Typically, two kinds of memory are associated with these microprocessors: permanent (unalterable or nonvolatile) memory for the program; and volatile memory for data used by the program. Permanent memory is typically Read Only Memory (ROM), Programmable Read Only Memory (PROM), or Erasable Programmable Read Only Memory (EPROM). Volatile memory is typically a static or dynamic Random Access Memory (RAM), which loses all stored data when power is removed.

Newer technologies allow the designer to use memory which is nonvolatile, but reprogrammable. That is, memory in which the data can be changed, but the contents are retained when the power is off. Several technologies can be used to obtain these characteristics. Flash EPROM (FEPROM) permits areas of memory to be erased electronically and then reprogrammed. Electrically Erasable PROM (EEPROM) permits individual bytes or bits to be rewritten much like RAM memory. Complementary Metal-Oxide Semiconductor (CMOS) RAM with battery back-up uses little power and retains RAM contents when system power is off.

These newer kinds of memory can be used in two ways to improve the value of the product.

First, if some or all of the microprocessor program is stored in nonvolatile, reprogrammable memory, the program can be changed after the product is manufactured. Thus, new features can be added and errors can be corrected. This prevents product obsolescence and protects the manufacturer from high warranty costs when errors occur.

Second, data stored in the memory can control the configuration of the product. One such use is to selectively enable or disable product features. In this way, the manufacturer can produce a standard product, and sell it for a variety of applications which need different features. Users can be charged for an upgrade to enable new features, which will be highly profitable to the manufacturer since no new hardware has to be shipped or installed.

There are many circumstances which would make it advantageous to be able to target such upgrades to a specific subset of the total population of devices. The reason may be to prevent applying an upgrade that is incompatible with the underlying hardware or software, or it may be to restrict the upgrade to a specific set of users or devices. For example, the manufacturer may want to apply the upgrade only to devices which have:

- a particular model number

- a manufacture date within a particular range of dates

- a particular version of software installed

- a certain ranges of serial numbers

- a specific combinations of features

It is easy to see why this kind of flexibility is highly desirable, for both the manufacturer and the user. There is a significant impediment to its use, however; security.

Both the manufacturer and user want to be sure they have control over programs that are loaded into the memory. The manufacturer may want to make sure only its programs are used, to ensure the programs meet quality and performance standards. The manufacturer may also want to prevent anyone from learning how the software works, or what the data is that is being sent to the user. The user, on the other hand, wants to make sure the programs in the devices are valid, and prevent any that might malfunction, or which might pose a security threat. An example of a security threat would be a "Trojan horse" program which would normally operate correctly, but which had "secret" features to circumvent the user's security practices, or to divulge the user's secret information.

Typically, there will be one source for all field upgrades to code or configuration data, although other scenarios are possible. For the purposes of discussion, assume that the device manufacturer is the only valid source of code or data updates; and the device is a security adapter card, with a secured area or module where data is protected from disclosure. The problem can then be described with two fundamental requirements:

First, data sent to the user must be kept secret. It must be impossible for anyone to discover or modify the contents of the data.

Second, the user must be able to verify that the data came from the valid source (e.g., the manufacturer). This is a form of non-repudiation.

SUMMARY OF THE INVENTION

The present invention overcomes the disadvantages and limitations of the related art by providing an apparatus and method for secure distribution of software, software updates, and configuration data. Cryptography is used to protect software or data updates sent to computer products or peripherals using non-secure distribution channels. In the preferred embodiment, the contents of the data cannot be read by anyone who obtains the data, and the data will not be accepted unless it is unmodified and originated with the valid source for such data.

An advantage of the invention is to provide an apparatus and method for secure distribution of software, software updates, and configuration data.

Another advantage of the invention is to provide an apparatus and method wherein data stored in memory controls the configuration of a product so as to selectively enable or disable product features.

Yet another advantage of the invention is to provide an apparatus and method wherein data stored in memory controls the acceptance or rejection of proposed data for a product.

The foregoing and other advantages of the present invention will be apparent to those skilled in the art of information handling technology in view of the accompanying drawings, description of the invention, and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram depicting a computer system and associated cryptographic system, wherein an enlargement of an embodiment of the cryptographic system is broken out.

FIG. 2 is a block diagram of an embodiment of the invented apparatus for secure distribution of software, software updates, and configuration data employing public key cryptography.

FIG. 3 is a flowchart of an embodiment of the invented method for secure distribution of software, software updates, and configuration data employing public key cryptography.

FIG. 4 is a block diagram of an embodiment of the invented apparatus for secure distribution of software, software updates, and configuration data employing public key cryptography and symmetric key cryptography.

FIG. 5 is a flowchart of an embodiment of the invented method for secure distribution of software, software updates, and configuration data employing public key cryptography and symmetric key cryptography.

FIG. 6 is a depiction of criteria information in tabular form.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to FIG. 1, a computer or computer system 10 is shown which includes a cryptographic system 12 comprising a microprocessor 14, memory 16, and cryptographic functions 18 mounted upon a device or adapter card 20. The microprocessor, memory, and cryptographic functions are housed within a secured area or module 22.

As shown in FIG. 2, a public key KPU is installed in the adapter card 20. Cryptographic system 12 includes the public key algorithm (e.g., RSA). The corresponding private key KPR would be held by, for example, the adapter card manufacturer, in a secure, secret manner so it would never be disclosed outside the manufacturer's organization. Preferably, the data is protected twofold:

First, as shown in FIG. 2, data, D, is encrypted by a public key cryptographic system 24 using the private key, KPR, or as shown in FIG. 4, data is encrypted by a symmetric key cryptographic system 25 using the symmetric key, KS. This provides the necessary secrecy; the data content cannot be determined by anyone intercepting the data, and any modification to the encrypted data will render it invalid.

Second, in FIGS. 2 and 4, a digital signature on the data is computed and sent to the adapter card users using a digital signature generator 26. This signature is verified before the data is accepted by digital signature verifier 28, which can be a component of cryptographic function 18 or a separate function as shown. Preferably, cryptographic function 18 include both a public key cryptographic system 18a and a symmetric cryptographic system 18b. A verified digital signature proves that the data has not been altered since its creation, and proves that the originator was, in this example, the manufacturer.

Two embodiments of the invention are described below.

Using only public key cryptography

The first four steps in FIG 3. are performed by the manufacturer, who sends the resulting data to the users. The remaining steps are performed by the user to load the data into the adapter card.

The manufacturer first generates the data to be loaded into the adapter cards in step 100. This data is designated D. The manufacturer already possesses private key KPR, and the corresponding public key KPU is with every adapter card manufactured. The key KPU may be embedded in the adapter card, or may be supplied externally on a diskette or other medium if it is protected against substitution (e.g., by a certification process). It does not need to be kept secret in order to maintain integrity of the loaded data.

In step 110, the manufacturer computes a digital signature on the data D using the private key KPR. The use of the digital signature is optional. Its use enhances the ability to prove the source of the data, but the data can be distributed successfully without a signature. The digital signature function is represented as dsig(). The signature will be verified before the data is accepted by the adapter card, assuring it came from the manufacturer in this example.

In step 120, the data D is encrypted using the private key algorithm with key KPR. This protects the data from disclosure or modification prior to its installation in the adapter card. The function pke() represents a public key encryption algorithm, such as the RSA algorithm.

The manufacturer, in step 130, sends the encrypted data pke(D) and the digital signature dsig(D) to the card users through any convenient channel; diskettes, electronic mail, or any other medium is sufficient. The user receives this information, and loads the data and signature into the secured area of the adapter card in step 140.

In step 150, the adapter decrypts the data using the public key KPU, recovering the clear data D. Following this, in step 160, the digital signature is verified using the same key. If the signature verifies, the data is genuine and it can only have been created by the manufacturer, who holds the private key KPR. Once the data has been decrypted and its validity has been determined, the data is applied to the nonvolatile memory in the adapter card, step 180; otherwise, the information is discarded, step 170.

Only the private key KPR needs to be kept secret. The public key KPU is present in every copy of the device, and there is no security exposure if its value is divulged. The nature of the public key algorithms guarantees that the private key cannot be determined from the public key, and that valid data cannot be generated with knowledge of the public key alone.

Using public key and symmetric key cryptography

Alternatively, the data can be encrypted using a symmetric key cryptographic algorithm (e.g., DES) instead of the public key algorithm used above. With current technology, symmetric key algorithms are generally faster to compute than public key algorithms, so this method is presently preferable. A randomly selected symmetric algorithm key is used each time new data is produced.

As shown in step 200 of FIG. 5, the manufacturer generates the data D to be sent to the installed cards in the field. In the step 210, a random symmetric algorithm key designated KS is generated. The users do not have key KS, so the manufacturer must sent it to them in a secure manner. In step 220, KS is encrypted with a public key algorithm using the private key KPR.

In step 230, the manufacturer computes a digital signature over the data D, and in step 240 the data is encrypted using the symmetric key algorithm with key KS. The encrypted KS, the encrypted data pke(D) and the digital signature dsig(D) are all sent to the user in step 250.

In step 260, the data is received at the user site where adapter cards are installed. The data is loaded into the secured area of the card, which contains the public key KPU. In step 270, KPU is used to decrypt the symmetric key KS using the public key algorithm. In step 280, the recovered KS is used to decrypt the data using the symmetric key algorithm.

In step 290, the digital signature is verified using KPU, in order to verify the origin of the data. If the signature verifies, it means that both the data D and the key KS were valid; in this case, the data is loaded into the nonvolatile memory on the adapter card and enabled for use, step 310. Otherwise, the data is discarded or otherwise rejected. All cryptographic calculations are preferably performed inside the secured area, so there is no threat of data manipulation while the data is recovered and verified.

With either method described above, other checking codes could be used as an alternative to the digital signature. An MDC, cyclic redundancy check (CRC), or any other valid checking code could be calculated over the data and appended to the data before it is encrypted. Once the data has been decrypted in the adapter card's secure environment, this value could be verified against the recovered data. If it verifies, the data is correct and originated with the holder of the private key KPR.

Use of information in the data as decision criteria

Once the data has been loaded into the adapter card, the decision of whether to permit the data to be employed can be made a function of information and/or instructions contained within the data itself.

In one embodiment, software contained in the device is used to compare "criteria information" in the data with "basic information" already contained in the device. Examples of such basic information include:

- serial number
- model codes
- date of manufacture
- version of software currently installed
- codes describing installed or available features

The basic information in the device is stored in memory (including hardware registers, permanent software, or resident loadable software). The criteria information is preferably included in the data in tabular form, for example, as shown in FIG. 6. The data, and therefore the criteria information, is securely distributed in the manner described in the previous sections herein. Control software within the device examines this table and compares it to the appropriate basic information in order to decide whether to apply the data.

The pseudocode in Table 1 is an example of how the criteria information from the table would be processed. Each item in the table would be compared with the appropriate basic information contained within the device itself. The results of the comparisons would be used to determine whether the data should be applied to the particular device.

TABLE 1

```
---------------------------------------------------------------

     Load_Permitted = FALSE;
     If SN_Min <= SN <= SN_Max then Do;
      If DT_Min <= DT <= DT_Max then Do;
      If Min_HW_Lvl <= HW_Lvl <= Max_HW_Lvl then Do;
       If Min_SW_Lvl <= SW_Lvl <= Max_SW_Lvl then Do;
        Get Feature_Vector;
        If all Features_Required features are present then Do;
        If no Features_Prohibited features are present then
               Do;
         If Model_List is empty then Load_Permitted = TRUE;
         Else do While Model_List not empty;
          Get Test_Model from head of Model_List;
          If Test_Model = model of this device
          then Load_Permitted = TRUE;
     If Load_Permitted = TRUE then load data to memory;
     Else Abort loading process
     ---------------------------------------------------------
```

*   SN_Min and SN_Max are the lowest and highest serial numbers the device can have for the data to be valid. In the pseudocode in Table 1, the serial number for a specific device is designated SN.

- DT_Min and DT_Max are the earliest and latest dates the device can have for the data to be valid, e.g., the manufacturing date, the microcode creation date, or some other date code. Several different dates could be compared if desired. In the pseudocode in Table 1, the date code for a specific device is designated DT.

- Min_HW_Level and Max_HW_Level are the lowest and highest hardware levels the device can have for the data to be valid. This represents the version of hardware in the device. HW_Level is used in the pseudocode to represent a particular device's hardware level.

- Min_SW_Level and Max_SW_Level are the lowest and highest software levels the device can have for the data to be valid. This represents the version of software in the device prior to application of the data. SW_Level is used in the pseudocode to represent the particular device's software level.

- Features_Required and Features_Prohibited are vectors of boolean values. They represent the features the device must have for the data to be valid, and the features the device must not have for the data to be valid. In the pseudocode, Feature_Vector represents a vector of boolean values representing the features present in a specific device.

- Model_List is a list of product models which are valid targets for the data. An empty list can be used to indicate that the data is valid for all models. Otherwise, the device looks for its own model code in the list; if it is not present, the data will not be applied.

In an alternative embodiment, one implementation of which is illustratively shown in pseudocode in Table 2, the data itself contains special software ("checking software") to determine if the data should be applied to the device. The data, and therefore the checking software, is securely distributed in the manner described in the previous sections herein.

This checking software is not a part of the operational software used in the everyday application of the device. The additional checking software may be optional; if present, it is called by the control software which resides in the device, and it determines whether the data should be applied. The same checking software can also contain special initialization instructions to prepare the device for the new software or data contained in the data.

TABLE 2

```
--------------------------------------------------------------

If checking software present in the data then Do;
   Load checking software;
   Verify checking software is valid;
   Abort if invalid;
   Execute checking software;
   If result = "ok to load data" then Do;
       Get data;
       If data is valid
       Then load data to memory;
   Else abort
--------------------------------------------------------------
```

This embodiment is more flexible than the first embodiment since its functions are not limited to a set conceived by the initial device designers. Functions can be added with any data update, simply by changing the checking program.

In operation, this embodiment can be combined with the first embodiment. A fixed set of checking functions can be permanently stored in the device, with additional functions contained in the checking software portion of the data.

The function performed by the checking software is completely up to the designer of that software. Its functions would typically be similar to those described for the first embodiment, but could include any checking or initialization deemed necessary by the designer.

A similar approach can be used to provide optional software that would be executed immediately after the data is loaded. This could perform initialization necessary to prepare the updated device for use.

Of course, many modifications and adaptations to the present invention could be made to advantage without departing from the spirit of this invention. Further some features of the present invention could be used without corresponding use of other features. Accordingly, this description should be considered as merely illustrative of the principles of the present invention and not in limitation thereof.

Furthermore disclosed is:

1. A method of securely controlling the configuration of a computer system so that features of the system may be conveniently enabled or disabled, said method including the steps of:
providing memory which is located within a secured area which is protected from physical and direct electrical access;
executing a program which requires specific information to be stored in the memory to permit the use of specific features of the system; and
updating the specific information with data decrypted from encrypted data originating from another computer system.

2. The controlling method of item 1 including the additional steps of:
encrypting the data at the other computer system under a first key of a public key encryption system; and
decrypting the data within the secured area with a second key of the public key encryption system.

3. The controlling method of claim 22 including the additional steps of:
generating a symmetric key for use with a symmetric cryptography algorithm;
encrypting the data under the generated symmetric key;

encrypting the generated symmetric key under a first key of a public key encryption system;
transferring the encrypted data and the encrypted symmetric key to a processing system which is located within the secured area;
decrypting the received symmetric key within the secured area with a second key of the public key encryption system;
decrypting the received data within the secured area under the decrypted symmetric key with a symmetric cryptography algorithm; and
storing the decrypted data in said memory.

4. The loading method of item 3 wherein
the first key is a private key used with said public key encryption system.

5. The loading method of item 3 or 4 wherein
the second key is a public key used with said public key encryption system.

6. The controlling method of one of items 1 to 5 wherein
the executed program is included in the data originating from the other computer system.

7. The controlling method of one of items 1 to 6 wherein said specific information corresponds to at least one of the following:
serial number of the computer system;
model number of the computer system;
date of manufacture of the computer system;
version of software currently installed in the computer system; and
codes describing installed or available features.

8. The controlling method of one of items 1 to 7 wherein
the features of the system are related to software updates included in the data originating from the other computer system.

9. A method of securely controlling the enablement of data loaded in memory within a secured area of a device, said method including the steps of:
providing information within said memory representing at least one characteristic related to said device;
providing criteria information within said data to be compared with said at least one characteristic;
comparing said criteria information with said at least one characteristic; and
enabling said data to be used within said device if said at least one characteristic meets said criteria information.

10. The controlling method of item 9, wherein
at least some portion of said comparing step is performed in accordance with instructions contained within said data.

11. The controlling method of item 9 or 10, wherein
said characteristic information corresponds to at least one of the following:
serial number of the device;
model number of the device;
date of manufacture of the device;
version of software currently installed in the device; and
codes describing installed or available features.

Claims

1. A method of transferring data into a secured area, said method including the steps of:
encrypting (120) said data under a first key of a public key encryption system (24);
transferring (130) said encrypted data to a processing system which is located within said secured area;
decrypting (150) said received data within said secured area with said public key encryption system (24) under a second key; and
storing said decrypted data within said secured area.

2. The method of claim 1, wherein
said transferring data into a secured area is a loading data into at least some portion of memory which is located within said secured area, and

said secured area is protected from physical and direct electrical access, thereby guarding against undesired detection of said transferreded data.

3. A method of loading data into at least some portion of memory which is located within a secured area which is protected from physical and direct electrical access, thereby guarding against undesired detection of said loaded data, said method including the steps of:
generating (210) a symmetric key (K_S) for use with a symmetric cryptography algorithm;
encrypting (240) said data under said generated symmetric key (K_S);
encrypting (220) said generated symmetric key (K_S) under a first key of a public key (K_{PU}) encryption system;
transferring (250) said encrypted data and said encrypted symmetric key (K_S) to a processing system which is located within said secured area;
decrypting (270) said received symmetric key (K_S) within said secured area with a second key of said public key (K_{PU}) encryption system;
decrypting (280) said received data within said secured area with said decrypted symmetric key (K_S) with a symmetric cryptography algorithm; and
storing said decrypted data into said at least some portion of memory.

4. The method of one of claims 1 to 3, wherein
said first key is a private key (K_{PR}) used with said public key (K_{PU}) encryption system.

5. The method of one of claims 1 to 4, wherein
said second key is a public key (K_{PU}) used with said public key (K_{PU}) encryption system.

6. The method of one of claims 1 to 5, wherein
said public key (K_{PU}) is stored within said secured area.

7. The method of one of claims 1 to 6 further including the step of:
adding a code to said encrypted data which is to be transferred for the purpose of providing the capability of authenticating said encrypted data.

8. The method of claim 7 wherein
said code is selected from said group consisting of a digital signature, a modification detection code (MDC), and a cyclic redundancy check (CRC).

9. The method of claim 7 or 8 further including the step of:
authenticating said decrypted data; and
enabling said decrypted data to be used if said decrypted data is authentic; otherwise, not enabling said decrypted data.

10. A system for securely holding data, said system comprising:
memory means located within a secured area which is protected from physical and direct electrical access;
means for providing a public key (K_{PU}) within said secured area;
means within said secured area for receiving data encrypted by a corresponding private key (K_{PR}); and
means within said secured area for decrypting (150) said received data under said public key (K_{PU}).

11. The system of claim 10 wherein
said decrypted data provides a symmetric key (K_S).

12. The system of claim 11 including:
means within said secured area for receiving data encrypted by a symmetric algorithm under said symmetric key (K_S);
means for decrypting (280) said data under said symmetric key (K_S) provided by said decryption under said public key (K_{PU}); and
means for storing said symmetric key decrypted data in said memory means.

13. The system of one of claims 10 to 12 further including
means for analyzing a code received by said system to authenticate said data received.

14. The system of claim 13, wherein said code is selected from said group consisting of a digital signature, a modification detection code (MDC), and a cyclic redundancy check (CRC).

15. A method of securely controlling the configuration of a computer system (10) so that features of said system may be conveniently enabled or disabled, said method including the steps of:
providing memory which is located within a secured area which is protected from physical and direct electrical access;
executing a program which requires specific information to be stored in said memory to permit the use of specific features of said system; and
updating said specific information with data decrypted from encrypted data originating from another computer system.

16. A method of securely controlling the enablement of data loaded in memory within a secured area of a device, said method including the steps of:
providing information within said memory representing at least one characteristic related to said device;
providing criteria information within said data to be compared with said at least one characteristic;
comparing said criteria information with said at least one characteristic; and
enabling said data to be used within said device if said at least one characteristic meets said criteria information.

FIG. 1

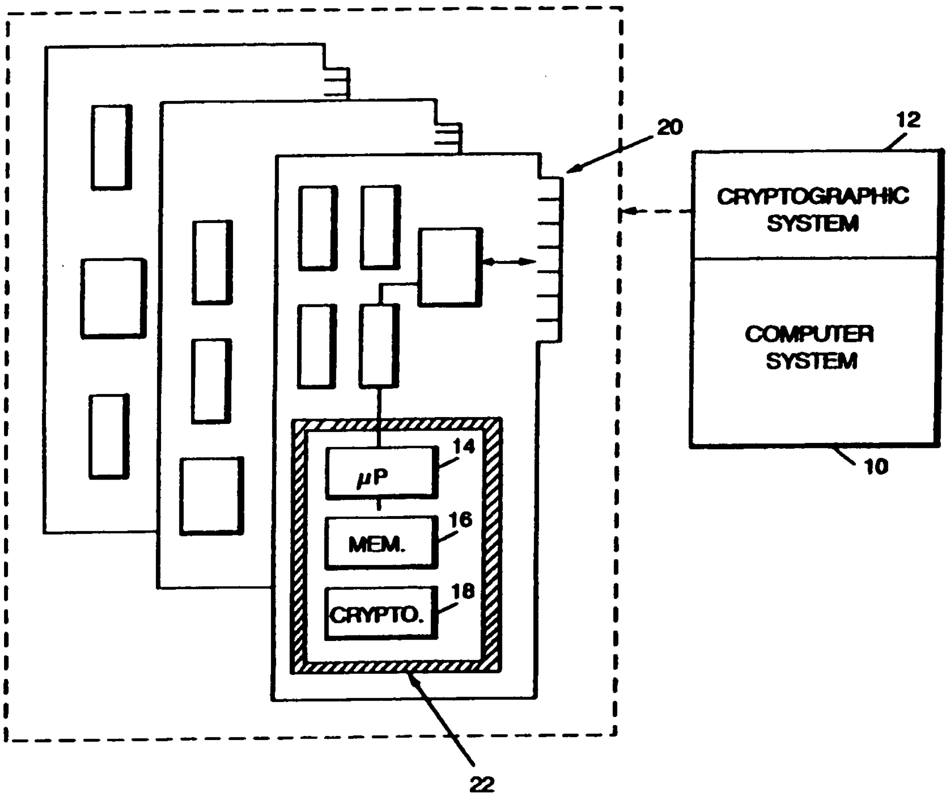

20
12
CRYPTOGRAPHIC SYSTEM
COMPUTER SYSTEM
10
14
μP
16
MEM.
18
CRYPTO.
22

FIG. 2

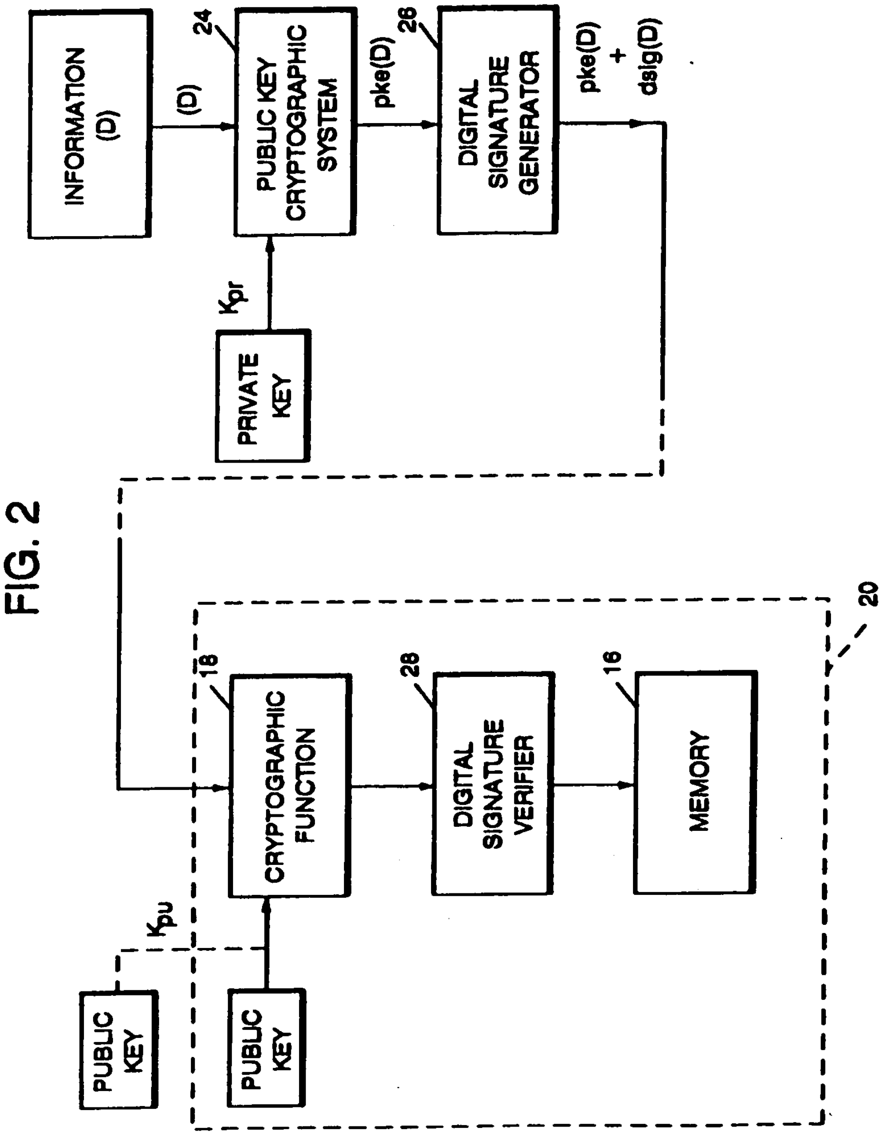
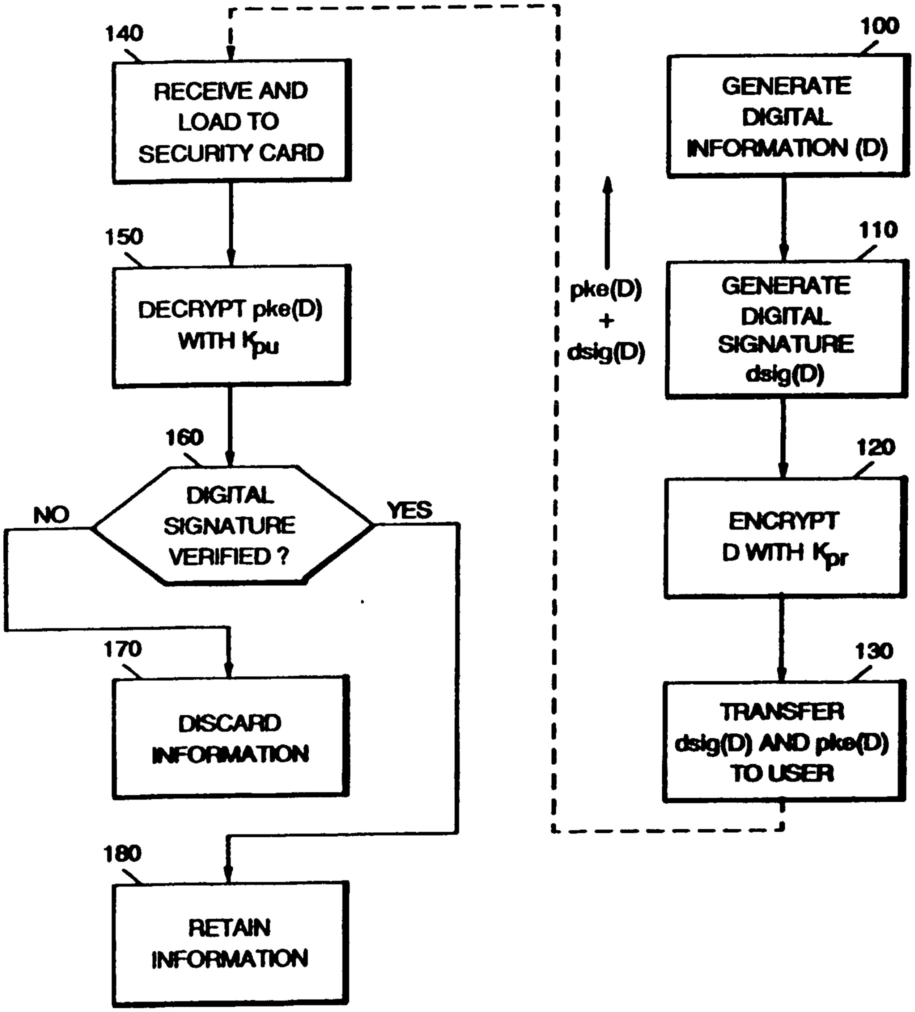

INFORMATION (D)
(D)
24
PUBLIC KEY CRYPTOGRAPHIC SYSTEM
pke(D)
26
DIGITAL SIGNATURE GENERATOR
pke(D) + dsig(D)
K_{pr}
PRIVATE KEY
18
CRYPTOGRAPHIC FUNCTION
28
DIGITAL SIGNATURE VERIFIER
16
MEMORY
20
K_{pu}
PUBLIC KEY
PUBLIC KEY

FIG. 3


140
RECEIVE AND LOAD TO SECURITY CARD
150
DECRYPT pke(D) WITH K_{pu}
160
DIGITAL SIGNATURE VERIFIED ?
NO
YES
170
DISCARD INFORMATION
180
RETAIN INFORMATION
pke(D) + dsig(D)
100
GENERATE DIGITAL INFORMATION (D)
110
GENERATE DIGITAL SIGNATURE dsig(D)
120
ENCRYPT D WITH K_{pr}
130
TRANSFER dsig(D) AND pke(D) TO USER

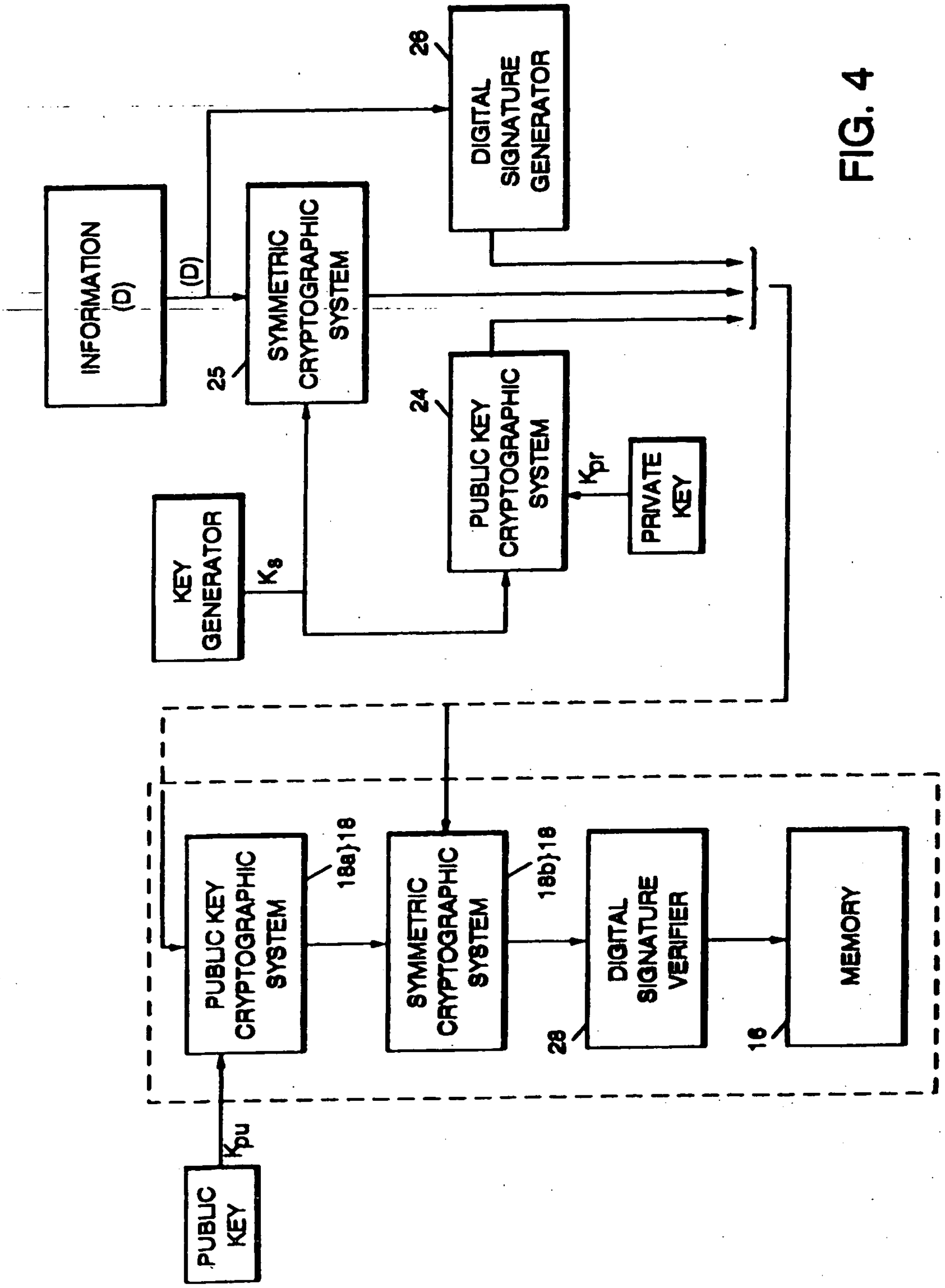

INFORMATION (D)
(D)
25
SYMMETRIC CRYPTOGRAPHIC SYSTEM
26
DIGITAL SIGNATURE GENERATOR
KEY GENERATOR
K_s
24
PUBLIC KEY CRYPTOGRAPHIC SYSTEM
K_{pr}
PRIVATE KEY
PUBLIC KEY CRYPTOGRAPHIC SYSTEM
18a}18
SYMMETRIC CRYPTOGRAPHIC SYSTEM
18b}18
28
DIGITAL SIGNATURE VERIFIER
16
MEMORY
PUBLIC KEY
K_{pu}

FIG. 4

FIG. 5

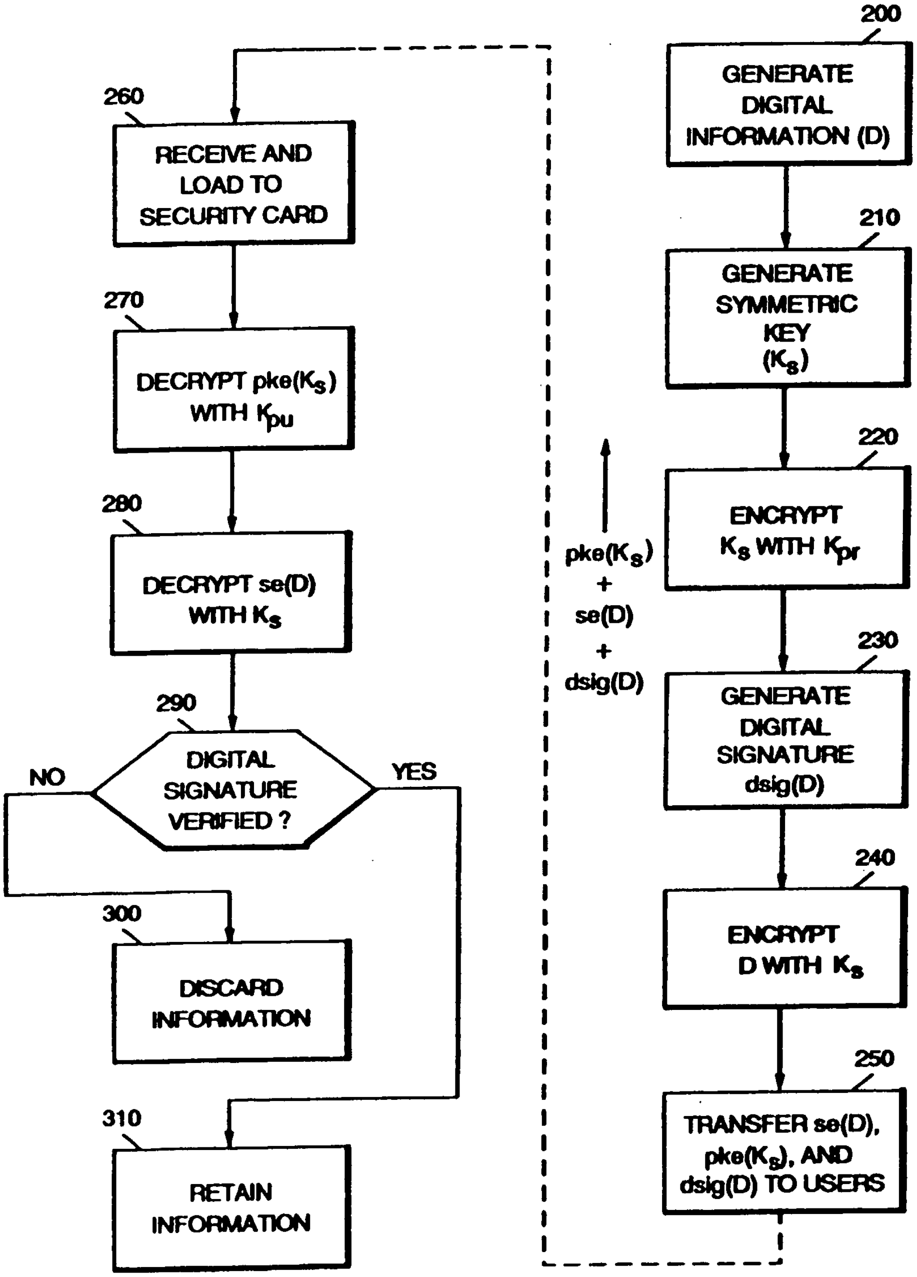
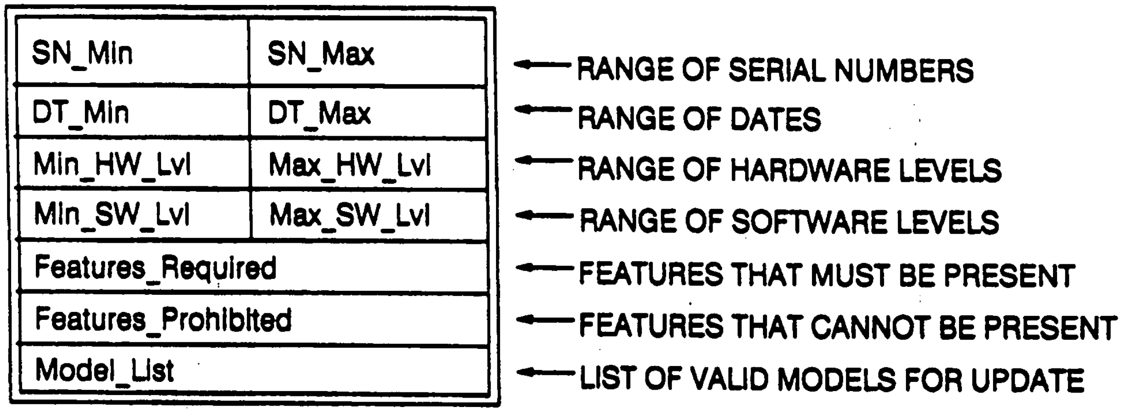

200
GENERATE DIGITAL INFORMATION (D)
210
GENERATE SYMMETRIC KEY (K_S)
220
ENCRYPT K_S WITH K_{pr}
230
GENERATE DIGITAL SIGNATURE dsig(D)
240
ENCRYPT D WITH K_S
250
TRANSFER se(D), pke(K_S), AND dsig(D) TO USERS
pke(K_S) + se(D) + dsig(D)
260
RECEIVE AND LOAD TO SECURITY CARD
270
DECRYPT pke(K_S) WITH K_{pu}
280
DECRYPT se(D) WITH K_S
290
DIGITAL SIGNATURE VERIFIED ?
NO
YES
300
DISCARD INFORMATION
310
RETAIN INFORMATION

FIG. 6



SN_Min	SN_Max	RANGE OF SERIAL NUMBERS
DT_Min	DT_Max	RANGE OF DATES
Min_HW_Lvl	Max_HW_Lvl	RANGE OF HARDWARE LEVELS
Min_SW_Lvl	Max_SW_Lvl	RANGE OF SOFTWARE LEVELS
Features_Required		FEATURES THAT MUST BE PRESENT
Features_Prohibited		FEATURES THAT CANNOT BE PRESENT
Model_List		LIST OF VALID MODELS FOR UPDATE

THIS PAGE BLANK (USPTO)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 689 325 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : 95304260.3

(51) Int. Cl.^{6} : **H04L 29/06**

(22) Date of filing : 20.06.95

(30) Priority : 22.06.94 GB 9412553

(43) Date of publication of application :
27.12.95 Bulletin 95/52

(84) Designated Contracting States :
DE ES FR GB IT

(71) Applicant : AT & T GLOBAL INFORMATION SOLUTIONS INTERNATIONAL INC.
1700 South Patterson Boulevard
Dayton, Ohio 45479 (US)

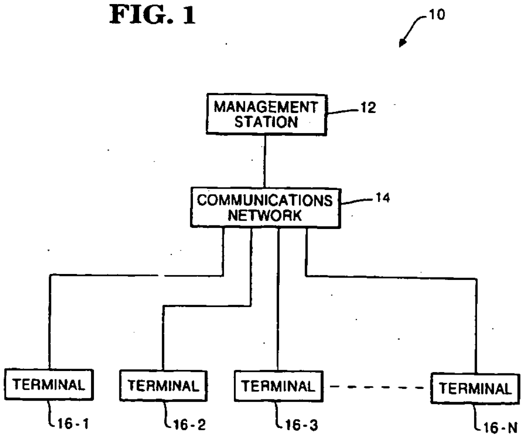
(72) Inventor : Shepherd, Bruce
5 McGill Road
Carnoustie, Angus (GB)
Inventor : McPherson, Robert P.
4 Greystaine Road
Invergowrie, Dundee (GB)

(74) Representative : Robinson, Robert George
International Patent Department,
AT&T GIS Limited,
915 High Road,
North Finchley
London N12 8QJ (GB)

(54) Method and apparatus for distributing software

(57) In a software management system, a software package held in a management station (12) is transferred across a communications network (14) to a plurality of destination terminals (16), of which there may be a large number. In order to save on distribution time, the management station (12) can cause terminals (16) which have received the software package to transmit it to further terminals, until all terminals (16) have received the package.

FIG. 1



Jouve, 18, rue Saint-Denis, 75001 PARIS

This invention relates to a method and apparatus for distributing software.

The invention has a particular application to the distribution of a software package to a plurality of terminals.

One example of a system wherein a plurality of terminals are connected to a management station is where the terminals are self-service terminals (SSTs) such as automated teller machines (ATMs). The terminals may be located at widely separated geographical locations, and are interconnected by a communications network such as a public data network, for example a network conforming to the CCITT X.25 standard. The transfer of signals over long distances via such a network may be via low speed lines and hence lengthy times may be involved in such transfer. With such a network of terminals, it is sometimes desirable that a common software package should be distributed to all the terminals in the network. Such software package may, for example, modify the manner in which the terminals operate and it is desirable that all the terminals should receive the common software package without undue delays.

It is an object of the present invention to provide a method and apparatus whereby software may be distributed to a plurality of terminals at high speed.

Therefore, according to one aspect of the present invention, there is provided a method of distributing a software package from a source station to a plurality of terminals, characterized by the steps of: transmitting said software package from said source station to at least one of said terminals; and utilizing at least one of said terminals which has received said software package to transmit said software package to another of said terminals.

According to another aspect of the present invention, there is provided a terminal system including a management station, a plurality of terminals and connection means adapted to interconnect said management station and said terminals, characterized in that said management station is adapted to transmit a software package to at least one of said terminals, and is that said management station is adapted to cause a terminal which has received said software package to transmit said software package to another of said terminals.

It will be appreciated that a method and apparatus according to the invention enable a significant saving in distribution time to be achieved by utilizing terminals which have received the software package to distribute the software package to other terminals.

One embodiment of the present invention will now be described by way of example, with reference to the accompanying drawings, in which:-

Fig. 1 is a block diagram of a terminal system including a management station and a plurality of terminals;

Fig. 2 is a simplified block diagram of the management station shown in Fig. 1;

Fig. 3 is a simplified block diagram of one of the terminals shown in Fig. 1;

Figs 4A and 4B, assembled as shown in Fig. 4, are a flowchart illustrating the operation of the management station during a software distribution operation; and

Fig. 5 is a flowchart illustrating the operation of a terminal during a software distribution operation.

Referring first to Fig. 1, there is shown a terminal system 10 including a management station 12 connected over a communications network 14 to a plurality of terminals 16, referenced individually as terminals 16-1, 16-2, 16-3 up to 16-N. In the preferred embodiment, the terminals 16 are SSTs (self-service terminals) such as ATMs (automated teller machines), adapted for operation by members of the public. Also in the preferred embodiment, the communications network 14 is a public data network to which the management station 12 and the terminals 16 are connected. The management station 12 may be a computer such as a personal computer (PC).

The management station 12 and terminals 16 transfer information in packet mode; that is, information is transferred by means of packets which pass through the communications network 14 via interfaces conforming to the CCITT X.25 standard, for example. However, other types of communications network may be utilized. It should be understood that the system 10 is a peer-to-peer system, that is, any of the terminals 16 can communicate directly with any other terminal 16, as well as with the management station 12. The number of terminals 16 in the system 10 may be quite large, for example there may be several hundred, or over one thousand terminals 16 in the system 10.

Referring now to Fig. 2, there is shown a simplified block diagram of the management station 12. The management station 12 includes a bus 20 to which are connected a processor 22, a display 24, a keyboard 26 and a memory device 28. Also connected to the bus 20 are a control software storage unit 30, which may be a part of the memory 28, and a database unit 32, the function of which will be described hereinafter. The bus 20 is also connected to a transceiver 34 which communicates with the communications network 14 over a channel 36.

Referring now to Fig. 3, there is shown a simplified block diagram of a terminal 16. The terminal 16 includes a bus 50 to which are connected a processor 52, a display 54, a keyboard 56 and a teller control unit 58 which controls the teller functions of the terminal 16, such as cash dispensing, cash receiving, document receiving and processing and the like. Also connected to the bus 50 are a memory 60 and a control software store 62, which may be physically part of the memory 60. The bus 50 is also connected to a transceiver 64 which communicates with the communications network 14 over a channel 66.

The present invention is concerned with the distribution of a common software package from the management station 12 to the terminals 16. In this connection it will be appreciated that it is desirable that such distribution should be effected with minimum delay, having regard to the delays inherent in the communications network 14, which may cover a wide geographical area, and the possibly large number of terminals 16 destined to receive the common software package.

The operation of the management station 12 during a software distribution procedure will now be described. It should first be understood that the database 32 (Fig. 2) stores a list of all the terminals 16 together with an indication of whether or not they have received the software package to be distributed. It should also be understood that the software package is initially stored in the memory 60 and is transmitted in conventional manner as a series of packets via the transceiver 34 over the communications network 14. Preferably, the management station 12 has the capability of transmitting simultaneously to a plurality of the terminals 16.

Referring now to Figs. 4A and 4B there is shown a flowchart 80 illustrating the operation of the management station 12 during a software distribution procedure. The procedure begins at the start block 82 and proceeds to block 84 where the database 32 (Fig. 2) is checked to determine whether any terminals 16 listed are without the software package. If no terminals are listed as being without the software package, the procedure terminates (block 86). If there are terminals listed as being without the software, the flowchart proceeds to block 88, where the database 32 (Fig. 2) is checked to ascertain whether any terminals are listed as having received the software package. If no, the flowchart proceeds to block 90 and a RECEIVE command is sent to a terminal 16 which does not have the software. It should be noted at this point that if the management station 12 has the necessary capability, then the RECEIVE command may be sent simultaneously to a plurality of the terminals 16. The RECEIVE command has the format

RECV (Filename)

where "Filename" identifies the software package to be distributed. The RECEIVE command conditions the terminal or terminals which receive it to receive the software package identified by its Filename. Next, (block 92) a SEND command effective in the management station 12, having the format

SEND (Filename)

causes the designated software package to be sent to the terminal (or terminals) which received the RECEIVE command. Next, the database 32 is updated to record the terminal or terminals which have just received the software package, and the flowchart returns over the line 96 to block 84.

If at block 88 it is found that there are terminals listed in the database 32 as having received the software package, then the flowchart proceeds to block 98, and a TRANSFER command is sent to one or more of the terminal 16. The TRANSFER command has the format

XFR (Filename, Destination)

where "Filename" identifies the software package and "Destination" identifies a terminal which is to receive the software package from a terminal which has received the TRANSFER command.

It should be understood that in block 98, a TRANSFER command maybe sent concurrently to a plurality of terminals 16 dependent on the capability of the management station 12. Also, of course, the TRANSFER command will only be sent to as many terminals having the software package as are needed in accordance with the number of terminals which have not yet received the software package.

The flowchart then proceeds to block 100 where it is seen that the management station 12 waits until it has received TRANSFER COMPLETE messages from the terminals having the software package which were designated to send the software package to other terminals. When this operation is completed the flowchart proceeds to block 94 where the database 32 is updated by marking the terminals which have now received the software, whereafter the flowchart returns to block 84 as shown by the line 96.

Referring now to Fig. 5, there is shown a flowchart 120 of the operation of one of the terminals 16 which is to receive a TRANSFER command from the management station 12. Such a terminal 16 can be regarded as an agent of the management station 12 for the transmission of the software package to another one of the terminals 16. The flowchart 120 commences at start block 122 and proceeds to block 124 where it is seen that the terminal receives a TRANSFER command (discussed hereinabove) from the management station 12. Next, as shown by block 126, a RECEIVE command is sent to the terminal specified in the TRANSFER command which is to receive the software package. The software package is then transferred by the agent terminal to the specified terminal (block 128). The agent terminal then sends a TRANSFER COMPLETE message to the management station 12 to advise the management station that the software package has been transmitted to the specified terminal. This terminates the agent terminal's software package transfer operation as shown at block 132.

It will be appreciated that the use of the procedure described hereinabove, wherein terminals which have received the software packages can be controlled to further distribute the software package to other terminals, enables a considerable reduction in the overall time for distributing the software package to other terminals as compared with a procedure wherein the management station itself sends the software package directly to all the terminals.

For example, assume that the management station can perform ten concurrent transmissions, and has to distribute a software package to 1000 terminals (T_0 to T_{999}). Assume also that the transmission time for one software package is one hour. Using the described procedure, the management station 12 will send the software package to the terminals T_0 to T_9 during the first hour. At the start of the second hour the management station will command terminals T_0 to T_9 to distribute to terminals T_{10} to T_{19} respectively. During the second hour terminals T_{10} to T_{19} will receive the software package from their peer terminals T_0 to T_9. During this time the management station 12 is free to distribute the software to another ten terminals (T_{20} to T_{29}). At the end of the second hour a total of 30 terminals (T_0 to T_{29}) will have received the software.

At the start of the third hour the management station 12 will command the terminals that have received the software (T_0 to T_{29}) to distribute to terminals T_{30} to T_{59} respectively. During the third hour terminals T_{30} to T_{59} will receive the software package from their peer terminals T_0 to T_{29}. During this time the management station is free to distribute the software to another ten terminals T_{60} to T_{69}. At the end of the third hour a total of 70 terminals (T_0 to T_{69}) will have received the software. The process is repeated at the end of every hour. This results in the number of terminals receiving the software being doubled every hour (i.e. 10,20,40,80,160, ... etc.) Using this method it will take only seven hours to distribute to 1000 terminals, as compared with the 100 hours it would take for the management station 12 to distribute the software packages directly to the terminals, ten at a time (since 1000/10 = 100).

Claims

1. A method of distributing a software package from a source station (12) to a plurality of terminals (16), characterized by the steps of: transmitting said software package from said source station (12) to at least one of said terminals (16); and utilizing at least one of said terminals (16) which has received said software package to transmit said software package to another of said terminals (16).

2. A method according to claim 1, characterized in that said utilizing step includes the steps of transmitting a transfer command from said source station (12) to one of said terminals (16) which has received said software package, said transfer command specifying another terminal (16) which has not received said software package; and transmitting said software package from said one of said terminals (16) to said another terminal (16).

3. A method according to claim 2, characterized by the steps of transmitting from said one of said terminals (16) which has received said package to said another terminal (16) which has not received said software package a receive command, thereby conditioning said another terminal (16) to receive said software package.

4. A method according to claim 3, characterized by the steps of maintaining at said source station (12) a list of said terminals (16), identifying which terminals (16) have and which terminals (16) have not received said software package.

5. A method according to claim 4, characterized by the steps of: transmitting to said source station (16) a transfer complete message from a terminal (16) which has completed transmission of said software package to another terminal (16), and updating said list of terminals (16).

6. A method according to any one of the preceding claims, characterized in that said step of transmitting said software package from said source station (12) includes transmitting said software package concurrently to a plurality of said terminals (16).

7. A terminal system including a management station (12), a plurality of terminals (16) and connection means (14) adapted to interconnect said management station (12) and said terminals (16), characterized in that said management station (12) is adapted to transmit a software package to at least one of said terminals (16), and is that said management station (12) is adapted to cause a terminal (16) which has received said software package to transmit said software package to another of said terminals (16).

8. A terminal network according to claim 7, characterized in that said management station includes a database (32) adapted to contain a list of said terminals (16) identifying which terminals (16) have and which terminals (16) have not, received said software package.

9. A terminal system according to claim 7 or claim 8, characterized in that said terminals (16) are self-service terminals.

10. A terminal system according to claim 9, characterized in that said self-service terminals (16) are automated teller machines.

FIG. 1

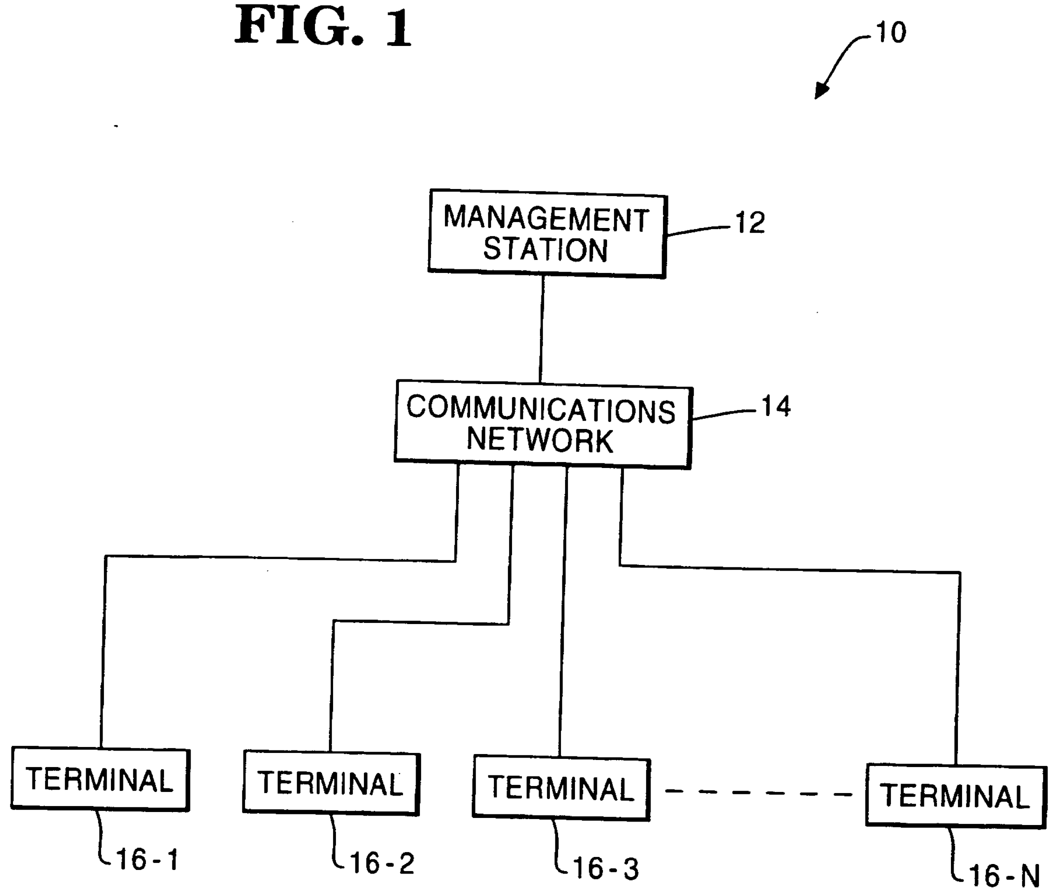

10
MANAGEMENT STATION
12
COMMUNICATIONS NETWORK
14
TERMINAL
16-1
TERMINAL
16-2
TERMINAL
16-3
TERMINAL
16-N

FIG. 2

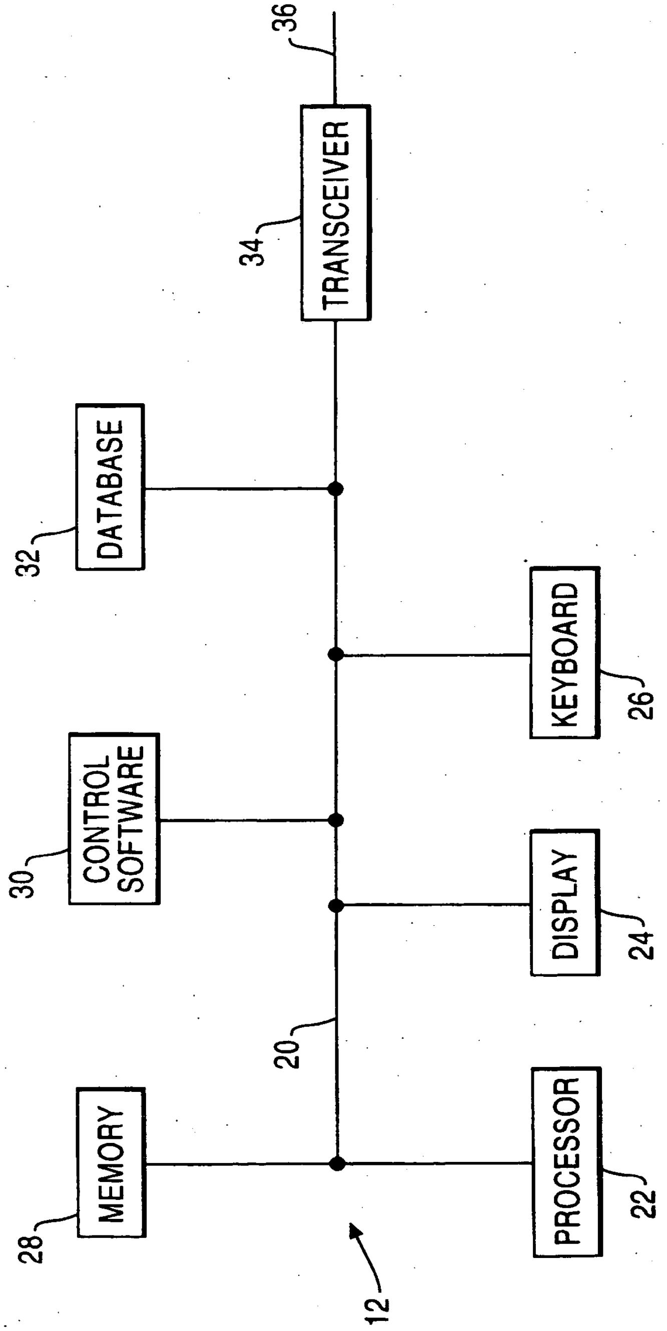

36
TRANSCEIVER
34
DATABASE
32
KEYBOARD
26
CONTROL SOFTWARE
30
DISPLAY
24
20
MEMORY
28
PROCESSOR
22
12

FIG. 3

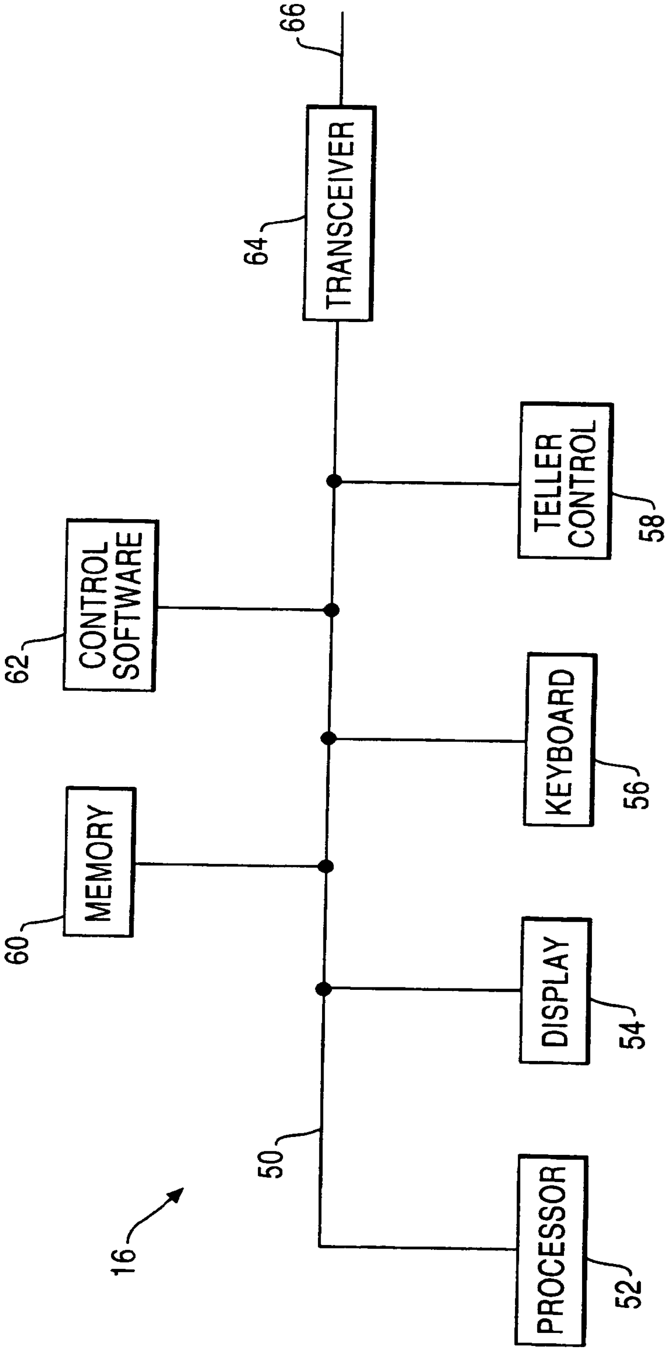

66
TRANSCEIVER
64
TELLER CONTROL
58
CONTROL SOFTWARE
62
KEYBOARD
56
MEMORY
60
DISPLAY
54
50
16
PROCESSOR
52

FIG. 4

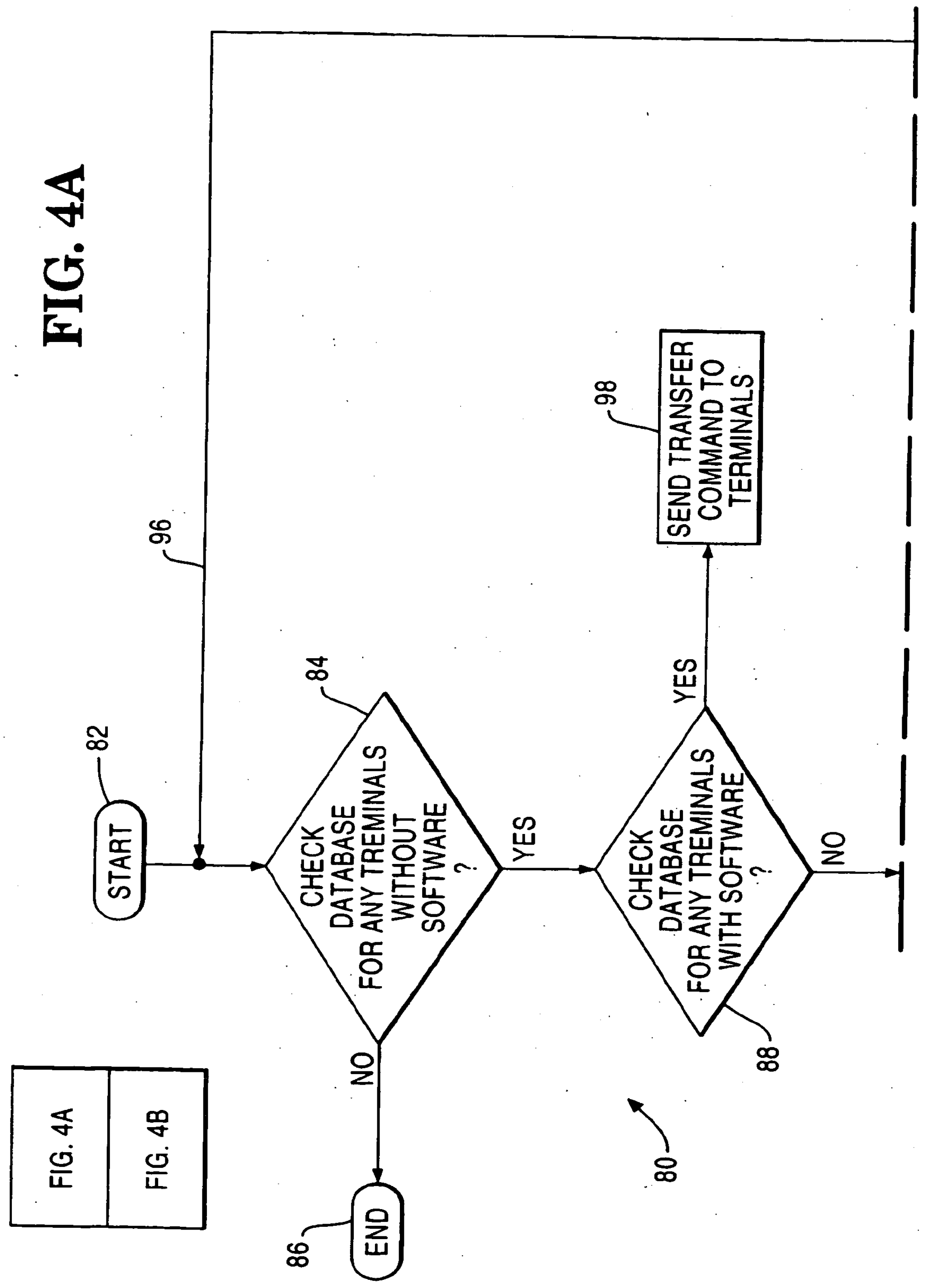


FIG. 4A
FIG. 4B
START
82
CHECK DATABASE FOR ANY TREMINALS WITHOUT SOFTWARE ?
84
YES
NO
END
86
CHECK DATABASE FOR ANY TREMINALS WITH SOFTWARE ?
88
YES
NO
SEND TRANSFER COMMAND TO TERMINALS
98
96
80

FIG. 4A

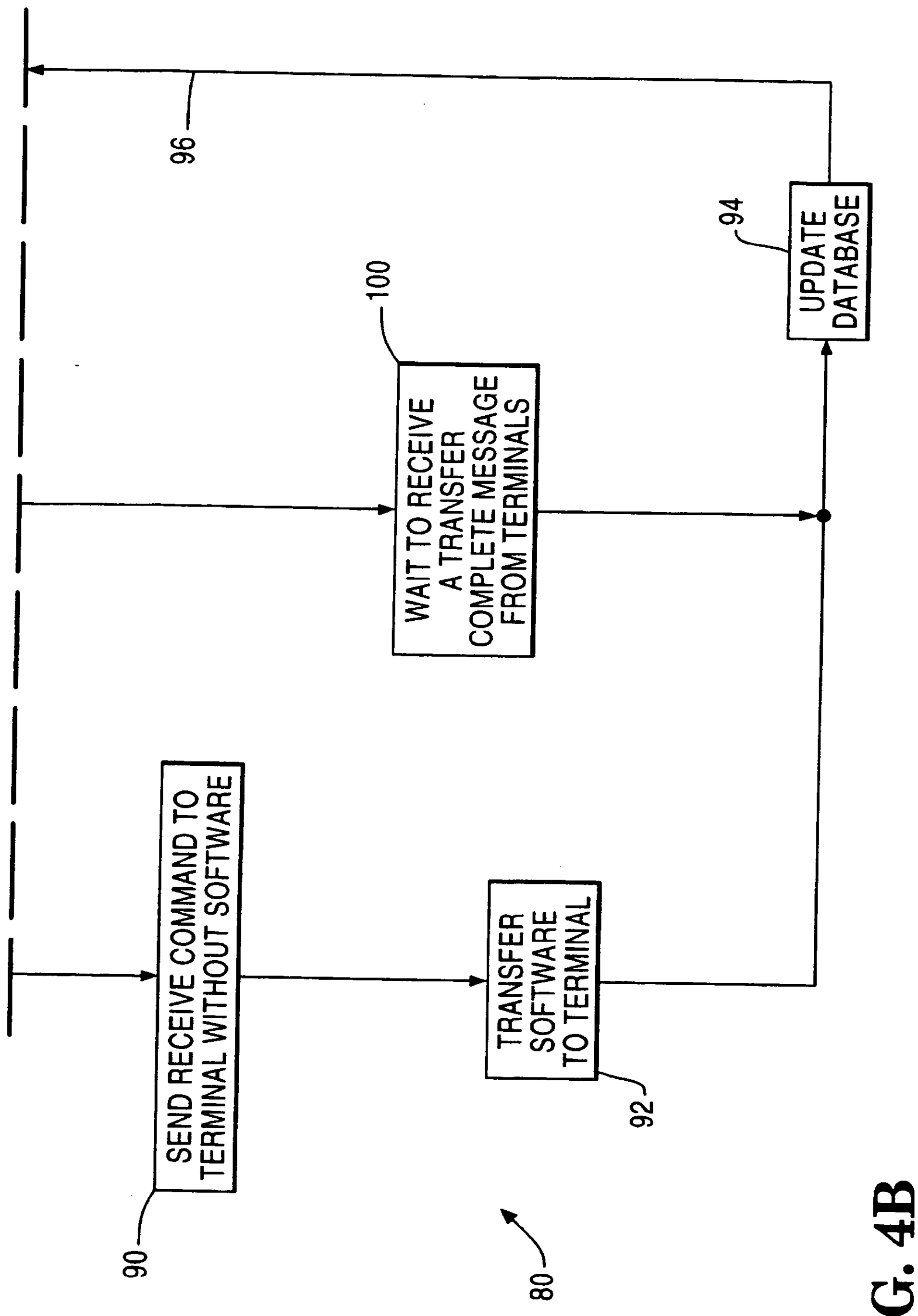
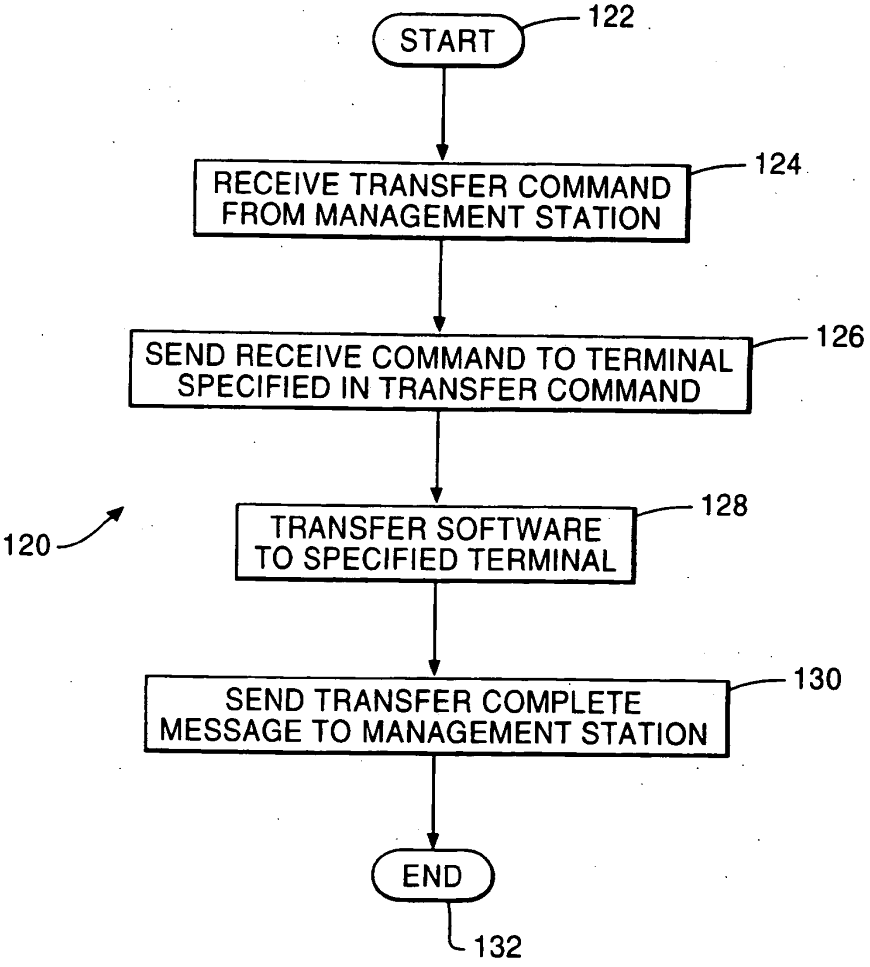

SEND RECEIVE COMMAND TO TERMINAL WITHOUT SOFTWARE
90
TRANSFER SOFTWARE TO TERMINAL
92
WAIT TO RECEIVE A TRANSFER COMPLETE MESSAGE FROM TERMINALS
100
UPDATE DATABASE
94
96
80

FIG. 4B

FIG. 5


START
122
RECEIVE TRANSFER COMMAND FROM MANAGEMENT STATION
124
SEND RECEIVE COMMAND TO TERMINAL SPECIFIED IN TRANSFER COMMAND
126
TRANSFER SOFTWARE TO SPECIFIED TERMINAL
128
120
SEND TRANSFER COMPLETE MESSAGE TO MANAGEMENT STATION
130
END
132

SHOOK, HARDY & BACON
Attn. KIRCHER, W.
One Kansas City Place
1200 Main Street
Kansas City, Missouri 64105-2118
UNITED STATES OF AMERICA

Date: 21/02/2001

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☑ BLACK BORDERS

☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

□ FADED TEXT OR DRAWING

□ BLURRED OR ILLEGIBLE TEXT OR DRAWING

□ SKEWED/SLANTED IMAGES

□ COLOR OR BLACK AND WHITE PHOTOGRAPHS

□ GRAY SCALE DOCUMENTS

☑ LINES OR MARKS ON ORIGINAL DOCUMENT

☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

□ OTHER: ______________________________

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 004 970 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
31.05.2000 Bulletin 2000/22

(51) Int. Cl.^{7}: **G06F 17/60**, G07F 17/32,
A63F 13/00

(21) Application number: 99119351.7

(22) Date of filing: 29.09.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 14.10.1998 US 172786

(71) Applicant:
International Game Technology
Reno, Nevada 89511-8986 (US)

(72) Inventors:
- Wells, Bill
Reno, Nevada 89502 (US)
- Wilder, Richard
Sparks, Nevada 89436 (US)

(74) Representative:
Manitz, Finsterwald & Partner
Postfach 22 16 11
80506 München (DE)

(54) Method for downloading data to gaming devices

(57) Memories coupled to a gaming terminal, are reprogrammed by a method and apparatus which includes identification, negotiation, downloading and verification information from an external information source to a gaming terminal. Hardware devices are used to identify gaming terminals or components.

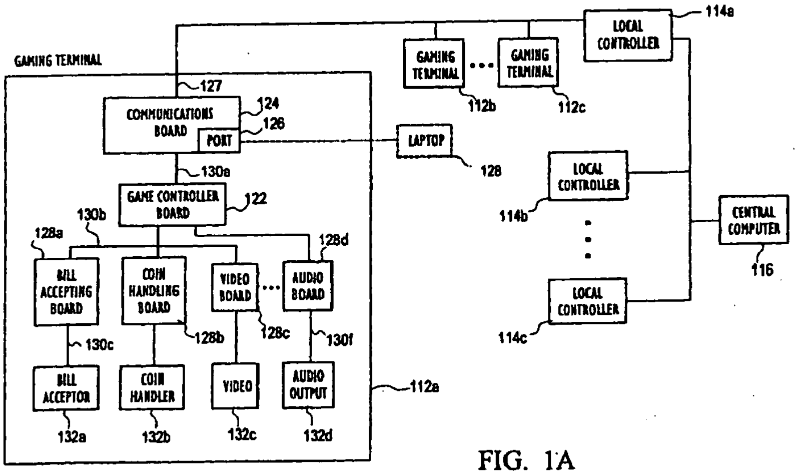


FIG. 1A

EP 1 004 970 A2

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

[0001] Cross-reference is made to U.S. Serial No. 09/088,205 (Attorney File No. 3735-905-CON) filed June 1, 1998, which is a continuation of Serial No. 08/600,311 (for "PERIPHERAL DEVICE DOWNLOAD METHOD AND APPARATUS" filed February 12, 1996), both incorporated herein by reference.

[0002] The present invention relates to a method and apparatus for downloading information to a gaming device and in particular, to a process for using a computer, directly or remotely, to transfer information to a gaming device in a secure fashion.

BACKGROUND INFORMATION

[0003] Many current gaming machines are configured with electronic components, commonly mounted on one or more printed circuit boards (PCBs). Many such electronic components use programming or other information stored in memories. In at least one typical configuration, a gaming terminal or gaming machine will include a controller board, a communications board or module, and one or more so-called peripheral boards such as a display controller board, a currency acceptor board, a coin handler board, and the like. Typically at least one board, such as the game controller board, includes a processor (e.g., a microprocessor) or other computer unit which often operates based on programming or other information (software) stored in a memory such as one or more electronically erasable programmable read-only memories (EEPROMS). Such software may be programmed or stored in the memory locations during the manufacturing or assembly of the gaming device. Additionally, software may be provided to replace or supplement the software in a gaming device which is in operation (in the field), e.g. to add new features, implement new games and the like, and/or to correct programming errors. In either case, the new software is transferred or "downloaded" from a source (which may be, e.g., a computer such as a workstation personal computer, laptop computer, and the like) to the "target" memory in a particular gaming terminal or machine.

[0004] Downloading from one computer to another is a process that is known, in general. In one previous system, information from a host system such as a state lottery host has been downloaded to a clerk validation terminal (CVT). A clerk validation terminal is used for verifying a ticket obtained from a lottery terminal e.g. to verify a validation number, amount and the like before a lottery ticket is paid, e.g. as an anti-counterfeiting procedure. However, downloading software to components of gaming devices and/or to a plurality of gaming devices or components thereof presents particular problems not readily addressed by conventional downloading techniques.

[0005] One aspect applicable to gaming devices is the stringent regulatory oversight and control exercised by regulatory authorities in many jurisdictions. In many, and perhaps all, regulated gaming jurisdictions, downloading of software to a gaming terminal will not be permitted without some assurance that the new software will comply with local regulations.

[0006] For example, a gaming regulatory authority in one jurisdiction may require assurance that downloading to, e.g., update bill acceptor software will result in a machine having bill acceptor software appropriate (and approved) for that jurisdiction (and will not, e.g., run the risk of inadvertently and/or intentionally downloading bill acceptor software that was approved in a different jurisdiction).

[0007] It is also commonly found that gaming devices occur in a wide variety of configurations, such as employing numerous different types of processors, memories, game configurations , versions and types, peripheral hardware and software and the like. Additionally, owing to differences in manufacturing dates, maintenance history and the like, gaming devices are often encountered with a wide variety of different hardware and software components which may not be apparent (or may be discernable only with difficulty) from a visual inspection of the gaming device, its components, or its operation. For this reason, when it is desired to download software to a particular gaming terminal, it is typically necessary to select a particular software version for downloading, bearing in mind the types of software and hardware found on the particular gaming terminal, lest the newly-downloaded software is incompatible with the gaming terminal or results in operation which is not approved by a particular jurisdiction. Additionally, it is possible that the software which is to be downloaded is, in fact, already present on a particular gaming terminal, so that the download process represents a waste of time and effort.

[0008] Although many types of memories can be modified to store other or additional programs (such as an erasable programmable read-only memory or EPROM), in many previous devices this was often a labor-intensive and time-consumptive procedure, sometimes involving removing the EPROM or other memory device and reprogramming it in a separate device and/or replacing it with a differently-programmed memory device. Many pin-type memory devices are configured to tolerate only a limited number of removal and insertion operations. Other memory devices are configured for solder connection or are otherwise not readily replaceable, necessitating replacement of an entire board to effect updating.

[0009] Such manual operations have, in the past, typically required a significant investment of time, especially when a relatively large number of gaming terminals are being programmed or reprogrammed. To make matters worse, the time investment is typically made by relatively highly-trained personnel. Such investment of time by relatively highly-trained personnel represents a significant expense involved in storing or updating gaming terminal programming or other information which, owing at least partly to the regulatory environment found for gaming devices, was previously believed to be a largely unavoidable cost. Furthermore, it has been found that even relatively highly-trained personnel have an undesirably high error rate when attempting to perform a download which may lead to inoperability or improper operation of a gaming device, or violation of gaming jurisdiction laws or rules and may require an additional investment of time to correct such errors.

[0010] This situation is particularly burdensome in the context of gaming devices in which it is sometimes necessary or desirable to change the programming in a large number of peripheral devices in a relatively short amount of time. One example of such a situation is when it is desired to reprogram a bill acceptor, e.g. to thwart a previously-unknown counterfeiting scheme. Previous systems which required labor-intensive and time-intensive reprogramming methods increased the risk of incurring losses during the time it took to perform this reprogramming for all the various gaming machines (e.g., in a plurality of different casinos) or their various components. An important feature of the invention is that it allows for download of data to multiple gaming devices simultaneously.

[0011] Another feature of many gaming devices which affects the manner in which revisions of software can or should be performed is the fact that gaming devices are often configured to dispense money so there is a potential for modifications or downloads to be performed in an unauthorized fashion in such a manner as to create unauthorized or improper payouts. This is a potential which is typically not present in many other types of downloads from one computer to another. Accordingly, it is important, not only to gaming regulatory authorities but also to casinos or other game operators, to achieve a level of confidence that not only will inadvertent (e.g. cross-jurisdictional) downloads be avoided but there are procedures in place to avoid or prevent intentional or unauthorized downloads.

[0012] Furthermore, previous reprogramming took place in a relatively conspicuous manner requiring personnel to access the interior of each individual peripheral and/or terminal, often for an extended period of time, thus potentially alerting the counterfeiters that they had been detected and decreasing the likelihood of using the new software to identify (possibly leading to apprehension of) the counterfeiters. In addition, the time during which a machine was being fitted with the new programs was time that the machine was out of service and not generating revenues.

[0013] In some situations, it may be advantageous to update the programming of two or more different gaming terminals and/or two or more different peripheral devices coupled to a single gaming device. Previous methods would, in this situation, typically have required separately accessing each of the gaming terminals and/or peripheral devices in order to modify or update programming.

[0014] As noted, it is often desirable to reprogram gaming terminals, e.g. to accommodate new games, regulatory changes, correct bugs or other programming errors, install new features and the like. Preferably, this should be accomplished with a minimum of down time of gaming devices (which often are intended normally to be accessible 24 hours a day) and a minimum of inconvenience to players.

[0015] Accordingly, it would be advantageous to provide a method and apparatus for downloading programming information in a manner which is less labor-intensive and less costly than previously provided, preferably without requiring individual direct access to each peripheral device which is being reprogrammed, and preferably while providing sufficient security and reliability safeguards that fully and partially automatic downloads will be permitted by gaming regulatory authorities.

SUMMARY OF THE INVENTION

[0016] The present invention provides for securely loading information, received from an external device (such as a laptop or a networked central computer) to one or more gaming devices. Preferably, the secure downloading system provides identification, negotiation, data transfer and verification features. Identification involves obtaining information for characterizing the hardware and/or software on a gaming terminal or other target. The identification information can be used to provide assurance that the programming or other data to be downloaded and/or the download procedures are appropriate for the target device. Negotiation involves providing information from the source to the target, relating to the download, such as where to load, compression information (if any) and the like. Preferably the source requests approval from the target device before data transfer begins. Preferably, data transfer is performed block-wise with checking of each block. Verification can be performed by the source requesting a digital signature calculated from the transferred data, preferably based on a public key decryption algorithm.

[0017] In one embodiment, the update or modified peripheral device program is received in the gaming terminal (or other computing device) from an external device (such as a hand-held or portable device or a central computer coupled via a communications link) and is downloaded from the gaming terminal controller board to one or mor coupled peripheral devices.

[0018] Preferably, the programming information is downloaded in such a way as to reduce or minimize the amount of down time or inconvenience to players. In one embodiment, when the new peripheral program is downloaded from a central computer to each gaming terminal, the method avoids disabling all gaming terminals at the same time, such as by waiting until the gaming terminal is idle for a predetermined period before downloading the new program to peripheral devices or by cycling through various gaming terminals or groups of gaming terminals so that a relatively small number of the gaming terminals are disabled (for reprogramming) at any one time. Additionally, the invention allows for download to multiple gaming devices or peripheral devices simultaneously.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019]

Fig. 1A is a block diagram depicting components of a multi-terminal gaming system, including components of a gaming terminal, of a type which may be used in connection with the present invention.

Fig. 1B is a block diagram of a plurality of gaming terminals, each coupled to a plurality of peripheral devices, and a central computer coupled to the gaming terminals which can be used according to an embodiment of the present invention;

Fig. 2 is a flow chart of a procedure for downloading information according to an embodiment of the present invention;

Fig. 3 is a block diagram of gaming terminals linked to a central system, usable according to an embodiment of the present invention;

Fig. 4 is a block diagram of a gaming terminal assembly and development system usable in accordance with an embodiment of the present invention; and

Fig. 5 is a flow chart depicting a download procedure in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0020] Although the present invention can be used in connection with many types of gaming terminals either as stand-alone devices or coupled in any number of different multi-terminal configurations, one example of a gaming terminal 112a coupled, along with other gaming terminals 112b,c, via one or more local controllers 114a,b,c to a central computer 116 is depicted in Fig. 1A. In the embodiment of Fig. 1A, gaming terminal 112a (and, typically, all gaming terminals in the group) includes a game controller board 122 which will typically include, among other items, a microprocessor and a memory such as an EEPROM storing programming and/or other information for controlling an operation of the controller board 122. Typically the hardware and software of the game controller board 122 will contain the information defining the type of game and making determinations of the win/loss local outcome (as opposed to, e.g., a progressive win/loss outcome) for the gaming terminal 112a. Because of the central role of the game controller board 122 in determining any monetary payout, it is particularly important to assure the presence of the correct software for the game controller board to avoid improper or incorrect payouts and to assure compliance with local regulatory authorities. Although it is possible to combine numerous functions onto a given board, typically numerous boards will be provided in a gaming terminal for forming a plurality of functions. In the depicted embodiment, the game controller board communicates with a communications board 124 which provides information to and, receives the information from a local controller 114 and/or central computer 116, for purposes such as monitoring use and performance, assuring compliance, performing accounting and similar functions, and facilitating implementation of progressive or other multi-terminal based games or prizes. In one embodiment, the communications board 124 includes one or more ports by which a laptop 128 or other computer may be coupled to the gaming terminal 112a for, among other purposes, downloading as described more fully below. In the embodiment of Fig. 1A, a plurality of peripheral boards 128 a-d communicate with the game controller board 122 and control various peripheral devices for performing various functions such as bill acceptor functions 132a, coin handling functions 132b, video functions 132c and audio output functions 132d. In many configurations, some or all of the peripheral and other boards 128 a-d, 124 will contain EEPROMs or other devices for storing software for running on microprocessors or other computing devices on such boards.

[0021] As depicted in Fig. 1B, a computing device such as one or more gaming terminals 1102a, 1102b may be coupled to various peripheral devices 1104a,b,c,d,e,f. Many types of peripheral deices can be provided, including the currency acceptor as depicted including, for example, printers, display screens or devices, keypads and the like. More than three peripheral devices may be provided, or fewer may be provided, the gaming terminal or other computing device may be housed in the same housing 1106a, 1106b as the peripheral devices 1104a-f, and more than two gaming devices may be used in connection with the download procedure. In one embodiment, download of information to the gaming terminals 1102a, 1102b is provided from a central computer 1108. However, it is possible to use the present invention in connection with stand-alone gaming terminals and peripherals which are not connected to a central computer 1108.

[0022] In the depicted embodiment, each gaming terminal includes a processor 1110a, 1110b, a memory 1112a, 1112b, and a communications module 1114a, 1114b. In the depicted embodiment, the processor 1110 is coupled to both the memory 1112 and the communications module 1114 and the memory and communications modules 1114, 1112 are coupled together to permit communication therebetween. In one embodiment, the processor 1110a is an Intel processor model 80960, although the invention can be used in connection with computing devices having other types of processors and in connection with gaming terminals which are controlled by devices other than microprocessors such as ASICS.

[0023] Following the establishment of the communication link 206, (Fig. 2) information is transferred from the information source to one or more gaming terminals. In one embodiment, if desired, the information is encrypted before being transmitted to the gaming terminal, particularly if the information is transmitted over a local area or wide area network to avoid the possibility of unscrupulous individuals gaining access to the information. Many types of data transfer can be used including serial and parallel transfer. In one embodiment, the information which is downloaded may include information within more than or different from information to be used for reprogramming the memory of one of the coupled peripherals. For example, the downloaded information may contain new programming information for two or more different peripherals coupled to a gaming terminal and/or may include information for programming the gaming terminal itself, in addition to, or rather than, one or more of the peripherals.

[0024] In the strict regulatory environment for many gaming devices, it is typically necessary to provide assurance that approved and proper software is provided in the peripheral and other boards, in addition to that provided on the game controller board.

[0025] Fig. 3 depicts an embodiment in which a network interface system 312 is used to connect a gaming terminal 112a, which may in turn be connected, such as in a daisy-chain fashion, to other gaming terminals 112b, 112c in a group, via a cluster controller 314 to a local server or controller 114. In the depicted embodiment, the gaming terminal 112a includes a central or controller (CPU) board 122 and one or more peripheral controller boards 128e, 128f. Although the present invention can be used in connection with a wide variety of systems and applications, in the depicted embodiment, while the gaming terminals 112 a-c would typically be located in a gaming area such as a gaming region of a casino, the local servers 114 and associated devices would typically be located in a casino local office 318. The local server 114 (and, in some embodiments, additional local servers for the same or other casinos) may be coupled, e.g. via modems 322a, 322b over a LAN line or wireless link 324 to a central computer 116 typically located in a central office 325 different from the local office 318 of the casino. As depicted, preferably each gaming terminal 112 also includes a port or other connector for coupling a computer such as a laptop computer 128 e.g. via a fiber-optic, cable or other connector 326. Thus, as illustrated in Figs. 1A, 1B and 3, transferring programming data or other information according to the present invention may be used in connection with transferring information from a remote location such as a central computer 116 or, in some cases, local server 114 to a gaming terminal 112. This procedure provides the desirable ability to download programs or other information to one, some, all or various combinations of the gaming machines 112a-c connected to the network, preferably substantially simultaneously, if desired. Such an ability is particularly useful when the target devices 112 may be relatively numerous, such as in the case of a casino or multi-casino network and/or when target devices are spread across a relatively wide region such as a plurality of lottery terminals. The download rates in such a system would typically be governed by the communication rates of the network or telecommunication system 324, 312. Also as depicted in Figs. 1A and 3, it is possible, in addition to or in place of downloading from a central computer or local controller, to download from a computer, such as a laptop 128, coupled directly to a gaming terminal. In one embodiment, the laptop computer 128 is coupled by a fiber-optic connection 326 directly to the game controller board 122. If the programming data or other information is intended for storing on a peripheral controller (end use device a-f) the data, in this embodiment, is channeled through the game controller board (in a pass-through mode) to the peripheral controller board, if desired. This procedure can be used, e.g., on a casino floor (for repairing or updating gaming terminal software) at a lottery location, or in the manufacturing process, such as in a final assembly stage. Preferably, such a download method does not require peripheral controllers 128a-f or other boards or components to be removed from the machine and can be used on machines that have no suitable network interface 312.

[0026] In addition to downloading programming or other information to gaming terminals or similar devices at a casino location, the present invention can also be used in connection with downloading information during a gaming terminal or similar device manufacturing process. Fig. 4 depicts a system usable in subassembly or final assembly downloading, e.g., in a gaming terminal manufacturing environment. Fig. 4 includes a plurality of computers such as workstation computers, network server computers, and/or PC-type computers coupled by network lines and a firewall 452 in a manner well-known to those of skill in computer network technologies.

[0027] At various stages in employing the system of Fig. 4, programming data or other information is stored in a number of different storage systems such as data bases (typically providing storage on hard drives or other well-known storage media). In the depicted embodiment, information, during program design process, is held in an engineering database 454. And software and firmware engineers use and modify such information via computers 456, 458 having at least indirect access to engineering database 454. Preferably, programs or other data which are still in the development phase are restricted to the engineering database 454 and are not stored in other databases. At some point, engineering will release the program or other information to product assurance 462 which, after review, will submit the programming or data to a gaming jurisdiction for approval. After the program or data is approved by the gaming jurisdiction, the program is copied to a production download server 466 and, preferably, stored in a released database 468. Information about the approved program is provided to a customer order system 472 and other systems such as engineering 474a and product assurance 474b. Although released programs may be provided in various forms such as on CD ROM 476a via a CD duplicator 476b, Fig. 4 also illustrates a system for downloading programming data or other information as part of a gaming terminal assembly or fabrication system. The programming or data may be loaded onto boards or other subassemblies 478, e.g. via a translator/power assembly 482 and download terminal 484 or may be loaded into one or more gaming terminals 486a,b, e.g. via connection to a communication board for downloading, in turn, to target peripheral devices or other subassemblies within the gaming terminals 486a, 486b, e.g. via a download terminal 488.

[0028] Downloading on the fabrication or assembly line, as depicted in Fig. 4 in the strict regulatory environment for many gaming devices, it is typically necessary to provide assurance that only approved and proper software and data is used in the gaming terminals, including peripheral and other boards (in addition to that provided on, e.g., the game controller board). Depending on the nature of the download, it will be advantageous, in performing assembly line downloading, to recognize or distinguish different boards, e.g. to obtain information regarding characteristics of the Board and/or its identity or history.

[0029] In the environment of the system of Fig. 4, a host device such as the download terminal 484 connects directly to the subassembly or through a test box 482 that provides the physical connection and power. A download terminal 488 can also be used to download information to boards which have already been assembled into gaming terminals 486a,b (which, provide physical connection and power and thus can be used for downloading without a test box 482). The host device 484, 488 can be network-connected as depicted or can be a standalone device. In a standalone configuration, the program information can be stored on a CD ROM 476a or other storage medium. The depicted download system can be used on the production floor as depicted or, at a service bench, e.g. for repair purposes. Preferably the download media 492a, 492b are configured to facilitate downloading of information (as opposed to, e.g., the components 312, 324 of a casino or multicasino system which may be configured for other purposes such as data gathering, progressive game systems and the like) and can thus be configured or optimized to achieve relatively high rates of data transfer.

[0030] In order to facilitate security in downloading information, preferably so as to achieve approval for such downloading by gaming regulatory bodies, a downloading process as depicted in Fig. 5 may be used. According to the process of Fig. 5, an initial or early stage of the process involves identification. Although it may be possible to configure gaming terminals to provide identification using only software procedures (such as by providing encrypted identification data, hand shaking procedures and the like), according to one embodiment, it is preferred to provide a gaming terminal with one or more hardware-based identification components such as one or more one-time programmable and/or add-only memory devices for storing information which identifies or characterizes the gaming terminal or components thereof. In one embodiment, a gaming identification apparatus and system can be used in accordance with that described in U.S. Patent Application Serial No. ________________ (Attorney File No. 3735-924) for "GAMING DEVICE IDENTIFICATION METHOD AND APPARATUS" filed on even date herewith and incorporated herein by reference. Providing one or more gaming terminals with such identification capability means that such gaming terminals have been placed in a "download ready" configuration according to an embodiment of the invention.

[0031] As depicted in Fig. 5, in the identification phase, the source device sends a message to the target device requesting identification information 512. When downloading is intended to download information to two or more devices, the identification (and/or the download) can be performed serially, by polling each device, or a single request addressing all target devices may be sent. If the identification response is not received 514, the system enters a failure mode and no connection is established 516. The identification response which is acceptable can include many types of information, examples of which include serial or other hardware identification numbers, manufacturing ID information or codes, manufacturer name, hardware or software revision designations, date of manufacture, installation, sale, shipping and the like, date of software revision, software file size, memory addresses and the like. Preferably, a starting address for the program to be downloaded is returned. Preferably, data integrity information such as a CRC (cyclic redundancy check) signature is returned. The identification information returned in response of the request 512 is used to verify that the information to be downloaded and/or the download procedures (such as data transfer rates) are appropriate for the hardware and software present in the target devices. For example, the returned identification information can be used to verify that the gaming jurisdiction to which the gaming terminal is subject, has approved the software which is to be downloaded, that the software which is to be downloaded is compatible with software or hardware already present in the gaming terminal and the like. If, on the basis of the identification information, it is determined that the gaming terminal already possesses the download information, the download step can be skipped.

[0032] Following the identification phase, a negotiation phase includes the sending of a negotiation message 518. The negotiation message includes information which is used to enable or facilitate the download procedure. For example, it may be necessary to inform the target device of the location or locations in memory where the downloaded information is to be stored, the size of the download file, the data transfer rate, whether any special transfer procedures such as compression, decompression, encryption, decryption and the like, are required. Preferably the negotiation message includes (or is interpreted to include) a request for a response such as an approval response, from the target device or devices. For example, waiting for approval from the target device is useful to, e.g., avoid initiating a download when there is someone currently playing the game, or when the gaming terminal is in an error mode. In one embodiment, if there are current credits on a gaming terminal, the gaming terminal is assumed to be in an actively played state. As depicted in Fig. 5, if the approval or "ready" response 522 is not received, a failure state is declared and error-handling procedures are required, such as outputting a notification to an operator and/or reinitiating the download procedure. If the ready response is received, the download phase can begin.

[0033] In the embodiment of Fig. 2, the data is transmitted in a block fashion, i.e., by transmitting a predetermined number of bits of the information (such as 1024 bits) from the source to the gaming terminal 208, and then checking for errors in the block 210. As will be well-known to those of skill in the art, other block lengths can also be used. Preferably, the data is transmitted by a serial transmission protocol. In one embodiment, verification or other checking is performed to assist in detecting data transmission or other errors. A number of well-known verification or error detection schemes can be used, such as a CRC. One type of CRC check is described in U.S. Patent Application Serial No: 08/348,268, filed November 30, 1994, for "METHOD AND APPARATUS FOR VERIFYING THE CONTENTS OF A STORAGE DEVICE" (incorporated herein by reference). These or other verification or error checking schemes can be adapted for use in the present invention in a manner that will be apparent to those of skill in the art, after understanding the present disclosure.

[0034] If there are errors detected in the block of information (using, e.g. a cyclic redundancy check error detection routine, or other error detection routines well-known to those of skill in the art), the procedure loops back 212 to retransmit the block. Preferably, after some blocks have been successfully downloaded, errors in subsequent blocks do not necessarily require reinitiating the download from the beginning but, only requires downloading, anew, those blocks which have not thus far been successfully transmitted. In one embodiment, only a limited number (e.g., 3) of the re-tries are permitted before a "total error" is declared and, e.g., the device is put out of service. At the end of each block transmission, it is determined 528 whether all blocks have been transmitted 214. If not, the procedure loops back 216 to transmit the next block. Preferably, following the CRC or other error detection for each block, an overall CRC or other error check (e.g. digital signature) is performed after all blocks have been downloaded to the gaming terminal. Thus, at the end of the first portion of the procedure 202, the entire desired information will have been transmitted, block-wise, with error detection, from the information source 108 to at least one gaming terminal 102.

[0035] After all blocks have been successfully downloaded, a verification stage is initiated by sending a message to the target device (or devices) which requests certain verification information 532. In one embodiment, the verification information is based on (such as being calculated from) information stored in the target device, and preferably including at least some of the downloaded information. For example, a CRC or other digital signature based on some or all of the downloaded information can be used. Preferably, the portion of the information which is used as the basis for calculating verification information or signature is selected in a fashion that is not readily known or predictable in advance or by unauthorized persons. For example, rather than always calculating the verification signature based on information starting from a predetermined and/or unchanging starting address, it is preferred that the verification signature be calculated from a starting address which is different for different download operations and/or different terminals. In one embodiment, the starting address is randomly selected and communicated (e.g. as part of the verification request message 532). For further promoting confidence in the verification system, it is possible to use a digital signature calculation procedure which is based on a private key value which is preferably randomly selected by the source computer and used to encrypt part of the download information. In response, the gaming terminal uses a known procedure (such as a decryption calculation procedure) to calculate the verification signature. If the calculated verification signature matches the expected verification signature, verification is considered to have been accomplished.

[0036] Upon receiving a valid verification 534, the download session can be completed. If a valid verification is not obtained, a failure is declared 538 and an error-handling procedure can be initiated e.g. to provide notification to operators and/or reinitialize the download procedure.

[0037] As will be apparent to those of skill in the art after understanding the present disclosure, the particular procedures illustrated in Fig. 5 may be modified or varied in a number of ways. For example, although it is believed a high and desirable level of security is achieved when all four phases (identification, negotiation, downloading and verification) are used, it is possible to provide for downloading procedures in which one or more of the phases is eliminated or abbreviated. For example, it would be possible to provide for a somewhat secure download procedure without including a verification step. Additionally, the download method according to the present invention is not necessarily strictly limited to the order of steps illustrated in Fig. 5. For example, it may be possible to perform some or all negotiation steps prior to some or all identification steps. Some or all of the steps or phases described in connection with Fig. 5 can be used in connection with purposes other than downloading, such as using identification and/or verification transactions to query and check loaded programs e.g. by regulatory agencies.

[0038] In light of the above description a number of advantages of the present invention can be seen. The present invention makes it feasible to reduce or eliminate the need for manual operations (such as physically visiting, and opening gaming terminals, analyzing, testing and/or replacing boards or components) in connection with program updating, replacement, modification and the like, while maintaining a high level of security and reliability. The present invention provides the ability to query a gaming terminal to obtain hardware and software information for regulatory, maintenance, repair, inventory, and similar purposes. The present invention makes it feasible to download information to one or many machines at the same time. The downloaded information may be information particularly directed to peripheral devices (such as a updating a bill acceptor program) and/or may involve changing features of a game such as upgrading or adding a bonus game or similar feature to a gaming terminal. The present invention is useful in facilitating the standardization of programming or other data across a variety of gaming terminals. The present invention provides the ability to permit local customers such as individual casinos or similar locations, to download their own customized video and/or audio files (e.g., using the security features described to provide regulators with assurance that downloading of such files will not change or result in unacceptable modifications to other features of game operation). The present invention facilitates the ability of casinos, game operators, game manufacturers and the like to obtain and maintain accurate inventories on programs and board modules in gaming machines. The present invention facilitates locating or identifying particular printed circuit boards (or particular classes or types of PCBs or other components on a casino floor). The present invention facilitates the secure and reliable automatic electronic loading of programs into machines in a manufacturing (assembly line) environment e.g. based on customer orders, with reduction or elimination of manual steps in such process. The present invention facilitates querying and verifying the presence and nature of hardware or software components thereof e.g. at the end of an assembly or fabrication process such as before shipping to customers, upon receipt, and the like. The present invention facilitates a verification of installed programs e.g. by gaming and/or lottery regulatory agencies.

[0039] Providing downloading from a central computer to individual gaming terminals has a number of advantages. The download can be easily performed on a number of gaming terminals at the same time, so that the amount of time required to perform the download for all the various gaming terminals is reduced. Further, it is not necessary to have personnel physically walk from terminal to terminal, and perform a download at each terminal, so that labor costs are also reduced.

[0040] The present invention makes it possible to provide for new or additional programming for peripheral devices in a manner which is secure, less labor intensive, less time-consumptive, and less obtrusive than previous methods. The present invention makes it possible to download the programming to a plurality of gaming terminals (or other computing devices) substantially simultaneously.

[0041] A number of variations and modifications of the invention can also be used. In addition to downloading computer program information, the invention can be used to download data such as data which defines the manner in which peripherals accept currency (or, detect counterfeiting). In addition to a central computer and a portable computer hand-held device, the information may be downloaded to the gaming terminal from other devices, such as a cluster controller. When reprogramming of two or more peripherals attached to a given gaming terminal is desired, in one embodiment, the new programming information for each peripheral to be reprogrammed is downloaded to the gaming terminal and the gaming terminal begins downloading the information to the attached peripherals preferably only after all information has been downloaded to the terminal. In this way, only a single session of downloading to the gaming terminal is needed in order to provide eventual updating of two or more coupled peripherals.

[0042] In situations in which security is a concern, such as systems in which money handling occurs (e.g., gaming terminals, lottery terminals, and the like) the information may be encrypted when it is transferred to the computing device and is decrypted either in the gaming device or in one or more peripheral devices.

[0043] Preferably the transactions are controlled and monitored automatically e.g. using an information file generated from information from firmware, mechanical, configuration, jurisdiction approvals and production bill of materials. Preferably such an information file is always encrypted, although program or other download data can be compressed and/or encrypted e.g. depending upon jurisdiction requirements. In one embodiment, the information file contains a number of fields including the filename, source directory or path, destination directory, version number or other version designator, CRC value, platform code (e.g. indicating the type of gaming terminal), target code (e.g. indicating the type of peripheral (e.g. bill validator)), agency approval(s), and game name or other game indicator.

[0044] Although the procedures and steps illustrated and described in connection with Fig. 5 are believed to provide a high level of security, it is believed that security of the entire system is particularly enhanced by the combination of the identification, especially hardware and/or memory-based identification (residing on the gaming terminal or gaming terminal components) and the procedures and steps illustrated in Fig. 5, particularly when combined with an information file as described.

[0045] In the embodiment of Fig. 1B it is possible to download the information to two or more gaming terminals 102a, 102b, substantially simultaneously. However, in some configurations, it will be necessary to suspend use of the gaming terminal during the downloading process. In this case, it may not be desirable to suspend operation of all gaming terminals at the same time. Therefore, in one embodiment information is downloaded from the central computer 108 to a first subset of the connected gaming terminals (during which time, use of that subset of gaming terminals is suspended), and following downloading to that subset of gaming terminals the first set of gaming terminals will be available for normal use, and downloading to the second subset of gaming terminals will be initiated, suspending use of the second subset of gaming terminals during downloading thereof. The process is repeated for various subsets of the gaming terminals until the information has been downloaded to all desired gaming terminals. In some situations, it may be desired to download information only to some of the connected gaming terminals. For example, if the information to be downloaded is intended to thwart passing of $10 counterfeit bills, there would be no need to download the new information to gaming terminals which are connected to currency acceptor peripherals that accept only $5 bills.

[0046] In the embodiment depicted in Fig. 1B, each gaming terminal 1102a, 1102b is coupled to a central computer 1108. The coupling may be by communication link 1124, such as a common local area network connection (e.g., Ethernet, Token Ring, LocalTalk, etc.), a wide area network and the like, using any of a variety of physical media such as cables, optical fibers, radio, infrared or other wireless links and the like. The type of communication module 1114a, 1122, which will be used depends on the type of communication link which is being used and may include, e.g., commercially-available network boards and supporting software, modems, universal asynchronous receiver/transmitter (UART) devices and the like.

[0047] As noted above, in some configurations it may be necessary to suspend operation of the gaming terminal during downloading from the information source to the gaming terminals, and/or from the gaming terminal to the peripheral. In one embodiment, the gaming terminal will provide an indication of the suspended status, so that a user will have the option to move to a different gaming terminal or to await reactivation. In one embodiment, the display 103 will provide an estimate of the amount of time before reactivation of the terminal. This estimate can be based, if desired, on an empirically-derived relationship between the average download time and the number of blocks of information to be downloaded, (or other indication of the size of the information to be downloaded).

[0048] In situations in which operation or use of the gaming terminal must be suspended while the information is being downloaded to peripherals, it may be desirable to configure the gaming terminal to wait until there is an apparent idle period on the gaming terminal before commencing downloading to a peripheral. Thus, in the procedure of Fig. 2, the gaming terminal will determine whether it has been idle for at least a predetermined minimum period (such as about one minute, 220). for example, when the gaming terminal is an electronic slot machine, the gaming terminal can use at timer circuit to determine if there has been any wager placed or any handle-pull or electronic equivalent thereof) for the predetermined period. If the gaming terminal has not been idle for at least the predetermined period, the gaming terminal will optionally wait another predetermined period 221 (such as about one minute) before testing to determine if the gaming terminal is idle. Once the gaming terminal is idle, the gaming terminal can commence procedures to transmit information to appropriate peripherals 224, preferably in a blockwise fashion, with error checking.

[0049] The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g. for achieving ease and reducing cost of implementation.

[0050] The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. Although the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g. as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended the appended claims be construed to include alternative embodiments to the extent permitted.

Claims

1. A method for downloading data from a source to a gaming device, wherein said gaming device is subject to governmental regulations, the method comprising;

   transmitting first information to said source, identifying at least a first hardware component of said gaming device;

   verifying that said data is appropriate for said at least first hardware;

   transmitting second information from said source to said gaming device describing at least a first characteristic of said download;

   transmitting third information from said gaming device to said source indicating that said gaming device is configured to receive said download;

   transmitting said data from said source to said gaming device;

   calculating a signature based at least partially on said data and transmitting said signature to said source; and

   comparing said signature with a signature available to said source.

2. A method as claimed in Claim 1 wherein said first information includes information identifying software stored on said gaming device.

3. A method as claimed in Claim 1 further comprising outputting a message when said first information indicates said data is already stored on said gaming device.

4. A method as claimed in Claim 1 wherein said gaming device includes a plurality of circuit boards, and wherein said source is coupled to a first of said circuit boards and wherein said first information identifies hardware on at least a second of said circuit boards.

5. A method as claimed in Claim 1 wherein said gaming device includes a plurality of circuit boards which contain a non-programmable memory storing hardware identification information.

6. A method, as claimed in Claim 1, wherein said data includes data for programming at least a first programmable memory chip.

7. A method, as claimed in Claim 1, wherein said step of transmitting said data from said source to said gaming device uses a serial data transmission protocol.

8. A method, as claimed in Claim 1, wherein said step of calculating a signature comprises calculating a signature based on data stored in a memory, beginning with a random address in said memory.

9. A method, as claimed in Claim 1, wherein said step of calculating a signature comprises calculating a signature using a seed value, wherein said seed value is available to both said source and said gaming terminal.

10. Apparatus for downloading data from a source to a gaming device, wherein said gaming device is subject to governmental regulations, the apparatus comprising;

    means for transmitting first information to said source, identifying at least a first hardware component of said gaming device;

    means for verifying that said data is appropriate for said at least first hardware;

    means for transmitting second information from said source to said gaming device describing at least a first characteristic of said download;

    means for transmitting third information from said gaming device to said source indicating that said gaming device is configured to receive said download;

    means for transmitting said data from said source to said gaming device;

    means for calculating a signature based at least partially on said data and transmitting said signature to said source; and

    means for comparing said signature with a signature available to said source.

11. Apparatus as claimed in Claim 10 wherein said first information includes information identifying software stored on said gaming device.

12. Apparatus as claimed in Claim 10 further comprising means for outputting a message when said first information indicates said data is already stored on

said gaming device.

13. Apparatus as claimed in Claim 10 wherein said gaming device includes a plurality of circuit boards, and wherein said source is coupled to a first of said circuit boards and wherein said first information identifies hardware on at least a second of said circuit boards.

14. Apparatus as claimed in Claim 10 wherein said gaming device includes a plurality of circuit boards which contain a non-programmable memory storing hardware identification information.

15. Apparatus, as claimed in Claim 10, wherein said data includes data for programming at least a first programmable memory chip.

16. Apparatus, as claimed in Claim 10, wherein said means for transmitting said data from said source to said gaming device uses a serial data transmission protocol.

17. Apparatus, as claimed in Claim 10, wherein said means for calculating a signature comprises means for calculating a signature based on data stored in a memory, beginning with a random address in said memory.

18. Apparatus, as claimed in Claim 10, wherein said means for calculating a signature comprises means for calculating a signature using a seed value, wherein said seed value is available to both said source and said gaming terminal.

19. Apparatus, as claimed in Claim 10, wherein said means for calculating a signature comprises means for calculating a digital signature based on data stored in memory using a public key encryption decryption algorithm.

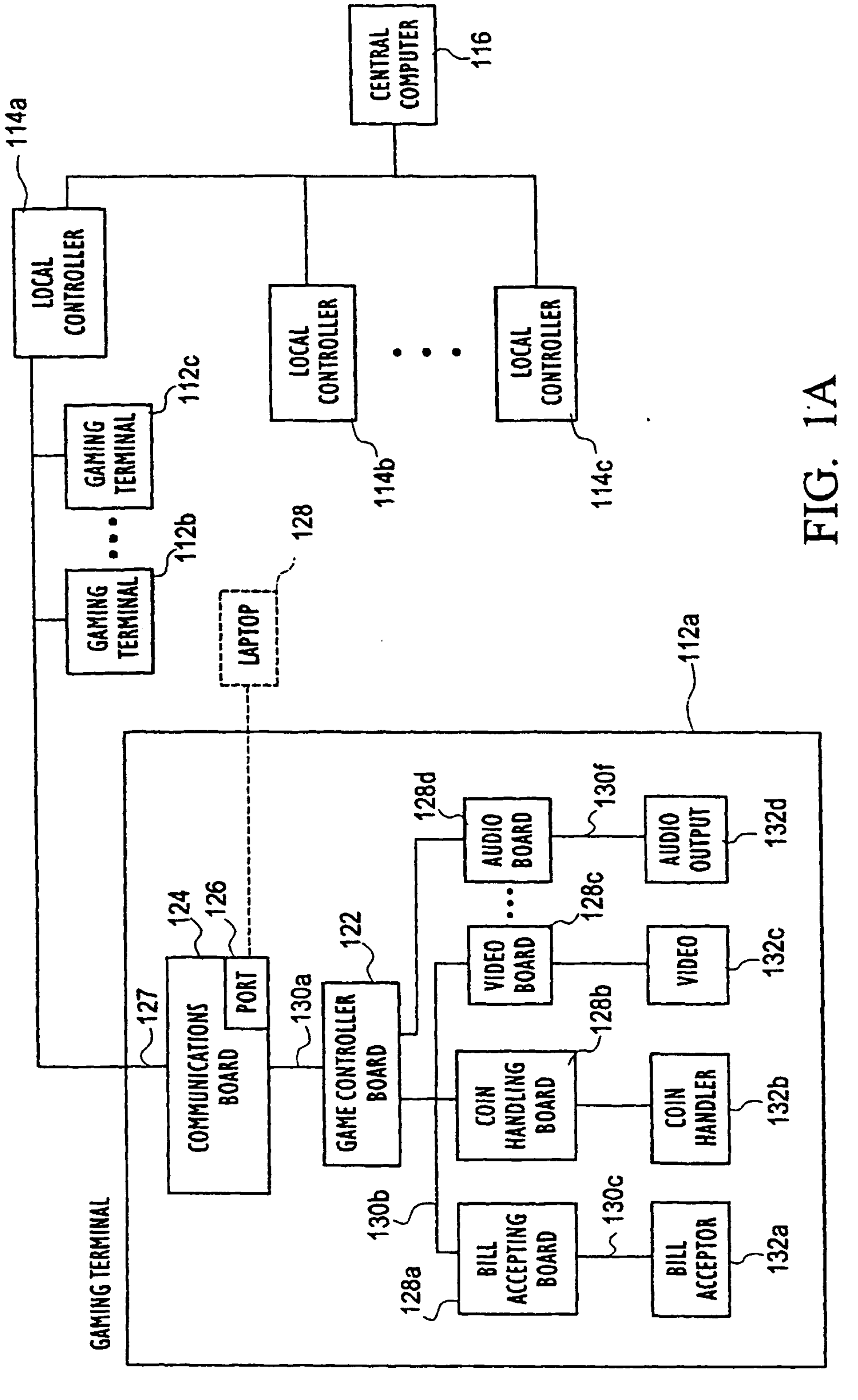

CENTRAL COMPUTER
116
114a
LOCAL CONTROLLER
LOCAL CONTROLLER
LOCAL CONTROLLER
114b
114c
GAMING TERMINAL
112c
GAMING TERMINAL
112b
LAPTOP
128
112a
GAMING TERMINAL
127
COMMUNICATIONS BOARD
124
126
PORT
130a
GAME CONTROLLER BOARD
122
128d
AUDIO BOARD
130f
AUDIO OUTPUT
132d
VIDEO BOARD
128c
VIDEO
132c
COIN HANDLING BOARD
128b
COIN HANDLER
132b
130b
BILL ACCEPTING BOARD
128a
130c
BILL ACCEPTOR
132a

FIG. 1A

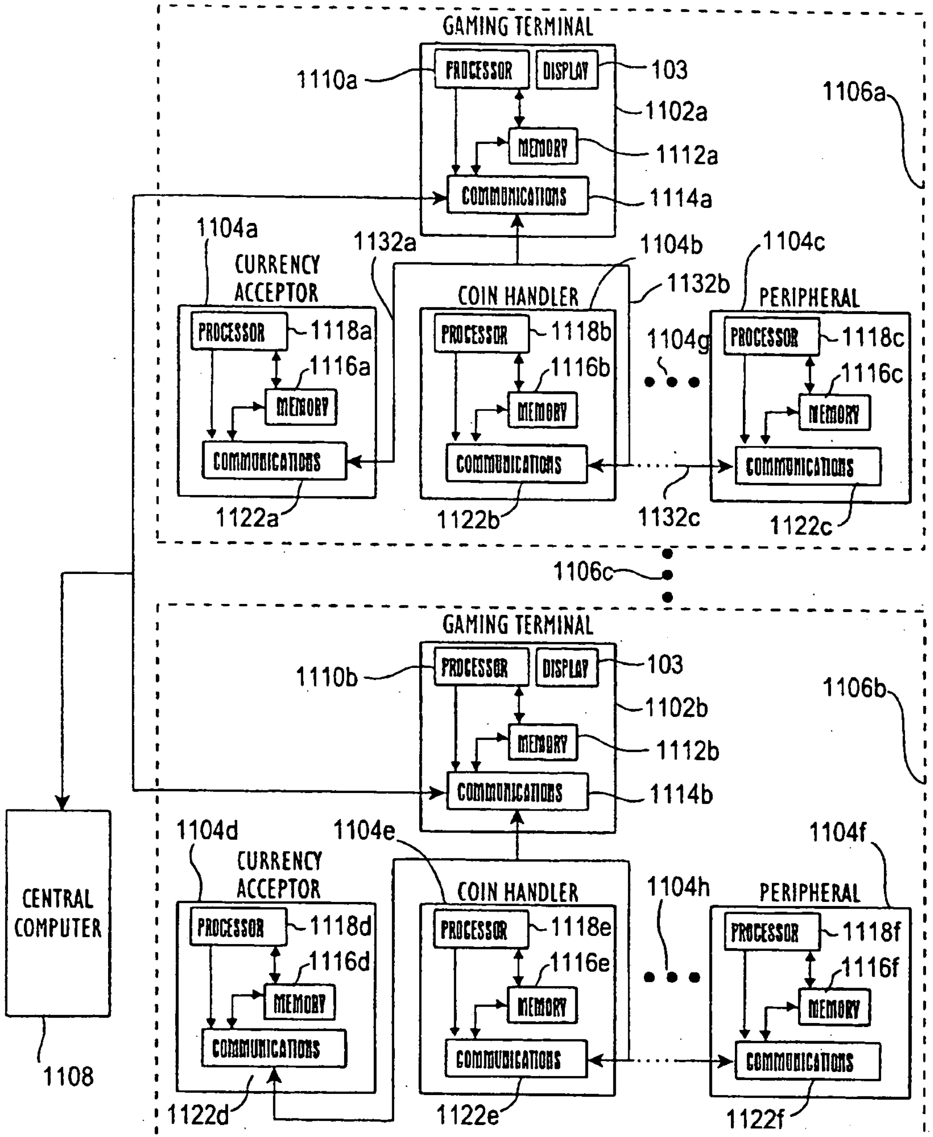

GAMING TERMINAL
PROCESSOR
DISPLAY
103
1110a
1102a
1106a
MEMORY
1112a
COMMUNICATIONS
1114a
1104a
CURRENCY ACCEPTOR
1132a
1104b
1104c
COIN HANDLER
1132b
PERIPHERAL
PROCESSOR
1118a
1116a
MEMORY
COMMUNICATIONS
1122a
1118b
1116b
1104g
1118c
1116c
1122b
1132c
1122c
1106c
GAMING TERMINAL
PROCESSOR
DISPLAY
103
1110b
1102b
1106b
MEMORY
1112b
COMMUNICATIONS
1114b
CENTRAL COMPUTER
1108
1104d
1104e
CURRENCY ACCEPTOR
COIN HANDLER
1104h
1104f
PERIPHERAL
1118d
1116d
1118e
1116e
1118f
1116f
1122d
1122e
1122f

FIG. 1B

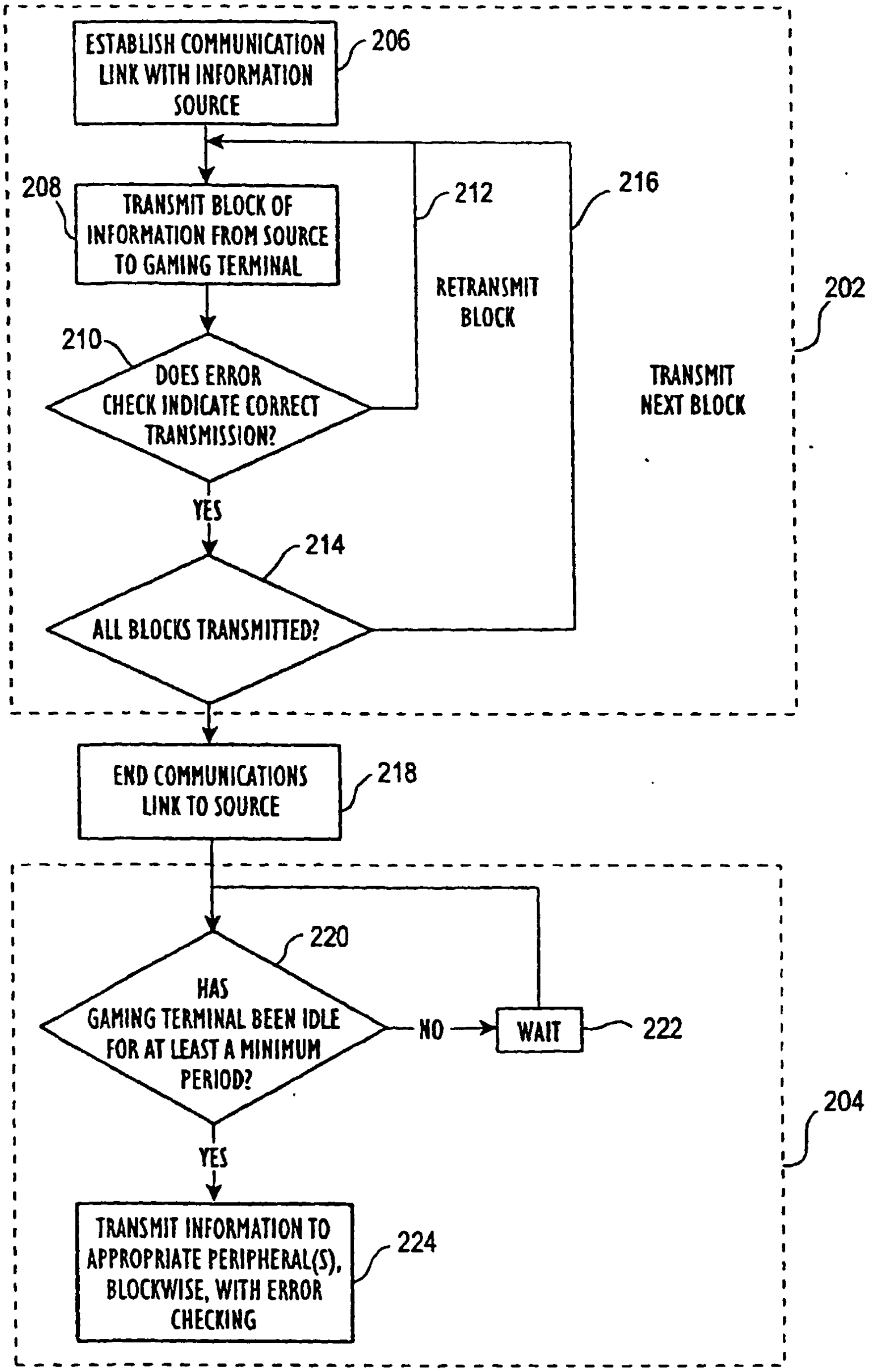

ESTABLISH COMMUNICATION LINK WITH INFORMATION SOURCE
206
208
TRANSMIT BLOCK OF INFORMATION FROM SOURCE TO GAMING TERMINAL
212
216
RETRANSMIT BLOCK
202
210
DOES ERROR CHECK INDICATE CORRECT TRANSMISSION?
TRANSMIT NEXT BLOCK
YES
214
ALL BLOCKS TRANSMITTED?
END COMMUNICATIONS LINK TO SOURCE
218
220
HAS GAMING TERMINAL BEEN IDLE FOR AT LEAST A MINIMUM PERIOD?
NO
WAIT
222
204
YES
TRANSMIT INFORMATION TO APPROPRIATE PERIPHERAL(S), BLOCKWISE, WITH ERROR CHECKING
224

FIG. 2

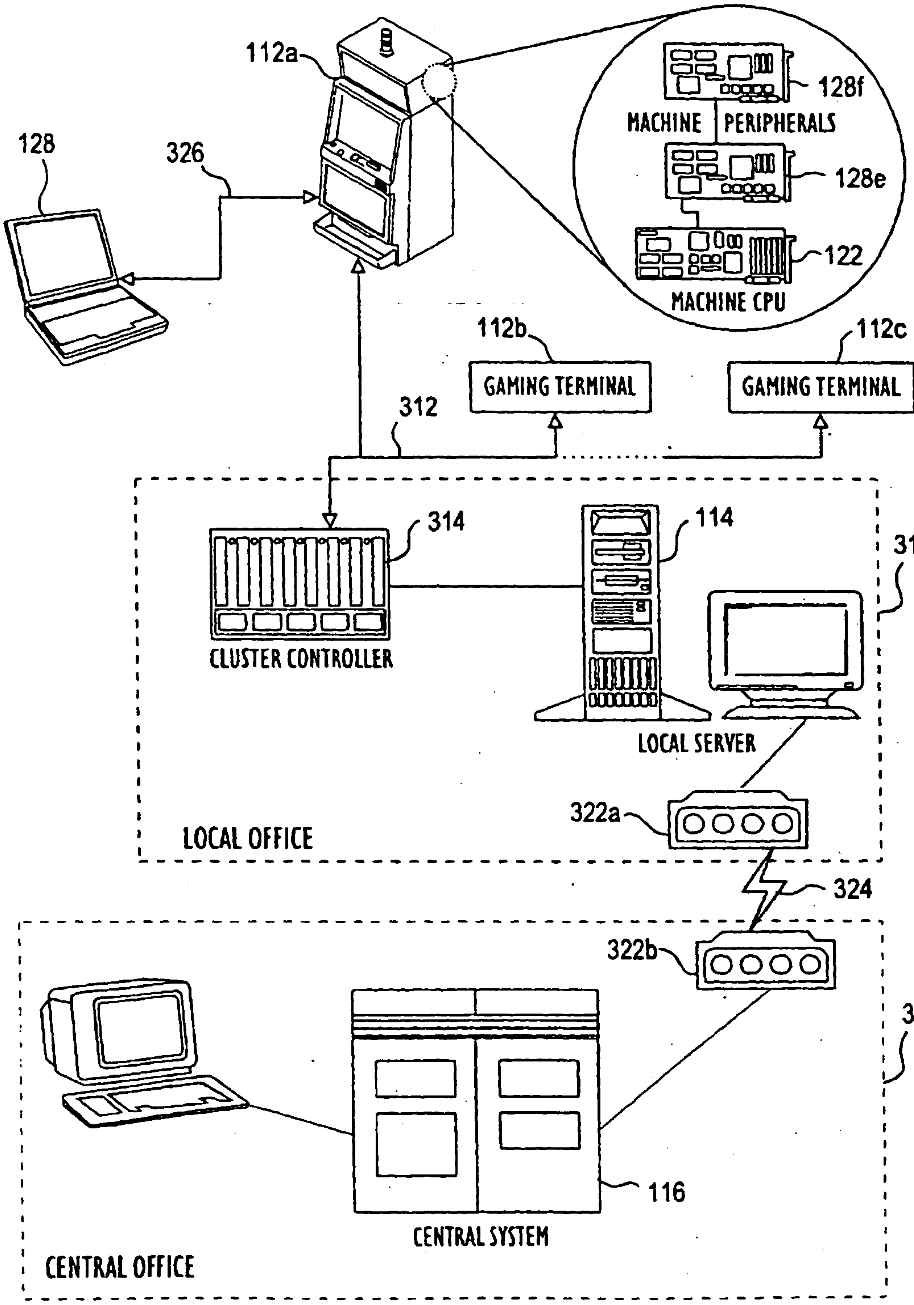
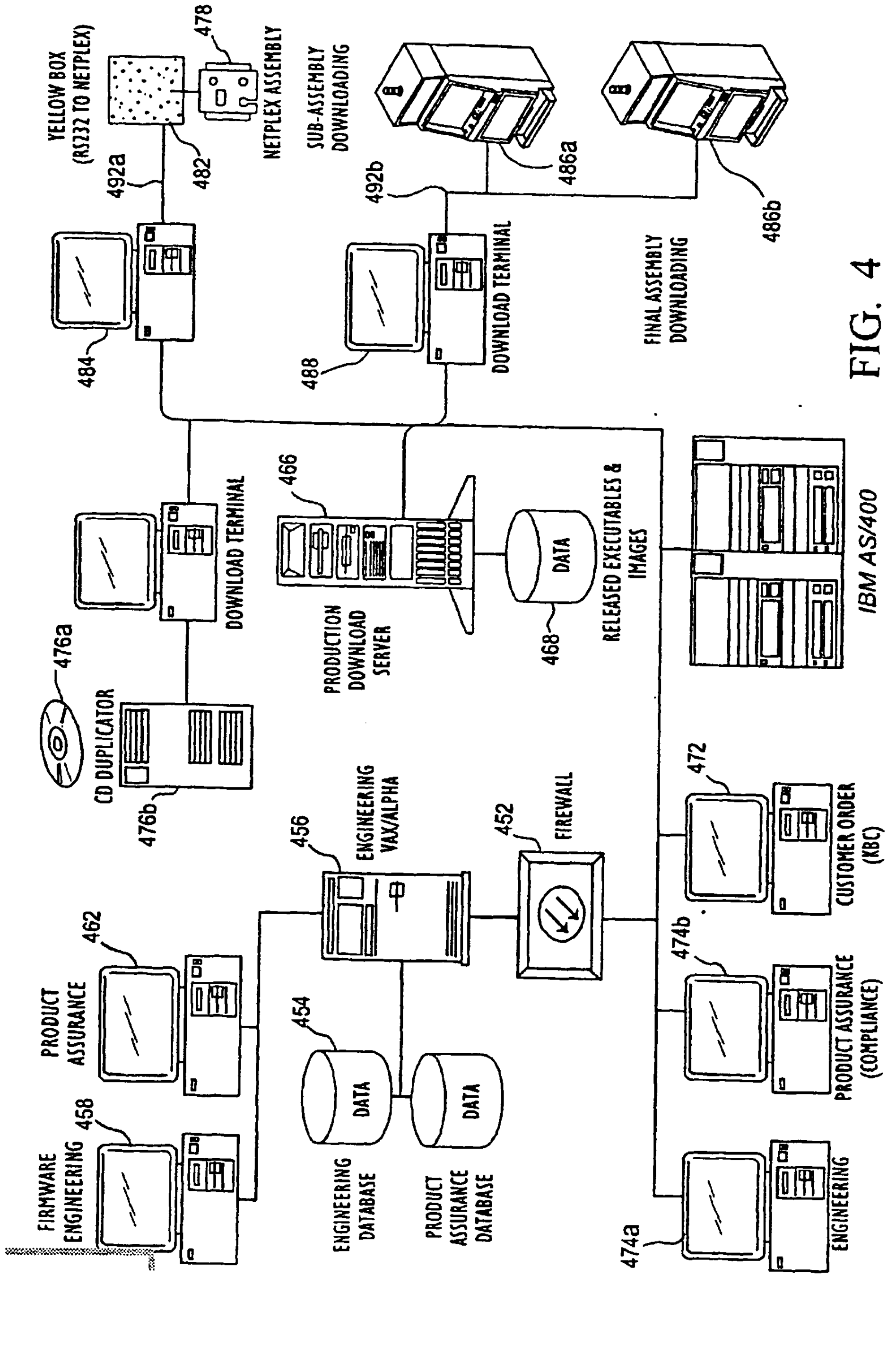

112a
128f
MACHINE
PERIPHERALS
128e
122
MACHINE CPU
128
326
112b
GAMING TERMINAL
112c
GAMING TERMINAL
312
314
114
318
CLUSTER CONTROLLER
LOCAL SERVER
322a
LOCAL OFFICE
324
322b
325
116
CENTRAL SYSTEM
CENTRAL OFFICE

FIG. 3



FIRMWARE ENGINEERING
458
PRODUCT ASSURANCE
462
ENGINEERING DATABASE
454
PRODUCT ASSURANCE DATABASE
DATA
DATA
456
ENGINEERING VAX/ALPHA
452
FIREWALL
474a
ENGINEERING
474b
PRODUCT ASSURANCE (COMPLIANCE)
472
CUSTOMER ORDER (KBC)
476b
CD DUPLICATOR
476a
DOWNLOAD TERMINAL
PRODUCTION DOWNLOAD SERVER
466
468
DATA
RELEASED EXECUTABLES & IMAGES
IBM AS/400
484
492a
YELLOW BOX (RS232 TO NETPLEX)
482
478
NETPLEX ASSEMBLY
488
DOWNLOAD TERMINAL
492b
SUB-ASSEMBLY DOWNLOADING
486a
FINAL ASSEMBLY DOWNLOADING
486b

FIG. 4

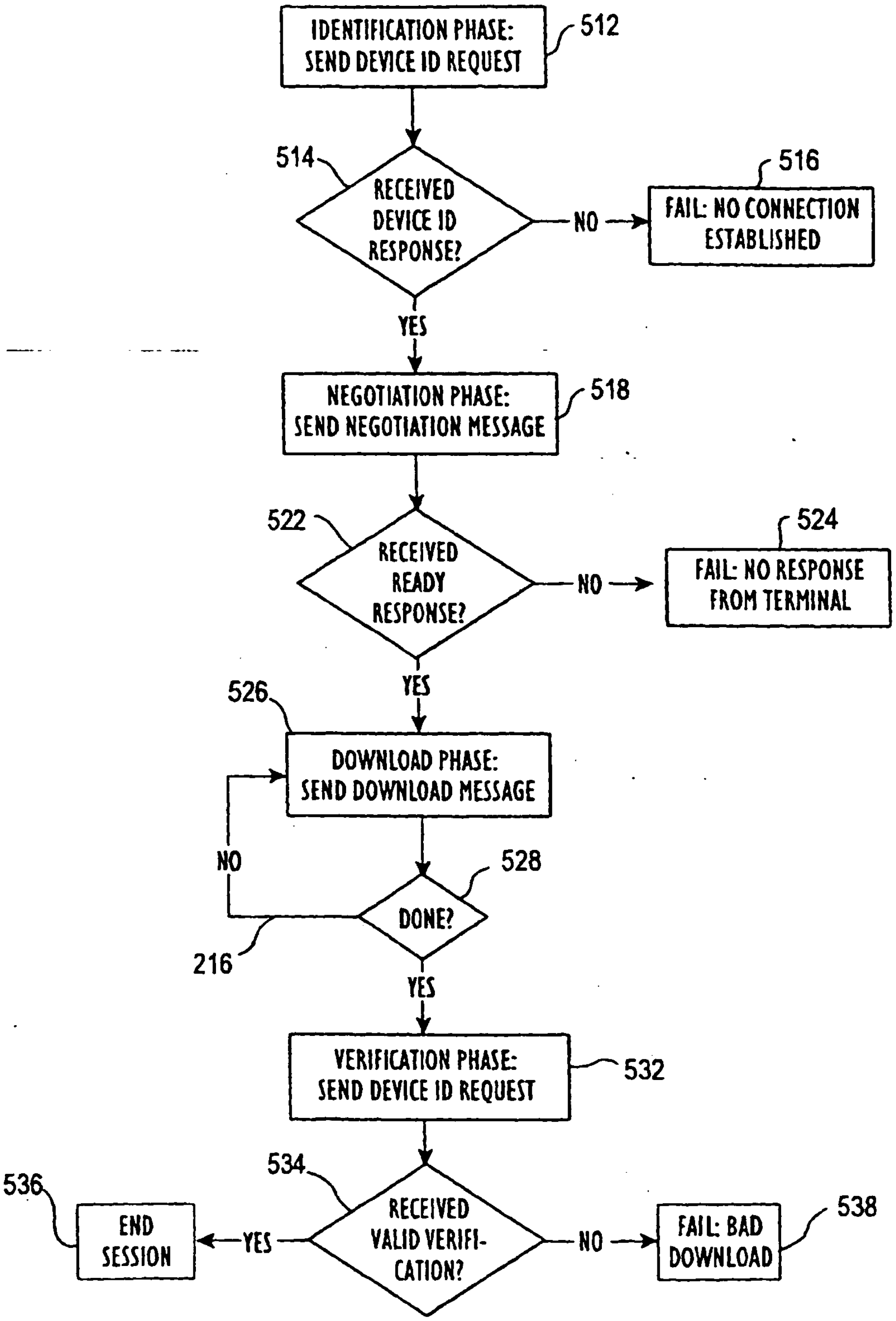

IDENTIFICATION PHASE: SEND DEVICE ID REQUEST
512
514
RECEIVED DEVICE ID RESPONSE?
NO
516
FAIL: NO CONNECTION ESTABLISHED
YES
NEGOTIATION PHASE: SEND NEGOTIATION MESSAGE
518
522
RECEIVED READY RESPONSE?
NO
524
FAIL: NO RESPONSE FROM TERMINAL
YES
526
DOWNLOAD PHASE: SEND DOWNLOAD MESSAGE
NO
528
DONE?
216
YES
VERIFICATION PHASE: SEND DEVICE ID REQUEST
532
534
536
END SESSION
YES
RECEIVED VALID VERIFI-CATION?
NO
FAIL: BAD DOWNLOAD
538

FIG. 5

ıhiS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen, et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: Secured Virtual Network in a Gaming Environment

Attorney Docket No.: IGT1P034X1/P-277 CIP

Examiner: Christopher Revak

Group: 2131

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on October 17, 2005 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Chereyce R. Brown
Chereyce R. Brown

INFORMATION DISCLOSURE STATEMENT 37 CFR §§1.56 AND 1.97(b)

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO Form 1449 may be material to examination of the above-identified patent application. Applicants submit the list of these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application. The above-identified application is a Continuation-in-part of prior application U.S. Patent Application No. 09/732,650. This prior application is being relied upon for an earlier filing date under 35 U.S.C. § 120. Because the listed references were either cited by the PTO, or submitted to the PTO in the prior application, under 37 CFR § 1.98(d) Applicants submit that copies need not be provided.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is: (i) filed within three (3) months of the filing date of the above-referenced application, (ii) believed to be filed before the mailing date of a first Office Action on the merits, or (iii) believed to be filed before the mailing of a first Office

Action after the filing of a Request for Continued Examination under §1.114. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1/P-277CIP Applicant: Nguyen, et al. Filing Date April 3, 2002	Application No.: 10/116,424 Group 2131

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	5,671,412	9/23/1997	Christiano			7/28/1995
	A2	5,715,403	2/3/1998	Stefik			11/23/1994
	A3	5,925,127	7/20/1999	Ahmad			4/9/1997
	A4	6,052,512	4/18/2000	Peterson, et al.			12/22/1997
	A5	6,125,185	9/26/2000	Boesch			5/27/1997
	A6	6,169,976	1/2/2001	Colosso			7/2/1998

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	B1							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	C1	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IFW 2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277 CIP

Examiner: Christopher A. Revak

Group: 2131

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on November 7, 2005 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Chereyce R. Brown
Chereyce R. Brown

REQUEST FOR STATUS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby requests status of the above-referenced patent application. This application was filed on April 3, 2002 and no response has been received as of this date.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100

	Type	L #	Hits	Search Text	DBs	Time Stamp
1	BRS	L1	152220	(authent$7 or author$7 or validat$3 or verif$7)with(device or console or component or machine or terminal or kiosk or client or server)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2005/12/15 08:40
2	BRS	L2	3380	1 with(game or gaming)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2005/12/15 08:40
3	BRS	L3	1267923	(transfer$4 or updat$3 or upgrad$3 or install$5 or renew$3)with(device or console or component or machine or terminal or kiosk or client or server)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2005/12/15 08:41
4	BRS	L4	566	2 same 3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2005/12/15 08:41

	Type	L #	Hits	Search Text	DBs	Time Stamp
5	BRS	L5	8259	(463/1,29 or 726/1,2,3,4,14,15 or 713/168,176 or 380/251,282,285 or 705/50,51,52,55,56,59).ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2005/12/15 08:43
6	BRS	L6	83	4 and 5	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2005/12/15 08:43

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

22434 7590 02/08/2006

BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/116,424	**Applicant(s)** NGUYEN ET AL.
	Examiner Christopher A. Revak	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-136* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-136* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 April 2002* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *see attached*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements submitted are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-136 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells et al, U.S. Patent 6,805,634 in view of Alcorn et al, U.S. Patent 5,643,086.

As per claims 1,28,52,65,73-75,77,84,103, and 123-125, it is taught by Wells et al of a software authorization agent that receives a gaming software transaction request from a first gaming device and authenticates the identity of the first gaming device. The gaming software includes a game of chance played on a gaming machine (col. 3, lines 48-60 and col. 8, lines 5-11). The teachings of Wells et al fail to disclose a transaction record used to facilitate transfer of the gaming software between two gaming devices whereby a gaming software transaction record is generated that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device. The teachings of Alcorn et al disclose of a transaction record used to facilitate transfer of the gaming software between two gaming devices whereby a gaming software transaction record is generated that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device (col. 3, lines 13-20 & 34-57). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply the secure transfer of gaming software from one device to another so that the integrity of the gaming software would be maintained. The teachings of Alcorn et al recite of motivational benefits for applying transaction records by disclosing that tampering with the contents of the gaming software can be detected and prevented (col. 3, lines 22-33). It is obvious that the teachings of Wells et al would have been further improved by ensuring that the gaming software was not maliciously altered during transfer as is disclosed by Alcorn et al.

As per claims 2,24,30,48,72,93,116, and 133, the teachings of Wells et al discloses that the game of chance is one that is in casinos (col. 8, lines 5-11) which is interpreted by the examiner as being games such as video slot games, video blackjack, or mechanical slot games.

As per claims 3,29,38-40,78,79,95-98,109,110,113-115,129-132, the teachings of Wells et al disclose that the first gaming device is a game server, the second device is a gaming machine, and a third gaming device is a portable device (col. 4, lines 10-12).

As per claims 4,7-10,15,17,18,32,33,43,53,68,81,85,86,89, and 100, it is disclosed by the combination of Wells et al and Alcorn et al that the gaming software transaction includes access information and gaming software identification information whereby the gaming software identification information in the gaming software transaction request is compared with the gaming software identification information stored in a database to see if they match and the request is denied if they do not match (Wells col. 3, lines 48-60 and Alcorn col. 3, lines 13-20 and col. 4, lines 45-48). Please refer above for the motivation of applying the teachings of Alcorn et al to the teachings of Wells et al.

As per claims 5,69, and 90, it is disclosed by Wells et al that the access information is machine identification for the first gaming device (col. 3, lines 53-55).

As per claims 6,70,91,111,120, and 134, Wells et al teaches that the gaming software identification information includes gaming software titles (col. 8, lines 5-11 & 44-51).

As per claims 11 and 12, it is disclosed by the combination of Wells et al and Alcorn et al of generating a identification sequence, encrypting the identification sequence with a public key for the first gaming device wherein information is encrypted with the public encryption key is decrypted with a private encryption key used by the first gaming device and sending the encrypted identification sequence to the first gaming device whereby the identification sequence is a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device (Wells col. 3, lines 48-67, col. 10, lines 18-28 and Alcorn col. 2, lines 42-65). Please refer above for the motivation of applying the teachings of Alcorn et al to the teachings of Wells et al.

As per claims 13 and 14, the combined teachings of Wells et al and Alcorn et al are relied upon for disclosing of receiving a second identification sequence encrypted with a public encryption key used by the software authorization agent, decrypting the second identification sequence with a private encryption key corresponding to the public encryption key used by the software authorization agent and comparing the second identification sequence to the identification sequence sent to the first gaming device to authenticate the identity of the first gaming device whereby the identification sequence is a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device (Wells col. 3, lines 48-67, col. 10, lines 18-28 and Alcorn col. 2, lines 42-65). Please refer above for the motivation of applying the teachings of Alcorn et al to the teachings of Wells et al.

As per claims 16,19,31,56,71,92, and 105, Wells et al discloses that the transaction information includes machine identification numbers (col. 8, lines 36-51).

As per claim 20, it is taught by Wells et al of sending a notification message to a gaming software provider identified in the gaming software request of a pending gaming software download request (col. 8, lines 36-51).

As per claims 21,41,66,87,117, and 127, it is disclosed by Wells et al that the software authorization agent communicates with the first gaming device using a local area network connection (col. 12, lines 52-59).

As per claims 22,42,67,88,118, and 128, Wells et al teaches that the software authorization agent communicates with the first gaming device using RF communication connections (col. 12, lines 52-59).

As per claims 23,47,80,99, and 119, Wells et al teaches that the transfer of gaming software is performed electronically (col. 4, lines 1-7).

As per claims 25,49,82,101,121, and 135, Wells et al discloses that the gaming software is used to upgrade a gaming software component on the first gaming device (col. 4, lines 1-7).

As per claims 26,50,83,102,122, and 136, Wells et al teaches that gaming software is used to correct an error in a gaming software component on the second gaming device (col. 12, lines 10-16).

As per claims 27 and 51, it is disclosed by Wells et al of a listing of gaming software titles installed on a gaming device (col. 8, lines 5-11).

As per claims 34 and 35, it is disclosed by Wells et al of decrypting the download request message and receiving a first download acknowledgement message from the first gaming device and receiving a second download acknowledgement message from the second gaming device (col. 3, lines 48-67 and col. 10, lines 18-28).

As per claim 36, Wells et al teaches of comparing gaming software transaction information in the first download acknowledgement message including a first digital signature determined for the gaming software and the gaming software transaction information in the second download acknowledgement message includes a second digital signature determined for the gaming device (col. 3, lines 48-67 and col. 10, lines 18-28).

As per claims 37,44-46,76, and 94, Wells et al discloses that the gaming software transaction information in the first download acknowledgement message includes a first digital signature determined for the gaming software and the gaming software transaction information in the second download acknowledgement message includes a second digital signature determined for the gaming software which they are compared to see if they match which determines the transaction to be authorized (col. 3, lines 48-67 and col. 10, lines 18-28).

As per claims 54,55,57-59,63,64,104, and 106, Wells et al teaches that the gaming software transaction database includes a record of gaming software installed on the gaming device and a record of gaming software usage (col. 8, lines 36-51).

As per claims 60,61, and 107, it is disclosed by Wells et al of generating a billing report and generating a fee, that varies with time, for the billing report based on the number of times a first gaming software has been used on the gaming device (col. 1, lines 61-67).

As per claims 108 and 126, Wells et al teaches of a database for storing public encryption keys for the gaming devices (col. 3, lines 48-67).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131
2/3/06

CR
February 3, 2006

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1 Applicant: Nguyen et al. Filing Date Herewith	Application No.: New Group Not yet assigned

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	6,149,522	11/21/00	Alcorn et al.	463	29	06/29/98
	A2	6,106,396	08/22/00	Alcorn et al.	463	29	06/17/96
	A3	6,104,815	08/15/00	Alcorn et al.	380	251	01/09/98
	A4	5,836,817	11/17/98	Acres et al.	463	26	06/06/95
	A5	5,643,086	07/01/97	Alcorn et al.	463	29	06/29/95
	A6	6,178,510	1/23/01	O'Connor et al.	713	201	9/4/97
	A7	6,099,408	8/8/00	Schneier et al.	463	29	12/31/96
	A8	5,768,382	6/16/98	Schneier et al.	380	23	11/22/95
	A9	6,285,868	9/4/01	LaDue	455	410	1/10/97
	A10	5,761,647	6/2/98	Boushy	705	10	5/24/96
	A11	5,999,808	12/7/99	LaDue	455	412	1/7/96
	A12	5,770,533	6/23/98	Franchi	463	42	5/2/94
	A13	6,270,410	8/7/01	DeMar et al.	463	20	2/10/99
	A14	5,779,545	7/14/98	Berg et al.	463	22	9/10/96

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	B1	WO 96/00950	11/1/96	WIPO	G06F	155/00	X	
	B2	WO 95/24689	14/9/95	WIPO	G06F	155/00	X	
	B3	WO 99/01188	14/1/99	WIPO	A63F		X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified)	Atty Docket No.	Application No.:
	IGT1P034X1/P-277CIP	10/116,424
Information Disclosure Statement By Applicant	Applicant:	
	Nguyen et al.	
	Filing Date	Group
(Use Several Sheets if Necessary)	4/3/02	3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	6,364,769	4/2/02	Weiss et al.	463	29	5/22/00
	A2	6,368,219	4/9/02	Szrek et al.	463	42	10/15/99
	A3	6,285,886	9/4/01	Kamel et al.	455	522	7/8/99

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	B1	US 2002/0049909	4/25/02	United States	713	188	X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1/P-277CIP Applicant: Nguyen et al. Filing Date April 3, 2002
	Application No.: 10/116,424 Group 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	5,762,552	06/09/98	Vuong et al.	463	25	12/05/95
	A2						
	A3						
	A4						
	A5						
	A6						
	A7						
	A8						
	A9						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	B1							
	B2							
	B3							
	B4							
	B5							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	C1	
	C2	
	C3	

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1/P-277CIP Applicant: Nguyen et al. Filing Date April 3, 2002	Application No.: 10/116,424 Group 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	4,454,594	6/12/84	Heffron et al.	364	900	11/25/81
	A2	4,430,728	2/7/84	Beitel et al.	364	900	12/29/81
	A3	5,851,149	12/22/98	Xidos et al.	463	42	8/4/95
	A4	6,446,257	9/3/02	Pradhan et al.	717	154	2/4/99
	A5	6,099,408	8/8/00	Schneier et al.	463	29	12/31/96
	A6	6,453,319	9/17/02	Mattis et al.	707	100	4/5/00
	A7	6,449,687	9/10/02	Moriya	711	112	10/28/99
	A8	3,931,504	1/6/76	Jacoby	235	153	12/12/73
	A9	6,253,374	6/26/01	Dresevic et al.	717	11	7/2/98
	A10	6,454,648	9/24/02	Kelly et al.	463	16	11/3/99

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Pg. 1 of 1

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277CIP **Application No.:** 10/116,424 **Applicant:** Binh T. Nguyen, *et al.* **Filing Date** April 3, 2002 **Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A	6,002,772	Dec. 14, 1999	Saito			Apr. 2, 1997
	B						
	C						
	D						
	E						
	F						
	G						
	H						
	I						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	J	1074955A2	07/02/2001	EPO			X	
	K	1061430A1	20/12/2000	EPO			X	
	L	0715245A1	05/06/1996	EPO			X	
	M	02/05229A2	17/01/2002	WIPO			X	
	N							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	O	
	P	
	Q	

Examiner	Date Considered 12\14\05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Pg. 1 of 1

ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18
Stylesheet Version v18.0

Title of Invention	SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Application Number:	10/116424
Confirmation Number:	3186
First Named Applicant:	BINH NGUYEN
Attorney Docket Number:	IGT1P034X1
Art Unit:	3711
Search string:	(6165072 or 6508709).pn.

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	6165072	2000-12-26	Davis et al.		463	29
	2	6508709	2003-01-21	Karmarkar		463	43

Signature

Examiner Name	Date
	12/14/05

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277 CIP **Application No.:** 10/116,424 **Applicant:** Binh T. Nguyen, et al. **Filing Date** April 3, 2002 **Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	2002/0045477	04/18/2002	Dabrowski	463	29	08/27/2001
	A2	2002/0071557	06/13/2002	Nguyen	380	251	12/07/2000

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	B1	EP 0744786	27.11.1996	EP			X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified) Information Disclosure Statement By Applicant (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277 CIP **Application No.:** 10/116,424 **Applicant:** Binh T. Nguyen **Filing Date** April 3, 2002 **Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
LA	1A	5,970,143	10/19/1999	Schneier, *et al.*			08/08/1996

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified)	**Atty Docket No.** IGT1P034X1/P-277 CIP	**Application No.:** 10/116,424
Information Disclosure Statement By Applicant	**Applicant:** Binh T. Nguyen, *et al.*	
(Use Several Sheets if Necessary)	**Filing Date** April 3, 2002	**Group** 3711

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
CM	A1	5,970,143	10/19/1999	Schneier			08/08/1996
	A2	5,421,009	05/30/1995	Stephen M. Platt			12/22/1993
	A3	5,759,102	06/02/1998	Pease, *et al.*			02/12/1996
	A4	5,905,523	05/18/1999	Woodfield, *et al.*			06/28/1996
	A5	6,029,046	02/22/2000	Khan, *et al.*			12/01/1995
	A6	6,104,815	08/15/2000	Alcorn, *et al.*			01/09/1998
	A7	5,870,723	02/09/1999	Pare, Jr. *et al.*			08/29/1996
	A8	5,654,746	08/05/1997	McMullan, Jr. *et al.*			12/01/1994
	A9	5,136,644	08/04/1992	Audebert, *et al.*			09/19/1989
	A10	5,845,090	12/01/1998	Theodore Joseph Collins, *et al.*			09/30/1996
	A11	6,317,827	11/13/2001	Cooper			08/16/1996
	A12	6,047,128	04/042000	Zander			12/09/1997
	A13	5,896,566	04/20/1999	Averbuch, *et al.*			07/28/1995
	A14	5,848,064	12/08/1998	Cowan			08/07/1996
	A15	6,154,878	11/28/2000	Saboff			07/21/1998
	A16	6,006,034	12/21/1999	Heath, *et al.*			09/05/1996
	A17	5,845,077	12/01/1998	Fawcett			11/27/1995
	A18	5,715,462	02/03/1998	Iwamoto, *et al.*			02/27/1995
	A19	5,473,772	12/05/1995	Halliwell, *et al.*			09/02/1993
	A20	5,155,837	10/13/1992	Liu, *et al.*			03/02/1989
	A21	5,410,703	04/25/1995	Nilsson, *et al.*			07/01/1992
	A22	5,421,017	05/30/1995	Scholz, *et al.*			01/14/1994
	A23	5,682,533	10/28/1997	Siljestroemer			09/27/1994
	A24	5,885,158	03/23/1999	Torango, *et al.*			09/10/1996
	A25	2002/0137217	09/26/2002	Rowe			12/21/2000
	A26	2003/0064771	04/03/2003	Morrow, *et al.*			09/28/2001
	A27	2003/0188306	10/02/2003	Harris, *et al.*			03/26/2003
	A28	5,643,086	07/01/1997	Alcorn, *et al.*			06/29/1995
CM	A29	5,555,418	09/10/1996	Nilsson, et al.			01/30/1995

Examiner	**Date Considered** 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	**Atty Docket No.** IGT1P034X1/P-277 CIP **Application No.:** 10/116,424 **Applicant:** Binh T. Nguyen, *et al.* **Filing Date** April 3, 2002 **Group** 3711

Foreign Patent or Published Foreign Patent Application

Examiner Initial	**No.**	**Document No.**	**Publication Date**	**Country or Patent Office**	**Class**	**Sub-class**	**Translation**	
							Yes	**No**
	B1	EP 0841 615	05/13/1998	EPO			X	
	B2	EP 0 706 275	04/10/1996	EPO			X	
	B3	EP 0 905 614	03/31/1999	EPO			X	
	B4	0 689 325	06/20/1995	EPO			X	
	B5	WO 01/20424 A2	22/03/2001	PCT			X	
	B6	EP 1 004 970	31/05/2000	EPO			X	

Other Documents

Examiner Initial	**No.**	**Author, Title, Date, Place (e.g. Journal) of Publication**
	C1	Hiroaki Higaki, 8 page document entitled "Group Communication Algorithm for Dynamically Updating in Distributed Systems" Copyright 1994 IEEE International Conference On Parallel and Distributed Systems (pages 56 – 62) 08-8186-655-6/94, higaki@sdesun.slab.ntt.jp
	C2	Steffen Hauptmann, *et al.*, 12 page document entitled "On-line Maintenance With On-The-Fly Software Replacement" Copyright 1996 IEEE Proceedings, Third International Conference On Configurable Distributed Systems, (pages 70 – 80) 0-8186-7395-8/96
	C3	Hiroaki Higaki, 9 page document entitled "Extended Group Communication Algorithm For Updating Distributed Programs" Copyright 1996, IEEE, International Conference ON Parallel and Distributed Systems, 0-8186-7267-6/96, , hig@takilab.k.dendai.as.jp

Examiner	**Date Considered** 12\14\05

xaminer: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form 1449 (Modified)	Atty Docket No. IGT1P034X1/P-277CIP	Application No.: 10/116,424
Information Disclosure Statement By Applicant	Applicant: Nguyen, et al.	
(Use Several Sheets if Necessary)	Filing Date April 3, 2002	Group 2131

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	5,671,412	9/23/1997	Christiano			7/28/1995
	A2	5,715,403	2/3/1998	Stefik			11/23/1994
	A3	5,925,127	7/20/1999	Ahmad			4/9/1997
	A4	6,052,512	4/18/2000	Peterson, et al.			12/22/1997
	A5	6,125,185	9/26/2000	Boesch			5/27/1997
	A6	6,169,976	1/2/2001	Colosso			7/2/1998

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	B1							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	C1	

Examiner	Date Considered 12/14/05

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Notice of References Cited	Application/Control No. 10/116,424	Applicant(s)/Patent Under Reexamination NGUYEN ET AL.
	Examiner Christopher A. Revak	Art Unit 2131 — Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,106,396	08-2000	Alcorn et al.	463/29
*	B	US-6,805,634	10-2004	Wells et al.	463/42
*	C	US-5,643,086	07-1997	Alcorn et al.	463/29
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No. 10/116,424	Applicant(s)/Patent under Reexamination NGUYEN ET AL.	
	Examiner Christopher A. Revak	Art Unit 2131	

SEARCHED

Class	Subclass	Date	Examiner
NONE	NONE	2/3/2006	CR

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)

	DATE	EXMR
BRS Text Search USPAT, US PGPUB, USOCR, DERWENT, JPO, EPO, IBM TDB	12/15/2005	CR
BRS Subclass Text Search USPAT, US PGPUB	12/15/2005	CR
PALM Inventor Name Search	2/2/2006	CR

Index of Claims

Application/Control No.	10/116,424
Applicant(s)/Patent under Reexamination	NGUYEN ET AL.
Examiner	Christopher A. Revak
Art Unit	2131

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	+	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	2/3/06								
	1	√								
	2	|								
	3	|								
	4	|								
	5	|								
	6	|								
	7	|								
	8	|								
	9	|								
	10	|								
	11	|								
	12	|								
	13	|								
	14	|								
	15	|								
	16	|								
	17	|								
	18	|								
	19	|								
	20	|								
	21	|								
	22	|								
	23	|								
	24	|								
	25	|								
	26	|								
	27	|								
	28	|								
	29	|								
	30	|								
	31	|								
	32	|								
	33	|								
	34	|								
	35	|								
	36	|								
	37	|								
	38	|								
	39	|								
	40	|								
	41	|								
	42	|								
	43	|								
	44	|								
	45	|								
	46	|								
	47	|								
	48	|								
	49	√								
	50	√								
	51	√								
	52	|								
	53	|								
	54	|								
	55	|								
	56	|								
	57	|								
	58	|								
	59	|								
	60	|								
	61	|								
	62	|								
	63	|								
	64	|								
	65	|								
	66	|								
	67	|								
	68	|								
	69	|								
	70	|								
	71	|								
	72	|								
	73	|								
	74	|								
	75	|								
	76	|								
	77	|								
	78	|								
	79	|								
	80	|								
	81	|								
	82	|								
	83	|								
	84	|								
	85	|								
	86	|								
	87	|								
	88	|								
	89	|								
	90	|								
	91	|								
	92	|								
	93	|								
	94	|								
	95	|								
	96	|								
	97	|								
	98	|								
	99	√								
	100	√								
	101	√								
	102	|								
	103	|								
	104	|								
	105	|								
	106	|								
	107	|								
	108	|								
	109	|								
	110	|								
	111	|								
	112	|								
	113	|								
	114	|								
	115	|								
	116	|								
	117	|								
	118	|								
	119	|								
	120	|								
	121	|								
	122	|								
	123	|								
	124	|								
	125	|								
	126	|								
	127	|								
	128	|								
	129	|								
	130	|								
	131	|								
	132	|								
	133	|								
	134	|								
	135	√								
	136	√								
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 3186

SERIAL NUMBER 10/116,424	FILING DATE 04/03/2002 RULE	CLASS 380	GROUP ART UNIT 2131	ATTORNEY DOCKET NO. IGT1P034X1/P-277CIP

APPLICANTS

Binh T. Nguyen, Reno, NV;

Michael M. Oberberger, Reno, NV;
Gregory Hopkins Parrott, Reno, NV;

** CONTINUING DATA *************************
This application is a CIP of 09/732,650 12/07/2000

** FOREIGN APPLICATIONS ********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
** 05/16/2002

Foreign Priority claimed □ yes ☒ no 35 USC 119 (a-d) conditions met □ yes ☑ no □ Met after Allowance Verified and Acknowledged ______ Examiner's Signature ______ Initials	STATE OR COUNTRY NV	SHEETS DRAWING 16	TOTAL CLAIMS 136	INDEPENDENT CLAIMS 7

ADDRESS
22434
BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND , CA
94612-0250

TITLE
Secured virtual network in a gaming environment

FILING FEE RECEIVED 3164	FEES: Authority has been given in Paper No. _________ to charge/credit DEPOSIT ACCOUNT No. _________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue)

		□ Other ______________ □ Credit

BEYER WEAVER & THOMAS, LLP

INTELLECTUAL PROPERTY LAW
500 12th Street, Suite 200, Oakland, CA 94607
Telephone: (510) 663-1100 Facsimile: (510) 663-0920
www.beyerlaw.com

FACSIMILE COVER SHEET

May 25, 2006

Receiver:	**Examiner Christopher A. Revak** **Group 2131**
TEL #:	
FAX #:	571-273-8300 (central fax)
Sender:	David P. Olynick
Our Ref. No.:	IGT1P034X1
Re:	U.S. Application No. 10/116,424

Pages Including Cover Sheet(s): 25

MESSAGE:

Attached please find the following documents for filing in the above-referenced application:

1. **Amendment Transmittal; and**
2. **Amendment A.**

Respectfully submitted,

David P. Olynick
Reg. No. 48,615

CONFIDENTIALITY NOTE

The information contained in this facsimile (FAX) message is legally privileged and confidential information intended only for the use of the receiver or firm named above. If the reader of this message is not the intended receiver, you are hereby notified that any dissemination, distribution or copying of this FAX is strictly prohibited. If you have received this FAX in error, please immediately notify the sender at the telephone number provided above and return the original message to the sender at the address above via the United States Postal Service. Thank you.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen, et al.

Application No: 10/116,424

Filed: April 3, 2002

Title: Secure Virtual Network in a Gaming Environment

Attorney Docket No.: IGT1P034X1/P-277CIP

Examiner: Revak, Christopher A

Group: 2131

CERTIFICATE OF TRANSMISSION
I hereby certify that this correspondence is being transmitted via facsimile to the U.S. Patent and Trademark Office, Attention: Examiner Revak at facsimile telephone number (571) 273-8300 on May 25, 2006.

Signed: ______________________
Mia Mitchell-Haynes

AMENDMENT TRANSMITTAL

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith is an Amendment in the above-identified application.

The fee has been calculated as shown below.

	Claims After Amendment		Highest Previously Paid For	Present Extra	Small Entity Rate Fee	Large Entity Rate Fee
Total Claims	136	MINUS	136	0	x 25 =	x 50 = 0
Independent Claims	7	MINUS	7	0	x 100 =	x 200 = 0
Multiple Dependent Claim Present and Fee Not Previously Paid						
				Total	$	$0

☒ Applicant(s) hereby petition for a one month extension(s) of time to respond to the aforementioned Office Action.

☒ Applicant(s) believe that no (additional) Extension of Time is required; however, if it is determined that such an extension is required, Applicant(s) hereby petition that such an extension be granted and authorize the Commissioner to charge the required fees for an Extension of Time under 37 CFR 1.136 to Deposit Account No. 500388.

☒ Please charge the required fees, or any additional fees required to facilitate filing the enclosed response, to Deposit Account No. 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Reg. No. 48,615

P.O. Box 70250
Oakland, CA 94612-0250

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen, et al.

Application No: 10/116,424

Filed: April 3, 2002

Title: Secure Virtual Network in a Gaming Environment

Attorney Docket No.: IGT1P034X1/P-277CIP

Examiner: Revak, Christopher A

Group: 2131

CERTIFICATE OF TRANSMISSION
I hereby certify that this correspondence is being transmitted via facsimile to the U.S. Patent and Trademark Office, Attention: Examiner Revak at facsimile telephone number (571) 273-8300 on May 25, 2006.

Signed:
Mia Mitchell-Haynes

AMENDMENT A

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Office Action dated February 8, 2006 please amend the above-identified patent application as follows:

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks/Arguments begin on page 21 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) In a software authorization agent, a method of generating a gaming software transaction record used to facilitate a transfer of gaming software between two gaming devices, the method comprising:

receiving a gaming software transaction request from a first gaming device;

authenticating an identity of the first gaming device;

generating a gaming software transaction record comprising gaming software transaction information that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device

sending an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to the second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on the gaming machine.

2. (Original)The method of claim 1, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

3. (Original)The method of claim 1, wherein the first gaming device is at least one of a gaming machine, game server and combinations thereof.

4. (Original)The method of claim 1, wherein the gaming software transaction request comprises access information and gaming software identification information.

5. (Original)The method of claim 4, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

6. (Original)The method of claim 4, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

7. (Original)The method of claim 1, further comprising:

comparing access information in the gaming software transaction request with access information stored in a database.

8. (Original)The method of claim 7, when the compared access information does not match the access information stored in the database,

denying the gaming software transaction request.

9. (Original)The method of claim 1, further comprising:

comparing gaming software identification information in the gaming software transaction request with gaming software identification information stored in a database.

10. (Original)The method of claim 9, when the gaming software identification information does not match the access information stored in the database,

denying the gaming software transaction request.

11. (Original)The method of claim 1, further comprising:

generating an identification sequence;

encrypting the identification sequence with a public encryption key for the first gaming device wherein information encrypted with the public encryption key is decrypted with a private encryption key used by the first gaming device;

sending the encrypted identification sequence to the first gaming device.

12. (Original)The method of claim 11, wherein the identification sequence is a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device.

13. (Original)The method of claim 11, further comprising:

receiving from the first gaming device a second identification sequence encrypted with a public encryption key used by the software authorization agent,

decrypting the second identification sequence with a private encryption key corresponding to the public encryption key used by the software authorization agent;

comparing the second identification sequence to the identification sequence sent to the first gaming device to authenticate the identity of the first gaming device.

14. (Original)The method of claim 13, wherein the second identification sequence is a symmetric encryption key used to transfer gaming software between the first gaming device and the second gaming device.

15. (Original)The method of claim 13, when the second identification sequence received from the first gaming device does not match the identification sequence sent to the first gaming device;

denying the gaming software transaction request.

16. (Original)The method of claim 1, wherein the gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number, a gaming software identification number, a gaming software provider identifier, a transaction number, a number of allowable downloads and combinations thereof.

17. (Original)The method of claim 1, further comprising:

storing the gaming transaction record information to a transaction database.

18. (Original)The method of claim 1, further comprising:

sending gaming software transaction information to the first gaming device.

19. (Original)The method of claim 18, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

20. (Original)The method of claim 1, further comprising:

sending a notification message to a gaming software provider identified in the gaming software request of a pending gaming software download request.

21. (Original)The method of claim 1, wherein the software authorization agent communicates with the first gaming device using an local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

22. (Original)The method of claim 1, wherein the software authorization agent and the first gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

23. (Original)The method of claim 1, wherein the transfer of gaming software is performed at least one of manually and electronically.

24. (Original)The method of claim 1, wherein the gaming software comprises one or more gaming software components for the game of chance, the bonus game of chance, the device driver, the player tracking service and the operating system.

25. (Original)The method of claim 1, wherein the gaming software is used to upgrade a gaming software component on the first gaming device.

26. (Original)The method of claim 1, wherein the gaming software is used to correct an error in a gaming software component on the second gaming device.

27. (Original)The method of claim 1, further comprising:

requesting a list of gaming software installed on a gaming device.

28. (Currently Amended) In a software authorization agent, a method of regulating a transfer of gaming software between two gaming devices, the method comprising;

receiving a gaming software download request message with gaming software transaction information from a first gaming device;

validating the gaming software download request using the gaming software transaction information;

~~sending an authorization message to the first gaming device authorizing the first gaming device to transfer gaming software to a second gaming device;~~

sending an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

29. (Original)The method of claim 28, wherein the second gaming device is at least one of a game server and a gaming machine.

30. (Original)The method of claim 28, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

31. (Original)The method of claim 28, wherein the gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and combinations thereof.

32. (Original)The method of claim 28, further comprising:

comparing the gaming transaction information in the gaming software download request message with gaming transaction information stored in a transaction database to validate the gaming software download request.

33. (Original)The method of claim 28, further comprising:

sending a message to the first gaming device denying authorization for the first gaming device to transfer gaming software to the second gaming device.

34. (Original)The method of claim 28, further comprising:

decrypting the download request message.

35. (Original)The method of claim 28, further comprising:

receiving a first download acknowledgement message from the first gaming device and receiving a second download acknowledgement message from the second gaming device.

36. (Original)The method of claim 35, further comprising:

comparing gaming software transaction information in the first download acknowledgement message with gaming software transaction information in the second download acknowledgement message to validate that the gaming software has been correctly transferred.

37. (Original)The method of claim 36, wherein the gaming software transaction information in the first download acknowledgement message includes at least a first digital signature determined for the gaming software and the gaming software transaction information in the second download acknowledgement message includes at least a second digital signature determined for the gaming software.

38. (Original)The method of claim 28, wherein the first gaming device a game server in communication with one or more gaming machines and the second gaming device is a gaming machine.

39. (Original)The method of claim 28, wherein the first gaming device is a game server maintained by a gaming software provider and the second gaming device is a game server in communication with one or more gaming machines.

40. (Original)The method of claim 28, wherein the first gaming device is a game server maintained by a gaming software provider and the second gaming device is a gaming machine.

41. (Original)The method of claim 28, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

42. (Original)The method of claim 28, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

43. (Original)The method of claim 28, further comprising:
receiving the gaming software from the first gaming device;
validating the gaming software; and
sending the gaming software to the second gaming device.

44. (Original)The method of claim 43, further comprising:
determining a digital signature for the gaming software; and
comparing the digital signature with an approved digital signature for the gaming software stored in a database to validate the gaming software.

45. (Original)The method of claim 28, further comprising:
storing gaming software transaction information indicating that a status of the download request.

46. (Original)The method of claim 28, wherein the status is at least one of authorized, pending, completed and void.

47. (Original)The method of claim 28, wherein the transfer of gaming software is performed at least one of manually and electronically.

48. (Original)The method of claim 28, wherein the gaming software comprises one or more gaming software components for the game of chance, the bonus game of chance, the device driver, the player tracking service and the operating system.

49. (Original)The method of claim 28, wherein the gaming software is used to upgrade a gaming software component on the second gaming device.

50. (Original)The method of claim 28, wherein the gaming software is used to correct an error in a gaming software component on the second gaming device.

51. (Original)The method of claim 28, further comprising:

requesting a list of gaming software installed on a gaming device.

52. (Currently Amended) In a software authorization agent, a method of providing gaming software transaction information, the method comprising:

receiving a gaming software transaction information request from a gaming device;

authenticating an identity of the gaming device;

querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device, said gaming software transaction database comprising a plurality of records of gaming software transactions wherein each gaming software transaction is related to a request to authorize a transfer of gaming software received by the software authorization agent; and

sending the requested gaming software transaction information to the gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

53. (Original)The method of claim 52,

wherein each gaming software transaction record includes gaming software transaction information that describes a transfer of gaming software from a first gaming device to a second gaming device.

54. (Original)The method of claim 52,

wherein the gaming software transaction database includes a record of gaming software installed on one or more gaming devices.

55. (Original)The method of claim 52, wherein the gaming software transaction database includes a record of gaming software usage on one or more gaming devices.

56. (Original)The method of claim 52, wherein the gaming transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time.

57. (Original)The method of claim 52, further comprising:

generating a gaming transaction report that presents the set of gaming software transaction requested by the gaming device.

58. (Original)The method of claim 52, further comprising:

generating a distribution of gaming software on a plurality of gaming machines at a specified time using the gaming software transaction information stored in the gaming software transaction database.

59. (Original)The method of claim 52, further comprising:

generating a distribution of gaming software on a plurality of gaming machines for a plurality of times using the gaming software transaction information stored in the gaming software transaction database.

60. (Original)The method of claim 52, further comprising:

generating a billing report.

61. (Original)The method of claim 60, further comprising:
generating a fee for the billing report based upon a number of times a first gaming software has been used on the gaming device.

62. (Original)The method of claim 61, wherein a usage fee charged each time the first gaming software is used varies with time.

63. (Original)The method of claim 52, further comprising:
requesting a list of gaming software installed on the gaming device.

64. (Original)The method of claim 63, further comprising:
storing the list of gaming software installed on the gaming device to the gaming software transaction database.

65. (Original) In a first gaming device, a method of requesting a transfer of gaming software from a second gaming device, said method comprising:
generating a gaming software transaction request;
sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and
receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device
wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

66. (Original)The method of claim 65, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

67. (Original)The method of claim 65, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

68. (Original)The method of claim 65, wherein the gaming software transaction request comprises access information and gaming software identification information.

69. (Original)The method of claim 68, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

70. (Original)The method of claim 68, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

71. (Original)The method of claim 65, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

72. (Original)The method of claim 65, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

73. (Original)The method of claim 65, further comprising:

sending authentication information used to identify the first gaming device to the gaming software authorization agent.

74. (Original)The method of claim 65, further comprising:

sending a message requesting the gaming software to the second gaming device.

75. (Original)The method of claim 65, further comprising:
receiving the gaming software from the second gaming device.

76. (Original)The method of claim 75, further comprising:
determining a digital signature for the gaming software and
sending a message with at least the digital signature to the gaming software authorization agent.

77. (Original)The method of claim 65, further comprising:
authenticating an identity of the second gaming device.

78. (Original)The method of claim 65, wherein the first gaming device is a gaming machine and the second gaming device is a game server.

79. (Original)The method of claim 65, wherein the first gaming device is a game server in communication with a plurality of gaming machines and the second gaming device is a game server maintained by a gaming software content provider.

80. (Original)The method of claim 65, wherein the transfer of gaming software is performed at least one of manually and electronically.

81. (Original)The method of claim 65, wherein the gaming software comprises one or more gaming software components.

82. (Original)The method of claim 65, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

83. (Original)The method of claim 65, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

84. (Currently Amended) In a first gaming device, a method of transferring gaming software to a second gaming device, said method comprising:

receiving a gaming software transaction request from the second gaming device;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software;

receiving an authorization message from the gaming software authorization agent wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to the second gaming device; and

transferring the gaming software to the second gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

85. (Original)The method of claim 84, further comprising:

receiving an approval of the gaming software transaction request from the gaming software authorization agent.

86. (Original)The method of claim 84, further comprising:

prior to transferring the gaming software, receiving a denial of the gaming software transaction request from the gaming software authorization agent; and

terminating the transfer of the gaming software.

87. (Original)The method of claim 84, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

88. (Original)The method of claim 84, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection, an infrared communication connection and combinations thereof.

89. (Original)The method of claim 84, wherein the gaming software transaction request comprises access information and gaming software identification information.

90. (Original)The method of claim 89, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

91. (Original)The method of claim 89, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

92. (Original)The method of claim 84, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

93. (Original)The method of claim 84, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

94. (Original)The method of claim 84, further comprising:
determining a digital signature for the gaming software and
sending a message with at least the digital signature to the gaming software authorization agent.

95. (Original)The method of claim 84, wherein the first gaming device is a gaming server and the second gaming device is a gaming machine.

96. (Original)The method of claim 84, wherein the first gaming device is a gaming machine and the second gaming device is a gaming machine.

97. (Original)The method of claim 84, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a game server maintained by a gaming entity.

98. (Original)The method of claim 84, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a gaming machine maintained by a gaming entity.

99. (Original)The method of claim 84, wherein the transfer of gaming software is performed at least one of manually and electronically.

100. (Original)The method of claim 84, wherein the gaming software comprises one or more gaming software components.

101. (Original)The method of claim 84, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

102. (Original)The method of claim 84, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

103. (Currently Amended) A software authorization agent for facilitating the transfer of gaming software between a plurality of gaming devices, the software authorization agent comprising:

a network interface allowing the authorization agent to communicate with each of the plurality of gaming devices; and

a processor configured or designed to (i) receive gaming software transfer requests via the network interface from a first gaming device for the transfer of gaming software from the first gaming device to a second gaming device ~~to a third gaming device~~ (ii) approve or reject the gaming software transaction request; and iii) send an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

104. (Original)The software authorization agent of claim 103, further comprising:
a transaction database containing gaming software transaction information.

105. (Original)The software authorization agent of claim 104, wherein the gaming software transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time.

106. (Original)The software authorization agent of claim 105, further comprising a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software distribution reports based upon the gaming software transaction information.

107. (Original)The software authorization agent of claim 105, further comprising:
a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software billing reports based upon the gaming software transaction information.

108. (Original)The software authorization agent of claim 103, further comprising:
a database storing public encryption keys for one or more of the plurality of gaming devices.

109. (Original)The software authorization agent of claim 103, further comprising:
a database storing identification information for one or more of the plurality of gaming devices.

110. (Original)The software authorization agent of claim 103, further comprising:
a database storing identification information for the gaming software that is transferred from the second gaming device to the third gaming device.

111. (Original)The software authorization agent of claim 110, wherein the identification information for the gaming software is a digital signature, a title, a manufacturer, an identification number and combinations thereof.

112. (Currently Amended)The software authorization agent of claim 103, wherein the first gaming device is a hand-held computing device~~, the second gaming device is a portable memory device storing the gaming software~~ and the ~~third~~ second gaming device is a gaming machine.

113. (Currently Amended)The software authorization agent of claim 103, wherein the first gaming device is a first gaming machine and [,] the second gaming device is a second gaming machine ~~and the third gaming device is the first gaming machine~~.

114. (Currently Amended)The software authorization agent of claim 103, wherein the first gaming device is a first game server and [,] the second gaming device is a second game server ~~and the third gaming device is a first gaming machine~~.

115. (Currently Amended)The software authorization agent of claim 103, wherein the first gaming device is a first game server~~, the second gaming device is a second game server~~ and the ~~third~~ second gaming device is a gaming machine ~~the first game server~~.

116. (Original)The software authorization agent of claim 103, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

117. (Currently Amended)The software authorization agent of claim 103, wherein the software authorization agent, the first gaming device and, the second gaming device ~~and the third gaming device~~ communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

118. (Currently Amended)The software authorization agent of claim 103, wherein the software authorization agent, the first gaming device and, the second gaming device ~~and the third gaming device~~ communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

119. (Original)The software authorization agent of claim 103, wherein the transfer of gaming software is performed at least one of manually and electronically.

120. (Original)The software authorization agent of claim 103, wherein the gaming software comprises one or more gaming software components.

121. (Original)The software authorization agent of claim 103, wherein the gaming software is used to upgrade a gaming software component on one of the gaming devices.

122. (Original)The software authorization agent of claim 103, wherein the gaming software is used to correct an error in a gaming software component on one of the gaming devices.

123. (Currently Amended) A first gaming device comprising:

a network interface allowing communications between the first gaming device, a software authorization agent and one or more other gaming devices; and

a processor configured or designed to (i) send a request for the transfer of gaming software from ~~a second~~ the first gaming device to a ~~third~~ second gaming device via the network interface to the software authorization agent (ii) receive from the software authorization agent a reply approving or rejecting the request for the transfer of the gaming software

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

124. (Original)The first gaming device of claim 123, further comprising:

a memory device that stores gaming software.

125. (Original)The first gaming device of claim 123, further comprising:

a master gaming controller that controls a game of chance played on the first gaming device.

126. (Original)The first gaming device of claim 123, further comprising:

a memory device that stores public encryption keys for one or more of the plurality of gaming devices and the software authorization agent.

127. (Original)The first gaming device of claim 123, wherein the network interface is connected to at least one of a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

128. (Original)The first gaming device of claim 123, wherein the network interface provides at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

129. (Original)The first gaming device of claim 123, wherein the first gaming device is a portable gaming device.

130. (Currently Amended)The first gaming device of claim 123, wherein the first gaming device is a first gaming machine and, the second gaming device is a second gaming machine ~~and the third gaming device is the first gaming machine~~.

131. (Currently Amended)The first gaming device of claim 123, wherein the first gaming device is a first game server and, the second gaming device is a second game server~~ and the third gaming device is a first gaming machine~~.

132. (Currently Amended)The first gaming device of claim 123, wherein the first gaming device is a first game server and, the second gaming device is a gaming machine ~~second game server and the third gaming device is the first game server~~.

133. (Original)The first gaming device of claim 123, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

134. (Original)The first gaming device of claim 123, wherein the gaming software comprises one or more gaming software components.

135. (Original)The first gaming device of claim 123, wherein the gaming software is used to upgrade a gaming software component on one of the gaming devices.

136. (Original)The first gaming device of claim 123, wherein the gaming software is used to correct an error in a gaming software component on one of the gaming devices.

REMARKS

Currently claims 1-136 remain in the application. Claims 1, 38, 52, 84, 103, 112-115, 117, 118, 123 and 130-132 have been amended. Claims 1-136 are rejected. Applicant believes no new matter has been added.

Rejections under 35 U.S.C. § 103

Claims 1-136 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells et al., USP 6, 805, 634 in view of Alcorn, et al USP 5,643,086.

The remaining claims are related to communications between three devices, a software authorization agent, a first gaming device and a second gaming device. In a particular embodiment, as described with respect to claim 28, the software authorization agent, receives "a gaming software download request message with gaming software transaction information from a first gaming device" and sends "an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent." In this embodiment, the transfer of software is between the first gaming device and the second gaming device whereas the software authorization agent provides the authorization for the transfer.

In the combination of Wells and Alcorn, software transfer between a source device and a target device is described. Prior to the transfer the source can request identification information from the target (Wells: Col. 8:36-38). However, in the citations provided by the Examiner for Wells and Alcorn, Applicant didn't see a description of a third device separate from the target device and the source that is operable, as recited in claim 103 for instance, to "receive gaming software transfer requests via the network interface from a first gaming device for the transfer of gaming software from the first gaming device to a second gaming device (ii) approve or reject the gaming software transaction request; and iii) send an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device." Further, in the citations provided by the Examiner for Wells and Alcorn, Applicant didn't see a description of communications between the third device and the target device or communications between the source device and the third device.

In claims 1-51 and 84-136, limitations related to apparatus and methods for communications between a software authorization agent, a first gaming device and a second gaming device are described in the context of the software authorization agent authorizing a gaming software transfer. For at least the previously recited reasons, Applicant doesn't believe the combination of Wells, et al, and Alcorn, defined by the citations provided by the Examiner from these references teach or suggest the limitations related to apparatus and methods for communications between a software authorization agent, a first gaming device and a second gaming device as described in the context of the software authorization agent authorizing a gaming software transfer. Therefore, for at least these reasons, the combination of Wells and Alcorn can't be said to render obvious claims 1-51 and 84-136.

Claims 52-83 describes a method where a software authorization agent receives a request for gaming software transaction information related to gaming software transfers previously processed by the gaming software authorization agent. The rejection of these claims was considered with other independent claims, such as 1 and 28. However, claim 52 comprises limitations that are not recited in the other independent claims. It did not appear that Examiner addressed the different limitations in the rejection. For instance, the Examiner doesn't appear to have considered the limitation, "querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device, said gaming software transaction database comprising a plurality of records of gaming software transactions wherein each gaming software transaction is related to a request to authorize a transfer of gaming software received by the software authorization agent." Therefore, for at least these reasons, the combination of Wells and Alcorn can't be said to render obvious claims 52-83 and the rejection is believed overcome thereby.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Reg. No.: 48,615

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100, ext. 231

```
Document code: WFEE

       United States Patent and Trademark Office
     Sales Receipt for Accounting Date: 06/21/2006


VGREEN   SALE #00000001    Mailroom Dt: 05/25/2006 500388 10116424
               01 FC:1251               120.00 DA
```

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

Application or Docket Number
10/116 424

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	136	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	136 minus 20=	* 116
INDEPENDENT CLAIMS	7 minus 3 =	* 4
MULTIPLE DEPENDENT CLAIM PRESENT		□

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE □ OR OTHER THAN SMALL ENTITY

RATE	FEE		RATE	FEE
BASIC FEE	370.00	OR	BASIC FEE	740.00
X$ 9=		OR 16	X$18=	2088
X42=		OR	X84=	336
+140=		OR	+280=	
TOTAL		OR	TOTAL	3164

5/25/06 CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	* 136	Minus	** 136	= /
Independent	* 7	Minus	*** 7	= /
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=.		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

☆U.S. GPO: 2001 482-124/ [illegible]

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

	Type	L #	Hits	Search Text	DBs	Time Stamp
1	BRS	L1	205600	(authent$7 or author$7 or valid$5 or verif$7)with(device or console or component or machine or terminal or kiosk or client or server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:52
2	BRS	L2	22305	1 with(game or gaming or casino or gambl$3 or card or poker or blackjack or keno or roulette or slot)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:40
3	BRS	L3	100108	(authent$7 or author$7 or valid$5 or verif$7)with(transfer$4 or send$3 or forward$3 or updat$3 or upgrad$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:53
4	BRS	L4	57856	3 with(software or data or content or information or application or program)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:55

	Type	L #	Hits	Search Text	DBs	Time Stamp
5	BRS	L5	2331	2 same 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:51
6	BRS	L6	21949	4 with(device or console or component or machine or terminal or kiosk or client or server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:54
7	BRS	L7	2117	5 same 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:52
8	BRS	L8	10529	3 with(provider or clearinghouse or "third party" or external or remote or separate)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:53
9	BRS	L9	284	7 same 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:54

	Type	L #	Hits	Search Text	DBs	Time Stamp
10	BRS	L10	4609	8 with(device or console or component or machine or terminal or kiosk or client or server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:54
11	BRS	L11	284	9 same 10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:55
12	BRS	L12	8448	4 with(record or transaction or log or table or chart)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:56
13	BRS	L13	95	11 same 12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	2006/09/12 10:56

li

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22434 7590 09/18/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/18/2006

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

TITLE OF INVENTION: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$300	$0	$1700	12/18/2006

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22434 7590 09/18/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

TITLE OF INVENTION: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$300	$0	$1700	12/18/2006

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2131	726-004000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 ____________________

2 ____________________

3 ____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ____________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number __________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ____________________ Date ____________________

Typed or printed name ____________________ Registration No. ____________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

22434 7590 09/18/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/18/2006

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 964 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 964 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	**Application No.** 10/116,424	**Applicant(s)** NGUYEN ET AL.	
	Examiner Christopher A. Revak	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *response filed on 5/25/06*.

2. ☒ The allowed claim(s) is/are *1-136*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *9/12/06* .
7. ☒ Examiner's Amendment/Comment
8. □ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER

9/13/06

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Olynick on September 12, 2006.

The application has been amended as follows:

In the specification, on page 34, line 30, delete –09/042,192- and replace with "09/595,798";

On page 42, line 7, after –November 16, 2001- insert ", which is now U.S. Patent 6,866,586,"

The claims have been amended as follows:

52. (Currently Amended) In a software authorization agent, a method of providing gaming software transaction information, the method comprising:

receiving a gaming software transaction information request from a gaming device;

authenticating an identity of the gaming device;

querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device, said gaming software transaction database comprising a plurality of records of gaming software transactions wherein each gaming software transaction is related to a request to authorize a transfer of gaming software received by the software authorization agent; and

sending the requested gaming software transaction information to the gaming device;

sending an authorization message to a first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

65. (Currently Amended) In a first gaming device, a method of requesting a transfer of gaming software from a second gaming device, said method comprising:

generating a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and

~~receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device~~

receiving an authorization message from the gaming software authorization agent wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to the second gaming device and wherein the first gaming device and the second gaming device are separate from the gaming software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

66. (Currently Amended)The method of claim 65, wherein the gaming software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

67. (Currently Amended)The method of claim 65, wherein the gaming software authorization agent, the first gaming device and the second gaming device communicate with another using at

least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

123. (Currently Amended) A first gaming device comprising:

a network interface allowing communications between the first gaming device, a software authorization agent and one or more other gaming devices; and

a processor configured or designed to (i) send a request for the transfer of gaming software from the first gaming device to a second gaming device via the network interface to the software authorization agent (ii) ~~receive from the software authorization agent a reply approving or rejecting the request for the transfer of the gaming software;~~ receive an authorization message from the software authorization agent wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to the second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

Conclusion

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CR
September 13, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

9/13/06

Examiner-Initiated Interview Summary	**Application No.** 10/116,424	**Applicant(s)** NGUYEN ET AL.
	Examiner Christopher A. Revak	**Art Unit** 2131

All Participants:

(1) *Christopher A. Revak*.

(2) *David Olynick*.

Status of Application: *response to non-final*

(3) _____.

(4) _____.

Date of Interview: *12 September 2006*

Time: *2:00pm*

Type of Interview:

☒ Telephonic
☐ Video Conference
☐ Personal (Copy given to: ☐ Applicant ☐ Applicant's representative)

Exhibit Shown or Demonstrated: ☐ Yes ☒ No
If Yes, provide a brief description: .

Part I.

Rejection(s) discussed:
n/a

Claims discussed:
52,65,123

Prior art documents discussed:
n/a

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
See Continuation Sheet

Part III.

☒ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.

☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

CAR 9/12/06
(Examiner/SPE Signature)

(Applicant/Applicant's Representative Signature – if appropriate)

Continuation of Substance of Interview including description of the general nature of what was discussed: The examiner contacted the applicant's representative in an attempt to compact prosecution. Argued features were not recited in claims 52,65, and 123. The applicant's representative proposed amending the claims to reflect the aguments and gave the examiner authorization for an examiner's amendment..

Issue Classification	**Application/Control No.** 10/116,424	**Applicant(s)/Patent under Reexamination** NGUYEN ET AL.
	Examiner Christopher A. Revak	**Art Unit** 2131

ISSUE CLASSIFICATION

ORIGINAL	
CLASS	SUBCLASS
726	4

CROSS REFERENCES				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)			
463	29			
713	168	176		
380	251			

INTERNATIONAL CLASSIFICATION									
CLAIMED					NON-CLAIMED				
H	04	L	9	/00	H	04	L	9	/00
G	06	F	15	/16	G	06	F	15	/16
A	63	F	9	/24	A	63	F	9	/24
H	04	K	1	/00	H	04	K	1	/00
				/					/
				/					/
				/					/

(Assistant Examiner) (Date)

9/15/06
(Legal Instruments Examiner) (Date)

CHRISTOPHER REVAK
PRIMARY EXAMINER

(Primary Examiner) (Date)
9/13/06

Total Claims Allowed: 136

O.G. Print Claim(s)	O.G. Print Fig.
1	10

☒ **Claims renumbered in the same order as presented by applicant** □ CPA □ T.D. □ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		31		61		91		121		151		181
	2		32		62		92		122		152		182
	3		33		63		93		123		153		183
	4		34		64		94		124		154		184
	5		35		65		95		125		155		185
	6		36		66		96		126		156		186
	7		37		67		97		127		157		187
	8		38		68		98		128		158		188
	9		39		69		99		129		159		189
	10		40		70		100		130		160		190
	11		41		71		101		131		161		191
	12		42		72		102		132		162		192
	13		43		73		103		133		163		193
	14		44		74		104		134		164		194
	15		45		75		105		135		165		195
	16		46		76		106		136		166		196
	17		47		77		107		137		167		197
	18		48		78		108		138		168		198
	19		49		79		109		139		169		199
	20		50		80		110		140		170		200
	21		51		81		111		141		171		201
	22		52		82		112		142		172		202
	23		53		83		113		143		173		203
	24		54		84		114		144		174		204
	25		55		85		115		145		175		205
	26		56		86		116		146		176		206
	27		57		87		117		147		177		207
	28		58		88		118		148		178		208
	29		59		89		119		149		179		209
	30		60		90		120		150		180		210

Search Notes	Application/Control No. 10/116,424	Applicant(s)/Patent under Reexamination NGUYEN ET AL.	
	Examiner Christopher A. Revak	Art Unit 2131	

SEARCHED			
Class	Subclass	Date	Examiner
NONE	NONE	9/12/2006	CR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
BRS Text Search USPAT, US PGPUB, USOCR, FPRS, DERWENT, IBM TDB, JPO, EPO	9/12/2006	CR
DIALOG Text Search COMPSCI, ELECTRON, SOFTWARE	9/12/2006	CR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
463	**1,29**	12/15/2005	**CR**
726	1-4,14,15	12/15/2005	CR
713	168,176	12/15/2005	CR
380/251,282,285		12/15/2005	CR

Search Notes (continued)	Application/Control No. 10/116,424	Applicant(s)/Patent under Reexamination NGUYEN ET AL.	
	Examiner Christopher A. Revak	Art Unit 2131	

SEARCHED			
Class	Subclass	Date	Examiner
NONE	NONE	9/12/2006	CR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
705	**50-52**	12/15/2005	**CR**
705	55,56,59	12/15/2005	CR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
N/A		

```
? show files
File   2:INSPEC 1898-2006/Sep W1
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Sep W1
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Sep W1
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Sep W1
         (c) 2006 The Thomson Corp
File  35:Dissertation Abs Online 1861-2006/Aug
         (c) 2006 ProQuest Info&Learning
File  56:Computer and Information Systems Abstracts 1966-2006/Aug
         (c) 2006 CSA.
File  60:ANTE: Abstracts in New Tech & Engineer 1966-2006/Aug
         (c) 2006 CSA.
File  65:Inside Conferences 1993-2006/Sep 12
         (c) 2006 BLDSC all rts. reserv.
File  92:IHS Intl.Stds.& Specs. 1999/Nov
         (c) 1999 Information Handling Services
File  94:JICST-EPlus 1985-2006/Jun W1
         (c)2006 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2006/Sep W2
         (c) 2006 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Jul
         (c) 2006 The HW Wilson Co.
File 103:Energy SciTec 1974-2006/Jul B2
         (c) 2006 Contains copyrighted material
File 144:Pascal 1973-2006/Aug W3
         (c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Oct
         (c) 2006 American Mathematical Society
File 275:Gale Group Computer DB(TM) 1983-2006/Sep 11
         (c) 2006 The Gale Group
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 2006 The Thomson Corp
File 647:CMP  Computer Fulltext 1988-2006/Oct W5
         (c) 2006 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Sep W1
         (c) 2006 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2006/Sep 11
         (c) 2006 Dialog
File   9:Business & Industry(R) Jul/1994-2006/Sep 11
         (c) 2006  The Gale Group
File  15:ABI/Inform(R) 1971-2006/Sep 12
         (c) 2006 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2006/Jun 12
         (c) 2006 The Gale Group
File  18:Gale Group F&S Index(R) 1988-2006/Sep 11
         (c) 2006 The Gale Group
File  20:Dialog Global Reporter 1997-2006/Sep 12
         (c) 2006 Dialog
File  36:MetalBase 1965-20060911
         (c) 2006 The Thomson Corporation
File  80:TGG Aerospace/Def.Mkts(R) 1982-2006/Sep 11
         (c) 2006 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2006/Sep 11
         (c)2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 256:TecInfoSource 82-2006/Dec
         (c) 2006 Info.Sources Inc
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Sep 11
```

```
         (c) 2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Sep 12
         (c) 2006 McGraw-Hill Co. Inc
File 635:Business Dateline(R) 1985-2006/Sep 12
         (c) 2006 ProQuest Info&Learning
File 636:Gale Group Newsletter DB(TM) 1987-2006/Sep 11
         (c) 2006 The Gale Group
? ds

Set     Items   Description
S1     421640   (AUTHENT??????? OR AUTHOR??????? OR VALID????? OR VERIF???-
             ????)(16N)(DEVICE OR CONSOLE OR COMPONENT OR MACHINE OR TERMI-
             NAL OR KIOSK OR CLIENT OR SERVER)
S2      15325   S1(16N)(GAME OR GAMING OR CASINO OR GAMBL??? OR CARD OR PO-
             KER OR BLACKJACK OR KENO OR ROULETTE OR SLOT)
S3     469329   (AUTHENT??????? OR AUTHOR??????? OR VALID????? OR VERIF???-
             ????)(16N)(TRANSFER??? OR SEND??? OR FORWARD??? OR UPDAT??? OR
              UPGRAD???)
S4     101870   S3(16N)(SOFTWARE OR DATA OR CONTENT OR INFORMATION OR APPL-
             ICATION OR PROGRAM)
S5        404   S2(S)S4
S6       9301   S3(16N)(PROVIDER OR CLEARINGHOUSE OR (THIRD(W)PARTY) OR EX-
             TERNAL OR REMOTE OR SEPERATE)
S7         28   S5(S)S6
?
```

IFW 2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nguyen et al.

Application No.: 10/116,424

Filed: April 3, 2002

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

Attorney Docket No.: IGT1P034X1/P-277 CIP

Examiner: Christopher Revak

Group: 2131

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on September 21, 2006 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: Chereyce Brown
Chereyce Brown

INFORMATION DISCLOSURE STATEMENT AFTER FINAL ACTION OR NOTICE OF ALLOWANCE (37 CFR §§ 1.56 AND 1.97(d))

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO Form 1449, a copy of which is attached, may be material to examination of the above-identified patent application. These references were cited in a corresponding PCT application. A copy of the International Search Report and Written Opinion dated July 19, 2006 is enclosed herewith as well. Applicants submit this reference in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. Accordingly, the Examiner is requested to make this citation of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that this reference indeed constitutes prior art.

This Information Disclosure Statement is being filed after the mailing date of final action under §1.113 or a notice of allowance under §1.311, but before payment of the issue fee.

Accompanying this Information Disclosure Statement is

☒ a statement as specified in 37 CFR 1.97(e); or

□ the fee set forth in 37 CFR 1.17(p).

The undersigned hereby states:

☒ that each item of information contained in the Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application no more than three months prior to the filing of the Information Disclosure Statement.

It is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

David P. Olynick
Registration No. 48,615

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100

Form 1449 (Modified)	Atty Docket No. IGT1P034X1/P-277 CIP	Application No.: 10/116,424
Information Disclosure Statement By Applicant	Applicant: Nguyen et al.	
(Use Several Sheets if Necessary)	Filing Date April 3, 2002	Group 2131

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A1	2004/0002385	1/1/04	Nguyen			
	A2	2003/0054880	3/20/03	Lam et al.			
	A3	2002/0155887	10/24/02	Criss-Puszkiewicz et al.			

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	B1	WO 03/085613	10/16/2003	PCT	G07F	17/32	X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	C1	International Search Report and Written Opinion dated July 19, 2006 from corresponding PCT Application No. PCT/US2006/008785 (11 pages). [Atty. Dkt. No. IGT1P034X2WO]

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2003 (16.10.2003)

PCT

(10) International Publication Number
WO 03/085613 A1

(51) International Patent Classification⁷: G07F 17/32, G06F 1/00

(21) International Application Number: PCT/US03/09669

(22) International Filing Date: 26 March 2003 (26.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/116,424 3 April 2002 (03.04.2002) CS

(71) Applicant (for all designated States except US): IGT [US/US]; 9295 Prototype Drive, Reno, NV 89510-0580 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): NGUYEN, Binh, T. [US/US]; 1445 Taos Court, Reno, NV 89511 (US). OBERBERGER, Michael, M. [US/US]; 4591 Lynnfield Court, Reno, NV 89509 (US). PARROTT, Greg [US/US]; 4955 Foxcreek Trail, Reno, NV 89509 (US).

(74) Agent: OLYNICK, David, P.; BEYER WEAVER & THOMAS LLP, P.O. Box 778, Berkeley, CA 94704-0778 (US).

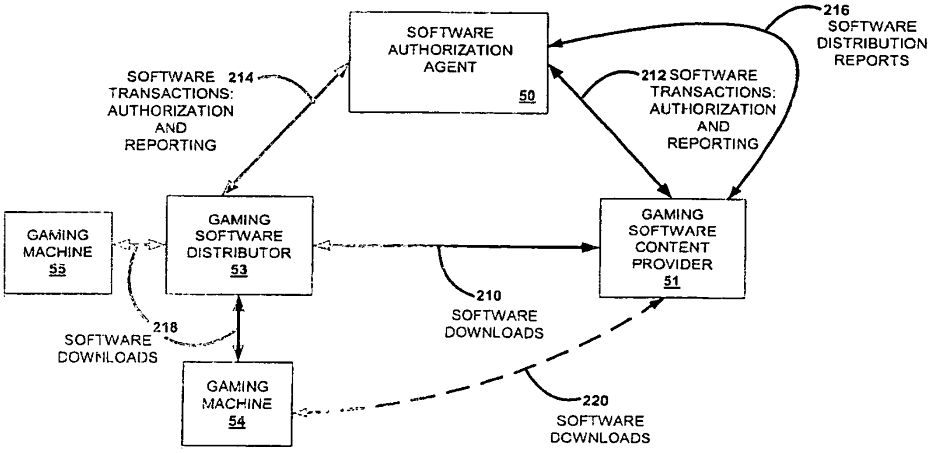
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT



(57) Abstract: A disclosed gaming machine may securely communicate with devices over a public network such as the Internet. The gaming machine utilizes a combination of symmetric and asymmetric encryption that allows a single gaming machine to securely communicate with a remote server using a public network. The secure communication methods may be used to transfer gaming software and gaming information between two gaming devices, such as between a game server and a gaming machine. For regulatory and tracking purposes, the transfer of gaming software between the two gaming devices may be authorized and monitored by a software authorization agent.

WO 03/085613 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PATENT APPLICATION

SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of US Patent Application No. 09/732,650 entitled "SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT ", filed December 7, 2000, naming Binh Nguyen as inventor, which is incorporated herein by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

This invention relates to game playing services for gaming machines such as slot machines and video poker machines. More particularly, the present invention relates to providing methods of communication for game services such as licensing and accounting on gaming machines.

There are a wide variety of associated devices that can be connected to a gaming machine such as a slot machine or video poker machine. Some examples of these devices are lights, ticket printers, card readers, speakers, bill validators, ticket readers, coin acceptors, display panels, key pads, coin hoppers and button pads. Many of these devices are built into the gaming machine or components associated with the gaming machine such as a top box which usually sits on top of the gaming machine.

Typically, utilizing a master gaming controller, the gaming machine controls various combinations of devices that allow a player to play a game on the gaming machine and also encourage game play on the gaming machine. For example, a game played on a gaming machine usually requires a player to input money or indicia of credit into the gaming machine, indicate a wager amount, and initiate a game play. These steps require the gaming machine to control input devices, such as bill validators and coin acceptors, to accept money into the gaming machine and recognize user inputs from devices, including key pads and button pads, to determine the wager amount and initiate game play. After game play has been initiated, the gaming machine determines a game outcome, presents the game outcome to the player and may dispense an award of some type depending on the outcome of the game.

The operations described above may be carried out on the gaming machine when the gaming machine is operating as a "stand alone" unit or linked in a network of some type to a group of gaming machines. As technology in the gaming industry progresses, more and more gaming services are being provided to gaming machines via communication networks that link groups of gaming machines to a remote computer that provides one or more gaming services. As an example, gaming services that may be provided by a remote computer to a gaming machine via a communication network of some type include player tracking, accounting, cashless award ticketing, lottery, progressive games and bonus games.

Typically, network gaming services enhance the game playing capabilities of the gaming machine or provide some operational advantage in regards to maintaining the gaming machine. Thus, network gaming services provided to groups of gaming machines linked over a dedicated communication network of some type have become very popular in the gaming industry. In general, the dedicated communication network is not accessible to the public. To justify the costs associated with the infrastructure needed to provide network gaming services on a dedicated communication network, a certain critical number of gaming machines linked in a network of some type must utilize the service. Thus, many of the network gaming services are only provided at larger gaming establishments where a large number of gaming machines are deployed.

A progressive game network offering progressive game services is one example where a group of gaming machines are linked together using a dedicated network to provide a network gaming service. The progressive game services enabled by the progressive game network increase the game playing capabilities of a particular gaming machine by enabling a larger jackpot than would be possible if the gaming machine was operating in a "stand alone" mode. The potential size of the jackpot increases as the number gaming machines connected in the progressive network is increased. The size of the jackpot tends to increase game play on gaming machines offering a progressive jackpot which justifies the costs associated with installing and maintaining the dedicated progressive game network.

Within the gaming industry, a particular gaming entity may desire to provide network gaming services and track the performance of all the gaming machines under the control of the entity. The gaming machines under the control of a particular entity may be globally distributed in many different types of establishments. Casinos, convenience stores, supermarkets, bars and boats are a few examples of establishments where gaming machines may be placed.

Figure 1 is a block diagram depicting gaming machines distributed in different establishments partially connected by a dedicated communication network for a typical gaming entity currently operating in the gaming industry. In FIG. 1, the gaming entity utilizes a central office 142. The gaming machines, 102, 104, 106, 114, 116, 136 and 138 for the gaming entity are located in two casinos, 110 and 122, and a store 140. A gaming entity may operate hundreds, thousands or ten of thousands of gaming machines. Since gaming is allowed in many locations throughout the world, the two casinos, 110 and 122, the central office 142 and the store may be distributed over a wide geographic area. For instance, the casino 110 may be located in Atlantic City, New Jersey, the casino 122 may be located in Australia, the central office may be located in Las Vegas, Nevada and the store may be located in Reno, Nevada.

Within the casinos, the gaming machines may be connected to one or more database servers via one or more dedicated networks. The database servers are usually located in the backroom of the casino. For instance, in casino 110, gaming machines 102, 104 and 106 are connected to a database server 100 via a dedicated network 108. The dedicated network 108 may be used to send accounting information and player tracking information from the gaming machines to the database server 110. In casino 122, the gaming machines 114, 116, 118 may send accounting information and player tracking information to a database server using the dedicated network 120. Other dedicated networks (not shown) in casinos, 110 and 112, may provide such network gaming services as bonus game play, progressive game play and cashless ticketing.

In casinos 110 and 122, the database servers 100 and 112 may store and process accounting data from the gaming machines in communication with the database servers. For instance, an accounting report detailing the performance of individual and groups of gaming machines may be generated from the data stored on the database servers 100 and 112. In addition, accounting data or reports may be sent to the database server 124 in the central office 142 from each casino. These reports may contain game performance data collected from a number of gaming machines as well as hotel operations data. The data from the casinos may be sent to the central office using an expensive dedicated leased line 132 using a frame relay network.

The database server 124 may be used to generate reports summarizing the performance of all the gaming machines within the gaming entity (e.g. casino 110, casino 122 and store 140). The reports may be accessed locally using the local access points 126 and 128 via the local network. In addition, reports may be remotely accessed using a dial in number for a limited number of users. For instance, an executive travelling on the road might view gaming machine performance data from the remote access point 134 where the remote access point 134 may be a hotel room.

For the store 140, the gaming machines, 136 and 138 may be leased by the store operator. However, the cost of a dedicated communication network for a small number of gaming machines is usually not justified. Thus, the gaming machines operate in a "stand alone" mode. While operating in "stand alone" mode, network gaming services are not available to these gaming machines. To obtain performance data for the gaming machines, 136 and 138, a route operator may regularly extract performance data from the machines and manually transmit the information to the central office 142. A route may consist of a number gaming machines located in various locations such as bars, convenience stores and supermarkets. Usually, the route operator manually extracts performance data for all of the gaming machines located on their route. For a large route, this process may be both time consuming and costly.

Within the gaming industry, there is some desire to provide centralized network gaming services, centralized data access and centralized data acquisition to all of the gaming machines or a larger proportion of gaming machines within a gaming entity. For the casinos, 110 and 122, the gaming machines are connected via local dedicated networks that do not generally allow, for security reasons, the gaming machines to communicate with devices located outside of the casino. For instance, in FIG. 1, the database server 124 may not directly communicate with gaming machine 102 or gaming machine 114. Further, as described above, a dedicated network is usually not cost effective for smaller gaming establishments. Thus, with the communication infrastructure described in FIG. 1 which is representative of the communication infrastructure currently available in the gaming industry, the implementation of centralized network gaming services, such as centralized data acquisition may be difficult.

A current barrier to providing centralized network gaming services and centralized data acquisition for gaming machines diversely distributed throughout a gaming entity is the complexity and costs of the dedicated communication networks currently used in the gaming industry. The costs of installing and maintaining a dedicated communication network typically limit the application of dedicated networks to large establishments with a large number of gaming machines. Further, even in the larger establishments, the dedicated network are usually only implemented locally and centralized network gaming services (e.g. from a central office) are usually not provided. In view of the above, it would be desirable to provide gaming communication methods for gaming machines that reduce the complexity of the gaming network environment, reduce the costs associated with adding new network gaming services and simplify the data acquisition process for gaming machines widely distributed within a gaming entity.

Another desire within the gaming industry is to electronically download gaming software from one or more remote locations to a gaming machine. The capability to electronically download gaming software is desirable because it may enable gaming machines to be quickly reconfigured to account for changes in popularity of various games played on the gaming machines and it may simplify software maintenance issues on the gaming machine such as gaming software updates. Currently, in a time consuming process, gaming software is manually loaded onto each gaming machine by a technician. The software is manually loaded because the gaming software is usually very highly regulated and in most gaming jurisdictions only approved gaming software may be installed on a gaming machine. Further, the gaming software is manually loaded for security reasons to prevent the source code from being obtained by individuals which might use the source code to try to find ways of cheating the gaming machine. In view of the above, it would be desirable to provide gaming software downloading methods for gaming machines that allow gaming software to be transferred electronically to the gaming machines from a remote location in a secure manner that satisfies regulatory requirements of the gaming jurisdiction where the gaming machine is located.

SUMMARY OF THE INVENTION

This invention addresses the needs indicated above by providing gaming machines that may securely communicate with devices over a public network such as the Internet.

The invention provides a combination of symmetric and asymmetric encryption that allows a single gaming machine to securely communicate with a remote server using a public network. The secure communication methods may be used to transfer gaming software and gaming information between two gaming devices such as between a gaming machine and a game server. For regulatory and tracking purposes, the transfer of gaming software between the two gaming devices may be authorized and monitored by a software authorization agent.

One aspect of the present invention describes a software authorization agent capable of generating a gaming software transaction record used to facilitate a transfer of gaming software between two gaming devices. The method may be generally characterized as comprising: 1) receiving a gaming software transaction request from a first gaming device; 2) authenticating an identity of the first gaming device 3) generating a gaming software transaction record comprising gaming software transaction information that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, the gaming software may comprise one or more gaming software components. The gaming software may be used to upgrade a gaming software component on the gaming machine or may be used to correct an error in a gaming software component on the gaming machine. The game of chance may be a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game. The gaming transaction information may be one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number, a gaming software identification number, a gaming software provider identifier, a transaction number, a number of allowable downloads and combinations thereof.

The first gaming device may be at least one of a gaming machine, game server and combinations thereof. The transfer of gaming software may be performed at least one of manually and electronically. The software authorization agent may communicate with the first gaming device using an local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. Further, the software authorization agent and the first gaming device may communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

In other embodiments, the gaming software transaction request comprises access information and gaming software identification information. The access information may be one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device. The gaming software identification information may bė one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

In additional embodiments, the method may comprise one or more of the following: a) comparing access information in the gaming software transaction request with access information stored in a database and when the compared access information does not match the access information stored in the database, denying the gaming software transaction request b) comparing gaming software identification information in the gaming software transaction request with gaming software identification information stored in a database and when the gaming software identification information does not match the access information stored in the database, denying the gaming software transaction request, c) generating an identification sequence; encrypting the identification sequence with a public encryption key for the first gaming device wherein information encrypted with the public encryption key is decrypted with a private encryption key used by the first gaming device; sending the encrypted identification sequence to the first gaming device where the identification sequence may a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device, d) receiving from the first gaming device a second identification sequence encrypted with a public encryption key used by the software authorization agent, decrypting the second identification sequence with a private encryption key corresponding to the public encryption key used by the software authorization agent; and comparing the second identification sequence to the identification sequence sent to the first gaming device to authenticate the identity of the first gaming device where the second identification sequence is a symmetric encryption key used to transfer gaming software between the first gaming device and the second gaming device, e) when the second identification sequence received from the first gaming device does not match the identification sequence sent to the first gaming device; denying the gaming software transaction request.

In yet other embodiments, the method may further comprise one or more of the following: i) storing the gaming transaction record information to a transaction database, ii) sending gaming software transaction information to the first gaming device where the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof, iii) sending a notification message to a gaming software provider identified in the gaming software request of a pending gaming software download request and iv) requesting a list of gaming software installed on a gaming device.

Another aspect of the present invention provides a method in a software authorization agent of regulating a transfer of gaming software between two gaming devices. The method may be generally characterized as comprising: 1) receiving a gaming software download request message with gaming software transaction information from a first gaming device; 2) validating the gaming software download request using the gaming software transaction information; 3) sending an authorization message to the first gaming device authorizing the first gaming device to transfer gaming software to a second gaming device; where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine. The game of chance may be a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game. The gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and combinations thereof.

In particular embodiments, the second gaming device may be at least one of a game server and a gaming machine. Further, the first gaming device may be a game server in communication with one or more gaming machines and the second gaming device may be a gaming machine. Also, the first gaming device may be a game server maintained by a gaming software provider and the second gaming device may be a game server in communication with one or more gaming machines. In addition, the first gaming device may be a game server maintained by a gaming software provider and the second gaming device may be a gaming machine. The software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. The software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

The method may also comprise one or more of the following: a) comparing the gaming transaction information in the gaming software download request message with gaming transaction information stored in a transaction database to validate the gaming software download, b) sending a message to the first gaming device denying authorization for the first gaming device to transfer gaming software to the second gaming device, c) decrypting the download request message, d) receiving a first download acknowledgement message from the first gaming device and receiving a second download acknowledgement message from the second gaming device, e) comparing gaming software transaction information in the first download acknowledgement message with gaming software transaction information in the second download acknowledgement message to validate that the gaming software has been correctly transferred where the gaming software transaction information in the first download acknowledgement message includes at least a first digital signature determined for the gaming software and the gaming software transaction information in the second download acknowledgement message includes at least a second digital signature determined for the gaming software, f) receiving the gaming software from the first gaming device; validating the gaming software; and sending the gaming software to the second gaming device, g) determining a digital signature for the gaming software; and comparing the digital signature with an approved digital signature for the gaming software stored in a database to validate the gaming software, h) storing gaming software transaction information indicating that a status of the download request where the status is at least one of authorized, pending, completed and void and i) requesting a list of gaming software installed on a gaming device.

Another aspect of the present invention provides a method in a software authorization agent of distributing gaming software transaction information. The method may be generally characterized as comprising: 1) receiving a gaming software transaction information request from a gaming device; 2) authenticating an identity of the gaming device; 3) querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device where the gaming software transaction database comprises a plurality of records of gaming software transactions; and 4) sending the requested gaming software transaction information to the gaming device where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, each gaming software transaction record may includes gaming software transaction information that describes a transfer of gaming software from a first gaming device to a second gaming device. For instance, the gaming transaction information may be one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time. The gaming software transaction database may also include a record of gaming software installed on one or more gaming devices.

The method may also comprise one or more of: a) generating a gaming transaction report that presents the set of gaming software transaction requested by the gaming device, b) generating a distribution of gaming software on a plurality of gaming machines at a specified time using the gaming software transaction information stored in the gaming software transaction database, c) generating a distribution of gaming software on a plurality of gaming machines for a plurality of times using the gaming software transaction information stored in the gaming software transaction database, d) generating a billing report and requesting a list of gaming software installed on the gaming device and e) storing the list of gaming software installed on the gaming device to the gaming software transaction database.

Another aspect of the present invention provides a method in a first gaming device of requesting a transfer of gaming software from a second gaming device. The method may be generally characterized as comprising: 1) generating a gaming software transaction request; 2) sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and 3) receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, the first gaming device may be a gaming machine and the second gaming device may be a game server. Also, the first gaming device may be a game server in communication with a plurality of gaming machines and the second gaming device may be a game server maintained by a gaming software content provider. The software authorization agent, the first gaming device and the second gaming device may communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. Further, the software authorization agent, the first gaming device and the second gaming device may communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

In other embodiments, the transfer of gaming software may be performed at least one of manually and electronically. The gaming software may comprise one or more gaming software components. The gaming software may be used to upgrade a gaming software component on the gaming machine or may be used to correct an error in a gaming software component on the gaming machine.

The gaming software transaction information in the method may be one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof. The gaming software transaction request may comprise access information and gaming software identification information. The access information may be one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device. The gaming software identification information may be one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

The method may also comprise one or more of the following: a) sending authentication information used to identify the first gaming device to the gaming software authorization agent, b) sending a message requesting the gaming software to the second gaming device, c) receiving the gaming software from the second gaming device, d) determining a digital signature for the gaming software and sending a message with at least the digital signature to the gaming software authorization agent and e) authenticating an identity of the second gaming device.

Another aspect of the present invention provides a method in a first gaming device of transferring gaming software to a second gaming device. The method may be characterized as comprising: 1) receiving a gaming software transaction request; 2) sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software; and 3) transferring the gaming software to the second gaming device; where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine.

In particular embodiments, the method may also comprise one or more of the following: i) receiving an approval of the gaming software transaction request from the gaming software authorization agent, ii) prior to transferring the gaming software, receiving a denial of the gaming software transaction request from the gaming software authorization agent; and terminating the transfer of the gaming software and iii) determining a digital signature for the gaming software and sending a message with at least the digital signature to the gaming software authorization agent.

In other embodiments, the first gaming device may be a gaming server and the second gaming device may be a gaming machine. Also, the first gaming device may be a gaming machine and the second gaming device may be a gaming machine. In addition, the first gaming device may be a game server maintained by a gaming software content provider and the second gaming device may be a game server maintained by a gaming entity. Further, the first gaming device may be a game server maintained by a gaming software content provider and the second gaming device may be a gaming machine maintained by a gaming entity. The software authorization agent, the first gaming device and the second gaming device may communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof. The software authorization agent, the first gaming device and the second gaming device may be communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

Another aspect of the present invention provides a software authorization agent for facilitating the transfer of gaming software between a plurality of gaming devices. The software authorization agent may be generally characterized as comprising: 1) a network interface allowing the authorization agent to communicate with each of the plurality of gaming devices; and 2) a processor configured or designed to (i) receive gaming software transfer requests via the network interface from a first gaming device for the transfer of gaming software from a second gaming device to a third gaming device (ii) approve or reject the gaming software transaction request wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine. The game of chance may be a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

In particular embodiments, the software authorization agent may further comprise one or more of the following: a) a transaction database containing gaming software transaction information where the gaming software transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time, b) a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software distribution reports based upon the gaming software transaction information, c) a memory containing software allowing the processor to analyze the gaming software transaction information stored in the transaction database and generate gaming software billing reports based upon the gaming software transaction information, d) a database storing public encryption keys for one or more of the plurality of gaming devices, e) a database storing identification information for one or more of the plurality of gaming devices and f) a database storing identification information for the gaming software that is transferred from the second gaming device to the third gaming device where the identification information for the gaming software is a digital signature, a title, a manufacturer, an identification number and combinations thereof.

In other embodiments, the first gaming device may be a hand-held computing device, the second gaming device may be a portable memory device storing the gaming software and the third gaming device may be a gaming machine. Also, the first gaming device may be a first gaming machine, the second gaming device may be a second gaming machine and the third gaming device may be the first gaming machine. In addition, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be a first gaming machine. Further, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be the first game server

Another aspect of the present invention may provide a first gaming device. The first gaming device may be generally characterized as comprising: 1) a network interface allowing communications between the first gaming device, a software authorization agent and one or more other gaming devices; and 2) a processor configured or designed to (i) send a request for the transfer of gaming software from a second gaming device to a third gaming device via the network interface to the software authorization agent (ii) receive from the software authorization agent a reply approving or rejecting the request for the transfer of the gaming software where the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine and d) a player tracking service on a gaming machine. The gaming software may comprise one or more gaming software components. The gaming software may be used to upgrade a gaming software component on one of the gaming devices and may be used to correct an error in a gaming software component on one of the gaming devices.

In particular embodiments, the first gaming device may further comprise one or more of the following: 1) a memory device that stores gaming software, 2) a master gaming controller that controls a game of chance played on the first gaming device where the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game and 3) a memory device that stores public encryption keys for one or more of the plurality of gaming devices and the software authorization agent. The network interface may be connected to at least one of a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof and the network interface may provide at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

In other embodiments, the first gaming device may be a portable gaming device. The first gaming device may be a first gaming machine, the second gaming device may be a second gaming machine and the third gaming device may be the first gaming machine. Alternatively, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be a first gaming machine. Further, the first gaming device may be a first game server, the second gaming device may be a second game server and the third gaming device may be the first game server.

Another aspect of the invention pertains to computer program products including a machine-readable medium on which is stored program instructions for implementing any of the methods described above. Any of the methods of this invention may be represented as program instructions and/or data structures, databases, etc. that can be provided on such computer readable media.

These and other features of the present invention will be presented in more detail in the following detailed description of the invention and the associated figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE **1** is a block diagram depicting gaming machines distributed in different establishments partially connected by a dedicated communication network for a typical gaming entity currently operating in the gaming industry.

FIGURE **2** is a perspective drawing of a gaming machine having a top box and other devices.

FIGURE **3** is a block diagram depicting gaming machines distributed in different establishments connected using a secure virtual network.

FIGURE **4** is an interaction diagram showing communications between a gaming machine, local server, local ISP and remote server over a public network.

FIGURE **5A** is a flow chart depicting a method of sending transaction data between a gaming machine and one or more remote servers.

FIGURE **5B** is a flow chart depicting a method of receiving transaction data between a gaming machine and one or more remote servers.

FIGURE **6** is a flow chart depicting a method of obtaining a game license on a gaming machine.

FIGURE **7** is a flow chart depicting a method of providing a game license to one or more gaming machines using a remote server.

FIGURE **8** is a block diagram of gaming software distribution network that uses a secure virtual network.

FIGURE **9** is a block diagram depicting software transactions in a gaming software distribution network controlled by a software authorization agent.

FIGURE **10** is an interaction diagram between a gaming software distributor, gaming software provider and a software authorization agent depicting an initialization of a gaming software transaction.

FIGURE **11** is an interaction diagram between a gaming software distributor, a gaming software provider and a software authorization agent depicting a gaming software transaction.

FIGURE **12** is an interaction diagram between a gaming software distributor, a gaming machine and a software authorization agent depicting a gaming software transaction.

FIGURE **13** is flow chart depicting a method in a software authorization agent initializing a gaming software transaction.

FIGURE **14** is flow chart depicting a method in a software authorization agent of authorizing a gaming software transaction.

FIGURE **15** is a block diagram of an interface used to provide information about gaming software transactions generated by a software authorization agent.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning first to FIGURE 2, a video gaming machine 2 of the present invention is shown. Machine 2 includes a main cabinet 4, which generally surrounds the machine interior (not shown) and is viewable by users. The main cabinet includes a main door 8 on the front of the machine, which opens to provide access to the interior of the machine. Attached to the main door are player-input switches or buttons 32, a coin acceptor 28, and a bill validator 30, a coin tray 38, and a belly glass 40. Viewable through the main door is a video display monitor 34 and an information panel 36. The display monitor 34 will typically be a cathode ray tube, high resolution flat-panel LCD, or other conventional electronically controlled video monitor. The information panel 36 may be a back-lit, silk screened glass panel with lettering to indicate general game information including, for example, a game denomination (e.g. $.25 or $1). The bill validator 30, player-input switches 32, video display monitor 34, and information panel are devices used to play a game on the game machine 2. The devices are controlled by circuitry (e.g. the master gaming controller) housed inside the main cabinet 4 of the machine 2. Many possible games, including mechanical slot games, video slot games, video poker, video black jack, video pachinko and lottery, may be provided with gaming machines of this invention.

The gaming machine 2 includes a top box 6, which sits on top of the main cabinet 4. The top box 6 houses a number of devices, which may be used to add features to a game being played on the gaming machine 2, including speakers 10, 12, 14, a ticket printer 18 which prints bar-coded tickets 20, a key pad 22 for entering player tracking information, a florescent display 16 for displaying player tracking information, a card reader 24 for entering a magnetic striped card containing player tracking information, and a video display screen 42. The ticket printer 18 may be used to print tickets for a cashless ticketing system. Further, the top box 6 may house different or additional devices than shown in the FIGs. 1. For example, the top box may contain a bonus wheel or a back-lit silk screened panel which may be used to add bonus features to the game being played on the gaming machine. As another example, the top box may contain a display for a progressive jackpot offered on the gaming machine. During a game, these devices are controlled and powered, in part, by circuitry (e.g. a master gaming controller) housed within the main cabinet 4 of the machine 2.

Understand that gaming machine 2 is but one example from a wide range of gaming machine designs on which the present invention may be implemented. For example, not all suitable gaming machines have top boxes or player tracking features. Further, some gaming machines have two or more game displays – mechanical and/or video. And, some gaming machines are designed for bar tables and have displays that face upwards. As another example, a game may be generated in on a host computer and may be displayed on a remote terminal or a remote gaming device. The remote gaming device may be connected to the host computer via a network of some type such as a local area network, a wide area network, an intranet or the Internet. The remote gaming device may be a portable gaming device such as but not limited to a cell phone, a personal digital assistant, and a wireless game player. Those of skill in the art will understand that the present invention, as described below, can be deployed on most any gaming machine now available or hereafter developed.

Returning to the example of Figure 1, when a user wishes to play the gaming machine 2, he or she inserts cash through the coin acceptor 28 or bill validator 30. Additionally, the bill validator may accept a printed ticket voucher which may be accepted by the bill validator 30 as an indicia of credit when a cashless ticketing system is used. At the start of the game, the player may enter playing tracking information using the card reader 24, the keypad 22, and the florescent display 16. Further, other game preferences of the player playing the game may be read from a card inserted into the card reader. During the game, the player views game information using the video display 34. Other game and prize information may also be displayed in the video display screen 42 located in the top box.

During the course of a game, a player may be required to make a number of decisions, which affect the outcome of the game. For example, a player may vary his or her wager on a particular game, select a prize for a particular game selected from a prize server, or make game decisions which affect the outcome of a particular game. The player may make these choices using the player-input switches 32, the video display screen 34 or using some other device which enables a player to input information into the gaming machine. In some embodiments, the player may be able to access various game services such as concierge services and entertainment content services using the video display screen 34 and one more input devices.

During certain game events, the gaming machine 2 may display visual and auditory effects that can be perceived by the player. These effects add to the excitement of a game, which makes a player more likely to continue playing. Auditory effects include various sounds that are projected by the speakers 10, 12, 14. Visual effects include flashing lights, strobing lights or other patterns displayed from lights on the gaming machine 2 or from lights behind the belly glass 40. After the player has completed a game, the player may receive game tokens from the coin tray 38 or the ticket 20 from the printer 18, which may be used for further games or to redeem a prize. Further, the player may receive a ticket 20 for food, merchandise, or games from the printer 18.

FIGURE 3 is a block diagram depicting gaming machines distributed in different establishments connected using a secure virtual network. Using the secure virtual network, network gaming services, data acquisition and data access may be provided to a large number of gaming machines distributed throughout a gaming entity 350 from a central location such as the central office 142. These services may be provided to gaming machines that have traditionally operated in a "stand alone" mode such as gaming machine 336 and 138 in the store 140. In FIG. 3, some of the communication infrastructure necessary to implement a secure virtual network for one embodiment of the present invention are described.

In one embodiment, the secured virtual network may be an IP based Virtual Private Networks (VPNs). An Internet-based virtual private network (VPN) uses the open, distributed infrastructure of the Internet to transmit data between corporate sites. A VPN may emulate a private IP network over public or shared infrastructures. A VPN that supports only IP traffic is called an IP-VPN. Virtual Private Networks provide advantages to both the service provider and its customers. For its customers, a VPN can extend the IP capabilities of a corporate site to remote offices and/or users with intranet, extranet, and dial-up services. This connectivity may be achieved at a lower cost to the gaming entity with savings in capital equipment, operations, and services. Details of VPN methods that may be used with the present invention are described in the reference, "Virtual Private Networks-Technologies and Solutions," by R. Yueh and T. Strayer, Addison-Wesley, 2001, ISBN#0-201-70209-6, which is incorporated herein by reference and for all purposes.

There are many ways in which IP VPN services may be implemented, such as, for example, Virtual Leased Lines, Virtual Private Routed Networks, Virtual Private Dial Networks, Virtual Private LAN Segments, etc. Additionally VPNs may be implemented using a variety of protocols, such as, for example, IP Security (IPSec) Protocol, Layer 2 Tunneling Protocol, Multiprotocol Label Switching (MPLS) Protocol, etc. Details of these protocols including RFC reports may be found from the VPN Consortium an industry trade group (http://www.vpnc.com, VPNC, Santa Cruz, California).

In FIG. 3, a number of embodiments of IP VPN services are implemented to allow connectivity between the various gaming machines and database servers in the gaming entity. For instance, the gaming machine 336 in the store 140 may directly communicate with the database server 124 in the central office 142 via the internet 304. The communication path between the gaming machine 336 and the database server 124 may be the local ISP 314, a number of routers on the Internet 304, a local ISP 313 accessed by the central office 142, the router 302 and the firewall 300. The firewall may be hardware, software or combinations of both that prevent illegal access of the gaming machine by an outside entity connected to the gaming machine. For instance, an illegal access may be an attempt to plant a program in the database server that alters the operation of the database server or allows someone to steal data. The internal firewall is designed to prevent someone such as a hacker from gaining illegal access to the gaming machine and tampering with it in some manner. Firewalls and routers used in FIG. 3 may be provided by CISCO Systems (San Jose, California).

The network interface between the gaming machine 336 and the local ISP may be a wireline interface, such as a wired Ethernet connection, a wired ATM connection, or a wired frame relay connection, or a wireless interface, such as a wireless cellular interface. For instance, the gaming machine 336 may include a wireless modem and an antenna that allows the gaming machine to connect with the local ISP 314. As another example, the gaming machine may contain a dial-in modem, a DSL modem or a cable modem that allows that gaming machine 336 to connect with the local ISP 314 via a coaxial cable or phone line 337. The gaming machine 336 may also contain an internal firewall to prevent illegal access to the gaming machine. Other gaming machines, such as 338 and 340, located at various locations throughout the gaming entity 350 may also include the hardware described above and transmit information via a local ISP, such as 315 and 320, and the Internet 304, to a remote server such as the database server 124 in the central office 142.

Using the network interface, the gaming machine 336 may send game performance data, game usage information and gaming machine status information or any other information of interest generated on the gaming machine from one or more gaming transactions to the database server 124 located in the central office or some other remote server. Using this method, the need to manually gather data from the gaming machine using a route operator may be eliminated, which may reduce gaming machine operating costs and may provide better tracking of the performance of gaming machines, such as 336, that have traditionally operated in a "stand alone" mode.

For security purposes, any information transmitted from the gaming machine 336 over a public network to a remote server may be encrypted. The encryption may be performed by the master gaming controller or by another logic device located on the gaming machine. In one embodiment, the information from the gaming machine may be symmetrically encrypted using a symmetric encryption key where the symmetric encryption key is asymmetrically encrypted using a private key. The public key may be obtained by the gaming machine 336 from a remote public key server. The encryption algorithm may reside in processor logic stored on the gaming machine. When a remote server receives a message containing the encrypted data, the symmetric encryption key is decrypted with a private key residing on the remote server and the symmetrically encrypted information sent from the gaming machine is decrypted using the symmetric encryption key. In addition, a different symmetric encryption key is used for each transaction where the key is randomly generated. Symmetric encryption and decryption is applied to most of the information because symmetric encryption algorithms tend to be 100-10,000 faster than asymmetric encryption algorithms.

Information needed to apply the encryption algorithm such as private keys and public keys may be stored on a memory residing in the gaming machine 336 where the memory may be a flash memory, an EPROM, a non-volatile memory, a ROM, a RAM, a CD, a DVD, a tape drive, a hard drive or other memory storage device. Typically, the public keys are stored on a writeable media such as a hard drive while the private keys are stored on a read only memory such as an EPROM or a CD-ROM. The same or a different memory residing on the gaming machine 336 may also include information used to authenticate communications between the gaming machine 336 and a remote server, such as 124. For instance, a serial number or some other identification numbers may be used by the firewall 300 or the database server 124 to authenticate the sender of a message.

The encrypted communications from the gaming machine 336 to a remote server may be implemented using a TCP/IP communication protocol. Thus, the encrypted information from the gaming machine may be encapsulated in multiple information packets and sent to the IP address and/or an unique ID (UID) of a remote server. The gaming machine 336 may contain a memory storing a number of IP addresses and/or unique IDs (UIDs) of remote servers or other devices where the gaming machine may send information. Prior to sending a message, the gaming machine may look up the IP address and/or the UID of the remote server or destination device.

For each information packet, the gaming machine may generate one or more signatures and may append them to the information packet. The signature may allow the recipient of the packet to unambiguously identify the sender of the packet as well as to determine if the correct amount of data was received. For instance, the signature may include a checksum of the data that was sent. Further, the information packet may contain routing information allowing subsequent communication with the gaming machine, such as an IP address and/or an UID of the gaming machine. General details of these types of processes, such as TCP/IP implementation and data authentication, are described in the text "Mobile IP Unplugged" by J. Solomon, Prentice Hall and the text "Computer Networks", A. S. Tanenbaum, Prentice Hall. Both of these references are incorporated herein by reference in their entireties and for all purposes.

Using the communication infrastructure and methods described above a gaming machine or other device connected to a remote server may request one or more gaming services from a remote server. For instance, a gaming machine may send a game license request to the remote server 124. A gaming machine may store code to play one or more games controlled by the master gaming controller such as a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game. Traditionally, installing a new game has involved manually exchanging (e.g., by hand) an EPROM (e.g. a read-only memory) containing the game on the gaming machine. Using the communication infrastructure described above, the gaming machine 336 may request a game license for one or more games stored in the gaming machine from a remote server acting as a game license server such as 124. The game license server may send a game license reply message containing a game license which allows the gaming machine to present the one or more games stored on the gaming machine. These game license requests may be performed prior to each game or the license may allow game play for some finite time period. For instance, the game license may be an annual license, a monthly license, a daily license, a per-use license or a site license. Details of the game license request and reply process between a gaming machine and a remote server are described with reference to FIGs. 6 and 7.

In another example, the gaming machine 336 may send a maintenance request message to a remote server when the gaming machine malfunctions. After receiving the maintenance request message, the remote server may perform one or more remote diagnostics on the gaming machine 336 via one or more diagnostic request messages. The remote diagnostics may include both software and hardware diagnostics. In addition, the remote server may develop service priority list based upon a plurality of maintenance requests received from a group of gaming machines in communication with the remote server. In yet another example, a remote server may obtain software version information or gaming configuration information, from gaming machine 336, by sending a software version request message or a gaming configuration request message to the machine.

Information contained in these messages may be used to provide software updates and gaming configuration updates to the gaming machine 336.

In a further example, the gaming machine 336 may generate a digital signature or some other type of unique identification information and may send a digital signature verification request or an identification verification request to a remote server. The verification request may be part of an electronic fund transfer. After receiving authorization from the remote server in an authorization reply, the gaming machine 336 may send a fund transfer request with fund transfer information to the remote server and may receive a fund transfer reply authorizing the gaming transaction.

A remote server may also provide performance reports or other services for the gaming machine 336. For instance, the gaming machine 336 may send a report request message to the remote server 124 requesting a performance report for the gaming machine over some prior time period. After remote server generates the report, it may be sent back to the gaming machine 336 or some other access point for display. For instance, the report may be displayed on a display screen of the gaming machine 336, a computer 316 located in the store 140 or on a portable network access point 134 located outside of the store.

An advantage of the virtual network described above is that it allows gaming services such as data acquisition, game licensing and report generation to be provided a single gaming machine without the use of a dedicated network which are typically expensive. This advantage may potentially increase the utility of a gaming machine while reducing the costs associated with operating and maintaining a machine. In particular, for gaming establishments with a small number of gaming machines operating in a "stand alone" mode, a virtual network may be the only viable way to provide cost effective gaming services via a network. The virtual network is enabled by an encryption scheme which utilizes multiple key encryption and symmetric encryption keys to provide secure communication of sensitive gaming data. For each session, the symmetric encryption keys may be randomly generated or may be rotated by selecting from a pool of keys.

The methods described above may be applied and may be advantageous to any gaming machine in the gaming entity 350. Also, many different embodiments of the methods are possible. For instance, using a wireless network interface, gaming machine 338 in Casino 110 may send game license requests or other requests to the database server via the router 308, the dedicated line 322, router 302 and the firewall 300. As another example, using a wireline network interface, such as a wired Ethernet connection, a wired ATM connection or a wired frame relay connection, gaming machine 340 in casino 122 may send may send a gaming report request to the database server 100 in casino 110 via the database server 112, the firewall 310, the router 312, the local ISP 320, the internet 304, the local ISP 315, the router 308 and the firewall 306. When a dedicated communication network is used, encryption may be optional over the dedicated network, e.g. if a dedicated network was used between the gaming machine 340 and the database server 112, the gaming machine 340 may not use encryption to send information to the database server 112. However, the database server would apply an encryption scheme such as the one described above before sending out information over a public network. Returning to the example, the database server 100 may serve as a regional report server. After generating a gaming report reply message to the gaming report request message from gaming machine 340, the database server 100 may send a message to the database server 124 in the central office 142 acknowledging that a report was generated.

The virtual network may also allow remote access to gaming information such as gaming performance information at various gaming establishments in the gaming entity from mobile access points. For example, the remote access point 134 may be a portable computer with a wireless modem. Typically, the remote access point 134 will have a high level of security such as special access software. Using the remote access point 134, a user such as a travelling employee of the game entity may access gaming information at casino 110 or casino 122 via the local ISP 314. The access may be routed through the central office 142 or may be routed directly to one of the casinos bypassing the central office. In addition, different access privileges may be accorded to different remote users. For instance, one remote user may be able to access information from any establishment in the gaming entity while another may only be able to access information from a particular establishment.

FIGURE 4 is an interaction diagram showing communications between a gaming machine, local server, local ISP and remote server over a public network. The diagram provides some details of a communication process between a gaming machine 340 in casino 122 and the database server 122 in the central office 142 as described with reference to FIG. 3 for one embodiment of the present invention. In 400, the gaming machine 340 may perform a gaming transaction such as a coin-in, initiating a game play or a coin-out. In 402, the gaming machine 340 symmetrically encrypts gaming transaction data from one or more gaming transactions using a symmetric encryption key. In 404, the symmetric encryption key may be encrypted using an asymmetric encryption key such as public key in a public-private encryption scheme which may only be decrypted using a matching private key at the message destination. For each gaming transaction, a symmetric encryption key is selected from a pool of symmetric encryption keys or randomly generated. Thus, the symmetric encryption key varies from gaming transaction to gaming transaction. When a dedicated or private communication network is used and extra security is desired, the symmetric key may also be asymmetrically encrypted with an asymmetric encryption key which is non-public. In 406, a message may be generated and the encrypted data and key may be sent to a local server 112.

As previously described with reference to FIG. 3, the encrypted information may be encapsulated in multiple information packets using a TCP/IP communication protocol. In addition other communication protocols such as a frame relay communication protocol, an ATM communication protocol or combination of protocols may also be utilized. Prior to sending the data, the gaming machine may look up the IP address and/or the UID of the remote server which may be stored in a memory on the gaming machine. When a dedicated communication network is used between the gaming machine and the remote server, such as local server 112, the encryption process performed by the gaming machine may be optional. Prior to sending the message, the gaming machine 340 may generate one or more signatures that allow the receiver of the message to authenticate the sender of the message as well as the accuracy of the data contained in the message. These signatures may be appended to the message or incorporated in the message in some manner.

In one embodiment, the gaming machine 340 may by-pass the local server and may send a message to the remote server 124 via the local ISP 320. In some embodiments, a local server may not be available to the gaming machine, such as gaming machine 336 in the store 140 in FIG. 3. In 438, when communications are not established between the local ISP 320 and the gaming machine 340, the gaming machine may contact the local ISP 320 using a network interface and establish communications with the local ISP 320. In 440, the gaming machine 340 may send a message with the encrypted gaming transaction data and the encrypted symmetric key to the IP address and/or the UID of the remote server 124 via the local ISP 320.

In 408, the local server 112 receives a message from the gaming machine 340. The local server 112 may authenticate that the message was sent from the gaming machine 340 and determine that the data sent in the message is complete. Next, the local server 112 may decrypt the symmetric encryption key using a private asymmetric encryption key stored on the local server. In 410, the local server decrypts the transaction information included in the message using the symmetric encryption key. In 412, the local server 112 may process and store the data generated from the gaming machine.

In 414, gaming transaction data from the gaming machine 340 may again be symmetrically encrypted using a symmetric encryption key. The gaming transaction data may also include additional gaming transaction data from other gaming machines. In one embodiment, the gaming transaction data may include game usage data that allows a game played on a gaming machine to be billed on a per use basis. In 416, the symmetric encryption key may be asymmetrically encrypted using an asymmetric encryption key such as a public key exchanged between the local server and the remote server 124 and a message containing the encrypted data may be generated. Prior to sending the message, the local server 112 may generate one or more signatures that allow the receiver of the message to authenticate the sender of the message as well as the accuracy of the data contained in the message. These signatures may be appended to the message or incorporated in the message in some manner. In 418, when a communication has not been established between the local server 112 and a local ISP 320, the local server may contact the local ISP 320 and establish communications using an appropriate communication protocol such as TCP/IP. In 420, the local server 112 may send a message with the encrypted gaming transaction data and the encrypted symmetric key to the IP address and/or the UID of the remote server 124 via the local ISP 320.

In 422, the local ISP 320 processes and forwards the message from the local server 112 or the gaming machine 340 to the public network 304. In 424, the public network processes the message from the local ISP 320 and forwards it to the remote server 124. Processing of the message by the local ISP 320 and the public network 304 may involve routing multiple data packets comprising the message.

In 426, the remote server receives a message from the gaming machine 340 or the local server 112. The remote server 124 may authenticate the sender of the message using one or more signatures included in the message and determine the accuracy of the data of the message. For instance, the remote server may generate a check sum, CRC, or other verification of the data in the message and compare that with a check sum, CRC, or other verification of the data generated by the sender of the message. Next, the asymmetrically encrypted symmetric encryption key may be decrypted using a private key residing on the remote server124. In 428, the symmetric key may be used to decrypt the symmetrically encrypted data. In 428, the remote server may process and store the data. The message from the gaming machine or local server 112 may include a request of some type for the remote server. In 430, the remote server may implement the request. For instance, the message may contain a request for a game license (See FIG. 6 and 7), a request for a report or a request for some other game service.

In 431, the remote server may generate a reply message. The reply message may include an acknowledgement that the original message was received and may also include requested information. For instance, the remote server may request diagnostic data or a report of some type from the gaming machine. The data in the reply message may be encrypted. Thus, in 442, the transaction reply data may be symmetrically encrypted using a symmetric encryption key and in 443 the symmetric encryption key may be asymmetrically encrypted using the recipient's public key. When the reply message is received by a gaming device, such as the gaming machine 340 or the local server 112, the gaming device may decrypt (e.g., as in 426) the asymmetrically encrypted symmetric encryption key using a private key stored on the gaming device.

In 432, the remote server sends the reply message to the local server 112 and/or the gaming machine 340 via the public network 304. The remote server 124 may access the public network via an ISP local to the remote server 124. In 434, the local server may receive a reply message and store data included in the message. In some embodiments, the acknowledgement may be forwarded to the gaming machine 340. In other embodiments, the local server 112 may be by-passed or a local server 112 may not be available to the gaming machine 340 and the reply message may be received directly by the gaming machine 340 via the local ISP 320.

FIGURE 5A is a flow chart depicting a method 500 of sending transaction data between a gaming machine and one or more remote servers. Although the method is described on a gaming machine for illustrative purposes, the method is not so limited and may be applied on other gaming devices such as the remote servers described above.

Thus, as described with reference to FIG. 4, the gaming machines and remote servers may send messages with encrypted data to one another in a similar manner. In 505, the gaming machine performs one or more gaming transactions. For example, a gaming transaction may be a coin-in or a pay-out on the gaming machine. Information from one or more gaming transactions may be stored in a non-volatile memory located on the gaming machine. In 510, the gaming transaction data may be symmetrically encrypted using a symmetric encryption key. The encrypted gaming transaction data may include data generated from a single gaming transaction or multiple gaming transactions. The symmetric key may be selected from a pool of symmetric keys or may be randomly generated such that the symmetric key is varied each time gaming transaction data is encrypted. In 515, the symmetric encryption key may be asymmetrically encrypted using a public key that was previously exchanged between the gaming machine and the recipient of the message. In the case, where a dedicated network is used the asymmetric encryption key is non-public i.e. it is not readily available to the public.

In 518, the gaming machine generates a message containing the symmetrically encrypted gaming transaction data and the asymmetrically encrypted symmetric encryption key over a communication protocol such as but not limited to TCP/IP. The message may include additional information such as signatures to authenticate the sender of the message, signatures to validate the accuracy of the data included in the message and an IP address and/or an UID of the sender as well as other message routing information. The message may also include a request for the recipient to return information to the gaming machine. For instance, the gaming machine may request a remote server to provide a gaming license that allows a game to be played on the gaming machine.

In 520, when communications have not been established between the gaming machine and a local ISP, the gaming machine may contact a local ISP. The gaming machine may also send messages to a local ISP by sending the message first to a local server which may then forward the message to the local ISP. The gaming machine may contact the local ISP using a communication protocol such as TCP/IP and a network interface such as a wireless modem. In 525, the gaming machine sends the message generated in 518 to a remote site such a game license server, a report server or some other device via the local ISP. In 530, the gaming machine may determine when an acknowledgement message has been received from the remote site. When an acknowledgement message has not been received, the gaming machine may resend the message one or more times. When the acknowledgement message has been received, the gaming machine may repeat process 500.

FIGURE **5B** is a flow chart depicting a method 550 of receiving transaction data between a gaming machine and one or more remote. Although the method is described on a remote server for illustrative purposes, the method is not so limited and may be applied on other gaming devices such as the gaming machines described above. Thus, as described with reference to FIG. 4, the gaming machines and remote servers may receive and process messages with encrypted data from one another in a similar manner.

In 555, the remote server receives a message with encrypted gaming transaction data from a gaming machine, another remote server or some other gaming device. In 560, an asymmetrically encrypted symmetric encryption key included in the message in 555 is decrypted using a private key stored on the remote server. In 565, the decrypted symmetric encryption key may be used to decrypt symmetrically encrypted gaming transaction data included in the message. In 570, the decrypted gaming transaction data or any service requests contained in the message are processed. For instance, gaming transaction data in the message may be archived.

FIGURE **6** is a flow chart depicting a method 600 of obtaining a game license on a gaming machine providing game play of one or more games. In 605, a gaming machine initiates a gaming license request. In one embodiment, the gaming license request may be initiated when a current gaming license on the gaming machine is about to expire. In another embodiment, the gaming license request may be initiated in response to a player on a gaming machine requesting a game play of a particular game. In 610, game license request data used to provide and implement gaming licenses is encrypted. The game license data may be encrypted using a symmetric encryption key and the symmetric encryption key may be asymmetrically encrypted using a public key. The game license request data may include the symmetric encryption key, a serial number of the software corresponding to one or more games or some other software identification number, a serial number of the gaming machine as well as other machine identification information, game owner identification information, game usage data including the number of times a gaming license has been used and license expiration data. The game usage data may be used to bill the gaming entity owning the gaming license for use of the game license. The software identification number in the gaming license data may correspond to one or more games such as a video slot game, a mechanical slot game, a video poker game, video blackjack game and video pachinko game.

In 612, a game license request message is generated with the encrypted game license request data. The game license request message may be sent to a remote server using a TCP/IP protocol. Thus, the game license request message may include an IP address and/or an UID of the remote server as well as an IP address and/or an UID of the gaming machine. The gaming machine may store the IP addresses and/or the UIDS of one or more remote servers in a memory residing on the gaming machine. Prior to sending the gaming license request message, the gaming machine may look-up the IP address and/or the UID of the destination remote server. The gaming license request message may include one or more signatures used by the recipient of the message to unambiguously identify the sender of the message and to validate the accuracy of the data contained in the message. The signatures may be generated by the gaming machine and appended to the message.

In 615, when communications between the gaming machine and a local ISP have not been established, the gaming machine may contact a local ISP and establish communications. In one embodiment, the gaming machine may not directly contact a local ISP. Instead, the gaming machine may contact and may send the gaming license request message to a local server which contacts a local ISP and sends the gaming license request message. In another embodiment, the gaming machine may send unencrypted gaming license request data to the local server. The local server may encrypt the gaming license request data, generate a gaming license request message and send the message to a remote server such as a gaming license request server.

In 620, the gaming machine sends the gaming license request message to a remote site such as a game license server via the local ISP. When a communication protocol such as TCP/IP is used, the message may be encapsulated in multiple information packets. In 625, the gaming machine determines whether an acknowledgement from the remote site has been received. When the acknowledgement from the remote site has not been received, the gaming machine may resend the message according to 620.

In 628, the gaming machine receives a game license reply message. The game license reply message may include a number of signatures used by the gaming machine to authenticate the sender of the message and to validate the data contained in the message. In 630, the gaming machine may decrypt an asymmetrically encrypted symmetric encryption key using a private key stored in memory on the gaming machine and then decrypt the game license reply data with the symmetric encryption key. The game license reply data may include a game license for one or more games available on the gaming machine. The game license may be an identification number of some type that allows software on the gaming machine corresponding to the license to be executed. The game license reply data may also include an expiration date for the license. In 635, the gaming machine may update game license data stored on the gaming machine when a new game license was included in the game license reply data. In one embodiment, the game license request message may include game usage data without a request for a new license. In this case, the game license reply message may include an acknowledgement that the game license request message was received but may not contain a new game license.

An advantage of the game license request method is that a gaming machine owner may be able operate gaming machines including many different types of games but only pay for each game on a per use basis. In a "pay-as-you go" billing scheme, an operator of the gaming machine is charged each time a game is played on the gaming machine. At regular intervals, a usage fee may be paid by the operator of the gaming machine to the owner's of the gaming software used on the gaming machine. The cost per use of each game may be varied from game to game and these costs may change with time. For example, the cost per use charged for newer gaming titles may be higher than the cost per use charged for older gaming titles. Thus, when a particular game is unpopular, the costs to the gaming machine operator are minimized as compared to when the gaming machine operator pays up front for a gaming machine with a game that receives little game play.

Another advantage of the game license request method is that it may also be used for other types of game service requests. For instance, a report request message with encrypted report request data may be generated in the manner described above and sent to a remote server via a local ISP. When a report reply message is received via the local ISP containing a report, the report may be displayed to the gaming machine. In another example, a gaming machine may send a maintenance request message via a local ISP in a manner described above.

FIGURE 7 is a flow chart depicting a method 700 of providing a game license to one or more gaming machines using a remote server. In 705, the remote server receives a game license request message from a gaming machine, local server or some other device. The message may have been received via a local ISP in communication with the remote server. As described above, although not shown in the flow chart, the remote server may also receive a report request, maintenance request or some other transaction request from the gaming machine, local server or remote device. After receiving the message, the remote server may authenticate the sender of the message using one or more signatures contained in the message and validate the accuracy of the data in the message using one or more signatures contained in the message. For instance, the remote server may generate a checksum on the data in the message and compare it with a checksum generated by the gaming machine on the data in the message which was appended to the message.

In 710, the remote server may decrypt a symmetric encryption key included in the game license request message using a private encryption key. With the symmetric encryption key, the remote server may decrypt the game license request data. The game license request data may include a serial number of the software corresponding to one or more games or some other software identification number, a serial number of the gaming machine as well as other machine identification information, game usage data including the number of times a gaming license has been used, license expiration data and game owner identification information.

In 715, using the serial number of the gaming machine and the other machine identification information the remote server may identify the gaming machine. The serial number of the gaming machine is one example of an UID that may be used with the present invention. A table of gaming machine identification information may be stored on the remote server. From the gaming machine identification information, the remote server may be able to determine the type of gaming machine and the games available on the gaming machine. In 720, when appropriate, the remote server may generate a new gaming license for the gaming machine. If the gaming license request message includes a request for a gaming license not available on the gaming machine or not enabled for some reason on the gaming machine, then the gaming license request may be denied. In another example, the game license request may include game usage information for billing purposes and a new game license may not be required.

In 725, when a new game license is generated, the game license reply data including the new game license may be encrypted with a symmetric encryption key and the symmetric encryption key may be asymmetrically encrypted with a public key. In other cases, the game license reply message may include an acknowledgement that the message was received but may not include a new game license. In 730, the information regarding the game license request such as the machine identification information, a type of game license request (e.g. type of game), a time of the request and whether the request was granted may be stored on the remote server.

In 732, a game license reply message with the game license reply data may be generated. In 735, via a local ISP and the Internet, the game license reply message may be sent to the local server and/or the gaming machine. In 740, a billing request message based upon the game usage data contained in the game license request or the type of license requested may generated. In 745, the billing request message may be sent to the gaming machine owner identified in the gaming license request message.

FIGURE 8 is a block diagram of gaming software distribution network that uses a secure virtual network. In the present invention, gaming software may be transferred between various gaming devices, in a gaming software distribution network 90, after receiving authorization from a gaming software authorization agent 50. The gaming software authorization agent 50 may be a conventional data server including but not limited to a database 202, a router 206, a network interface 208, a CPU 204, a memory 205 and a firewall (not shown). The CPU 204 executes software to provide the functions of the authorization agent 50 as will be described below in more detail. In general, the gaming software authorization agent 50 approves all gaming software transactions between two gaming devices in the gaming software distribution network and stores a record of the gaming software transactions. Database 202 may be used to store gaming software transaction records. Details of the gaming devices and network connections used in the gaming distribution network 90 are described in FIGURE 8. Details of the types of gaming software transaction that may be implemented in gaming software distribution network and the implementation of the transactions for some embodiments of the present invention are described with respect to FIGs. 9-14.

In the gaming industry, gaming software that is used to play a game of chance on a gaming machine is typically highly regulated to ensure fair play and prevent cheating.

Thus, at any given time, it is important for a gaming regulatory entity to know what gaming software is installed on a gaming machine at any particular time. Currently, gaming software is often programmed into an EEPROM and installed on a gaming machine. When the EEPROM is installed in the gaming machine, it is manually checked by a representative of the gaming regulatory board prior to installation to ensure approved gaming software is being installed on the gaming machine. This process is time consuming and relatively inflexible. In the gaming industry, there is a desire to simplify the gaming software installation process so that gaming machine operators may more easily reconfigure gaming machines with different gaming software to respond to shifting customer tastes and demands. The gaming software authorization agent 50 meets this need by allowing gaming software to be electronically transferred between gaming devices, such as game servers and gaming machines, in a manner that may be easily monitored and regulated. For instance, the software authorization agent 50 may be maintained or supervised by a gaming regulatory agency. However, the software authorization agent 50 may also be maintained by a gaming entity that controls many gaming properties to track software distributions on various gaming machines. In addition, besides monitoring electronic transfers of gaming software, the software authorization agent 50 may also be used to store a record of any change of gaming software on a gaming machine such as changes resulting from a manual installation of gaming software. For instance, a technician may manually load gaming software on to a gaming machine using a portable memory device storing the gaming software.

Details of gaming devices and the network connections in the gaming software distribution network are now described. In the present invention, gaming software may be transferred between gaming software providers, such as 51 and 52, gaming software distributors, such as 53 and 60, and gaming machines, such as 54, 55, 56, 57, 58 and 59. A gaming software provider may be a gaming device, such as a game server, that is maintained by a gaming software developer, such as IGT (Reno, Nevada), that develops gaming software for various gaming platforms. A gaming software content provider, such as 51 and 52, may maintain a plurality of gaming software titles, versions of gaming software titles and gaming software components that may be requested by another gaming device for an electronic download. The gaming software content provider may download gaming software to various customers after the customer has entered a licensing agreement with the content provider. Some details of obtaining game licenses for operating gaming software on a gaming machine have been described above with respect to FIGs. 6 and 7.

A set of gaming software components may be executed on a gaming machine to play a gaming of chance. The game of chance may include gaming software components used to play a bonus game in conjunction with the game of chance. Thus, a complete set of gaming software components used to play a game of chance may be downloaded or a portion of the gaming software components needed to play a game the game of chance may be downloaded. For instance, a complete package of gaming software components may be downloaded to replace a game executed on a gaming machine with a new game. As another example, a single game software component may be downloaded to fix an error in a game of chance executed on the gaming machine. In yet another example, a set of gaming software components may be downloaded to install a new graphical "feel" for the game of chance while other gaming software components for the game are not changed. In the present invention, any gaming device that stores gaming software for downloads may download a complete set of the gaming software components used to play the game of chance or portions of a complete set of the gaming software components. Some examples of gaming software components may include but are not limited to: 1) a banking modules for coin-in, coin-out, credits cards, fund transfers, 2) security modules for tracking security events such as door open, lost power, lost communication, 3) bet modules for handling betting configurations such as a number of paylines, a number of coins per line and denominations, 4) communication modules allowing a gaming device to communicate with other gaming devices using different communication protocols and 5) an operating system modules used in an operating system installed on the gaming machine. Details of some of the gaming software components that may be downloaded in the present invention are described in co-pending U.S. application no. 10/040,239, by LeMay et al., filed on January 3, 2002 and titled "Game Development Architecture That Decouples The Game Logic From The Graphics Logic," which is incorporated herein in its entirety and for all purposes.

Gaming software related to other aspects of game play and operation of a gaming machine may also be authorized and downloaded using the methods and hardware of the present invention. For instance, device drivers used to operate a particular gaming device may be downloaded from a content provider or another gaming device. As another example, gaming software used to provide player tracking services and accounting services may be downloaded from a content provider or another gaming device. Even when the gaming software is not regulated by a gaming entity, it may be useful to perform the authorization process because the transaction records may be used to track the distribution of the gaming software on various gaming devices. The transaction records may be helpful to both providers of gaming software and operators of gaming devices in determining necessary upgrades and maintenance of gaming software on a gaming device such as a gaming machine.

A gaming software distributor, such as 53 and 60, may maintain a plurality of gaming software titles, versions of gaming software titles and gaming software components that may be transferred to another gaming device, such as a gaming device, for an electronic download. The gaming software distributors, such as 53 and 60, may be gaming devices, such as game servers, that are maintained by a gaming entity such as a casino. For instance, game server 53 may be operated by a first casino and game server 60 may be operated by a second casino. The game servers may store gaming software that has been licensed to the gaming entity from one or more gaming software providers such as 51 and 52. In one embodiment, a game server may also be a gaming machine. One example of a game server that may be used with the present invention is described in co-pending U.S. patent application 09/042,192, filed on June 16, 2000, entitled "Using a Gaming Machine as a Server" which is incorporated herein in its entirety and for all purposes.

The game servers operated by a gaming entity may be used to provide gaming software to a plurality of gaming machines. For instance, game server 53 may be used to provide gaming software to gaming machine 54, 55, 56 and game server 60 may be used to provide gaming software to gaming machines 57, 58 and 59. In one embodiment, the game servers may be programmed to download gaming software in response to a software request on a gaming machine. For instance, a game player playing a game on a gaming machine, such as 55, may request to play a particular game of chance on the gaming machine 55 which is downloaded to the gaming machine from the game server 53. In another embodiment, the game servers, such as 53 and 60, may be used to update and reconfigure the gaming software on one or more gaming machines. For instance, the game server 53, may be used to regularly change the games of chance or bonus games of chance available for play on gaming machines 54, 55 and 56.

In the present invention, gaming software transferred between two gaming devices and communications between two gaming devices may use a variety of network architectures including but not limited to local area networks, wide area networks, private networks, a virtual private network, the Internet 304 and combinations thereof. Details of methods of using the Internet 304 in a secure manner have been described with respect with 3, 4, 5A and 5B.

In one embodiment, gaming software and other gaming information may be transferred between two gaming devices using a satellite connection. For instance, the gaming information transferred via satellite may include but is not limited to metering information generated on the gaming machine. In a gaming device using a satellite communication system, the gaming device is connected to a satellite dish. For instance, a gaming machine located in a store, as described with respect to FIG. 3, or a cruise ship may use a satellite connection. Two standard coaxial cables may connect the gaming device to the satellite dish. The gaming device, such as a gaming machine, may include a satellite modem to enable the satellite connection.

The satellite dish may send requcsts to the Internet 304 and receive Internet content via the satellite 72. The satellite 72, in turn, may communicate with a hub facility 70, which has a direct connection with the Internet 304. Typically, the transfer rate of information from the gaming device, such as gaming machine 59, to the satellite 72 (uplink rate) is less than the transfer of rate of information from the satellite 72 to the gaming device (downlink rate). For example, the uplink rate may be 28 Kilobytes per second while the downlink rate may be 500 kilobytes per second or higher. However, for software downloads, a high downlink rate may only be required for efficient gaming software downloads. Satellite Internet services may be provided by a company such as Starband Corporation (Mclean, Virginia).

In another embodiment, gaming software and other gaming information may be transferred between two gaming devices using an RF connection. The gaming information transferred via the RF connection may include but is not limited metering information generated on the gaming machine. As one example, US Telemetry corporation (UTSC, Dallas, Texas), uses radio frequency transmissions in the 218-222 MHz band to provide communications services to fixed end point devices as well as mobile devices. The fixed end point device may be a gaming machine located in a store or located in a casino, such as gaming machine 54, as well as a mobile gaming device such as a gaming machine located in a riverboat or portable gaming device that may be carried by a player and used to play a game of chance.

The RF network in a metropolitan service area may include cell transceiver sites or towers, such as 84 and 86, a system hub or master cell transceiver site, such as 82. The MCTS 82 is connected to a Network Operations Center (NOC) 80, which is essentially a data clearinghouse. Data is transferred from a CTS, such as 84 and 86, to a Master CTS (MCTS) 82 through a Publicly Switched Telephone Network. Data is transferred from the MCTS 82 to the NOC 80 database via an ATM or a Frame Relay. Data transfer protocol and user access to various end-point devices may be provided through web interfaces. Thus, using an RF network and the secured virtual network methods as described with respect to FIG. 3, 4, 5A and 5B, gaming information as well as gaming software may be transferred between various gaming devices. For instance, a remote casino accounting office 142 may obtain information from gaming devices connected to the RF network via the Internet 304.

In the present invention, records of authorizations for the transfer of gaming software between gaming devices may be stored in the database 202. Thus, given an initial distribution of gaming software in the gaming software distribution network 90 for each gaming device, the gaming software authorization records may be used to track the gaming software distribution for gaming devices in the gaming distribution network as a function time. This tracking capability may be useful for various gaming entities such as a gaming regulatory board, a gaming software content provider and gaming operators. For instance, a gaming regulatory board may be able to see the gaming software installed on all gaming devices it regulates at any given time using the database 202. As another example, a gaming software content provider, such as 51 and 52, may be able to view gaming software requests for their gaming software products as a function of time. In yet another example, a remote casino accounting office 142 may be view the distribution of their gaming software on the gaming machine under their control.

The database 202 may be partitioned and include various security protocols to limit access of the data in transaction database according to various criteria. For instance, a gaming software provider 51 may be able to view records only of gaming software transactions involving their products but not of a competitors products. As another example, a gaming entity may be able to view records of gaming software transactions involving gaming machine that they operate but not view gaming software transactions for gaming machines that another competitor controls. Further details of an interface for providing gaming software distributions is described with respect to FIG. 15.

FIGURE 9 is a block diagram depicting software transactions in a gaming software distribution network controlled by a software authorization agent. Gaming software transactions between a software authorization agent 50, a gaming software distributor 53, a gaming software content provider 51 and two gaming machines, 54 and 55 in a gaming software distribution network are described. In FIG. 9, the number and types of gaming devices are provided for illustrative purposes only and the present invention is not limited to the gaming devices shown in the Figure.

As described with respect to FIG. 8, the software authorization agent 50 is used to authorize gaming software transfer between two gaming devices. For instance, in 214, the gaming software distributor 53, which may be a game server maintained by a casino, may contact the software authorization agent 50 to request a transfer of gaming software from the gaming software provider 51 to the gaming distributor 53. The gaming distributor may also contact the software authorization agent to request a transfer of gaming software from the gaming software provider 51 to another gaming device such as gaming machine. The software authorization agent 50 may approve or deny the request depending on the gaming software transaction information contained in the request. For instance, if a gaming device, such as the gaming software distributor 53, can not be identified and authenticated by the software authorization agent 50, then the software authorization agent 50 will deny the request for the transfer of gaming software. As another example, if the gaming device, has requested a software title that is unknown to the software authorization agent 50, then the software authorization agent will deny the request for the transfer of gaming software. Some details of this gaming software transaction are described with respect to FIG. 11, 13 and 14.

After receiving authorization from the software agent, the gaming software distributor 53 may contact the gaming software content provider 51 and receive an electronically download of gaming software from the content provider via an electronic transfer in 210. The electronic transfer may use the network infrastructure and communication methods including encryption described with respect to FIGs.3, 4, 5A, 5B and 8. Details of this gaming software transaction are described with respect to FIG. 11. The gaming software may also be manually shipped to the gaming software content distributor 53, such as through the mail or by a courier, and then locally loaded onto a gaming device.

In one embodiment of the present invention, gaming software transfers involving the actual transfer of gaming software occur directly between two gaming devices as shown in 210. In another embodiment of the present invention, gaming software transfers may be routed through the software authorization agent 50. For instance, to transfer gaming software to the gaming software distributor 53, the gaming software content provider 51 sends the gaming software to the software authorization agent 50 which then forwards the software to the gaming software distributor. When the software authorization agent 50 receives the gaming software it may perform one or more checks on the gaming software to insure it has been approved for use or just simply forward to the destination gaming device without additional checks. All or a portion of the gaming software transfers may be routed through the software authorization agent 50.

In 212, prior to downloading gaming software to the gaming distributor or any other gaming device, the gaming software content provider 51, which may be a game server maintained by a company that develops gaming software or owns the rights to gaming software, may validate the gaming software transaction with the software authorization agent 50. The gaming software content provider 51 may send gaming software transaction information received in a request for a transfer of gaming software received from a gaming device, such as the gaming software distributor 53, to the gaming software authorization agent 50. The software authorization agent 50 may use the gaming software transaction information to approve or reject the transfer of the gaming software. The details of this gaming software transaction are described with respect to FIG. 11.

After sending the gaming software to the gaming software distributor 53, the gaming software content provider 51 may report details of this transaction to the software authorization agent 50 in 212. For instance, the gaming software provider may generate a gaming software transaction receipt that includes a unique digital signature for the gaming software that was sent. Similarly, after receiving the gaming software from the gaming software content provider 51, the gaming software distributor 53 may report details of this transaction to the software authorization agent 50 in 214. For instance, the gaming software distributor 53 may generate a gaming software transaction receipt that includes a unique digital signature for the gaming software that was received. The software authorization agent 50 may compare receipts from the sender and the receiver of the gaming software to insure the correct gaming software has been transferred between the sender and the receiver.

The gaming software distributor 53 may be connected to a plurality of gaming machines and other gaming devices that use gaming software such as gaming machine 54 and 55. The connection between the gaming distributor 53 and the gaming machines, 54 and 55 may be a local area network within a casino but is not limited to local area network within a casino. In one embodiment, gaming software transferred from the gaming software provider may be targeted to a particular gaming machine, such as 55, and the gaming software distributor 55 may forward the gaming software to the gaming machine 55 after receiving it from the gaming software content provider 51. The gaming machine 55 may unpack the gaming software and calculate a digital signature. The digital signature may be sent to the gaming distributor 53 through the local area network and forwarded to the software authorization agent 50 to complete the transaction.

In another embodiment, after a request from a gaming software distributor 53, in 220, a gaming software content provider 51 may download gaming software directly to a gaming machine 54 bypassing the gaming software distributor 53. For example, a gaming software provider 51 may download software to a gaming machine located in a store as described with respect to FIG. 3 via a satellite connection described with respect to FIG. 8. The gaming machine may unpack the software, which may have been compressed, and send acknowledgements of the transfer directly to the gaming software content provider 51, the gaming software distributor and the software authorization agent.

In yet other embodiments, a game server, such as the gaming software distributor 53, may be used to reconfigure the gaming software on a group of gaming machines, such as 54 and 55 via software downloads 218. The game server 53 may transfer a plurality of gaming software titles from one or more gaming software content providers, such as 51 and store these titles on the game server. When the gaming software is transferred from the gaming software content provider, the gaming software content provider and the gaming software distributor may agree to a license (see FIGs. 6 and 7) that allows for a certain number of gaming software downloads over a specific period of time. A gaming machine operator controlling a number of gaming machine may use a game server storing the plurality of gaming software titles to regularly re-distribute gaming software on gaming machines. The redistribution of gaming software via electronic downloads may be performed automatically, i.e., a distribution pattern may be programmed into the game server. Also, gaming software programs may be distributed to a gaming machine via a request from the gaming machine. For instance, a player may request to play a certain game on the gaming machine and the game server may transfer the requested gaming software to the gaming machine.

The transfer of gaming software from the game server to the gaming machine may require an approval from the software authorization agent 50. Further, even if the an approval is not required, gaming software transaction information may be sent to the software authorization agent so that the gaming software residing on any gaming machine at a particular time may be known. Details of a gaming software transaction between a gaming machine 54, a game server 53 and software authorization agent 50 are described with respect to FIG. 12.

The present invention is not limited to only electronic transfers of gaming software between gaming devices. The authorization methods may be also be applied to the manual installation of gaming software. For example, prior to manually installing gaming software on a gaming machine, an installation technician may request approval of the gaming software transaction from a software authorization agent 50 using a hand-held wireless device. The gaming software, which may be stored on a memory device such as CD-ROM may been shipped to gaming machine operator. Gaming software information regarding the gaming software to be manually installed on a gaming machine and information regarding the gaming machine may be entered into the hand-held wireless device and then sent to the software authorization agent. The software authorization agent may use this information to approve the gaming software transaction and to track the gaming software installed on gaming machines.

In another example, a technician may use the software authorization agent to manually check gaming software installed on a gaming machine. The technician may read gaming software information from a particular gaming machine and then using a hand-held wireless device relay the gaming machine software information and gaming machine information to the software authorization agent 50. The software authorization agent 50 may compare the information received from the hand-held wireless device with gaming software information stored in a gaming software registration database to determine whether the gaming machine has the correct software installed on it. The software authorization agent may send a message to the hand-held wireless gaming device indicating whether or not the correct gaming software is installed on a gaming machine. Further, the gaming software registration database may contain information regarding what software is installed on a particular gaming machine and what gaming software upgrades are available. When performing gaming machine maintenance, a gaming machine operator may request this information from the software authorization agent 50 to aid in the maintenance process.

Gaming software may be transferred between two gaming devices using a wireless communication connection. For example, within a casino, a game server may download gaming software to a plurality of gaming machines using a wireless network located within the casino. In another example, gaming software may be downloaded from a hand-held device to a gaming machine using an infrared communication interface. Examples of wireless communication standards that may be supported by a wireless communication connection and associated hardware/software include but are not limited to Bluetooth, IEEE 802.11a, IEEE 802.11b, IEEE 802.11x (e.g. other IEEE 802.11 standards such as IEEE 802.11c, IEEE 802.11d, IEEE 802.11e, etc.), hiperlan/2, HomeRF and IrDA. Wireless communications may also be performed using cellular communication technologies with cellular communication standards used in the cellular communication industry.

As described with respect to FIG. 8, the software authorization agent 50 may include a gaming software transaction database. The gaming software transaction database may be used to track the distribution of gaming software on various gaming machines. For instance, in 216, a gaming software content provider may request a report regarding downloads of their gaming software from game servers to gaming machines. The software authorization agent 50 may receive the request, query the gaming software transaction database and generate a report for the gaming software content provider. This type of report may also be generated for a casino operator with many game servers distributed over gaming properties. Advantages of the gaming software transaction database is that it may provide an electronic data trail for billing, security, auditing, dispute resolution, game usage and market trending involving the transfer and the use of gaming software.

FIGURE **10** is an interaction diagram between a gaming software distributor 53, gaming software provider 51 and a software authorization agent 50 depicting an initialization of a gaming software transaction for one embodiment of the present invention. The example is provided for illustrative purposes only. A number of operations used to perform a given function in the gaming software transaction process, an order of the operations and information used in each operation may be varied and is not limited to the examples described with respect to FIGs. 10-15.

In 902, the distributor 53 generates a session request message for the transfer of gaming software and sends the session request message to the agent 50. The initial session request message may comprise gaming software information that is used by the agent 50 to authenticate the identity of the gaming device requesting the session. For instance, prior to beginning the session request, the distributor 53 and the agent 50 may have exchanged public encryption keys and other security information that may be used to establish the identity of the sender of a message to the agent 50 and to identify messages sent from the agent 50. Details of exchanging encryption keys in a secure manner which may be applied to the present invention are described in co-pending U.S. application no. 09/993,163, by Rowe et al., filed November 16, 2001 and entitled "A Cashless Transaction Clearinghouse," which are incorporated herein by reference in its entirety and for all purposes. The message request may also include additional information that is used in a later software transfer request such as a software title, information regarding the sender of the gaming software and information regarding the receiver of the gaming software. The additional information may be used by the agent 50 after the identity of the session requestor has been authenticated.

In 906, the agent 50 receives the session request message from the distributor 53. The agent 50 may attempt to validate the distributor 53 by checking information about the distributor 53, such as its licensing status and access status to the agent 50. Transfers s of gaming software may be a revocable privilege that is granted to a gaming operator. Thus, status checks of session requestor may be necessary. When the session requestor, e.g., the distributor has been validated, the agent may initialize an authentication sequence.

In 908, the agent 50 may send an authentication message containing a symmetric encryption key, K(M). K(M) is stored by the agent 50. A symmetric encryption key is used to decrypt information encrypted with the symmetric encryption key. The authentication message including K(M) and any other additional information is encrypted with a public encryption key, M(P), used by the distributor 53. M(P) was previously received, authenticated and stored by the agent 50. The public encryption key M(P) is part of a public-private asymmetric encryption key pair comprising M(P) and M(PP), where only the distributor 53 should have knowledge of the private key. In an asymmetric encryption key pair, only the private key of the encryption public-private key pair may be used to decrypt information encrypted with the public key.

In 910, when the distributor 53 receives the authentication message, it decrypts the message with its private key, M(PP) which corresponds to the public encryption key M(P). In 912, the distributor 53 generates and sends an acknowledgement message encrypted with K(M). In 914, when the agent 50 receives the acknowledgement message, it decrypts it with the session key K(M) stored in 906. Since only the distributor has the private key M(PP) needed to decrypt K(M), when a correct acknowledgement message is received, the distributor 53 is authenticated. The agent 50 may generate and send an additional message acknowledging the distributor has been authenticated and may now proceed with a gaming software download request.

In 916 and 918, the distributor 53 may generate a software download request message and send it to the agent. The download request message may include combinations of gaming software transaction information selected from but not limited to: a) operator identification information for the gaming device to receive the gaming software, b) machine identification information for the gaming device to receive the gaming software (e.g., an identification number for a gaming machine or a game server), c) operator identification information for the gaming device that is to send the gaming software, d) machine identification information for the second gaming device, e) a gaming software title or gaming software titles to be transferred, f) a gaming software provider identifier such as a name of a company (e.g., IGT) , g) a gaming software version number, h) a gaming software identification number and i) information on gaming software currently installed on the gaming device to receive the gaming software. The download request message may be encrypted with symmetric encryption key, K(M). In addition, the download request message may be encrypted with the public encryption key of the agent 50. In one embodiment, the agent 50 may send a request to a gaming device requesting the software currently installed on the gaming device for tracking and regulatory purposes. Further, once it is determined what gaming software is installed on a plurality of gaming machine, the process of upgrading and fixing errors in gaming software may be simplified.

In 920, the agent 50 receives the download request message, decrypts the message and evaluates the request. In one embodiment, the download request information may be included in the session request message sent in 904. Thus, after authenticating and identity of the distributor 53, the agent 50 may begin processing the request in 920 without receiving additional information from the distributor 53. To evaluate the download request, the agent 50 may compare gaming software transaction information in the request message with information stored in a database. For instance, the request message may include a location, address and identification number for a gaming device that is to receive the gaming software. The agent 50 may compare this information with information from a database containing information for gaming devices that are allowed to receive gaming software downloads. The agent 50 may only authorize the download request when the gaming device identification information in the request message matches the gaming device identification information stored in the database. In another example, the request message may include gaming software identification information such as a title, version number and manufacturer. The agent 50 may only authorize the download request when the gaming software identification information in the request message matches gaming software identification information contained in a database used by the agent 50.

In 922, when the download request is approved, the software authorization agent creates a gaming software transaction record and stores the record to a gaming software transaction database. The gaming software transaction record may include but is not limited to gaming software transaction information such as: a) a symmetric encryption key, K(S), that will be used to transfer the gaming software from a first gaming device to a second gaming device, b) a time that the transaction was initiated, c) transaction expiration time, d) a destination ID number (e.g., a number identifying a casino), e) an identification number of the gaming device on which the software is to be installed, f) a gaming software identification number, g) a software title, h) a game signature for the gaming software such as from a CRC or a hash, i) a manufacturer's identification number,

j) a public encryption key used by the manufacturer and k) a transaction number for the record. In some embodiments, the gaming software transaction record may include a number of permitted downloads of the gaming software. For instance, a gaming software program may be loaded to a game server. Each time the game server downloads the gaming software to a gaming machine, it may request permission from the software authorization agent 50 using the transaction number in the original record. The software authorization agent may authorize the game server to download the software to a gaming machine as long as the number of permitted downloads has not been exceeded.

In 922 and 923, the software authorization agent may send an approval message with all or a portion of the gaming software transaction information stored in the gaming software transaction record to the gaming software distributor. The message may be encrypted with the session key, K(M), generated in 906. In 924, the distributor 53 may receive the message, decrypt it using the session key, K(M), and generate an acknowledgement message. In 926, the software distributor 53 may send the acknowledgement message to the authorization agent 50. In 928, the authorization agent 50 may receive the acknowledgement and store the record for the gaming software transaction. In 930, the gaming software agent may send a notification message to the gaming software provider 51. The message may notify the gaming software content provider 51 that a gaming software transaction has been authorized that allows some of the provider's 51 to be transferred to another gaming device.

FIGURE 11 is an interaction diagram between a gaming software distributor, a gaming software provider and a software authorization agent depicting a gaming software transaction. In 850, the distributor may generate a software download request message. The download request message may include gaming software transaction information generated in the gaming software transaction request described with respect to FIG. 10. The download request message may also include a session key, K(S), encrypted with the provider's public encryption key. In 852, the distributor 53 sends the request to the provider 51. In 854, the provider 51 receives the message and decrypts the session key, K(S), with the provider's private encryption key. In 854, the provider generates an acknowledgement message encrypted with the session key K(S). In 856, the provider 51 sends the message to the distributor 53. In 857, the distributor receives the message and decrypts it with the K(S) received from the software authorization agent 50 in the authorization message.

In 859, the software provider 51 may optionally generate a download request message to validate the gaming software transaction requested by the distributor. The download request message may include gaming software transaction information, such as a transaction number, received from the distributor 53. In 858, the provider 51 may optionally send the download request message to the authorization agent 50. The message may be encrypted with the agent's public encryption key. In 860, the agent 50 may receive the download request message from the provider, decrypt it and compare the gaming software transaction information in the message with a gaming software transaction information stored in a gaming software transaction record corresponding to the request. When the request is valid, the agent 50 may generate a download reply message authorizing the provider 51 to transfer the gaming software. When the request is invalid, the agent 50 may generate a download reply message requesting the provider 51 not to send the gaming software to the distributor 53. In 864, the agent sends the download request message to the provider 51. In 862, the agent may store a record of the download request and whether it was authorized or not authorized.

In 866, the provider 51 may generate a download reply with a receipt. In one embodiment, the download reply may require the authorization of the agent 50. In another embodiment, the download reply may be sent without approval from the agent 50. The download reply may include but is not limited to a game package with the following information: 1) the requested game software, 2) the expiration date of the game or a number of plays until expiration which may be built into the gaming software, 3) a destination machine number (in some embodiments, the gaming software may be designed to operate only on a particular machine), 4) a destination address (e.g., a casino name), 5) a time stamp for the transaction, 6) a digital signature generated for the game (e.g., a CRC or a Hash of the game software), 7) the transaction number received from the distributor. The download reply may also include a separate receipt including but not limited to the following information: a) game title or identification number, b) original game transfer request data received in the request from the distributor 53, c) destination machine's identification number, d) destination address and e) a transaction number.

The download reply may be compressed to reduce the information transferred. The download reply may also include information regarding the compression algorithm used so that the destination device may properly uncompress the download reply. The download package and the download receipt may be encrypted with combinations of a public encryption key used by the destination gaming device and the session encryption key, K(S). In one embodiment, the download package and reply may be routed through the software authorization agent 50 which may perform checks on the gaming software before forwarding it to the destination gaming machine. Thus, the download package and receipt may be encrypted with the public encryption key used by the software authorization agent 50.

The download package and the download receipt may go to separate gaming devices. In one embodiment, the download package may be forwarded by the distributor 53 to a destination gaming device such as a gaming machine and the receipt may be forwarded to another gaming device for accounting purposes. In another embodiment, the receipt and download package may go to the same gaming device such as a game server operated by the gaming software distributor 53. In 868, the content provider 51 may send a receipt encrypted with the session key, K(S) to the agent 50. Since only the provider 51 and the distributor have the session key, K(S), the identity of the provider 51 may be authenticated. In 870, the agent 50 may receive the receipt, decrypt it and store gaming software transaction information contained in the receipt.

In 872, the provider sends the download reply with the gaming software and receipt to the distributor 53. In 874, the distributor 53 receives the download message, the message may be forwarded to a destination gaming device or may be stored on a game server. The destination gaming device may decrypt the download message, unpack the gaming software, which may include uncompressing the gaming software, and generate a digital signature for the gaming software. The digital signature may be generated using an algorithm such as a CRC or a Hash. In 876, the destination gaming device may send an acknowledgement message to provider indicating it has received the download message with the gaming software.

In 878, the gaming software distributor 53 generates a receipt. The receipt may include but is not limited to the following information: a) game title or identification number, b) original game transfer request data received in the request from the agent, c) destination machine's identification number, d) destination address and e) a transaction number. The receipt may be encrypted with the session encryption key, K(M), exchanged between the agent 50 in the distributor as described with respect to FIG. 10. Thus, when the agent 50 receives the receipt and decrypts it with K(M), the identity of the distributor may be authenticated.

In 879, the distributor 53 sends the receipt to the agent 50, the agent decrypts the receipt. In 880, the agent 50 may compare gaming software transaction information in the receipt received from the provider 51 in 868 with gaming software transaction information from the receipt received from the distributor 53 in 879. For example, to validate the gaming software transaction, the agent 50 may compare the digital signature for the gaming software received from the provider 51 in the receipt with the digital signature for the gaming software received from the distributor 53. When the digital signatures match, the gaming software transaction is completed and communications are terminated. As an additional check, the agent may compare the digital signatures for the gaming software with a digital signature for an approved copy of the gaming software stored in a database maintained by the agent 50. When the transaction is complete, the agent 50 may store a record of the transaction in a database. As described with respect to FIG. 9, the database may be used to track the distribution of gaming software on various gaming devices that use the authorization agent 50. Also, the records may be used for billing and auditing purposes.

In 880, when gaming software transaction information in the receipts does not match, the agent 50 may send messages to the provider 51 and the distributor 53 revoking the transaction. The message to the provider 51 may be encrypted with the session key, K(S) and the message to the distributor 53 may be encrypted with the session key, K(M). The messages may also be encrypted with public keys of public-private key pairs used by the distributor 53 and the provider 51. In response to receiving the revocation message, the content provider 51 and the distributor 53 may repeat the transaction. For example, the digital signatures for the gaming software may not match because of a transmission error. In another embodiment, the entire gaming software transaction may be revoked and the distributor 53 may have to initiate an entirely new transaction as was described with respect to FIG. 9.

FIGURE 12 is an interaction diagram between a gaming software distributor 53, a gaming machine 54 and a software authorization agent 50 depicting a gaming software transaction. In this example, the distributor 53 may be a game server operated by a casino and the gaming machine 54 may be one of a plurality of gaming machine in communication with the gaming server. The game server may have been loaded with gaming software provided by various content providers using gaming software transactions as described with respect to FIG. 11. In general, the operations shown in FIG. 12 are similar to those described with respect to FIG. 11.

In 950, the gaming machine 54 may generate a gaming software request. The gaming software request may be in response to different gaming events that occur on the gaming machine. For example, a request may be initiated when a game player using the gaming machine requests to play a game of chance currently not installed on a gaming machine. As another example, the gaming machines may include software programs that request gaming software at particular times of the day or the week. For instance, particular bonus games may only be provided on the gaming machines at certain times of the day to increase player interest. In yet another example, a software request may be generated when a game license (see FIGs. 6 and 7) installed on a gaming machine has expired.

In 952, the gaming machine 54 sends the software transfer request to the distributor 53 which in this case is a game server. In 954, the distributor 53 receives the gaming software request message and generates an acknowledgement message. The message may or may not be decrypted. When the gaming machine and the game server communicate via a private local area network, such as within a casino, encryption procedures may not be necessary. However, the game server may communicate with a gaming machine located at different gaming properties, such as stores, via a virtual private network, as was described with respect to FIG. 3. In this case, encryption procedures such as the use of public-private key pairs and symmetric encryption keys may be used. In 956, the distributor 53 sends the acknowledgement message to the gaming machine 54. In 957, the gaming machine 54 receives the acknowledgement message and may authenticate the sender of the message.

In another embodiment of the present invention, the gaming software download request may be initiated by the game server. For example, the game server may be used to regularly redistribute gaming software on gaming machine distributed on a gaming floor according to perceived customer desires and market trends. A market trend may be a "hot" game that is desired by a lot of customers. Further, the gaming server may be also used to provide regularly software upgrades and error fixes to gaming software executed on various gaming machines. The software upgrades and error fixes may be prompted by notices of upgrades and fixes received from a content provider. When the distributor 53 initiates the gaming software transaction, the gaming machine 54 may be simply sent the gaming software. An authentication process may or may not proceed the game server sending the gaming software to the gaming machine.

In 959, the distributor 53 may generate a download request message for the requested gaming software. The request message may have been initiated by the gaming machine 54 or the distributor 53. In 958, the distributor sends the download request to the agent 50. In 960, the agent 50 may generate a reply message that authorizes or denies the transaction and store a record of the gaming software transaction 962. In some embodiments, the distributor 53 may simply send a record of the gaming software transaction to the agent but not ask for or expect an approval message from the agent 50. The agent 50 may store this record. In another embodiment, the agent 50 may have previously approved a certain number of gaming software transfers and may determine if additional downloads are available.

In 964, the distributor receives the download reply from the agent 50. When an authorization has been requested and it has been approved, the gaming distributor 53 may generate a download reply message containing the gaming software. In this embodiment, a receipt may not be required since the gaming software downloaded to the gaming distributor may have already been approved by the agent 50 in a previous gaming software transaction. In 972, the download reply with the gaming software is sent to the gaming machine 54. In 974, the gaming machine receives the download reply and may decrypt and unpack the gaming software. The gaming machine may also calculate one or more digital signatures for the gaming software which may be used to validate that the software has been successfully transferred. In 976, the gaming machine 54 may send an acknowledgement message to the game server of the distributor 53 that it has received the requested gaming software. The gaming machine 54 may also store a gaming software transaction record of the gaming software download in a non-volatile memory device. The gaming software transaction record may be used for used for auditing and security purposes.

Optionally, in 978, the gaming machine 54 may generate a receipt or some other type of acknowledgement message that it has received the gaming software and send it to the authorization agent 50. In 968, the game server of the distributor 53 may also send a receipt or acknowledgement message to the agent 50. In 970 and 980, the agent 50 may receive the acknowledgement messages from the gaming machine 50 and the distributor 53 and store a record of the gaming software transaction. The agent may also use gaming software transaction information included with the acknowledgement messages to determine if the gaming software transaction has been correctly carried out.

FIGURE 13 is flow chart depicting a method in a software authorization agent initializing a gaming software transaction. In 1000, the agent receives a gaming software transaction session request message from a gaming software distributor or another gaming entity desiring a transfer of gaming software. The transfer of gaming software may be implemented electronically or manually. In a manual transmission, the gaming software may be shipped to the distributor and loaded locally onto a gaming device, such as a gaming machine. In 1002, the authorization may check to determine if the requestor identified in the message is in a local of database of gaming entities that are authorized to request transfers of gaming software. When the requestor is not in the database, in 1004, the agent may terminate the transaction and generate a record of the attempted transaction and store the record. Records of failed transactions may be analyzed for security purposes.

When the requestor is in a local database, the agent may generate a symmetric encryption key that may be used to encrypt messages sent between the agent and the requestor and store the symmetric encryption key. Further, for authentication purposes, the agent may encrypt the symmetric encryption key with a public encryption key used by the requestor and send a message with the encrypted symmetric encryption key to the requestor. In one embodiment, prior to the session request, the requestor and the agent may have exchanged public encryption keys of public-private encryption key pairs. In 1008, the agent receives a reply message from the requestor. The message may contain a symmetric encryption key encrypted with the agents public key. The agent decrypts the symmetric encryption key with the agent's private key.

In 1010, the agent compares the symmetric encryption key to the symmetric encryption key sent to the requestor in 1006. When the encryption keys agree, the identity of the requestor is assumed to be authenticated. In addition to a symmetric encryption key, other types of information, such as passwords or random bits, may be encrypted and exchanged between the requestor and agent. The other types of exchanged information may be compared as part of the authentication process. When the requestor is not authenticated, in 1004, the transaction is terminated and a record of the failed transaction may be generated.

When the identity of the requestor is authenticated, in 1012, the agent may evaluate and validate one or more parts of a download request for gaming software from the requestor. For instance, the agent may determine if a requested gaming software title has been approved for downloads or transfers. As another example, the download request may include identification information for a gaming device that will receive the requested gaming software. The agent may compare identification information for the destination gaming device with identification information from a database of gaming devices approved for receiving gaming software. In 1014, when the information in the download request is not valid, the agent may generate an error message and it to the requestor. The error message may indicate detected errors in the request such as missing information or a request for a gaming software title unknown to the agent.

In 1016, when information in the download request has been validated, the agent may generate an authorization record for the gaming software transaction as previously described with respect to FIG. 9. The agent may also generate an acknowledgement message and send it to the requestor. In 1018, the agent may check to determine whether a reply has been received for the acknowledgement message. In 1014, when an acknowledgement reply message has not been received, the agent may generate an error message and send it to the requestor. In 1020, when the acknowledgement reply message has been received, the agent may store a record of the authorized transaction to a database. In one embodiment, the agent may also notify a software content provider that has been authorized to transfer the gaming software of the pending gaming software transaction that has been authorized.

FIGURE **14** is flow chart depicting a method in a software authorization agent of authorizing a gaming software transaction. In 1100, the agent receives a gaming software transfer request form a gaming device. The transfer request may describe a gaming software transaction previously generated and authorized by the agent. The gaming device may be a game server, a gaming machine or any other gaming device that is allowed to receive gaming software. Further, the gaming device may request a transfer of the gaming software to another gaming device different from itself. For instance, a game server may request a transfer of gaming software to a gaming machine. In 1102, the agent may determine whether the transfer request is a valid gaming software transaction. For example, the transfer request may contain a transaction number and the agent may use this transaction number to locate a gaming software transaction record including gaming software transaction information describing the transaction. The agent may compare the information from the gaming software transaction record with gaming software transaction information contained in the transfer request. The transaction record may also include status information such as whether the transaction has been completed or is pending and an expiration date for the transaction, which may be checked by the agent.

In 1104, when the gaming software transaction is invalid the agent denies the transfer request, may send an error message and may also store a record of the denied transfer request. In 1106, when the gaming software transaction has been validated, the agent may change the status of the transaction to pending and store the status. In 1108, the agent may send a transfer reply to the gaming device requesting the gaming device to proceed with the transaction. In 1110, the agent may receive acknowledgement messages from the gaming device that has sent the gaming software (e.g., a content provider) and from the gaming device that has received the gaming software (e.g., a gaming machine or a game server). The acknowledgement messages may include information about the transferred gaming software. For example, the acknowledgement message may include a digital game signature for the gaming software generated by the both the sender and the receiver of the gaming software.

In 1112, the agent may validate the transaction by comparing gaming software transaction information received from both the receiver and the sender of the gaming software. For instance, the agent may compare digital signatures for the gaming software generated by the sender and the receiver. In 1114, when the transaction is invalid, the agent may change the status of the transaction from pending and generate an error message. The error message may be sent to the requestor of the gaming software and the sender of the gaming software and identify any deficiencies detected by the agent. In 1116, when the transaction is valid, the agent may change the status of the transaction to downloaded and store additional information in the transaction record such as the time that the transaction was completed. In 1118, the agent may optionally notify the requestor of the gaming software and the provider of the gaming software that the transaction has been successfully completed. In some embodiments, the agent may even bill the requestor of the gaming software and arrange for an electronic fund transfer or other payment method.

FIGURE 15 is a block diagram of an interface 1200 used to provide information about gaming software transactions generated by a software authorization agent. The interface menu 1210 may allow a user to view information in different formats, perform queries of a gaming software transaction and perform other operations on gaming software transaction data such as analyzing market trends. The interface may be used from a remote site to access gaming software transaction stored in a database. The access to the gaming software transaction database may be limited according to the identity of a particular user. For example, a gaming regulatory agency maintaining the transaction database may be able to look at all of the gaming software transactions stored in a database. A gaming software content provider may be able to access transactions involving the transfer of their gaming software. A gaming entity such as a casino operator may be able to access transactions involving gaming devices operated by the casino.

In 1202, 1204, 1206 and 1208, a few examples of plots that may be derived form a gaming software transaction database are shown. The plots are shown for illustrative purposes only and are not limited to the examples shown in the figure. In 1202, a total number of game downloads as a function of location are shown. This type of plot may be generated for a gaming entity with gaming devices at locations A, B, C and D or even a content provider that provides gaming software to each of these locations via gaming software transactions. In 1204, a number of game downloads as a function of time are plotted for property A. The plot shows the variation in game downloads from month to month. In 1206, a gaming software distribution for five different types of games at property A are shown. As described with respect to FIG. 9, if an initial distribution of gaming software on different gaming devices are known, then the gaming software transaction records may be used to track the distribution of games on the gaming devices. In 1208, a game distribution for the five different types of games is shown across multiple gaming properties.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, while the gaming machines of this invention have been depicted as having top box mounted on top of the main gaming machine cabinet, the use of gaming devices in accordance with this invention is not so limited. For example, gaming machine may be provided without a top box.

CLAIMS

What is claimed is:

1. In a first gaming device, a method of requesting a transfer of gaming software from a second gaming device, said method comprising:

generating a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and

receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

2. The method of claim 1, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

3. The method of claim 1, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

4. The method of claim 1, wherein the gaming software transaction request comprises access information and gaming software identification information.

5. The method of claim 4, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

6. The method of claim 4, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

7. The method of claim 1, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

8. The method of claim 1, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

9. The method of claim 1, further comprising:

sending authentication information used to identify the first gaming device to the gaming software authorization agent.

10. The method of claim 1, further comprising:

sending a message requesting the gaming software to the second gaming device.

11. The method of claim 1, further comprising:

receiving the gaming software from the second gaming device.

12. The method of claim 11, further comprising:

determining a digital signature for the gaming software and

sending a message with at least the digital signature to the gaming software authorization agent.

13. The method of claim 1, further comprising:

authenticating an identity of the second gaming device.

14. The method of claim 1, wherein the first gaming device is a gaming machine and the second gaming device is a game server.

15. The method of claim 1, wherein the first gaming device is a game server in communication with a plurality of gaming machines and the second gaming device is a game server maintained by a gaming software content provider.

16. The method of claim 1, wherein the transfer of gaming software is performed at least one of manually and electronically.

17. The method of claim 1, wherein the gaming software comprises one or more gaming software components.

18. The method of claim 1, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

19. The method of claim 1, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

20. In a first gaming device, a method of transferring gaming software to a second gaming device, said method comprising:

receiving a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software; and

transferring the gaming software to the second gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

21. The method of claim 20, further comprising:

receiving an approval of the gaming software transaction request from the gaming software authorization agent.

22. The method of claim 20, further comprising:

prior to transferring the gaming software, receiving a denial of the gaming software transaction request from the gaming software authorization agent; and

terminating the transfer of the gaming software.

23. The method of claim 20, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

24. The method of claim 20, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection, an infrared communication connection and combinations thereof.

25. The method of claim 20, wherein the gaming software transaction request comprises access information and gaming software identification information.

26. The method of claim 25, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

27. The method of claim 25, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

28. The method of claim 20, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number, a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

29. The method of claim 20, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

30. The method of claim 20, further comprising:

determining a digital signature for the gaming software and

sending a message with at least the digital signature to the gaming software authorization agent.

31. The method of claim 20, wherein the first gaming device is a gaming server and the second gaming device is a gaming machine.

32. The method of claim 20, wherein the first gaming device is a gaming machine and the second gaming device is a gaming machine.

33. The method of claim 20, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a game server maintained by a gaming entity.

34. The method of claim 20, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a gaming machine maintained by a gaming entity.

35. The method of claim 20, wherein the transfer of gaming software is performed at least one of manually and electronically.

36. The method of claim 20, wherein the gaming software comprises one or more gaming software components.

37. The method of claim 20, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

38. The method of claim 20, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

39. A first gaming device comprising:

a network interface allowing communications between the first gaming device, a software authorization agent and one or more other gaming devices; and

a processor configured or designed to (i) send a request for the transfer of gaming software from a second gaming device to a third gaming device via the network interface to the software authorization agent (ii) receive from the software authorization agent a reply approving or rejecting the request for the transfer of the gaming software

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

40. The first gaming device of claim 39, further comprising:

a memory device that stores gaming software.

41. The first gaming device of claim 39, further comprising:

a master gaming controller that controls a game of chance played on the first gaming device.

42. The first gaming device of claim 39, further comprising:

a memory device that stores public encryption keys for one or more of the plurality of gaming devices and the software authorization agent.

43. The first gaming device of claim 39, wherein the network interface is connected to at least one of a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

44. The first gaming device of claim 39, wherein the network interface provides at least one of a satellite communication connection, a RF communication connection and an infrared communication connection.

45. The first gaming device of claim 39, wherein the first gaming device is a portable gaming device.

46. The first gaming device of claim 39, wherein the first gaming device is a first gaming machine, the second gaming device is a second gaming machine and the third gaming device is the first gaming machine.

47. The first gaming device of claim 39, wherein the first gaming device is a first game server, the second gaming device is a second game server and the third gaming device is a first gaming machine.

48. The first gaming device of claim 39, wherein the first gaming device is a first game server, the second gaming device is a second game server and the third gaming device is the first game server.

49. The first gaming device of claim 39, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

50. The first gaming device of claim 39, wherein the gaming software comprises one or more gaming software components.

51. The first gaming device of claim 39, wherein the gaming software is used to upgrade a gaming software component on one of the gaming devices.

52. The first gaming device of claim 39, wherein the gaming software is used to correct an error in a gaming software component on one of the gaming devices.

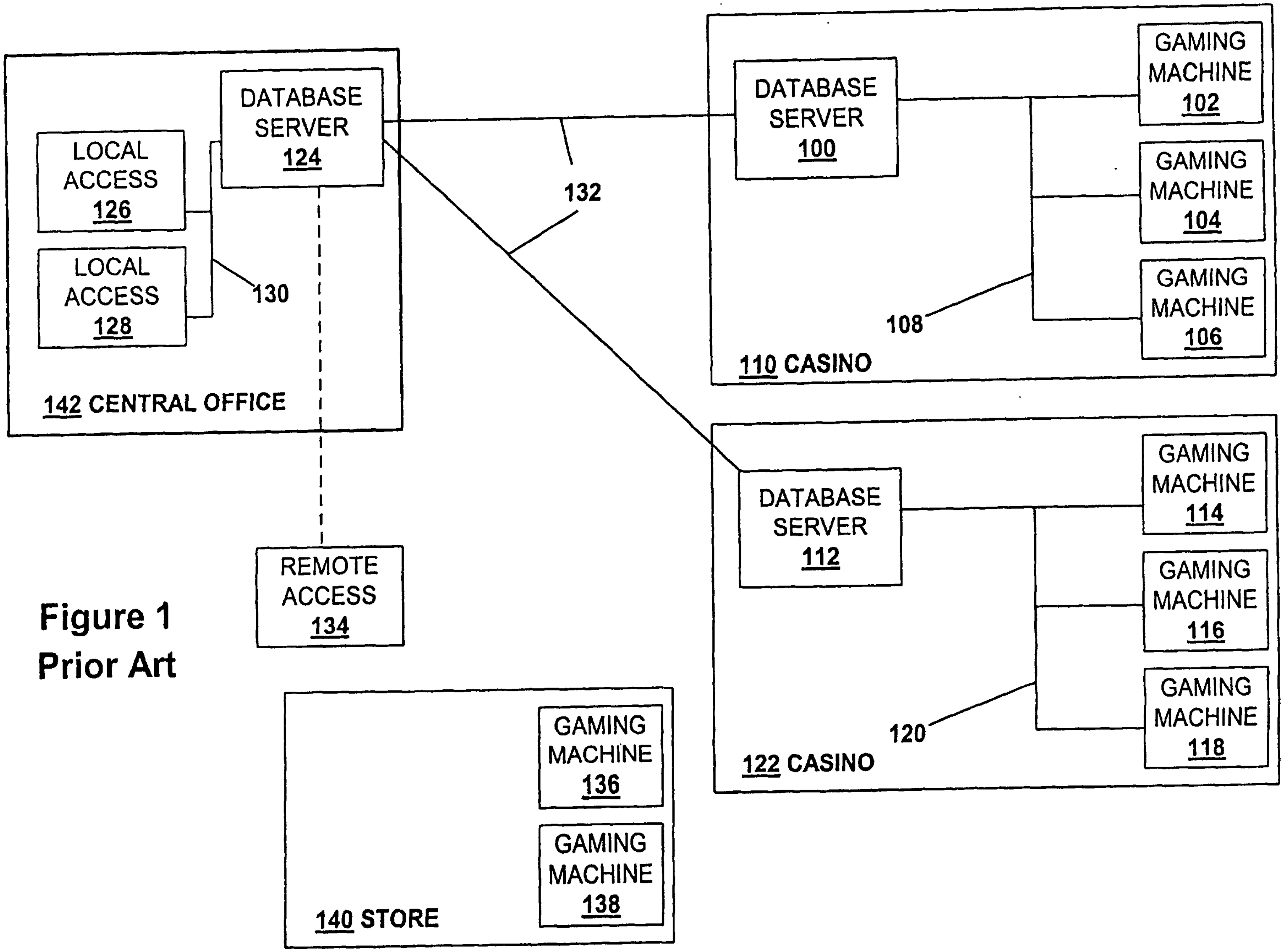


Figure 1
Prior Art

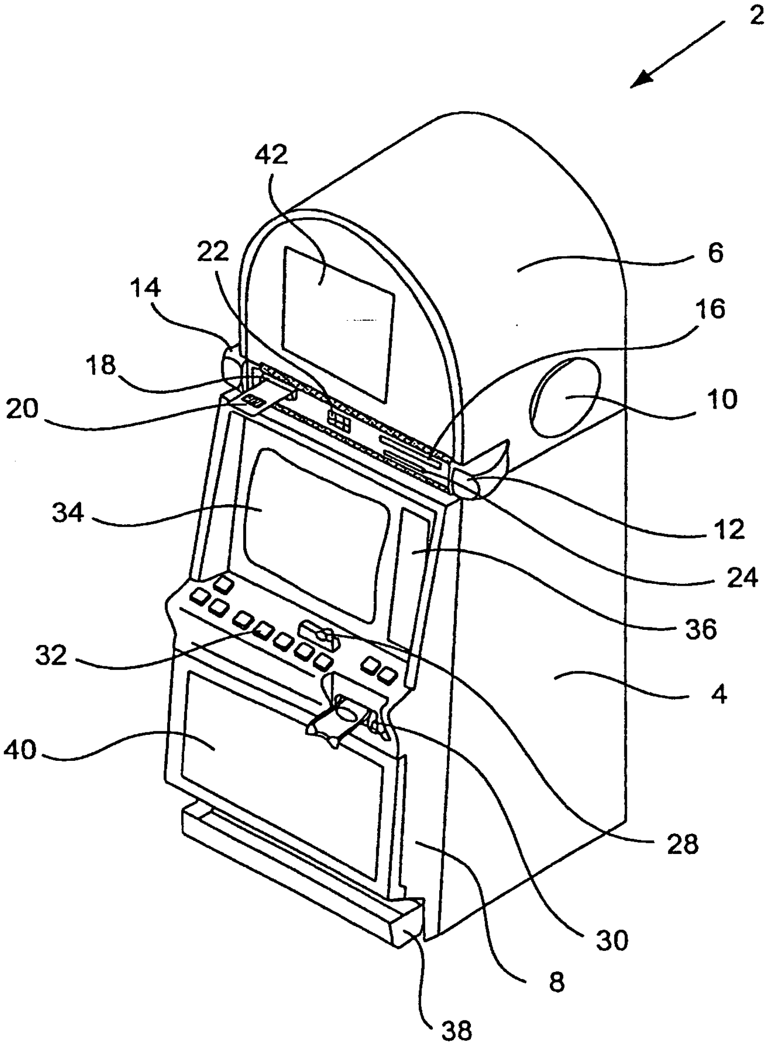


FIGURE 2

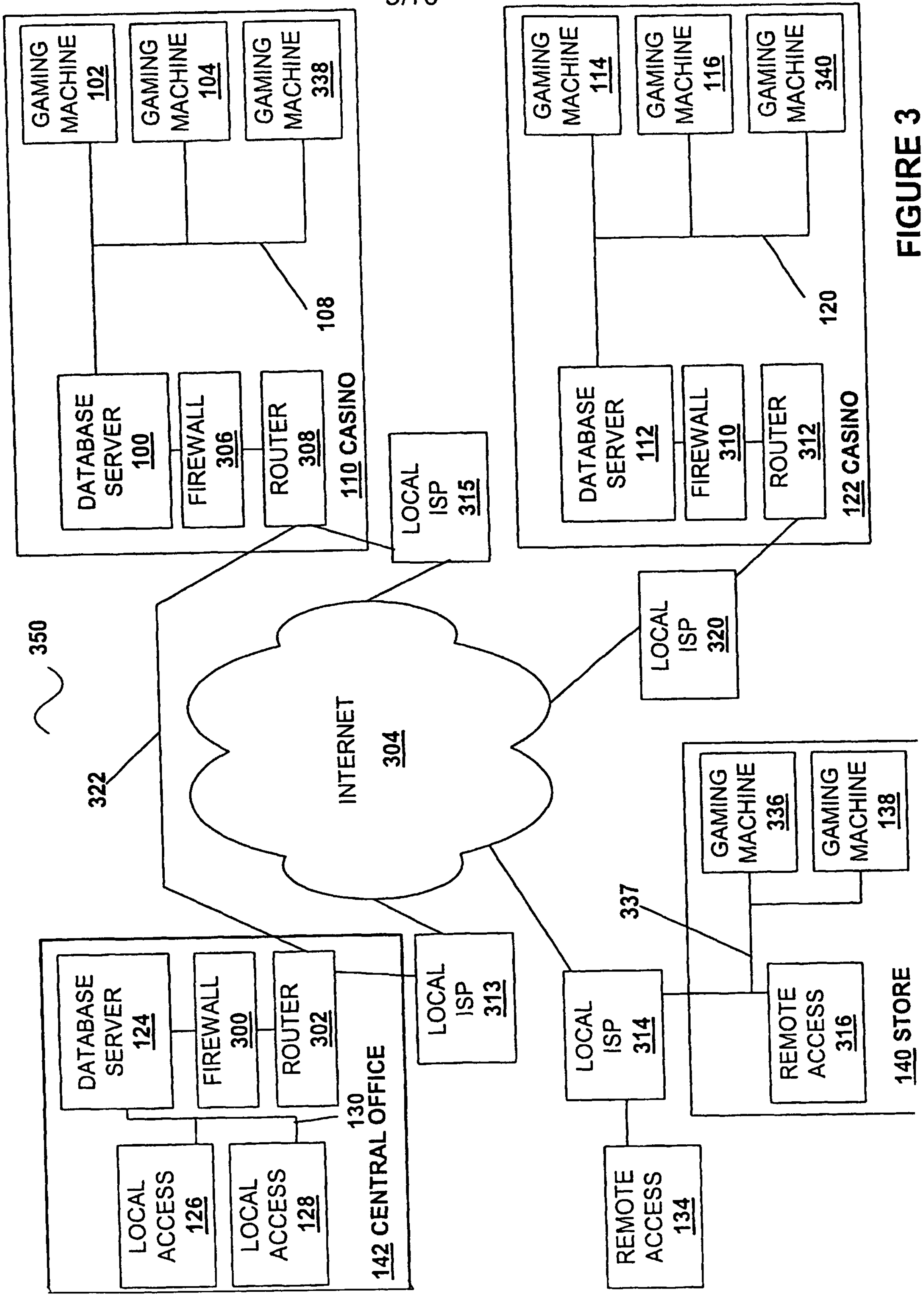

GAMING MACHINE 102
GAMING MACHINE 104
GAMING MACHINE 338
108
DATABASE SERVER 100
FIREWALL 306
ROUTER 308
110 CASINO
LOCAL ISP 315
GAMING MACHINE 114
GAMING MACHINE 116
GAMING MACHINE 340
120
DATABASE SERVER 112
FIREWALL 310
ROUTER 312
122 CASINO
LOCAL ISP 320
350
322
INTERNET 304
GAMING MACHINE 336
GAMING MACHINE 138
337
REMOTE ACCESS 316
140 STORE
LOCAL ISP 314
REMOTE ACCESS 134
LOCAL ISP 313
DATABASE SERVER 124
FIREWALL 300
ROUTER 302
130
LOCAL ACCESS 126
LOCAL ACCESS 128
142 CENTRAL OFFICE

FIGURE 3

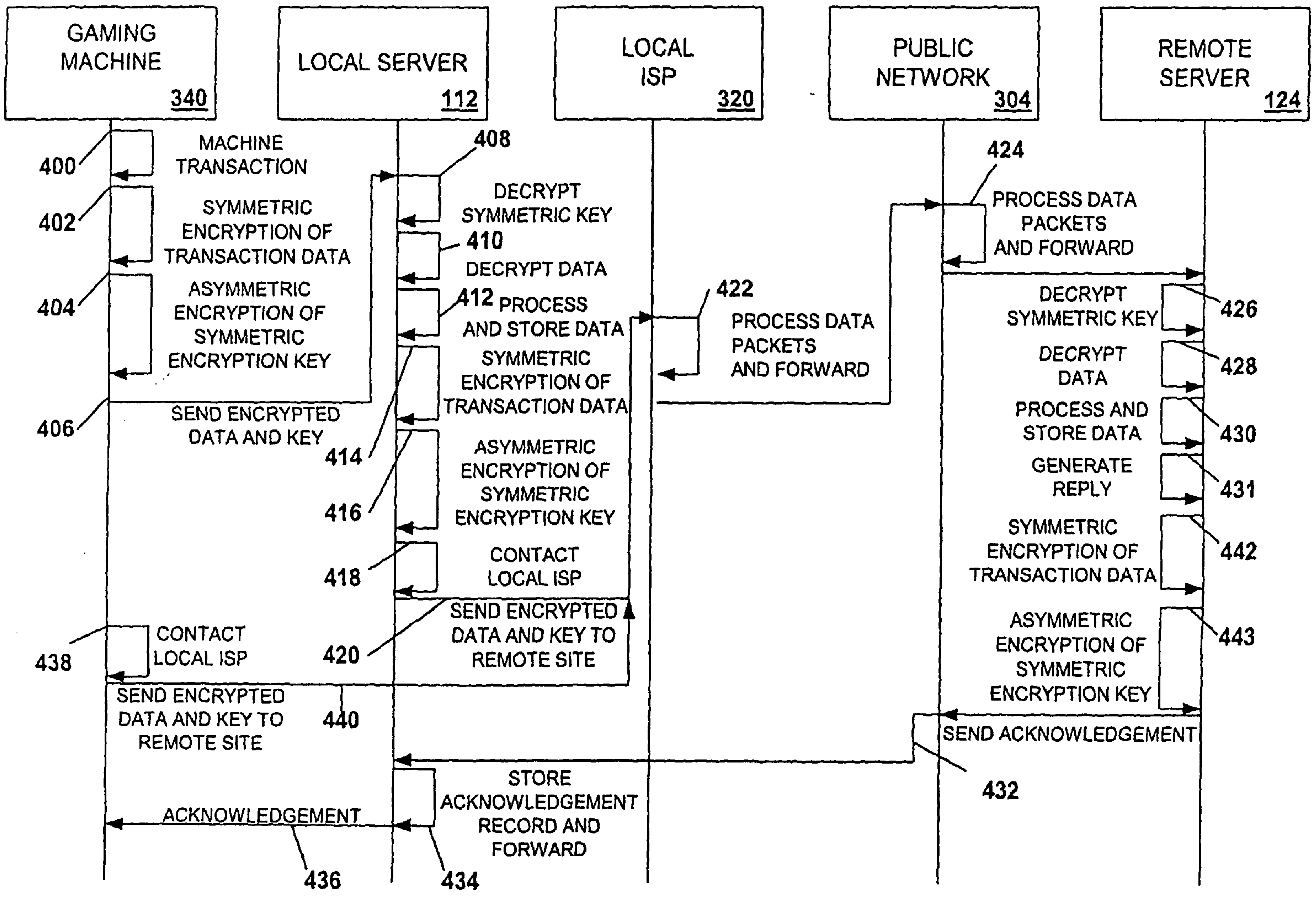

GAMING MACHINE 340
LOCAL SERVER 112
LOCAL ISP 320
PUBLIC NETWORK 304
REMOTE SERVER 124
400 MACHINE TRANSACTION
402 SYMMETRIC ENCRYPTION OF TRANSACTION DATA
404 ASYMMETRIC ENCRYPTION OF SYMMETRIC ENCRYPTION KEY
406 SEND ENCRYPTED DATA AND KEY
408 DECRYPT SYMMETRIC KEY
410 DECRYPT DATA
412 PROCESS AND STORE DATA
414 SYMMETRIC ENCRYPTION OF TRANSACTION DATA
416 ASYMMETRIC ENCRYPTION OF SYMMETRIC ENCRYPTION KEY
418 CONTACT LOCAL ISP
420 SEND ENCRYPTED DATA AND KEY TO REMOTE SITE
422 PROCESS DATA PACKETS AND FORWARD
424 PROCESS DATA PACKETS AND FORWARD
426 DECRYPT SYMMETRIC KEY
428 DECRYPT DATA
430 PROCESS AND STORE DATA
431 GENERATE REPLY
442 SYMMETRIC ENCRYPTION OF TRANSACTION DATA
443 ASYMMETRIC ENCRYPTION OF SYMMETRIC ENCRYPTION KEY
432 SEND ACKNOWLEDGEMENT
434 STORE ACKNOWLEDGEMENT RECORD AND FORWARD
436 ACKNOWLEDGEMENT
438 CONTACT LOCAL ISP
440 SEND ENCRYPTED DATA AND KEY TO REMOTE SITE

FIGURE 4

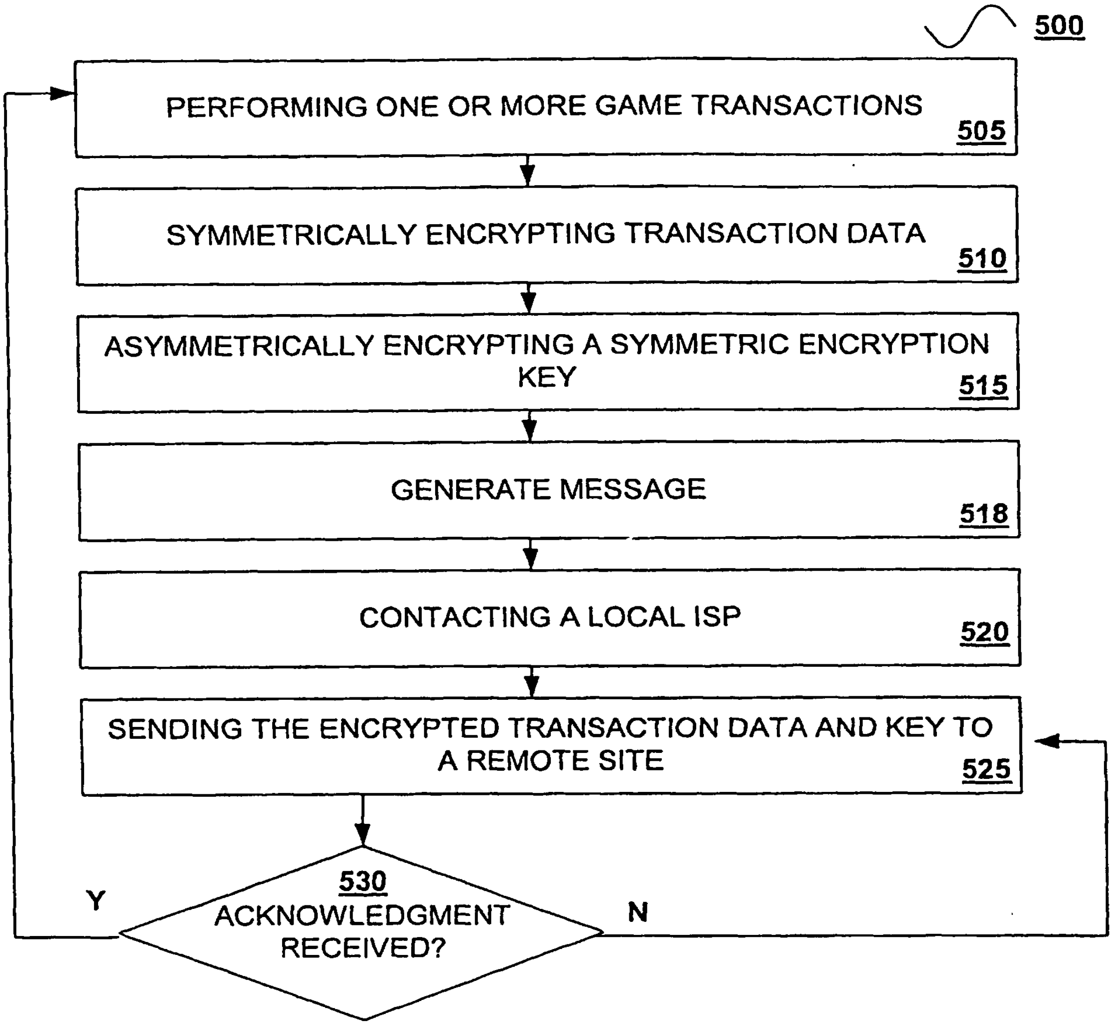

500
PERFORMING ONE OR MORE GAME TRANSACTIONS
505
SYMMETRICALLY ENCRYPTING TRANSACTION DATA
510
ASYMMETRICALLY ENCRYPTING A SYMMETRIC ENCRYPTION KEY
515
GENERATE MESSAGE
518
CONTACTING A LOCAL ISP
520
SENDING THE ENCRYPTED TRANSACTION DATA AND KEY TO A REMOTE SITE
525
530
ACKNOWLEDGMENT RECEIVED?
Y
N

FIGURE 5A

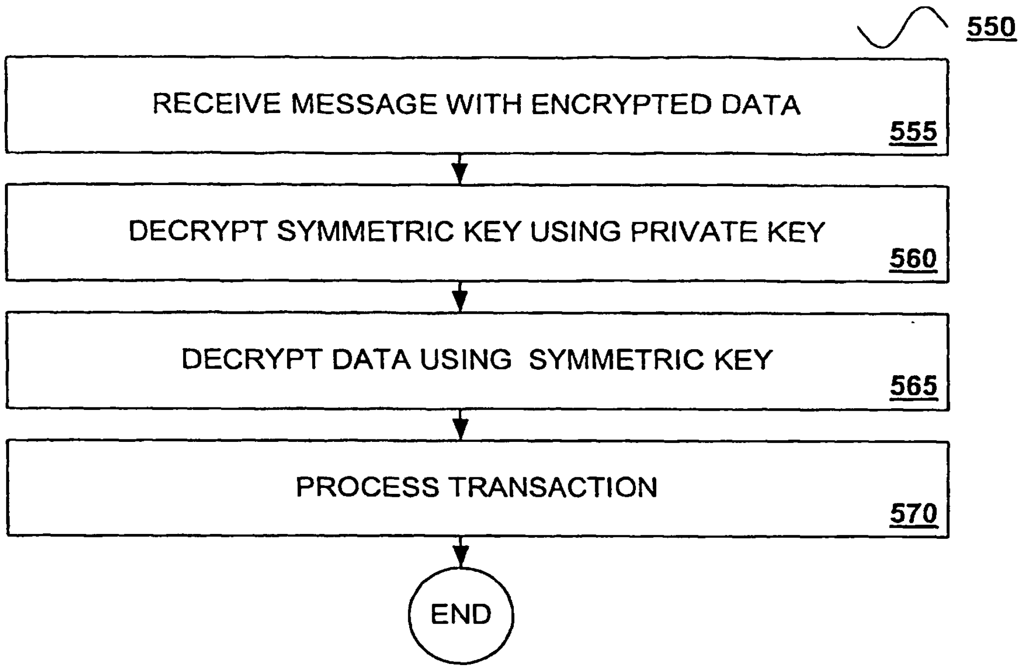

550
RECEIVE MESSAGE WITH ENCRYPTED DATA
555
DECRYPT SYMMETRIC KEY USING PRIVATE KEY
560
DECRYPT DATA USING SYMMETRIC KEY
565
PROCESS TRANSACTION
570
END

FIGURE 5B

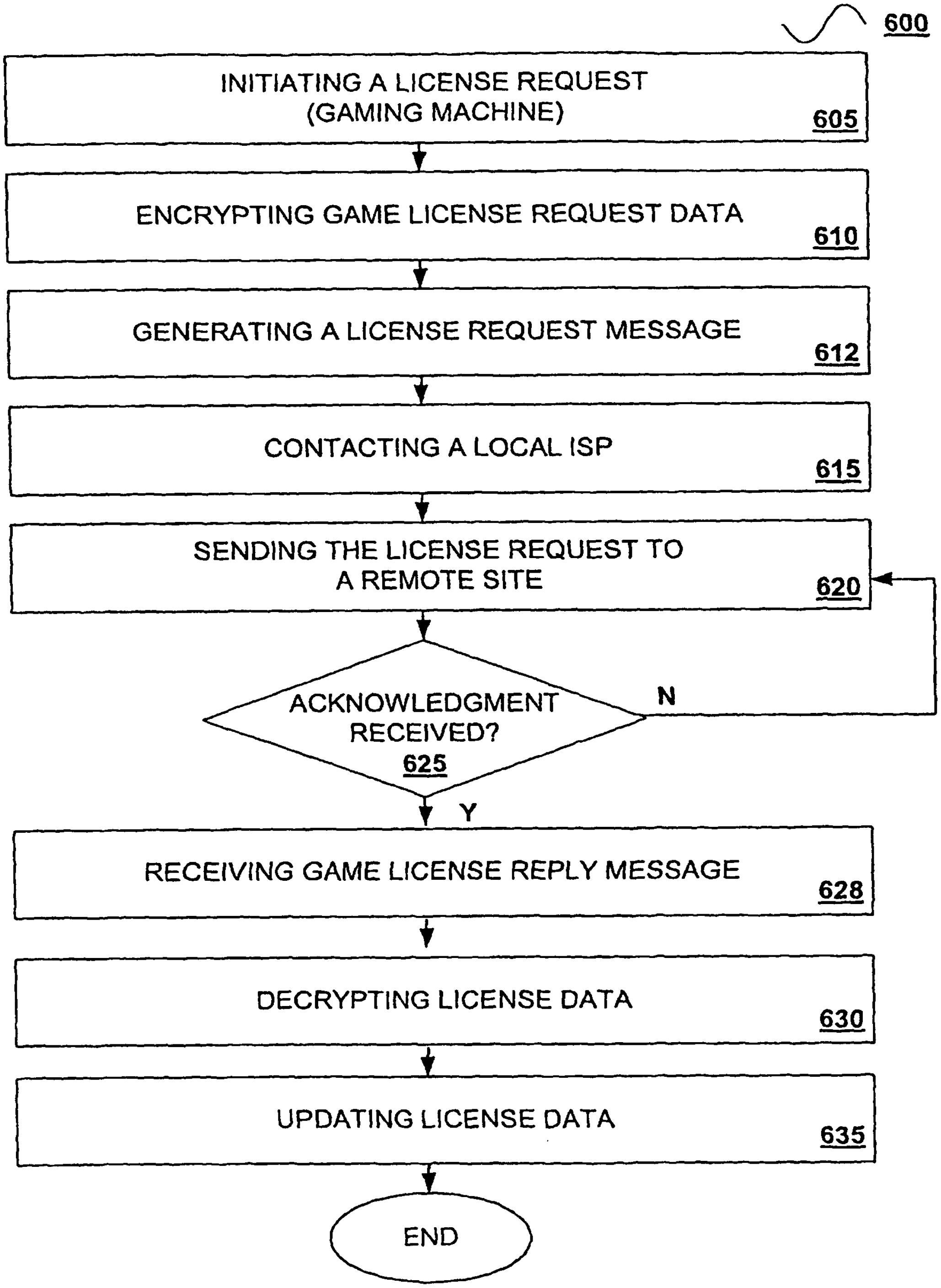

600
INITIATING A LICENSE REQUEST (GAMING MACHINE)
605
ENCRYPTING GAME LICENSE REQUEST DATA
610
GENERATING A LICENSE REQUEST MESSAGE
612
CONTACTING A LOCAL ISP
615
SENDING THE LICENSE REQUEST TO A REMOTE SITE
620
ACKNOWLEDGMENT RECEIVED?
625
N
Y
RECEIVING GAME LICENSE REPLY MESSAGE
628
DECRYPTING LICENSE DATA
630
UPDATING LICENSE DATA
635
END

FIGURE 6

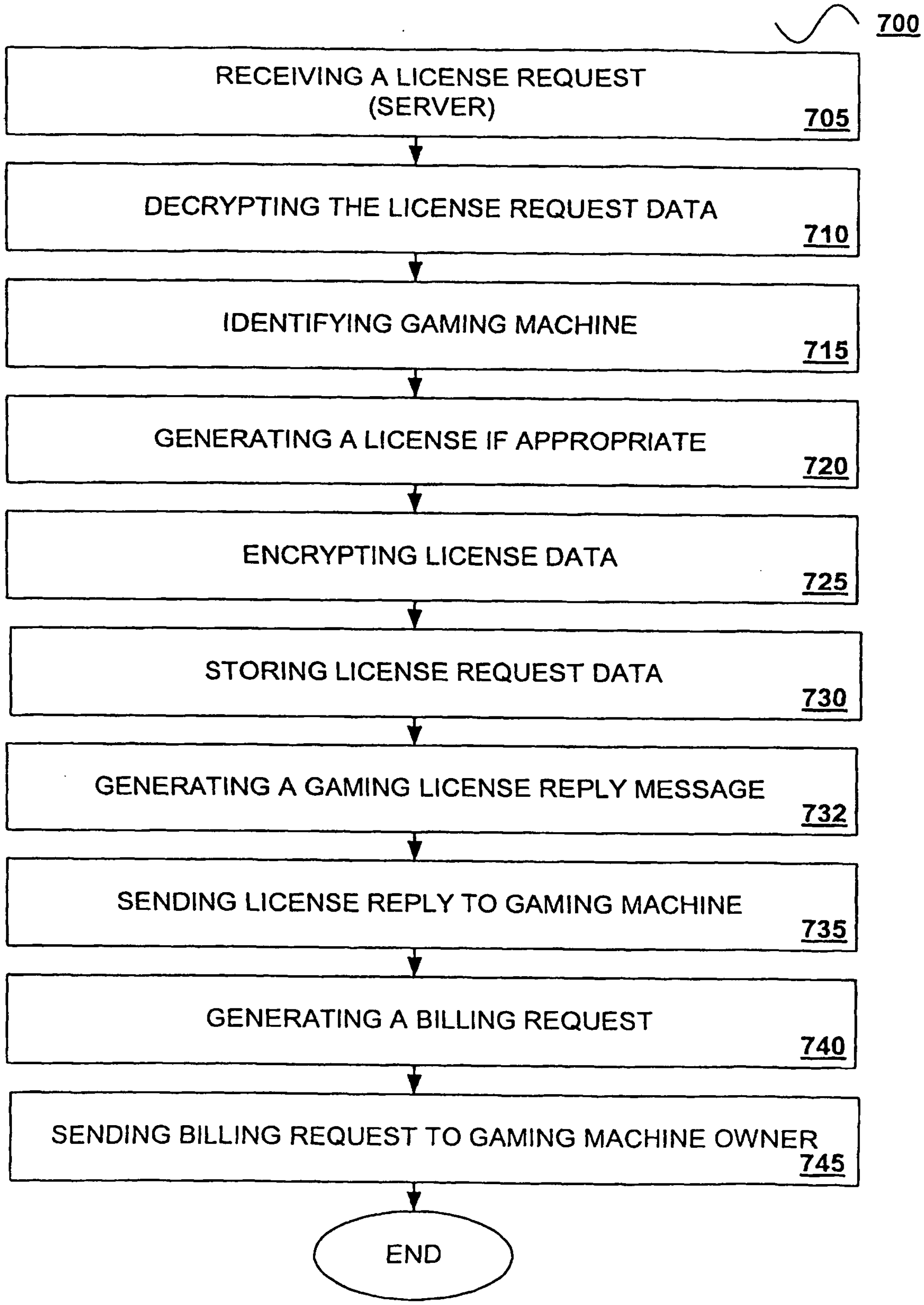

700
RECEIVING A LICENSE REQUEST (SERVER)
705
DECRYPTING THE LICENSE REQUEST DATA
710
IDENTIFYING GAMING MACHINE
715
GENERATING A LICENSE IF APPROPRIATE
720
ENCRYPTING LICENSE DATA
725
STORING LICENSE REQUEST DATA
730
GENERATING A GAMING LICENSE REPLY MESSAGE
732
SENDING LICENSE REPLY TO GAMING MACHINE
735
GENERATING A BILLING REQUEST
740
SENDING BILLING REQUEST TO GAMING MACHINE OWNER
745
END

FIGURE 7

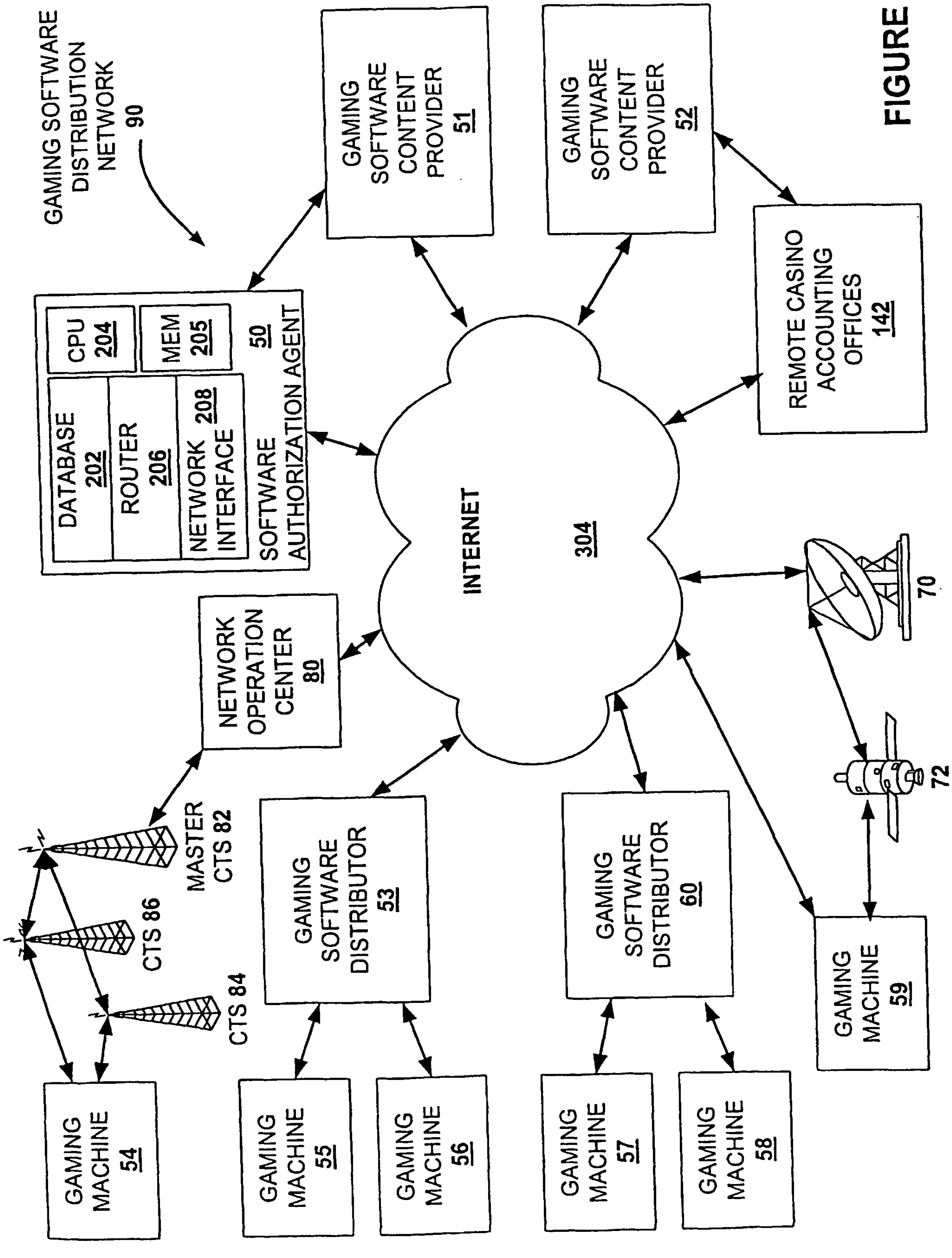

GAMING SOFTWARE DISTRIBUTION NETWORK 90
DATABASE 202
ROUTER 206
NETWORK INTERFACE 208
CPU 204
MEM 205
SOFTWARE AUTHORIZATION AGENT 50
GAMING SOFTWARE CONTENT PROVIDER 51
GAMING SOFTWARE CONTENT PROVIDER 52
REMOTE CASINO ACCOUNTING OFFICES 142
INTERNET
304
NETWORK OPERATION CENTER 80
70
72
MASTER CTS 82
CTS 86
CTS 84
GAMING SOFTWARE DISTRIBUTOR 53
GAMING SOFTWARE DISTRIBUTOR 60
GAMING MACHINE 59
GAMING MACHINE 54
GAMING MACHINE 55
GAMING MACHINE 56
GAMING MACHINE 57
GAMING MACHINE 58

FIGURE 8

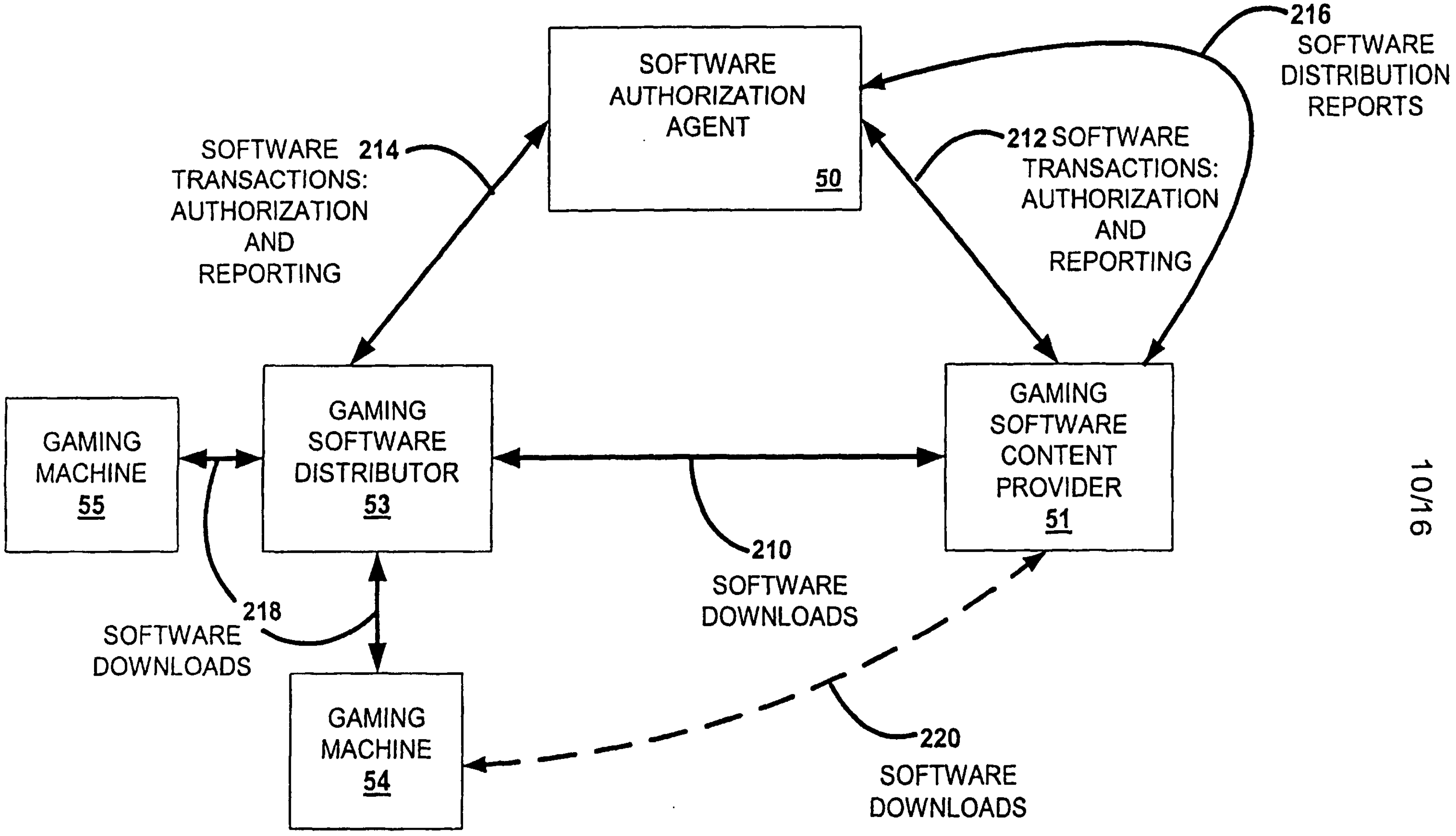

SOFTWARE
AUTHORIZATION
AGENT
50
GAMING
SOFTWARE
CONTENT
PROVIDER
51
GAMING
SOFTWARE
DISTRIBUTOR
53
GAMING
MACHINE
54
GAMING
MACHINE
55
210
SOFTWARE
DOWNLOADS
212 SOFTWARE
TRANSACTIONS:
AUTHORIZATION
AND
REPORTING
SOFTWARE 214
TRANSACTIONS:
AUTHORIZATION
AND
REPORTING
216
SOFTWARE
DISTRIBUTION
REPORTS
218
SOFTWARE
DOWNLOADS
220
SOFTWARE
DOWNLOADS

FIGURE 9

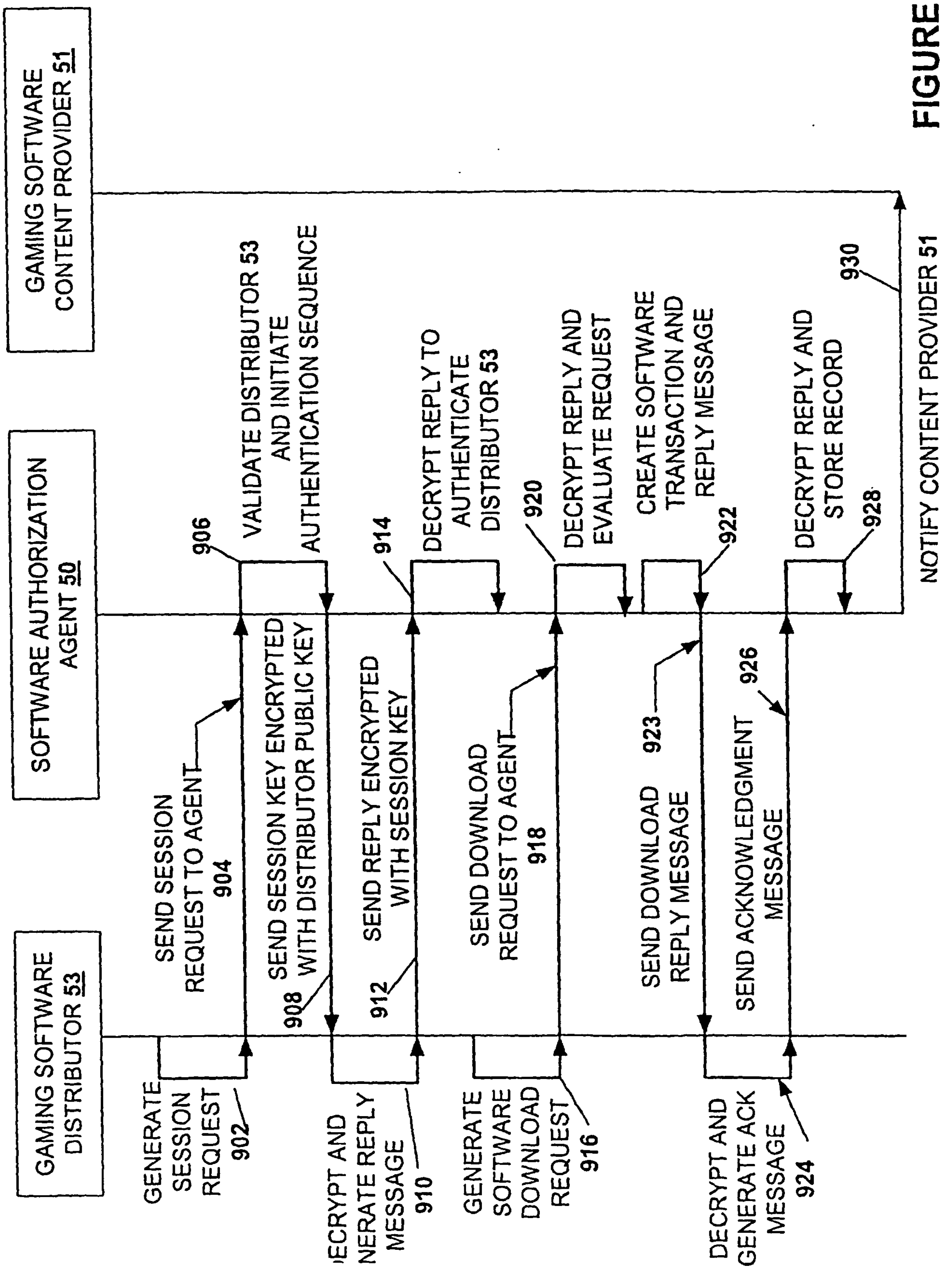

GAMING SOFTWARE DISTRIBUTOR 53
SOFTWARE AUTHORIZATION AGENT 50
GAMING SOFTWARE CONTENT PROVIDER 51
GENERATE SESSION REQUEST 902
SEND SESSION REQUEST TO AGENT 904
906
VALIDATE DISTRIBUTOR 53 AND INITIATE AUTHENTICATION SEQUENCE
SEND SESSION KEY ENCRYPTED WITH DISTRIBUTOR PUBLIC KEY
908
ECRYPT AND NERATE REPLY MESSAGE 910
SEND REPLY ENCRYPTED WITH SESSION KEY
912
914
DECRYPT REPLY TO AUTHENTICATE DISTRIBUTOR 53
GENERATE SOFTWARE DOWNLOAD REQUEST 916
SEND DOWNLOAD REQUEST TO AGENT 918
920
DECRYPT REPLY AND EVALUATE REQUEST
CREATE SOFTWARE TRANSACTION AND REPLY MESSAGE
922
SEND DOWNLOAD REPLY MESSAGE
923
DECRYPT AND GENERATE ACK MESSAGE 924
SEND ACKNOWLEDGMENT MESSAGE
926
DECRYPT REPLY AND STORE RECORD
928
NOTIFY CONTENT PROVIDER 51
930

FIGURE 10

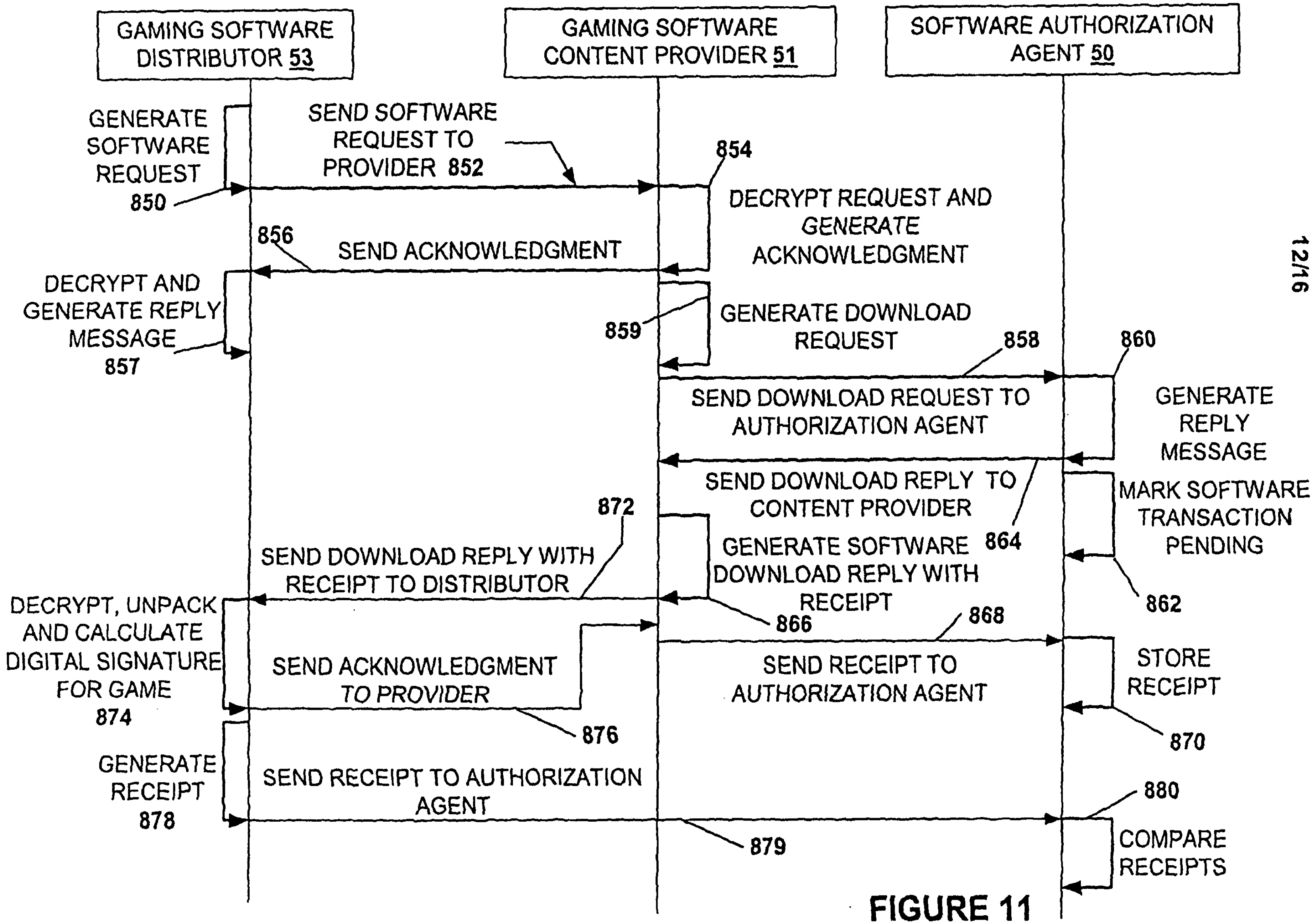

GAMING SOFTWARE DISTRIBUTOR 53
GAMING SOFTWARE CONTENT PROVIDER 51
SOFTWARE AUTHORIZATION AGENT 50
GENERATE SOFTWARE REQUEST
850
SEND SOFTWARE REQUEST TO PROVIDER 852
854
DECRYPT REQUEST AND GENERATE ACKNOWLEDGMENT
856
SEND ACKNOWLEDGMENT
DECRYPT AND GENERATE REPLY MESSAGE
857
859
GENERATE DOWNLOAD REQUEST
858
860
SEND DOWNLOAD REQUEST TO AUTHORIZATION AGENT
GENERATE REPLY MESSAGE
SEND DOWNLOAD REPLY TO CONTENT PROVIDER
MARK SOFTWARE TRANSACTION PENDING
872
864
GENERATE SOFTWARE DOWNLOAD REPLY WITH RECEIPT
SEND DOWNLOAD REPLY WITH RECEIPT TO DISTRIBUTOR
862
866
868
DECRYPT, UNPACK AND CALCULATE DIGITAL SIGNATURE FOR GAME
874
SEND ACKNOWLEDGMENT TO PROVIDER
SEND RECEIPT TO AUTHORIZATION AGENT
STORE RECEIPT
876
870
GENERATE RECEIPT
878
SEND RECEIPT TO AUTHORIZATION AGENT
880
879
COMPARE RECEIPTS

FIGURE 11

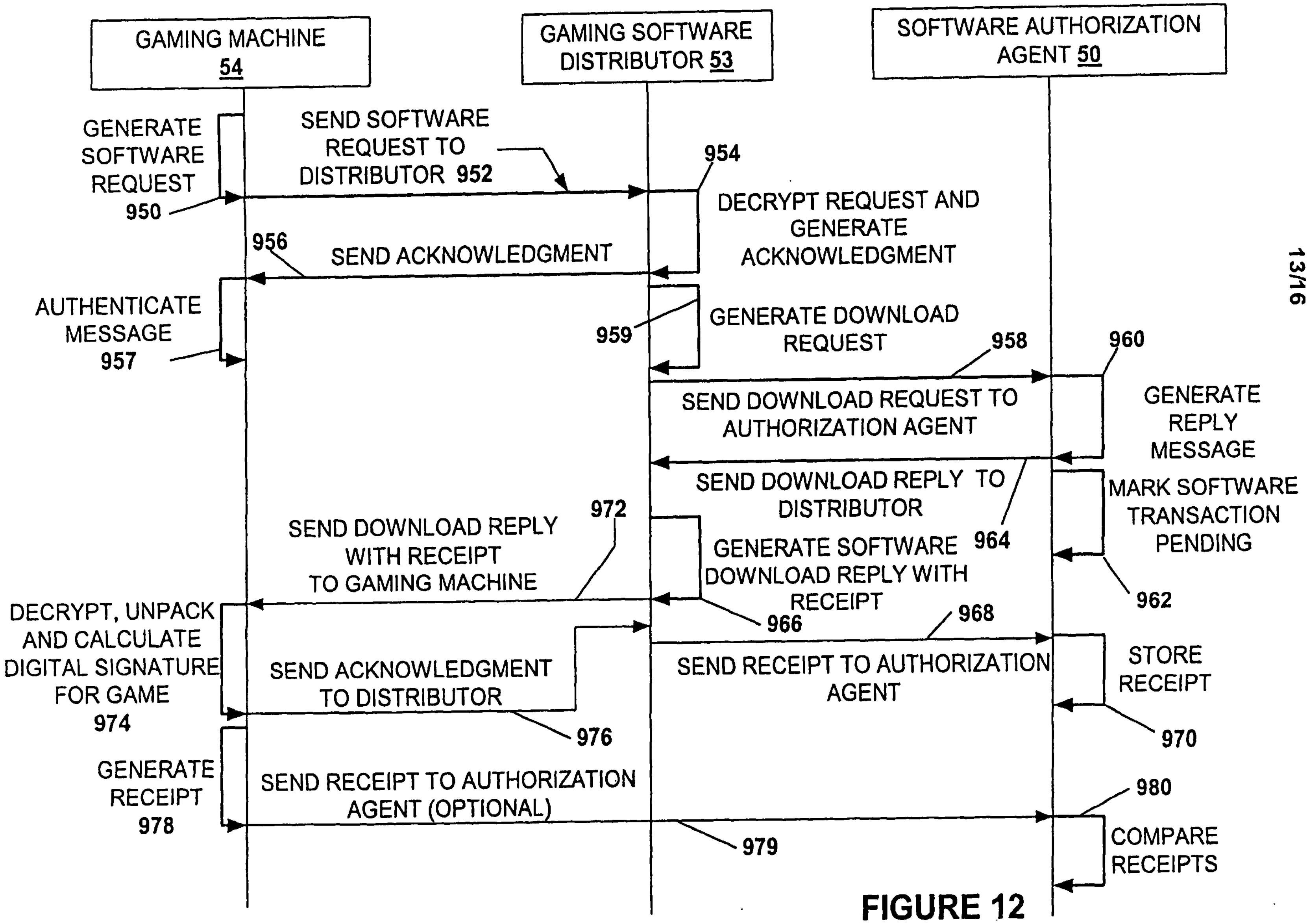

GAMING MACHINE 54
GAMING SOFTWARE DISTRIBUTOR 53
SOFTWARE AUTHORIZATION AGENT 50
GENERATE SOFTWARE REQUEST 950
SEND SOFTWARE REQUEST TO DISTRIBUTOR 952
954
DECRYPT REQUEST AND GENERATE ACKNOWLEDGMENT
956
SEND ACKNOWLEDGMENT
AUTHENTICATE MESSAGE 957
959
GENERATE DOWNLOAD REQUEST
958
960
SEND DOWNLOAD REQUEST TO AUTHORIZATION AGENT
GENERATE REPLY MESSAGE
SEND DOWNLOAD REPLY TO DISTRIBUTOR
964
MARK SOFTWARE TRANSACTION PENDING
962
972
SEND DOWNLOAD REPLY WITH RECEIPT TO GAMING MACHINE
GENERATE SOFTWARE DOWNLOAD REPLY WITH RECEIPT
966
968
DECRYPT, UNPACK AND CALCULATE DIGITAL SIGNATURE FOR GAME 974
SEND ACKNOWLEDGMENT TO DISTRIBUTOR
976
SEND RECEIPT TO AUTHORIZATION AGENT
STORE RECEIPT
970
GENERATE RECEIPT 978
SEND RECEIPT TO AUTHORIZATION AGENT (OPTIONAL)
979
980
COMPARE RECEIPTS

FIGURE 12

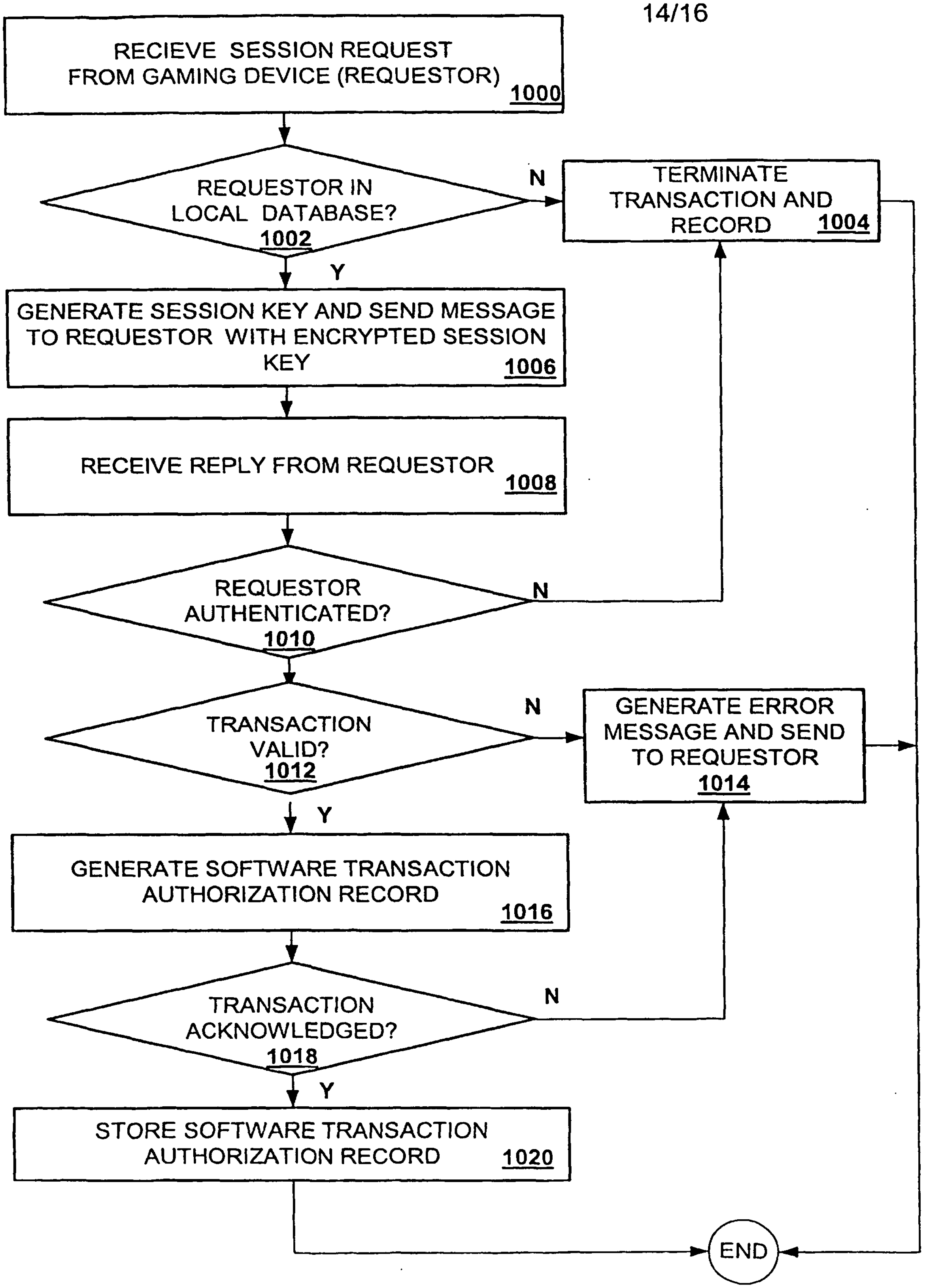

RECIEVE SESSION REQUEST FROM GAMING DEVICE (REQUESTOR) 1000
REQUESTOR IN LOCAL DATABASE? 1002
N
Y
TERMINATE TRANSACTION AND RECORD 1004
GENERATE SESSION KEY AND SEND MESSAGE TO REQUESTOR WITH ENCRYPTED SESSION KEY 1006
RECEIVE REPLY FROM REQUESTOR 1008
REQUESTOR AUTHENTICATED? 1010
N
TRANSACTION VALID? 1012
N
Y
GENERATE ERROR MESSAGE AND SEND TO REQUESTOR 1014
GENERATE SOFTWARE TRANSACTION AUTHORIZATION RECORD 1016
TRANSACTION ACKNOWLEDGED? 1018
N
Y
STORE SOFTWARE TRANSACTION AUTHORIZATION RECORD 1020
END

FIGURE 13

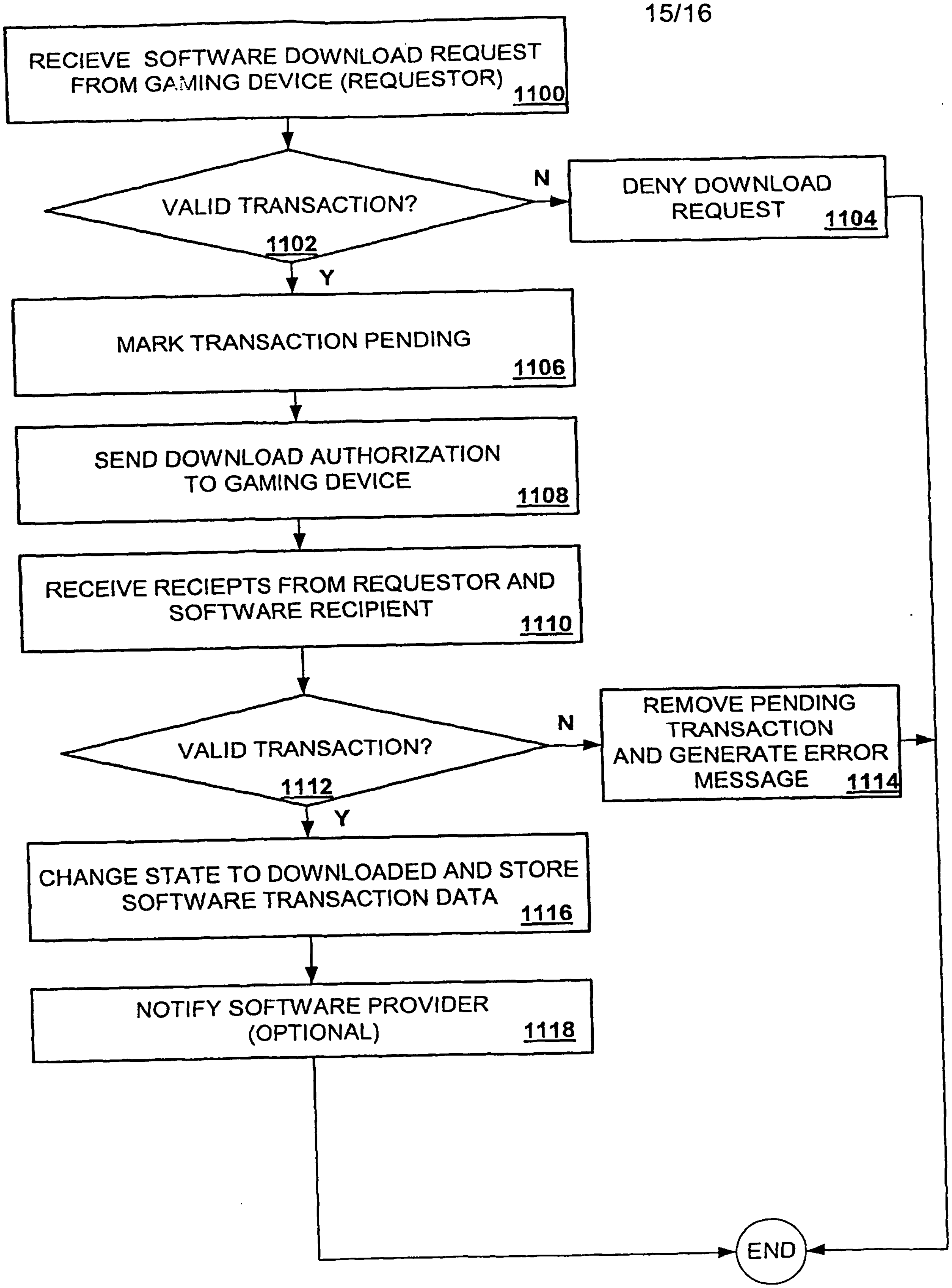

RECIEVE SOFTWARE DOWNLOAD REQUEST FROM GAMING DEVICE (REQUESTOR) 1100
VALID TRANSACTION? 1102
N
DENY DOWNLOAD REQUEST 1104
Y
MARK TRANSACTION PENDING 1106
SEND DOWNLOAD AUTHORIZATION TO GAMING DEVICE 1108
RECEIVE RECIEPTS FROM REQUESTOR AND SOFTWARE RECIPIENT 1110
VALID TRANSACTION? 1112
N
REMOVE PENDING TRANSACTION AND GENERATE ERROR MESSAGE 1114
Y
CHANGE STATE TO DOWNLOADED AND STORE SOFTWARE TRANSACTION DATA 1116
NOTIFY SOFTWARE PROVIDER (OPTIONAL) 1118
END

FIGURE 14

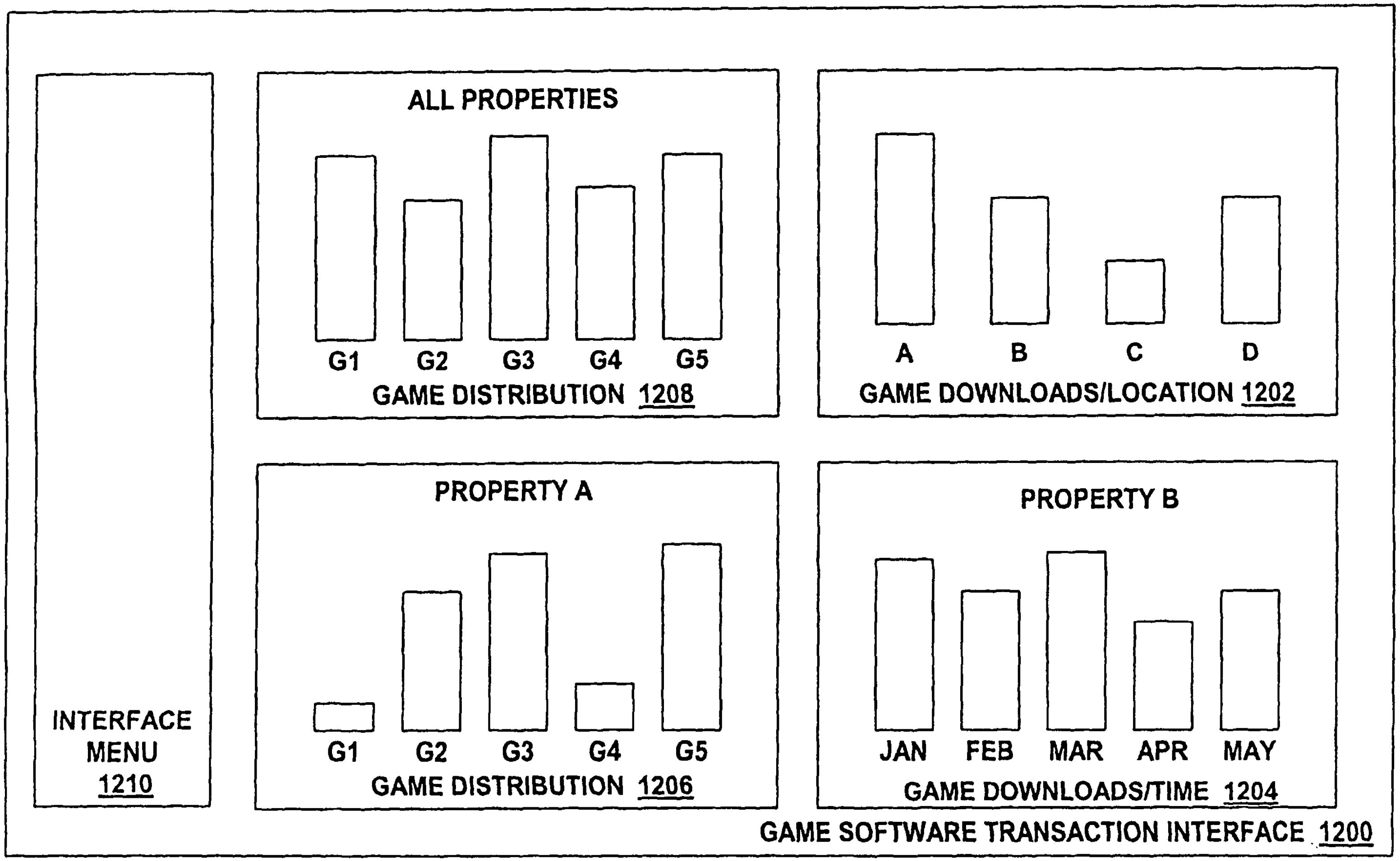

ALL PROPERTIES
G1
G2
G3
G4
G5
GAME DISTRIBUTION 1208
A
B
C
D
GAME DOWNLOADS/LOCATION 1202
INTERFACE
MENU
1210
PROPERTY A
G1
G2
G3
G4
G5
GAME DISTRIBUTION 1206
PROPERTY B
JAN
FEB
MAR
APR
MAY
GAME DOWNLOADS/TIME 1204
GAME SOFTWARE TRANSACTION INTERFACE 1200

FIGURE 15

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/09669

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F17/32 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F A63F H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 715 245 A (XEROX CORP) 5 June 1996 (1996-06-05)	1,20,39
A	page 2, line 35 - line 41 page 4, line 17 - line 37 page 21, line 52 -page 22, line 15 page 25, line 35 -page 26, line 7 ---	2-19, 21-38, 40-52
Y	EP 1 074 955 A (MAYGAY MACHINES) 7 February 2001 (2001-02-07)	1,20,39
A	paragraph ‘0019! - paragraph ‘0034!; claims 1-3; figure 5 ---	2-19, 21-38, 40-52
A	WO 02 05229 A (ONLINE GAMES LLC) 17 January 2002 (2002-01-17) page 2, line 26 -page 3, line 6; figure 1 --- -/--	1-52

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 31 July 2003	Date of mailing of the international search report 07/08/2003
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Reule, D

INTERNATIONAL SEARCH REPORT

Interna l Application No
PCT/US 03/09669

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 061 430 A (PULSE ENTERTAINMENT INC) 20 December 2000 (2000-12-20) paragraph ‘0002! - paragraph ‘0008! ---	1,20,39
A	US 6 002 772 A (SAITO MAKOTO) 14 December 1999 (1999-12-14) column 5, line 16 - line 61 -----	1,20,39

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/09669

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 0715245	A	05-06-1996	US	5629980	A	13-05-1997
			EP	1293871	A2	19-03-2003
			EP	1293872	A2	19-03-2003
			EP	1293873	A2	19-03-2003
			EP	1329795	A1	23-07-2003
			EP	1329796	A1	23-07-2003
			EP	1331542	A1	30-07-2003
			EP	0715245	A1	05-06-1996
			JP	8263441	A	11-10-1996
EP 1074955	A	07-02-2001	EP	1074955	A2	07-02-2001
			GB	2356279	A	16-05-2001
WO 0205229	A	17-01-2002	AU	7586601	A	21-01-2002
			WO	0205229	A2	17-01-2002
EP 1061430	A	20-12-2000	US	6460023	B1	01-10-2002
			AU	3013400	A	21-12-2000
			AU	5333700	A	02-01-2001
			BR	0002393	A	02-01-2001
			CA	2306984	A1	16-12-2000
			CN	1278083	A	27-12-2000
			EP	1061430	A1	20-12-2000
			JP	2001216042	A	10-08-2001
			NZ	504145	A	30-11-2001
			SG	87106	A1	19-03-2002
			TW	472183	B	11-01-2002
			WO	0077639	A1	21-12-2000
US 6002772	A	14-12-1999	US	2002059238	A1	16-05-2002
			US	2003012385	A1	16-01-2003
			US	5974141	A	26-10-1999
			US	2002052850	A1	02-05-2002
			US	2002112173	A1	15-08-2002
			US	6408390	B1	18-06-2002
			US	2001013021	A1	09-08-2001
			US	5867579	A	02-02-1999
			US	6424715	B1	23-07-2002
			US	6128605	A	03-10-2000

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 11/06/2006

```
BHARRISO     SALE   #00000001     Mailroom Dt:  09/25/2006     500388    10116424
                     01     FC : 1806                    180.00  DA
```

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

22434 7590 10/27/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.

EXAMINER

ART UNIT	PAPER
	20061026

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

PTO 1449 filed on 9/25/06 has been considered by the examiner.

CHRISTOPHER REVAK
PRIMARY EXAMINER

10/25/06

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty Docket No. IGT1P034X1/P-277 CIP Applicant: Nguyen et al. Filing Date April 3, 2002	Application No.: 10/116,424 Group 2131

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
CR	A1	2004/0002385	1/1/04	Nguyen			
CR	A2	2003/0054880	3/20/03	Lam et al.			
CR	A3	2002/0155887	10/24/02	Criss-Puszkiewicz et al.			

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
CR	B1	WO 03/085613	10/16/2003	PCT	G07F	17/32	X	

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
CR	C1	International Search Report and Written Opinion dated July 19, 2006 from corresponding PCT Application No. PCT/US2006/008785 (11 pages). [Atty. Dkt. No. IGT1P034X2WO]

Examiner /Christopher Revak/	Date Considered 10/26/2006

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22434 7590 09/18/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

```
12/13/2006 WABDELR3 00000008 10116424

01 FC:1501                1400.00 OP
02 FC:1504                 300.00 OP
03 FC:A001                  20.00 OP
```

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Chereyce Brown (Depositor's name)
Chereyce Brown (Signature)
December 11, 2006 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

TITLE OF INVENTION: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$300	$0	$1700	12/18/2006

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2131	726-004000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Beyer Weaver & Thomas LLP
2 ______
3 ______

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE
IGT

(B) RESIDENCE: (CITY and STATE OR COUNTRY)
RENO, NEVADA

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual ☒ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☒ Advance Order - # of Copies 10

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☒ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge ~~the required fee(s)~~ any deficiency, or credit any overpayment, to Deposit Account Number 50-0388 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ______ Date December 11, 2006

Typed or printed name David P. Olynick Registration No. 48,615

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	01/23/2007	7168089	IGT1P034X1/P-277CIP	3186

22434 7590 01/03/2007

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 931 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Binh T. Nguyen, Reno, NV;
Michael M. Oberberger, Reno, NV;
Gregory Hopkins Parrott, Reno, NV;

IR103 (Rev. 11/05)

10/116424

COFC

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: 10/116,424

Attorney Docket No.: IGT1P034X1

Patent: 7,168,089 B2

Issued: January 23, 2007

Title: SECURED VIRTUAL NETWORK IN A GAMING ENVIRONMENT

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on October 2, 2007 in an envelope addressed to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450.

Signed: ______________________
Juan D. Petris

REQUEST FOR CERTIFICATE OF CORRECTION OF OFFICE MISTAKE (35 U.S.C. §254, 37 CFR §1.322)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Attn: Certificate of Correction

Dear Sir:

Attached is Form PTO-1050 (Certificate of Correction) at least one copy of which is suitable for printing. The errors together with the exact page and line number where the errors are shown correctly in the application file are as follows:

SPECIFICATION:

1. Column 4, line 32, change "gaining" to --gaming--. This appears correctly in the patent application as filed on April 3, 2002, on page 5, line 26.

CLAIMS:

1. In line 1 of claim 18 (column 42, line 44) change "meted" to --method--. This appears correctly in Amendment A as filed on May 25, 2006, on page 4, paragraph 7, line 1.
2. In line 2 of claim 27 (column 43, line 18) change "an a" to --on a--. This appears correctly in Amendment A as filed on May 25, 2006, on page 6, paragraph 1, line 1.

3. In line 14 of claim 28 (column 43, line 33) change "are from" to --are separate from--. This appears correctly in Amendment A as filed on May 25, 2006, on page 6, paragraph 2, line 12.

4. In line 2 of claim 47 (column 44, line 64) change "preformed" to --performed--. This appears correctly in Amendment A as filed on May 25, 2006, on page 9, paragraph 1, line 1.

5. In line 21 of claim 52 (column 45, line 32) change "warning" to --gaming--. This appears correctly in the Notice of Allowability as mailed on September 18, 2006, on page 3, paragraph 1, line 3.

6. In line 3 of claim 56 (column 45, line 56) delete "on". This appears correctly in Amendment A as filed on May 25, 2006, on page 10, paragraph 4, line 2.

7. In line 1 of claim 60 (column 46, line 11) change "tho" to --the--. This appears correctly in Amendment A as filed on May 25, 2006, on page 10, paragraph 8, line 1.

8. In line 20 of claim 65 (column 46, line 44) change "tacking" to --tracking--. This appears correctly in Amendment A as filed on May 25, 2006, on page 11, paragraph 6, line 10.

9. In line 2 of claim 80 (column 47, line 42) change "preformed" to --performed--. This appears correctly in Amendment A as filed on May 25, 2006, on page 13, paragraph 7, line 1.

10. In line 13 of claim 84 (column 47, line 65) change "gamma" to --gaming--. This appears correctly in Amendment A as filed on May 25, 2006, on page 14, paragraph 1, line 8

11. In line 3 of claim 90 (column 48, line 32) change "flit" to --first--. This appears correctly in Amendment A as filed on May 25, 2006, on page 15, paragraph 2, line 2.

12. In line 2 of claim 92 (column 48, line 42) change "mare" to --more--. This appears correctly in Amendment A as filed on May 25, 2006, on page 15, paragraph 4, line 2.

13. In line 2 of claim 93 (column 48, line 51) change "gain" to --game--. This appears correctly in Amendment A as filed on May 25, 2006, on page 15, paragraph 5, line 1.

14. In line 4 of claim 93 (column 48, line 53) change "panchinko" to --pachinko--. This appears correctly in Amendment A as filed on May 25, 2006, on page 15, paragraph 5, line 3.

15. In line 2 of claim 101 (column 49, line 13) change "on to" to --on the--. This appears correctly in Amendment A as filed on May 25, 2006, on page 16, paragraph 5, line 2.

16. In line 7 of claim 103 (column 49, line 24) change "at designed" to --or designed--. This appears correctly in Amendment A as filed on May 25, 2006, on page 16, paragraph 7, line 6.

17. In line 16 of claim 103 (column 49, line 33) change "gamma" to --gaming--. This appears correctly in Amendment A as filed on May 25, 2006, on page 16, paragraph 7, line 11.

Patentee hereby requests expedited issuance of the Certificate of Correction because the error lies with the Office and because the error is clearly disclosed in the records of the Office. As required for expedited issuance, enclosed is documentation that unequivocally supports the patentee's assertion without needing reference to the patent file wrapper.

It is noted that the above-identified errors were printing errors that apparently occurred during the printing process. Accordingly, it is believed that no fees are due in connection with the filing of this Request for Certificate of Correction. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 50-0388 (Order No. IGT1P034X1).

Respectfully submitted,
BEYER WEAVER LLP

David P. Olynick
Registration No. 48,615

P.O. Box 70250
Oakland, CA 94612-0250
510-663-1100

gaming network environment, reduce the costs associated with adding new network gaming services and simplify the data acquisition process for gaming machines widely distributed within a gaming entity.

Another desire within the gaming industry is to electronically download gaming software from one or more remote locations to a gaming machine. The capability to electronically download gaming software is desirable because it may enable gaming machines to be quickly reconfigured to account for changes in popularity of various games played on the gaming machines and it may simplify software maintenance issues on the gaming machine such as gaming software updates. Currently, in a time consuming process, gaming software is manually loaded onto each gaming machine by a technician. The software is manually loaded because the gaming software is usually very highly regulated and in most gaming jurisdictions only approved gaming software may be installed on a gaming machine. Further, the gaming software is manually loaded for security reasons to prevent the source code from being obtained by individuals which might use the source code to try to find ways of cheating the gaming machine. In view of the above, it would be desirable to provide gaming software downloading methods for gaming machines that allow gaming software to be transferred electronically to the gaming machines from a remote location in a secure manner that satisfies regulatory requirements of the gaming jurisdiction where the gaming machine is located.

SUMMARY OF THE INVENTION

This invention addresses the needs indicated above by providing gaming machines that may securely communicate with devices over a public network such as the Internet. The invention provides a combination of symmetric and asymmetric encryption that allows a single gaming machine to securely communicate with a remote server using a public network. The secure communication methods may be used to transfer gaming software and gaming information between two gaming devices such as between a gaming machine and a game server. For regulatory and tracking purposes, the transfer of gaming software between the two gaming devices may be authorized and monitored by a software authorization agent.

One aspect of the present invention describes a software authorization agent capable of generating a gaming software transaction record used to facilitate a transfer

12. (Original)The method of claim 11, wherein the identification sequence is a symmetric encryption key used to encrypt gaming software transferred between the first gaming device and the second gaming device.

13. (Original)The method of claim 11, further comprising:

receiving from the first gaming device a second identification sequence encrypted with a public encryption key used by the software authorization agent,

decrypting the second identification sequence with a private encryption key corresponding to the public encryption key used by the software authorization agent;.

comparing the second identification sequence to the identification sequence sent to the first gaming device to authenticate the identity of the first gaming device.

14. (Original)The method of claim 13, wherein the second identification sequence is a symmetric encryption key used to transfer gaming software between the first gaming device and the second gaming device.

15. (Original)The method of claim 13, when the second identification sequence received from the first gaming device does not match the identification sequence sent to the first gaming device;

denying the gaming software transaction request.

16. (Original)The method of claim 1, wherein the gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number, a gaming software identification number, a gaming software provider identifier, a transaction number, a number of allowable downloads and combinations thereof.

17. (Original)The method of claim 1, further comprising:

storing the gaming transaction record information to a transaction database.

18. (Original)The method of claim 1, further comprising:

sending gaming software transaction information to the first gaming device.

requesting a list of gaming software installed on a gaming device.

28. (Currently Amended) In a software authorization agent, a method of regulating a transfer of gaming software between two gaming devices, the method comprising:

receiving a gaming software download request message with gaming software transaction information from a first gaming device;

validating the gaming software download request using the gaming software transaction information;

~~sending an authorization message to the first gaming device authorizing the first gaming device to transfer gaming software to a second gaming device;~~

sending an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

29. (Original)The method of claim 28, wherein the second gaming device is at least one of a game server and a gaming machine.

30. (Original)The method of claim 28, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

31. (Original)The method of claim 28, wherein the gaming transaction information is one or more of a transaction encryption key, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and combinations thereof.

((

47. (Original)The method of claim 28, wherein the transfer of gaming software is performed at least one of manually and electronically.

48. (Original)The method of claim 28, wherein the gaming software comprises one or more gaming software components for the game of chance, the bonus game of chance, the device driver, the player tracking service and the operating system.

49. (Original)The method of claim 28, wherein the gaming software is used to upgrade a gaming software component on the second gaming device.

50. (Original)The method of claim 28, wherein the gaming software is used to correct an error in a gaming software component on the second gaming device.

51. (Original)The method of claim 28, further comprising:

requesting a list of gaming software installed on a gaming device.

52. (Currently Amended) In a software authorization agent, a method of providing gaming software transaction information, the method comprising:

receiving a gaming software transaction information request from a gaming device;

authenticating an identity of the gaming device;

querying a gaming software transaction database for a set of gaming software transaction information requested by the gaming device, said gaming software transaction database comprising a plurality of records of gaming software transactions wherein each gaming software transaction is related to a request to authorize a transfer of gaming software received by the software authorization agent; and

sending the requested gaming software transaction information to the gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

53. (Original)The method of claim 52,

wherein each gaming software transaction record includes gaming software transaction information that describes a transfer of gaming software from a first gaming device to a second gaming device.

54. (Original)The method of claim 52,

wherein the gaming software transaction database includes a record of gaming software installed on one or more gaming devices.

55. (Original)The method of claim 52, wherein the gaming software transaction database includes a record of gaming software usage on one or more gaming devices.

56. (Original)The method of claim 52, wherein the gaming transaction information is one or more of a transaction number, a time stamp, a transaction expiration time, a destination identifier, a machine identification number for the first gaming device, a machine identification number for the second gaming device, a gaming software identification number, operator information for the first gaming device, operator information for the second gaming device, a transaction number and a transaction completion time.

57. (Original)The method of claim 52, further comprising:

generating a gaming transaction report that presents the set of gaming software transaction requested by the gaming device.

58. (Original)The method of claim 52, further comprising:

generating a distribution of gaming software on a plurality of gaming machines at a specified time using the gaming software transaction information stored in the gaming software transaction database.

59. (Original)The method of claim 52, further comprising:

generating a distribution of gaming software on a plurality of gaming machines for a plurality of times using the gaming software transaction information stored in the gaming software transaction database.

60. (Original)The method of claim 52, further comprising:

generating a billing report.

61. (Original)The method of claim 60, further comprising:

generating a fee for the billing report based upon a number of times a first gaming software has been used on the gaming device.

62. (Original)The method of claim 61, wherein a usage fee charged each time the first gaming software is used varies with time.

63. (Original)The method of claim 52, further comprising:

requesting a list of gaming software installed on the gaming device.

64. (Original)The method of claim 63, further comprising:

storing the list of gaming software installed on the gaming device to the gaming software transaction database.

65. (Original) In a first gaming device, a method of requesting a transfer of gaming software from a second gaming device, said method comprising:

generating a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and

receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

66. (Original)The method of claim 65, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

sending a message requesting the gaming software to the second gaming device.

75. (Original)The method of claim 65, further comprising:
receiving the gaming software from the second gaming device.

76. (Original)The method of claim 75, further comprising:
determining a digital signature for the gaming software and
sending a message with at least the digital signature to the gaming software authorization agent.

77. (Original)The method of claim 65, further comprising:
authenticating an identity of the second gaming device.

78. (Original)The method of claim 65, wherein the first gaming device is a gaming machine and the second gaming device is a game server.

79. (Original)The method of claim 65, wherein the first gaming device is a game server in communication with a plurality of gaming machines and the second gaming device is a game server maintained by a gaming software content provider.

80. (Original)The method of claim 65, wherein the transfer of gaming software is performed at least one of manually and electronically.

81. (Original)The method of claim 65, wherein the gaming software comprises one or more gaming software components.

82. (Original)The method of claim 65, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

83. (Original)The method of claim 65, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

84. (Currently Amended) In a first gaming device, a method of transferring gaming software to a second gaming device, said method comprising:

receiving a gaming software transaction request from the second gaming device;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software;

receiving an authorization message from the gaming software authorization agent wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to the second gaming device; and

transferring the gaming software to the second gaming device;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

85. (Original)The method of claim 84, further comprising:

receiving an approval of the gaming software transaction request from the gaming software authorization agent.

86. (Original)The method of claim 84, further comprising:

prior to transferring the gaming software, receiving a denial of the gaming software transaction request from the gaming software authorization agent; and

terminating the transfer of the gaming software.

87. (Original)The method of claim 84, wherein the software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

88. (Original)The method of claim 84, wherein the software authorization agent, the first gaming device and the second gaming device communicate with another using at least one of a satellite communication connection, a RF communication connection, an infrared communication connection and combinations thereof.

89. (Original)The method of claim 84, wherein the gaming software transaction request comprises access information and gaming software identification information.

90. (Original)The method of claim 89, wherein the access information is one or more of operator identification information for the first gaming device, machine identification information for the first gaming device, operator identification information for the second gaming device and machine identification information for the second gaming device.

91. (Original)The method of claim 89, wherein the gaming software identification information is one or more of a gaming software title, a gaming software provider identifier, a gaming software version number and a gaming software identification number.

92. (Original)The method of claim 84, wherein the gaming software transaction information is one or more of a one or more of a transaction encryption key, a public encryption key used by the second gaming device, a transaction number, a time stamp, a transaction expiration time, a destination identifier, a destination machine identification number, a gaming software identification number,. a gaming software provider identifier, a number of allowable downloads, a transaction number and combinations thereof.

93. (Original)The method of claim 84, wherein the game of chance is a video slot game, a mechanical slot game, a lottery game, a video poker game, a video black jack game, a video lottery game, and a video pachinko game.

94. (Original)The method of claim 84, further comprising:

determining a digital signature for the gaming software and

sending a message with at least the digital signature to the gaming software authorization agent.

95. (Original)The method of claim 84, wherein the first gaming device is a gaming server and the second gaming device is a gaming machine.

96. (Original)The method of claim 84, wherein the first gaming device is a gaming machine and the second gaming device is a gaming machine.

97. (Original)The method of claim 84, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a game server maintained by a gaming entity.

98. (Original)The method of claim 84, wherein the first gaming device is a game server maintained by a gaming software content provider and the second gaming device is a gaming machine maintained by a gaming entity.

99. (Original)The method of claim 84, wherein the transfer of gaming software is performed at least one of manually and electronically.

100. (Original)The method of claim 84, wherein the gaming software comprises one or more gaming software components.

101. (Original)The method of claim 84, wherein the gaming software is used to upgrade a gaming software component on the gaming machine.

102. (Original)The method of claim 84, wherein the gaming software is used to correct an error in a gaming software component on the gaming machine.

103. (Currently Amended) A software authorization agent for facilitating the transfer of gaming software between a plurality of gaming devices, the software authorization agent comprising:

a network interface allowing the authorization agent to communicate with each of the plurality of gaming devices; and

a processor configured or designed to (i) receive gaming software transfer requests via the network interface from a ~~first~~ gaming device for the transfer of gaming software from the first gaming device to a second gaming device ~~to a third gaming device~~ (ii) approve or reject the gaming software transaction request; and iii) send an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device;

sending an authorization message to a first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to a second gaming device and wherein the first gaming device and the second gaming device are separate from the software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

65. (Currently Amended) In a first gaming device, a method of requesting a transfer of gaming software from a second gaming device, said method comprising:

generating a gaming software transaction request;

sending the gaming software transaction request to a gaming software authorization agent that approves or rejects the transfer of gaming software from the second gaming device; and

~~receiving gaming transaction information from the gaming software authorization agent that is used to transfer the gaming software from the second gaming device~~

receiving an authorization message from the gaming software authorization agent wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming software to the second gaming device and wherein the first gaming device and the second gaming device are separate from the gaming software authorization agent;

wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a for a device installed on a gaming machine d) a player tracking service on a gaming machine and e) an operating system installed on a gaming machine.

66. (Currently Amended)The method of claim 65, wherein the gaming software authorization agent, the first gaming device and the second gaming device communicate with one another a local area network, a wide area network, a private network, a virtual private network, the Internet and combinations thereof.

67. (Currently Amended)The method of claim 65, wherein the gaming software authorization agent, the first gaming device and the second gaming device communicate with another using at

PTO/SB/44 (10-96)
Approved for use through 6/30/99. OMB 0651-0033
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB Control number

(Also Form PT-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,168,089 B2 Page 1 of 2

DATED : January 23, 2007

INVENTOR(S) : Nguyen et al.

It is certified that error appears in the above-identified patent and that said Letters Patent are hereby corrected as shown below:

In the Specification:

Column 4, line 32, change “gaining” to --gaming--.

In the Claims:

In line 1 of claim 18 [column 42, line 44] change “meted” to --method--.

In line 2 of claim 27 [column 43, line 18] change “an a” to --on a--.

In line 14 of claim 28 [column 43, line 33] change “are from” to --are separate from--.

In line 2 of claim 47 [column 44, line 64] change “preformed” to --performed--.

In line 21 of claim 52 [column 45, line 32] change “warning” to --gaming--.

In line 3 of claim 56 [column 45, line 56] delete “on”.

In line 1 of claim 60 [column 46, line 11] change “tho” to --the--.

In line 20 of claim 65 [column 46, line 44] change “tacking” to --tracking--.

In line 2 of claim 80 [column 47, line 42] change “preformed” to --performed--.

In line 13 of claim 84 [column 47, line 65] change “gamma” to --gaming--.

In line 3 of claim 90 [column 48, line 32] change “flit” to --first--.

In line 2 of claim 92 [column 48, line 42] change “mare” to --more--.

MAILING ADDRESS OF SENDER: PATENT NO. 7,168,089 B2

David P. Olynick
BEYER WEAVER LLP
P.O. Box 70250
Oakland, CA 94612-0250

No. of Additional Copies

1

Burden Hour Statement: This form is estimated to take 1.0 hour to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PTO/SB/44 (10-96)
Approved for use through 6/30/99. OMB 0651-0033
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB Control number

(Also Form PT-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,168,089 B2 Page 2 of 2

DATED : January 23, 2007

INVENTOR(S) : Nguyen et al.

It is certified that error appears in the above-identified patent and that said Letters Patent are hereby corrected as shown below:

In the Claims (continued):

In line 2 of claim 93 [column 48, line 51] change “gain” to --game--.

In line 4 of claim 93 [column 48, line 53] change “panchinko” to --pachinko--.

In line 2 of claim 101 [column 49, line 13] change “on to” to --on the--.

In line 7 of claim 103 [column 49, line 24] change “at designed” to --or designed--.

In line 16 of claim 103 [column 49, line 33] change “gamma” to --gaming--.

MAILING ADDRESS OF SENDER: PATENT NO. 7,168,089 B2

David P. Olynick
BEYER WEAVER LLP
P.O. Box 70250
Oakland, CA 94612-0250

No. of Additional Copies

1

Burden Hour Statement: This form is estimated to take 1.0 hour to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,168,089 B2 Page 1 of 2
APPLICATION NO. : 10/116424
DATED : January 23, 2007
INVENTOR(S) : Nguyen et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Specification:

Column 4, line 32, change “gaining” to --gaming--.

In the Claims:

In line 1 of claim 18 [column 42, line 44] change “meted” to --method--.

In line 2 of claim 27 [column 43, line 18] change “an a” to --on a--.

In line 14 of claim 28 [column 43, line 33] change “are from” to --are separate from--.

In line 2 of claim 47 [column 44, line 64] change “preformed” to --performed--.

In line 21 of claim 52 [column 45, line 32] change “warning” to --gaming--.

In line 3 of claim 56 [column 45, line 56] delete “on”.

In line 1 of claim 60 [column 46, line 11] change “tho” to --the--.

In line 20 of claim 65 [column 46, line 44] change “tacking” to --tracking--.

In line 2 of claim 80 [column 47, line 42] change “preformed” to --performed--.

In line 13 of claim 84 [column 47, line 65] change “gamma” to --gaming--.

In line 3 of claim 90 [column 48, line 32] change “flit” to --first--.

In line 2 of claim 92 [column 48, line 42] change “mare” to --more--.

In line 2 of claim 93 [column 48, line 51] change “gain” to --game--.

In line 4 of claim 93 [column 48, line 53] change “panchinko” to --pachinko--.

In line 2 of claim 101 [column 49, line 13] change “on to.” to --on the--.

In line 7 of claim 103 [column 49, line 24] change “at designed” to --or designed--.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 7,168,089 B2	Page 2 of 2
APPLICATION NO.	: 10/116424	
DATED	: January 23, 2007	
INVENTOR(S)	: Nguyen et al.	

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims (continued):

In line 16 of claim 103 [column 49, line 33] change "gamma" to --gaming--.

Signed and Sealed this

Eleventh Day of December, 2007

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
10/116,424	7168089	2131	9200

OC000000030922649

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 79646 on 07/10/2008

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 79646 is:

79646
Weaver Austin Villeneuve & Sampson LLP - IGT
Attn: IGT
P.O. Box 70250
Oakland, CA 94612-0250

PART 1 - ATTORNEY/APPLICANT COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/116,424	04/03/2002	Binh T. Nguyen	IGT1P034X1/P-277CIP	3186

79646 7590 12/18/2008
Weaver Austin Villeneuve & Sampson LLP - IGT
Attn: IGT
P.O. Box 70250
Oakland, CA 94612-0250

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
12/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
10116424	4/3/02	NGUYEN ET AL.	IGT1P034X1/P-277CIP

Weaver Austin Villeneuve & Sampson LLP - IGT
Attn: IGT
P.O. Box 70250
Oakland, CA 94612-0250

EXAMINER	
BRANDON S. HOFFMAN	
ART UNIT	PAPER
2436	20081211

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

You are hereby notified under 37 CFR 1.607(d) that an applicant is seeking to provoke an interference with your U.S. Patent No. (7,168,089)
The identify of the applicant will not be disclosed unless an interference is declared.
If a final decision is made not to declare an interference, a notice to that effect will be placed in the patent file and will be sent to the patentee.
If an interference is declared, notice thereof will be made under 37 CFR 1.611.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2436

PTO-90C (Rev.04-03)

Paper 1

Mail Stop Interference
P.O. Box 1450
Alexandria Va 22313-1450
Tel: 571-272-4683
Fax: 571-273-0042

Filed: March 5, 2010

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Legal iGaming, Inc.
Junior Party
(Application 10/658,836;
Inventors: Rolf E. Carlson and Michael W. Saunders),

v.

IGT
Senior Party
(Patent 7,168,089;
Inventors: Binh T. Nguyen, Michael M. Oberberger and
Gregory Hopkins Parrott).

Patent Interference No. 105,747 (RES)
(Technology Center 2400)

DECLARATION - 37 CFR § 41.203(b)

Part A. Declaration of interference

An interference is declared (35 U.S.C. § 135(a)) between the above-identified parties. Details of the application and patent, count and claims designated as corresponding to the count appear in Parts E and F of this DECLARATION.

No papers may be filed in the involved application or patent file without authority of the board.[1]

Part B. Judge managing the interference

Administrative Patent Judge Richard E. Schafer has been designated to manage the interference. 37 CFR § 41.104(a).

Part C. Standing order

A Trial Section STANDING ORDER [SO] (Paper 2) accompanies this DECLARATION. The STANDING ORDER applies to this interference.

Part D. Initial conference call

A telephone conference call to discuss the interference is set for April 30, 2010 at 4:00 p.m. (the Board will initiate the call).

No later than two business days prior to the conference call, each party shall file and serve (SO ¶¶ 10.1 ¶ 105) a list of the motions (37 CFR § 41.120; 37 CFR § 41.204; SO ¶¶ 104.2.1, 120 & 204) the party would like to file with a short explanation of the motion.

No later than two business days prior to the conference call, each party shall file and serve (SO ¶¶ 10.1 & 105) a list of the motions (37 CFR §§ 41.120 & 41.204; SO ¶¶ 104.2.1, 120 & 204) the party would like to file.

The time periods for taking action during the motion phase are set in an order accompanying this declaration.

[1] Any fees that are or become due may be paid.

Part E. Identification and order of the parties

Junior Party

Named inventors:	Rolf E. Carlson Michael W. Saunders
Involved Application:	10/658,836 filed August 21, 2003
Title:	Universal Gaming Engine
Assignee:	Legal iGaming, Inc.

Senior Party

Named Inventors:	Binh T. Nguyen Michael M. Oberberger Gregory Hopkins Parrott
Involved Patent:	7,168,089 based on Application 10/116,424 filed April 3, 2002
Title:	Secured Virtual Network in a Gaming Environment
Assignee:	IGT

The senior party is assigned exhibit numbers 1001-1999. The junior party is assigned exhibit numbers 2001-2999. 37 CFR § 41.154(c)(1); SO ¶ 154.2.1. The senior party is responsible for initiating settlement discussions. SO ¶ 126.1.

Part F. Count and claims of the parties

Count 1

The subject matter of Claim 1 or Claim 28 or Claim 52 or Claim 65 of Claim 84 or Claim 103 or Claim 123 of Patent 7,168,089.

The claims of the parties are:

Application:	10/658,836:	Claims	29-32, 35-43, 49, 56-58, 60-72, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167
Patent:	7,168,089:	Claims	1-136

The claims of the parties which correspond to Count 1 are:

Application:	10/658,836:	Claims	29-32, 35-43, 49, 56-58, 60-72, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167
Patent:	7,168,089:	Claims	1-136

The claims of the parties which do not correspond to Count 1 and are not involved in the interference are:

Application:	10/658,836:	Claims	None
Patent:	7,168,089:	Claims	None

The parties are accorded the following benefit for Count 1:

Legal iGaming, Inc:	None
IGT:	None

Part G. Heading to be used on papers

The following heading must be used on all papers filed in this interference, see SO ¶ 106.1.1:

Filed on behalf of: *Party @* Paper *Leave blank*
By: *Counsel Name(s) @*
Address @
(@@@) @@@- @@@@ (telephone)
(@@@) @@@- @@@@ (facsimile)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Legal iGaming, Inc.
Junior Party
(Application 10/658,836
Inventors: Rolf E. Carlson and Michael W. Saunders),

v.

IGT
Senior Party
(Patent 7,168,089
Inventors: Binh T. Nguyen, Michael M. Oberberger and
Gregory Hopkins Parrott).

Patent Interference No. 105,474 (RES)
(Technology Center 2400)

Title of Paper

Part H. Order form for requesting file copies

When requesting copies of files, use of SO Form 4 will greatly expedite processing of the request. Please attach a copy of Parts E and F of this DECLARATION with a hand-drawn circle around the patents and applications for which a copy of a file wrapper is requested.

/Richard E. Schafer/
Administrative Patent Judge

Enc:
Copy of STANDING ORDER
Copy of claims of Application 10/658,836

cc (via overnight delivery):

Attorney for Legal iGaming:
Knobbe Martens Olson & Bear LLP
2040 Main Street
Fourteenth Floor
Irvine CA 92614

Attorney for IGT:
Weaver Austin Villeneuve & Sampson LLP - IGT
500 12th Street
Suite 200
Oakland CA 94607

Paper 1

Mail Stop Interference
P.O. Box 1450
Alexandria Va 22313-1450
Tel: 571-272-4683
Fax: 571-273-0042

Filed: March 5, 2010

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Legal iGaming, Inc.
Junior Party
(Application 10/658,836;
Inventors: Rolf E. Carlson and Michael W. Saunders),

v.

IGT
Senior Party
(Patent 7,168,089;
Inventors: Binh T. Nguyen, Michael M. Oberberger and
Gregory Hopkins Parrott).

Patent Interference No. 105,747 (RES)
(Technology Center 2400)

DECLARATION - 37 CFR § 41.203(b)

Part A. Declaration of interference

An interference is declared (35 U.S.C. § 135(a)) between the above-identified parties. Details of the application and patent, count and claims designated as corresponding to the count appear in Parts E and F of this DECLARATION.

No papers may be filed in the involved application or patent file without authority of the board.[1]

Part B. Judge managing the interference

Administrative Patent Judge Richard E. Schafer has been designated to manage the interference. 37 CFR § 41.104(a).

Part C. Standing order

A Trial Section STANDING ORDER [SO] (Paper 2) accompanies this DECLARATION. The STANDING ORDER applies to this interference.

Part D. Initial conference call

A telephone conference call to discuss the interference is set for **April 30, 2010 at 4:00 p.m.** (the Board will initiate the call).

No later than **two business days** prior to the conference call, each party shall file and serve (SO ¶¶ 10.1 ¶ 105) a list of the motions (37 CFR § 41.120; 37 CFR § 41.204; SO ¶¶ 104.2.1, 120 & 204) the party would like to file with a short explanation of the motion.

No later than two business days prior to the conference call, each party shall file and serve (SO ¶¶ 10.1 & 105) a list of the motions (37 CFR §§ 41.120 & 41.204; SO ¶¶ 104.2.1, 120 & 204) the party would like to file.

The time periods for taking action during the motion phase are set in an order accompanying this declaration.

[1] Any fees that are or become due may be paid.

Part E. Identification and order of the parties

Junior Party

Named inventors:	Rolf E. Carlson Michael W. Saunders
Involved Application:	10/658,836 filed August 21, 2003
Title:	Universal Gaming Engine
Assignee:	Legal iGaming, Inc.

Senior Party

Named Inventors:	Binh T. Nguyen Michael M. Oberberger Gregory Hopkins Parrott
Involved Patent:	7,168,089 based on Application 10/116,424 filed April 3, 2002
Title:	Secured Virtual Network in a Gaming Environment
Assignee:	IGT

The senior party is assigned exhibit numbers 1001-1999. The junior party is assigned exhibit numbers 2001-2999. 37 CFR § 41.154(c)(1); SO ¶ 154.2.1. The senior party is responsible for initiating settlement discussions. SO ¶ 126.1.

Part F. Count and claims of the parties

Count 1

The subject matter of Claim 1 or Claim 28 or Claim 52 or Claim 65 of Claim 84 or Claim 103 or Claim 123 of Patent 7,168,089.

The claims of the parties are:

Application:	10/658,836:	Claims	29-32, 35-43, 49, 56-58, 60-72, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167
Patent:	7,168,089:	Claims	1-136

The claims of the parties which correspond to Count 1 are:

Application:	10/658,836:	Claims	29-32, 35-43, 49, 56-58, 60-72, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167
Patent:	7,168,089:	Claims	1-136

The claims of the parties which do not correspond to Count 1 and are not involved in the interference are:

Application:	10/658,836:	Claims	None
Patent:	7,168,089:	Claims	None

The parties are accorded the following benefit for Count 1:

Legal iGaming, Inc:	None
IGT:	None

Part G. Heading to be used on papers

The following heading must be used on all papers filed in this interference, see SO ¶ 106.1.1:

Filed on behalf of: *Party @* Paper *Leave blank*
By: *Counsel Name(s) @*
Address @
(@@@) @@@- @@@@ (telephone)
(@@@) @@@- @@@@ (facsimile)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Legal iGaming, Inc.
Junior Party
(Application 10/658,836
Inventors: Rolf E. Carlson and Michael W. Saunders),

v.

IGT
Senior Party
(Patent 7,168,089
Inventors: Binh T. Nguyen, Michael M. Oberberger and
Gregory Hopkins Parrott).

Patent Interference No. 105,474 (RES)
(Technology Center 2400)

Title of Paper

Part H. Order form for requesting file copies

When requesting copies of files, use of SO Form 4 will greatly expedite processing of the request. Please attach a copy of Parts E and F of this DECLARATION with a hand-drawn circle around the patents and applications for which a copy of a file wrapper is requested.

/Richard E. Schafer/
Administrative Patent Judge

Enc:
Copy of STANDING ORDER
Copy of claims of Application 10/658,836

cc (via overnight delivery):

Attorney for Legal iGaming:
Knobbe Martens Olson & Bear LLP
2040 Main Street
Fourteenth Floor
Irvine CA 92614

Attorney for IGT:
Weaver Austin Villeneuve & Sampson LLP - IGT
500 12th Street
Suite 200
Oakland CA 94607

BoxInterferences@uspto.gov
Tel: 571-272-4683

Paper 146
Entered: February 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT TRIAL AND APPEAL BOARD

Patent Interference No. 105,747 (RES)
(Technology Center 2400)

Zynga Inc.,
Junior Party
(Application 10/658,836;
Inventors: Rolf E. Carlson and Michael W. Saunders),

v.

IGT,
Senior Party
(Patent 7,168,089;
Inventors: Binh T. Nguyen, Michael M. Oberberger and
Gregory Hopkins Parrott).

Before: FRED E. McKELVEY, RICHARD E. SCHAFER, and
RICHARD TORCZON, *Administrative Patent Judges.*

SCHAFER, *Administrative Patent Judge.*

Judgment - Motions - 37 CFR § 41.127

We granted IGT's motion that the subject matter of Zynga's involved claims was not supported by an adequate written description. Paper 145. Because our decision deprives Zynga of an adequate basis to be involved in this interference (37 CFR § 41.201, definition of threshold issue), we enter judgment against Zynga.

Accordingly, it is:

ORDERED that Junior Party Zynga Inc. and inventors Rolf E. Carlson and Michael W. Saunders are not entitled to a patent including the subject matter of Claims 29-32, 35-43, 49, 56-58, 60-71, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167 of Application 10/658,836;

FURTHER ORDERED that Claims 29-32, 35-43, 49, 56-58, 60-71, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167 of Application 10/658,836 are finally refused (35 U.S.C. § 135(a) (2010));

FURTHER ORDERED that a copy of this judgment and the decision on motions (Paper 145) be placed in each of the administrative records of Application 10/658,836 and Patent 7,168,089; and

FURTHER ORDERED that if there is a settlement agreement, attention is directed to 35 U.S.C. § 135(c).

cc (via electronic transmittal):

IGT:

Matthew I. Kreeger, Esq.
Parisa Jorjani, Esq
Morrison & Foerster, LLP
425 Market Street
San Francisco, CA 94105-2482
Tel: (415) 268-7000
Fax: (415) 268-7522
E-mail: mkreeger@mofo.com
E-mail: pjorjani@mofo.com

Zynga:

Brenton R. Babcock, Esq.
Frederick S. Berretta, Esq.
Eric M. Nelson, Esq.
Derek Bayles, Esq.
Knobbe, Martens, Olson & Bear,
LLP
2040 Main Street, 14th Floor
Irvine, CA 92614
Tel: (949) 760-0404
Fax: (949) 760-9502
E-mail: BoxZynga@knobbe.com

BoxInterferences@uspto.gov
Tel: 571-272-4683

Paper 145
Entered: February 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT TRIAL AND APPEAL BOARD

Patent Interference No. 105,747 (RES)
(Technology Center 2400)

Zynga Inc.,
Junior Party
(Application 10/658,836;
Inventors: Rolf E. Carlson and Michael W. Saunders),

v.

IGT,
Senior Party
(Patent 7,168,089;
Inventors: Binh T. Nguyen, Michael M. Oberberger and
Gregory Hopkins Parrott).

Before: FRED E. McKELVEY, RICHARD E. SCHAFER, and RICHARD TORCZON, *Administrative Patent Judges*.

Opinion for the Board filed by SCHAFER, *Administrative Patent Judge*.

Dubitante opinion filed by TORCZON, *Administrative Patent Judge*.

Concurring opinion filed by McKELVEY, *Administrative Patent Judge*.

DECISION - MOTIONS - 37 CFR § 41.125(a)

I.

The interference is before a motions panel for consideration of non-priority motions.

There was no oral argument.

Four substantive motions are currently pending:

1. IGT Motion 2[1] (Paper 94) for a judgment that Zynga's involved claims lack sufficient written descriptive support under 35 U.S.C. § 112, ¶ 1 (2010);

2. Zynga's Substantive Motion 1 (Paper 89) to substitute a new count and designate all of the parties' currently involved claims as corresponding to the new count;

3. Zynga's contingent Motion 2 (Paper 90) for the benefit of the filing dates of Applications 09/698,507 and 60/161,591 as to the proposed new count; and

4. Zynga's Substantive Motion 3 (Paper 91) for a judgment that IGT's involved claims are unpatentable over prior art.

We grant IGT's Motion 2. Because we find that Zynga's specification does not provide written descriptive support for its involved claims, it is inappropriate and unfair to allow this interference to continue based upon the unsupported claims. We therefore terminate this interference with a judgment against Zynga and dismiss Zynga's motions as moot. See 37 CFR §41.201 (definition of threshold issue).

II.

This interference is between Zynga's Application 10/658,836 and IGT's Patent 7,168,089. The interference was declared on March 5, 2010, between Legal iGaming, Inc. and IGT. Zynga is the successor-in-interest to Legal iGaming. The interference was suspended due to Legal iGaming's bankruptcy proceeding. *In re Legal iGaming, Inc.*, Case No. 11-12771-BTB (Bankr. E.D. Nev). During the

[1] IGT Substantive Motion 1 (Paper 25), asserting no interference-in-fact between the parties' claimed subject matter, was previously denied in a panel decision. Paper 50.

bankruptcy, Legal iGaming's intellectual property rights were sold to Atwater Ventures, Ltd. which subsequently assigned its interests to Zynga.[2] The bankruptcy was terminated on April 5, 2013.

III.

The subject matter claimed relates to the authorization of electronic transfers between networked computer gaming machines or devices, particularly casino-type gaming machines. The parties employ an "authorization agent" or "gaming server" that determines whether to allow the transfer. In Zynga's claims the agent approves the transfer of "gaming information." In IGT's claims the agent approves the transfer of "gaming software." We reproduce Zynga's Claim 29 and IGT's Claim 1 below with paragraphing, bracketing, strikethrough, and emphasis added:

Zynga Claim 29

> 29. In an *authorization agent*, a method of generating a gaming transaction record used to facilitate a *transfer of gaming information* between two gaming devices, the method comprising:
>
> receiving *a gaming transaction request* from a first gaming device;
>
> authenticating an identity of the first gaming device;
>
> generating a gaming transaction record comprising gaming transaction information;
>
> and sending a message to the first gaming device wherein the message includes information authorizing the first gaming device *to transfer the gaming information* to ~~the~~ [a[3]] second gaming device wherein the first gaming device and the second gaming device are separate from the *authorization agent*,
>
> whereby the first gaming device transfers the gaming information to the second gaming device in response to the message;

[2] Legal iGaming, Atwater, and Zynga will collectively be referred to as "Zynga."

[3] As presented by Zynga, there is no antecedent in Claim 29 for "the second gaming device".

> wherein the *gaming information* is for a game of chance played on a gaming machine.

IGT Claim 1

> 1. In a *software authorization agent*, a method of generating a gaming software transaction record used to facilitate a *transfer of gaming software* between two gaming devices, the method comprising:
>
> receiving a *gaming software transaction request* from a first gaming device;
>
> authenticating an identity of the first gaming device;
>
> generating a *gaming software transaction record* comprising gaming software transaction information that is used to approve or reject the transfer of gaming software from a second gaming device to the first gaming device
>
> sending an authorization message to the first gaming device
>
> wherein the authorization message includes information indicating whether the first gaming device is *authorized to transfer the gaming software* to the second gaming device and
>
> wherein the first gaming device and the second gaming device are separate from the *software authorization agent*;
>
> wherein the gaming software is for at least one of a) a game of chance played on a gaming machine, b) a bonus game of chance played on a gaming machine, c) a device driver for a device installed on a gaming machine, d) a player tracking service on a gaming machine and e) an operating system installed on the gaming machine.

Legal iGaming's Clean Copy of Claims, Paper 14, p. 2; IGT Clean Copy of Claims, Paper 9, p. 2.

IV.

IGT Substantive Motion 2 (Paper 94) argues, inter alia, that the concept of using an "authorization agent" in Zynga's claims is not described in Zynga's specification: Paper 94, pp. 12-17.

A.

Relying on *Robertson v. Timmermans*, 603 F.3d 1309, 1312, (Fed. Cir. 2010) and *In re Spina*, 975 F.2d 854, 856 (Fed. Cir. 1992), IGT argues that because Zynga copied the claims from IGT's published application, "authorization agent" should be construed in light of IGT's specification. Paper 94, pp. 3-4.

Zynga disagrees arguing that the claims are not copies of IGT'claims. Paper 118, p. 2. For example, Zynga argues that there are several differences, including that its claims generically specify the use of an "authorizing agent" while IGT's claims specify a "software authorizing agent." We also observe that Zynga's claims require the authorization agent control the transfer of "gaming information," while IGT's claims require that the authorization agent control the transfer of "gaming software." Because of the differences, Zynga argues, the claims are not copies and cases holding that the originating disclosure provides the meaning of the pertinent claim language do not compel that its claims be interpreted in light of IGT's disclosure. Paper 118, p. 2.

IGT does not contest that there are differences between its claims and Zynga's. However, it argues that Zynga's claims are "essentially copied" and remain closer in substance to IGT's claims than to any of the Zynga's original claims. Paper 135, p. 2, ll. 3-8.

B.

A review of the prosecution history of Zynga's involved application shows that Zynga submitted claims copied from IGT's published application (U.S. Patent Application Publication 2002/0116616 (Aug. 22, 2002) (Ex. 1010). Application 10/658,836, Transmittal letter filed August 21, 2003 (Ex 2010, Board page 1209). As originally copied from IGT's published application, Zynga included claims that that were identical to claims in IGT's involved application. Application 10/658,836, Amendment filed August 21, 2003 (Ex 2010, starting at Board page 1265). Thus, Zynga's copied claims required the use of a software authorizing agent to facilitate transfer of gaming software. Those claims were amended four times before the Examiner indicated they were patentable to Zynga. See generally Application 10/658,836 amendments filed November 15, 2006 (Ex. 1012 or Ex. 2017); May 18, 2007 (Ex. 2022); January 10, 2008 (Ex. 2026); and December 12, 2008 (Ex. 2029). The amendments resulted in the deletion of all references to "software" from Zynga's claims. E.g., Application 10/658,836, amendment filed November 15, 2006 (Ex. 2017).

During the prosecution, Zynga also added a limitation that mimicked a limitation added during the prosecution IGT's application. In an amendment filed May 25, 2006 (Ex. 2033), IGT had amended some of its then-pending independent claims by adding the following limitation:

> sending an authorization message to the first gaming device wherein the authorization message includes information indicating whether the first gaming device is authorized to transfer the gaming *software* to the second gaming device and wherein the first gaming device and the second gaming device are separate from the *software* authorization agent; . . . .

Application 10/116,424, Amendment filed May 25, 2006 (Ex. 2033, Board page 1859) (emphasis added). In a subsequently filed amendment, Zynga added a limitation to some of its claims that was identically worded to IGT's amendment, except that Zynga's amendment substituted "information" for the first occurrence of "software" and deleted the second occurrence of "software." Application 10/658836, Amendment filed November 15, 2006 (Ex. 2017).

C.

While Zynga's claims, as allowed by the Examiner, clearly are not identical copies of IGT's, we think they are substantial copies. Zynga originally identically copied claims from IGT's published application and followed IGT's lead in adding limitations that tracked IGT's amendments to its application. Although Zynga's claims were amended to recite "authorization agent" and "gaming information," resulting in claims broadened in scope, the amendments did not create significant differences in the concepts and steps involved. Under these circumstances, Zynga's claims remain substantial copies of IGT's notwithstanding the different breadth of coverage.

Additionally, when this interference was declared the parties were advised:

> Pursuant to *Koninklijke Philips Electronics N.V. v. Cardiac Science Operating Co.*, 590 F.3d 1326, 1335 (Fed. Cir. 2010) and *Agilent Technologies Inc. v. Affymetrix Inc.*, 567 F.3d 1366, 1375 (Fed. Cir. 2009) and notwithstanding 37 CFR § 41.200(b),[4] for the purposes of written description support under 35 USC § 112, ¶ 1, language appearing in the applicant's claims and not supported by the same language in applicant's written description shall be construed in light of the patentees' written description.

Paper 3, p. 4.

Zynga's claim language will be interpreted in light of IGT's specification. "Because this is an interference and [the applicant] substantially copied [patentee's] claim 1, we give the claim its broadest reasonable construction in light of the . . . patent specification." *Harari v. Lee*, 656 F.3d 1331, 1340 (Fed. Cir. 2011).

D.

1.

IGT argues that "authorization agent," when interpreted in light of its specification, should be construed to mean "a device that authorizes (that is approves or rejects) **specific transfers** of **gaming software** based on the

[4] The regulation was subsequently removed by the Director. Final Rule, Cancellation of Rule of Practice 41.200(b) Before the Board of Patent Appeals and Interferences in Interference Proceedings, 75 Fed. Reg. 19558 (April 15, 2010).

applicable rules, and **monitors (that is tracks) these transfers** . . . .". Paper 94, p. 1, l. 26 – p. 2, l. 1 (bolding added). To support its position, IGT relies on portions of its specification and on the testimony of Dr. William K. Bertram, Ph.D. Paper 94, pp. 6-9.

Zynga responds that this definition is not the broadest reasonable interpretation. Paper 118, p. 4. According to Zynga:

> IGT's definition of "authorization agent" is not the broadest reasonable interpretation because it includes fully four separate limitations (in bold type above) that are, for example, internally inconsistent with the remainder of the claim language or improperly imported from the specification of [IGT's] patent.

Paper 118, p. 4, ll. 26-29.

We are persuaded that IGT's definition is too narrow, at least in construing the phrase "authorization agent" in Zynga's claims to mean "software authorization agent." To interpret the phrase in this way would effectively render superfluous the word "software" in the phrase "software authorization agent" as used in IGT's claims and written description. IGT's use of the word "software" at least implies that an "authorizing agent," when used without the modifier, does not connote an agent limited solely to authorizing software transfers. We therefore decline to limit the phrase to an agent that authorizes the transfer of gaming software.

We hold that "authorization agent" as used in Zynga's claims is not limited to a device that only authorizes transfers of gaming software. Rather, it is generic to both the transfer of gaming software and to other types of gaming information.

2.

IGT also argues that, if "authorization agent" is not limited solely to authorizing software transfers, Zynga's claims still fail to have written descriptive support. Paper 94, p. 17, ll., 13-28. IGT argues that Zynga's original specification does not provide written descriptive support for the full scope of the subject matter encompassed by "authorization agent." According to IGT, to the extent that phrase encompasses an agent for authorizing the transfer of gaming software, the authorization of such transfer is not supported by Zynga's specification. Paper 94, p. 17, ll. 13-28.

IGT directs us to *ICU Med., Inc. v. Alaris Med. Sys., Inc.*, 558 F.3d 1368, 1376-79 (Fed. Cir. 2009), and *LizardTech, Inc. v. Earth Res. Mapping, Inc.*, 424 F.3d 1336, 1345-47 (Fed. Cir. 2005). These cases hold that, under the particular facts there involved, generic subject matter added by amendment was not supported by the disclosure of a species encompassed by the later claimed generic subject matter. *ICU Med.*, 558 F.3d at 1378 (Generic claims covering both valves with and without spikes were not supported by specification that only described valves with spikes); *Lizard Tech.*, 424 F.3d at 1345 (Claim directed to a generic method creating seamless discrete wave transformation coefficients was not supported by a specification directed only to a particular method of creating those coefficients).

As support for its position, IGT correctly notes that the phrase "authorization agent" does not appear in Zynga's specification other than in its amended claims. Paper 94, p. 12, ll. 3-4. IGT also relies upon Dr. Bertram's testimony. Paper 94, p. 17, ll. 16-22. Dr. Bertram testifies that Zynga's "application does not teach a device that authorizes and monitors the transfer of gaming software . . . ." He also testifies that "one of ordinary skill would not have understood that the [Zynga] inventors invented a device that authorizes and monitors transfers of gaming software." Ex. 1016, p. 22, ll. 15-17.

Zynga responds arguing that IGT has made only the naked assertion that its claims encompass more than what is described. Citing to *LizardTech*, Zynga argues that claims do not fail to comply with § 112, first paragraph, simply because the specification does not include examples explicitly covering the full scope of the claimed subject matter. Paper 118, p. 22, ll. 13-24.

3.

A purpose of the written description requirement is to ensure that the scope of the right to exclude, as set forth in the claims, does not overreach the scope of the inventor's contribution to the field of art as described in the patent specification. *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1353-54 (Fed. Cir. 2010) (en banc). The test for the adequacy of written description support "is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Id.* at 1351. That is, the specification must "set forth enough detail to allow a person of ordinary skill in the art to understand what is claimed and to recognize that the inventor invented what is claimed." *Univ. of Rochester v. G.D. Searle & Co.*, 358 F.3d 916, 928 (Fed. Cir. 2004). The invention is, for purposes of the "written description" inquiry, whatever is now claimed." *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1563-64 (Fed. Cir. 1991). Possession means "possession as shown in the disclosure" and "requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art." *Crown Packaging Tech., Inc. v. Ball Metal Beverage Container, Corp.*, 635 F.3d 1373, 1380 (Fed. Cir. 2011); *Ariad*, 598 F.3d at 1351. However, "the exact terms need not be used in haec verba." *Id.; In re Hayes Microcomputer Prods., Inc.*, 982 F.2d 1527, 1533 (Fed. Cir. 1992) ("[the applicant] does not have to describe exactly the subject matter claimed"). Additionally, a single embodiment supports a generic claim only if the specification would "reasonably convey to a person skilled in the art that the inventor had possession of the broader claimed subject matter at the time of filing." *See Bilstad v. Wakalopulos,* 386 F.3d 1116, 1125 (Fed.Cir.2004).

4.

We have reviewed Zynga's amended specification and drawings (Ex. 2020) and do not see a disclosure of an agent that authorizes the transfer of gaming software. The discussions in Zynga's specification describing the transfer of information related to non-software information. For example, the transfers include financial information (Ex. 2020, ¶¶ 23 and 108); player initiated events (*id.*, ¶¶ 56 and 93), encryption keys and encrypted information (*id.*, ¶¶ 114-116); gaming server responses to player initiated events (*id.*, ¶¶ 90); and information allowing remote computer controlled play of a separate gaming machine (*id.*, ¶¶ 106 and 150-152).

Dr. Bertram, IGT's witness, testifies that he reviewed the specification, claims, and drawings, as well as the prosecution history, of Zynga's involved application. Ex. 1016, p. 2, ¶ 9. He testifies Zynga's specification teaches a "centralized architecture with unchanging game software residing at a central system." *Id.*, p. 21, l. 17. He further testifies that Zynga's "application does not teach a device that authorizes and monitors the transfer of gaming software . . . ." *Id.*, p. 22, ll. 15-17. He additionally testifies that "one of ordinary skill would not have understood that the [Zynga] inventors invented a device that authorizes and monitors transfers of gaming software." *Id.*

In responding to IGT's argument, Zynga does not identify a portion of its written description that would be understood by a person skilled in the art to expressly or implicitly describe an authorization agent for the transfer of gaming software or that would otherwise convey that Zynga possessed the concept of transferring gaming software between gaming machines. Paper 118, p. 22, ll. 13-24. Zynga only argues that it is not necessary to describe examples that cover the full scope of the claim language and that IGT has not provided any analysis beyond the bare assertion that Zynga's claims encompass more than what is disclosed. Paper 118, p. 22, ll. 13-24.

While it is not necessary to provide examples covering the full scope of the claim language, it is necessary to provide sufficient information to convey to one skilled in the art that the inventors had possession of the claimed subject matter at the time they filed their application. *Ariad*, 598 F.3d at 1351. Contrary to Zynga's argument, IGT does not rely solely on an assertion that Zynga's claims "encompass more than what is disclosed." IGT relies on Dr. Bertrams's testimony that Zynga's application does not teach a device that authorizes the transfer of gaming software and that one having ordinary skill in the art would not have understood from Zynga's specification that the inventors contemplated a device that authorizes the transfer of gaming software. Paper 94, p. 17, ll. 13-28 referring to Ex 1016, ¶ 77. We find that Dr. Bertram's testimony is credible and stands unrebutted.

Zynga's Claims 166 and 167 do not use the phrase "authorization agent." Instead they are directed to a system that employs a "gaming server." The gaming server, however, performs the same functions as the authorization agent. Thus, the gaming server is configured to authenticate a request for gaming information from a remote computer for transferring information from the gaming machine, generating a gaming record authorizing the transfer of gaming information from the gaming machine to the remote computer, and sending a message including the authorization to the remote computer. Compare Zynga's Claims 29 and 166, Paper 14, pp. 2 and 10. We perceive no substantive distinction between the recitations of a "authorization agent" and "gaming server" as used in Zynga's claims with respect to the written descriptive support for authorization of the transfer gaming software.

Zynga points to the testimony of Charles R. Berg and a portion of its specification related to the exchange of encryption keys for support for the concept of authorizing and transferring "gaming information." Paper 118, p. 24, ll. 11-18; Ex. 2020, ¶ 149; Ex. 2035, ¶¶ 125-128. Accepting for the purposes of this opinion that the evidence provides an example of the authorization and transfer of "gaming information," that evidence does not show possession of the concept of authorizing the transfer of gaming software between gaming machines. Zynga has not directed us to testimony or other evidence establishing that one skilled in the art would understand Zynga's specification as showing possession of the concept of a device that authorizes the transfer of gaming software. We are aware of Mr. Berg's testimony that one skilled in the art would understand "gaming information" to encompass "gaming software:"

> As discussed further herein, a person having ordinary skill in the art would understand "gaming information" to include "any information associated with game play or a gaming device."... In contrast, a person having ordinary skill in the art would understand "gaming software" to have the narrower definition of "one or more software components which may be executed on a gaming device or machine." ... Because "gaming software" is "associated with game play" in that it includes computer instructions for carrying out game play, a person having ordinary skill in the art would understand "gaming software" as a specific type of "gaming information." In other words, a person having ordinary skill in the art would understand "gaming software" as a species of the "gaming information" genus. This position is further supported by the fact that the specification of the Nguyen '089 patent explicitly and repeatedly states that "gaming software" is included within the scope of the meaning of the term "gaming information." For example, the Nguyen '089 patent repeatedly refers to "gaming software and other gaming information." (Ex. 1001 at 27:4-5; 27:31-32).

Ex. 2015, ¶ 11. We have been given no credible reason to disagree with the accuracy of his testimony on the understanding of one skilled in the art with respect to the meaning of "gaming information." However, that phrase and the generic concept of "gaming information" as encompassing "gaming software" was not introduced into the Zynga's application until the amendment filed November 15, 2006, more than three years after Zynga's involved application was filed. While Zynga's written description describes the transfer of a number of different types of "gaming information" we could not locate, and Zynga has not identified, the portions of its written description that would convey possession of the concept of authorizing the transfer of gaming software between gaming devices. Dr. Bertram's testimony, that one skilled in the art would not have understood, from Zynga's specification, that the inventors contemplated a device that authorizes the transfer of gaming software stands unrebutted. Zynga's use of the phrase "gaming information" to encompass "gaming software" goes beyond the scope of its original disclosure. "[A] purpose of the written description requirement is to 'ensure that the scope of the right to exclude, as set forth in the claims, does not overreach the scope of the inventor's contribution to the field of art as described in the patent specification.'" *Ariad*, 598 F.3d at 1353-54.

A preponderance of the evidence establishes, and we find, that at the time Zynga filed its involved application, one skilled in the art would not have understood from Zynga's specification, that Zynga had possession of the concept of an authorization agent or gaming server that controls the transfer of gaming software between gaming devices.

IGT has persuaded us that Zynga's disclosure does not provide a written description supporting the full scope of the subject matter of its involved claims. Accordingly, we grant IGT's motion that Zynga's Claims 29-32, 35-43, 49, 56-58, 60-71, 93, 94, 96, 100, 101, 103-106, 112, 113, 115, 117, 119-124, 131, 136, 144, 145, 151, 152, 155, 157, 161, and 165-167 are unpatentable under 35 U.S.C. § 112, ¶ 1 (2010).

V.

We have granted IGT's motion that Zynga's written description does not support the subject matter it now claims. See 37 CFR § 41.125(a). Under the circumstances of this interference, it is appropriate to terminate the interference with a judgment against Zynga. Zynga originally copied IGT's claimed subject matter. As a result, this interference was declared and IGT's patented subject matter was brought into this interference and put at risk. Because Zynga's original specification does not provide written descriptive support for the full scope of the subject matter of its involved claims, Zynga is not an appropriate party, and this interference is not an appropriate forum, to challenge IGT's patent. See 37 CFR § 41.201, definition of "threshold issue." Therefore, we will not consider Zynga's attacks on IGT's claims. We decline to consider Zynga's Substantive Motion 3 asserting IGT's claims are unpatentable over prior art. We similarly will not allow this interference to proceed to the priority phase subjecting IGT's claims to be challenged on priority grounds. Because this interference will not proceed to the priority phase, it is unnecessary to consider Zynga's Substantive Motion 1 to substitute a different count[5] or it's Substantive Motion 2 for the benefit of the filing dates of its earlier applications. Zynga's Substantive Motions 1-3 are dismissed.

ORDER

1. IGT Motion 2 (Paper 94) asserting that Zynga's claims are not supported by the written description required by 35 U.S.C. § 112, ¶ 1, is granted.

2. Zynga's Substantive Motions 1-3 (Papers 89-91) are dismissed.

[5] Granting the motion to substitute a different count would not have resulted in a change in the parties' respective claim correspondence. Paper 89, p. 1.

TORCZON, *Administrative Patent Judge*, dubitante.

This case underscores the peril in claim copying.

For more than a generation, claim copying has not been necessary to suggest an interference. *E.g.*, *Aelony v. Arni*, 547 F.2d 566, 570 (CCPA 1977) (claimed subject matter need not even overlap). Nevertheless, patent practitioners persist in copying claims. Claim copying is a nuisance (inevitably leading to a mismatch between the language of the claim and the disclosure with resulting confusion or otherwise unneeded analysis), but it once was essentially harmless.

Now claim copying is destructive to applicants and their counsel. Although neither statute nor interference practice provide a basis for it, case law has created an exception in written description law for copied claims, albeit only at the United States Patent and Trademark Office. *In re Spina*, 975 F.2d 854, 856 (Fed. Cir. 1992); *Agilent Techs., Inc. v. Affymetrix, Inc.*, 567 F.3d 1366 (Fed. Cir. 2009); *Koninklijke Philips Elecs. N.V. v. Cardiac Sci. Operating Co.*, 590 F.3d 1326, 1332 (Fed. Cir. 2010); *but see Cultor Corp. v. A.E. Staley Mfg. Co.*, 224 F.3d 1328, 1332 (Fed. Cir. 2000) (declining to extend *Spina* to the district courts).

Whether a doctrine unsupported by statute or logic, messy to administer and catastrophic to unwary applicants and patent practitioners should persist[6] is a question only the courts can resolve.

Resolution is needed. Until it happens, "caveat inventor".

1

[6] For a catalogue of some of the difficulties the doctrine has created, *see, e.g.*, *Lazaridis v. Eggleston*, 2011 WL 1676301 (BPAI 2011) (dubitante opinion); *Rilo v. Benedict*, 2011 WL 729494 n.55 (BPAI 2011).

McKELVEY, *Administrative Patent Judge*, concurring.

I concur with the decision on IGT Motion 2 for the reasons set out in Judge Schafer's opinion. I add the following comments to further address thoughtful remarks made by Judge Torczon's dubitante opinion.

In deciding cases on the merits, it is our practice to apply the applicable statute, rules, and precedent. *Eberhart v. U.S.*, 546 U.S. 12 (2005). Consistent with our practice, Judge Schafer advised the parties are follows (footnote omitted):

> Pursuant to *Koninklijke Philips Electronics N.V. v. Cardiac Science Operating Co.*, 590 F.3d 1326, 1335 (Fed. Cir. 2010) and *Agilent Technologies Inc. v. Affymetrix Inc.*, 567 F.3d 1366, 1375 (Fed. Cir. 2009) and notwithstanding 37 CFR § 41.200(b), for the purposes of written description support under 35 USC § 112, ¶ 1, language appearing in the applicant's claims and not supported by the same language in applicant's written description shall be construed in light of the patentees' written description.

In deciding IGT Motion 2, we have relied upon and hopefully properly applied the Federal Circuit's binding precedent in *Agilent* and its progeny.

Like suggestions made by the Seventh Circuit in *Eberhart* and by Judge Theis in *Long v. Citizen's Bank & Trust Co. of Manhattan, Kansas*, 563 F. Supp. 1203, 1211 (D. Kan. 1983), the following observations are respectfully noted.

Agilent did not change, or involve, the long-standing "rule" that if a count (not a claim) has ambiguous language, the language is construed in light of the application or patent where it originated. 1 Rivise & Caesar, INTERFERENCE LAW AND PRACTICE, § 56 (1940) ("If the language of a count is ambiguous or susceptible of more than one meaning, the count will, if at all possible, be interpreted in light of the application or patent in which it originated."). Interpretation of the count would have been necessary to determine if priority proofs fall within the scope of the count.

As Judge Torczon notes, despite PTO observations that copying of claims is not necessary, applicants continue to "copy" claims from patents. The better approach is for an applicant to (1) present a claim which complies with the written description in the descriptive portion of a specification, (2) establish to the satisfaction of the examiner that there is an interference-in-fact and (3) ask the examiner to recommend an interference.

If an interference is declared based on a "copied" claim, the patentee will insist consistent with *Agilent* that that the copied claim be construed in light of the patent as to any authorized motion for judgment based on lack of written description. If there is a motion for judgment based on unpatentability over the prior art, the claim will be construed in light of the application—not the patent. Hence, depending on the motion *Agilent* authorizes different claim constructions of the same claim.

To be sure, *Agilent* might not apply when a copied claim is a means-plus-function claims. Why? Because, § 112 explicitly provides how means-plus-function claims are to be construed. The statute would trump *Agilent*. However, as to non-means-plus-function claims, *Agilent* is applicable precedent. Accordingly, depending on the nature of the claim, *Agilent* may or may not apply.

Respectfully, it is suggested that the *Agilent* rule is not necessary to resolve issues arising interference cases in resolution of the principal issue of priority. An interference is a contest for the right to a patent as to a commonly claimed patentable invention where the claims do not have to overlap in scope. *Aelony v. Arni*, 547 F.2d 566 (CCPA 1977).[7]

[7] Actually, an interference is about defeating the opponent's right to patent because prevailing in an interference does not mean the winning party is awarded a patent. *Krasnow v. Bender*, 170 F.2d 560, 564 (CCPA 1948). *See* 35 U.S.C.

If an interference is declared, an applicant's claim can be reviewed for compliance with written description by patentee seeking authorization to file a motion for judgment based on applicant's lack of a written description. The motion can be resolved by determining whether the applicant's specification provides the necessary support avoiding the awkward need to construe the applicant's claim in light of someone else's specification. *Cf. U.S v. Adams*, 383 U.S. 39, 49 (1966) (claims are to be construed in light of the specification and both the specification and claims are to be read with a view to ascertaining the invention); *Am. Fruit Growers v. Brogdex Co.*, 283 U.S. 1, 5 (1931) (claim of a patent must always be explained by and read in connection with specification).

Contingent on it being determined that the applicant complies with the written description requirement, the patentee can seek authorization to file a contingent motion for judgment based on no interference-in-fact alleging that its claimed invention does not interfere with applicant's claimed invention. If construction of the parties' claims reveals there is no interference-in-fact, then the need for an interference no longer exits.

These two motions provide the tools necessary to determine whether an applicant has support and whether there is an interference-in-fact without any need to interpret an applicant's claim in light of a patent involved in the interference.

I agree Judge Torczon's observation that the Agilent rule is "messy to administer". I also agree that at this stage any change in the *Agilent* rule is a matter only the courts can resolve.

In the meantime, our role is to apply faithfully the applicable precedent.

§ 135(a) mentioning cancellation of patent claims and final refusal of an applicant's claim.

cc (via electronic transmittal):

IGT:

Matthew I. Kreeger, Esq.
Parisa Jorjani, Esq
Morrison & Foerster, LLP
425 Market Street
San Francisco, CA 94105-2482
Tel: (415) 268-7000
Fax: (415) 268-7522
E-mail: mkreeger@mofo.com
E-mail: pjorjani@mofo.com

Zynga:

Brenton R. Babcock, Esq.
Frederick S. Berretta, Esq.
Eric M. Nelson, Esq.
Derek Bayles, Esq.
Knobbe, Martens, Olson & Bear, LLP
2040 Main Street, 14th Floor
Irvine, CA 92614
Tel: (949) 760-0404
Fax: (949) 760-9502
E-mail: BoxZynga@knobbe.com

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE** **FILING OR DETERMINATION OF AN** **ACTION REGARDING A PATENT OR** **TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:21-cv-331	DATE FILED 4/6/2021	U.S. DISTRICT COURT Western District of Texas

PLAINTIFF IGT and IGT Canada Solutions ULC	DEFENDANT Zynga Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 See Attachment 1		
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Attachment 1 to Form AO 120

IGT & IGT Canada Sols. ULC v. Zynga Inc. (W.D. Tex.)

Patent or Trademark No.	Date of Patent or Trademark	Holder of Patent or Trademark
8,708,791	Apr. 29, 2014	IGT
9,159,189	Oct. 13, 2015	IGT Canada Solutions ULC
7,168,089	Jan. 23, 2007	IGT
7,303,473	Dec. 4, 2007	IGT
8,795,064	Aug. 5, 2014	IGT
8,266,212	Sept. 11, 2012	IGT