

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	UN-NP-SC-085
		Application Number	
Title of Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

**Secrecy Order 37 CFR 5.2**

<input type="checkbox"/>	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2. (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	--

**Inventor Information:**

<b>Inventor 1</b>					<input type="button" value="Remove"/>
<b>Legal Name</b>					
<b>Prefix</b>	<b>Given Name</b>	<b>Middle Name</b>	<b>Family Name</b>	<b>Suffix</b>	
	Craig	S.	ETCHEGOYEN		
<b>Residence Information (Select One)</b> <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					
<b>City</b>	Newport Beach	<b>State/Province</b>	CA	<b>Country of Residence</b>	US
<b>Mailing Address of Inventor:</b>					
<b>Address 1</b>	7160 N. Dallas Parkway				
<b>Address 2</b>	Suite 380				
<b>City</b>	Plano	<b>State/Province</b>	TX		
<b>Postal Code</b>	75024	<b>Country</b>	US		
<b>Inventor 2</b>					<input type="button" value="Remove"/>
<b>Legal Name</b>					
<b>Prefix</b>	<b>Given Name</b>	<b>Middle Name</b>	<b>Family Name</b>	<b>Suffix</b>	
	Dono		HARJANTO		
<b>Residence Information (Select One)</b> <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					
<b>City</b>	Irvine	<b>State/Province</b>	CA	<b>Country of Residence</b>	US
<b>Mailing Address of Inventor:</b>					
<b>Address 1</b>	7160 N. Dallas Parkway				
<b>Address 2</b>	Suite 380				
<b>City</b>	Plano	<b>State/Province</b>	TX		
<b>Postal Code</b>	75024	<b>Country</b>	US		
<b>Inventor 3</b>					<input type="button" value="Remove"/>
<b>Legal Name</b>					
<b>Prefix</b>	<b>Given Name</b>	<b>Middle Name</b>	<b>Family Name</b>	<b>Suffix</b>	
	Sean	D.	BURDICK		
<b>Residence Information (Select One)</b> <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	UN-NP-SC-085		
		Application Number			
Title of Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES				
City	Dallas	State/Province	TX	Country of Residence i	US
<b>Mailing Address of Inventor:</b>					
Address 1	7160 N. Dallas Parkway				
Address 2	Suite 380				
City	Plano	State/Province	TX		
Postal Code	75024	Country i	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the <b>Add</b> button.					<input type="button" value="Add"/>

**Correspondence Information:**

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
<input type="checkbox"/> An Address is being provided for the correspondence information of this application.	
Customer Number	96051
Email Address	<input type="button" value="Add Email"/> <input type="button" value="Remove Email"/>

**Application Information:**

Title of the Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES				
Attorney Docket Number	UN-NP-SC-085	Small Entity Status Claimed	<input checked="" type="checkbox"/>		
Application Type	Nonprovisional				
Subject Matter	Utility				
Suggested Class (if any)		Sub Class (if any)			
Suggested Technology Center (if any)					
Total Number of Drawing Sheets (if any)	9	Suggested Figure for Publication (if any)	6		

**Publication Information:**

<input type="checkbox"/> Request Early Publication (Fee required at time of Request 37 CFR 1.219)
<input type="checkbox"/> <b>Request Not to Publish.</b> I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application <b>has not and will not</b> be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

**Representative Information:**

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.
--

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	UN-NP-SC-085
		Application Number	
Title of Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	96051		

**Domestic Benefit/National Stage Information:**

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.			
Prior Application Status	Pending	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61595599	2012-02-06
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the <b>Add</b> button.			<input type="button" value="Add"/>

**Foreign Priority Information:**

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			<input type="button" value="Remove"/>
Application Number	Country <sup>i</sup>	Filing Date (YYYY-MM-DD)	Priority Claimed
2012100462	AU	2012-04-24	<input checked="" type="radio"/> Yes <input type="radio"/> No
Additional Foreign Priority Data may be generated within this form by selecting the <b>Add</b> button.			<input type="button" value="Add"/>

**Authorization to Permit Access:**

<input checked="" type="checkbox"/> Authorization to Permit Access to the Instant Application by the Participating Offices
--

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	UN-NP-SC-085
		Application Number	
Title of Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

## Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
<b>Applicant 1</b>			<input type="button" value="Remove"/>
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.			
<input type="button" value="Clear"/>			
<input checked="" type="radio"/> Assignee	<input type="radio"/> Legal Representative under 35 U.S.C. 117	<input type="radio"/> Joint Inventor	
<input type="radio"/> Person to whom the inventor is obligated to assign.		<input type="radio"/> Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor : <input type="text"/>			
If the Applicant is an Organization check here. <input checked="" type="checkbox"/>			
Organization Name	UNILOC LUXEMBOURG S.A.		
<b>Mailing Address Information:</b>			
Address 1	15, Rue Edward Steichen		
Address 2			
City	Luxembourg	State/Province	
Country <sup>i</sup>	LU	Postal Code	L-2450
Phone Number		Fax Number	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	UN-NP-SC-085
		Application Number	
Title of Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

**Non-Applicant Assignee Information:**

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

<b>Assignee 1</b>			
Complete this section only if non-applicant assignee information is desired to be included on the patent application publication in accordance with 37 CFR 1.215(b). Do not include in this section an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest), as the patent application publication will include the name of the applicant(s).			
			<input type="button" value="Remove"/>
If the Assignee is an Organization check here. <input checked="" type="checkbox"/>			
Organization Name	Uniloc Luxembourg S. A.		
<b>Mailing Address Information:</b>			
Address 1	15, Rue Edward Steichen		
Address 2			
City	Luxembourg	State/Province	
Country i	LU	Postal Code	
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

**Signature:**

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Sean D. Burdick/		Date (YYYY-MM-DD)	2013-01-04	
First Name	Sean	Last Name	Burdick	Registration Number	51513
Additional Signature may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	UN-NP-SC-085
		Application Number	
Title of Invention	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

# **NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES**

## **BACKGROUND OF THE INVENTION**

[0001] This application claims priority to U.S. Provisional Application No. 61/595,599, which was filed February 6, 2012, and which is fully incorporated herein by reference.

### **1. Field of the Invention**

[0002] The present invention relates generally to technology for near field authentication of users and their computing devices. More specifically, the invention relates to effecting near field authentication for digital communications by means of encoded sound waves.

### **2. Description of the Related Art**

[0003] The use of a user's electronic device to complete a purchase has been suggested, for example, utilizing Bluetooth technology or a WiFi Internet connection to transmit the data to the register. However, such technology requires a transactional device such as a register or ATM machine to be upgraded and retrofitted with expensive equipment and software to securely receive the data and authenticate the user's electronic device. Thus, while it may be desirable for the user, it could be prohibitively expensive for the commercial entity utilizing the transactional device, especially for small businesses.

[0004] The use of other technology aside from the Internet or the Bluetooth may also require not only that the transactional device be upgraded and retrofitted, but also that the user's electronic device be similarly modified. In addition, alternative technology may also have range limitations which can degrade the user's experience when performing a transaction. For



example, in a conventional near field communication, radio communication is utilized to facilitate transactions. However, the conventional near field communication requires that the two transacting devices be in extremely close proximity to each other, i.e., within about 4 centimeters from each other to ensure reliable communication. This requirement for close proximity places a very restrictive limitation on practical applications for near field transactions in the real world. If one of the transacting devices is a cash register, and the other transacting device is a customer's mobile phone, the customer would need to extend the phone to within centimeters of the register and risk dropping the phone. The proximity limitation may also prevent the user from making further use of the phone while the transaction is taking place and while the phone is extended away from the customer. For example, should complications in the transaction arise, or if the user is required to provide a manual input, the customer may not be able to complete the transaction.

[0005] Another drawback of the conventional near field communication is the lack of security, despite the close proximity of the two devices. That is, the conventional near field communication offers no protection against eavesdropping and can be vulnerable to data modifications. Needless to say, this is undesirable for financial transactions and other confidential communications.

[0006] Thus, there is a need for improved technology for effecting near field communications.

#### SUMMARY OF THE INVENTION

[0007] The present invention provides a method for source authentication in network communications. A source such as a mobile computing device transmits an authentication request by executing the following salient steps using an audio transceiver: scanning a plurality

of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, encoding a carrier wave with the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. The audio transceiver, in one example, may be a mobile phone having both a speaker and a microphone.

[0008] The periodic enclosed content message includes an enclosed content message at each period. The enclosed content message comprises a beginning indication, a content, and an ending indication. The beginning indication indicates when the enclosed content message begins, while the ending indication indicates when the enclosed content ends. This allows for verification that the enclosed content message is completely instead of partially received. Furthermore, the content can include biometric data or device identification data, or both, which can be used to authenticate the user or the mobile computing device. Furthermore, the content may also include financial information for the user, or other data which might be used for gaining access to a secure network for facilitating a transaction once the user or the mobile computing device, or both, have been authenticated.

[0009] In another embodiment, the present invention includes a computer readable medium useful in association with an audio transceiving computing device that includes one or more processors and a memory, the computer readable medium including instructions configured to cause the audio transceiving computing device, by execution of the instructions in the one or more processors from the memory, to request authentication by executing the salient steps.

[0010] In another embodiment, the present invention includes a mobile computer system including at least one processor, a computer readable medium that is operatively coupled to the

processor, and a transmission logic that (i) executes in the processor from the computer readable medium and (ii) when executed by the processor causes the mobile computer system to request authentication by executing the salient steps.

[0011] The invention also provides a method for receiving an authentication request using an audio or microphone input of a receiving computing device by executing the following second set of salient steps: scanning a plurality of predetermined frequencies to detect a signal using the microphone input, verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message, and extracting a content from the enclosed content message.

[0012] Another embodiment of the invention comprises a computer readable medium useful in association with an audio receiving computing device that includes one or more processors, an audio or microphone input, and a memory, the computer readable medium including computer instructions which are configured to cause the audio receiving computing device, by execution of the computer instructions in the one or more processors from the memory, to receive an authentication request by execution of the second set of salient steps.

[0013] In another embodiment, a present invention is a computer system including at least one processor, an audio input that is operatively coupled to the processor, a computer readable medium that is operatively coupled to the processor, and a near field authentication receiver logic that (i) executes in the processor from the computer readable medium and (ii) when executed by the processor causes the computer system to receive an authentication request via the audio input by execution of the second set of salient steps.

[0014] In an embodiment, the near field authentication of sources using audio waves can be used in conjunction with a conventional online transaction to provide enhanced security for

transactions, such as payments and electronic or personal access to confidential files or secure locations.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims. Component parts shown in the drawings are not necessarily to scale, and may be exaggerated to better illustrate the important features of the invention. In the drawings, like reference numerals may designate like parts throughout the different views, wherein:

[0016] FIG. 1 is a block diagram showing an audio transceiving computing device transmitting data to an audio receiving computing device in accordance with one embodiment of the present invention.

[0017] FIG. 2 is a block diagram showing functional components that make up an audio transceiving computing device according to an embodiment of the present invention.

[0018] FIG. 3 depicts a periodic enclosed content message according to an embodiment of the present invention.

[0019] FIG. 4 is a block diagram depicting message content in an enclosed content message according to an embodiment of the present invention.

[0020] FIG. 5 is a block diagram showing functional components of an audio receiving computing device according to an embodiment of the present invention.

[0021] FIG. 6 is a process flow diagram showing steps for an audio transceiving computing device to request authentication from an audio receiving computing device according to an embodiment of the present invention.

[0022] FIG. 7 depicts additional process steps for inputting content for an enclosed content message into an audio transceiving computing device in advance of requesting authentication according to an embodiment of the present invention.

[0023] FIG. 8 is a process flow diagram showing steps for receiving an audio transmission of enclosed content data using a microphone input of a receiving computing device according to an embodiment of the present invention.

[0024] FIG. 9 depicts additional process steps for authenticating an audio transceiving device according to an embodiment of the present invention.

#### DETAILED DESCRIPTION

[0025] The present invention relates to a method and system for near field authentication of users and computing devices using sound waves. Such users and computing devices may be referred to collectively herein as “sources”. Authenticating a source according to the present invention may involve authenticating only a user, only a computing device, or both a user and a computing device.

[0026] As seen in FIG. 1, a system 100 for authenticating sources using sounds waves can

include, for example, an audio transceiving computing device 102, and an audio receiving computing device 104. The audio transceiving computing device 102 can transmit data to the audio receiving computing device 104 as a modulated carrier wave 106. The modulated carrier wave 106 can be, for example, a sound wave. Sound waves can transmit information accurately over a very short distance (near field communications) using inexpensive equipment. In different embodiments, the sound wave can have a frequency that is substantially below, within, or above the audible frequencies, such as below 20 Hz, between 20 Hz and 20 kHz, or above 20 kHz. For example, the sound wave could be an ultrasonic wave.

[0027] The audio transceiver computing device 102 can be, for example, a mobile phone, a personal digital assistant, a tablet, a laptop, a music player, or any other device having a processor operatively coupled to memory and capable of transmitting the modulated carrier wave 106 responsive to operation of the processor. As seen in FIG. 2, the audio transceiver computing device 102 can include, for example one or more microprocessors, which are collectively shown as CPU 202. The audio transceiver computing device 102 also includes, for example, a memory 204, an interconnect 206, an input 208, an output 210, and/or a network access circuitry 212. The CPU 202 can retrieve data and/or instructions from the memory 204 and execute the retrieved instructions. The memory 204 can include generally any computer-readable medium including, for example, persistent memory such as magnetic and/or optical disks, ROM, and PROM and volatile memory such as RAM.

[0028] The CPU 202 and the memory 204 are connected to one another through the interconnect 206, which is a bus in this illustrative embodiment. The interconnect 206 connects the CPU 202 and the memory 204 to the input devices 208, the output devices 210, and the network access circuitry 212. The input devices 208 can include, for example, a keyboard, a

keypad, a touch-sensitive screen, a mouse, a microphone, and/or one or more cameras. The output devices 210 can include, for example, a display – such as a liquid crystal display (LCD) – and/or one or more speakers. The network access circuitry 212 sends and receives data through computer networks such as an intranet or the Internet.

[0029] A number of components of the audio transceiver computing device 102 are stored in the memory 204. In particular, a near field authentication transceiver logic 214 is part of one or more computer processes executed within the CPU 202 from the memory 204 in this illustrative embodiment, but can also be implemented using digital logic circuitry. As used herein, “logic” refers to (i) logic implemented as computer instructions and/or data within one or more computer processes and/or (ii) logic implemented in electronic circuitry.

[0030] In an embodiment, the near field authentication transceiver logic 214 is executable software stored within the memory 204. For example, when the audio transmitting computing device 102 receives a request from the user to transmit the modulated carrier wave 106, the audio transceiver computing device 102 executes the near field authentication transceiver logic 214 to transmit the modulated carrier wave 106 to the audio receiving computing device 104. As previously noted the modulate carrier wave 106 can be an analog signal, such as a sound signal. Advantageously, an analog signal has an infinite amount of signal resolution. Furthermore, the use of sound signals increases the permissible transmission distance. That is, the theoretical and practical working distance for completing a transaction using the present invention is increased and can be measured, for example, in feet or meters instead of centimeters. This allows the user to utilize the audio transceiver computing device 102 for additional functions simultaneously while completing a transaction. It also reduces a likelihood that the user will be prone to dropping or otherwise damaging the audio transceiver computing device 102 by moving the

audio transceiver computing device 102 into very close proximity with the audio receiving computing device 104.

[0031] When the near field authentication transceiver logic 214 is executed, the audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. The predetermined frequencies can be, for example, frequencies for which the audio transceiver computing device 102 is authorized to transmit the modulated carrier wave or which are known to the audio receiving computing device 104. In an embodiment, the predetermined frequencies can be selected to be outside the audible frequencies. From the predetermined frequencies, the near field authentication transceiver logic 214 can select a free frequency. The free frequency can be, for example, a frequency which has a noise level below a predetermined noise level threshold or a frequency that has an interference level below a predetermined interference level threshold.

[0032] The near field authentication transceiver logic 214 can also generate a periodic enclosed content message 216 as shown in FIG. 2. To generate the periodic enclosed content message 216, the near field authentication transceiver logic 214 can utilize a device ID generation logic 218 or a biometric data input logic 220, or both. The device ID generation logic 218 can generate, for example, device identification data of the audio transceiver computing device 102. In an embodiment, the device ID generation logic 218 can utilize known techniques for generating a device fingerprint. The biometric data input logic 220 can display, for example, a user interface for requesting and receiving a voice or image input representing biometric data. The device identification data or the biometric data, or both, can be included in a content of the periodic enclosed content message 216, which will be described later.



[0033] The near field authentication transceiver logic 214 can also generate a modulated carrier wave 106 representing the periodic enclosed content message. The modulated carrier wave 106 can be transmitted at the free frequency to the audio receiving computing device 104. Preferably, the periodic enclosed content message is generated initially in digital format, and is then converted into an analog signal and used to modulate the carrier wave. In an embodiment, the digital form of the periodic enclosed content message 216 can be encrypted using standard RSA (PKI) keys. Key exchanges may occur out-of-band, such as during registration of the audio transceiver computing device 102, or may be built-in to the near field authentication transceiver logic 214.

[0034] As can be seen in FIG. 3, the periodic enclosed content message 216 includes, for example, multiple periods with each period including an enclosed content message 302. Thus, the periodic enclosed content message 216 includes a plurality of enclosed content messages 302 such as enclosed content messages 302a – 302n for a total of N enclosed content messages. Each of the enclosed content messages includes a begin indication 304, a content 306, and an end indication 308. The begin indication 304 can be any type of signal that uniquely indicates the beginning of the enclosed content message, for example, a specified sequence of binary bits. Similarly, the end indication 308 can be any type of signal that indicates the ending of the enclosed content message. In one embodiment, the begin indication 304 and the end indication 308 comprise different signals. In another embodiment, the begin indication 304 and the end indication 308 comprise identical signals, i.e. two of the same signals in sequence. In another embodiment, an end indication 308(n-1) and the next begin indication 304(n) may be one and the same signal.

[0035] Referring to FIG. 4, the content 306 can include, for example, biometric data 402 or a

device identification data 404 or a combination of both. The biometric data 402 can include, for example, the data corresponding to a voice of a user, a fingerprint of the user, an image of the user, or any other physiological data of the user which can be used to verify an identity of the user. The device identification data 404 can include, for example, a MAC address of the audio transceiver computing device 102, a hard disk serial number of the audio transceiver computing device 102, a device ID number of the audio transceiver computing device 102, a device phone number of the audio transceiver computing device 102, a device fingerprint of the audio transceiver computing device 102, or any other information which could be used to identify and verify the authenticity of the audio transceiver computing device 102.

[0036] A device fingerprint comprises binary data that identifies the audio transceiver computing device 102 by deriving a unique data string from multiple portions of indicia stored in memory locations within the device, where such indicia can include, for example, data representing a manufacture name, a model name, or a device type. Device fingerprints and generation thereof are known and are described, e.g., in U.S. Patent 5,490,216 (sometimes referred to herein as the '216 Patent), and in related U.S. Patent Application Publications 2007/0143073, 2007/0126550, 2011/0093920, and 2011/0093701 (the “related applications”), the descriptions of which are fully incorporated herein by reference.

[0037] In general, the device fingerprint comprises a bit string or bit array that includes or is derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device 102. Non-user-configurable data includes data such as hardware component model numbers, serial numbers, and version numbers, and hardware component parameters such as processor speed, voltage, current, signaling, and clock specifications. User-configurable data includes data such as registry entries, application usage data, file list information, and MAC

address. In an embodiment, the audio transceiver computing device 102 can also include, for example, manufacture name, model name, and/or device type of the audio transceiver computing device 102.

[0038] Generation of the device fingerprint includes a combination of operations on the data specific to the audio transceiver computing device 102, which may include processing using a combination of sampling, concatenating, appending (for example, with a nonce value or a random number), obfuscating, hashing, encryption, and/or randomization algorithms to achieve a desired degree of uniqueness. For example, the desired degree of uniqueness may be set to a practical level such as 99.999999% or higher, to achieve a probability of less than 1 in 100,000,000 that any two of the audio transceiver computing devices will generate identical fingerprints. In an embodiment, the desired degree of uniqueness may be such that the device fingerprint generated is unlike any other device fingerprint generatable responsive to a request to transmit the modulated carrier wave 106 to the audio receiving computing device 104.

[0039] In one embodiment, the device fingerprint may be stored in volatile memory and erased after transmission of the modulated carrier wave 106 to the audio receiving computing device 104. In another embodiment, the device fingerprint may be stored in persistent memory and written over each time a new fingerprint is generated by the device ID generation logic 218.

[0040] Referring back to FIG. 3, the amount of time it takes to transmit the modulated carrier wave 106 representing the periodic enclosed content message,  $T_{PECM}$ , can be a sum of the time it takes to transmit a modulated carrier wave representing each of the enclosed content messages 302 in the periodic enclosed content message 216. For example, the time it takes to transmit each of the modulated carrier waves representing an enclosed content message 302 can be  $T_{ECM}$ .

Thus, the amount of time it takes to transmit the modulated carrier wave 106  $T_{PECM}$  can be, for example, represented by the equation  $T_{PECM} = N \times T_{ECM}$  where N represents the total number of enclosed content messages 302 in the periodic enclosed content message 216.

[0041] The total number N of enclosed content messages 302 in the periodic enclosed content messages 216 can be a function of the total number of frequencies in the plurality of predetermined frequencies. That is, the total number N of enclosed content messages 302 should be sufficient such that the audio receiving computing device 104 can scan through the predetermined frequencies to determine the free frequency on which the modulated carrier wave 106 is transmitted, and have time enough to receive at least one of the enclosed content messages 302. This will be discussed in more detail below. In an embodiment, the near field authentication transceiver logic 214 can transmit the modulated carrier wave 106 for a predetermined number of periods, or a predetermined period of time. In another embodiment, the near field authentication transceiver logic 214 can transmit the modulated carrier wave 106 until a stop indication is received from the user. Such indication can come, for example, from the input 208 in the form of a button depression, a tap on a screen, a vocal indication, or any other type of indication from the user to stop transmission of the modulated carrier wave 106.

[0042] In an embodiment, the near field authentication transceiver logic 214 using the biometric data input logic 220 can display a user interface on the output 210 when the output 210 is, for example, a display screen. The user interface can request the biometric data 402 from the user. For example, the user interface can prompt the user for voice input to be newly received by the biometric data input logic 220 and subsequently the near field authentication transceiver logic 214 through a microphone input on the audio transceiver computing device 102. A characteristic voice print in digital form may be derived from the voice input using technology

known in the art. In another example, the user interface can prompt the user for photographic input, such as the user's face or biometric fingerprint using a camera or scanning device on the audio transceiving computing device 102. A digital representation of the facial image or biometric fingerprint may be derived using technology known in the art. Responsive to receiving the biometric data 402, the near field authentication transceiver logic 214 can generate the periodic enclosed content message 216, wherein the content 306 in each period of the periodic enclosed content message 216 includes the biometric data (or a derivation thereof) 402.

[0043] Referring to FIGS. 1 and 5, the audio receiving computing device 104 can be, for example, a register, an ATM machine, a kiosk, a mobile phone, a personal digital assistant, a tablet, a laptop, a music player, or any other device capable of receiving the modulated carrier wave 106. As seen in FIG. 5, the audio receiving computing device 104 can include, for example one or more microprocessors, which are collectively shown as CPU 502. The audio receiving computing device 104 also includes, for example, a memory 504, an interconnect 506, an input 508, an output 510, and/or a network access circuitry 512. The CPU 502 can retrieve data or instructions from the memory 504 and execute the retrieved instructions. The memory 504 can include generally any computer-readable medium including, for example, persistent memory such as magnetic or optical disks, ROM, and PROM and volatile memory such as RAM.

[0044] The CPU 502 and the memory 504 are connected to one another through an interconnect 506, which is a bus in this illustrative embodiment. The interconnect 506 connects the CPU 502 and the memory 504 to the input devices 508, the output devices 510, and the network access circuitry 512. The input devices 508 can include, for example, a keyboard, a keypad, a touch-sensitive screen, a mouse, a microphone, and/or one or more cameras. The

output devices 510 can include, for example, a display – such as a liquid crystal display (LCD) – or one or more loudspeakers. The network access circuitry 512 sends and receives data through computer networks such as an intranet or the Internet.

[0045] A number of components of the audio receiving computing device 104 are stored in the memory 504. In particular, a near field authentication receiver logic 514 is part of one or more computer processes executed within CPU 502 from memory 504 in this illustrative embodiment, but can also be implemented using digital logic circuitry.

[0046] In an embodiment, the near field authentication receiver logic 514 is executable software stored within the memory 504. For example, the near field authentication receiver logic 514 can receive signals such as the modulated carrier wave 106 to verify the authenticity of the audio transceiver computing device 102.

[0047] When the near field authentication receiver logic 514 is executed, it scans a plurality of predetermined frequencies to detect a signal using the microphone disclosed as the input 508. In an embodiment, the signal is a sound wave. In another embodiment, the microphone may be a specialized band-pass microphone that is mechanically configured or otherwise designed to receive frequencies within the range of the predetermined frequencies. Such a microphone may be tuned, for example, to receive only ultrasonic frequencies of interest, and attenuate all frequencies outside the desired range. Such a microphone may be designed to plug in to the audio receiving computing device 104 through a standard audio input such as TRS or USB.

[0048] In an embodiment, the near field authentication receiver logic 514 scans each of the frequencies in the predetermined frequencies for a predetermined scanning period of time. The predetermined scanning period of time at each frequency,  $T_{SCAN}$ , is equal to at least twice the

time  $T_{ECM}$ , which is the time it takes to transmit each period of the modulated carrier wave representing the enclosed content message 302. This ensures that the near field authentication receiver logic 514 has the opportunity to receive the complete enclosed content message instead of a partial enclosed content message.

[0049] That is, the enclosed content message 302 should include the begin indication 304, the content 306, and the end indication 308. In some embodiments, however, only the begin indication 304 and the end indication 308 need be detected by the near field authentication receiver logic 514 in order for the near field authentication receiver logic 514 to consider the enclosed content message 302 to be a complete enclosed content message. Otherwise, if the enclosed content message 302 is missing, for example, the begin indication 304 or the end indication 308, it is not considered a complete enclosed content message, and instead is considered a partial enclosed content message.

[0050] However, the predetermined scanning period of time  $T_{SCAN}$  may also include an additional period of time  $K_{ECM}$  to compensate for any delays or lag. Thus, the predetermined scanning period of time at each frequency may be represented as  $T_{SCAN} = 2 \times T_{ECM} + K_{ECM}$ . If there are  $F$  predetermined frequencies, then the minimum amount of time spent scanning the predetermined frequencies,  $T_{MIN\ TOTAL\ SCAN}$ , will be represented by the equation  $T_{MIN\ TOTAL\ SCAN} = F \times (T_{SCAN})$ .

[0051] Since the near field authentication receiver logic 514 will spend at least a  $T_{MIN\ TOTAL\ SCAN}$  time period scanning the predetermined frequencies, the near field authentication transceiver logic 214 should transmit the modulated carrier wave for at least a  $T_{MIN\ TOTAL\ SCAN}$  time period. Thus, the amount of time it takes to transmit the modulated carrier wave 106

representing the periodic enclosed content message,  $T_{PECM}$ , should be equal to or greater than the  $T_{MIN\ TOTAL\ SCAN}$  time period. However,  $T_{PECM} = N \times T_{ECM}$ . Therefore,  $T_{MIN\ TOTAL\ SCAN} = N \times T_{ECM}$ . Thus, the total number of enclosed content messages 302 in the periodic enclosed content message 216 (N) is represented by the equation  $N = T_{MIN\ TOTAL\ SCAN} / T_{ECM}$ . Substituting for  $T_{MIN\ TOTAL\ SCAN}$  yields  $N = F \times (T_{SCAN}) / T_{ECM}$ . We can also replace  $T_{SCAN}$  such that we get  $N = [F \times (2 \times T_{ECM} + K_{ECM})] / T_{ECM}$  or more succinctly,  $N = 2 \times F + (F \times K_{ECM}) / T_{ECM}$ .

[0052] Thus, at a minimum the number of enclosed content messages (N) should be equal to twice the number of frequencies in the frequency period (F) plus some additional number of enclosed content messages with a minimum number of  $(F \times K_{ECM} / T_{ECM})$ . For convenience,  $K_{ECM}$  may be expressed in integral multiples of  $T_{ECM}$ , so that N results in an integer value. The additional number of enclosed content messages  $(F \times K_{ECM} / T_{ECM})$  can be selected to be sufficiently large to allow for any latency in execution of the near field authentication receiver logic 514, or switching between frequencies by the near field authentication receiver logic 514.

[0053] Referring back to FIG. 5, responsive to detecting the signal, the near field authentication receiver logic 514 can verify that the signal includes at least one enclosed content message. The enclosed content message should be a complete enclosed content message, instead of a partial enclosed content message. Partial enclosed content messages are discarded. In one embodiment, the near field authentication receiver logic 514 can stop scanning the predetermined frequencies once a signal is detected, or when the signal is verified to include at least one enclosed content message.

[0054] In an embodiment, the near field authentication receiver logic 514 can extract a content from the enclosed content message. Such extraction can occur through demodulation, A/D



conversion, decryption, decoding, deciphering, descrambling, or any other methods needed to recover the original content so that it is recognizable and useable by the near field authentication receiver logic 514. Furthermore, when keys are used for decryption of the content, standard RSA (PKI) keys can be used. Key exchanges may occur out-of-band, such as during registration of the audio receiving computing device 104, or built-in to the near field authentication receiver logic 514.

[0055] In an embodiment, the near field authentication receiver logic 514 can also compare the extracted content to an authorized content 516. The authorized content 516 can include, for example, authenticated biometric data or authenticated device identification data, or both. The authenticated biometric data and authenticated device identification data can be, respectively, biometric data and device identification data that the user of the transceiver computing device 102 has registered beforehand as being authentic.

[0056] The near field authentication receiver logic 514 can determine if there is a match between the extracted content and the authorized content 516 to authenticate the audio transceiver computing device 102. In FIG. 5, the authorized content 516 is stored in the memory 504. However, the authorized content 516 could also be kept in other storage devices which have a database or memory accessible by the audio receiving computing device 104. In one embodiment, the near field authentication receiver logic 514 can stop scanning the predetermined frequencies when the audio transceiver computing device 102 has been authenticated.

[0057] In an embodiment, when the audio transceiver computing device 102 is authenticated, the near field authentication receiver logic 514 can, for example, perform a financial transaction

based on the content. In such a case, the content can include, for example, financial data such as a credit card number, a bank account number, or other data needed to complete a financial transaction. Of course additional functions could also be performed by the near field authentication receiver logic 514 once the audio transceiver computing device 102 is authenticated, such as ticket verification, entry into a restricted area, or any other type of function which would require authentication of the audio transceiver computing device 102, its user, or both.

[0058] Once the near field authentication receiver logic 514 authenticates the audio transceiver computing device 102, the near field authentication receiver logic 514 can display or provide an acknowledgement indication that the authentication has occurred. The acknowledgement indication may be provided locally by the device 104, for example, in the form of a visual indication or an audible tone. Alternatively or in combination, the acknowledgement indication may also be provided to the user of the device 102 by means of a locally generated audible tone, locally generated visual indication (such as an LED illuminating or changing color), or by sending a remote indication to the device 102 via a network link or by means of a sound wave using a free frequency according to the same methods disclosed herein for generating and transmitting the enclosed content message. The user of device 102, responsive to receiving the indication, may then stop transmission of the modulated carrier wave 106 by manual or automatic action. However, if the near field authentication receiver logic 514 fails to authenticate the audio transceiver computing device 102, such as if the content does not match the authorized content 516, or if no content was discovered, then the near field authentication receiver logic 514 can display or provide some sort of indication to indicate that an authentication failure has occurred. Furthermore, a log could be stored indicating the time,

location, and/or the content if available. This can help with any troubleshooting requests, and/or any investigations of fraud.

[0059] In one implementation of an acknowledgment indication, the device 104 may scan for a free frequency from among the plurality of predetermined frequencies until one is found, or it may transmit acknowledgements on a special predetermined frequency that is reserved only for transmitting such acknowledgements. In an acknowledgement message so transmitted, device 104 may include acknowledgement content in the form of a special binary code that is recognized by transceiver logic 214 within device 102 as an acknowledgement signal, and it may also include a device identifier of either or both of devices 102 and 104. In such case, device 104 may also include its own device identifier (not shown) stored in local memory 504 and recognizable by transceiver logic 214.

[0060] In an embodiment, a transaction flow diagram 600 as shown in FIG. 6 illustrates a near field authentication of sources to an audio receiving computing device 104 using an audio transceiver computing device 102. To facilitate appreciation and understanding of the invention, transaction flow diagram 600 is described in the context of an illustrative example of a user seeking to purchase a product at a register using his mobile phone. Of course the near field authentication of sources could occur for other transactions.

[0061] In step 602, the audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. For example, the mobile phone through its microphone can scan a plurality of predetermined frequencies for a free frequency.

[0062] In step 604, the audio transceiver computing device 102 selects the free frequency from the plurality of predetermined frequencies. For example, the mobile phone can identify the first

free frequency it scans that has no discernable signal, or that has no signal strength that satisfies a minimum amplitude threshold, or that otherwise meets a pre-established criteria for being a free frequency.

[0063] In step 606, the audio transceiver computing device 102 generates a periodic enclosed content message. For example, the mobile phone can generate the periodic enclosed content message by representing one or more of user biometric data, device identification data, and the user's credit card information in binary form.

[0064] In step 608, the audio transceiver computing device 102 generates a modulated carrier wave representing the periodic enclosed content message. For example, the mobile phone can generate a carrier wave and modulate the carrier wave using the periodic enclosed content message. Amplitude, frequency, or phase modulation may be used.

[0065] In step 610, the audio transceiver computing device 102 transmits the modulated carrier wave at the free frequency. For example, the mobile phone can transmit the modulated carrier wave at the free frequency through its output speaker in a directional or omnidirectional broadcast.

[0066] Thus, the user need not use a credit card to purchase the product. Instead, the user can use a device such as a mobile phone that can store credit card information. Furthermore, the mobile phone need not have its physical components modified with expensive equipment, but can use the speaker already included in the mobile phone. Thus, the user can complete the transaction using sound waves. In addition, the mobile phone need not be adjacent the register. Therefore, the user does not need to extend his arm to place the mobile phone adjacent the register, but instead can safely hold the mobile phone in a more comfortable and secure position.

Furthermore, the user can also simultaneously perform other actions on the phone while the transaction is occurring, which would not be possible if the user had to extend his arm to place the phone adjacent the register. Should any issues arise in the transaction, the user can more easily troubleshoot the issue because the user is able to manipulate the mobile phone.

[0067] In an embodiment, a transaction flow diagram 700 as shown in FIG. 7 illustrates additional steps to the transactional flow diagram 600 (FIG. 6), in which there is a near field authentication of sources associated with an audio transceiver computing device 102 by an audio receiving computing device 104.

[0068] In step 702, a user interface is displayed on the audio transceiver computing device 102 requesting biometric data from the user. For example, a user interface can be displayed on a screen of the mobile phone. The user interface can request the biometric data such as a voice recording of the user, to be received by means of biometric data input logic operating within the mobile phone when the user speaks a requested word or phrase into a microphone on the mobile phone.

[0069] In step 704, responsive to receiving the biometric data, the audio transceiver computing device 102 generates the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data. For example, responsive to receiving voice data corresponding to a voice of the user, near field authentication transceiver logic operating within the mobile phone generates the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes a digital representation of the voice data corresponding to the voice of the user.

[0070] In an embodiment, a transaction flow diagram 800 as shown in FIG. 8 illustrates a near

field authentication of sources using a microphone input of an audio receiving computing device 104. To facilitate appreciation and understanding of the invention, transaction flow diagram 800 is described in the context of an illustrative example of a seller seeking to sell a product at a register to a user transmitting financial data using his mobile phone. Of course the near field authentication of sources could occur for other transactions.

[0071] In step 802, the audio receiving computing device 104 scans a plurality of predetermined frequencies using a microphone input to detect a signal. For example, the register scans a plurality of predetermined frequencies to detect a signal using a microphone input of the register. The predetermined frequencies can be, for example, a set of known frequencies in which the mobile phone will be transmitting the periodic enclosed content message. Also, step 802 may commence automatically responsive to the audio receiving computing device 104 being powered on. Scanning may occur continuously, that is, the audio receiving computing device may scan all predetermined frequencies in some sequence, such that each frequency is scanned for a period  $T_{SCAN}$ , and that each pass across all scanned frequencies  $F$  requires a scanning period of  $F \times (T_{SCAN})$ . When all frequencies are scanned, the scanning may be repeated, and scanning in this manner may repeat indefinitely, to allow audio receiving computing device 104 to listen continuously for enclosed content messages.

[0072] In step 804, responsive to detecting the signal, the audio receiving computing device 104 verifies that the signal includes at least one enclosed content message. For example, responsive to detecting the signal, a near field authentication receiver logic in the register checks to ensure that there is a beginning indication and an ending indication in the signal to verify that the signal includes at least one enclosed content message. Any signal which does not include both the begin indication and the end indication will be discarded.

[0073] In step 806, the audio receiving computing device 104 extracts a content from the enclosed content message. For example, the near field authentication receiver logic in the register extracts the content from the enclosed content message. The content can include, for example, biometric data of the user, device identification data of the mobile phone, and the user's financial account information. Thus, the content can include the user's voice data, the device fingerprint of the mobile phone, and the user's credit card number.

[0074] In an embodiment, a transaction flow diagram 900 as shown in FIG. 9 illustrates additional steps to the transactional flow diagram 800 (FIG. 8), to enhance near field authentication of sources using a microphone input of an audio receiving computing device 104.

[0075] In step 902, the audio receiving computing device 104 compares the extracted content to authorized content to authenticate a transceiver computing device 102 that transmitted the enclosed content message. For example, the near field authentication receiver logic in the register compares the extracted content to authorized content to authenticate the mobile phone that transmitted the enclosed content message. For example, the register can compare the user's voice data and the device fingerprint of the mobile phone to authenticated versions of the user's voice data and the device fingerprint of the mobile phone to authenticate the user or the mobile phone, or both.

[0076] In step 904, the audio receiving computing device 104 performs a financial transaction based on the enclosed content message when the transceiver computing device 102 is authenticated. For example, the register debits the user's financial account based on the enclosed content message when the user or the mobile phone, or both, are authenticated. Thus, the

register can debit the user's financial account using the credit card number when the user or the mobile phone, or both, are authenticated.

[0077] Thus, to perform a transaction, the register need not be modified with expensive equipment. Instead, a relatively inexpensive microphone can be added to allow the register to perform the transaction using sound waves.

[0078] In an embodiment, the near field authentication of sources using audio waves can be used in conjunction with a more conventional online transaction to provide enhanced security for transactions, such as payments and electronic or personal access to confidential files or secure locations. In other words, near field authentication according to the invention may provide an additional layer of security during a more complex authentication procedure. For example, a transaction may be initiated by a user of a mobile device using an on-line log-in procedure in a first phase of authentication. If the first phase of authentication procedure is successful, the authenticating authority may require a second phase of authentication using a near-field authentication technique described herein to complete the procedure.

[0079] In another example, where secure information is large or requires additional security, it may be stored at a remote location from the audio transceiver computing device. Once multiples layers of authentication have occurred for the user or the audio transceiver computing device, or both, the audio receiver computing device can directly access, indirectly access, or receive the secure information from the remote location. Of course, such examples are only exemplary and are non-limiting as the quantity, manner, and amount of information stored remotely from the audio transceiver computing device can be varied as desired. This can also vary how the near



field authentication of sources using audio waves can be used in conjunction with the conventional online transaction.

[0080] Exemplary embodiments of the invention have been disclosed in an illustrative style. Accordingly, the terminology employed throughout should be read in an exemplary rather than a limiting manner. Although minor modifications to the teachings herein will occur to those well versed in the art, it shall be understood that what is intended to be circumscribed within the scope of the patent warranted hereon are all such embodiments that reasonably fall within the scope of the advancement to the art hereby contributed, and that that scope shall not be restricted, except in light of the appended claims and their equivalents.

## CLAIMS

What is claimed is:

1. A method for near field authentication of a source the source using an audio transceiver computing device comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message;

and

transmitting the modulated carrier wave at the free frequency.

2. The method of claim 1 further comprising

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. The method of claim 1 to 4 wherein the modulated carrier wave comprises a sound wave.

## ABSTRACT

A method for near field authentication of sources using an audio transceiver computing device includes scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, generating a modulated carrier wave representing the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. A method for near field authentication of sources using a microphone input of a receiving computing device includes scanning a plurality of predetermined frequencies to detect a signal using the microphone input, verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message, and extracting a content from the enclosed content message.

1/9

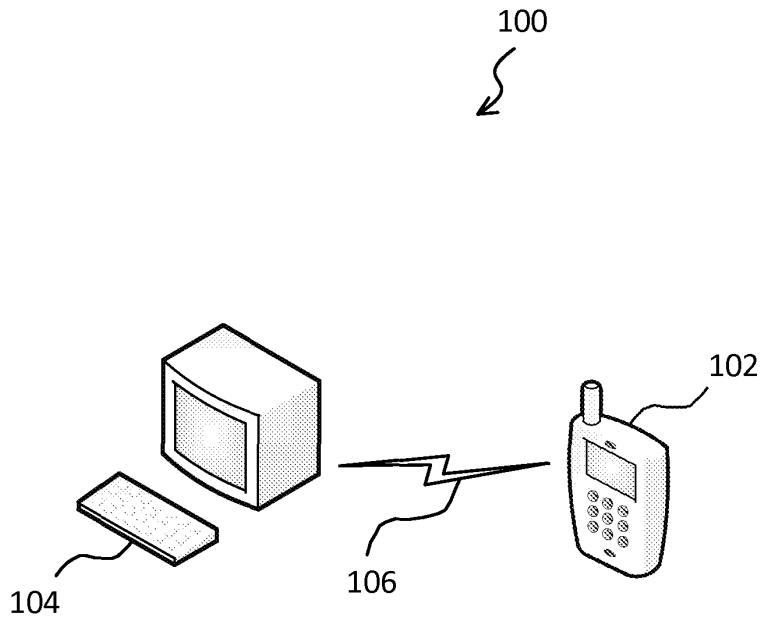


FIG. 1

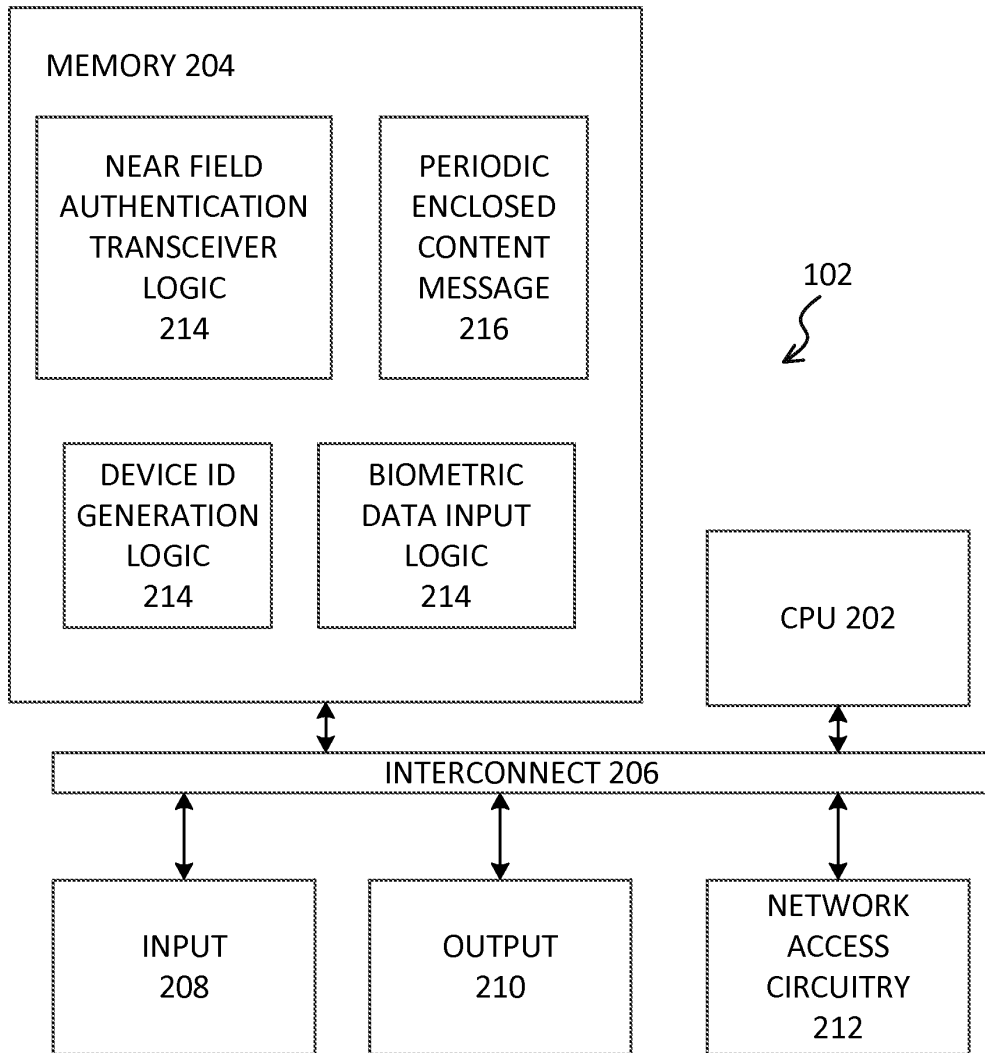


FIG. 2

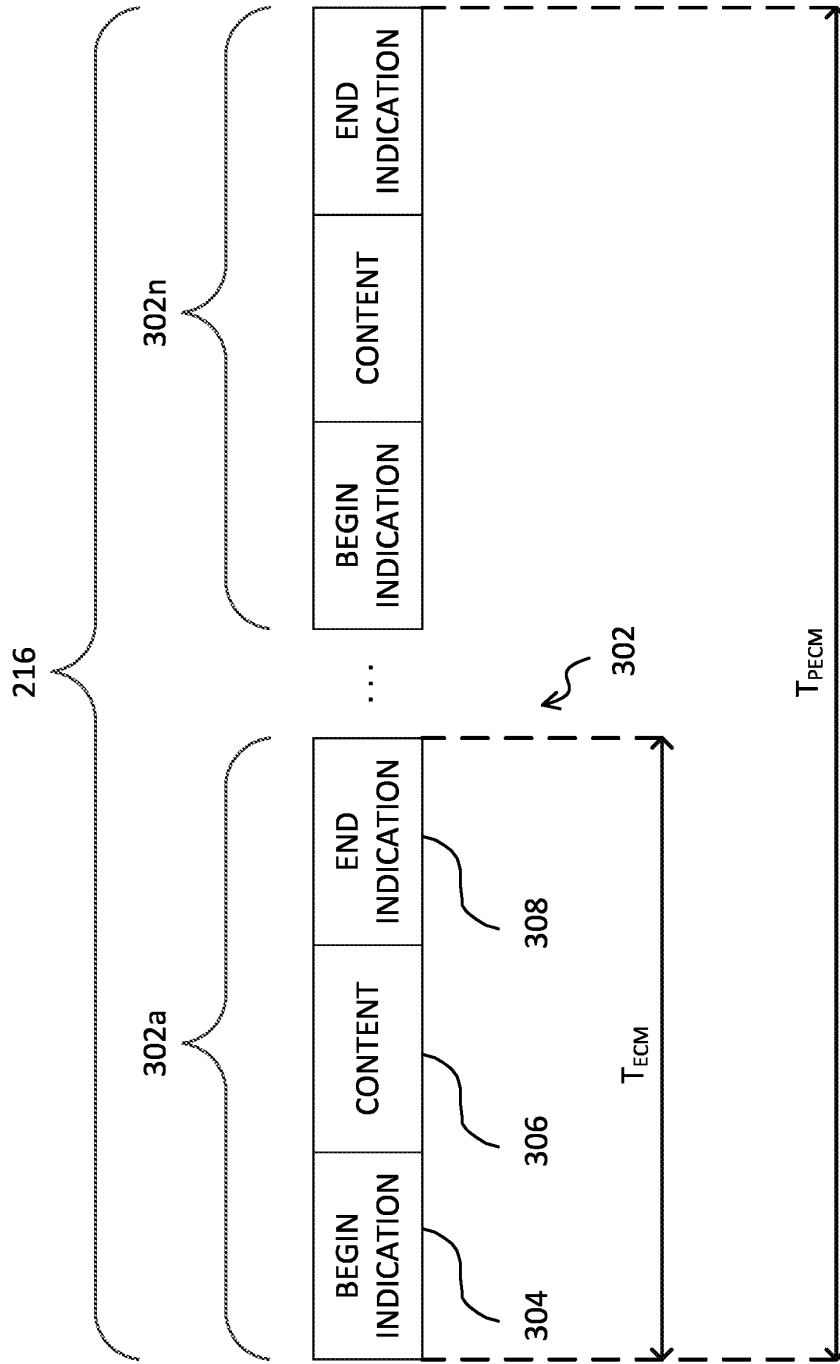


FIG. 3

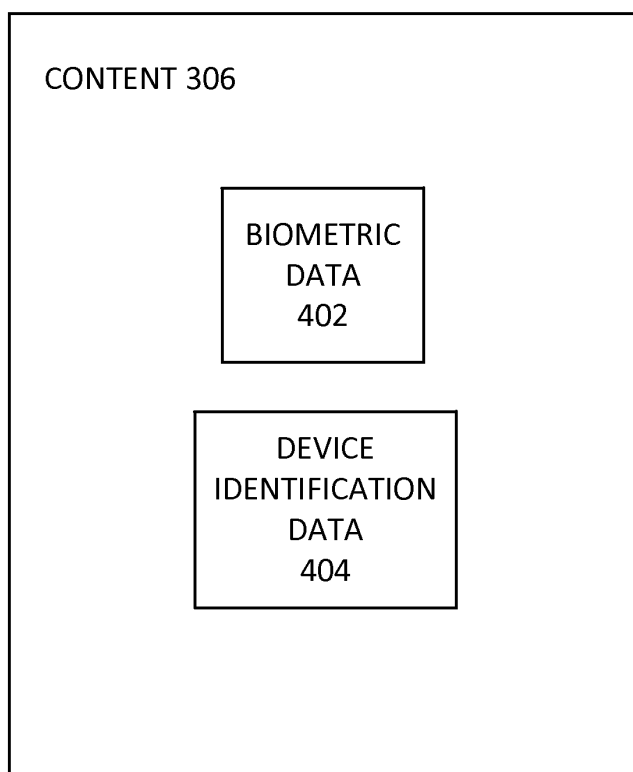


FIG. 4



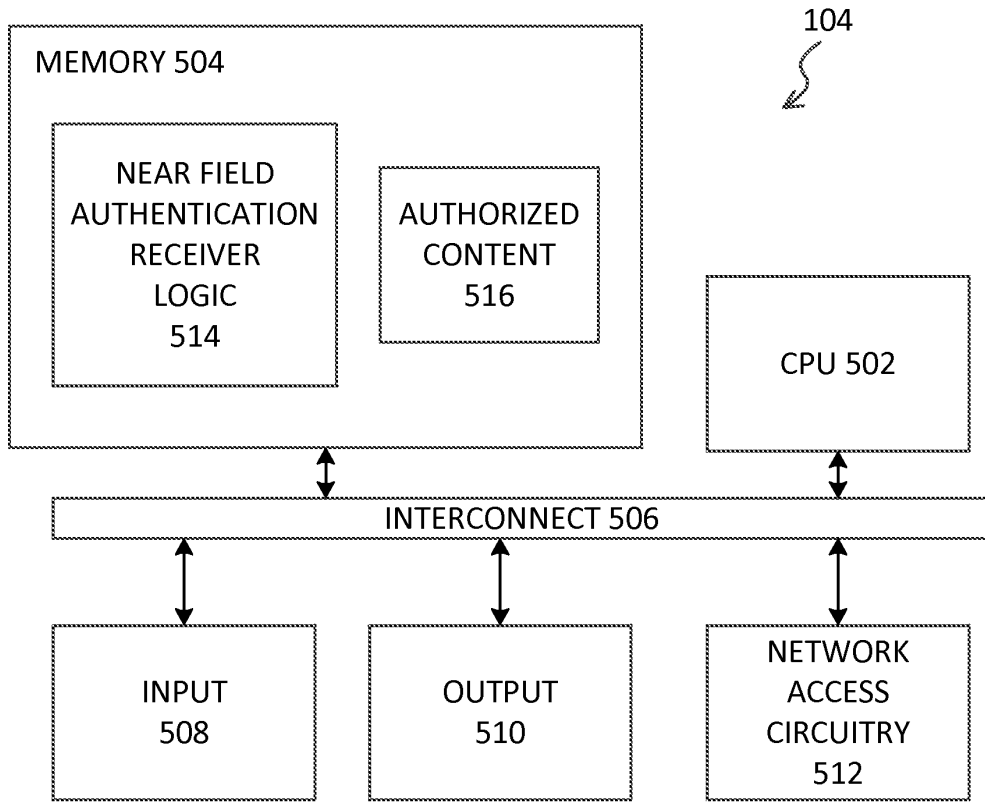


FIG. 5

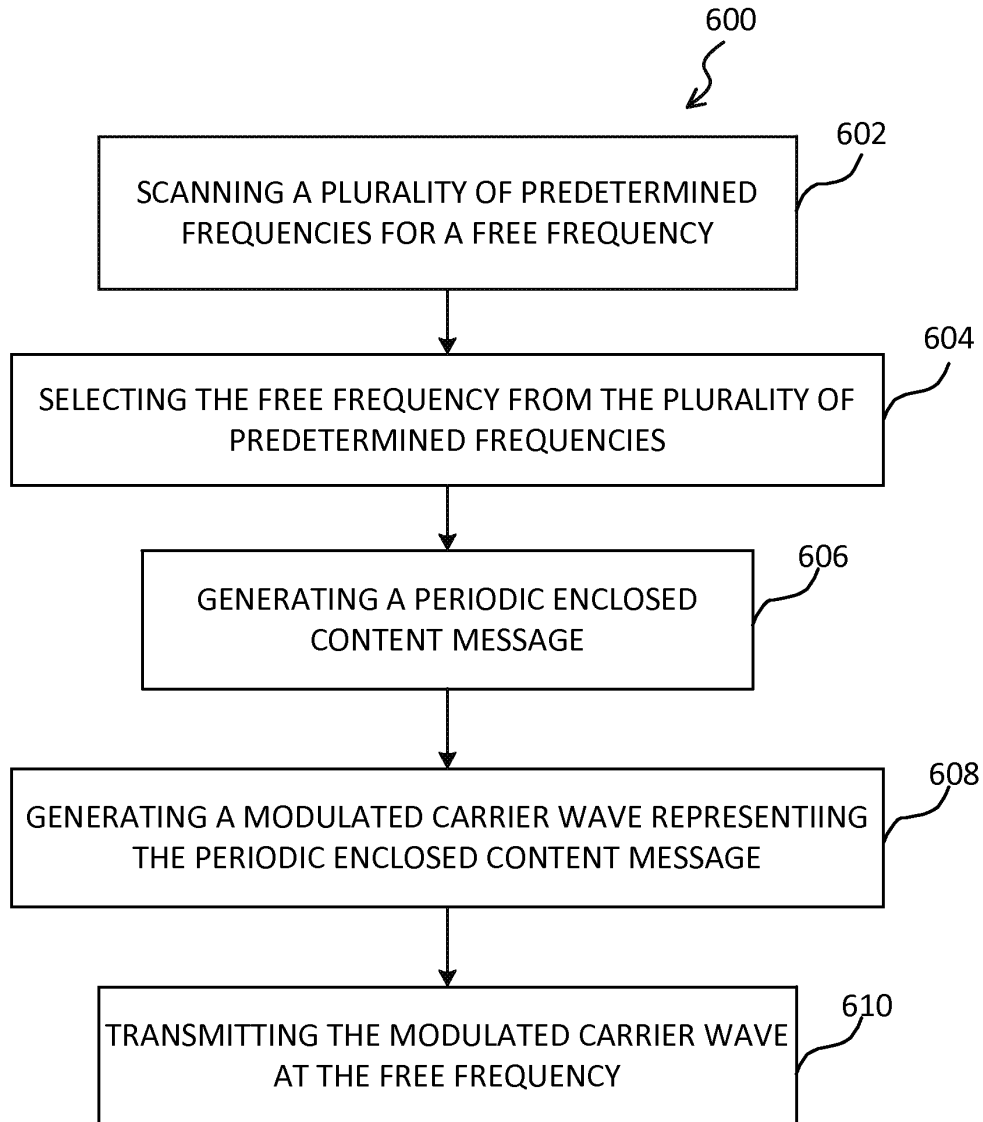


FIG. 6

700  
↙

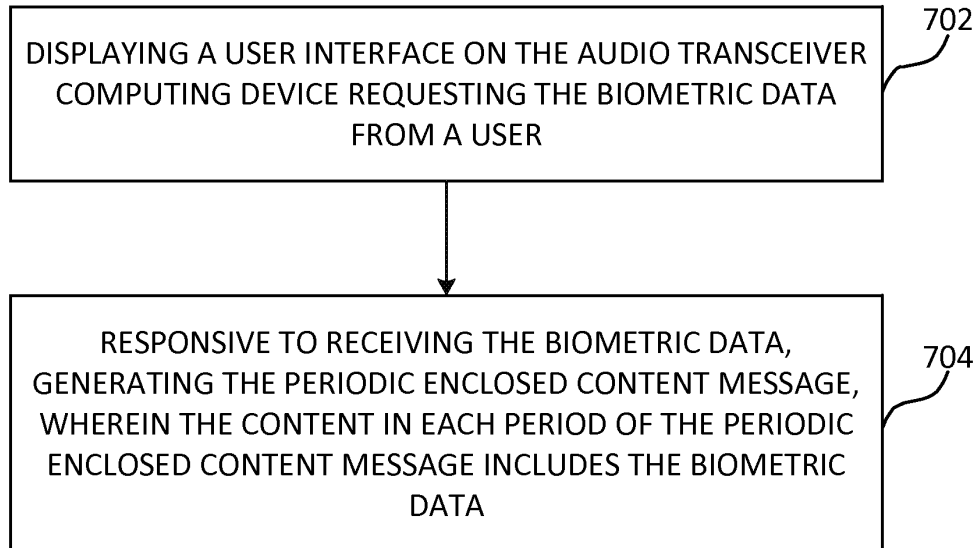


FIG. 7

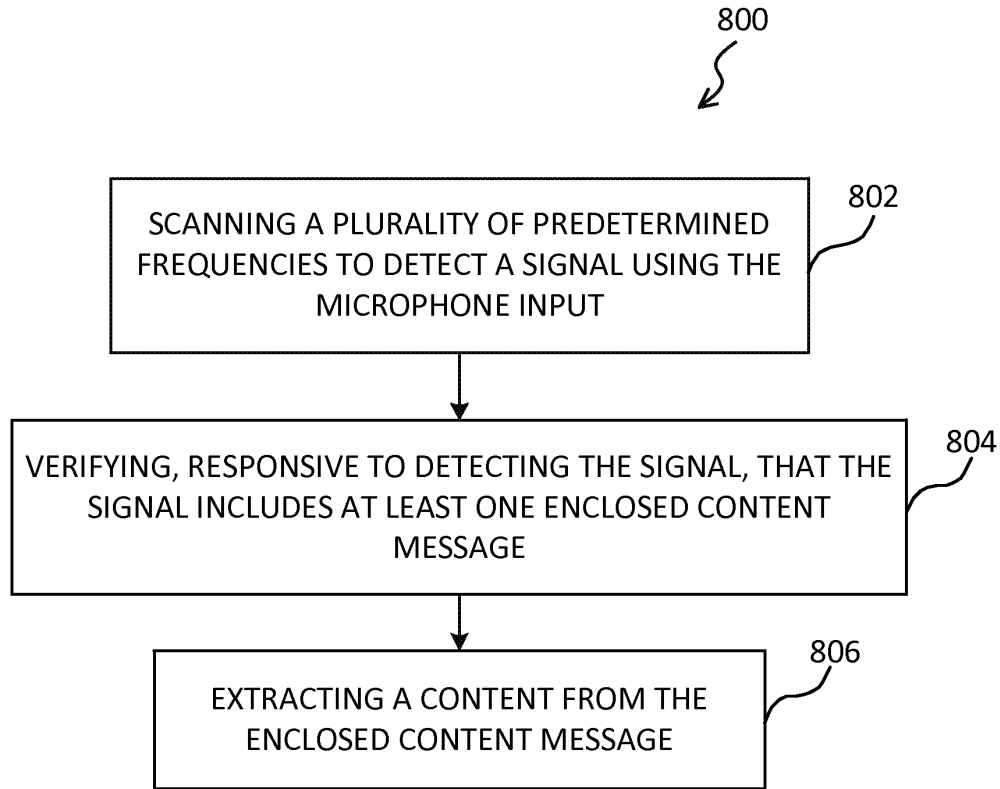


FIG. 8

900

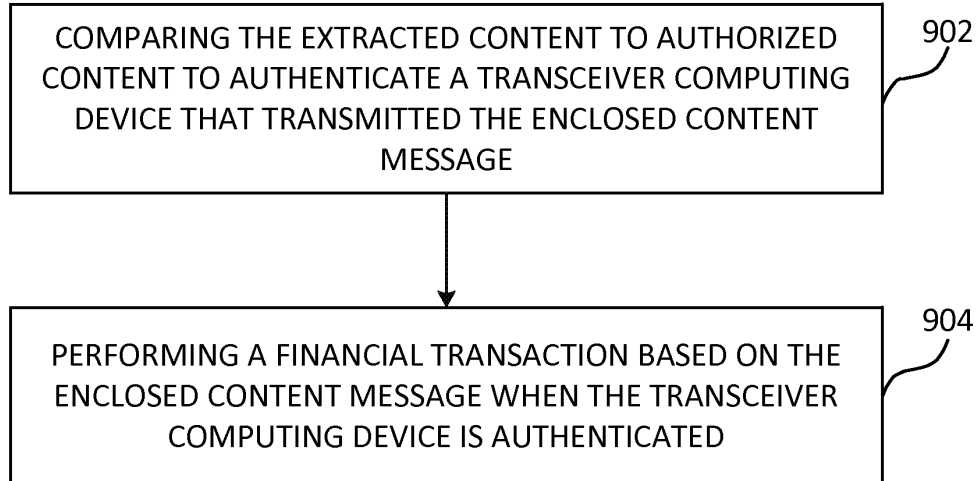


FIG. 9

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>					
<b>Filing Date:</b>					
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES				
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN				
<b>Filer:</b>	Sean Dylan Burdick				
<b>Attorney Docket Number:</b>	UN-NP-SC-085				
Filed as Small Entity					
<b>Utility under 35 USC 111(a) Filing Fees</b>					
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>	
<b>Basic Filing:</b>					
Utility filing Fee (Electronic filing)	4011	1	98	98	
Utility Search Fee	2111	1	310	310	
Utility Examination Fee	2311	1	125	125	
<b>Pages:</b>					
<b>Claims:</b>					
<b>Miscellaneous-Filing:</b>					
<b>Petition:</b>					
<b>Patent-Appeals-and-Interference:</b>					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>533</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	14601772
<b>Application Number:</b>	13734178
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3155
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN
<b>Customer Number:</b>	96051
<b>Filer:</b>	Sean Dylan Burdick
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	UN-NP-SC-085
<b>Receipt Date:</b>	04-JAN-2013
<b>Filing Date:</b>	
<b>Time Stamp:</b>	14:02:42
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$533
RAM confirmation Number	204
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------



1	Application Data Sheet	aia0014.pdf	1433119	no	7
			fa53ec78a892ad9015ee280fce08b3686ef32742		
<b>Warnings:</b>					
<b>Information:</b>					
2		UN-NP- SC-085_Spec_Claims_abstract. pdf	122781	yes	29
			7e3e45509b7903c83deba78231bf9359571f389b		
	<b>Multipart Description/PDF files in .zip description</b>				
	<b>Document Description</b>		<b>Start</b>	<b>End</b>	
	Specification		1	26	
	Claims		27	28	
	Abstract		29	29	
<b>Warnings:</b>					
<b>Information:</b>					
3	Drawings-only black and white line drawings	UN-NP- SC-085_Forma1_Figures.pdf	198595	no	9
			462a8461032e9bb066bb4d4621a01caa23be451c		
<b>Warnings:</b>					
<b>Information:</b>					
4	Fee Worksheet (SB06)	fee-info.pdf	33111	no	2
			eb8a645f43aac3ab9d64ccca21f0819ee41e29d7		
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			1787606		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

## SCORE Placeholder Sheet for IFW Content

Application Number: 13734178

Document Date: 01/04/2013

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://es/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO (modified by Applicant)  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>				<b>Complete if Known</b>		
				Application Number	13/734,178	
				Filing Date	January 4, 2012	
				First Named Inventor	Craig S. ETCHEGOYEN	
				Art Unit		
				Examiner Name		
Sheet	1	of	1	Attorney Docket Number	UN-NP-SC-085	

U. S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code <small>(if known)</small>			
		US-5,239,648	08/24/1993	Nukui, Harumi	
		US-5,313,637	05/17/1994	Rose, David K.	
		US-6,098,106	08/01/2000	Philyaw et al.	
		US-2004/0187018	09/23/2004	Owen et al.	
		US-2006/0130135	06/15/2006	Krstulich et al.	
		US-2010/0281261	11/04/2010	Razzell, Charles	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		Country Code – Number – Kind Code				

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**(12) CERTIFIED INNOVATION PATENT**  
**(19) AUSTRALIAN PATENT OFFICE**

(11) Application No. **AU 2012100462 B4**

(54) Title  
**Near field authentication through communication of enclosed content sound waves**

(51) International Patent Classification(s)  
**H04L 9/28** (2006.01)                      **H04L 29/06** (2006.01)

(21) Application No: **2012100462**                      (22) Date of Filing: **2012.04.24**

(30) Priority Data

(31) Number	(32) Date	(33) Country
<b>61/595,599</b>	<b>2012.02.06</b>	<b>US</b>

(45) Publication Date: **2012.05.24**

(45) Publication Journal Date: **2012.05.24**

(45) Granted Journal Date: **2012.05.24**

(45) Certified Journal Date: **2012.11.08**

(71) Applicant(s)  
**Uniloc USA, Inc.**

(72) Inventor(s)  
**Etchegoyen, Craig S.;Harjanto, Dono;Burdick, Sean D.**

(74) Agent / Attorney  
**Madderns Patent & Trade Mark Attorneys, GPO Box 2752, Adelaide, SA, 5001**

(56) Related Art  
**US 2010/0281261 A1**

**ABSTRACT**

A method for near field authentication of sources using an audio transceiver computing device includes scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, generating a modulated carrier wave representing the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. A method for near field authentication of sources using a microphone input of a receiving computing device includes scanning a plurality of predetermined frequencies to detect a signal using the microphone input, verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message, and extracting a content from the enclosed content message.

2012100462 24 Apr 2012

Regulation 3.2

AUSTRALIA  
PATENTS ACT 1990

**COMPLETE SPECIFICATION**  
FOR AN INNOVATION PATENT

**ORIGINAL**

---

Name of Applicant: Uniloc USA, Inc.

Actual Inventors: Craig S Etchegoyen  
Dono Harjanto  
Sean D Burdick

Address for Service: C/- MADDERNS, GPO Box 2752, Adelaide, South Australia,  
Australia

Invention title: NEAR FIELD AUTHENTICATION THROUGH  
COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

The following statement is a full description of this invention, including the best method of performing it known to us.

**NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT  
SOUND WAVES**

**BACKGROUND**

1. Field of the Invention

**[0001]** The present invention relates generally to technology for near field authentication of users and their computing devices. More specifically, the invention relates to effecting near field authentication for digital communications by means of encoded sound waves.

2. Description of the Related Art

**[0002]** The use of a user's electronic device to complete a purchase has been suggested, for example, utilizing Bluetooth technology or a WiFi Internet connection to transmit the data to the register. However, such technology requires a transactional device such as a register or ATM machine to be upgraded and retrofitted with expensive equipment and software to securely receive the data and authenticate the user's electronic device. Thus, while it may be desirable for the user, it could be prohibitively expensive for the commercial entity utilizing the transactional device, especially for small businesses.

**[0003]** The use of other technology aside from the Internet or the Bluetooth may also require not only that the transactional device be upgraded and retrofitted, but also that the user's electronic device be similarly modified. In addition, alternative technology may also have range limitations which can degrade the user's experience when performing a transaction. For example, in a conventional near field communication, radio communication is utilized to facilitate transactions. However, the conventional near field communication requires that the two transacting devices be in extremely close proximity to each other, i.e., within about 4 centimeters from each other to ensure reliable communication. This requirement for close proximity places a very restrictive limitation on practical applications for near field transactions in the real world. If one of the transacting devices is a cash register, and the other transacting device is a customer's mobile phone, the customer would need to extend the phone to within centimeters of the register and risk dropping the phone. The proximity limitation may also prevent the user from making further use of the phone while the transaction is taking place and while the phone is extended away from the customer. For example, should complications in the transaction arise, or if the user is required to provide a manual input, the customer may not be able to complete the transaction.

**[0004]** Another drawback of the conventional near field communication is the lack of security, despite the close proximity of the two devices. That is, the conventional near field communication offers no



2012100462

03 Jul 2012

protection against eavesdropping and can be vulnerable to data modifications. Needless to say, this is undesirable for financial transactions and other confidential communications.

[0005] Thus, there is a need for improved technology for effecting near field communications.

#### SUMMARY

[0006] The present invention provides a method for source authentication in network communications. A source such as a mobile computing device transmits an authentication request by executing the following salient steps using an audio transceiver: scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, encoding a carrier wave with the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. The audio transceiver, in one example, may be a mobile phone having both a speaker and a microphone.

[0007] The periodic enclosed content message includes an enclosed content message at each period. The enclosed content message comprises a beginning indication, a content, and an ending indication. The beginning indication indicates when the enclosed content message begins, while the ending indication indicates when the enclosed content ends. This allows for verification that the enclosed content message is completely instead of partially received. Furthermore, the content includes biometric data or device identification data, or both, which can be used to authenticate the user or the mobile computing device. Furthermore, the content may also include financial information for the user, or other data which might be used for gaining access to a secure network for facilitating a transaction once the user or the mobile computing device, or both, have been authenticated.

[0008] In another form, the method further comprises displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

[0009] In another form, the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

[0010] In another form, the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

[0011] In another form, the modulated carrier wave comprises a sound wave.

**Paragraphs [0012] and [0013] have been intentionally deleted.**

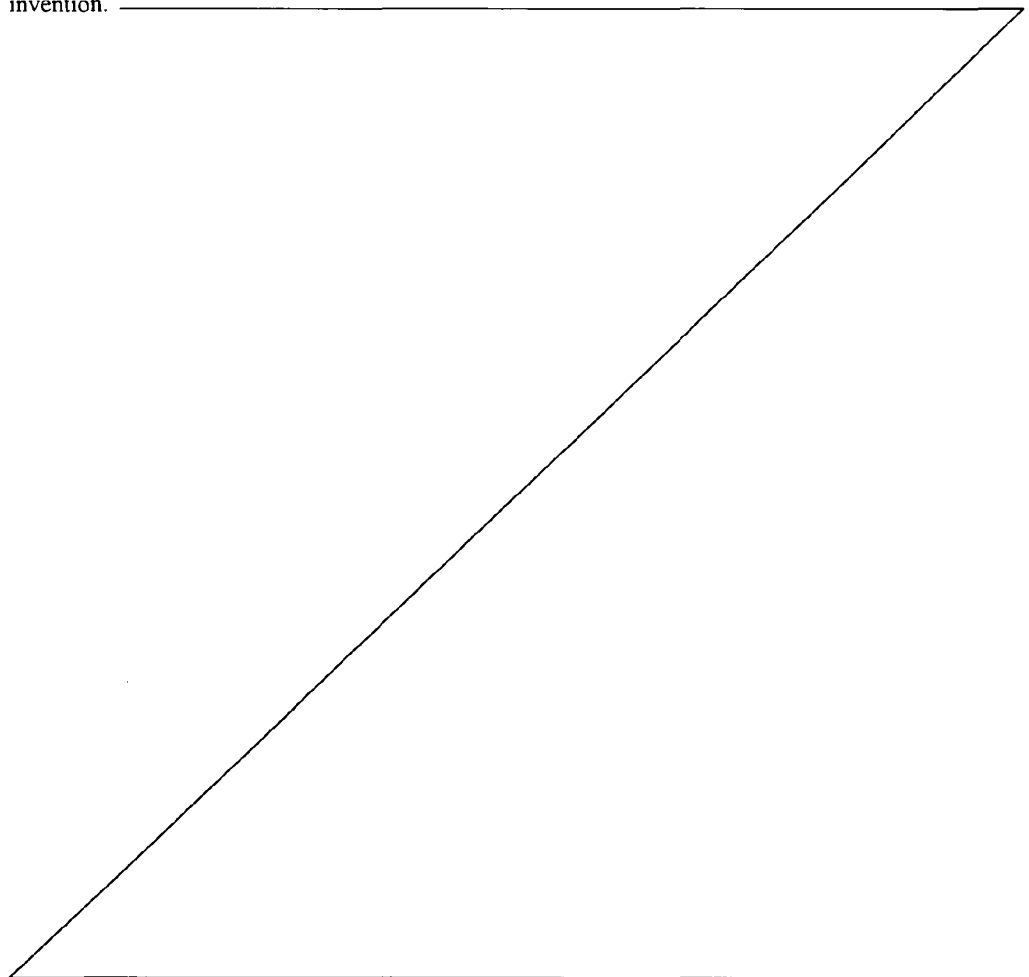
**BRIEF DESCRIPTION OF THE DRAWINGS**

[0014] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims. Component parts shown in the drawings are not necessarily to scale, and may be exaggerated to better illustrate the important features of the invention. In the drawings, like reference numerals may designate like parts throughout the different views, wherein:

[0015] FIG. 1 is a block diagram showing an audio transceiving computing device transmitting data to an audio receiving computing device in accordance with one embodiment of the present invention.

[0016] FIG. 2 is a block diagram showing functional components that make up an audio transceiving computing device according to an embodiment of the present invention.

[0017] FIG. 3 depicts a periodic enclosed content message according to an embodiment of the present invention.



[0018] FIG. 4 is a block diagram depicting message content in an enclosed content message according to an embodiment of the present invention.

[0019] FIG. 5 is a block diagram showing functional components of an audio receiving computing device according to an embodiment of the present invention.

[0020] FIG. 6 is a process flow diagram showing steps for an audio transceiving computing device to request authentication from an audio receiving computing device according to an embodiment of the present invention.

[0021] FIG. 7 depicts additional process steps for inputting content for an enclosed content message into an audio transceiving computing device in advance of requesting authentication according to an embodiment of the present invention.

[0022] FIG. 8 is a process flow diagram showing steps for receiving an audio transmission of enclosed content data using a microphone input of a receiving computing device according to an embodiment of the present invention.

[0023] FIG. 9 depicts additional process steps for authenticating an audio transceiving device according to an embodiment of the present invention.

#### **DETAILED DESCRIPTION**

[0024] The present invention relates to a method and system for near field authentication of users and computing devices using sound waves. Such users and computing devices may be referred to collectively herein as “sources”. Authenticating a source according to the present invention may involve authenticating only a user, only a computing device, or both a user and a computing device.

[0025] As seen in FIG. 1, a system 100 for authenticating sources using sounds waves can include, for example, an audio transceiving computing device 102, and an audio receiving computing device 104. The audio transceiving computing device 102 can transmit data to the audio receiving computing device 104 as a modulated carrier wave 106. The modulated carrier wave 106 can be, for example, a sound wave. Sound waves can transmit information accurately over a very short distance (near field communications) using inexpensive equipment. In different embodiments, the sound wave can have a frequency that is substantially below, within, or above the audible frequencies, such as below 20 Hz, between 20 Hz and 20 kHz, or above 20 kHz. For example, the sound wave could be an ultrasonic wave.

[0026] The audio transceiver computing device 102 can be, for example, a mobile phone, a personal digital assistant, a tablet, a laptop, a music player, or any other device having a processor operatively coupled to memory and capable of transmitting the modulated carrier wave 106 responsive to operation of the processor. As seen in FIG. 2, the audio transceiver computing device 102 can include, for example

one or more microprocessors, which are collectively shown as CPU 202. The audio transceiver computing device 102 also includes, for example, a memory 204, an interconnect 206, an input 208, an output 210, and/or a network access circuitry 212. The CPU 202 can retrieve data and/or instructions from the memory 204 and execute the retrieved instructions. The memory 204 can include generally any computer-readable medium including, for example, persistent memory such as magnetic and/or optical disks, ROM, and PROM and volatile memory such as RAM.

**[0027]** The CPU 202 and the memory 204 are connected to one another through the interconnect 206, which is a bus in this illustrative embodiment. The interconnect 206 connects the CPU 202 and the memory 204 to the input devices 208, the output devices 210, and the network access circuitry 212. The input devices 208 can include, for example, a keyboard, a keypad, a touch-sensitive screen, a mouse, a microphone, and/or one or more cameras. The output devices 210 can include, for example, a display – such as a liquid crystal display (LCD) – and/or one or more speakers. The network access circuitry 212 sends and receives data through computer networks such as an intranet or the Internet.

**[0028]** A number of components of the audio transceiver computing device 102 are stored in the memory 204. In particular, a near field authentication transceiver logic 214 is part of one or more computer processes executed within the CPU 202 from the memory 204 in this illustrative embodiment, but can also be implemented using digital logic circuitry. As used herein, “logic” refers to (i) logic implemented as computer instructions and/or data within one or more computer processes and/or (ii) logic implemented in electronic circuitry.

**[0029]** In an embodiment, the near field authentication transceiver logic 214 is executable software stored within the memory 204. For example, when the audio transmitting computing device 102 receives a request from the user to transmit the modulated carrier wave 106, the audio transceiver computing device 102 executes the near field authentication transceiver logic 214 to transmit the modulated carrier wave 106 to the audio receiving computing device 104. As previously noted the modulate carrier wave 106 can be an analog signal, such as a sound signal. Advantageously, an analog signal has an infinite amount of signal resolution. Furthermore, the use of sound signals increases the permissible transmission distance. That is, the theoretical and practical working distance for completing a transaction using the present invention is increased and can be measured, for example, in feet or meters instead of centimeters. This allows the user to utilize the audio transceiver computing device 102 for additional functions simultaneously while completing a transaction. It also reduces a likelihood that the user will be prone to dropping or otherwise damaging the audio transceiver computing device 102 by moving the audio transceiver computing device 102 into very close proximity with the audio receiving computing device 104.

**[0030]** When the near field authentication transceiver logic 214 is executed, the audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. The predetermined frequencies can be, for example, frequencies for which the audio transceiver computing device 102 is authorized to transmit the modulated carrier wave or which are known to the audio receiving computing device 104. In an embodiment, the predetermined frequencies can be selected to be outside the audible frequencies. From the predetermined frequencies, the near field authentication transceiver logic 214 can select a free frequency. The free frequency can be, for example, a frequency which has a noise level below a predetermined noise level threshold or a frequency that has an interference level below a predetermined interference level threshold.

**[0031]** The near field authentication transceiver logic 214 can also generate a periodic enclosed content message 216 as shown in FIG. 2. To generate the periodic enclosed content message 216, the near field authentication transceiver logic 214 can utilize a device ID generation logic 218 or a biometric data input logic 220, or both. The device ID generation logic 218 can generate, for example, device identification data of the audio transceiver computing device 102. In an embodiment, the device ID generation logic 218 can utilize known techniques for generating a device fingerprint. The biometric data input logic 220 can display, for example, a user interface for requesting and receiving a voice or image input representing biometric data. The device identification data or the biometric data, or both, can be included in a content of the periodic enclosed content message 216, which will be described later.

**[0032]** The near field authentication transceiver logic 214 can also generate a modulated carrier wave 106 representing the periodic enclosed content message. The modulated carrier wave 106 can be transmitted at the free frequency to the audio receiving computing device 104. Preferably, the periodic enclosed content message is generated initially in digital format, and is then converted into an analog signal and used to modulate the carrier wave. In an embodiment, the digital form of the periodic enclosed content message 216 can be encrypted using standard RSA (PKI) keys. Key exchanges may occur out-of-band, such as during registration of the audio transceiver computing device 102, or may be built-in to the near field authentication transceiver logic 214.

**[0033]** As can be seen in FIG. 3, the periodic enclosed content message 216 includes, for example, multiple periods with each period including an enclosed content message 302. Thus, the periodic enclosed content message 216 includes a plurality of enclosed content messages 302 such as enclosed content messages 302a – 302n for a total of N enclosed content messages. Each of the enclosed content messages includes a begin indication 304, a content 306, and an end indication 308. The begin indication 304 can be any type of signal that uniquely indicates the beginning of the enclosed content message, for example, a specified sequence of binary bits. Similarly, the end indication 308 can be any type of signal that indicates the ending of the enclosed content message. In one embodiment, the begin indication 304

and the end indication 308 comprise different signals. In another embodiment, the begin indication 304 and the end indication 308 comprise identical signals, i.e. two of the same signals in sequence. In another embodiment, an end indication 308(n-1) and the next begin indication 304(n) may be one and the same signal.

**[0034]** Referring to FIG. 4, the content 306 can include, for example, biometric data 402 or a device identification data 404 or a combination of both. The biometric data 402 can include, for example, the data corresponding to a voice of a user, a fingerprint of the user, an image of the user, or any other physiological data of the user which can be used to verify an identity of the user. The device identification data 404 can include, for example, a MAC address of the audio transceiver computing device 102, a hard disk serial number of the audio transceiver computing device 102, a device ID number of the audio transceiver computing device 102, a device phone number of the audio transceiver computing device 102, a device fingerprint of the audio transceiver computing device 102, or any other information which could be used to identify and verify the authenticity of the audio transceiver computing device 102.

**[0035]** A device fingerprint comprises binary data that identifies the audio transceiver computing device 102 by deriving a unique data string from multiple portions of indicia stored in memory locations within the device, where such indicia can include, for example, data representing a manufacture name, a model name, or a device type. Device fingerprints and generation thereof are known and are described, e.g., in U.S. Patent 5,490,216 (sometimes referred to herein as the '216 Patent), and in related U.S. Patent Application Publications 2007/0143073, 2007/0126550, 2011/0093920, and 2011/0093701 (the "related applications"), the descriptions of which are fully incorporated herein by reference.

**[0036]** In general, the device fingerprint comprises a bit string or bit array that includes or is derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device 102. Non-user-configurable data includes data such as hardware component model numbers, serial numbers, and version numbers, and hardware component parameters such as processor speed, voltage, current, signaling, and clock specifications. User-configurable data includes data such as registry entries, application usage data, file list information, and MAC address. In an embodiment, the audio transceiver computing device 102 can also include, for example, manufacture name, model name, and/or device type of the audio transceiver computing device 102.

**[0037]** Generation of the device fingerprint includes a combination of operations on the data specific to the audio transceiver computing device 102, which may include processing using a combination of sampling, concatenating, appending (for example, with a nonce value or a random number), obfuscating, hashing, encryption, and/or randomization algorithms to achieve a desired degree of uniqueness. For example, the desired degree of uniqueness may be set to a practical level such as 99.999999% or higher, to achieve a probability of less than 1 in 100,000,000 that any two of the audio transceiver computing

devices will generate identical fingerprints. In an embodiment, the desired degree of uniqueness may be such that the device fingerprint generated is unlike any other device fingerprint generatable responsive to a request to transmit the modulated carrier wave 106 to the audio receiving computing device 104.

**[0038]** In one embodiment, the device fingerprint may be stored in volatile memory and erased after transmission of the modulated carrier wave 106 to the audio receiving computing device 104. In another embodiment, the device fingerprint may be stored in persistent memory and written over each time a new fingerprint is generated by the device ID generation logic 218.

**[0039]** Referring back to FIG. 3, the amount of time it takes to transmit the modulated carrier wave 106 representing the periodic enclosed content message,  $T_{PECM}$ , can be a sum of the time it takes to transmit a modulated carrier wave representing each of the enclosed content messages 302 in the periodic enclosed content message 216. For example, the time it takes to transmit each of the modulated carrier waves representing an enclosed content message 302 can be  $T_{ECM}$ . Thus, the amount of time it takes to transmit the modulated carrier wave 106  $T_{PECM}$  can be, for example, represented by the equation  $T_{PECM} = N \times T_{ECM}$  where  $N$  represents the total number of enclosed content messages 302 in the periodic enclosed content message 216.

**[0040]** The total number  $N$  of enclosed content messages 302 in the periodic enclosed content messages 216 can be a function of the total number of frequencies in the plurality of predetermined frequencies. That is, the total number  $N$  of enclosed content messages 302 should be sufficient such that the audio receiving computing device 104 can scan through the predetermined frequencies to determine the free frequency on which the modulated carrier wave 106 is transmitted, and have time enough to receive at least one of the enclosed content messages 302. This will be discussed in more detail below. In an embodiment, the near field authentication transceiver logic 214 can transmit the modulated carrier wave 106 for a predetermined number of periods, or a predetermined period of time. In another embodiment, the near field authentication transceiver logic 214 can transmit the modulated carrier wave 106 until a stop indication is received from the user. Such indication can come, for example, from the input 208 in the form of a button depression, a tap on a screen, a vocal indication, or any other type of indication from the user to stop transmission of the modulated carrier wave 106.

**[0041]** In an embodiment, the near field authentication transceiver logic 214 using the biometric data input logic 220 can display a user interface on the output 210 when the output 210 is, for example, a display screen. The user interface can request the biometric data 402 from the user. For example, the user interface can prompt the user for voice input to be newly received by the biometric data input logic 220 and subsequently the near field authentication transceiver logic 214 through a microphone input on the audio transceiver computing device 102. A characteristic voice print in digital form may be derived from the voice input using technology known in the art. In another example, the user interface can

prompt the user for photographic input, such as the user's face or biometric fingerprint using a camera or scanning device on the audio transceiving computing device 102. A digital representation of the facial image or biometric fingerprint may be derived using technology known in the art. Responsive to receiving the biometric data 402, the near field authentication transceiver logic 214 can generate the periodic enclosed content message 216, wherein the content 306 in each period of the periodic enclosed content message 216 includes the biometric data (or a derivation thereof) 402.

**[0042]** Referring to FIGS. 1 and 5, the audio receiving computing device 104 can be, for example, a register, an ATM machine, a kiosk, a mobile phone, a personal digital assistant, a tablet, a laptop, a music player, or any other device capable of receiving the modulated carrier wave 106. As seen in FIG. 5, the audio receiving computing device 104 can include, for example one or more microprocessors, which are collectively shown as CPU 502. The audio receiving computing device 104 also includes, for example, a memory 504, an interconnect 506, an input 508, an output 510, and/or a network access circuitry 512. The CPU 502 can retrieve data or instructions from the memory 504 and execute the retrieved instructions. The memory 504 can include generally any computer-readable medium including, for example, persistent memory such as magnetic or optical disks, ROM, and PROM and volatile memory such as RAM.

**[0043]** The CPU 502 and the memory 504 are connected to one another through an interconnect 506, which is a bus in this illustrative embodiment. The interconnect 506 connects the CPU 502 and the memory 504 to the input devices 508, the output devices 510, and the network access circuitry 512. The input devices 508 can include, for example, a keyboard, a keypad, a touch-sensitive screen, a mouse, a microphone, and/or one or more cameras. The output devices 510 can include, for example, a display – such as a liquid crystal display (LCD) – or one or more loudspeakers. The network access circuitry 512 sends and receives data through computer networks such as an intranet or the Internet.

**[0044]** A number of components of the audio receiving computing device 104 are stored in the memory 504. In particular, a near field authentication receiver logic 514 is part of one or more computer processes executed within CPU 502 from memory 504 in this illustrative embodiment, but can also be implemented using digital logic circuitry.

**[0045]** In an embodiment, the near field authentication receiver logic 514 is executable software stored within the memory 504. For example, the near field authentication receiver logic 514 can receive signals such as the modulated carrier wave 106 to verify the authenticity of the audio transceiver computing device 102.

**[0046]** When the near field authentication receiver logic 514 is executed, it scans a plurality of predetermined frequencies to detect a signal using the microphone disclosed as the input 508. In an embodiment, the signal is a sound wave. In another embodiment, the microphone may be a specialized



band-pass microphone that is mechanically configured or otherwise designed to receive frequencies within the range of the predetermined frequencies. Such a microphone may be tuned, for example, to receive only ultrasonic frequencies of interest, and attenuate all frequencies outside the desired range. Such a microphone may be designed to plug in to the audio receiving computing device 104 through a standard audio input such as TRS or USB.

**[0047]** In an embodiment, the near field authentication receiver logic 514 scans each of the frequencies in the predetermined frequencies for a predetermined scanning period of time. The predetermined scanning period of time at each frequency,  $T_{SCAN}$ , is equal to at least twice the time  $T_{ECM}$ , which is the time it takes to transmit each period of the modulated carrier wave representing the enclosed content message 302. This ensures that the near field authentication receiver logic 514 has the opportunity to receive the complete enclosed content message instead of a partial enclosed content message.

**[0048]** That is, the enclosed content message 302 should include the begin indication 304, the content 306, and the end indication 308. In some embodiments, however, only the begin indication 304 and the end indication 308 need be detected by the near field authentication receiver logic 514 in order for the near field authentication receiver logic 514 to consider the enclosed content message 302 to be a complete enclosed content message. Otherwise, if the enclosed content message 302 is missing, for example, the begin indication 304 or the end indication 308, it is not considered a complete enclosed content message, and instead is considered a partial enclosed content message.

**[0049]** However, the predetermined scanning period of time  $T_{SCAN}$  may also include an additional period of time  $K_{ECM}$  to compensate for any delays or lag. Thus, the predetermined scanning period of time at each frequency may be represented as  $T_{SCAN} = 2 \times T_{ECM} + K_{ECM}$ . If there are  $F$  predetermined frequencies, then the minimum amount of time spent scanning the predetermined frequencies,  $T_{MIN\ TOTAL\ SCAN}$ , will be represented by the equation  $T_{MIN\ TOTAL\ SCAN} = F \times (T_{SCAN})$ .

**[0050]** Since the near field authentication receiver logic 514 will spend at least a  $T_{MIN\ TOTAL\ SCAN}$  time period scanning the predetermined frequencies, the near field authentication transceiver logic 214 should transmit the modulated carrier wave for at least a  $T_{MIN\ TOTAL\ SCAN}$  time period. Thus, the amount of time it takes to transmit the modulated carrier wave 106 representing the periodic enclosed content message,  $T_{PECM}$ , should be equal to or greater than the  $T_{MIN\ TOTAL\ SCAN}$  time period. However,  $T_{PECM} = N \times T_{ECM}$ . Therefore,  $T_{MIN\ TOTAL\ SCAN} = N \times T_{ECM}$ . Thus, the total number of enclosed content messages 302 in the periodic enclosed content message 216 ( $N$ ) is represented by the equation  $N = T_{MIN\ TOTAL\ SCAN} / T_{ECM}$ . Substituting for  $T_{MIN\ TOTAL\ SCAN}$  yields  $N = F \times (T_{SCAN}) / T_{ECM}$ . We can also replace  $T_{SCAN}$  such that we get  $N = [F \times (2 \times T_{ECM} + K_{ECM})] / T_{ECM}$  or more succinctly,  $N = 2 \times F + (F \times K_{ECM}) / T_{ECM}$ .

**[0051]** Thus, at a minimum the number of enclosed content messages ( $N$ ) should be equal to twice the number of frequencies in the frequency period ( $F$ ) plus some additional number of enclosed content

messages with a minimum number of  $(F \times K_{ECM} / T_{ECM})$ . For convenience,  $K_{ECM}$  may be expressed in integral multiples of  $T_{ECM}$ , so that  $N$  results in an integer value. The additional number of enclosed content messages  $(F \times K_{ECM} / T_{ECM})$  can be selected to be sufficiently large to allow for any latency in execution of the near field authentication receiver logic 514, or switching between frequencies by the near field authentication receiver logic 514.

**[0052]** Referring back to FIG. 5, responsive to detecting the signal, the near field authentication receiver logic 514 can verify that the signal includes at least one enclosed content message. The enclosed content message should be a complete enclosed content message, instead of a partial enclosed content message. Partial enclosed content messages are discarded. In one embodiment, the near field authentication receiver logic 514 can stop scanning the predetermined frequencies once a signal is detected, or when the signal is verified to include at least one enclosed content message.

**[0053]** In an embodiment, the near field authentication receiver logic 514 can extract a content from the enclosed content message. Such extraction can occur through demodulation, A/D conversion, decryption, decoding, deciphering, descrambling, or any other methods needed to recover the original content so that it is recognizable and useable by the near field authentication receiver logic 514. Furthermore, when keys are used for decryption of the content, standard RSA (PKI) keys can be used. Key exchanges may occur out-of-band, such as during registration of the audio receiving computing device 104, or built-in to the near field authentication receiver logic 514.

**[0054]** In an embodiment, the near field authentication receiver logic 514 can also compare the extracted content to an authorized content 516. The authorized content 516 can include, for example, authenticated biometric data or authenticated device identification data, or both. The authenticated biometric data and authenticated device identification data can be, respectively, biometric data and device identification data that the user of the transceiver computing device 102 has registered beforehand as being authentic.

**[0055]** The near field authentication receiver logic 514 can determine if there is a match between the extracted content and the authorized content 516 to authenticate the audio transceiver computing device 102. In FIG. 5, the authorized content 516 is stored in the memory 504. However, the authorized content 516 could also be kept in other storage devices which have a database or memory accessible by the audio receiving computing device 104. In one embodiment, the near field authentication receiver logic 514 can stop scanning the predetermined frequencies when the audio transceiver computing device 102 has been authenticated.

**[0056]** In an embodiment, when the audio transceiver computing device 102 is authenticated, the near field authentication receiver logic 514 can, for example, perform a financial transaction based on the content. In such a case, the content can include, for example, financial data such as a credit card number,

a bank account number, or other data needed to complete a financial transaction. Of course additional functions could also be performed by the near field authentication receiver logic 514 once the audio transceiver computing device 102 is authenticated, such as ticket verification, entry into a restricted area, or any other type of function which would require authentication of the audio transceiver computing device 102, its user, or both.

**[0057]** Once the near field authentication receiver logic 514 authenticates the audio transceiver computing device 102, the near field authentication receiver logic 514 can display or provide an acknowledgement indication that the authentication has occurred. The acknowledgement indication may be provided locally by the device 104, for example, in the form of a visual indication or an audible tone. Alternatively or in combination, the acknowledgement indication may also be provided to the user of the device 102 by means of a locally generated audible tone, locally generated visual indication (such as an LED illuminating or changing color), or by sending a remote indication to the device 102 via a network link or by means of a sound wave using a free frequency according to the same methods disclosed herein for generating and transmitting the enclosed content message. The user of device 102, responsive to receiving the indication, may then stop transmission of the modulated carrier wave 106 by manual or automatic action. However, if the near field authentication receiver logic 514 fails to authenticate the audio transceiver computing device 102, such as if the content does not match the authorized content 516, or if no content was discovered, then the near field authentication receiver logic 514 can display or provide some sort of indication to indicate that an authentication failure has occurred. Furthermore, a log could be stored indicating the time, location, and/or the content if available. This can help with any troubleshooting requests, and/or any investigations of fraud.

**[0058]** In one implementation of an acknowledgment indication, the device 104 may scan for a free frequency from among the plurality of predetermined frequencies until one is found, or it may transmit acknowledgements on a special predetermined frequency that is reserved only for transmitting such acknowledgements. In an acknowledgement message so transmitted, device 104 may include acknowledgement content in the form of a special binary code that is recognized by transceiver logic 214 within device 102 as an acknowledgement signal, and it may also include a device identifier of either or both of devices 102 and 104. In such case, device 104 may also include its own device identifier (not shown) stored in local memory 504 and recognizable by transceiver logic 214.

**[0059]** In an embodiment, a transaction flow diagram 600 as shown in FIG. 6 illustrates a near field authentication of sources to an audio receiving computing device 104 using an audio transceiver computing device 102. To facilitate appreciation and understanding of the invention, transaction flow diagram 600 is described in the context of an illustrative example of a user seeking to purchase a product

at a register using his mobile phone. Of course the near field authentication of sources could occur for other transactions.

[0060] In step 602, the audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. For example, the mobile phone through its microphone can scan a plurality of predetermined frequencies for a free frequency.

[0061] In step 604, the audio transceiver computing device 102 selects the free frequency from the plurality of predetermined frequencies. For example, the mobile phone can identify the first free frequency it scans that has no discernable signal, or that has no signal strength that satisfies a minimum amplitude threshold, or that otherwise meets a pre-established criteria for being a free frequency.

[0062] In step 606, the audio transceiver computing device 102 generates a periodic enclosed content message. For example, the mobile phone can generate the periodic enclosed content message by representing one or more of user biometric data, device identification data, and the user's credit card information in binary form.

[0063] In step 608, the audio transceiver computing device 102 generates a modulated carrier wave representing the periodic enclosed content message. For example, the mobile phone can generate a carrier wave and modulate the carrier wave using the periodic enclosed content message. Amplitude, frequency, or phase modulation may be used.

[0064] In step 610, the audio transceiver computing device 102 transmits the modulated carrier wave at the free frequency. For example, the mobile phone can transmit the modulated carrier wave at the free frequency through its output speaker in a directional or omnidirectional broadcast.

[0065] Thus, the user need not use a credit card to purchase the product. Instead, the user can use a device such as a mobile phone that can store credit card information. Furthermore, the mobile phone need not have its physical components modified with expensive equipment, but can use the speaker already included in the mobile phone. Thus, the user can complete the transaction using sound waves. In addition, the mobile phone need not be adjacent the register. Therefore, the user does not need to extend his arm to place the mobile phone adjacent the register, but instead can safely hold the mobile phone in a more comfortable and secure position. Furthermore, the user can also simultaneously perform other actions on the phone while the transaction is occurring, which would not be possible if the user had to extend his arm to place the phone adjacent the register. Should any issues arise in the transaction, the user can more easily troubleshoot the issue because the user is able to manipulate the mobile phone.

[0066] In an embodiment, a transaction flow diagram 700 as shown in FIG. 7 illustrates additional steps to the transactional flow diagram 600 (FIG. 6), in which there is a near field authentication of sources associated with an audio transceiver computing device 102 by an audio receiving computing device 104.

[0067] In step 702, a user interface is displayed on the audio transceiver computing device 102 requesting biometric data from the user. For example, a user interface can be displayed on a screen of the mobile phone. The user interface can request the biometric data such as a voice recording of the user, to be received by means of biometric data input logic operating within the mobile phone when the user speaks a requested word or phrase into a microphone on the mobile phone.

[0068] In step 704, responsive to receiving the biometric data, the audio transceiver computing device 102 generates the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data. For example, responsive to receiving voice data corresponding to a voice of the user, near field authentication transceiver logic operating within the mobile phone generates the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes a digital representation of the voice data corresponding to the voice of the user.

[0069] In an embodiment, a transaction flow diagram 800 as shown in FIG. 8 illustrates a near field authentication of sources using a microphone input of an audio receiving computing device 104. To facilitate appreciation and understanding of the invention, transaction flow diagram 800 is described in the context of an illustrative example of a seller seeking to sell a product at a register to a user transmitting financial data using his mobile phone. Of course the near field authentication of sources could occur for other transactions.

[0070] In step 802, the audio receiving computing device 104 scans a plurality of predetermined frequencies using a microphone input to detect a signal. For example, the register scans a plurality of predetermined frequencies to detect a signal using a microphone input of the register. The predetermined frequencies can be, for example, a set of known frequencies in which the mobile phone will be transmitting the periodic enclosed content message. Also, step 802 may commence automatically responsive to the audio receiving computing device 104 being powered on. Scanning may occur continuously, that is, the audio receiving computing device may scan all predetermined frequencies in some sequence, such that each frequency is scanned for a period  $T_{SCAN}$ , and that each pass across all scanned frequencies  $F$  requires a scanning period of  $F \times (T_{SCAN})$ . When all frequencies are scanned, the scanning may be repeated, and scanning in this manner may repeat indefinitely, to allow audio receiving computing device 104 to listen continuously for enclosed content messages.

[0071] In step 804, responsive to detecting the signal, the audio receiving computing device 104 verifies that the signal includes at least one enclosed content message. For example, responsive to detecting the signal, a near field authentication receiver logic in the register checks to ensure that there is a beginning indication and an ending indication in the signal to verify that the signal includes at least one

enclosed content message. Any signal which does not include both the begin indication and the end indication will be discarded.

**[0072]** In step 806, the audio receiving computing device 104 extracts a content from the enclosed content message. For example, the near field authentication receiver logic in the register extracts the content from the enclosed content message. The content can include, for example, biometric data of the user, device identification data of the mobile phone, and the user's financial account information. Thus, the content can include the user's voice data, the device fingerprint of the mobile phone, and the user's credit card number.

**[0073]** In an embodiment, a transaction flow diagram 900 as shown in FIG. 9 illustrates additional steps to the transactional flow diagram 800 (FIG. 8), to enhance near field authentication of sources using a microphone input of an audio receiving computing device 104.

**[0074]** In step 902, the audio receiving computing device 104 compares the extracted content to authorized content to authenticate a transceiver computing device 102 that transmitted the enclosed content message. For example, the near field authentication receiver logic in the register compares the extracted content to authorized content to authenticate the mobile phone that transmitted the enclosed content message. For example, the register can compare the user's voice data and the device fingerprint of the mobile phone to authenticated versions of the user's voice data and the device fingerprint of the mobile phone to authenticate the user or the mobile phone, or both.

**[0075]** In step 904, the audio receiving computing device 104 performs a financial transaction based on the enclosed content message when the transceiver computing device 102 is authenticated. For example, the register debits the user's financial account based on the enclosed content message when the user or the mobile phone, or both, are authenticated. Thus, the register can debit the user's financial account using the credit card number when the user or the mobile phone, or both, are authenticated.

**[0076]** Thus, to perform a transaction, the register need not be modified with expensive equipment. Instead, a relatively inexpensive microphone can be added to allow the register to perform the transaction using sound waves.

**[0077]** In an embodiment, the near field authentication of sources using audio waves can be used in conjunction with a more conventional online transaction to provide enhanced security for transactions, such as payments and electronic or personal access to confidential files or secure locations. In other words, near field authentication according to the invention may provide an additional layer of security during a more complex authentication procedure. For example, a transaction may be initiated by a user of a mobile device using an on-line log-in procedure in a first phase of authentication. If the first phase of authentication procedure is successful, the authenticating authority may require a second phase of authentication using a near-field authentication technique described herein to complete the procedure.

2012100462 03 Jul 2012

[0078] In another example, where secure information is large or requires additional security, it may be stored at a remote location from the audio transceiver computing device. Once multiples layers of authentication have occurred for the user or the audio transceiver computing device, or both, the audio receiver computing device can directly access, indirectly access, or receive the secure information from the remote location. Of course, such examples are only exemplary and are non-limiting as the quantity, manner, and amount of information stored remotely from the audio transceiver computing device can be varied as desired. This can also vary how the near field authentication of sources using audio waves can be used in conjunction with the conventional online transaction.

[0079] Exemplary embodiments of the invention have been disclosed in an illustrative style. Accordingly, the terminology employed throughout should be read in an exemplary rather than a limiting manner. Although minor modifications to the teachings herein will occur to those well versed in the art, it shall be understood that what is intended to be circumscribed within the scope of the patent warranted hereon are all such embodiments that reasonably fall within the scope of the advancement to the art hereby contributed, and that that scope shall not be restricted, except in light of the appended claims and their equivalents.

[0080] The reference to any prior art in this specification is not, and should not be taken as, an acknowledgement of any form of suggestion that such prior art forms part of the common general knowledge.

[0081] It will be understood that the term "comprise" and any of its derivatives (eg. comprises, comprising) as used in this specification is to be taken to be inclusive of features to which it refers, and is not meant to exclude the presence of any additional features unless otherwise stated or implied.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for near field authentication of a source, the source using an audio transceiver computing device comprising:
  - scanning a plurality of predetermined frequencies for a free frequency;
  - selecting the free frequency from the plurality of predetermined frequencies;
  - generating a periodic enclosed content message;
  - generating a modulated carrier wave representing the periodic enclosed content message; and
  - transmitting the modulated carrier wave at the free frequency;wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and
  - wherein the content includes at least one of biometric data, or device identification data.
2. The method of claim 1 further comprising:
  - displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and
  - responsive to receiving the biometric data, generating the periodic enclosed content message,wherein the content in each period of the periodic enclosed content message includes the biometric data.
3. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.
4. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.
5. The method of any one of claims 1 to 4 wherein the modulated carrier wave comprises a sound wave.



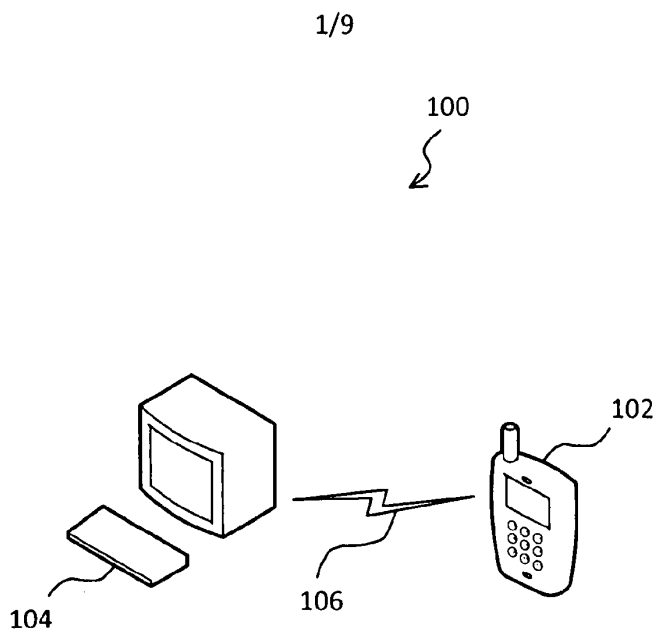


FIG. 1

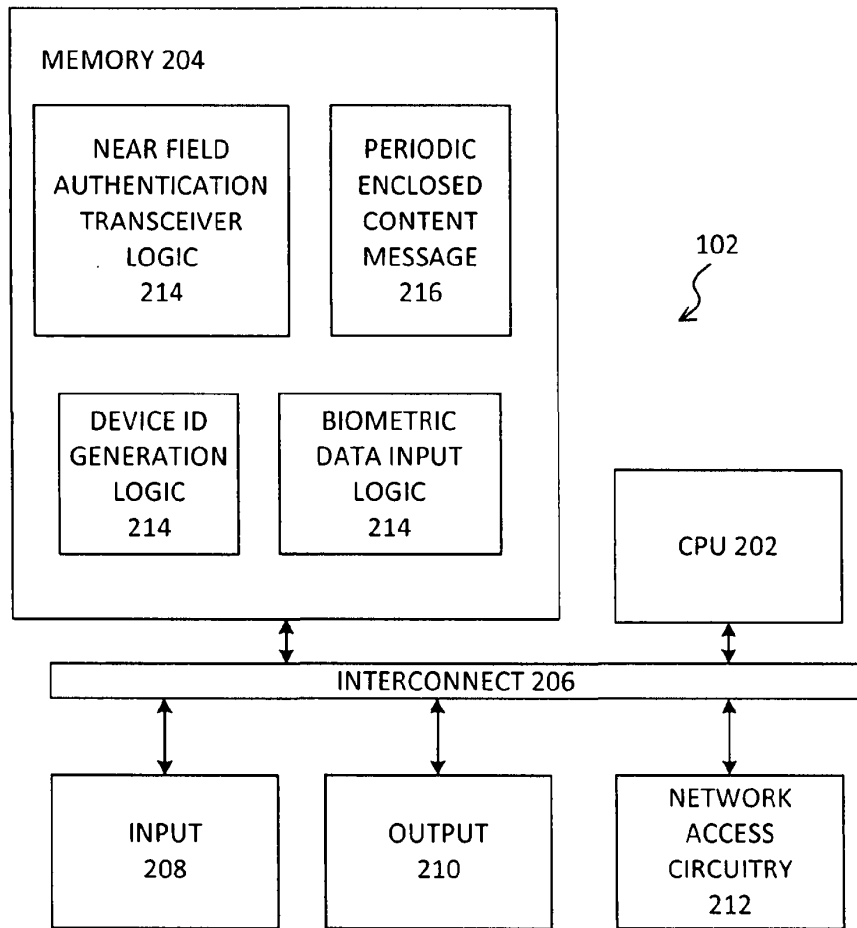


FIG. 2

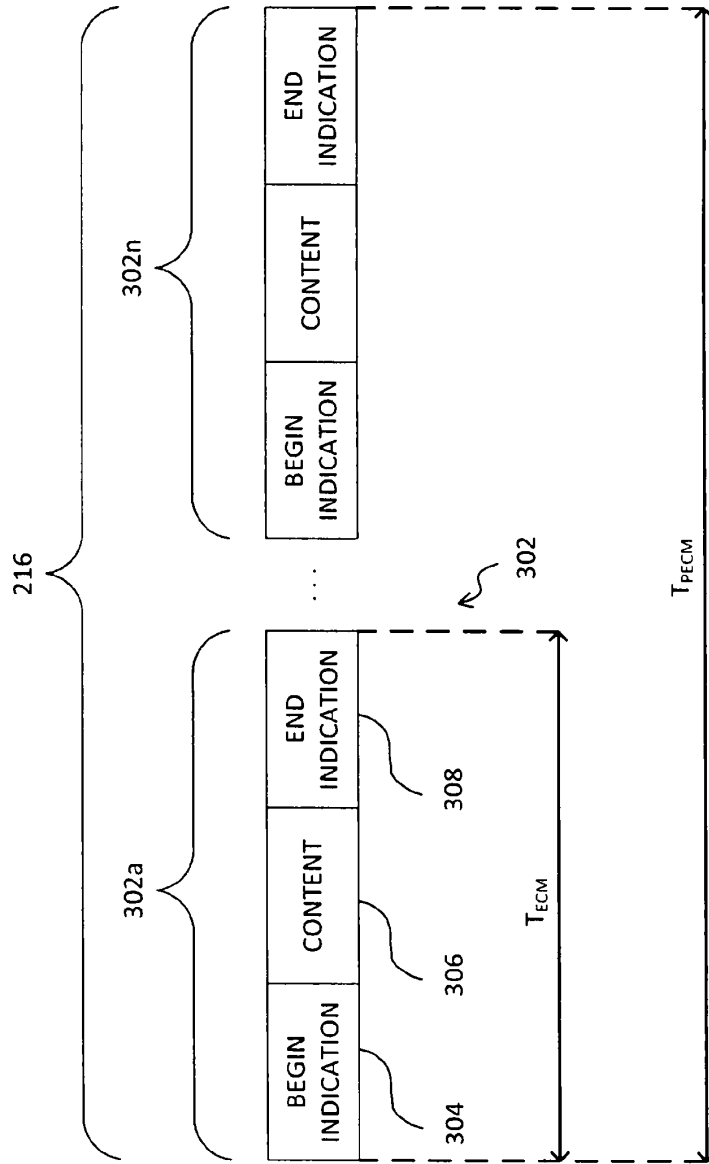


FIG. 3

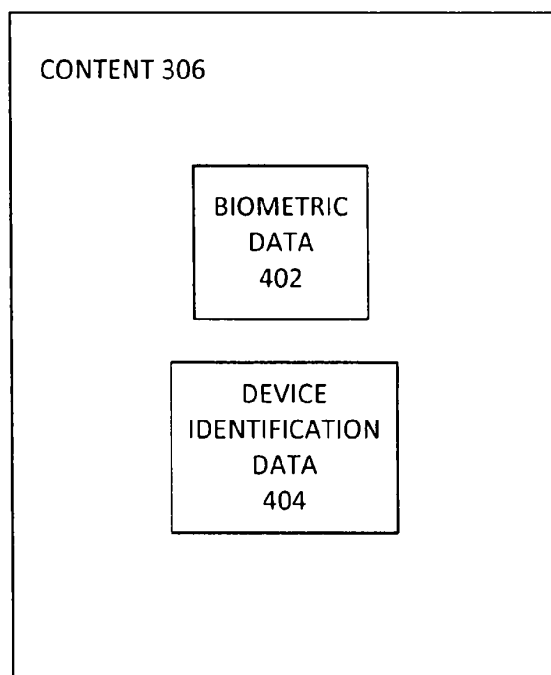


FIG. 4

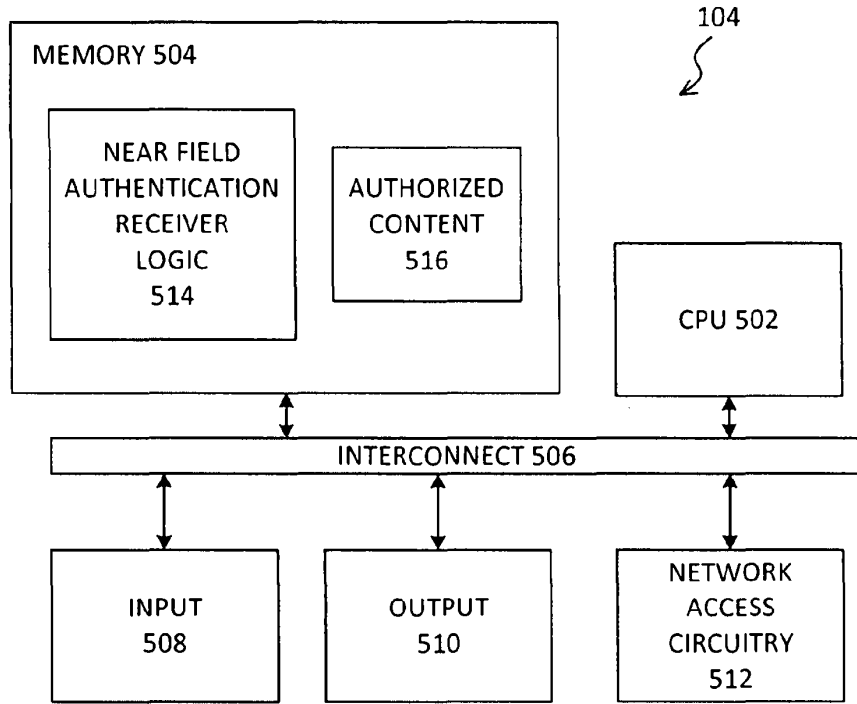


FIG. 5

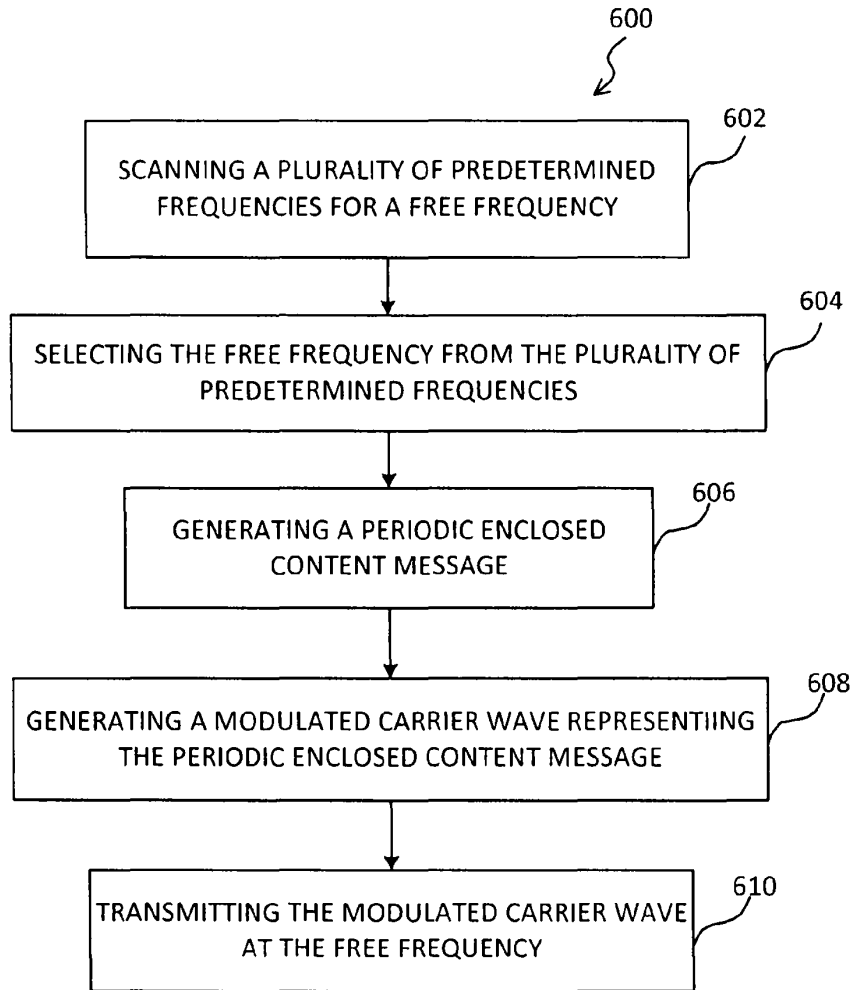


FIG. 6

7/9

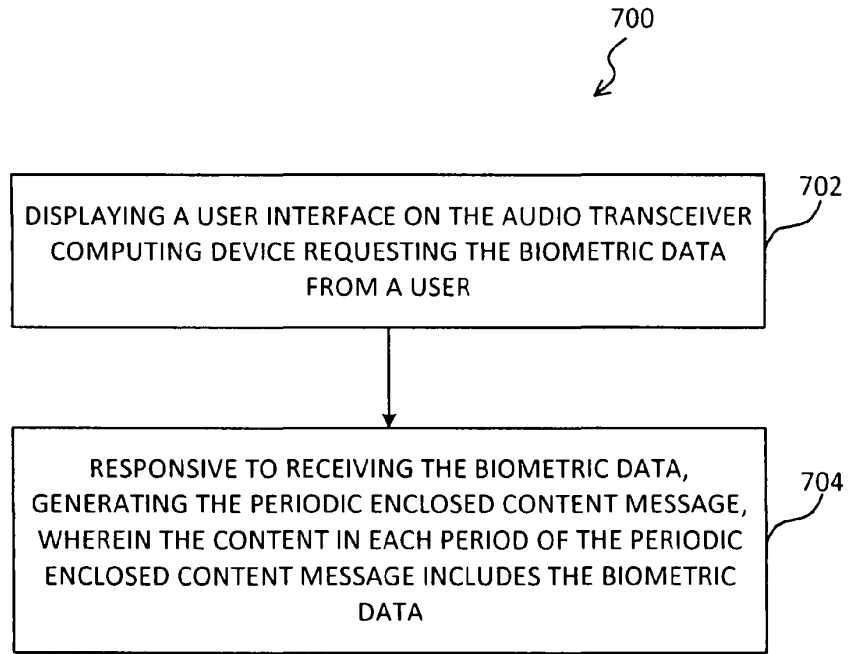


FIG. 7

8/9

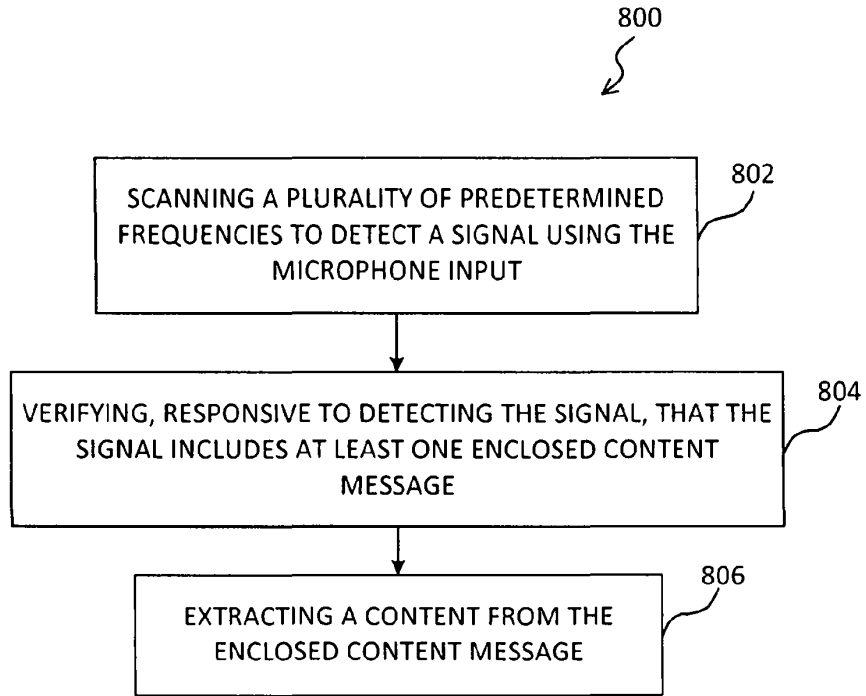


FIG. 8



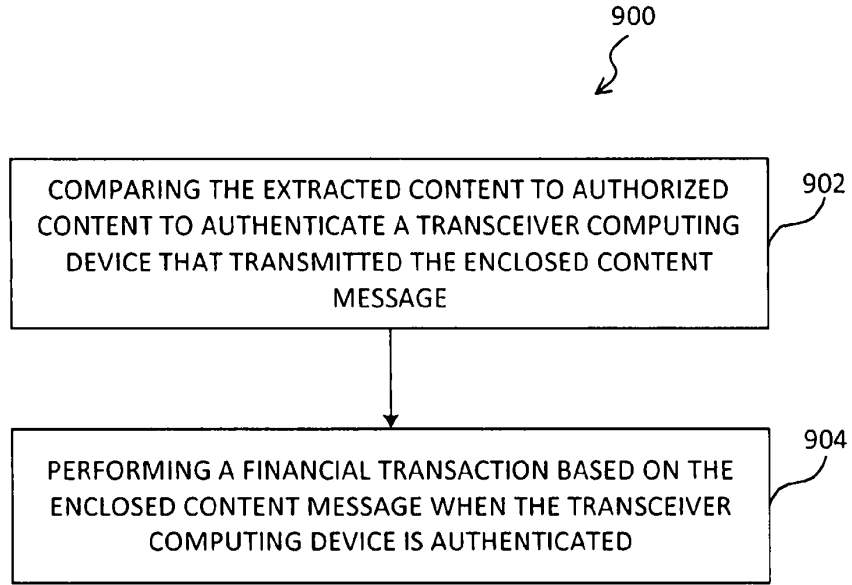


FIG. 9



Australian Government  
IP Australia

Discovery House, Phillip ACT 2606  
PO Box 200, Woden ACT 2606  
Australia  
Phone: 1300 651 010  
International Callers: +61-2 6283 2999  
Facsimile: +61-2 6283 7989  
Email: assist@ipaustralia.gov.au  
Website: www.ipaustralia.gov.au

21 May 2012

Madderns Patent & Trade Mark Attorneys  
GPO Box 2752  
Adelaide SA 5001  
Australia

Your Ref: 40665 AAL:AP

Examination Requested by: Madderns Patent & Trade Mark Attorneys  
c/o GPO Box 2752  
Adelaide SA 5001  
Australia

Their Ref:

Examiner's first report on Innovation Patent No. 2012100462 by Uniloc USA, Inc.

Last proposed amendment no.

Dear Madam/Sir,

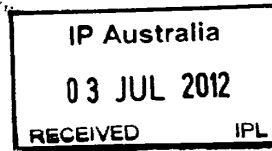
I have examined the Innovation Patent and I believe there are lawful grounds for revocation of the patent. These grounds of revocation are:

1. Your Innovation Patent application does not comply with Section 40(2)(c) of the Patents Act because it has more than five claims defining the invention. You will need to file amended claims having no more than five claims.  
**Consequently, I reserve search and opinion in regards to all examination issues pending the applicant's response to this report.**

You have 6 months from the date of this report to remove all grounds of revocation otherwise your Innovation Patent will cease.

Yours faithfully,

ANISH SINGH  
Patent Examination B  
C3 - Electronics and Communications  
Phone: (02) 6283 7915



Level 4, 19 Gouger Street  
Adelaide SA 5000 Australia  
GPO Box 2752  
Adelaide SA 5001 Australia  
Phone: +61 8 8311 8311  
Fax: +61 8 8311 8300  
mail@madderns.com.au  
www.madderns.com.au  
ABN: 98 056 210 140

3 July 2012

The Commissioner of Patents  
P O Box 200  
WODEN ACT 2606

MA SPEED DIAL 534

Dear Sir/Madam

**Australian Innovation Patent No 2012100462  
NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF  
ENCLOSED CONTENT SOUND WAVES**

**Uniloc USA, Inc.**

Our Ref: 40665 AAL:KR

Examiner: Khalid Ahmad

We refer to the Examiner's First Report dated 21 May 2021 and **enclose** amendments as set forth in the accompanying Schedule of Proposed Amendments.

Regarding item 1 the Report, we trust that the amendments to the claim set address the objection.

The application has also been amended to accord with Australian practice by bringing the consistency clauses in line with the claims.

We would request that the Examiner also consider the following six (6) documents identified by the Applicant when determining acceptance of the above application.

**US Patents References**

- D1: US 5,239,648 (Nukui)
- D2: US 5,313,637 (Rose)
- D3: US 6,098,106 (Philyaw)
- D4: US 2004/0187018 (Owen et al)
- D5: US 2006/0130135 (Krstulich et al)
- D6: US 2010/0281261 (Razzell)

Favourable reconsideration of the application is respectfully requested.

Yours faithfully  
MADDERNS

ANTHONY LEE

Enc

**Partners**  
Craig Vinall  
BE (Mech)  
Bill McFarlane  
BSc (Physics) MIEAust  
Grad Dip ElecSys  
Tom Melville  
BE (Mech) MBA  
Alun Thomas  
BAppSc (App Chem)  
Notary Public  
Martin Pannall  
BE (Elec) (Hons)  
Mark O'Donnell  
BSc (Hons)  
Anthony Lee  
PhD LLB (Hons) CPEng  
Louise Emmett  
LLM LLB/LP (Hons) BA  
**Professionals**  
Megan Ryder  
LLB (Hons) GDLP BA  
Grad Dip IP Law  
(Senior Associate)  
Jeff Holman  
PhD BSc (Hons)  
(Senior Associate)  
Stephen Worthley  
BSc LLB (Hons) MIP  
(Associate)  
Lucy Deane  
LLB (Hons) BA (Hons)  
(Associate)  
Phillip Boehm  
BE (Mech) (Hons) MIP  
(Associate)  
Stephen O'Brien  
BE (Elec) (Hons)  
(Associate)  
Irena Fizulic  
BBus (CommLaw)  
Grad Cert TMLP  
Karen Heilbronn Lee  
PhD BSc (Hons) MIP  
Christopher Wilkinson  
PhD BSc (Hons) MIP  
**Professional Support**  
Kin Seong Leong  
PhD BE (Elec) (Hons)  
Nick McLeod  
BE (Mech) (Hons)  
BMA&CompSci  
Greg Maloney  
BE (Elec)  
Richard Catt  
1949 - 2007

2012100462 03 Jul 2012

**AUSTRALIA**

Patents Act 1990

**FIRST SCHEDULE OF PROPOSED AMENDMENTS**

**Agent Name:** MADDERNS Patent & Trade Mark Attorneys  
**Agent Address:** GPO Box 2752, Adelaide, South Australia, 5001, Australia  
**Agent Reference:** 40665 AAL:KR  
**Application No:** 2012100462  
**Applicant:** Uniloc USA, Inc.  
**Report No:** 1  
**Report Date:** 21 May 2012

---

1. Cancel existing specification pages 3, 4 and 17 as currently on file and substitute in place thereof new specification pages 3, 4 and 17 as attached hereto.
2. Cancel existing claim pages 18 to 23 (claims 1 to 39) as currently on file and substitute in place thereof new claim page 18 (claims 1 to 5) as attached hereto.



Date: 3 July 2012

\_\_\_\_\_  
ANTHONY LEE  
MADDERNS

protection against eavesdropping and can be vulnerable to data modifications. Needless to say, this is undesirable for financial transactions and other confidential communications.

[0005] Thus, there is a need for improved technology for effecting near field communications.

**SUMMARY**

[0006] The present invention provides a method for source authentication in network communications. A source such as a mobile computing device transmits an authentication request by executing the following salient steps using an audio transceiver: scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, encoding a carrier wave with the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. The audio transceiver, in one example, may be a mobile phone having both a speaker and a microphone.

[0007] The periodic enclosed content message includes an enclosed content message at each period. The enclosed content message comprises a beginning indication, a content, and an ending indication. The beginning indication indicates when the enclosed content message begins, while the ending indication indicates when the enclosed content ends. This allows for verification that the enclosed content message is completely instead of partially received. Furthermore, the content can include biometric data or device identification data, or both, which can be used to authenticate the user or the mobile computing device. Furthermore, the content may also include financial information for the user, or other data which might be used for gaining access to a secure network for facilitating a transaction once the user or the mobile computing device, or both, have been authenticated.

[0008] In another embodiment, the present invention includes a computer-readable medium useful in association with an audio transceiving computing device that includes one or more processors and a memory, the computer readable medium including instructions configured to cause the audio transceiving computing device, by execution of the instructions in the one or more processors from the memory, to request authentication by executing the salient steps.

[0009] In another embodiment, the present invention includes a mobile computer system including at least one processor, a computer readable medium that is operatively coupled to the processor, and a transmission logic that (i) executes in the processor from the computer readable medium and (ii) when executed by the processor causes the mobile computer system to request authentication by executing the salient steps.

[0010] The invention also provides a method for receiving an authentication request using an audio or microphone input of a receiving computing device by executing the following second set of salient steps:

In another form, the method further comprises displaying a user (... claim 2)  
In another form, the transmitting step further comprises (... claim 3)  
" " " " " " (... claim 4)

This data for application number 2012100462 is dated 2012-12-28 22:09 AEST

scanning a plurality of predetermined frequencies to detect a signal using the microphone input, verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message, and extracting a content from the enclosed content message.

[0011] Another embodiment of the invention comprises a computer readable medium useful in association with an audio receiving computing device that includes one or more processors, an audio or microphone input, and a memory, the computer readable medium including computer instructions which are configured to cause the audio receiving computing device, by execution of the computer instructions in the one or more processors from the memory, to receive an authentication request by execution of the second set of salient steps.

[0012] In another embodiment, a present invention is a computer system including at least one processor, an audio input that is operatively coupled to the processor, a computer readable medium that is operatively coupled to the processor, and a near field authentication receiver logic that (i) executes in the processor from the computer readable medium and (ii) when executed by the processor causes the computer system to receive an authentication request via the audio input by execution of the second set of salient steps.

[0013] In an embodiment, the near field authentication of sources using audio waves can be used in conjunction with a conventional online transaction to provide enhanced security for transactions, such as payments and electronic or personal access to confidential files or secure locations.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims. Component parts shown in the drawings are not necessarily to scale, and may be exaggerated to better illustrate the important features of the invention. In the drawings, like reference numerals may designate like parts throughout the different views, wherein:

[0015] FIG. 1 is a block diagram showing an audio transceiving computing device transmitting data to an audio receiving computing device in accordance with one embodiment of the present invention.

[0016] FIG. 2 is a block diagram showing functional components that make up an audio transceiving computing device according to an embodiment of the present invention.

[0017] FIG. 3 depicts a periodic enclosed content message according to an embodiment of the present invention.

[0078] In another example, where secure information is large or requires additional security, it may be stored at a remote location from the audio transceiver computing device. Once multiples layers of authentication have occurred for the user or the audio transceiver computing device, or both, the audio receiver computing device can directly access, indirectly access, or receive the secure information from the remote location. Of course, such examples are only exemplary and are non-limiting as the quantity, manner, and amount of information stored remotely from the audio transceiver computing device can be varied as desired. This can also vary how the near field authentication of sources using audio waves can be used in conjunction with the conventional online transaction.

[0079] Exemplary embodiments of the invention have been disclosed in an illustrative style. Accordingly, the terminology employed throughout should be read in an exemplary rather than a limiting manner. Although minor modifications to the teachings herein will occur to those well versed in the art, it shall be understood that what is intended to be circumscribed within the scope of the patent warranted hereon are all such embodiments that reasonably fall within the scope of the advancement to the art hereby contributed, and that that scope shall not be restricted, except in light of the appended claims and their equivalents.

*cyh para  
comprising/including para*

most revised  
claims

CLAIMS:

1. A method for near field authentication of sources using an audio transceiver computing device comprising:
  - scanning a plurality of predetermined frequencies for a free frequency;
  - selecting the free frequency from the plurality of predetermined frequencies;
  - generating a periodic enclosed content message;
  - generating a modulated carrier wave representing the periodic enclosed content message; and
  - transmitting the modulated carrier wave at the free frequency.
2. The method of claim 1 wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication.
3. The method of claim 2 wherein the content includes at least one of biometric data, or device identification data.
4. The method of claim 3 further comprising
  - displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and
  - responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.
5. The method of claim 1 wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.
6. The method of claim 1 wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.
7. The method of claim 1 wherein the modulated carrier wave comprises a sound wave.
8. A computer readable medium useful in association with an audio transceiver computing device which includes one or more processors and a memory, the computer readable medium including computer instructions which are configured to cause the audio transceiver computing device, by execution of the



computer instructions in the one or more processors from the memory, to implement near field authentication of sources by:

- scanning a plurality of predetermined frequencies for a free frequency;
- selecting the free frequency from the plurality of predetermined frequencies;
- generating a periodic enclosed content message;
- generating a modulated carrier wave representing the periodic enclosed content message;

and

- transmitting the modulated carrier wave at the free frequency.

9. The computer readable medium of claim 8 wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication.

10. The computer readable medium of claim 9 wherein the content includes at least one of biometric data, or device identification data.

11. The computer readable medium of claim 10 wherein the near field authentication of sources further comprises:

- displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

- responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

12. The computer readable medium of claim 8 wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

13. The computer readable medium of claim 8 wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

14. The computer readable medium of claim 8 wherein the modulated carrier wave comprises a sound wave.

15. A mobile computer system comprising:  
at least one processor;

a computer readable medium that is operatively coupled to the processor; and  
a near field authentication transceiver logic that (i) executes in the processor from the computer readable medium and (ii) when executed by the processor causes the mobile computer system to implement near field authentication of sources by:

- scanning a plurality of predetermined frequencies for a free frequency;
- selecting the free frequency from the plurality of predetermined frequencies;
- generating a periodic enclosed content message;
- generating a modulated carrier wave representing the periodic enclosed content message;

and

- transmitting the modulated carrier wave at the free frequency.

16. The system of claim 15 wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication.

17. The system of claim 16 wherein the content includes at least one of biometric data, or device identification data.

18. The system of claim 17 wherein the near field authentication transceiver logic further causes the mobile computer system to implement near field authentication of sources by:

- displaying a user interface on the mobile computer system requesting the biometric data from a user; and

- responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

19. The system of claim 15 wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

20. The system of claim 15 wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

21. The system of claim 15 wherein the modulated carrier wave comprises a sound wave.

22. A method for near field authentication of sources using a microphone input of a receiving computing device comprising:

scanning a plurality of predetermined frequencies to detect a signal using the microphone input; verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message; and

extracting a content from the enclosed content message.

23. The method of claim 22 wherein the enclosed content message includes a begin indication, the content, and an end indication.

24. The method of claim 23 wherein the content includes at least one of biometric data, or device identification data.

25. The method of claim 22 further comprising comparing the extracted content to authorized content to authenticate a transceiver computing device that transmitted the enclosed content message.

26. The method of claim 25 further comprising performing a financial transaction based on the enclosed content message when the transceiver computing device is authenticated.

27. The method of claim 22 wherein the signal is a sound wave.

28. A computer readable medium useful in association with an audio receiving computing device which includes one or more processors, a microphone input, and a memory, the computer readable medium including computer instructions which are configured to cause the audio transceiver computing device, by execution of the computer instructions in the one or more processors from the memory, to implement near field authentication of sources by:

scanning a plurality of predetermined frequencies to detect a signal using the microphone input; verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message; and

extracting a content from the enclosed content message.

29. The computer readable medium of claim 28 wherein the enclosed content message includes a begin indication, the content, and an end indication.

30. The computer readable medium of claim 29 wherein the content includes at least one of biometric data, or device identification data.

31. The computer readable medium of claim 28 wherein the near field authentication of sources further comprises comparing the extracted content to authorized content to authenticate a transceiver computing device that transmitted the enclosed content message.

32. The computer readable medium of claim 31 wherein the near field authentication of sources further comprises performing a financial transaction based on the enclosed content message when the transceiver computing device is authenticated.

33. The computer readable medium of claim 28 wherein the signal is a sound wave.

34. A computer system comprising:  
at least one processor;  
a microphone input that is operatively coupled to the processor;  
a computer readable medium that is operatively coupled to the processor; and  
a near field authentication receiver logic that (i) executes in the processor from the computer readable medium and (ii) when executed by the processor causes the computer system to implement near field authentication of sources by:  
scanning a plurality of predetermined frequencies to detect a signal using the microphone input;  
verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message; and  
extracting a content from the enclosed content message.

35. The system of claim 34 wherein the enclosed content message includes a begin indication, the content, and an end indication.

36. The system of claim 35 wherein the content includes at least one of biometric data, or device identification data.

37. The system of claim 34 wherein the near field authentication receiver logic further causes the computer system to implement near field authentication of sources by comparing the extracted content to authorized content to authenticate a transceiver computing device that transmitted the enclosed content message.

38. ~~The system of claim 37 wherein the near field authentication receiver logic further causes the computer system to implement near field authentication of sources by performing a financial transaction based on the enclosed content message when the transceiver computing device is authenticated.~~

39. The system of claim 34 wherein the signal is a sound wave.

03 Jul 2012

2012100462

protection against eavesdropping and can be vulnerable to data modifications. Needless to say, this is undesirable for financial transactions and other confidential communications.

[0005] Thus, there is a need for improved technology for effecting near field communications.

#### SUMMARY

[0006] The present invention provides a method for source authentication in network communications. A source such as a mobile computing device transmits an authentication request by executing the following salient steps using an audio transceiver: scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, encoding a carrier wave with the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. The audio transceiver, in one example, may be a mobile phone having both a speaker and a microphone.

[0007] The periodic enclosed content message includes an enclosed content message at each period. The enclosed content message comprises a beginning indication, a content, and an ending indication. The beginning indication indicates when the enclosed content message begins, while the ending indication indicates when the enclosed content ends. This allows for verification that the enclosed content message is completely instead of partially received. Furthermore, the content includes biometric data or device identification data, or both, which can be used to authenticate the user or the mobile computing device. Furthermore, the content may also include financial information for the user, or other data which might be used for gaining access to a secure network for facilitating a transaction once the user or the mobile computing device, or both, have been authenticated.

[0008] In another form, the method further comprises displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

[0009] In another form, the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

[0010] In another form, the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

[0011] In another form, the modulated carrier wave comprises a sound wave.

**Paragraphs [0012] and [0013] have been intentionally deleted.**

2012100462 03 Jul 2012

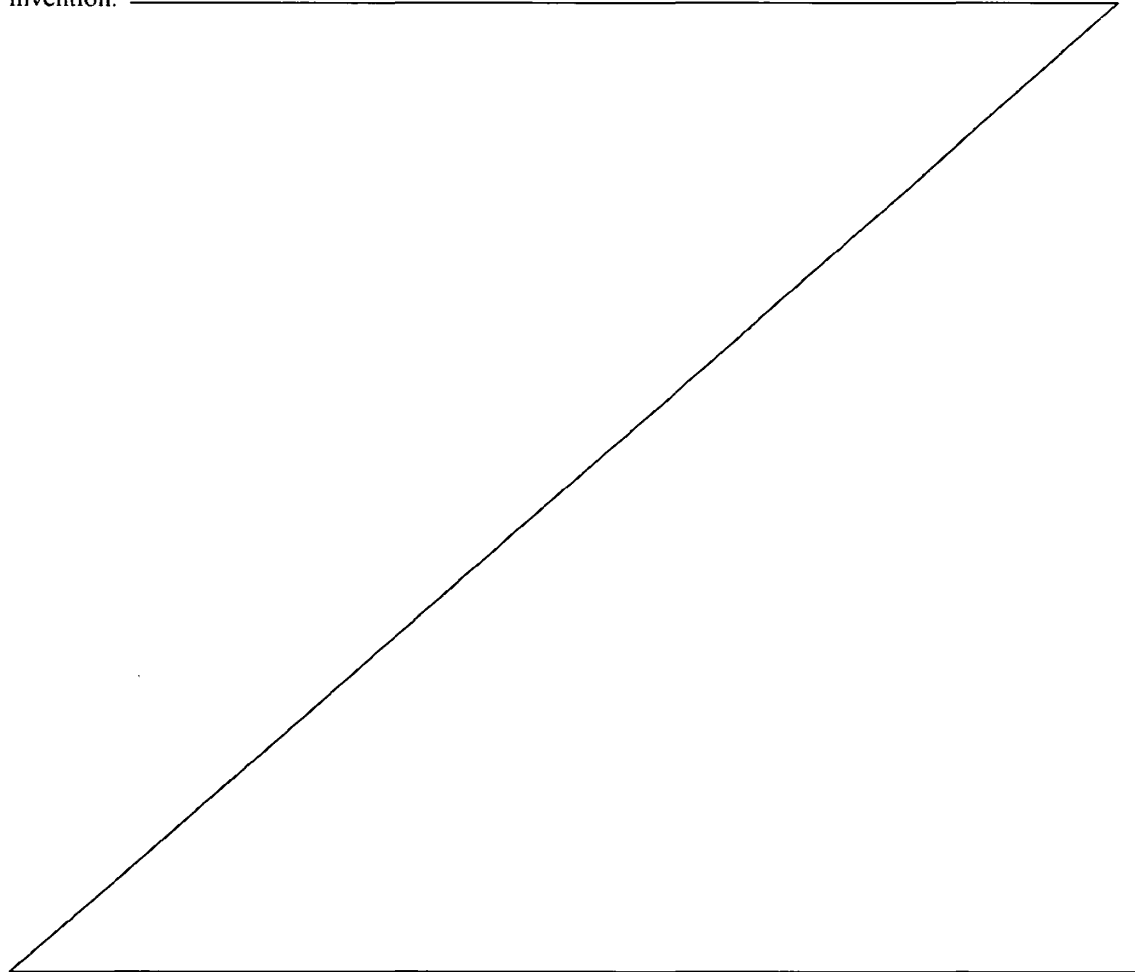
**BRIEF DESCRIPTION OF THE DRAWINGS**

[0014] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims. Component parts shown in the drawings are not necessarily to scale, and may be exaggerated to better illustrate the important features of the invention. In the drawings, like reference numerals may designate like parts throughout the different views, wherein:

[0015] FIG. 1 is a block diagram showing an audio transceiving computing device transmitting data to an audio receiving computing device in accordance with one embodiment of the present invention.

[0016] FIG. 2 is a block diagram showing functional components that make up an audio transceiving computing device according to an embodiment of the present invention.

[0017] FIG. 3 depicts a periodic enclosed content message according to an embodiment of the present invention.



2012100462 03 Jul 2012

**[0078]** In another example, where secure information is large or requires additional security, it may be stored at a remote location from the audio transceiver computing device. Once multiples layers of authentication have occurred for the user or the audio transceiver computing device, or both, the audio receiver computing device can directly access, indirectly access, or receive the secure information from the remote location. Of course, such examples are only exemplary and are non-limiting as the quantity, manner, and amount of information stored remotely from the audio transceiver computing device can be varied as desired. This can also vary how the near field authentication of sources using audio waves can be used in conjunction with the conventional online transaction.

**[0079]** Exemplary embodiments of the invention have been disclosed in an illustrative style. Accordingly, the terminology employed throughout should be read in an exemplary rather than a limiting manner. Although minor modifications to the teachings herein will occur to those well versed in the art, it shall be understood that what is intended to be circumscribed within the scope of the patent warranted hereon are all such embodiments that reasonably fall within the scope of the advancement to the art hereby contributed, and that that scope shall not be restricted, except in light of the appended claims and their equivalents.

**[0080]** The reference to any prior art in this specification is not, and should not be taken as, an acknowledgement of any form of suggestion that such prior art forms part of the common general knowledge.

**[0081]** It will be understood that the term “comprise” and any of its derivatives (eg. comprises, comprising) as used in this specification is to be taken to be inclusive of features to which it refers, and is not meant to exclude the presence of any additional features unless otherwise stated or implied.



## THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for near field authentication of sources using an audio transceiver computing device comprising:
  - scanning a plurality of predetermined frequencies for a free frequency;
  - selecting the free frequency from the plurality of predetermined frequencies;
  - generating a periodic enclosed content message;
  - generating a modulated carrier wave representing the periodic enclosed content message;and
  - transmitting the modulated carrier wave at the free frequency;
  - wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and
  - wherein the content includes at least one of biometric data, or device identification data.
2. The method of claim 1 further comprising:
  - displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and
  - responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.
3. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.
4. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.
5. The method of any one of claims 1 to 4 wherein the modulated carrier wave comprises a sound wave.

2012100462 03 Jul 2012



US005239648A

**United States Patent** [19]  
**Nukui**

[11] **Patent Number:** **5,239,648**  
[45] **Date of Patent:** **Aug. 24, 1993**

- [54] **COMPUTER NETWORK CAPABLE OF ACCESSING FILE REMOTELY BETWEEN COMPUTER SYSTEMS**
- [75] **Inventor:** Harumi Nukui, Kanagawa, Japan
- [73] **Assignee:** Kabushiki Kaisha Toshiba, Kanagawa, Japan
- [21] **Appl. No.:** 762,456
- [22] **Filed:** Sep. 19, 1991
- [30] **Foreign Application Priority Data**  
Sep. 21, 1990 [JP] Japan ..... 2-252864
- [51] **Int. Cl.<sup>5</sup>** ..... H04L 9/00; G06F 12/14
- [52] **U.S. Cl.** ..... 395/600; 380/4; 380/25; 364/286.5; 364/222.5; 364/242.94; 364/DIG. 1
- [58] **Field of Search** ..... 395/725, 575, 425, 200, 395/325, 600; 380/4, 25, 49, 23; 235/380, 382; 340/825.31, 825.34; 379/95

*Symposium on Security and Privacy*, Apr. 7-9, 1986, Oakland, California, pp. 204-222.  
Paul A. Karger, "Authentication and Discretionary Access Control in Computer Networks", *8246 Computers & Security* 5 (1986) Dec., No. 4, Amsterdam, The Netherlands, pp. 314-324.  
Ching-Yi Wang et al., "Access Control in a Heterogeneous Distributed Database Management System", *Sixth Symposium on Reliability in Distributed Software and Database Systems*, pp. 84-92.

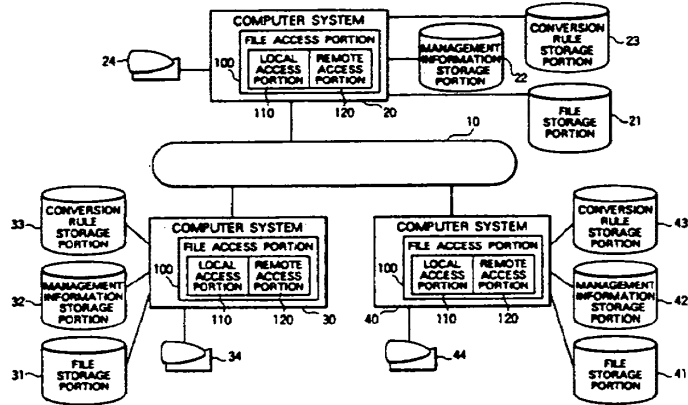
**Primary Examiner**—Michael R. Fleming  
**Assistant Examiner**—Gopal C. Ray  
**Attorney, Agent, or Firm**—Finnegan, Henderson, Farabow, Garrett & Dunner

[57] **ABSTRACT**  
Each computer system of the computer network according to the present invention has a management information storage portion for storing information with respect to an access authority in accordance with an owner ID and a conversion rule storage portion for storing a rule for converting the formats of a user ID and an access authority. Each computer system adds a machine ID to a user ID and sends the resultant ID to another computer system when a remote access request is issued. In addition, the computer system determines whether or not the formats of the user ID and the access authority being received accord with those of a local computer system when a remote access is accepted. The computer system converts the formats of the user ID and the access authority being received into those of the local computer system in accordance with a predetermined conversion rule when the formats of the local computer system are not matched with those on the remote computer system. Thereafter, the computer system compares the user ID and the access authority whose formats have been converted with information of the access authority stored in the access authority storage portion and determines whether or not to execute the remote access.

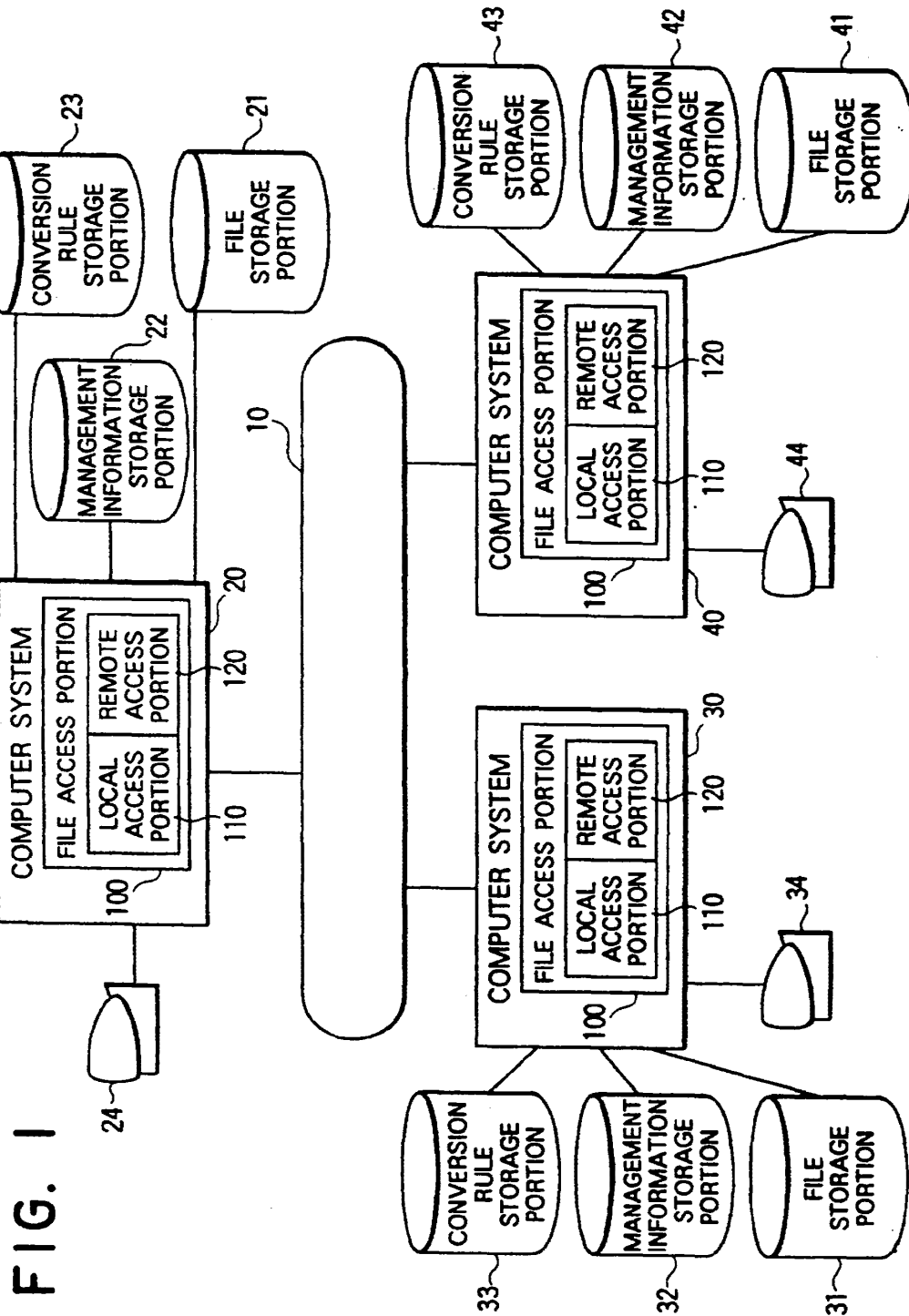
- [56] **References Cited**
- U.S. PATENT DOCUMENTS**
- 4,135,240 1/1979 Ritchie ..... 364/200
- 4,218,738 8/1980 Matyas et al. .... 364/200
- 4,531,023 7/1985 Levine ..... 179/2 R
- 4,825,354 4/1989 Agrawal et al. .... 364/200
- 4,962,449 10/1990 Schlesinger ..... 364/200
- 5,012,515 4/1991 McVitie ..... 380/49
- 5,032,979 7/1991 Hecht et al. .... 364/200
- 5,050,207 9/1991 Hitchcock ..... 379/96
- 5,060,263 10/1991 Bosen et al. .... 380/25
- 5,101,373 3/1992 Tanioka et al. .... 364/900
- 5,133,053 7/1992 Johnson et al. .... 395/200

**OTHER PUBLICATIONS**  
R. Reinauer, "UNIX System V. 3 Remote File Sharing Capabilities and Administration", Unisphere, Sep. 1986 pp. 64-69.  
A. Osadzinski, "Remote File Access", *Systems International* (Jul. 1986), vol. 14, No. 7, pp. 51 & 54, Networking.  
D. M. Nessett, "Factors Affecting Distributed System Security", Lawrence Livermore National Laboratory, Livermore, CA 94550, *Proceedings of the 1986 IEEE*

12 Claims, 6 Drawing Sheets

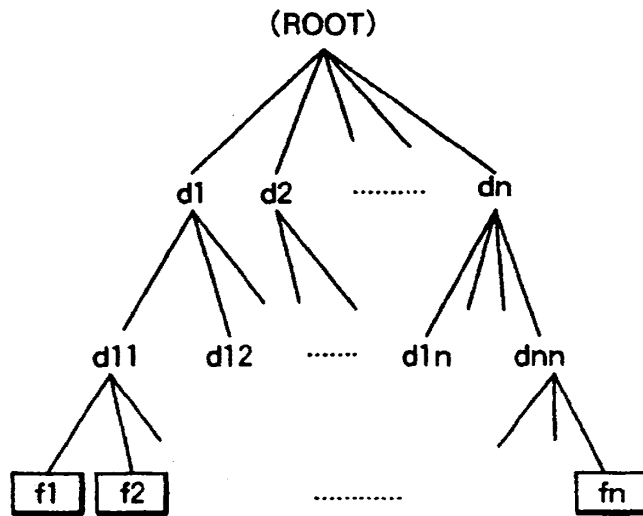


This data, for application number 2012100462, is current as of 2012-12-28 22:09 AEST

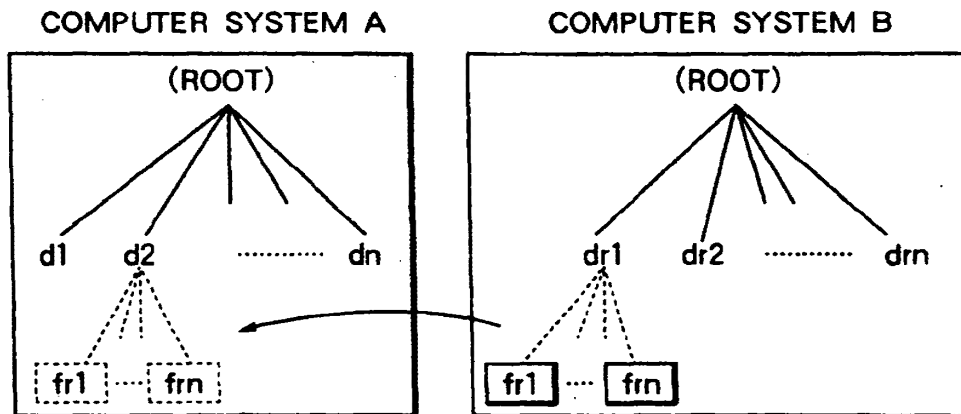


2012100462 03 Jul 2012

# FIG. 2



# FIG. 3



2012100462 03 Jul 2012

FIG. 4

ACCESS AUTHORITY ID	READ	WRITE	EXECUTE	MOVE	DELETE
OWNER PERSONAL	○	○	○	○	○
OWNER GROUP	-	○	-	○	○
OTHER	-	○	-	-	-

○ REPRESENTS PRESENCE OF AUTHORITY.

FIG. 5

A \ B	READ	WRITE	EXECUTE	MOVE	DELETE
READ	○	-	-	-	-
WRITE	-	○	-	○	○
EXECUTE	-	-	○	-	-

2012100462 03 Jul 2012

FIG. 6

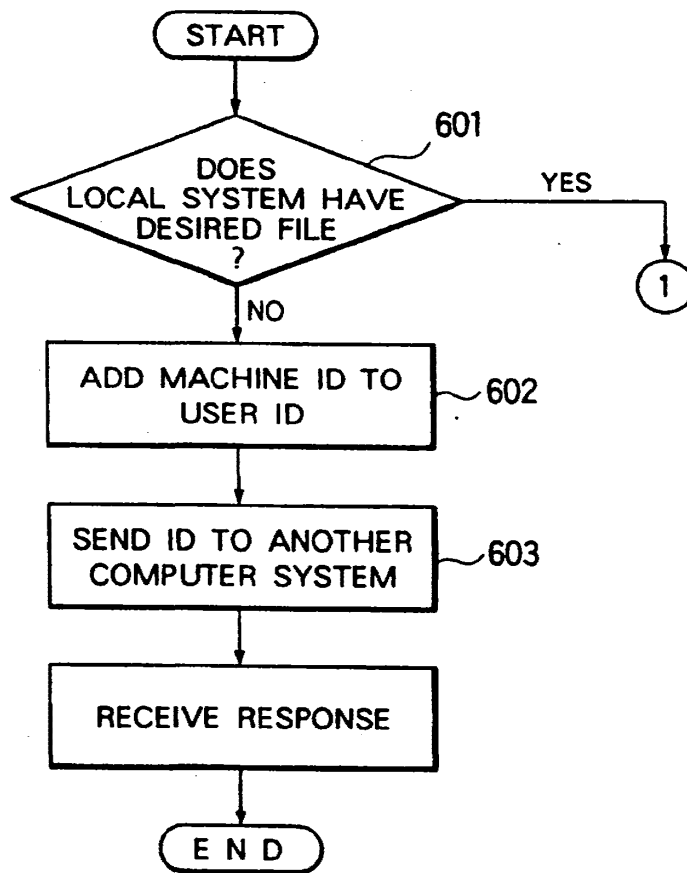
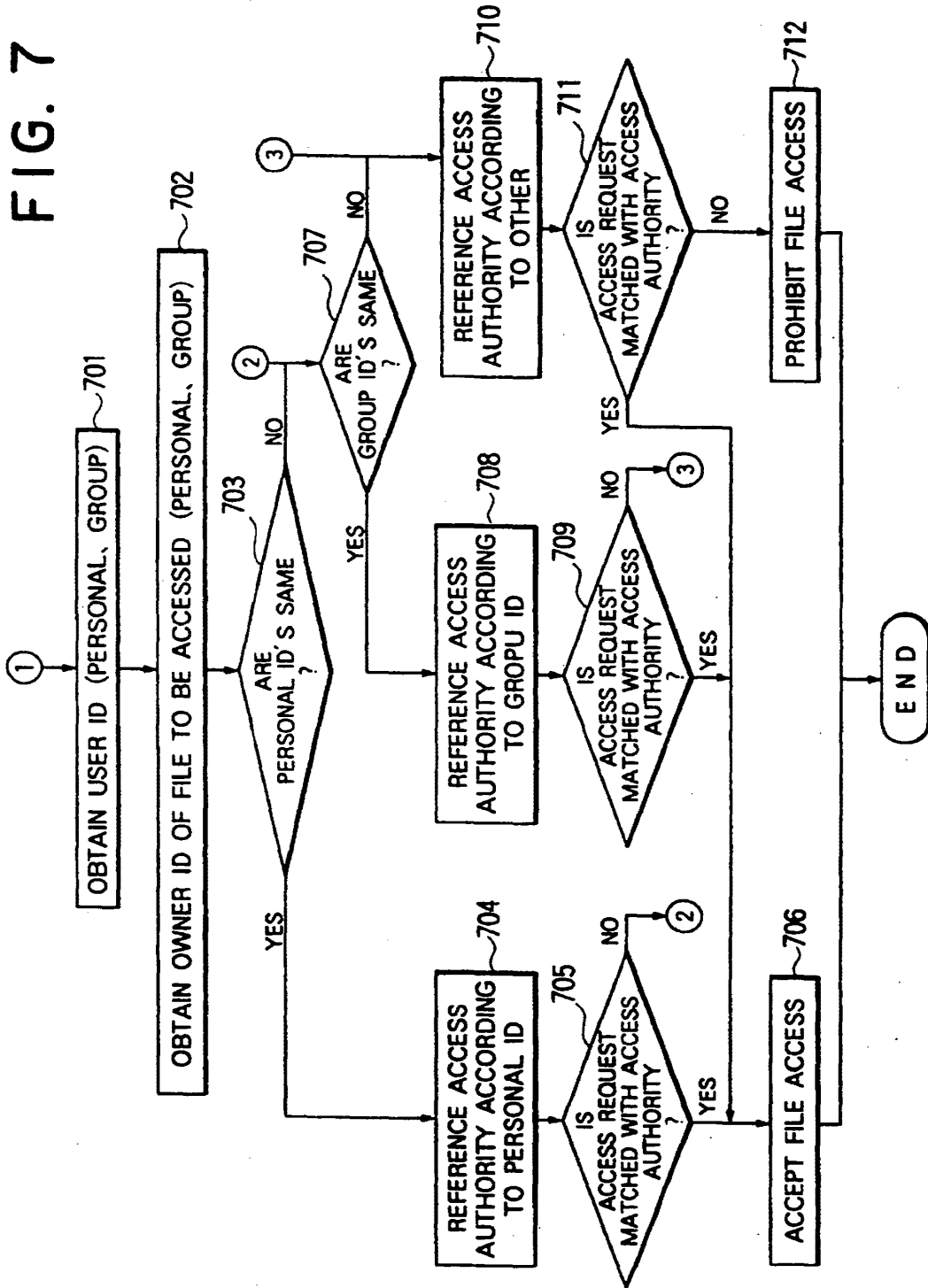
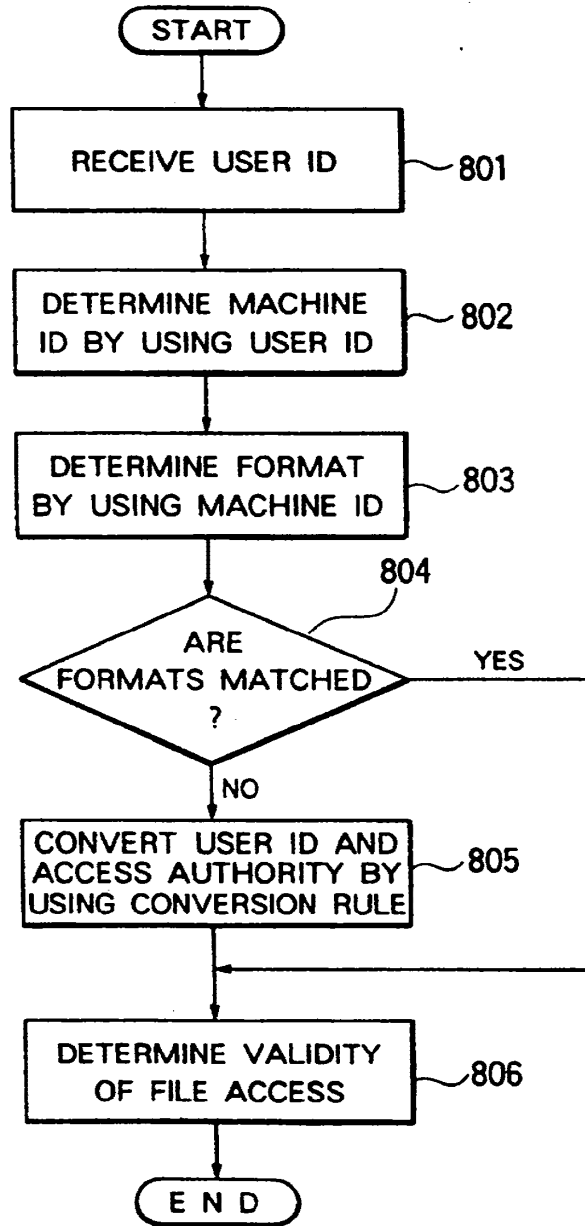


FIG. 7



2012100462 03 Jul 2012

# FIG. 8





2012100462 03 Jul 2012

COMPUTER NETWORK CAPABLE OF ACCESSING FILE REMOTELY BETWEEN COMPUTER SYSTEMS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a computer network for connecting a plurality of computer systems through a communication medium and a method of accessing files thereof.

2. Description of the Related Art

Thus far, there has been a computer network where the user of a computer system can remotely access a file that another computer system has without necessity of a complicated log-on procedure.

The file access in such a computer network is performed under condition that a user ID and an access authority on the request side are matched with those on the accept side.

However, when the computer type on the request side differs from that on the accept side, because of differences of the formats of the user ID and the access authority, the computer system on the access accept side may not correctly determine the validity of an access request from the computer system on the access request side. In this case, the computer system on the request side has to perform a particular procedure so as to validly access a file that the computer system on the accept side has. Thus, the advantage of the remote access is lost.

SUMMARY OF THE INVENTION

Therefore, an object of the present invention is to provide a computer network for validly performing a remote access of files even if the formats of the user ID and the access authority on the access request side differ from those on the access accept side.

To accomplish such an object, the computer network according to the present invention comprises a computer network connected with a plurality of computer systems through a communication medium for accessing files that the plurality of computer systems have from all of the plurality of computer systems, each of the plurality of computer systems comprising access authority information storage means for storing information with respect to an access authority in accordance with an owner ID, means for adding a machine ID to a user ID and for sending the resultant ID to another computer system of the plurality of computer systems when a remote access request is issued, means for determining whether or not the formats of the user ID and the access authority being received accord with those of a local computer system of the plurality of computer systems when a remote access is accepted, means for converting the formats of the user ID and the access authority being received into those of the local computer system of the plurality of computer systems in accordance with a predetermined conversion rule when the formats of the local computer system are not matched with those on the remote computer system, and means for comparing the user ID and the access authority whose formats have been converted with information of the access authority stored in the access authority storage means and for determining whether or not to execute the remote access.

Thereby, according to the present invention, even if the formats of the user ID and the access authority on

the access request side differ from those on the access accept side, remote files can be validly accessed.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a block diagram showing an overall construction of a computer network of an embodiment according to the present invention;

FIG. 2 is a schema showing a tree construction of a file group that a computer system has;

FIG. 3 is a schema describing relations of file groups that two computer systems have;

FIG. 4 is a table outlining information with respect to access authority;

FIG. 5 is a table outlining a conversion rule;

FIG. 6 is a flow chart showing a flow of a process for issuing an access request;

FIG. 7 is a flow chart showing a flow of a process for determining the validity of a file access; and

FIG. 8 is a flow chart showing a flow of a process performed when a remote access request is accepted.

DESCRIPTION OF PREFERRED EMBODIMENT

FIG. 1 is a block diagram showing an overall construction of a computer network of an embodiment according to the present invention.

In the FIGURE, reference numeral 10 is a communication medium. Reference numerals 20, 30, and 40 are computer systems which are connected each other through the communication medium 10. The computer system 20, 30, 40 is connected with a file storage portion 21, 31, 41 for storing a plurality of files, a management information storage portion 22, 32, 42 for storing information necessary for managing a file access, a conversion rule storage portion 23, 33, 43 for storing a conversion rule for compensating differences of the formats of a user ID and an access authority in accordance with a computer type, and a keyboard/CRT 24, 34, 44.

The management information storage portion 22, 32, 42 stores a path to each file stored in the file storage portion 21, 31, 41. A file group stored in the file storage portion 21, 31, 41 is identified by a path which is routed from "ROOT" disposed at the top of the tree construction to a directory d. Thus, the path to a file fl is represented with "/d1/d11/fl/."

In this computer network, files that other computer systems have can be treated as those that a particular computer system has. For example, assume that two computer systems have respective file groups in a tree construction as shown in FIG. 3. In such a construction, the operator of one computer system A declares that the directory d2 is the same as the directory dr1 between the tree construction of the file group which the computer system A has and that which the computer system B has. Thus, the computer system A can treat a sub file group in the directory dr1 or below of a file group that the computer system B has as a file group in the directory d2 or below that the computer system A has.

The management information storage portion 22, 32, 42 stores information with respect to access authority of each file as information for determining the validity of executing a file access.

FIG. 4 is a table outlining information with respect to access authority. In other words, the information with respect to access authority is composed of an owner ID (a personal ID and a group ID) of each file and an

2012100462 03 Jul 2012

3

4

access authority type (for example, read, write, delete, move, and execute) permitted to the owner ID.

In addition, the management information storage portion 22, 32, 42 stores a user ID (a personal ID and a group ID) which is used to request a file access.

In such a construction, a problem takes place when the format of the access authority on the access request side differs from that on the access accept side due to difference of computer types and the like therebetween. For example, when the access authority of one computer system and that of another computer system are set with respect to five types "read, write, delete, move, and execute" and three types "read, write, and execution", respectively, since the access authority on one side does not match that on another side, a file access cannot be validly performed.

To prevent that, in the embodiment according to the present invention, the conversion rule storage portion 23, 33, 34 stores a conversion rule. FIG. 5 shows a table outlining a conversion rule with respect to the access authority. In other words, in the conversion rule, the access request types "delete and move" issued from the computer system B to the computer system A are substituted into the access authority type "write" by the computer system A.

In addition, the conversion rule storage portion 23, 33, 43 also stores another conversion rule for compensating a difference between the format of the user ID on one side and that on the other side.

For example, assume that the user ID is represented with 16 bits in the computer system A and with 32 bits in the computer system B. In this case, as the conversion rule that the computer system A has, a data mapping rule with respect to an ID reading memory area for treating 32 bit data as 16 bit data is defined, while as another conversion rule that the computer system B has, another mapping rule for treating 16 bit data as 32 bit data is defined.

A file access portion 100 of the computer system 20, 30, 40 is functionally categorized as a local access portion 110 for executing a file access in a local computer system and a remote access portion 120 for executing a remote file access with another computer system.

Then, with reference to FIGS. 6 to 8, a file access operation in the computer network according to the present invention will be described.

As shown in FIG. 6, when the computer system 20 issues a file access request, the file access portion 100 looks into the presence of a desired file in the file storage portion 21 thereof in accordance with information stored in the management information storage portion 22 (in the step 601).

When the file access portion 100 found the desired file in the local computer system 20, it obtains a personal user ID and a group user ID from the management information storage portion 22 as shown in FIG. 7 (in the step 701).

Thereafter, the file access portion 100 looks into an owner ID (a personal ID and a group ID) stored in the management information storage portion 22 (in the step 702).

Thereafter, the file access portion 100 compares the personal ID of the user ID with that of the owner ID (in the step 703). When they are matched, the file access portion 100 references the access authority in accordance with the owner personal ID (in the step 704).

Thereafter, the file access portion 100 looks into the presence of the type of the real access request which is

matched with one of the types of the access authority being referenced (in the step 705). When the file access portion 100 found the type of the access authority which was matched, it accepts the file access (in the step 706).

When the file access portion 100 could find the type of the access authority which was matched or when it found that the personal ID of the user ID did not accord with that of the owner ID, it compares the group ID of the user ID with that of the owner ID (in the step 707).

When the group ID of the user ID is matched with that of the owner ID, the file access portion 100 references the access authority in accordance with the owner group ID (in the step 708).

Thereafter, the file access portion 100 looks into the presence of the type of the real access request which is matched with one of the types of the access authority being referenced (in the step 709). When the file access portion 100 found the type of the access authority which was matched, it accepts the file access (in the step 706).

When the file access portion 100 could not find the type of the access authority which was matched or when it found that the personal ID of the user ID did not accord with that of the owner ID in the step 707, it references another type of the access authority (in the step 710).

Thereafter, the file access portion 100 looks into the presence of the type of the real access request which is matched with one of the types of the access authority being referenced (in the step 711). When the file access portion 100 found the type of the access authority which was matched, it accepts the file access (in the step 706). When the file access portion 100 could not find the type of the access authority which was matched, it prohibits the file access (in the step 712).

When the file access portion 100 determined that the desired file was present in another computer system 30, 40 in the step 601, it adds a machine ID of the local computer system 20 to the user ID (the personal ID and the group ID) in the management information storage portion 22 (in the step 602) and then sends them to another computer system 30, 40 so as to issue a remote access request (in the step 603). Thereafter, the file access portion 100 enters a standby state for waiting for a response from the other computer system 30, 40.

The file access portion 100 of the other computer system 30, 40 which accepted the remote access request receives the user ID (in the step 801) and looks into the machine ID from the user ID being received (in the step 802).

Thereafter, the file access portion 100 determines the formats of the user ID and the access authority in accordance with the machine ID (in the step 803).

Thereafter, the file access portion 100 determines whether or not the formats being determined are matched with those of the local computer system (in the step 804).

When the file access portion 100 determined that the formats were not matched, it converts the formats of the user ID and the access authority stored in the conversion rule storage portion 33, 43 into those of the local computer system 30, 40 (in the step 805).

Thereafter, the file access portion 100 determines whether or not to accept the file access in the procedure shown in FIG. 7 in accordance with the user ID and the access authority where their formats have been converted (in the step 806).

2012100462 03 Jul 2012

5

Thus, according to the computer network of the present invention, even if the formats of the user ID and the access authority of one computer system 20, 30, 40 differ from those of the other computer system 20, 30, 40, by compensating the differences with the conversion rules, a remote file access can be validly performed without necessity of a special procedure.

What is claimed is:

1. A computer network, where a plurality of computer systems are connected through a communication medium, each computer system being capable of accessing files of another computer system, each computer system being given a specific machine ID, each computer system having set kinds of file operations per file, each file being given a specific file ID, and a format of the file ID being set per computer system, comprising:

- a computer system accessing the file, including
  - means for adding the machine ID to the file ID of the requested file when access to the file of another computer system is requested; and
  - means for sending the file ID and the added machine ID to the other computer system; and
- a computer system whose the file is accessed, including
  - a first table storing correspondence relationships between the kinds of file operations in the computer accessing the file, and the kinds of file operations in the computer whose the file is accessed;
  - a second table storing correspondence relationships between the format of the file ID in the computer accessing the file, and the format of the file ID in the computer whose the file is accessed;
  - a third table storing the file ID and the kinds of capable operations per file;
  - means for receiving the file ID and the added machine ID from the computer system accessing the file;
  - means for discriminating the computer system whose file is accessed based on the machine ID received by the receiving means;
  - first determination means for determining whether the kinds of file operations of the discriminated computer system coincide with the kinds of file operations of the computer system whose file is accessed;
  - first conversion means for, when the kinds of the two computer systems do not coincide with each other, converting the kinds of file operations system to the kinds of file operations of the computer system whose file is accessed in accordance with the first table;
  - second determination means for determining whether the format of the file ID of the discriminated computer system coincides with the format of the file ID of the computer system whose file is accessed;
  - second conversion means for, when the formats of the two computer systems do not coincide with each other, converting the format of the file ID system to the format of the file ID of the computer system whose file is accessed in accordance with the second table; and
  - means for judging whether the requested access is allowed based on comparison of the converted file ID and the converted kinds of file operations

6

with the file ID and the kinds of file operation stored in the third table.

2. The computer system of claim 1, the computer system accessing the file, further including:

- means for determining whether the file, to which access is requested, exists in the computer system accessing the file; and for, when the file does not exist, sending the file ID and the added machine ID to the other computer machine by the sending means.

3. The computer system of claim 1, wherein the kinds of file operations are reading, writing, deleting, moving, and executing a file.

4. The computer system of claim 1, wherein a difference in the format of file ID is a difference in the number of bits per frame.

5. A computer network, where a plurality of computer systems are connected through a communication medium, each computer system being capable of accessing files of another computer system, each computer system being given a specific machine ID, each computer system having set kinds of file operations per file, each file being given a specific file ID, comprising:

- a computer system accessing the file, including
  - means for adding the machine ID to the file ID of the requested file when access to the file of another computer system is requested; and
  - means for sending the file ID and the added machine ID to the other computer system; and
- a computer system whose the file is accessed, including
  - a first table storing correspondence relationships between the kinds of file operations in the computer accessing the file, and the kinds of file operations in the computer whose file is accessed;
  - a second table storing the file ID and the kinds of capable operations per file;
  - means for receiving the file ID and the added machine ID from the computer system accessing the file;
  - means for discriminating the computer system whose file is accessed based on the machine ID received by the receiving means;
  - means for determining whether the kinds of file operations of the discriminated computer system coincide with the kinds of file operations of the computer system whose the file is accessed;
  - means for, when the kinds of the two computer systems do not coincide with each other, converting the kinds of file operations to the kinds of file operations so the computer system whose file is accessed in a accordance with the first table; and
  - means for judging whether the requested access is allowed based on comparison of the converted kinds of file operations and the sent file ID with the file ID and the kinds of file operations stored in the second table.

6. The computer system of claim 5, wherein the computer system accessing the file, further includes

- means for determining whether the file, to which access is requested, exists in the computer system accessing the file; and for, when the file does not exist, sending the file ID and the added machine ID to the other computer machine by the sending means.

7

7. The computer system of claim 5, wherein the kinds of file operations are reading, writing, deleting, moving, and executing a file.

8. A computer network, where a plurality of computer systems are connected through a communication medium, each computer system being capable of accessing files of another computer system, each computer system being given a specific machine ID, each file being given a specific file ID, a format of the file ID being set per computer system, comprising:

- a computer system accessing the file, including means for adding the machine ID to the file ID of the requested file when access to the file of another computer system is requested; and
- means for sending the file ID and the added machine ID to the other computer system; and
- a computer system whose file is accessed, including a first table storing correspondence relationships between the format of the file ID in the computer accessing the file, and the format of the file ID in the computer whose file is accessed;
- a second table storing the file ID per file;
- means for receiving the file ID and the added machine ID from the computer system accessing the file;
- means for discriminating the computer system whose file is accessed based on the machine ID received by the receiving means;
- means for determining whether the format of the file ID of the discriminated computer system coincides with the format of the file ID of the computer system whose file is accessed;
- means for, when the formats of the two computer systems do not coincide with each other, converting the format of the file ID to the format of the file ID of the computer system whose file is accessed in accordance with the first table; and
- means for judging whether the requested access is allowed based on comparison of the converted file ID with the file ID stored in the second table.

9. The computer system of claim 8, wherein the computer system accessing the file, further includes means for determining whether the file, to which access is requested, exists in the computer system accessing the file; and for, when the file does not exist, sending the file ID and the added machine ID to the other computer machine by the sending means.

10. The computer system of claim 8, wherein a difference in the format of file ID is a difference in the number of bits per frame.

11. A method for accessing a file in a computer network, where a plurality of computer systems are connected through a communication medium, each computer system being capable of accessing files of another computer system, each computer system being given a specific machine ID, each computer system being set kinds of file operations per file, each file being given a

8

specific file ID, a format of the file ID being set per computer system, comprising the steps of:

- in the computer system accessing the file, adding the machine ID to the file ID of the requested file when access to the file of another computer system is requested; and
- sending the file ID and the added machine ID to the other computer system; and

in the computer system whose file is accessed, having a first table storing correspondence relationships between the kinds of file operations in the computer accessing the file, and the kinds of file operations in the computer whose file is accessed; a second table storing correspondence relationships between the format of the file ID in the computer accessing the file, and the format of the file ID in the computer whose file is accessed; and a third table storing the file ID and the kinds of capable operations per file,

- receiving the file ID and the added machine ID from the computer system accessing the file;
- discriminating the computer system whose file is accessed based on the machine ID received by the receiving means;
- determining whether the kinds of file operations of the discriminated computer system coincide with the kinds of file operations of the computer system whose file is accessed;
- converting the kinds of file operations of the discriminated computer system to the kinds of file operations of the computer system whose file is accessed in accordance with the first table, when the kinds of the two computer systems do not coincide with each other;
- determining whether the format of the file ID of the discriminated computer system coincides with the format of the file ID of the computer system whose file is accessed;
- converting the format of the file ID system to the format of the file ID of the computer system whose file is accessed in accordance with the second table when the formats of the two computers systems do not coincide with each other; and
- judging whether the requested access is allowed based on comparison of the converted file ID and the converted kinds of file operations with the file ID and the kinds of file operations stored in the third table.

12. The method of claim 11, wherein the computer system accessing the file, is the further step of: determining whether the file, to which access is requested, exists in the computer system accessing the file; and for, when the file does not exist, sending the file ID and the added machine ID to another computer machine by the sending means.

\* \* \* \* \*

60

65

2012100462 03 Jul 2012



US005313637A

**United States Patent** [19]  
**Rose**

[11] **Patent Number:** 5,313,637  
[45] **Date of Patent:** May 17, 1994

[54] **METHOD AND APPARATUS FOR VALIDATING AUTHORIZATION TO ACCESS INFORMATION IN AN INFORMATION PROCESSING SYSTEM**

4,652,698 3/1987 Hale et al. .... 902/1 X  
4,713,753 12/1987 Boebert et al. .... 364/200

[76] **Inventor:** David K. Rose, 800 E. Ocean Blvd.  
Apt. #1410, Long Beach, Calif.  
90802

**OTHER PUBLICATIONS**

Horgan, John, "Thwarting the information thieves,"  
*IEEE Spectrum*, Jul. 1985, pp. 30-41.

[21] **Appl. No.:** 807,957

*Primary Examiner*—Paul V. Kulik  
*Attorney, Agent, or Firm*—Stanger, Stempler & Dreyfus

[22] **Filed:** Dec. 10, 1991

[57] **ABSTRACT**

**Related U.S. Application Data**

Access authorization is validated for an information processing system wherein a "slave device" such as a terminal desires access to information contained in or controlled by a "master device" such as a computer. Apparatus associated with the slave device receives validation data from the master device, modifies it according to a pre-determined algorithm implemented through logical circuitry in the apparatus, and returns the resulting "convoluted" data to the master device. The same validation data is convoluted in the master device through mathematical implementation of the algorithm. If the two sets of convoluted data match, it is presumed that the slave device is authorized to access information through the master device.

[63] Continuation of Ser. No. 277,673, Nov. 29, 1988, abandoned.

[51] **Int. Cl.<sup>5</sup>** ..... G06F 13/00

[52] **U.S. Cl.** ..... 395/725; 380/4; 380/28; 340/825.31; 364/DIG. 2; 364/940; 364/942.3; 364/942.4; 364/918.7; 364/949.71

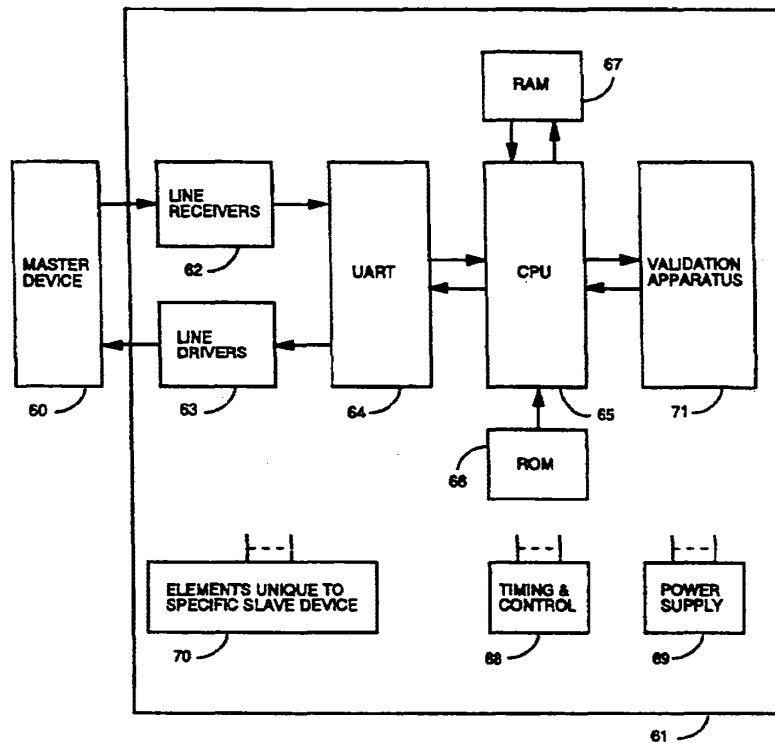
[58] **Field of Search** ..... 380/4, 28; 340/825.3, 340/825.31, 825.34; 902/1, 2; 395/725

[56] **References Cited**

**U.S. PATENT DOCUMENTS**

4,450,535 5/1984 de Pommery et al. .... 364/900  
4,467,139 8/1984 Mollier ..... 902/2 X  
4,601,011 7/1986 Grynberg ..... 364/900

17 Claims, 7 Drawing Sheets



2012100462 03 Jul 2012

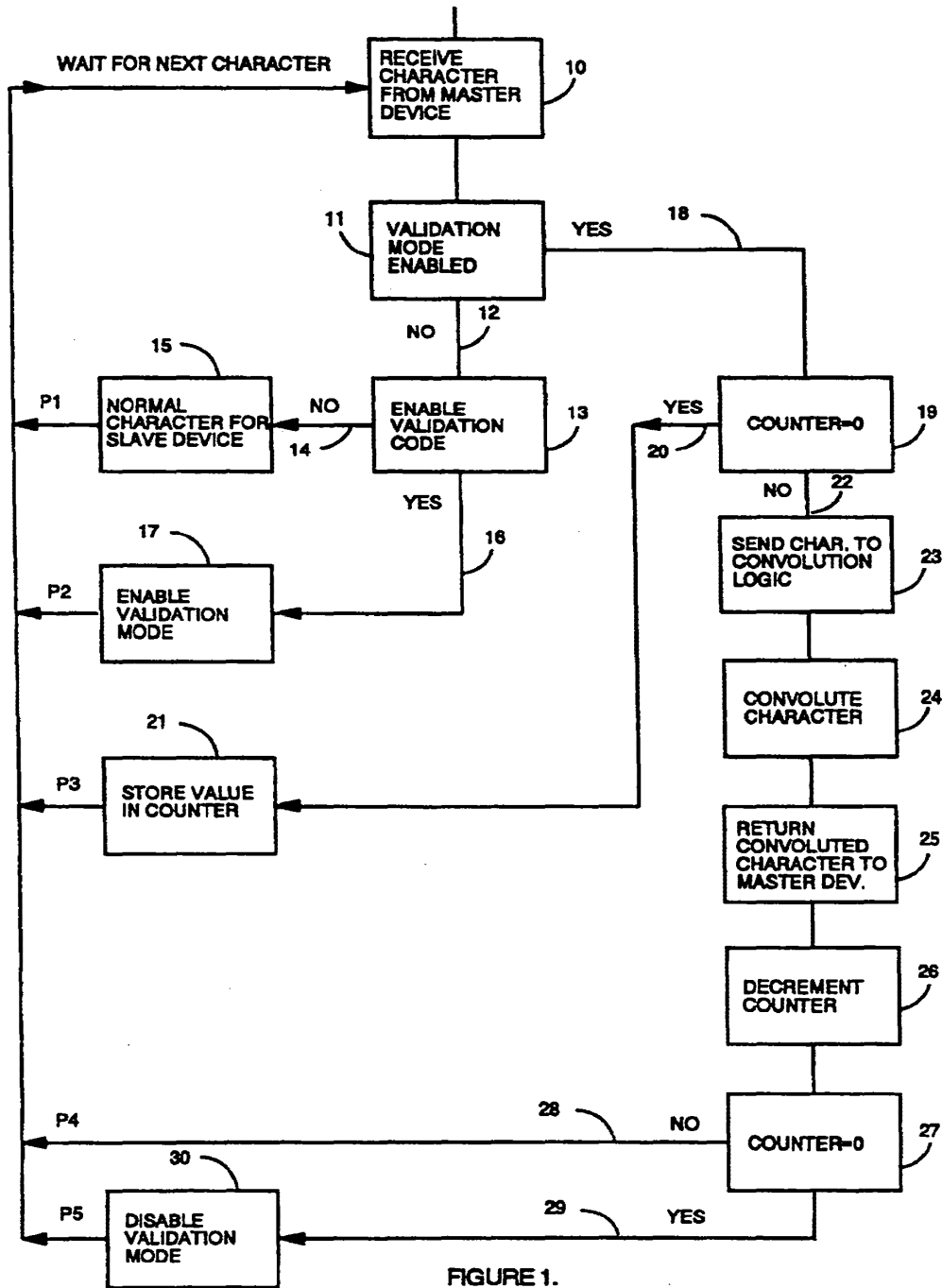


FIGURE 1.

2012100462 03 Jul 2012

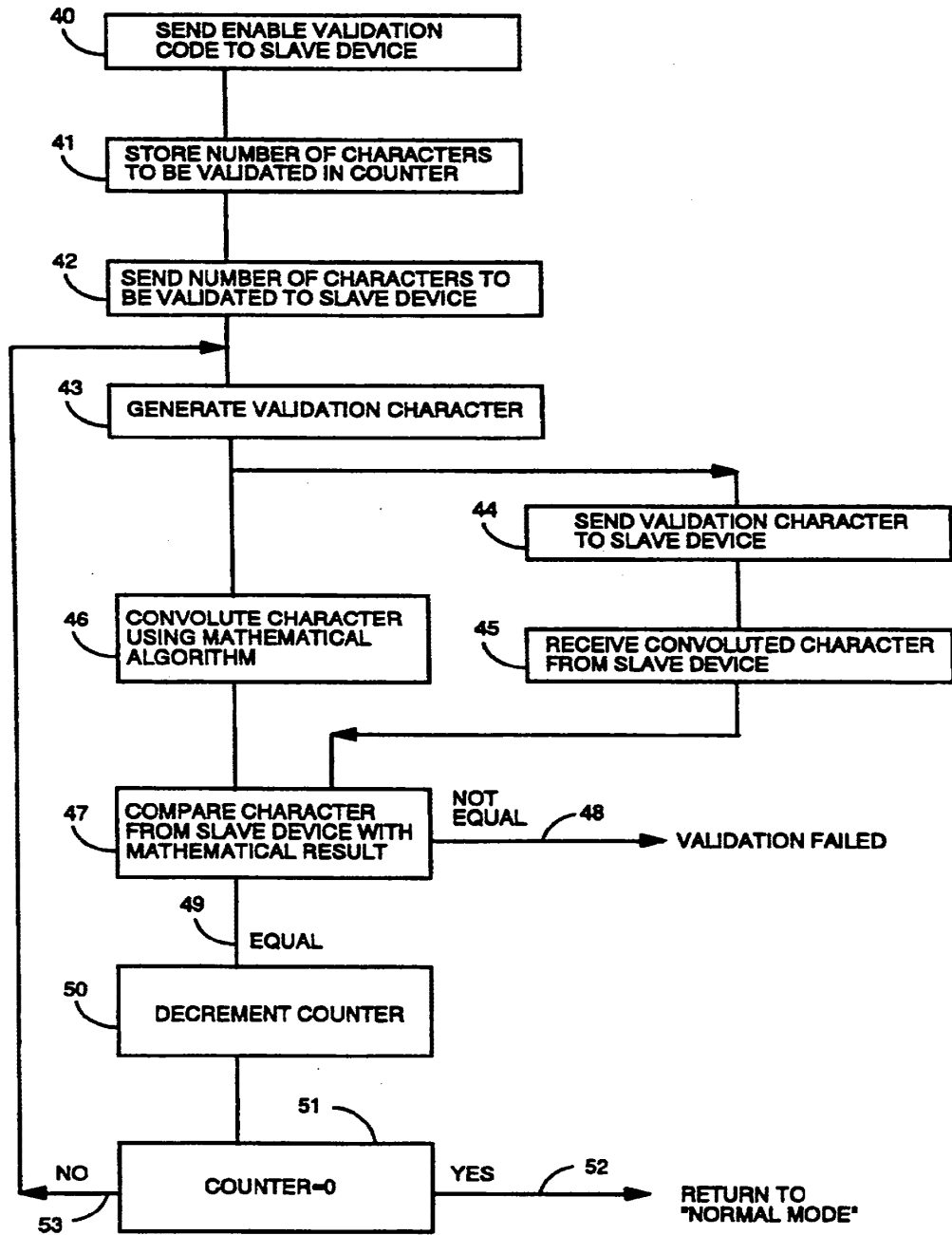


FIGURE 2.

2012100462 03 Jul 2012

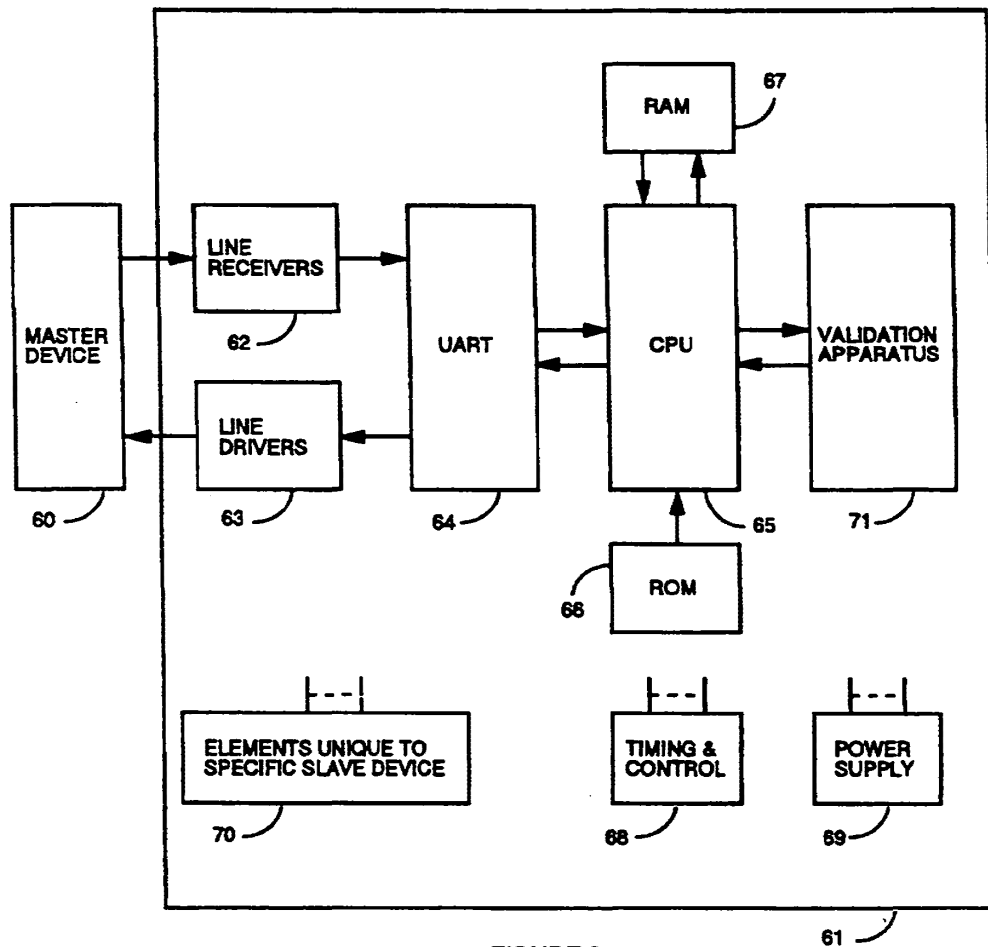


FIGURE 3.



2012100462 03 Jul 2012

2012100462

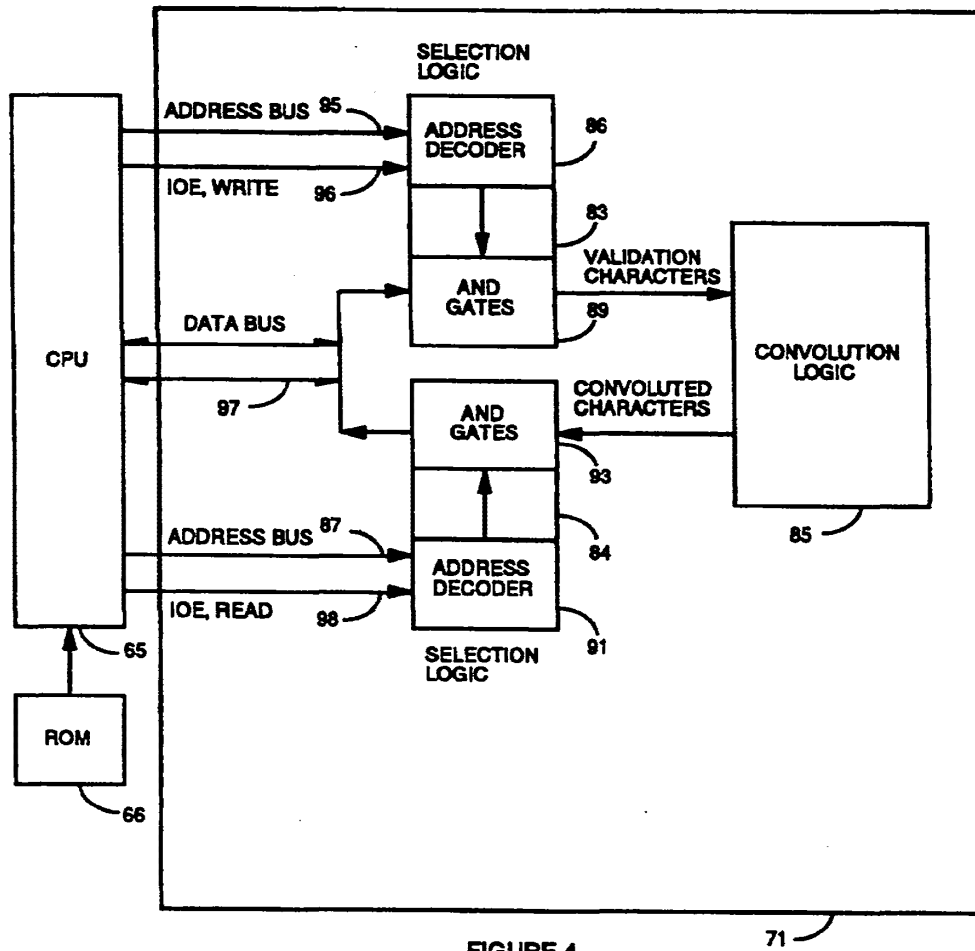


FIGURE 4.

2012100462 03 Jul 2012

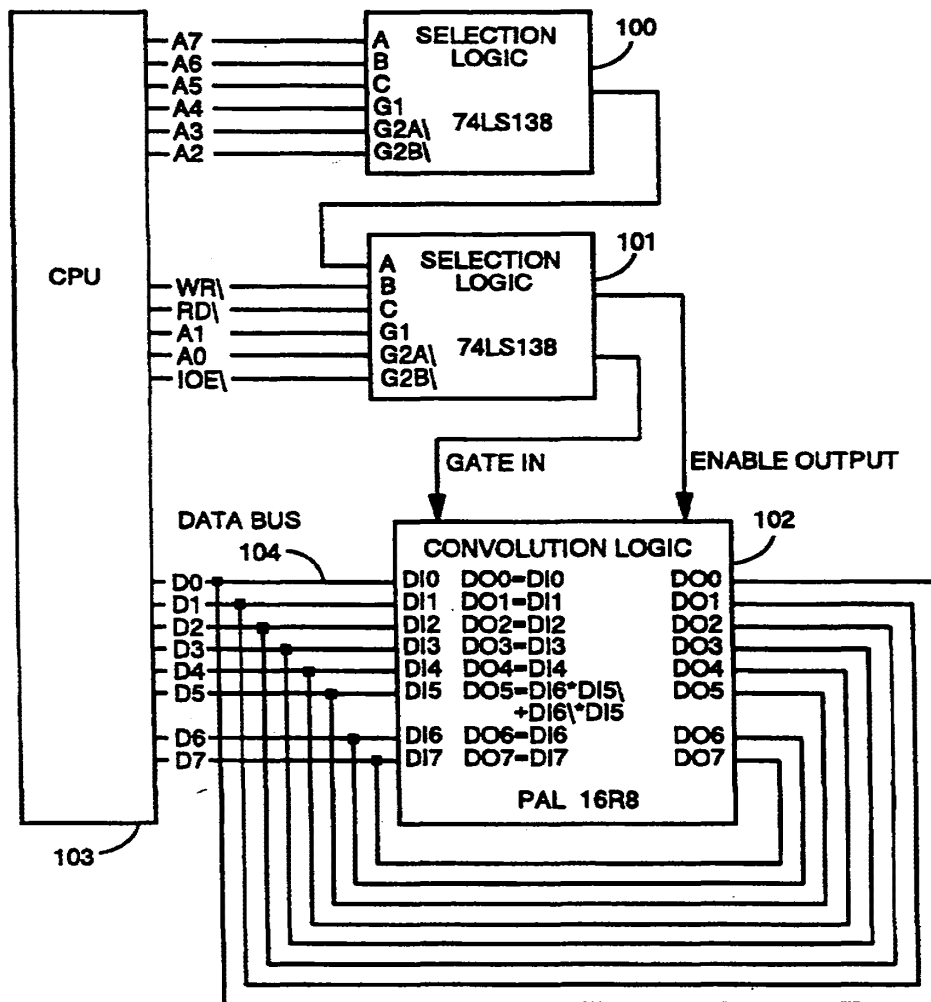


FIGURE 5.

2012100462 03 Jul 2012

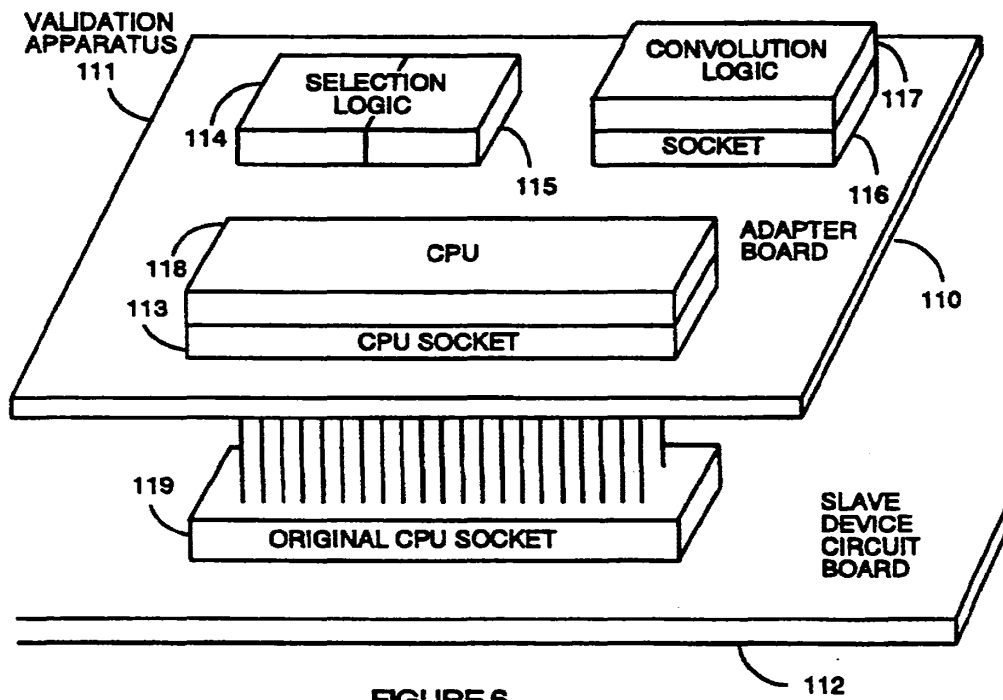


FIGURE 6.

2012100462 03 Jul 2012

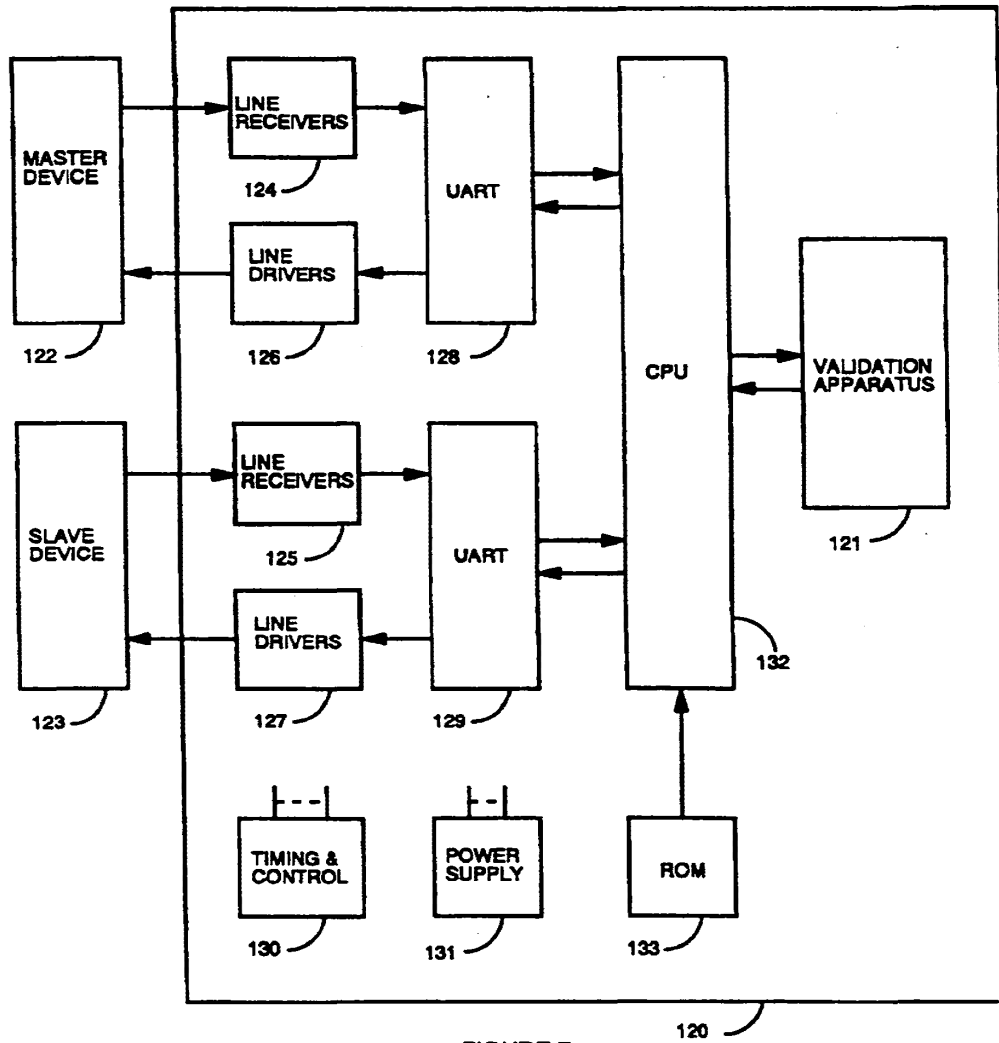


FIGURE 7.

## METHOD AND APPARATUS FOR VALIDATING AUTHORIZATION TO ACCESS INFORMATION IN AN INFORMATION PROCESSING SYSTEM

This is a continuation of application Ser. No. 277,673, filed Nov. 29, 1988 now abandoned.

### FIELD OF THE INVENTION

The present invention relates to the security of information associated with an information processing system. More specifically, it provides a method and apparatus for determining whether a "slave device" is authorized to access data, programs, operations, or other information contained or controlled by a "master device". Typical applications include multi-user computer systems, in which the computer is the master device and peripheral devices such terminals and printers are slave devices, and multi-computer networks, where the computer controlling access to the desired information is the master device and the computer desiring access is the slave device.

### BACKGROUND OF THE INVENTION

Information security is a major concern relating to information processing systems. Many approaches have been conceived to prevent unauthorized access to sensitive, confidential, or proprietary data, programs, or operations.

These approaches range from simple, physical control to complex and highly sophisticated electronic implementations of mathematical techniques. A summary of prior art techniques follows; these are shown in order of generally increasing complexity:

- physical control
  - mechanically locked enclosure or facility
  - key-operated switch
  - user must have proper program or data media
- electronic lock
  - plug-in access module
  - key-pad whose keys must be depressed in specific sequence
- identification
  - computer queries device for electrical identification code
  - user enters personal name, code name, or password
  - access card with magnetic or optical card identification
  - computer verifies user's physical characteristic (e.g., fingerprint, voice, typing pattern)
- transmission coordination
  - transmitting or receiving device signals or requests data transfer
  - receiving device confirms receipt for transmission to continue
- transmission security
  - data encoding: received data must be decoded (e.g., conversion of ASCII codes to alphanumeric characters)
  - data encryption: received data must be decrypted (e.g., character substitution)
  - data scrambling received data must be filtered and re-assembled (e.g., data manipulation and removal of extraneous data)
- Physical control, electronic locks, identification, and transmission coordination restrict access to the devices, data, programs, or operations. Transmission security

does not necessarily preclude access to information, but data is not meaningful unless processed properly.

It has been demonstrated that no single nor combination of approaches or implementations can provide total security; at best, the amount of time, effort, or cost to gain unauthorized access is so great that it provides an effective deterrent.

### BRIEF DESCRIPTION OF THE INVENTION

The present invention is directed at apparatus, method, and system means for determining whether a slave device is authorized to access information such as data, programs, or operations contained in or controlled by a master device. It is applicable to both entry and retrieval of information.

Information processing systems typically include a computer or computer-controlled master device, one or more slave devices physically separate from the master device, and interface links to electronically interconnect the devices. Examples of such systems include time-sharing and multi-user networks where a "host computer" acts as the master device, and local area networks where a "file server" acts as the master device.

- Slave devices include, but are not limited to:
- input devices (keyboards, terminals, card readers, etc.)
  - output devices (printers, plotters, displays, monitors, etc.)
  - storage devices (disk units, tape units, etc.)
  - other computers (work stations, remote computers, etc.)
  - communication devices connected to other slave devices
- The inventive system employs validation apparatus associated with the slave device and validation means associated with the master device. The system has two modes of operation: a "normal" mode and a "validation" mode.

In the normal mode of operation, all information transferred between the master device and the slave device is unaffected; the inventive system is "transparent" to the master device, slave device, user, programs, operations, and data.

In the validation mode, the apparatus receives "validation data" from the master device. This validation data is "convoluted" in accordance with a pre-determined algorithm implemented through electronic logic circuitry in the apparatus, and the resulting "convoluted data" is returned to the master device. The master device contains a mathematical equivalent of the convolution algorithm, used to predict the data to be returned by the apparatus. The master device compares the data returned by the apparatus to the predicted data to validate whether the slave device specifically associated with the apparatus is authorized to access information through the master device.

The master device initiates the validation process by sending a pre-defined "enable validation code" to the apparatus. The master device then sends a number to the apparatus; this defines how much subsequent data is to be convoluted by the apparatus and returned to the master device for validation.

A simple example illustrates the concept and basic operation of the validation process. In this example, the master device is a computer, the slave device is a terminal, the enable validation code is the unique combination of characters XBF, the validation data are the 8

characters abcdefgh, and the convolution algorithm converts upper-case characters to lower-case and vice versa. The computer transmits XBF8abcdefgh to the apparatus; the apparatus should return ABCDefgh to the computer.

If the response from the apparatus matches the predicted response, it is presumed that the terminal specifically associated with the apparatus is authorized to access information in the computer. If the responses do not match, it is presumed that access is not authorized (for instance, if the authorized terminal were replaced by an unauthorized device lacking the validation apparatus). The action to be taken if a validation fails is established by the management of the information processing system and can range from notifying the computer operator to automatic discontinuance of communication between the computer and terminal.

The level of security realized in accordance with the principles of the invention can be enhanced through more sophisticated implementation of the convolution process than illustrated in this example. For instance, the convolution algorithm can be much more complex, and the apparatus can include multiple sets of convolution logic with different algorithms; the algorithm to be used for each set of validation data can be specified by the computer at the start of each validation.

There are also other ways in which the start and length of the validation process can be implemented to further frustrate discovery and circumvention of the validation process. The enable validation code and specification of the number of characters to be convoluted can be "embedded" in apparently normal characters transmitted by the computer. For example, the apparatus can be connected to receive all information transmitted by the computer to the terminal. "Normal" information will pass unchanged to the terminal, and will not affect the apparatus. The validation process in the apparatus can be enabled upon occurrence of a specific bit pattern in any character or set of characters sent by the computer, with the bit pattern of another character or set of characters defining the number of characters to be convoluted.

The computer's program can include a response-time check to determine whether the apparatus has returned convoluted characters within an expected time; if not, it is presumed that the proper apparatus/terminal/computer connection is not intact.

Three basic implementations of the apparatus are possible. The "self-contained" version comprises all circuitry necessary to install the apparatus as an independent unit, typically between the master device and the slave device. This version includes data transmission and reception circuitry, a microprocessor, read-only memory for controlling the microprocessor, the convolution logic, and associated support circuits for power, timing, and control functions.

The "add-on" version takes advantage of elements such as data reception and transmission circuitry, microprocessor, read-only memory, and power, timing, and control circuitry already incorporated in many slave devices. This implementation typically uses an adapter board inserted between the slave device's microprocessor and its socket, with the adapter board containing the convolution logic and circuitry to enable it under control of the microprocessor. The add-on version requires minor changes to the slave device's read-only memory program; these allow the microprocessor to recognize the enable validation code, to

route signals to and from the convolution logic, and to synchronize completion of the validation mode through a character counter.

In the "designed-in" version, the convolution logic and associated signal routing circuitry are incorporated into the design of the slave device. This is similar to the add-on version, but the elements required for the invention are included as part of the slave device's circuitry, rather than on an adapter board.

The present invention offers several unique advantages:

First, logic circuitry, rather than program code stored in read-only memory, is used for implementing convolution algorithms in the invention's apparatus. The contents of virtually all read-only memory elements (PROMs, EPROMs, etc.) can be retrieved—and duplicated—through the use of widely-available, relatively low-cost equipment. The logic circuitry in the apparatus can be encapsulated; attempts to remove encapsulation material typically destroy the circuitry, as well. This circuitry can also be implemented through elements such as programmable logic devices which include a "fusible link" that can be "blown" after programming to prevent retrieval of the logical coding.

Second, the convolution logic can be implemented as plug-in modules, allowing algorithms to be changed at random intervals for increased security.

Third, operation of the invention can be totally "transparent" to the user. The master device can initiate the validation mode at any time, without involving or notifying the user. (In the example above, with the transmission link between the computer and terminal operating at the common data rate of 9600 bits/second, the process for validating a set of 8 characters requires approximately 20 milliseconds. For comparison, keyboard entry averages about 100 milliseconds per character when typing 100 words per minute.)

If desired, however, the operation can be implemented to involve the user. For example, the master device can request the user to enter an access code, with the apparatus convoluting that code before transmitting it to the master device.

Fourth, no changes are required to the master device circuitry to implement a system in accordance with the principles of this invention. Changes are required in the "front end" or device input/output portions of the master device's software; the main information processing routines are not affected.

Fifth, the invention can be used with most existing slave devices, and it can be used alone or in conjunction with most existing data transmission, access, and security techniques. It allows these to operate as at present, but adds or augments security by introducing another level of deterrence to be overcome in gaining unauthorized access.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow diagram of information within the validation apparatus and the slave device with which it is associated in an access authorization system in accordance with the principles of this invention.

FIG. 2 is a flow diagram of information within the master device during the validation process in an access authorization system in accordance with the principles of this invention.

FIG. 3 is a block diagram of a typical slave device, with the validation apparatus of this invention added onto or implemented inside the slave device.

FIG. 4 is a detailed block diagram of an embodiment of the validation apparatus of FIG. 3.

FIG. 5 is a circuit diagram of an embodiment of the validation apparatus of FIG. 4 designed to perform upper-case-to-lower-case and lower-case-to-upper-case convolution.

FIG. 6 illustrates the physical form of an "add-on" implementation of the validation apparatus of FIG. 5, in which an adapter board provides interconnection and mounting for the elements of the validation apparatus.

FIG. 7 is a block diagram of a "self-contained", "serial" implementation of the validation apparatus and required support elements of FIG. 3, in which the apparatus is installed as a unit physically separate from the slave device.

#### DETAILED DESCRIPTION OF EMBODIMENTS OF THIS INVENTION

A typical embodiment of this invention is for use in a system in which the master device is a computer and the slave device is a terminal. The terminal and the computer are connected through a serial data link, with information represented by ASCII character codes. The validation apparatus is "added onto" an existing terminal, and the invention makes use of the terminal's microprocessor, read-only memory, and interface and support circuitry.

FIG. 1 shows the five functional paths for information flow in the validation apparatus and the terminal with which it is associated, in accordance with the principles of this invention.

Path P1 is the "normal" mode of operation, in which information between the computer and terminal is unchanged and unaffected by the invention. In this mode, the invention is "transparent" to the computer, terminal, programs, data, operations, and to the user; all operate as if the invention were not present, and the "validation" mode of the invention is disabled.

During the normal mode of operation, all information received by the terminal from the computer (master device) is monitored, as indicated by block 10. The "validation mode enabled" condition (block 11) is tested after receipt of each character. Since the validation mode is not enabled (line 12), each incoming character is checked to determine if it is an "enable validation code" (Block 13). If the character is not an enable validation code (line 14), the character is processed by the terminal as a "normal" character (block 15).

If an enable validation code is received (line 16), the validation mode of operation is enabled (block 17); this is Path P2. Receipt of an enable validation code also sets the validation mode enabled condition (block 11); this condition remains set (line 18) until it is reset by completion of the validation process, as will be shown below. The enable validation code in this embodiment can be a pre-defined single character or unique combination of characters which would not be transmitted by the computer to the terminal for operations other than to enable the validation mode.

In this embodiment, the numeric value of the next character received from the computer after the enable validation code is used with a "character counter" (block 19) to specify the number of subsequent characters to be used to validate access authorization. A value of zero in the counter (line 20) signifies the start of the validation mode, and the numeric value from the computer is stored in the counter (block 21); (Path P3).

Path P4 represents the operations during the validation mode. With the validation mode enabled (line 18) and the character counter value not zero (line 22), each "validation character" received from the computer is routed (block 23) to the "convolution logic" in the apparatus. The character is altered or "convoluted" by this logic (block 24), and the resultant "convoluted character" is returned to the computer (master device), as indicated by block 25.

After return of the convoluted character, the character counter is decremented (block 26) and tested (block 27). If the counter value is not zero (line 28), the receive-a-validation-character/convolute-the-character/-return-the-convoluted-character/decrement-and-test-the-counter process is repeated. When the counter value reaches zero (line 29), the validation mode is disabled (block 30); (Path P5). Disabling the validation mode also resets the validation mode enabled condition (block 11), thereby re-enabling the normal mode of operation.

In this embodiment of the invention, the operations described above are controlled by the terminal's microprocessor, which receives instructions from the terminal's read-only memory (ROM), as indicated more fully hereinafter. The microprocessor does not perform the actual convolution of the validation data; it routes validation characters to and resultant convoluted characters from the convolution logic.

FIG. 2 shows the functional flow of operations within the master device during the validation process. The computer sends the enable validation code to the terminal (slave device, block 40) to initiate its validation mode. The computer then specifies the number of characters to be used for validation; this value is stored in a counter in the computer (block 41), and the same value is sent to the terminal (block 42), where it is also stored. This number is used to synchronize completion of the validation process.

The computer generates the validation data (block 43); a validation character may be any character which can be generated by the computer and accepted by the terminal. Each validation character sent to the validation apparatus by the computer (block 44) is convoluted by the apparatus' convolution logic and the resultant convoluted character is returned to the computer (block 45).

The computer software includes a mathematical algorithm equivalent to the convolution process implemented through electronic circuit elements in the validation apparatus. Concurrent with convolution by the validation apparatus, each validation character is also convoluted by the computer, using this mathematical algorithm (block 46).

The computer compares the electronically-convoluted result returned by the convolution apparatus to the mathematically-convoluted result from the computer software (block 47). If the results are not equal (line 48), it is presumed that the terminal associated with the validation apparatus is not authorized to access information contained in or controlled by the computer. If the results are equal (line 49), the validation process continues.

The character counter in the computer is decremented (block 50) and tested (block 51) after each convolution. A zero value in the counter (line 52) indicates successful completion of the validation process; it is presumed that the terminal is authorized to access information, and the computer resumes normal operation. If

the value in the counter is not zero (line 53), the generate-a-validation-character/mathematically-convolute-the-character/send-the-validation-character/receive-a-convoluted-character/compare-convoluted-characters/decrement-and-test-the-counter process is repeated.

FIGS. 1 and 2, as discussed above, show the flow of information in the terminal, validation apparatus, and computer in a typical implementation in accordance with the principles of this invention. FIGS. 3-7, discussed below, show electrical signal flow and physical aspects of the invention.

FIG. 3 shows the major elements of one embodiment of an add-on implementation of the present invention. The computer (master device) 60 performs the operations shown in FIG. 2 and described above.

A typical terminal (slave device) 61 includes interface elements which allow it to communicate with the computer. With the commonly-used RS-232C serial data interface, these elements comprise signal line receivers 62, line drivers 63, and a universal asynchronous receiver/transmitter (UART) 64 which acts as a communication controller. The UART is connected to a microprocessor CPU 65 through data, address, and control lines. The CPU receives instructions from read-only memory ROM 66 and can store information to and retrieve information from random-access read/write memory RAM 67. Timing and control circuitry 68, a power supply 69, and additional elements unique to the specific device 70 are also included in the slave device. The character counter need not be a separate element; a register in the CPU or a storage location in RAM can serve as the counter. In this add-on embodiment, the validation apparatus 71 is physically inside the terminal.

The terminal's CPU receives validation characters in the same manner as any other data sent by the computer to the terminal. When the validation mode of the invention is enabled, however, these characters are routed to the validation apparatus instead of to the terminal's normal circuitry. Similarly, the validation apparatus provides convoluted characters to the terminal's CPU for return to the computer; these characters are sent to the computer in the same manner as other data from the terminal.

FIG. 4 shows the functional elements of a validation apparatus 71 of FIG. 3. The terminal's microprocessor CPU (65 of FIG. 3), which is controlled by program instructions contained in the terminal's ROM (66 of FIG. 3), sends address and control signals to "selection logic" 83 and 84 in the validation apparatus. The selection logic uses these signals to route validation characters to and convoluted characters from the convolution logic 85.

Selection logic 83 and 84 each include an address decoder 86 and 91 and AND gates 89 and 93, respectively. The output of address decoder 86 becomes "active" when the terminal's CPU places a specific address on the terminal's address bus 95 and generates "input/output enable" (IOE) and "WRITE" signals 96. This active output enables AND gates 89, which electronically connect the data inputs of the convolution logic to the terminal's bidirectional data bus 97. The CPU concurrently places a validation character on the data bus for receipt by the convolution logic.

Similarly, the output of address decoder 91 becomes active when the CPU places a specific address on the address bus and generates IOE and "READ" signals 98. This active output enables AND gates 93, which elec-

tronically connect the data outputs of the convolution logic to the data bus, thereby providing a convoluted character to the terminal's CPU.

Some embodiments of the invention may not require separate AND gate elements as described above, since specific circuit elements which can be used in the convolution logic inherently perform the AND function (e.g., where the input elements are "flip-flops", or where the output elements are "tri-state buffers"). Selection logic techniques are well known in the art, and details of their implementation need not be discussed herein.

The convolution logic functionally comprises logical elements such as AND gates, OR gates, inverters, etc. These elements are selected and interconnected to perform logical manipulation of validation characters in accordance with a pre-determined pattern or algorithm.

A simple example illustrates character convolution by the convolution logic. In this example, information between the computer and the terminal is represented by ASCII code, and the convolution algorithm converts upper-case alphabetic characters to lower-case and vice versa.

In ASCII code, upper-case alphabetic characters are assigned decimal code values from 65 to 90; lower-case characters have codes from 97 to 122. The difference between upper- and lower-case code values for a specific alphabetic character is 32 (e.g., "A" has a code value of 65; "a" has a code value of 97).

Each ASCII character is defined by 7 data bits (D0-D6). Bit D6 is "active" for all characters with decimal codes from 64 to 127; this range includes all upper- and lower-case alphabetic characters. (For simplicity, the characters @[\]^\_<`{|}~ and delete, also having bit D6 active, with codes 64, 91-96, and 123-127, are convoluted in this example.) If bit D5 is inactive, the character is upper-case; if bit D5 is active, the character is lower-case. Thus, to convert alphabetic characters from uppercase to lower-case and from lower-case to upper-case, the convolution process is: if D6 is active, invert D5.

FIG. 5 is a circuit diagram of an embodiment of the validation apparatus for this example. The selection logic 100 and 101 comprises two integrated circuit chips such as type 74LS138 3-to-8-line decoders. The convolution logic 102 is a programmable array logic chip (PAL) with registered outputs, such as type 16R8, electronically programmed to perform the specific upper-case-to-lower-case/lower-case-to-upper-case convolution.

In this embodiment, the hexadecimal value F2 is used to address the validation apparatus; this value is present when address bits A7, A6, A5, A4, and A1 are active and bits A3, A2, and A0 are inactive. When the terminal's CPU 103 (compare 65 of FIG. 3) executes an OUT F2 instruction, this bit pattern is placed on the address bus and the bit pattern for a validation character is placed on the data bus 104. The input/output enable (IOE) and WRITE (WR) signals also become active, thereby "gating" the validation character's bit pattern into the PAL. The logical elements in the PAL perform the pre-defined convolution (if data bit D6 is active, invert data bit D5), and store the resultant data bit values in the PAL's internal flip-flops. When the CPU executes an IN F2 instruction, the same address is placed on the address bus and the IOE and READ (RD) signals become active. This enables the PAL's internal tri-state output buffers, thereby gating the out-



puts of the flip-flops onto the data bus, and thus providing the convoluted character to the CPU.

To minimize the likelihood of successful attempts to discover the algorithm to gain unauthorized access to the computer, a different algorithm can be developed for each specific installation of the invention. Development of algorithms suitable for the convolution process is known through the art of mathematical techniques for data communications, and a detailed discussion is outside the scope of this description.

It is obvious, however, that convolution algorithms can be far more sophisticated than in this example. Outputs of logical elements which provide "registered" or "feedback" operations allow the result of one convolution to be dependent on the result of one or more preceding convolutions. Multiple sets of convolution logic can be implemented in the validation apparatus, with the computer specifying which set is to be used for each convolution. To further frustrate discovery of the algorithm, part of the convolution can be performed by the logic circuitry in the validation apparatus and part by operations implemented in the terminal's ROM program and performed by its CPU.

FIG. 6 represents a physical embodiment of the add-on implementation of FIG. 5. A small printed circuit adapter board 110 provides mechanical support and electrical interconnection between the elements of the validation apparatus 111 and between these elements and the terminal.

A CPU socket 113 with pins long enough to provide clearance between the adapter board and the terminal's (slave device) circuit board 112 is mounted on the adapter board. The selection logic 114 and 115 and a socket 116 for the convolution logic are also mounted on the adapter board. Interconnection between these elements is provided by printed circuit wiring traces on the adapter board.

The convolution logic 117 is inserted into its socket on the adapter board. The CPU chip 118 is removed from its original socket 119 on the terminal's circuit board and inserted into the CPU socket on the adapter board. The adapter board is connected to the terminal by inserting the long pins from its CPU socket into the original CPU socket on the terminal's circuit board.

The convolution logic comprises a set of individual logic elements (such as standard integrated circuit chips with a fixed type of operation for each chip) selected and interconnected to implement the desired convolution algorithm, or it can be a single large-scale programmable logic device element (such as a PAL) electronically programmed for the algorithm. Socketing the convolution logic allows it to be replaced when a different algorithm is desired. If multiple algorithms are desired for increased security, additional sets of convolution logic, sockets, and selection and control logic are included on a larger adapter board (not shown).

The code in the terminal's ROM (66 of FIG. 3) is augmented to perform several of the operations shown in FIG. 1. These include: testing whether the validation mode is enabled, testing whether an enable validation code has been received, storing a numeric value in the character counter and decrementing and testing the counter value, and sending data to and receiving data from the convolution logic. Other operations, such as receiving characters from and sending characters to the computer and sending normal characters to other elements of the terminal are typically implemented in the terminal's existing ROM program code.

Similarly, the computer's software is augmented to perform operations shown in FIG. 2. (Sending information to and receiving information from peripheral devices are implemented in the computer's existing software, and remain unchanged.) The additions to the computer's software for the validation process can be in the input/output routines; changes are not required in the main information processing routines.

The description above pertains to an add-on embodiment of this invention for validating access through an existing terminal to information contained in or controlled by a computer. Of course, many other functional and physical embodiments are possible for specific applications in accordance with the principles of this invention; some other possible embodiments are outlined below.

The validation apparatus can be implemented as a "designed-in" embodiment, wherein it is integrated directly into a slave device by including the convolution logic and related selection logic in the design of the device. Such an implementation is functionally similar to the add-on implementation described above, but it eliminates the need for an adapter board and the long-pin CPU socket shown in FIG. 6, as the selection and control elements and convolution logic of the validation apparatus can be mounted directly on the slave device's circuit board.

A "self-contained" implementation of the validation apparatus can be used for applications where it is not feasible or desirable to use an add-on or "designed-in" implementation. The self-contained implementation comprises a separate unit whose functions and information flow are similar to those shown in FIG. 1.

A self-contained implementation can be a "serial" embodiment or a "parallel" embodiment. In a serial embodiment, the validation apparatus is placed physically and functionally between the master device and the slave device, and validation data does not have to reach the slave device. In a parallel embodiment, the validation apparatus is placed functionally "along-side" the slave device. In one form of parallel embodiment, the validation apparatus is connected to the interface link which connects the slave device to the master device, and both the slave device and the validation apparatus receive all data sent to either by the master device. In a second form of parallel embodiment, a separate interface link connects the validation apparatus to the master device or to validation means associated with the master device.

FIG. 7 is a block diagram of a self-contained implementation 120 in a serial embodiment. This embodiment includes two sets of interface elements to allow the validation apparatus 121 to communicate with both the master device 122 and the slave device 123. These elements include duplicate communication line receivers 124 and 125, line drivers 126 and 127, and UARTs 128 and 129. Timing and control circuitry 130 and a power supply 131 support the other elements in the unit.

The microprocessor (CPU) 132 and ROM 133 can be separate elements, or a micro-controller that incorporates both CPU and ROM functions can be used. Random-access memory is not required for a self-contained implementation of the validation apparatus.

What is claimed is:

1. Apparatus comprising processing means for processing validation data; said processing means including means for receiving validation data from an interconnected validation device which autogenically generates

11

and transmits validation data and commands, means for convoluting said validation data in accordance with a pre-defined algorithm to produce convoluted data, and means for returning said convoluted data to said validation device; and means responsive to the validation device for selectively enabling and disabling the processing of said processing means.

2. Apparatus in accordance with in claim 1, wherein said processing means includes means for selective return of said convoluted data upon command from said validation device.

3. Apparatus as in claim 1, wherein said processing means includes means for convoluting the validation data according to a second algorithm, and means for selecting one of said algorithms in response to a command from said validation device.

4. An access authority validation system comprising a slave device operative to access a master device through an interconnecting interface link, said system also including validation means associated with said master device for validating authority of said slave device to access said master device, said system also including apparatus associated with said slave device interconnected through said interface link to said validation means, said apparatus being responsive to an access validation command from said validation means to convolute in a predetermined manner a set of data transmitted to it by said validation means so as to produce a set of convoluted data and to return the set of convoluted data to said validation means;

said validation means including means for autogenically generating and transmitting said validation command and said set of data to said apparatus, means for receiving said set of convoluted data returned by said apparatus, means for convoluting the transmitted set of data to produce a convoluted data set, and means for comparing the convoluted data set to the said set of convoluted data returned by said apparatus.

5. A system as set forth in claim 4, wherein said validation means also includes means operative autogenically for switching between a normal access mode and an access validation mode.

6. A system as set forth in claim 4, wherein said predetermined manner of convolution includes a plurality of algorithms for said convolution and wherein each said access validation command specifies which of said plurality of algorithms defines the convolution of each said transmitted set of associated data.

7. A system as set forth in claim 4, wherein each said access validation command specifies the number of data units to be convoluted in each said transmitted set of associated data.

8. A system as set forth in claim 4, wherein said apparatus includes electronic circuitry for said convolution of said data transmitted to it.

9. A system as set forth in claim 4, wherein said validation means includes means for signaling the occurrence of a mismatch as determined by said comparison of said two sets of convoluted data.

12

10. A system as set forth in claim 4, wherein said validation means is incorporated into said master device.

11. A system as set forth in claim 4, wherein said apparatus is incorporated into said slave device.

12. A system as set forth in claim 4, wherein a single, common interface link functions both as said interface link interconnecting said master device and said slave device and as said interface link interconnecting said validation means and said apparatus.

13. A system as set forth in claim 4, wherein a plurality of said slave devices are operative to access said master device.

14. A system as set forth in claim 4, wherein said slave device is operative to access at least one device external to said master device and wherein access to said external device is controlled by said master device.

15. An information process network comprising a master device which controls information, at least one slave device which desires access to said information, an interface link interconnecting said master device and said slave device, and a system to validate authority of said slave device to access said information controlled by said master device, said validation system including apparatus associated with said slave device interconnected to validation means associated with said master device, said apparatus being responsive to a validation command from said validation means to convolute in a predetermined manner validation data transmitted to it by said validation means and to return the convoluted data to said validation means, said validation means including means for generating said validation command said validation data autogenically, means for transmitting said validation command said validation data to said apparatus, means for receiving said convoluted data returned by said apparatus, means for convoluting said transmitted data in accordance with said validation command, and means for comparing the thus convoluted data with the said convoluted data returned by said apparatus, a mismatch determined by said comparison signifying that said slave device is not authorized to access said information controlled by said master device.

16. A network in accordance with claim 15, including means to autogenically switch between at least two modes of operation, a first such mode being a normal access mode in which information passes unchanged between said master device and said slave device, and a second such mode being an access authority validation mode, said validation mode including said generation, said transmission, said convolutions, said return, and said comparison.

17. A network in accordance with claim 16, further including means for operating in a combination mode wherein said validation data is embedded in a normal data stream, and wherein said slave device and said master device operate in said normal access mode using said normal data stream, and said apparatus and said validation means concurrently operate in said access validation mode using said embedded validation data.

\* \* \* \* \*



US006098106A

**United States Patent** [19]  
**Philyaw et al.**

[11] **Patent Number:** **6,098,106**  
 [45] **Date of Patent:** **Aug. 1, 2000**

[54] **METHOD FOR CONTROLLING A COMPUTER WITH AN AUDIO SIGNAL**

5,357,276 10/1994 Banker et al. .... 348/7  
 5,438,355 8/1995 Palmer ..... 348/1

(List continued on next page.)

[75] Inventors: **Jeffry Jovan Philyaw**, Dallas; **David Kent Mathews**, Carrollton; **Brad Maxwell Smith**, Irving; **Paul Scovell Adams**, Dallas, all of Tex.

**FOREIGN PATENT DOCUMENTS**

0 152 341 8/1985 European Pat. Off. .  
 2 692 613 9/1994 France .  
 0 601 437 A1 6/1994 Germany .  
 WO 91/03891 3/1991 WIPO .  
 WO 95/28044 10/1995 WIPO .

[73] Assignee: **DigitalConvergence.com inc.**, Dallas, Tex.

**OTHER PUBLICATIONS**

"Integrating Traditional Media with the Web", web page located at [www.webchoicetv.com/products](http://www.webchoicetv.com/products), 4 pages, by Web-Choice, Inc., Santa Monica, CA.  
 Web page for Symbol, located at [www.symbol.com](http://www.symbol.com), 5 pages.  
 "Symbol CyberPen (previously know as InfoPen)", web page located at [www.symbol.com/products/consumer\\_systems/consumer\\_cyberpen](http://www.symbol.com/products/consumer_systems/consumer_cyberpen), 2 pages.

[21] Appl. No.: **09/151,530**

[22] Filed: **Sep. 11, 1998**

[51] Int. Cl.<sup>7</sup> ..... **G06F 15/00; G06F 15/16**

[52] U.S. Cl. .... **709/238; 709/218; 709/219; 709/224; 709/239**

[58] Field of Search ..... **709/238, 239, 709/245, 218, 224, 719; 345/327**

*Primary Examiner*—Zarni Maung  
*Assistant Examiner*—Almari Romero  
*Attorney, Agent, or Firm*—Gregory M. Howison

[56] **References Cited**

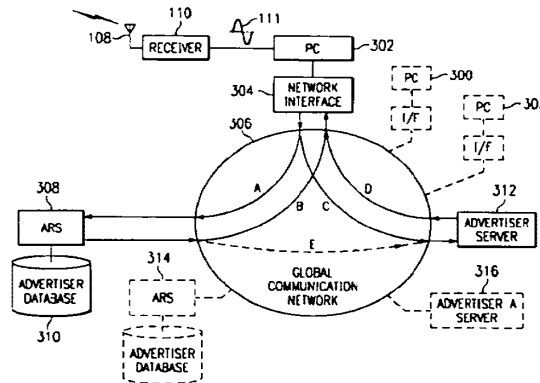
**U.S. PATENT DOCUMENTS**

3,668,312	6/1972	Yamamoto et al. ....	348/17
4,042,792	8/1977	Pakenham et al. ....	179/90
4,621,259	11/1986	Schepers et al. ....	345/180
4,654,482	3/1987	DeAngelis .....	379/95
4,816,904	3/1989	McKenna et al. ....	348/13
4,817,136	3/1989	Rhoads .....	379/375
4,841,132	6/1989	Kajitani et al. ....	235/462.46
4,894,789	1/1990	Yee .....	348/552
4,899,370	2/1990	Kameo et al. ....	379/104
4,905,094	2/1990	Pocock et al. ....	386/106
4,907,264	3/1990	Seiler et al. ....	379/216
4,937,853	6/1990	Brule et al. ....	379/91
4,947,028	8/1990	Gorog .....	235/380
4,975,948	12/1990	Andresen et al. ....	379/355
4,984,155	1/1991	Geier et al. ....	364/401
5,128,752	7/1992	Von Kohorn .....	705/10
5,144,654	9/1992	Kelley et al. ....	379/356
5,189,630	2/1993	Barstow et al. ....	364/514
5,247,347	9/1993	Litteral et al. ....	348/7
5,262,860	11/1993	Fitzpatrick et al. ....	348/461
5,285,278	2/1994	Holman .....	348/10
5,287,181	2/1994	Holman .....	348/473
5,305,195	4/1994	Murphy .....	705/1
5,319,454	6/1994	Schutte .....	348/5.5

[57] **ABSTRACT**

A method for controlling a computer by inputting an analog signal into the computer to control a web browser software application. The analog signal contains a trigger signal which activates proprietary software, and a product identifier. The proprietary software launches the web browser application on the computer, extracts the product identifier, and creates an appended data string by appending server address (URL) routing information to the product identifier information. The appended data string is automatically inserted into the web browser as keystroke data and routed to an advertiser reference server. The appended routing information directs communication to the advertiser reference server which contains a cross-referenced database of advertiser product identifier information and associated advertiser server URLs. The advertiser server URL and a request for product information relevant to the product identifier is returned to the computer web browser where it is automatically redirected to the advertiser server containing the advertiser product information. The advertiser product information is then returned to the computer for display.

**18 Claims, 6 Drawing Sheets**



## U.S. PATENT DOCUMENTS

5,446,490	8/1995	Blahut et al.	348/7	5,905,251	5/1999	Knowles	235/472.01
5,446,919	8/1995	Wilkins	455/6.2	5,905,665	5/1999	Rim	364/746
5,491,508	2/1996	Friedell et al.	348/16	5,905,865	5/1999	Palmer et al.	395/200.47
5,570,295	10/1996	Isenberg et al.	379/90.01	5,907,793	5/1999	Reams	455/3.1
5,572,643	11/1996	Judson	395/793	5,915,090	6/1999	Joseph et al.	709/202
5,592,551	1/1997	Lett et al.	380/20	5,925,865	7/1999	Steger	235/379
5,594,226	1/1997	Steger	235/379	5,929,850	7/1999	Broadwin et al.	345/327
5,604,542	2/1997	Dedrick	348/552	5,933,468	11/1998	Guy et al.	434/350
5,640,193	6/1997	Wellner	348/7	5,933,829	8/1999	Durst et al.	707/10
5,664,110	9/1997	Green et al.	705/26	5,948,061	9/1999	Merriman et al.	709/219
5,675,721	10/1997	Freedman et al.	395/129	5,957,695	9/1999	Redford et al.	434/307 R
5,694,163	12/1997	Harrison	348/13	5,960,411	9/1999	Hartman et al.	705/26
5,708,780	1/1998	Levergood et al.	709/229	5,961,603	10/1999	Kunkel et al.	709/229
5,715,314	2/1998	Payne et al.	705/78	5,970,471	10/1999	Hill	705/26
5,724,424	3/1998	Gifford	705/79	5,970,472	10/1999	Allsop et al.	705/26
5,754,906	5/1998	Yoshida	396/448	5,971,277	10/1999	Cragun et al.	235/462.01
5,761,606	6/1998	Wolzien	455/6.2	5,974,443	10/1999	Jeske	709/202
5,768,528	6/1998	Stumm	709/231	5,974,451	10/1999	Simmons	709/218
5,774,664	6/1998	Hidary et al.	709/218	5,976,833	11/1999	Furukawa et al.	435/69.1
5,774,870	6/1998	Storey	705/14	5,978,773	11/1999	Hudetz et al.	709/219
5,778,367	7/1998	Wesinger, Jr.	707/10	5,991,739	11/1999	Cupps et al.	705/26
5,790,793	8/1998	Higley	709/218	6,002,394	12/1999	Schein et al.	345/327
5,794,210	8/1998	Goldhaber et al.	705/14	6,003,073	12/1999	Solvason	709/219
5,796,952	8/1998	Davis et al.	305/200.54	6,006,257	12/1999	Slezak	709/219
5,854,897	12/1998	Radziewicz et al.	709/224	6,009,410	12/1999	LeMole et al.	709/219
5,864,823	1/1999	Levitan	105/14	6,009,465	12/1999	Decker et al.	709/219
				6,018,764	1/2000	Field et al.	709/217

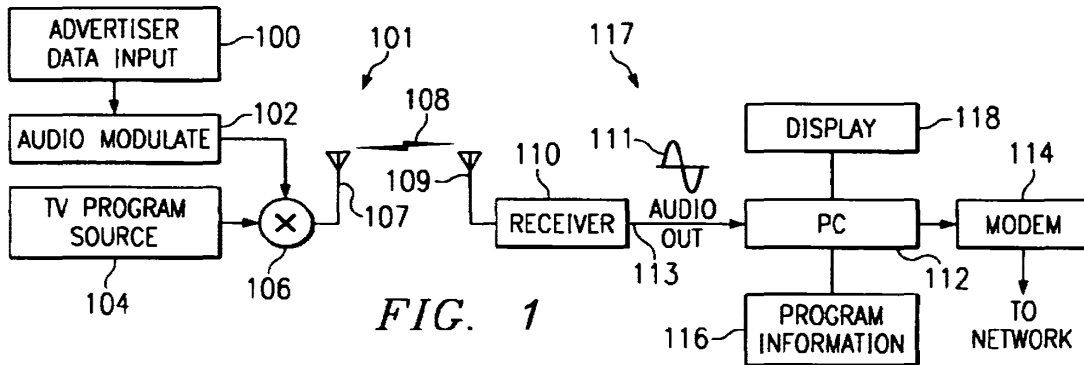


FIG. 1

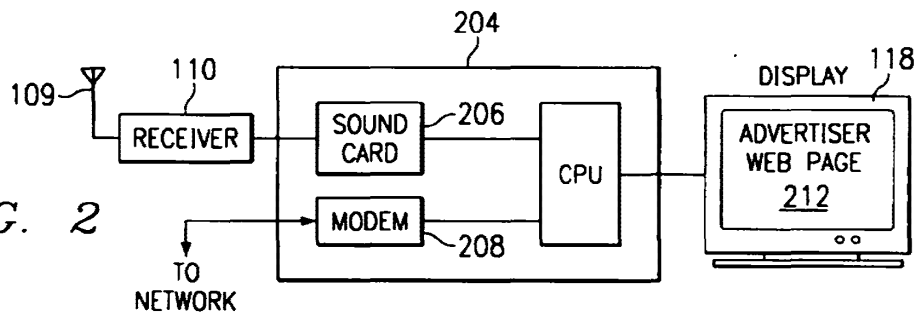


FIG. 2

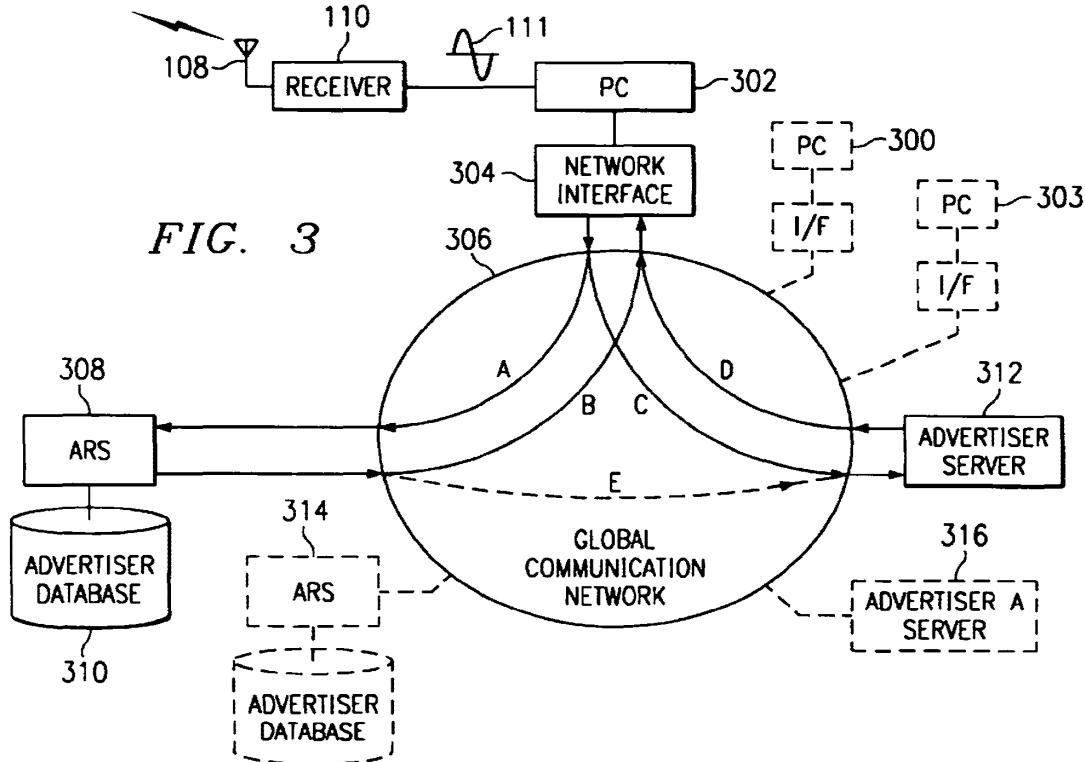


FIG. 3

2012100462 03 Jul 2012

PATH A: SOURCE TO ARS



FIG. 4a

PATH B: ARS TO SOURCE



FIG. 4b

PATH C: SOURCE TO ADVERTISER



FIG. 4c

PATH D: ADVERTISER TO SOURCE

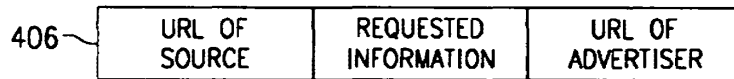


FIG. 4d

PATH E: ARS TO ADVERTISER (OPTIONAL)

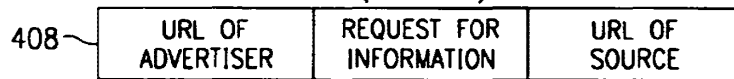


FIG. 4e

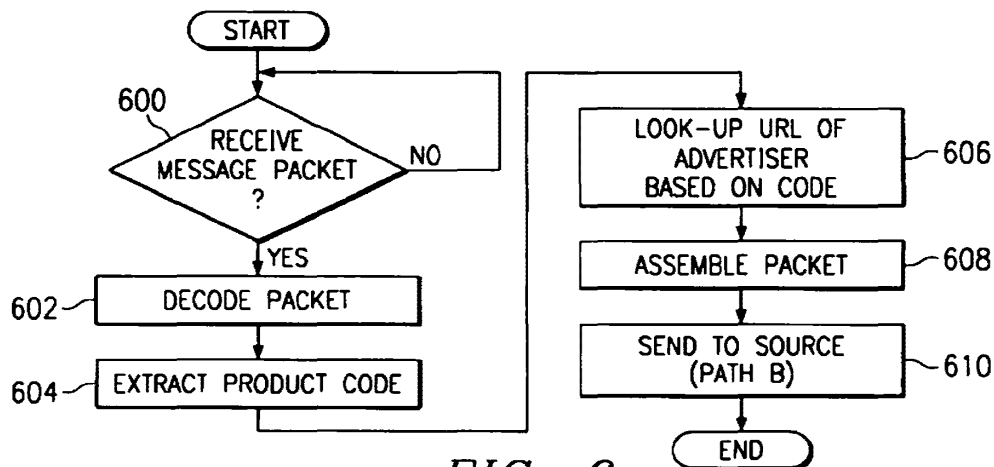


FIG. 6

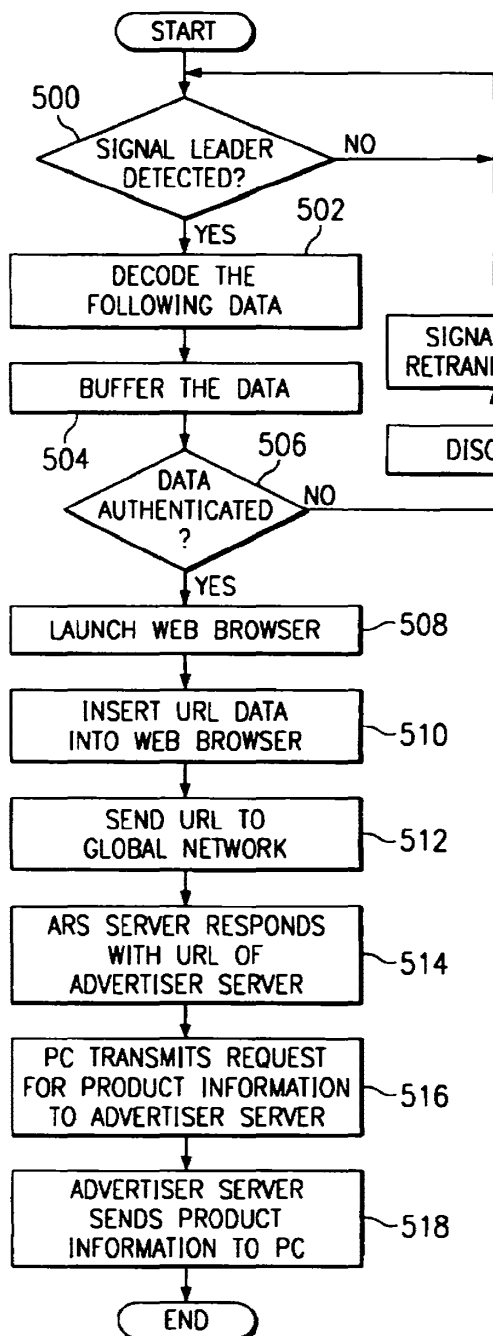


FIG. 5

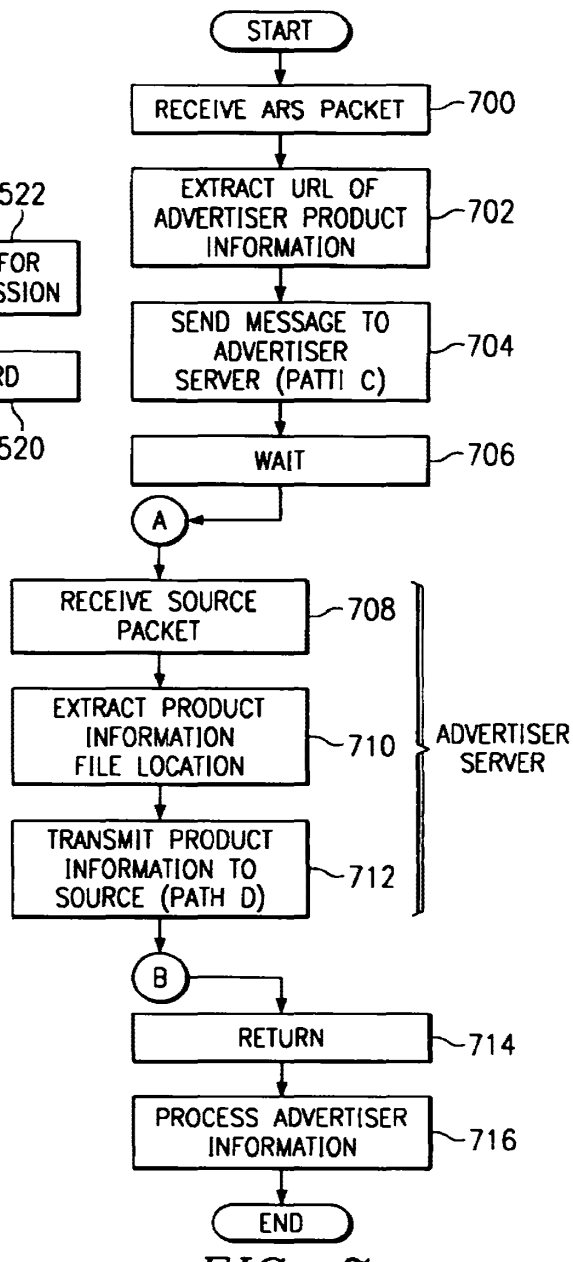


FIG. 7

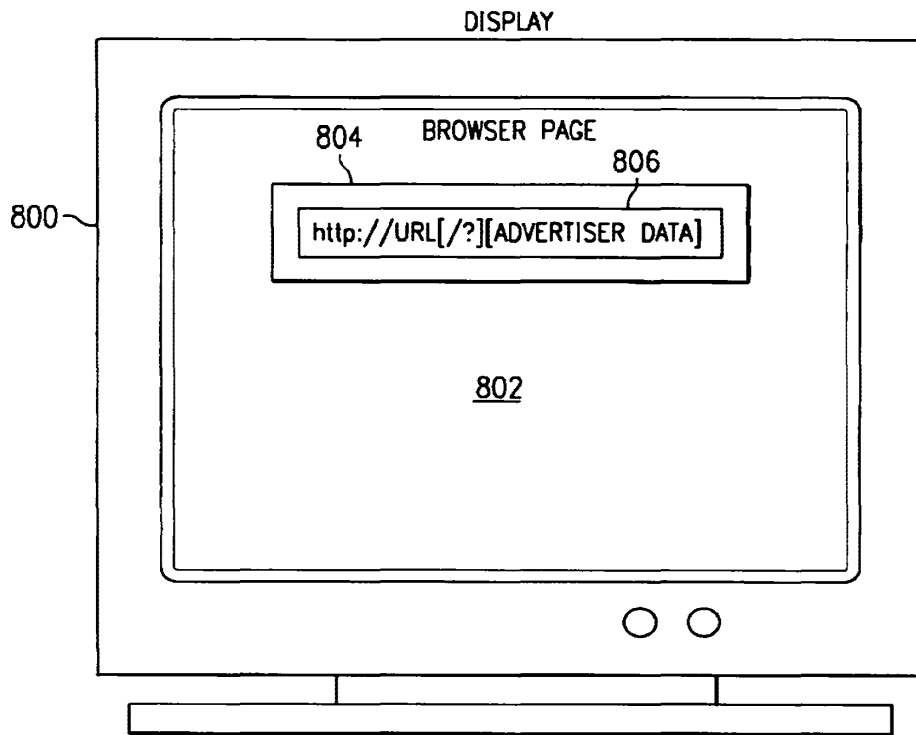


FIG. 8

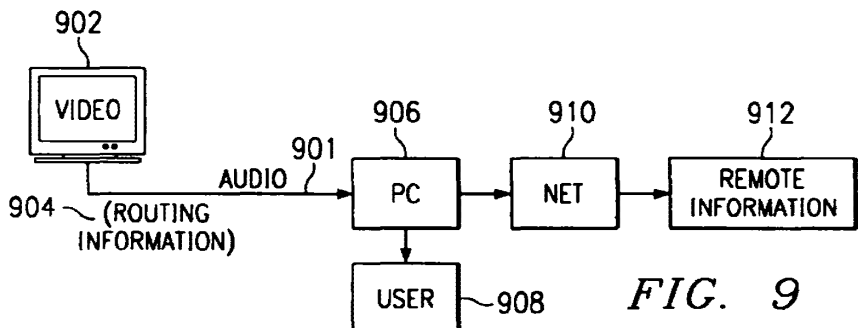
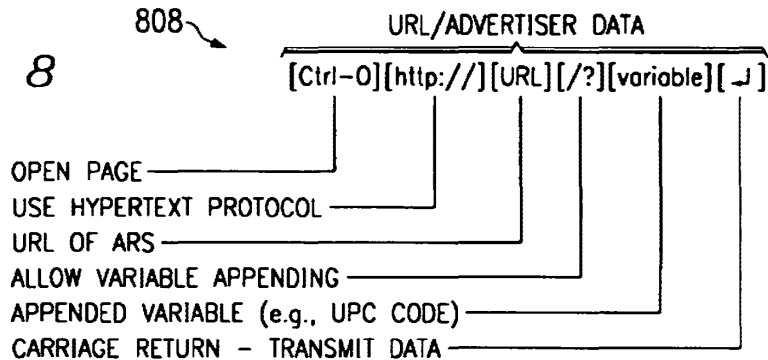
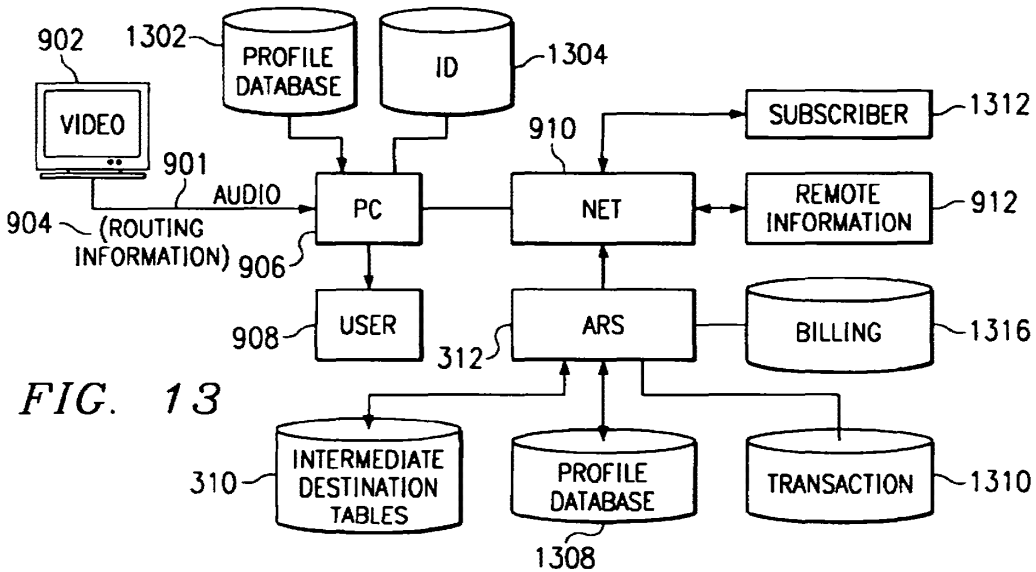
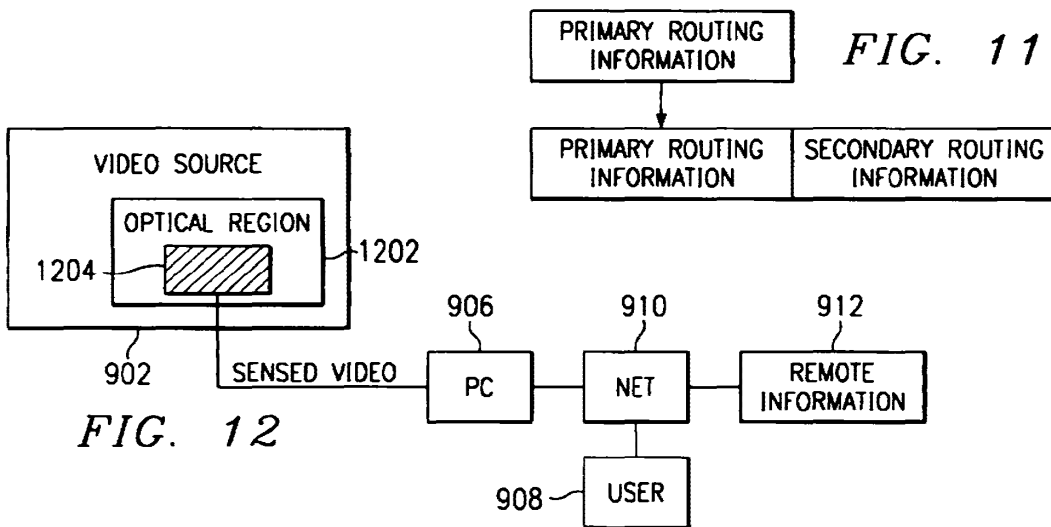
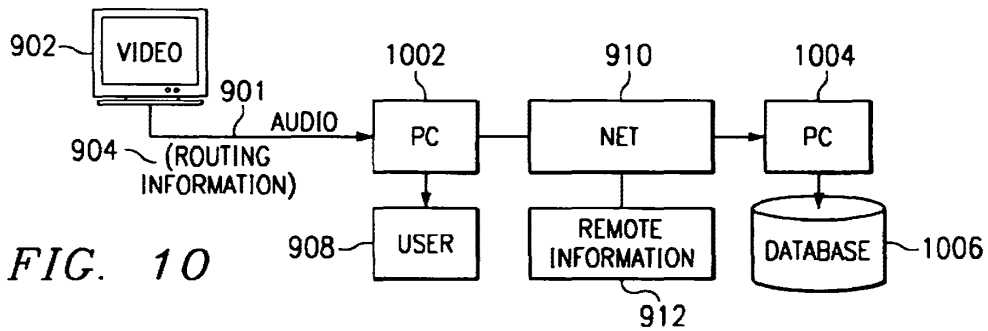


FIG. 9



2012100462 03 Jul 2012



2012100462 03 Jul 2012

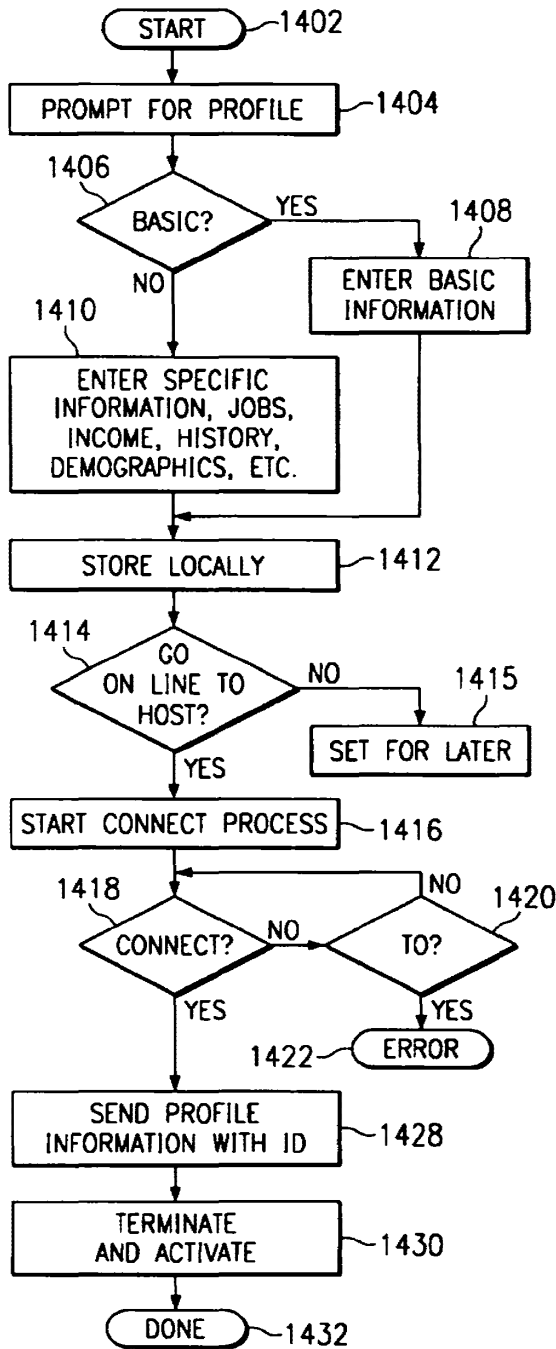


FIG. 14

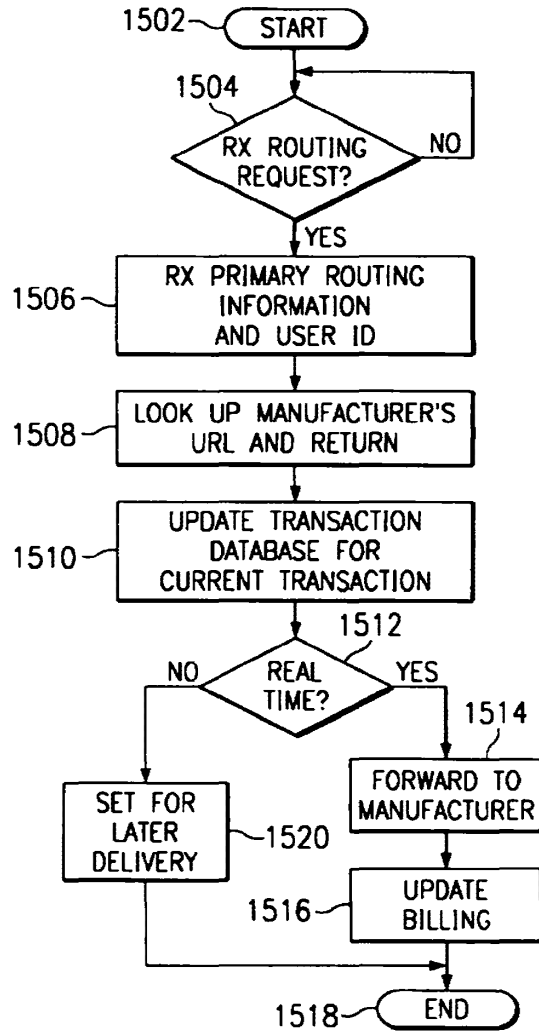


FIG. 15

## METHOD FOR CONTROLLING A COMPUTER WITH AN AUDIO SIGNAL

This application is related to copending U.S. patent application Ser. No. 09/151,471, entitled, "METHOD FOR INTERFACING SCANNED PRODUCT INFORMATION WITH A SOURCE FOR THE PRODUCT OVER A GLOBAL NETWORK" filed of even date herewith.

### TECHNICAL FIELD OF THE INVENTION

This invention is related to a method of computer control, and particularly for automatically directing a web browser application on the computer to retrieve and display information in response to an analog signal.

### BACKGROUND OF THE INVENTION

With the growing numbers of computer users connecting to the "Internet," many companies are seeking the substantial commercial opportunities presented by such a large user base. For example, one technology which exists allows a television ("TV") signal to trigger a computer response in which the consumer will be guided to a personalized web page. The source of the triggering signal may be a TV, video tape recorder, or radio. For example, if a viewer is watching a TV program in which an advertiser offers viewer voting, the advertiser may transmit a unique signal within the television signal which controls a program known as a "browser" on the viewer's computer to automatically display the advertiser's web page. The viewer then simply makes a selection which is then transmitted back to the advertiser.

In order to provide the viewer with the capability of responding to a wide variety of companies using this technology, a database of company information and Uniform Resource Locator ("URL") codes is necessarily maintained in the viewer's computer, requiring continuous updates. URLs are short strings of data that identify resources on the Internet: documents, images, downloadable files, services, electronic mailboxes, and other resources. URLs make resources available under a variety of naming schemes and access methods such as HTTP, FTP, and Internet mail, addressable in the same simple way. URLs reduce the tedium of "login to this server, then issue this magic command . . ." down to a single click. The Internet uses URLs to specify the location of files on other servers. A URL includes the type of resource being accessed (e.g., Web, gopher, FTP), the address of the server, and the location of the file. The URL can point to any file on any networked computer. Current technology requires the viewer to perform periodic updates to obtain the most current URL database. This aspect of the current technology is cumbersome since the update process requires downloading information to the viewer's computer. Moreover, the likelihood for error in performing the update, and the necessity of redoing the update in the event of a later computer crash, further complicates the process. Additionally, current technologies are limited in the number of companies which may be stored in the database. This is a significant limitation since worldwide access presented by the Internet and the increasing number of companies connecting to perform on-line commerce necessitates a large database.

### SUMMARY OF THE INVENTION

The present invention disclosed and claimed herein comprises a method for retrieving information from a storage

region having a defined location. A program is broadcasted having embedded therein a routing signal having routing information contained therein. The routing signal is then extracted from the broadcast. Thereafter, a personal computer is controlled to allow a user to retrieve the information from a storage region at the defined location, which defined location is located with the extracted routing information, providing it at the personal computer for use by the user.

### BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying Drawings in which:

FIG. 1 illustrates a block diagram of the preferred embodiment;

FIG. 2 illustrates the computer components employed in this embodiment;

FIG. 3 illustrates system interactions over a global network;

FIGS. 4a-4e illustrate the various message packets transmitted between the source PC and network servers used in the preferred embodiment; and

FIG. 5 is a flowchart depicting operation of the system according to the preferred embodiment.

FIG. 6 illustrates a flowchart of actions taken by the Advertiser Reference Server ("ARS") server;

FIG. 7 illustrates a flowchart of the interactive process between the source computer and ARS;

FIG. 8 illustrates a web browser page receiving the modified URL/advertiser product data according to the preferred embodiment;

FIG. 9 illustrates a simplified block diagram of the disclosed embodiment;

FIG. 10 illustrates a more detailed, simplified block diagram of the embodiment of FIG. 9;

FIG. 11 illustrates a diagrammatic view of a method for performing the routing operation;

FIG. 12 illustrates a block diagram of an alternate embodiment utilizing an optical region in the video image for generating the routing information;

FIG. 13 illustrates a block diagram illustrating the generation of a profile with the disclosed embodiment;

FIG. 14 illustrates a flowchart for generating the profile and storing at the ARS; and

FIG. 15 illustrates a flowchart for processing the profile information when information is routed to a user.

### DETAILED DESCRIPTION OF THE INVENTION

Referring now to FIG. 1, there is illustrated a block diagram of a system for controlling a personal computer ("PC") 112 via an audio tone transmitted over a wireless system utilizing a TV. In the embodiment illustrated in FIG. 1, there is provided a transmission station 101 and a receive station 117 that are connected via a communication link 108. The transmission station 101 is comprised of a television program source 104, which is operable to generate a program in the form of a broadcast signal comprised of video and audio. This is transmitted via conventional techniques along channels in the appropriate frequencies. The program source is input to a mixing device 106, which mixing device is operable to mix in an audio signal. This audio signal is

derived from an audio source **100** which comprises a coded audio signal which is then modulated onto a carrier which is combined with the television program source **104**. This signal combining can be done at the audio level, or it can even be done at the RF level in the form of a different carrier. However, the preferred method is to merely sum the audio signal from the modulator **102** into the audio channel of the program that is generated by the television program source **104**. The output thereof is provided from the mixing device **106** in the form of broadcast signal to an antenna **107**, which transmits the information over the communication link **108** to an antenna **109** on the receive side.

On the receive side of the system, a conventional receiver **110**, such as a television is provided. This television provides a speaker output which provides the user with an audible signal. This is typically associated with the program. However, the receiver **110** in the disclosed embodiment, also provides an audio output jack, this being the type RCA jack. This jack is utilized to provide an audio output signal on a line **113** which is represented by an audio signal **111**. This line **113** provides all of the audio that is received over the communication link **108** to the PC **112** in the audio input port on the PC **112**. However, it should be understood that, although a direct connection is illustrated from the receiver **110** to the PC **112**, there actually could be a microphone pickup at the PC **112** which could pick the audio signal up. In the disclosed embodiment the audio signal generated by the advertiser data input device **100** is audible to the human ear and, therefore, can be heard by the user. Therefore, no special filters are needed to provide this audio to the PC **112**.

The PC **112** is operable to run programs thereon which typically are stored in a program file area **116**. These programs can be any type of programs such as word processing programs, application programs, etc. In the disclosed embodiment, the program that is utilized in the system is what is referred to as a "browser." The PC **112** runs a browser program to facilitate the access of information on the network, for example, a global communication network known as the "Internet" or the World-Wide-Web ("Web"). The browser is a hypertext-linked application used for accessing information. Hypertext is a term used to describe a particular organization of information within a data processing system, and its presentation to a user. It exploits the computer's ability to link together information from a wide variety of sources to provide the user with the ability to explore a particular topic. The traditional style of presentation used in books employs an organization of the information which is imposed upon it by limitations of the medium, namely fixed sized, sequential paper pages. Hypertext systems, however, use a large number of units of text or other types of data such as image information, graphical information, video information, or sound information, which can vary in size. A collection of such units of information is termed a hypertext document, or where the hypertext documents employ information other than text, hypermedia documents. Multimedia communications may use the Hypertext Transfer Protocol ("HTTP"), and files or formatted data may use the Hypertext Markup Language ("HTML"). This formatting language provides for a mingling of text, graphics, sound, video, and hypertext links by "tagging" a text document using HTML. Data encoded using HTML is often referred to as an "HTML document," an "HTML page," or a "home page." These documents and other Internet resources may be accessed across the network by means of a network addressing scheme which uses a locator referred to as a Uniform Resource Locator ("URL"), for example, "http://www.digital.com."

The Internet is one of the most utilized networks for interconnecting distributed computer systems and allows users of these computer systems to exchange data all over the world. Connected to the Internet are many private networks, for example, corporate or commercial networks. Standard protocols, such as the Transport Control Protocol ("TCP") and the Internet Protocol ("IP") provide a convenient method for communicating across these diverse networks. These protocols dictate how data are formatted and communicated. As a characteristic of the Internet, the protocols are layered in an IP stack. At higher levels of the IP stack, such as the application layer (where HTTP is employed), the user information is more readily visible, while at lower levels, such as the network level (where TCP/IP are used), the data can merely be observed as packets or a stream of rapidly moving digital signals. Superimposed on the Internet is a standard protocol interface for accessing Web resources, such servers, files, Web pages, mail messages, and the like. One way that Web resources can be accessed is by browsers made by Netscape® and Microsoft Internet Explorer®.

Referring again now to FIG. 1, the user can load this program with the appropriate keystrokes such that a browser window will be displayed on a display **118**. In one embodiment, the user can run the browser program on the PC **112** such that the browser window is displayed on the display **118**. While watching a preferred program, the user can also view display **118**. When an audio signal is received by the receiver **110** and the encoded information is contained therein that was input thereto by the advertiser, the PC **112** will then perform a number of operations. The first operation, according to the disclosed embodiment, is to extract the audio information within the received audio signal in the form of digital data, and then transmit this digital data to a defined location on the global communication network via a modem connection **114**. This connection will be described hereinbelow. This information will be relayed to a proprietary location and the instructions sent back to the PC **112** as to the location of the advertiser associated with the code, and the PC **112** will then effect a communication link to that location such that the user can view on the display **118** information that the advertiser, by the fact of putting the tone onto the broadcast channel, desires the viewer to view. This information can be in the form of interactive programs, data files, etc. In one example, when an advertisement appears on the television, the tone can be generated and then additional data displayed on the display **118**. Additionally, a streaming video program could be played on the PC received over the network, which streaming video program is actually longer than the advertising segment on the broadcast. Another example would be a sports game that would broadcast the tone in order to allow a user access to information that is not available over the broadcast network, such as additional statistics associated with the sports program, etc.

By utilizing the system described herein with respect to the disclosed embodiment of FIG. 1, an advertiser is allowed the ability to control a user's PC **112** through the use of tones embedded within a program audio signal. As will be described hereinbelow, the disclosed embodiment utilizes particular routing information stored in the PC **112** which allows the encoded information in the received audio signal to route this information to a desired location on the network and then allow other routing information to be returned to the PC **112** for control thereof to route the PC **112** to the appropriate location associated with that code.

Referring now to FIG. 2, there is illustrated a computer **204**, similar to computer **112**, connected to display infor-

mation on display 118. The computer 204 comprises an internal audio or "sound" card 206 for receiving the transmitted audio signal through receive antenna 109 and receiver 110. The sound card 206 typically contains analog-to-digital circuitry for converting the analog audio signal into a digital signal. The digital signal may then be more easily manipulated by software programs. The receiver 110 separates the audio signal from the video signal. A special trigger signal located within the transmitted advertiser audio signal triggers proprietary software running on the computer 204 which launches a communication application, in this particular embodiment, the web browser application located on the PC 204. Coded advertiser information contained within the audio signal is then extracted and appended with the address of a proprietary server located on the communication network. The remote server address is in the form of a URL. This appended data, in addition to other control codes, is inserted directly into the web browser application for automatic routing to the communication network. The web browser running on PC 204, and communicating to the network with a through an internal modem 208, in this embodiment, transmits the advertiser information to the remote server. The remote server cross-references the advertiser product information to the address of the advertiser server located on the network. The address of the advertiser server is routed back through the PC 204 web browser to the advertiser server. The advertiser product information is returned to PC 204 to be presented to the viewer on display 118. In this particular embodiment, the particular advertiser product information displayed is contained within the advertiser's web page 212. As mentioned above, the audio signal is audible to the human ear. Therefore the audio signal, as emitted from the TV speakers, may be input to the sound card 206 via a microphone. Furthermore, the audio signal need not be a real-time broadcast, but may be on video tapes, CDs, DVD, or other media which may be displayed at a later date. With the imminent implementation of high definition digital television, the audio signal output from the TV may also be digital. Therefore, direct input into a sound card for A/D purposes may not be necessary, but alternative interfacing techniques to accommodate digital-to-digital signal formats would apply.

Referring now to FIG. 3, there is illustrated a source PC 302, similar to PCs 204 and 112, connected to a global communication network 306 through an interface 304. In this embodiment, the audio signal 111 is received by PC 302 through its sound card 206. The audio signal 111 comprises a trigger signal which triggers proprietary software into launching a web browser application residing on the PC 302. The audio signal 111 also comprises advertiser product information which is extracted and appended with URL information of an Advertiser Reference Server ("ARS") 308. The ARS 308 is a system disposed on the network that is defined as the location to which data in the audio signal 111 is to be routed. As such, data in the audio signal 111 will always be routed to the ARS 308, since a URL is unique on the network system. Connected to the ARS 308 is a database 310 of product codes and associated manufacturer URLs. The database 310 undergoes a continual update process which is transparent to the user. As companies sign-on, e.g., subscribe, to this technology, manufacturer and product information is added to the database 310 without interrupting operation of the source PC 302 with frequent updates. When the advertiser server address URL is obtained from the ARS database 310, it and the request for the particular advertiser product information is automatically routed back through the web browser on PC 302, over to the respective

advertiser server for retrieval of the advertiser product information to the PC 302. It should be noted that although the disclosed invention discusses a global communication network, the system is also applicable to LANs, WANs, and peer-to-peer network configurations. It should be noted that the disclosed architecture is not limited to a single source PC 302, but may comprise a plurality of source PCs, e.g., PC 300 and PC 303. Moreover, a plurality of ARS 308 systems and advertiser servers 312 may be implemented, e.g., ARS 314, and advertiser server A 316, respectively.

The information transactions, in general, which occur between the networked systems of this embodiment, over the communication network, are the following. The web browser running on source PC 302 transmits a message packet to the ARS 308 over Path "A." The ARS 308 decodes the message packet and performs a cross-reference function with product information extracted from the received message packet to obtain the address of an advertiser server 312. A new message packet is assembled comprising the advertiser server 312 address, and sent back to the source PC 302 over Path "B." A "handoff" operation is performed whereby the source PC 302 browser simply reroutes the information on to the advertiser server 312 over Path "C," with the appropriate source and destination address appended. The advertiser server 312 receives and decodes the message packet. The request-for-advertiser-product-information is extracted and the advertiser 312 retrieves the requested information from its database for transmission back to the source PC 302 over Path "D." The source PC 302 then processes the information, i.e., for display to the viewer. The optional Path "E" is discussed hereinbelow. It should be noted that the disclosed methods are not limited to only browser communication applications, but may accommodate, with sufficient modifications by one skilled in the art, other communication applications used to transmit information over the Internet or communication network.

Referring now to FIG. 4a, the message packet 400 sent from the source PC 302 to ARS 308 via Path "A" comprises several fields. One field comprises the URL of the ARS 308 which indicates where the message packet is to be sent. Another field comprises the advertiser product code or other information derived from the audio signal 111, and any additional overhead information required for a given transaction. The product code provides a link to the address of the advertiser server 312, located in the database 310. Yet another field comprises the network address of the source PC 302. In general, network transmissions are effected in packets of information, each packet providing a destination address, a source address, and data. These packets vary depending upon the network transmission protocol utilized for communication. Although the protocols utilized in the disclosed embodiment are of a conventional protocol suite commonly known as TCP/IP, it should be understood that any protocols providing the similar basic functions can be used, with the primary requirement that a browser can forward the routing information to the desired URL in response to keystrokes being input to a PC. However, it should be understood that any protocol can be used, with the primary requirement that a browser can forward the product information to the desired URL in response to keystrokes being input to a PC. Within the context of this disclosure, "message packet" shall refer to and comprise the destination URL, product information, and source address, even though more than a single packet must be transmitted to effect such a transmission.

Upon receipt of the message packet 400 from source PC 302, ARS 308 processes the information in accordance with

instructions embedded in the overhead information. The ARS 308 specifically will extract the product code information from the received packet 400 and, once extracted, will then decode this product code information. Once decoded, this information is then compared with data contained within the ARS advertiser database 310 to determine if there is a "hit." If there is no "hit" indicating a match, then information is returned to the browser indicating such. If there is a "hit," a packet 402 is assembled which comprises the address of the source PC 302, and information instructing the source PC 302 as to how to access, directly in a "handoff" operation, another location on the network, that of an advertiser server 312. This type of construction is relatively conventional with browsers such as Netscape® and Microsoft Internet Explorer® and, rather than displaying information from the ARS 308, the source PC 302 can then access the advertiser server 312. The ARS 308 transmits the packet 402 back to source PC 302 over Path "B." Referring now to FIG. 4b, the message packet 402 comprises the address of the source PC 302, the URL of the advertiser server 312 embedded within instructional code, and the URL of the ARS 308.

Upon receipt of the message packet 402 by the source PC 302, the message packet 402 is disassembled to obtain pertinent routing information for assembly of a new message packet 404. The web browser running on source PC 302 is now directed to obtain, over Path "C," the product information relevant to the particular advertiser server 312 location information embedded in message packet 404. Referring now to FIG. 4c, the message packet 404 for this transaction comprises the URL of the advertiser server 312, the request-for-product-information data, and the address of the source PC 302.

Upon receipt of the message packet 404 from source PC 302, advertiser server 312 disassembles the message packet 404 to obtain the request-for-product-information data. The advertiser server 312 then retrieves the particular product information from its database, and transmits it over Path "D" back to the source PC 302. Referring now to FIG. 4d, the message packet 406 for this particular transaction comprises the address of the source PC 302, the requested information, and the URL of the advertiser server 312.

Optionally, the ARS 308 may make a direct request for product information over Path "E" to advertiser server 312. In this mode, the ARS 308 sends information to the advertiser server 312 instructing it to contact the source PC 302. This, however, is unconventional and requires more complex software control. The message packet 408 for this transaction is illustrated in FIG. 4e, which comprises the URL of the advertiser server 312, the request-for-product-information data, and the address of the source PC 302. Since product information is not being returned to the ARS 308, but directly to the source PC 302, the message packet 408 requires the return address to be that of the source PC 302. The product information is then passed directly to PC 302 over Path "D."

Referring now to FIG. 5, the method for detecting and obtaining product information is as follows. In decision block 500, a proprietary application running resident on a source computer PC 302 (similar to PC 204) monitors the audio input for a special trigger signal. Upon detection of the trigger signal, data following the trigger signal is decoded for further processing, in function block 502. In function block 504, the data is buffered for further manipulation. In decision block 506, a determination is made as to whether the data can be properly authenticated. If not, program flow continues through the "N" signal to function block 520

where the data is discarded. In function block 522, the program then signals for a retransmission of the data. The system then waits for the next trigger signal, in decision block 500. If properly authenticated in decision block 506, program flow continues through the "Y" signal path where the data is then used to launch the web browser application, as indicated in function block 508. In function block 510, the web browser receives the URL data, which is then automatically routed through the computer modem 208 to the network interface 304 and ultimately to the network 306. In function block 514, the ARS 308 responds by returning the URL of advertiser server 312 to the PC 302.

In function block 516, the web browser running on the source PC 302, receives the advertiser URL information from the ARS 308, and transmits the URL for the product file to the advertiser server 312. In block 518, the advertiser server 312 responds by sending the product information to the source PC 302 for processing.

The user may obtain the benefits of this architecture by simply downloading the proprietary software over the network. Other methods for obtaining the software are well-known; for example, by CD, diskette, or pre-loaded hard drives.

Referring now to FIG. 6, there is illustrated a flowchart of the process the ARS 308 may undergo when receiving the message packet 400 from the source PC 302. In decision block 600, the ARS 308 checks for the receipt of the message packet 400. If a message packet 400 is not received, program flow moves along the "N" path to continue waiting for the message. If the message packet 400 is received, program flow continues along path "Y" for message processing. Upon receipt of the message packet 400, in function block 602, the ARS 308 decodes the message packet 400. The product code is then extracted independently in function block 604 in preparation for matching the product code with the appropriate advertiser server address located in the database 310. In function block 606, the product code is then used with a look-up table to retrieve the advertiser server 312 URL of the respective product information contained in the audio signal data. In function block 608, the ARS 308 then assembles message packet 402 for transmission back to the source PC 302. Function block 610 indicates the process of sending the message packet 402 back to the source PC 302 over Path "B."

Referring now to FIG. 7, there is illustrated a flowchart of the interactive processes between the source PC 302 and the advertiser server 312. In function block 700, the source PC 302 receives the message packet 402 back from the ARS 308 and begins to decode the packet 402. In function block 702, the URL of the advertiser product information is extracted from the message packet 402 and saved for insertion into the message packet 404 to the advertiser server 312. The message packet 404 is then assembled and sent by the source PC 302 over Path "C" to the advertiser server 312, in function block 704. While the source PC 302 waits, in function block 706, the advertiser server 312 receives the message packet 404 from the source PC 302, in function block 708, and disassembles it. The product information location is then extracted from the message packet 404 in function block 710. The particular product information is retrieved from the advertiser server 312 database for transmission back to the source PC 302. In function block 712, the product information is assembled into message packet 406 and then transmitted back to the source PC 302 over Path "D." Returning to the source PC 302 in function block 714, the advertiser product information contained in the message packet 406 received from the advertiser server 312, is then extracted and processed in function block 716.

Referring now to FIG. 8, after receipt of a trigger signal, a web browser application on a source PC 302 is automatically launched and computer display 800 presents a browser page 802. Proprietary software running on the source PC 302 processes the audio signal data after being digitized through the sound card 206. The software appropriately prepares the data for insertion directly into the web browser by extracting the product information code and appending keystroke data to this information. First, a URL page 804 is opened in response to a Ctrl-O command added by the proprietary software as the first character string. Opening URL page 804 automatically positions the cursor in a field 806 where additional keystroke data following the Ctrl-O command will be inserted. After URL page 804 is opened, the hypertext protocol preamble http:// is inserted into the field 806. Next, URL information associated with the location of the ARS 308 is inserted into field 806. Following the ARS 308 URL data are the characters /? to allow entry of variables immediately following the /? characters. In this embodiment, the variable following is the product information code received in the audio signal. The product code information also provides the cross-reference information for obtaining the advertiser URL from the ARS database 310. Next, a carriage return is added to send the URL/product data and close the window 804. After the message packet 400 is transmitted to the ARS 308 from the source PC 302, transactions from the ARS 308, to the source PC 302, to the advertiser server 312, and back to the source PC 302, occur quickly and are transparent to the viewer. At this point, the next information the viewer sees is the product information which was received from the advertiser server 312.

Referring now to FIG. 9, there is illustrated a block diagram of a more simplified embodiment. In this embodiment, a video source 902 is provided which is operable to provide an audio output on an audio cable 901 which provides routing information referred to by reference numeral 904. The routing information 904 is basically information contained within the audio signal. This is an encoded or embedded signal. The important aspect of the routing information 904 is that it is automatically output in realtime as a function of the broadcast of the video program received over the video source 902. Therefore, whenever the program is being broadcast in realtime to the user 908, the routing information 904 will be output whenever the producer of the video desires it to be produced. It should be understood that the box 902 representing the video source could be any type of media that will result in the routing information being output. This could be a cassette player, a DVD player, an audio cassette, a CD ROM or any such media. It is only important that this is a program that the producer develops which the user 908 watches in a continuous or a streaming manner. Embedded within that program, at a desired point selected by the producer, the routing information 904 is output.

The audio information is then routed to a PC 906, which is similar to the PC 112 in FIG. 1. A user 908 is interfaced with the PC to receive information thereof, the PC 906 having associated therewith a display (not shown). The PC 906 is interfaced with a network 910, similar to the network 306 in FIG. 3. This network 910 has multiple nodes thereon, one of which is the PC 906, and another of which is represented by a network node 912 which represents remote information. The object of the present embodiment is to access remote information for display to the user 908 by the act of transmitting from the video program in block 902 the routing information 904. This routing information 904 is utilized to allow the PC 906 which has a network "browser"

running thereon to "fetch" the remote information at the node 912 over the network 910 for display to the user 908. This routing information 904 is in the form of an embedded code within the audio signal, as was described hereinabove.

Referring now to FIG. 10, there is illustrated a more detailed block diagram of the embodiment of FIG. 9. In this embodiment, the PC 906 is split up into a couple of nodes, a first PC 1002 and a second PC 1004. The PC 1002 resides at the node associated with the user 908, and the PC 1004 resides at another node. The PC 1004 represents the ARS 308 of FIG. 3. The PC 1004 has a database 1006 associated therewith, which is basically the advertiser database 310. Therefore, there are three nodes on the network 910 necessary to implement the disclosed embodiment, the PC 1002, the PC 1004 and the remote information node 912. The routing information 904 is utilized by the PC 1002 for routing to the PC 1004 to determine the location of the remote information node 912 on the network 910. This is returned to the PC 1002 and a connection made directly with the remote information node 912 and the information retrieved therefrom to the user 908. The routing information 904 basically constitutes primary routing information.

Referring now to FIG. 11, there is illustrated a diagrammatic view of how the network packet is formed for sending the primary routing information to the PC 1004. In general, the primary routing information occupies a single field which primary routing information is then assembled into a data packet with the secondary routing information for transfer to the network 910. This is described hereinabove in detail.

Referring now to FIG. 12, there is illustrated an alternate embodiment to that of FIG. 9. In this embodiment, the video source 902 has associated therewith an optical region 1202, which optical region 1202 has disposed therein an embedded video code. This embedded video code could be relatively complex or as simple as a grid of dark and white regions, each region in the grid able to have a dark color for a logic "1" or a white region for a logic "0." This will allow a digital value to be disposed within the optical region 1202. A sensor 1204 can then be provided for sensing this video code. In the example above, this would merely require an array of optical detectors, one for each region in the grid to determine whether this is a logic "1" or a logic "0" state. One of the sensed video is then output to the PC 906 for processing thereof to determine the information contained therein, which information contained therein constitutes the primary routing information 904. Thereafter, it is processed as described hereinabove with reference to FIG. 9.

Referring now to FIG. 13, there is illustrated a block diagram for an embodiment wherein a user's profile can be forwarded to the original subscriber or manufacturer. The PC 906 has associated therewith a profile database 1302, which profile database 1302 is operable to store a profile of the user 908. This profile is created when the program, after initial installation, requests profile information to be input in order to activate the program. In addition to the profile, there is also a unique ID that is provided to the user 908 in association with the browser program that runs on the PC 906. This is stored in a storage location represented by a block 1304. This ID 1304 is accessible by a remote location as a "cookie" which is information that is stored in the PC 906 in an accessible location, which accessible location is actually accessible by the remote program running on a remote node.

The ARS 308, which basically constitutes the PC 1004 of FIG. 10, is operable to have associated therewith a profile

database 1308, which profile database 1308 is operable to store profiles for all of the users. The profile database 1308 is a combination of the stored in profile database 1302 for all of the PCs 906 that are attachable to the system. This is to be distinguished from information stored in the database 310, the advertiser's database, which contains intermediate destination tables. When the routing information in the primary routing information 904 is forwarded to the ARS 308 and extracted from the original data packet, the look-up procedure described hereinabove can then be performed to determine where this information is to be routed. The profile database 1302 is then utilized for each transaction, wherein each transaction in the form of the routing information received from the primary routing information 904 is compared to the destination tables 310 to determine what manufacturer it is associated with. The associated ID 1304 that is transmitted along with the routing information in primary routing information 904 is then compared with the profile database 1308 to determine if a profile associated therewith is available. This information is stored in a transaction database 1310 such that, at a later time, for each routing code received in the form of the information in primary routing information 904, there will be associated therewith the IDs 1304 of each of the PCs 906. The associated profiles in database 1308, which are stored in association with IDs 1304, can then be assembled and transmitted to a subscriber as referenced by a subscriber node 1312 on the network 910. The ARS 308 can do this in two modes, a realtime mode or a non-realtime mode. In a realtime mode, each time a PC 906 accesses the advertiser database 310, that user's profile information is uploaded to the subscriber node 1312. At the same time, billing information is generated for that subscriber 1312 which is stored in a billing database 1316. Therefore, the ARS 308 has the ability to inform the subscriber 1312 of each transaction, bill for those transactions, and also provide to the subscriber 1312 profile information regarding who is accessing the particular product advertisement having associated therewith the routing information field 904 for a particular routing code as described hereinabove. This information, once assembled, can then be transmitted to the subscriber 1312 and also be reflected in billing information and stored in the billing information database 1316.

Referring now to FIG. 14, there is illustrated a flowchart depicting the operation for storing the profile for the user. The program is initiated in a block 1402 and then proceeds to a function block 1404, wherein the system will prompt for the profile upon initiation of the system. This initiation is a function that is set to activate whenever the user initially loads the software that he or she is provided. The purpose for this is to create, in addition to the setup information, a user profile. Once the user is prompted for this, then the program will flow to a decision block 1406 to determine whether the user provides basic or detailed information. This is selectable by the user. If selecting basic, the program will flow to a function block 1408 wherein the user will enter basic information such as name and serial number and possibly an address. However, to provide some incentive to the user to enter more information, the original prompt in function block 1404 would have offers for such things as coupons, discounts, etc, if the user will enter additional information. If the user selects this option, the program from the decision block 1406 to a function block 1410. In the function block 1410, the user is prompted to enter specific information such as job, income level, general family history, demographic information and more. There can be any amount of information collected in this particular function block.

Once all of the information is collected, in either the basic mode or the more specific mode, the program will then flow to a function block 1412 where this information is stored locally. The program then flows to a decision block 1414 to then go on-line to the host or the ARS 308. In general, the user is prompted to determine whether he or she wants to send this information to the host at the present time or to send it later. If he or she selects the "later" option, the program will flow to a function block 1415 to prompt the user at a later time to send the information. In the disclosed embodiment, the user will not be able to utilize the software until the profile information is sent to the host. Therefore, the user may have to activate this at a later time in order to connect with the host.

If the user has selected the option to upload the profile information to the host, the program will flow to the function block 1416 to initiate the connect process and then to a decision block 1418 to determine if the connection has been made. If not, the program will flow along a "N" path to a time to decision block 1420 which will time to an error block 1422 or back to the input of the connect decision block 1418. The program, once connected, will then flow along a "Y" path from decision block 1418 to a function block 1428 to send the profile information with the ID of the computer or user to the host. The ID is basically, as described hereinabove, a "cookie" in the computer which is accessed by the program when transmitting to the host. The program will then flow to a function block 1430 to activate the program such that it, at later time, can operate without requiring all of the set up information. In general, all of the operation of this flowchart is performed with a "wizard" which steps the user through the setup process. Once complete, the program will flow to a Done block 1432.

Referring now to FIG. 15, there is illustrated a flowchart depicting the operation of the host when receiving a transaction. The program is initiated at a start block 1502 and then proceeds to decision block 1504, wherein it is determined whether the system has received a routing request, i.e., the routing information 904 in the form of a tone, etc., embedded in the audio signal as described hereinabove with respect to FIG. 9. The program will loop back around to the input of decision block 1504 until the routing request has been received. At this time, the program will flow along the "Y" path to a function block 1506 to receive the primary routing information and the user ID. Essentially, this primary routing information is extracted from the audio tone, in addition to the user ID. The program then flows to a function block 1508 to look up the manufacturer URL that corresponds to the received primary routing information and then return the necessary command information to the originating PC 108 in order to allow that PC to connect to the destination associated with the primary routing information. Thereafter, the program will flow to a function block 1510 to update the transaction database 1310 for the current transaction. In general, the routing information 904 will be stored as a single field with the associated IDs. The profile database, as described hereinabove, has associated therewith detailed profiles of each user on the system that has activated their software in association with their ID. Since the ID was sent in association with the routing information, what is stored in the transaction database is the routing code, in association with all of the IDs transmitted to the system in association with that particular routing code. Once this transaction database has been updated, as described hereinabove, the transactions can be transferred back to the subscriber at node 312 with the detailed profile information from the profile database 1308.



The profile information can be transmitted back to the subscriber or manufacturer in the node 312 in realtime or non-realtime. A decision block 1512 is provided for this, which determines if the delivery is realtime. If realtime, the program will flow along a "Y" path to a function block 1514 wherein the information will be immediately forwarded to the manufacturer or subscriber. The program will then flow to a function block 1516 wherein the billing for that particular manufacturer or subscriber will be updated in the billing database 1316. The program will then flow into an End block 1518. If it was non-realtime, the program moves along the "N" path to a function block 1520 wherein it is set for a later delivery and it is accrued in the transaction database. In any event, the transaction database will accrue all information associated with a particular routing code.

With a realtime transaction, it is possible for a manufacturer to place an ad in a magazine or to place a product on a shelf at a particular time. The manufacturer can thereafter monitor the times when either the ads are or the products are purchased. Of course, they must be scanned into a computer which will provide some delay. However, the manufacturer can gain a very current view of how a product is moving. For example, if a cola manufacturer were to provide a promotional advertisement on, for example, television, indicating that a new cola was going to be placed on the shelf and that the first 1000 purchasers, for example, scanning their code into the network would receive some benefit, such as a chance to win a trip to some famous resort in Florida or some other incentive, the manufacturer would have a very good idea as to how well the advertisement was received. Further, the advertiser would know where the receptive markets were. If this advertiser, for example, had placed the television advertisement in ten cities and received overwhelming response from one city, but very poor response from another city, he would then have some inclination to believe that either one poor response city was not a good market or that the advertising medium he had chosen was very poor. Since the advertiser can obtain a relatively instant response and also content with that response as to the demographics of the responder, very important information can be obtained in a relatively short time.

It should be noted that the disclosed embodiment is not limited to a single source PC 302, but may encompass a large number of source computers connected over a global communication network. Additionally, the embodiment is not limited to a single ARS 308 or a single advertiser server 312, but may include a plurality of ARS and advertiser systems, indicated by the addition of ARS 314 and advertiser server A 316, respectively. It should also be noted that this embodiment is not limited only to global communication networks, but also may be used with LAN, WAN, and peer-to-peer configurations.

It should also be noted that the disclosed embodiment is not limited to a personal computer, but is also applicable to, for example, a Network Computer ("NetPC"), a scaled-down version of the PC, or any system which accommodates user interaction and interfaces to information resources.

One typical application of the above noted technique is for providing a triggering event during a program, such as a sport event. In a first example, this may be generated by an advertiser. One could imagine that, due to the cost of advertisements in a high profile sports program, there is a desire to utilize this time widely. If, for example, an advertiser contracted for 15 seconds worth of advertising time, they could insert within their program a tone containing the routing information. This routing information can then be output to the user's PC which will cause the user's PC to, via

the network, obtain information from a remote location typically controlled by the advertiser. This could be in the form of an advertisement of a length longer than that contracted for. Further, this could be an interactive type of advertisement. An important aspect to the type of interaction between the actual broadcast program with the embedded routing information and the manufacturer's site is the fact that there is provided in the information as to the user's PC and a profile of the user themselves. Therefore, an advertiser can actually gain realtime information as to the number of individuals that are watching their particular advertisement and also information as to the background of those individuals, demographic information, etc. This can be a very valuable asset to an advertiser.

In another example, the producer of the program, whether it be an on-air program, a program embedded in a video tape, CD-ROM, DVD, or a cassette, can allow the user to automatically access additional information that is not displayed on the screen. For example, in a sporting event, various statistics can be provided to the user from a remote location, merely by the viewer watching the program. When these statistics are provided, the advertiser can be provided with demographic information and background information regarding the user. This can be important when, for example, the user may record a sports program. If the manufacturer sees that this program routing code is being output from some device at a later time than the actual broadcast itself, this allows the advertisers to actually see that their program is still being used and also what type of individual is using it. Alternatively, the broadcaster could determine the same and actually bill the advertiser an additional sum for a later broadcast. This is all due to the fact that the routing information automatically, through a PC and a network, will provide an indication to the advertiser for other intermediary regarding the time at which the actual information was broadcast.

The different type of medium that can be utilized with the above embodiment are such things as advertisements, which are discussed hereinabove, contests, games, news programs, education, coupon promotional programs, demonstration media (demos), photographs, all of which can be broadcast on a private site or a public site. This all will provide the ability to allow realtime interface with the network and the remote location for obtaining the routed information and also allow for realtime billing and accounting.

Although the preferred embodiment has been described in detail, it should be understood that various changes, substitutions and alterations can be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

What is claimed is:

1. A method for controlling a computer disposed at a user location on a network, comprising the steps of:

inputting an analog signal at the user location on the network, the analog signal comprising a commerce identifier, which commerce identifier has an association with information disposed on a remote information provider location on the network;

in response to the step of inputting:

appending routing information to the commerce identifier, which routing information defines the location of the remote information provider location on the network;

creating a link between the user location and the remote information provider location over the network in accordance with the appended routing information,

15

which routing information defines the network connection between the user location and the remote location on the network; and  
transmitting the commerce identifier from the user location to the remote information provider location over the network utilizing the created link, wherein the information associated with the commerce identifier can be returned to the user location from the remote information provider location.

2. The method of claim 1, wherein the analog signal is input to a sound card on the computer.

3. The method of claim 1, wherein the step of appending routing information comprises the steps of:  
providing a database of routing information at a secondary location on the network which provides an association between a predetermined commerce identifier and a predefined remote information provider location on the network, there being a plurality of such routing information stored in the database;  
transmitting to the secondary location on the network the commerce identifier;  
accessing the database in response to receiving at the secondary location a transmitted commerce identifier from the user location;  
comparing the received commerce identifier with the stored routing information in the database;  
if there is a match between the received commerce identifier and any of the stored routing information, transmitting the matching routing information back to the user location; and  
at the user location, in response to receiving the matching routing information, appending the matching routing information to the commerce identifier.

4. The method of claim 3, and further comprising the step of displaying the received information from the remote information provider location.

5. The method of claim 1, wherein the network is a global communication network that provides a universal resource locator (URL) for each remote information provider location on the network and the routing information is comprised of the URL for the remote information provider location.

6. The method of claim 1, wherein the appended routing information in the step of appending includes instructional information as to how the remote information provider location is to process the transmitted commerce identifier.

7. A method for retrieving information from a storage region having a defined information provider location on a network, comprising the steps of:  
broadcasting a program having embedded therein an encoded signal having unique identifier information contained therein, wherein the unique identifier has an association with the location on the network of the storage region;  
extracting the encoded signal from the broadcast; and  
controlling a personal computer for a user at a user location on the network in response to the step of extracting to connect to the storage region on the network and retrieve information from the storage region at the defined location thereof on the network, which defined location is located with the extracted

16

encoded signal, and providing it at the personal computer for use by the user.

8. The method of claim 7, wherein the personal computer has a display associated therewith, wherein the retrieved information is displayed on the display.

9. The method of claim 7, wherein the broadcast program is a video program.

10. The method of claim 7, wherein the broadcast program is an audio program.

11. The method of claim 7, wherein the encoded signal comprises an audio signal and wherein the step of extracting comprises decoding the unique identifier information in the audio signal by the personal computer.

12. The method of claim 11, wherein the broadcast program is a video program.

13. The method of claim 11, wherein the broadcast program is an audio program.

14. The method of claim 11, wherein the step of extracting routing information comprises connecting the video source to the personal computer with a cable which carries at least audio information, the personal computer then decoding from the audio information in the step of extracting the unique identifier information from the encoded signal.

15. The method of claim 7, wherein the encoded signal is a video signal and the broadcast program is a video program and the step of extracting comprises extracting the unique identifier information from the video encoded signal.

16. The method of claim 7, wherein the storage region is disposed on a remote information provider location on the network, and the step of controlling comprises:  
transferring the extracted unique identifier information to an intermediate node on the network;  
storing at the intermediate node on the network lookup information associated with the location of the storage region on the network with the unique identifier information, such that the unique identifier information is associated with the location of the storage region on the network;  
looking up at the intermediate node the associated location of the storage region for the received unique identifier information and returning the location information to the personal computer; and  
the step of controlling using the returned location information to retrieve information from the storage region at the defined remote information provider location on the network.

17. The method of claim 16 and further comprising the step of storing at the intermediate node profile information associated with the user of the personal computer and storing at the personal computer identification information associated with the profile information at the intermediate node and further comprising the step of transmitting the identification information to the intermediate node when transmitting the unique identifier information thereto.

18. The method of claim 17, and further comprising the step of transmitting profile information from the intermediate node to the personal computer with the returned routing information, such that profile information is transmitted with the unique identifier information from the personal computer to the defined location on the network.

\* \* \* \* \*



US 20040187018A1

03 Jul 2012

2012100462

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2004/0187018 A1**

**Owen et al.** (43) **Pub. Date: Sep. 23, 2004**

(54) **MULTI-FACTOR AUTHENTICATION SYSTEM**

(52) **U.S. Cl. .... 713/200**

(76) **Inventors: William N. Owen, Atlanta, GA (US);  
Eric Shoemaker, Roswell, GA (US)**

(57) **ABSTRACT**

**Correspondence Address:  
Brian D MacDonald  
Morris Manning & Martin  
Suite 1125  
6000 Fairview Road  
Charlotte, NC 28210 (US)**

A suspect user (110) seeks access to a network resource from an access authority (150) utilizing a passcode received from an authentication authority (130). Initially, an ID of a device is bound with a PIN, the device ID is bound with a private key of the device, and the device ID is bound with a user ID that has been previously bound with a password of an authorized user. The device ID is bound with the user ID by authenticating the user ID using the password. Thereafter, the suspect user communicates the device ID and the PIN from the device over an ancillary communications network (112); the authentication authority responds back over the ancillary communications network with a passcode encrypted with the public key of the device; and the suspect user decrypts and communicates over a communications network (114) the passcode with the user ID to the access authority.

(21) **Appl. No.: 10/491,949**

(22) **PCT Filed: Oct. 9, 2002**

(86) **PCT No.: PCT/US02/32403**

(30) **Foreign Application Priority Data**

**Oct. 9, 2001 (US)..... 60328310**

**Publication Classification**

(51) **Int. Cl.<sup>7</sup> ..... H04L 9/32**

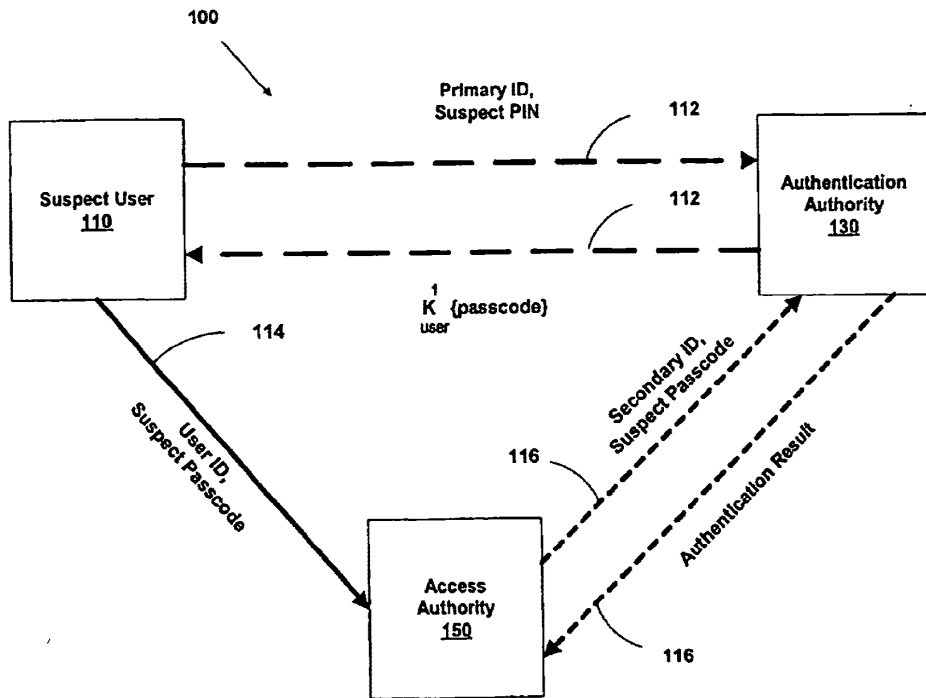


FIG. 1

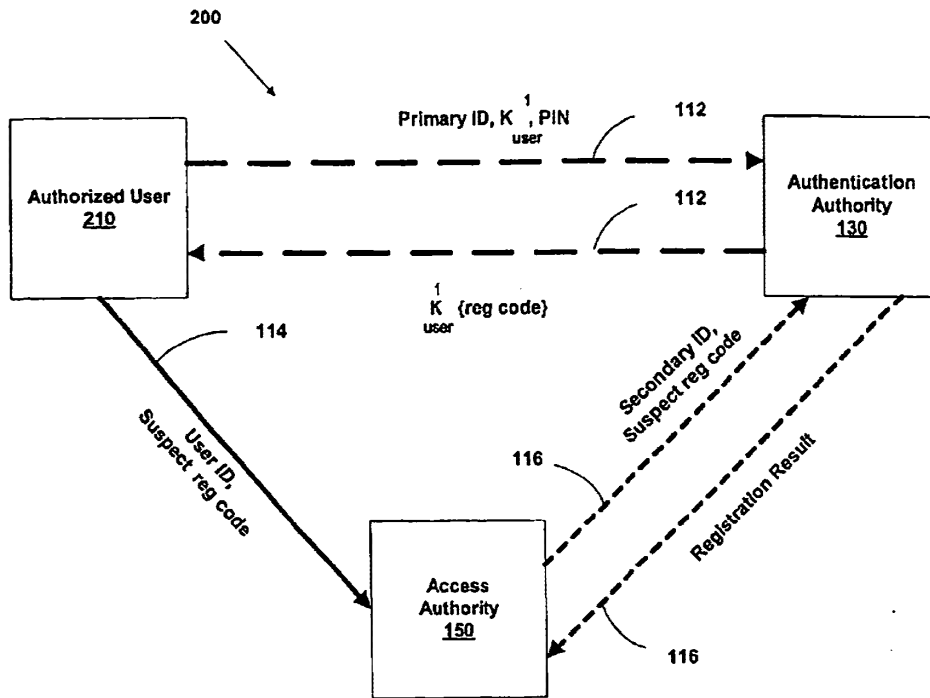


FIG. 2

2012100462 03 Jul 2012

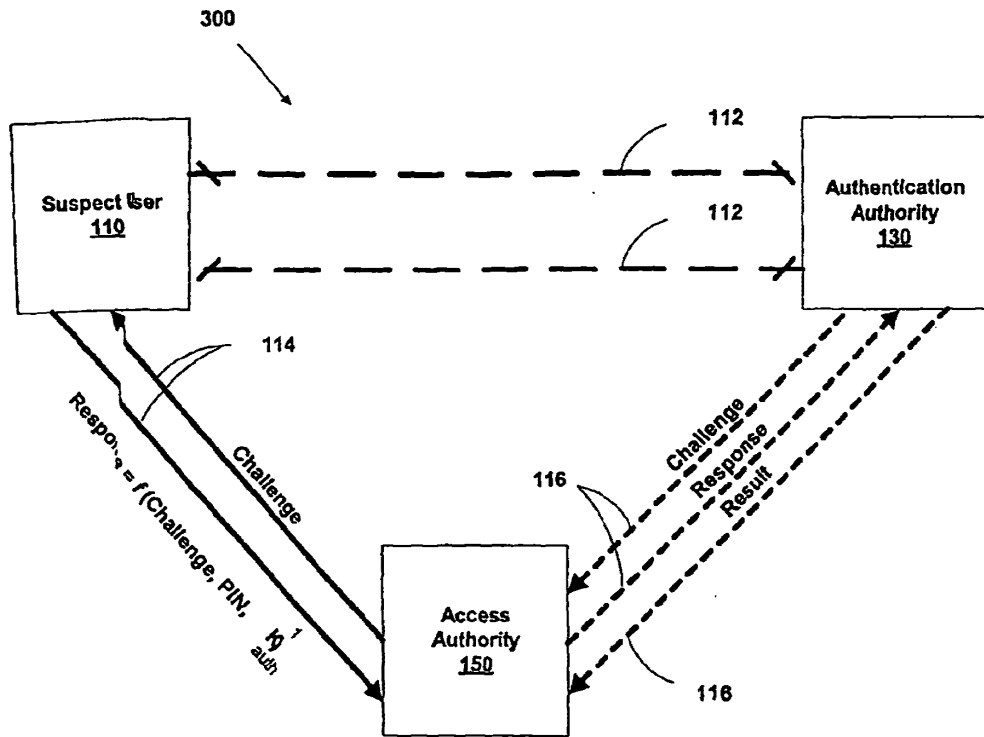


FIG. 3

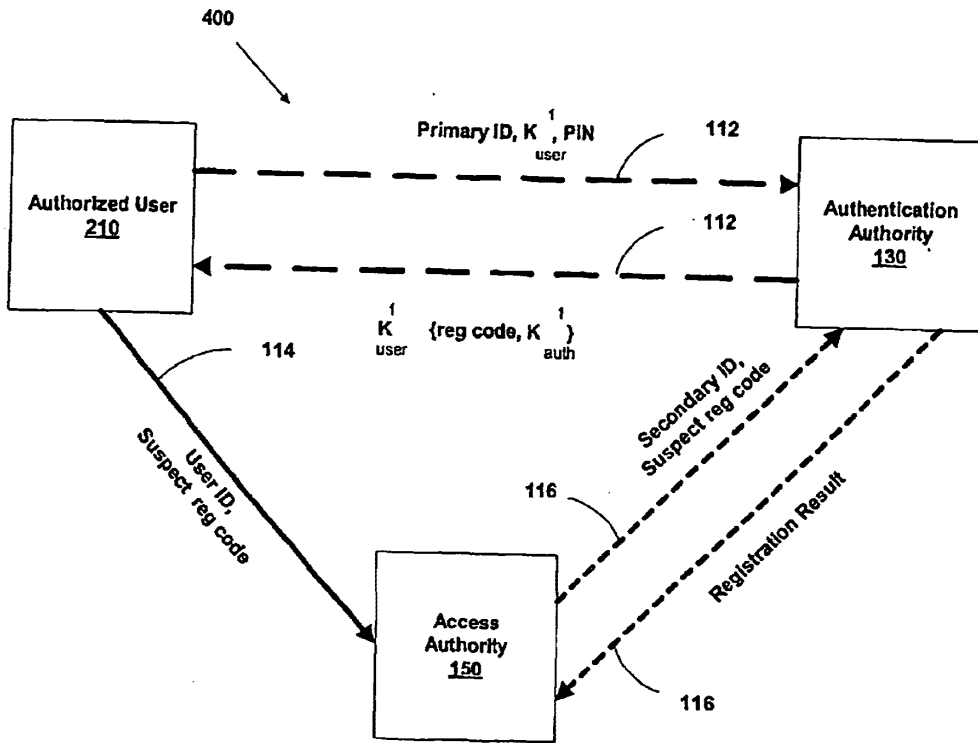


FIG. 4

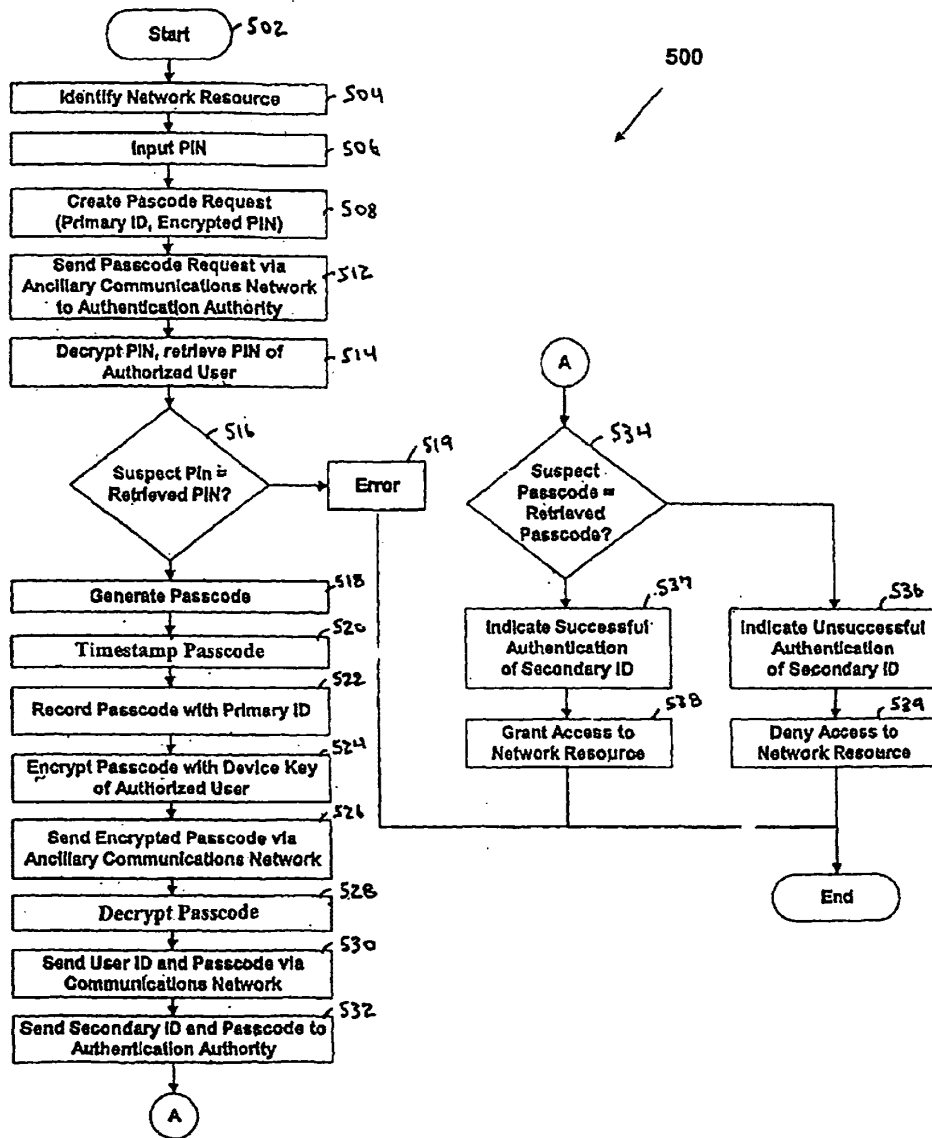


FIG. 5



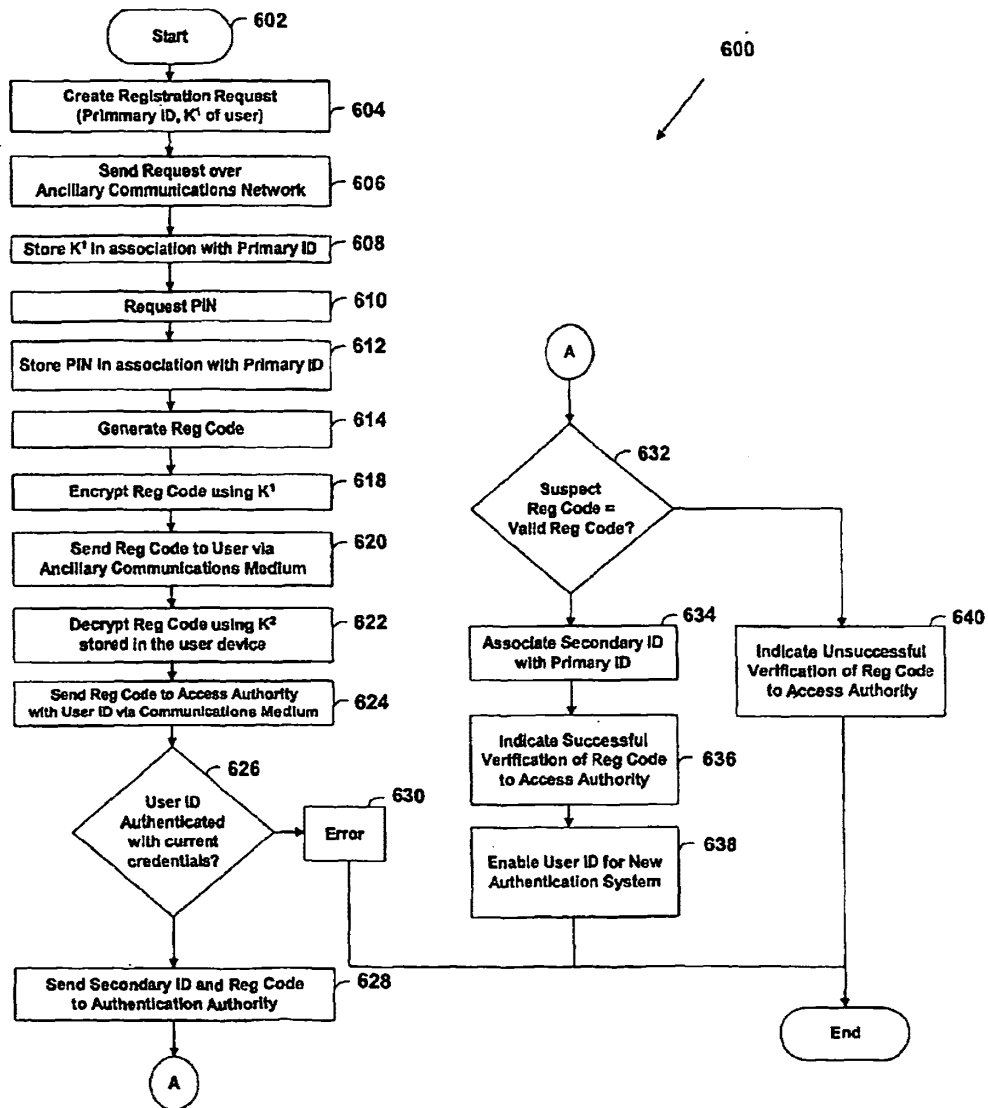


FIG. 6

2012100462 03 Jul 2012

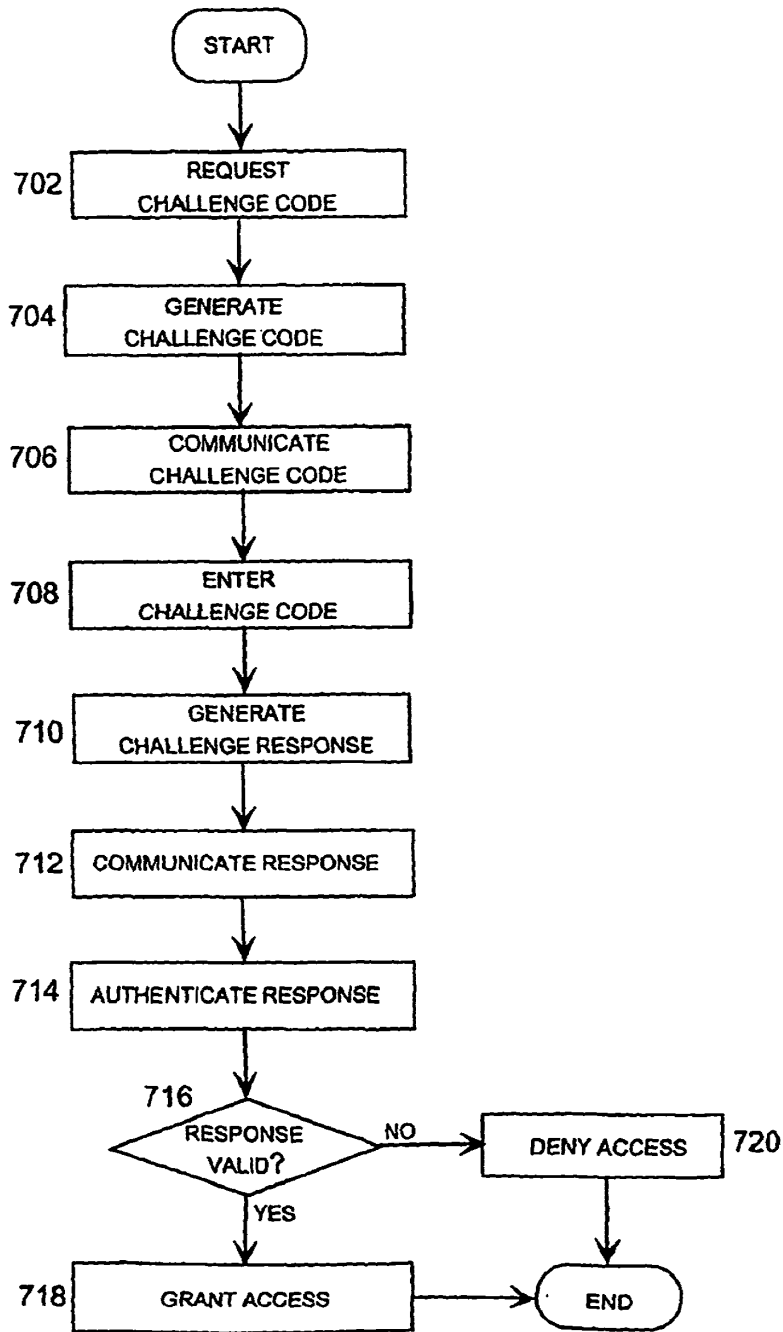
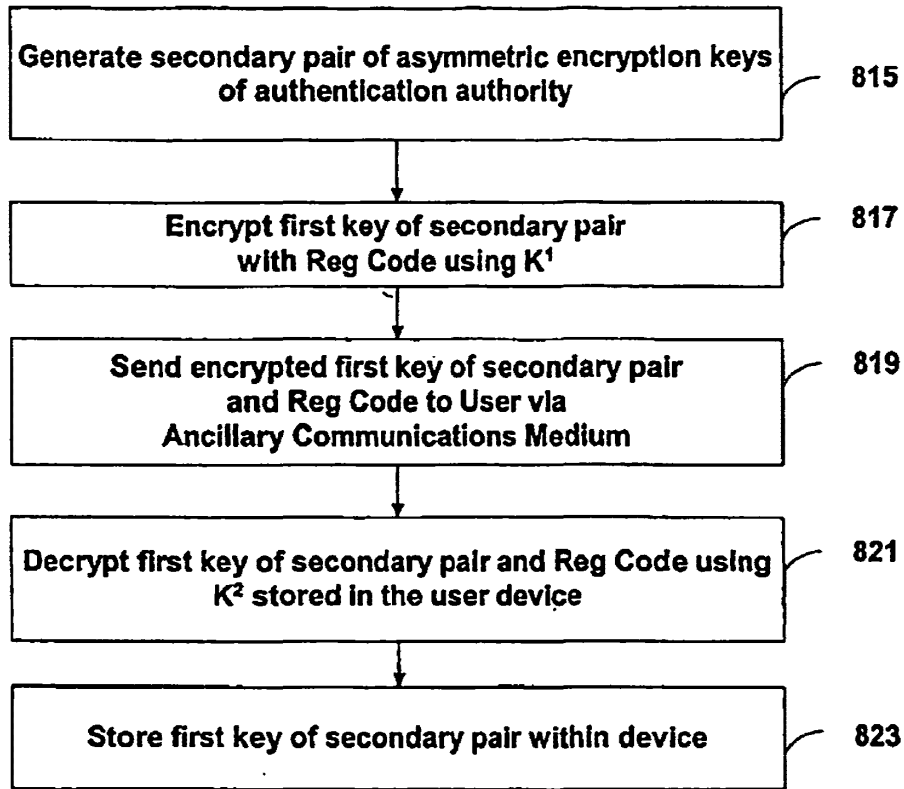


FIG.7

2012100462 03 Jul 2012



**FIG. 8**

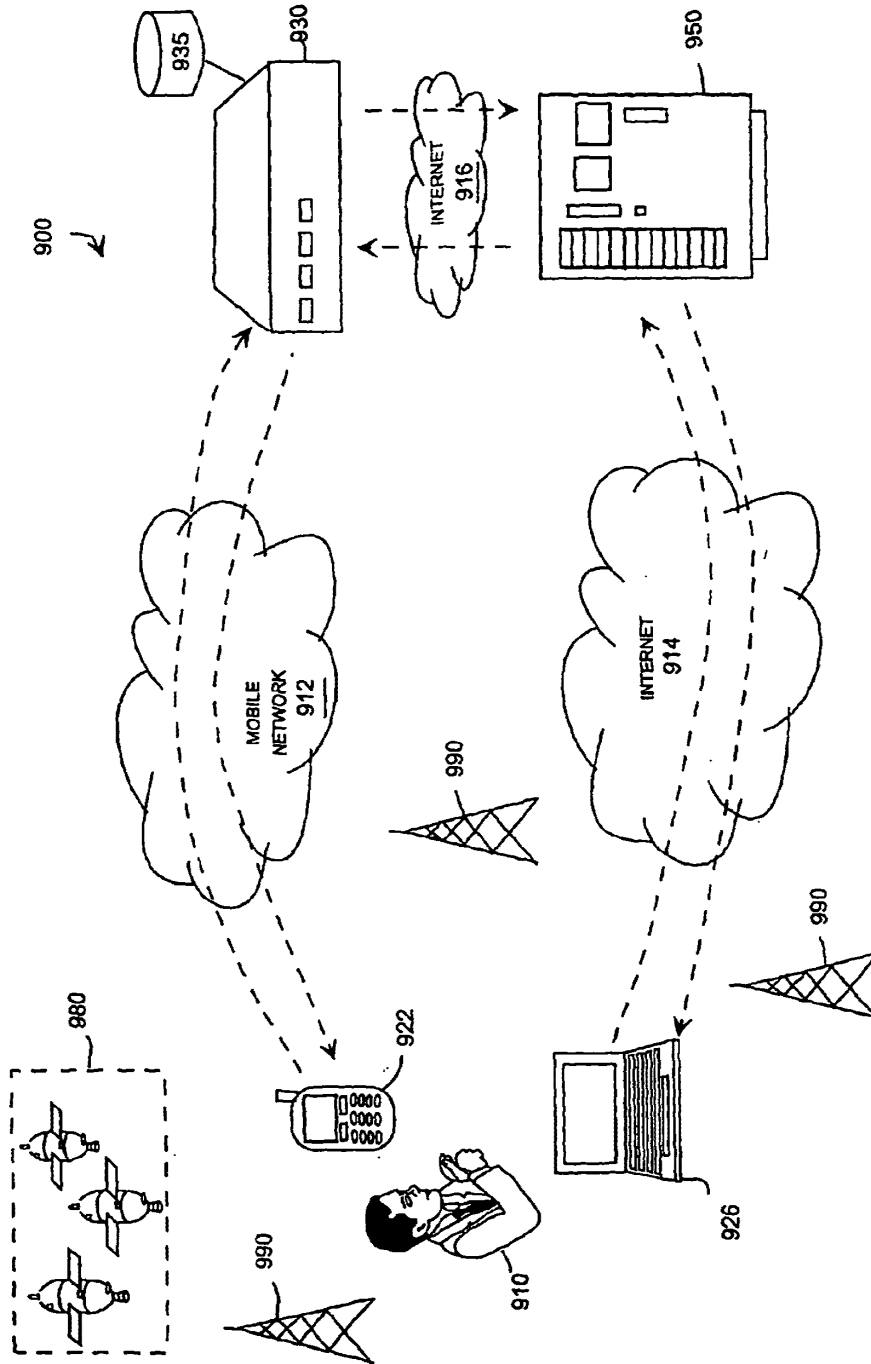


FIG. 9

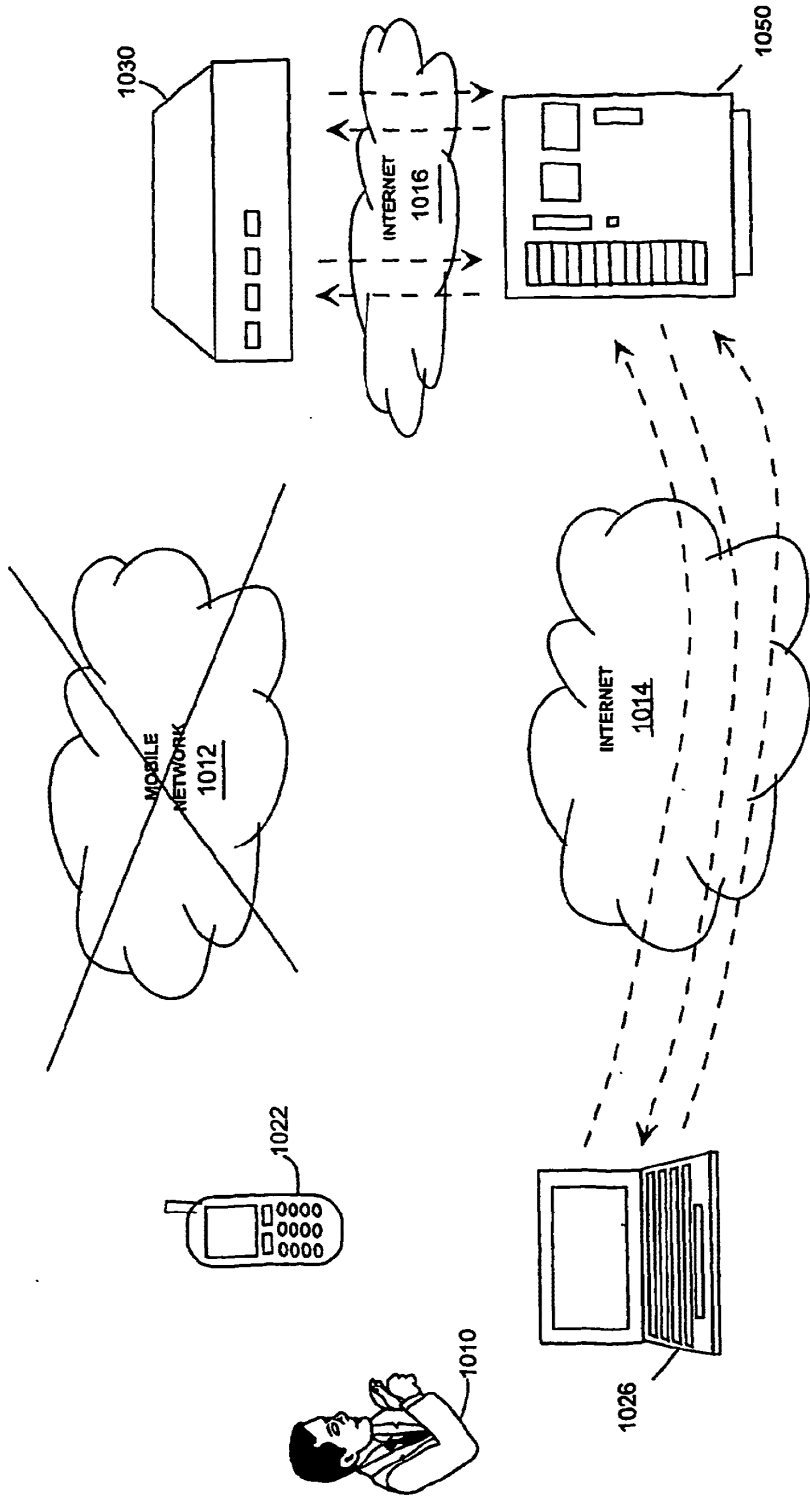


FIG. 10

### MULTI-FACTOR AUTHENTICATION SYSTEM

[0001] A portion of disclosure of this patent document including said computer code contains material that is subject to copyright protection. The copyright owner has no objection to the reproduction by anyone of the patent document or the patent disclosure in its entirety, as it appears in the patent file or records of the U.S. Patent & Trademark Office, WIPO, or other governmental organization, but otherwise reserves all copyrights whatsoever.

### FIELD OF THE PRESENT INVENTION

[0002] The present invention generally relates to authentication systems and, in particular, to a multi-factor authentication system used for authenticating a suspect user seeking access to a network resource from an access authority of a computer network.

### BACKGROUND OF THE PRESENT INVENTION

[0003] A user ID and password often is required in order for a suspect user to gain access to a network resource from an access authority of a computer network. In such a system, the network resource may comprise an application, service, or device of the computer network, or even access to the computer network itself. The access authority may comprise a server of the computer network, which grants access once the user ID has been authenticated using the password received from the suspect user. Moreover, the access authority may include security privileges for granting specific types of access by authenticated users, and the access authority may additionally perform the authentication of suspect users.

[0004] The increasing number of systems each requiring a user ID and password in order for a suspect user to gain access to a network resource ultimately confuses users. To reduce confusion, users typically choose easy-to-remember passwords. Otherwise, users tend to forget complex passwords and record the passwords in easily accessible areas for later reference. For example, many users maintain a list of user IDs and passwords in a spreadsheet or text file on their computer or personal digital assistant. Programs even have been written to help maintain user ID and password combinations.

[0005] Enterprises, such as corporations, Internet service providers, portals, application service providers (ASPs), e-commerce providers, online financial services, etc., must manage user IDs and passwords for their users. Allowing users to employ simple passwords reduces security at a time when security attacks are increasing and are increasingly expensive when they occur. On the other hand, enforcing the use of complex passwords and requiring passwords to be changed frequently increases security, but also increases cost in the form of help desk and customer service calls for the resetting of passwords. The systems that have been developed to allow users to use personal information to reset a password automatically without human intervention tend to be less secure because personal information can be guessed or obtained surreptitiously. Some systems, for example, use information from credit reports—despite the fact that credit bureaus are in the business of proactively selling that information.

[0006] For user convenience, single sign-on systems also have been developed in which a user is able to authenticate to a single trusted authentication server, which then propagates that authentication to multiple access authorities. While the use of a single authentication server eases the user burden of remembering multiple passwords for accessing various network resources, such a system typically is limited to accessing network resources of a single enterprise. Such a system also is susceptible to a security problem known as “keys to the kingdom.” If an attack gains access to the user ID and password required to authenticate to the authentication server, then access to all network resources relying upon that authentication server are compromised.

[0007] Stronger forms for authenticating user IDs also have been developed beyond the single-factor authentication employed in using passwords. Notably, hardware tokens such as USB tokens and time-based tokens—RSA’s SecureID is an example—are now being utilized in some multi-factor authentication systems wherein these tokens are able to uniquely identify themselves. For example, a token utilizing physical access to a device and knowledge of a shared secret, such as a PIN, can construct a rotating key that matches a synchronized server key. Such a system is a “two-factor” authentication system because it requires something the user has, i.e., the token, in addition to something the user knows, i.e., the password. Unfortunately, each token in one of these two-factor authentication system is expensive, subject to loss, and typically restricted to use with one or more network resources of a particular computer network.

[0008] In view of the foregoing, a need exists for an improved multi-factor authentication system that overcomes one or more of the aforementioned disadvantages of current authentication systems. One or more of these disadvantages are overcome by one or more embodiments of the present invention, as described in detail below.

### SUMMARY OF THE PRESENT INVENTION

[0009] Briefly described, the present invention relates to multi-factor authentication systems.

### A FIRST ASPECT OF THE PRESENT INVENTION

[0010] With regard to a first aspect of the present invention, both a PIN of a user authorized to access a network resource and a first key of an asymmetric key pair of the authorized user are maintained in association with a first primary identification by an authentication authority such that each of the PIN and the first key are retrievable based on the first primary identification. Within this system, a method of the first aspect of the present invention is performed by the authentication authority whereby the authorized user gains access to the network resource from an access authority by utilizing a passcode. The method includes the steps of: receiving the first primary identification and a suspect PIN from a suspect user; authenticating the first primary identification by considering at least one authentication factor, including comparing the suspect PIN with the PIN of the authorized user maintained in association with the first primary identification by the authentication authority; and following a successful authentication of the first primary identification, generating the passcode.

encrypting the passcode using the first key of the asymmetric key pair of the authorized user, and communicating the encrypted passcode to the suspect user for subsequent decryption and presentation to the access authority.

[0011] The first primary identification may include a device ID and/or a domain ID that identifies the access authority for the network resource. Preferably, the primary identification includes both the device ID and the domain ID. Furthermore, the device ID may be an identification of a personal communications device, such as, for example, a PDA, a mobile phone (cellular or digital), or a two-way pager device like a RIM Blackberry wireless unit.

[0012] The authorized user preferably gains access to the network resource over a communications network, and the first primary identification and suspect PIN preferably is received by the authentication authority over a communications medium different from the communications network. The communications network may comprise, for example, the Internet or an intranet. The communications medium may comprise a telecommunications network. Preferably, the suspect PIN is received encrypted with a first key of an asymmetric key pair of the authentication authority, with the key pair of the authentication authority is generally unique to the domain ID.

[0013] The method preferably includes the further steps of: receiving a suspect passcode from the access authority; comparing the suspect passcode with the passcode that was encrypted and communicated to the suspect user by the authentication authority; and communicating a result of the comparison to the access authority. Additionally, the passcode preferably must be received by the access authority and/or the authentication authority within a predetermined amount of time after being generated in order for the user to gain access to the network resource. The predetermined period of time preferably is short, such as less than ninety seconds in some instances or less than an hour in other instances.

[0014] The passcode communicated to the suspect user preferably is maintained by the authentication authority such that the passcode is retrievable based on a first secondary identification. The first secondary identification comprises the combination of (i) a user ID that represents an identification of the authorized user to the access authority, and (ii) the domain ID. The passcode received by the access authority preferably is communicated to the authentication authority with the user ID.

[0015] In a feature of this method, biometric information of the authorized user further is maintained in association with the first primary identification such that the biometric information is retrievable based on the first primary identification, and the step of considering at least one authentication factor by the authentication authority further includes comparing suspect biometric information received with the first primary identification with the biometric information of the authorized user maintained in association with the first primary identification by the authentication authority. Such biometric information may include individual physical characteristics believed to be unique to a user, such as a retinal pattern, fingerprint, or voice pattern.

[0016] In another feature of this method, a geographical location for the authorized user is maintained in association

with the first primary identification such that the geographical information is retrievable based on the first primary identification, and the step of considering at least one authentication factor by the authentication authority further includes comparing a geographical location identified as the origin of communication of the suspect PIN with the geographic location maintained in association with the first primary identification by the authentication authority.

[0017] In yet another feature of this method, a time range for the authorized user is maintained in association with the first primary identification such that the time range is retrievable based on the first primary identification. In this feature, the step of considering at least one authentication factor by the authentication authority further includes comparing with the time range with a time of receipt of the first primary authentication and the suspect PIN. The time range may comprise a window of time or a plurality of discontinuous windows of time for permitted receipt of the suspect PIN, such as during only the daily hours of 6am to midnight, or only business hours for weekdays and mornings on weekends.

[0018] In accordance with the first aspect of the present invention, the authorized user is additionally authorized to access a second network resource, and both a second PIN of the authorized user and a first key of a second asymmetric key pair of the authorized user are maintained by the authentication authority in association with a second primary identification such that each of the second PIN and the first key of the second key pair of the authorized user are retrievable based on the second primary identification. Furthermore, in preferred embodiments the second asymmetric key pair may in fact be the same as the first asymmetric key pair.

[0019] Moreover, the method preferably includes the additional steps of: receiving the second primary identification and a suspect second PIN; authenticating the second primary identification by considering at least one authentication factor, including comparing the suspect second PIN with the second PIN of the authorized user maintained in association with the second primary identification by the authentication authority; and following a successful authentication of the second primary identification, generating a second passcode, encrypting the second passcode using the first key of the second asymmetric key pair of the authorized user, and communicating the encrypted second passcode to the suspect user for subsequent decryption and presentation to the access authority.

[0020] The second primary identification preferably comprises the combination of the device ID and a second domain ID, and the second passcode communicated to the suspect user preferably is maintained by the authentication authority such that the second passcode is retrievable based on a second secondary identification. The second secondary identification preferably comprises the combination of (i) a second user ID that represents an identification of the authorized user to an access authority with respect to the second network resource, and (ii) the second domain ID.

[0021] Additionally, a first key of a second asymmetric key pair of the authentication authority preferably is maintained by the authentication authority in association with the second domain ID such that the first key is retrievable based on the second domain ID, with the second key pair being generally unique to the second domain ID.

#### A SECOND ASPECT OF THE PRESENT INVENTION

[0022] With regard to a second aspect of the present invention, both a PIN of a user authorized to access a network resource and a first key of an asymmetric key pair generally unique to a personal communications device of the authorized user are maintained by an authentication authority in association with an identifier such that each of the PIN and the first key are retrievable based on the identifier.

[0023] Within this system, the second aspect relates to a method whereby the authorized user gains access to the network resource from an access authority. The method includes the steps of: receiving a challenge request with respect to a suspect user seeking to gain access to the network resource from the access authority; in response to the challenge request, communicating a challenge to the suspect user, receiving a challenge response and the identifier; and authenticating the identifier by comparing the challenge response to a function of the challenge, the PIN maintained by the authentication authority in association with the identifier, and the first key maintained by the authentication authority in association with the identifier. The key pair preferably is generated by the authentication authority and the first key of the key pair is communicated by the authentication authority to the personal communications device of the authorized user. Furthermore, the first key preferably is communicated to the personal communications device of the authorized user upon initial receipt of the PIN from the authorized user for maintaining in association with the identifier.

[0024] The function preferably includes the hashing of the challenge, PIN, and first key. The identifier preferably includes a user ID that identifies the authorized user to an access authority that grants access to the network resource and, additionally, a domain ID that identifies the access authority for the network resource. The identifier thus preferably comprises the secondary ID of the aforementioned preferred methods.

[0025] In other preferred embodiments of this aspect of the present invention, the function preferably includes the hashing of the (i) challenge, (ii) PIN, and (iii) first key of the asymmetric pair that is generally unique to the user device and that was provided by the authentication authority, as well as (i) a first key of an asymmetric key pair that is generally unique to the user device but that was generated within the device and not provided by the authentication authority, (ii) a first key of a key pair of the authentication authority that is generally unique to the domain ID, and (iii) the domain ID itself.

#### A THIRD ASPECT OF THE PRESENT INVENTION

[0026] A third aspect of the present invention relates to a method for gaining access by a user to a network resource. The method includes the steps of: communicating a PIN and a first primary identification over an ancillary communications network to an authentication authority; receiving an encrypted passcode over the ancillary communications network from the authentication authority; decrypting the passcode using a key of an asymmetric key pair; and communicating the passcode and a user ID over a communications network to an access authority. Additionally, the method

preferably includes the additional step of manually entering the PIN into the personal communications device for communicating the PIN over the ancillary communications network to the authentication authority. Preferably, the encrypted passcode is received and decrypted by the personal communications device, and the key with which the passcode is decrypted preferably is stored within and generally unique to the personal communications device. The passcode and the user ID also preferably are communicated over the communications network using another device different from the personal communications device, such as a laptop or desktop computer.

[0027] The method preferably further includes the step of manually reading the passcode from a display of the personal communications device for communicating the passcode over the communications network. The method also preferably includes the additional steps of communicating a second PIN and a second primary identification over the ancillary communications network to the authentication authority, receiving a second encrypted passcode over the ancillary communications network from the authentication authority, decrypting the second passcode using a key of a second asymmetric key pair; and communicating the passcode and a second user ID over the communications network to another access authority.

#### A FOURTH ASPECT OF THE PRESENT INVENTION

[0028] A fourth aspect of the present invention relates to a method for registering for access by an authorized user with respect to a network resource. The method includes the steps of: generating a first asymmetric key pair generally unique to a device of the authorized user; communicating in association with a device ID of the device to an authentication authority over an ancillary communications network both a first key of the first asymmetric key pair and a PIN of the authorized user; receiving an encrypted registration code over the ancillary communications network from the authentication authority; decrypting the registration code using the second key of the first asymmetric key pair of the device; and communicating the registration code to an access authority over a computer network in associating with a user ID that identifies the authorized user to the access authority. Preferably, the PIN is not stored within the device following its encryption and communication to the authentication authority and wherein the second key of the key pair of the device is not exported from the device.

#### A FIFTH ASPECT OF THE PRESENT INVENTION

[0029] A fifth aspect of the present invention relates to a method in which an authorized user is registered with an authentication authority for later authenticating of a suspect user seeking to gain access from an access authority to a network resource. The method includes the steps of: generating within a device of the authorized user a first asymmetric key pair of the authorized user that is generally unique to the device, and communicating with the device a first key of the first asymmetric key pair in association with a device ID of the device to the authentication authority over an ancillary communications network; receiving and maintaining by the authentication authority the first key in association with the device ID, and communicating by the



authentication authority to the device of the authorized user over the ancillary communications network a first key of a first key asymmetric key pair of the authentication authority that is generally unique to a domain ID; encrypting by the authorized user with the device using the first key of the asymmetric key pair of the authentication authority a PIN of the authorized user that is entered into the device, and communicating by the authorized user the encrypted PIN in association with the device ID to the authentication authority over the ancillary communications network; decrypting by the authentication authority the PIN and maintaining the PIN in association with the device ID and the domain ID, encrypting by the authentication authority using the first key associated with the device ID a registration code, and communicating by the authentication authority the registration code to the device of the authorized user over the ancillary communications network; decrypting by the authorized user within the device the encrypted registration code using the second key of the first asymmetric key pair of the authorized user, and communicating by the authorized user over a communications network the registration code to an access authority in association with a user ID identifying the authorized user to the access authority; and comparing the registration code received with the user ID with the registration code encrypted and sent to the authorized user. Preferably the PIN is not stored within the device following its encryption and communication to the authentication authority, and preferably the first key of the key pair of the device is not exported from the device. Moreover, the first asymmetric key pair of the authorized user preferably is generally unique to the domain ID.

[0030] The method preferably further includes the step of communicating by the access authority the user ID and the registration code to the authentication authority, and the step of comparing the registration code received with the user ID with the registration code encrypted and sent to the user is performed by the authentication authority. In this regard, the device ID preferably is communicated by the access authority with the registration code to the access authority. The user ID preferably is maintained by the authentication authority in association with the device ID such that a passcode maintained in association with the device ID is retrievable based on the user ID and/or the device ID.

#### A SIXTH ASPECT OF THE PRESENT INVENTION

[0031] A sixth aspect of the present invention relates to a method of granting access to a suspect user seeking to access a network resource. This method includes the steps of first, (i) maintaining credentials of the authorized user such that the credentials are retrievable based on the user ID, (ii) receiving a user ID, registration code, and suspect credentials, (iii) comparing the suspect credentials with the credentials maintained in association with the user ID, and (iv) upon a successful authentication of the user ID by matching the suspect credentials with the maintained credentials, communicating the user ID and registration code to an authentication authority. The credentials of the authorized user include (i) a password of the authorized user and/or (ii) information transmitted from a token of an authorized user, including a temporal-based or sequential-based value. Thereafter, the method includes the steps of granting access to the network resource to a suspect user upon, (i) receiving a user ID and passcode from the suspect user, (ii) commu-

nicating the user ID and passcode to the authentication authority, and (iii) receiving an indication of a successful passcode comparison by the authentication authority.

[0032] In accordance with the sixth aspect, the method preferably further includes the steps of additionally receiving suspect credentials with the user ID and passcode, comparing the suspect credentials with the password maintained in association with the user ID, and communicating the user ID to the authentication authority only upon a successful match of the suspect credentials with the maintained credentials.

#### A SEVENTH ASPECT OF THE PRESENT INVENTION

[0033] A seventh aspect of the present invention relates to a method of upgrading a single-factor authentication system to a two-factor authentication system wherein a suspect user seeks access to a network resource and the single-factor authentication system includes the binding of a user ID with credentials of an authorized user. The method of the seventh aspect includes the steps of: (i) initially binding a device ID of a device with a PIN, (ii) binding the device ID with a private key of the device, and (iii) binding the device ID with the user ID, including authenticating the user ID with the credentials; and, thereafter, (i) authenticating the device ID including, as part thereof, communicating from the device the device ID and the PIN over an ancillary communications network, (ii) authenticating the device including, as part thereof, communicating to the device over the ancillary communications network a passcode encrypted with the public key corresponding to the device private key, and (iii) communicating the unencrypted passcode over a communications network with the user ID.

#### OTHER ASPECTS AND FEATURES

[0034] Other aspects of the present invention include, inter alia, computer-readable media having computer-executable instructions for performing part or all of the methods of the aforementioned aspects of the present invention and modifications and variations thereof.

[0035] In aspects of the present invention, additional features include: the device as a wireless device, a GPS device, and/or a JAVA-enabled device; the ancillary communications network as a trusted network; the communications network as an untrusted network; and transporting communications over the communications network and/or the ancillary communications network using a secure transport protocol. Moreover, the authentication authority may comprise a program, module, or a server, or refer to an entity maintaining such program, module, or server, and the access authority may comprise a second program, module, or server, or refer to a second entity maintaining the second program, module, or server. In either case, the authentication authority and the access authority preferably are distinct. Indeed, the authentication authority preferably works in conjunction with several access authorities in accordance with these aspects of the present invention.

[0036] These and other features of the invention will be more readily understood upon consideration of the attached drawings and of the following detailed description of those drawings and the presently preferred embodiments of the invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0037] Further features and benefits of the present invention will be apparent from a detailed description of preferred embodiments thereof taken in conjunction with the following drawings, wherein similar elements are referred to with similar reference numbers, and wherein:

[0038] FIG. 1 illustrates a first preferred multi-factor authentication system according to the present invention;

[0039] FIG. 2 illustrates a preferred system for user registration for the multi-factor authentication system of FIG. 1;

[0040] FIG. 3 illustrates a second preferred multi-factor authentication system according to the present invention;

[0041] FIG. 4 illustrates a preferred system for user registration for the multi-factor authentication system of FIG. 3;

[0042] FIG. 5 illustrates a flowchart of steps of a method of the multi-factor authentication system of FIG. 1;

[0043] FIG. 6 illustrates a flowchart of steps of a method of the preferred, user registration system of FIG. 2;

[0044] FIG. 7 illustrates a flowchart of steps of a method of the multi-factor authentication system of FIG. 3;

[0045] FIG. 8 illustrates a flowchart of steps of a method of the preferred user registration system of FIG. 4;

[0046] FIG. 9 illustrates a first preferred commercial embodiment of a multi-factor authentication system according to the present invention; and

[0047] FIG. 10 illustrates a second preferred commercial embodiment of a multi-factor authentication system according to the present invention.

## DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

[0048] As a preliminary matter, it will readily be understood by those persons skilled in the art that the present invention is susceptible of broad utility and application in view of the following detailed description of the preferred devices and methods of the present invention. Many devices, methods, embodiments, and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the following detailed description thereof, without departing from the substance or scope of the present invention. Accordingly, while the present invention is described herein in detail in relation to preferred devices, methods and systems, it is to be understood that this disclosure is illustrative and exemplary and is made merely for purposes of providing a full and enabling disclosure of the preferred embodiments of the invention. The disclosure herein is not intended nor is to be construed to limit the present invention or otherwise to exclude any such other embodiments, adaptations, variations, modifications and equivalent arrangements, the present invention being limited only by the claims appended hereto and the equivalents thereof.

[0049] Furthermore, as used herein, "PIN," "passcode," and "password" each broadly refers to a shared secret used

for authentication purposes and all are considered synonyms herein, with none intended to imply any particular syntax of the secret itself.

[0050] The use of "asymmetric key pair" refers to a pair of keys in which that encrypted with at least one of the keys may be decrypted only with the second key. However, in accordance with the present invention, that encrypted with the second key may or may not be decrypted with the first key.

[0051] Finally, in accordance with the present invention, "ancillary communications network" and "communications network" identify different communications networks, with the ancillary communications network referring to a communications network between a user and an authentication authority over which a PIN is sent and a passcode is received by the user, and with "communications network" referring to a communications network between a user and an access authority over which the passcode is sent by the user to the access authority. The ancillary communications network preferably comprises a telecommunications network and the communications network preferably comprises a computer network. Furthermore, a network resource preferably is accessed by the user over the communications network through which the user communicates with the access authority. The communications network and the ancillary communications network also may overlap to certain extents such as, for example, where a computer utilizes a telephone line to connect to an Internet service provider.

[0052] With reference now to FIG. 1, a preferred embodiment of a multi-factor authentication system 100 in accordance with the present invention is illustrated. The system 100 includes a suspect user 110, an authentication authority 130, and an access authority 150. The suspect user 110 seeks to gain access to a network resource from the access authority 150 utilizing an encrypted passcode provided to the suspect user 110 by the authentication authority 130.

[0053] Specifically, when the suspect user 110 desires to gain access to the network resource, the suspect user 110 communicates to the authentication authority 130 over an ancillary communications network 112 a primary ID and a suspect PIN. In response, the authentication authority 130 compares the suspect PIN with a PIN of an authorized user that is retrieved based on the primary ID. If the suspect PIN matches the retrieved PIN of the authorized user, and if the primary ID otherwise successfully authenticates, then the authentication authority 130 communicates back to the user 110 over the ancillary communications network 112 a passcode that is encrypted with a first key ( $K^1$ ) of an asymmetric key pair of the authorized user. The authentication authority 130 maintains the passcode in association with the primary ID in the computer-readable storage medium.

[0054] The passcode comparison may be the only factor considered by the authentication authority 130 at this time. Alternatively, the authentication authority 130 also may utilize additional factors in authenticating the device ID. Thus, for example, since the device can utilize a telecommunications network such as a wireless network, the geographical location of the user 110 at the time of generating the passcode request can be determined. An authorized user can set the boundaries of the geographical locations from which a valid password request can originate. Additionally, certain time ranges can also be set. Furthermore, a geo-

graphical location can be coupled with a time range. For example, on weekdays during working hours, a valid request may only originate from an area around the user's office, while a residence may be valid during the weekends. In addition, the system 100 can track usage patterns and determine if a request is within normal parameters. Furthermore, voice patterns and other biometrics of the user 110 can be stored at the authentication authority 130 and utilized for authentication.

[0055] In any event, upon the receipt of an encrypted passcode by the suspect user 110, the suspect user 110 decrypts the encrypted passcode using a second key of the asymmetric key pair and communicates to the access authority 150 over a communications network 114 a suspect passcode and a user ID of the authorized user. The user ID identifies the authorized user to the access authority 150.

[0056] The access authority 150, in turn, communicates the suspect passcode and, if the passcode itself also does not already serve as a secondary ID to identify the suspect user 110 to the authentication authority 130, then a secondary ID of the suspect user 110 is also included with the suspect passcode in the communication to the authentication authority 130. The access authority 150 may communicate the suspect passcode over the ancillary communications network 112, the communications network 114, or yet a third communications network, and the particular communications network itself that is utilized by the access authority 150 in communicating with the authentication authority 130 forms no part of the broadest definitions of the invention herein.

[0057] In response to the access authority 150 communicating the suspect passcode to the authentication authority 130, and based on the secondary ID of the suspect user 110, the authentication authority 130 then authenticates the secondary ID by comparing the suspect passcode with the passcode previously encrypted and communicated to the suspect user 110. The authentication authority 130 then communicates an indication of the result of the passcode comparison back to the access authority 150. The access authority 150, in turn, grants access to the network resource to the suspect user 110 as a function of the authentication result received from the authentication authority 130. In other words, if the suspect user 110 is an authorized user of the network resource based on the authentication result, then the suspect user 110 is granted access to the network resource by the access authority 150. Conversely, if the suspect user 110 is not an authorized user of the network resource based on the authentication result, then the suspect user 110 is not granted access to the network resource by the access authority 150.

[0058] With reference to FIG. 2, a registration system 200 is illustrated by which an authorized user 210 registers with the authentication authority 130 for later seeking access to the network resource from the access authority 150 in accordance with the system 100 of FIG. 1. The authentication authority 130 is identified by inputting a server code—preferably of only twelve digits—into the user device as more fully described below with reference to commercial embodiments.

[0059] In the registration system 200, the authorized user 210 provides his or her primary ID, the first key ( $K^1_{user}$ ), and PIN to the authentication authority 130 over the ancillary

communications network 112, and the authentication authority 130 provides its first key ( $K^1_{auth}$ ) to the authorized user 110 together with configuration information. In particular, a preferred sequence of communications in this key exchange includes: first, the provision of the primary ID with a registration request made to the authentication authority 130 and, in response thereto, the provision of the first key ( $K^1_{auth}$ ) of the authentication authority 130 to the authorized user 110; and, second, the provision of the first key ( $K^1_{user}$ ) of the user in combination with the PIN to the authentication authority 130, all encrypted with the first key ( $K^1_{auth}$ ) of the authentication authority 130. Preferably, this key exchange occurs entirely over the ancillary communication network 112.

[0060] The authentication authority 130 receives and maintains the first key and PIN of the authorized user 210 in association with the primary ID in a computer-readable storage medium such that each of the first key and the PIN of the authorized user 210 is subsequently retrievable based on receipt of the primary ID of the authorized user 210. The authentication authority 130 then encrypts a registration code (reg code) using the first key of the authorized user 210 and communicates the encrypted registration code to the authorized user 210 over the ancillary communications network 112.

[0061] Upon receipt thereof, the authorized user 210 decrypts the encrypted registration code using the second of the asymmetric key pair and communicates the unencrypted registration code together with a user ID to the access authority 150 over the communications network 114. Furthermore, credentials (not shown) of the authorized user 210 preferably are communicated with the user ID and registration code for authentication of the user ID in accordance with the then-current authentication system that is utilized by the access authority 150.

[0062] Upon authentication of the user ID using the credentials, the access authority 150 communicates the suspect registration code and a secondary ID to identify the authorized user 210 to the authentication authority 130. The access authority 150 may communicate the suspect registration code and secondary ID over the ancillary communications network 112, the communications network 114, or yet a third communications network 116, and the particular communications network itself that is utilized by the access authority 150 in communicating with the authentication authority 130 forms no part of the broadest definitions of the invention herein.

[0063] In response to the access authority 150 communicating the suspect registration code and secondary ID to the authentication authority 130, the authentication authority 130 first confirms that the suspect registration code matches a valid registration code (i.e., one that was previously encrypted and communicated to an authorized user). If so, then the authentication authority 130 associates the secondary ID of the authorized user 210 with the primary ID of the authorized user 210 in the computer-readable storage medium such that any subsequent passcode assigned to or otherwise associated with the primary ID is subsequently retrievable based on receipt of the secondary ID. If the suspect registration code does not match a valid registration code, then no association is made between the secondary ID

of the authorized user **210** with the primary ID of the authorized user **210** in the computer-readable storage medium.

[0064] The authentication authority **130** then communicates an indication of the result of the registration code comparison back to the access authority **150**. The access authority **150**, in turn, enables the authorized user **210** for authentication by way of the system **100** if the indicated result from the authentication authority **130** is a successful match.

[0065] In preferred embodiment of the systems **100,200**, the primary ID includes a device ID of a device of the authorized user in which is generated and stored the second key of the asymmetric key pair of the authorized user. Furthermore, if the passcode does not also function as the secondary ID in the system **100**, then the secondary ID includes the user ID, and, upon a successful registration code match by the authentication authority **130** in system **200**, the authentication authority **130** associates the secondary ID with the primary ID such that, in the system **100**, a passcode associated with the primary ID is retrievable by the authentication authority **130** based upon the later receipt of the secondary ID.

[0066] The methods of the systems **100,200** also may be repeated in conjunction with a plurality of access authorities **150** for a single authentication authority **130**. In such case, each of the primary ID and secondary ID preferably further includes a domain ID that generally uniquely identifies the appropriate access authority **150** to the authentication authority **130** with respect to the network resource sought to be accessed.

[0067] FIG. 3 illustrates another preferred embodiment of a multi-factor authentication system **300** in accordance with the present invention. Like the system **100** of FIG. 1, the system **300** includes a suspect user **110**, an authentication authority **130**, and an access authority **150**. The suspect user **110** also seeks to gain access to a network resource from the access authority **150**, but not by utilizing an encrypted passcode received by the suspect user **110** from the authentication authority **130**. In the system **300**, the suspect user **110** is unable to communicate with the authentication authority over the ancillary communications network **112**. This may occur, for example, when the suspect user **110** is out of communications range with the ancillary communications network **112**. In this situation, the suspect user **110** nevertheless may be able to communicate with the access authority **150** and the network resource assuming access is granted. Accordingly, the system **300** provides a method by which the suspect user **110** is able to seek and gain access without having to communicate at that time over the ancillary communications network **112**.

[0068] In accordance with this preferred system **300**, the suspect user **110** requests from the access authority **150** access to the network resource preferably by communicating over communications network **114** to the access authority **150** a user ID without a passcode (not shown). The absence of the passcode indicates to the access authority the unavailability of the ancillary communications network **112** to the suspect user **110**. Accordingly, the access authority **150** requests from the authentication authority **130** over the communications network **116** a challenge for the secondary ID corresponding to the user ID (not shown).

[0069] In response to the challenge request, the authentication authority **130** issues a challenge to the access authority **150** over communications network **116**. The access authority **150**, in turn, communicates the challenge to the suspect user **110**. Alternatively, the access authority **150** may generate the challenge itself.

[0070] Upon receipt of the challenge, the suspect user **110** communicates a challenge response back to the access authority **150**. The challenge response comprises a function of the challenge itself, a PIN of an authorized user **210**, and a first key of an asymmetric key pair that is generally unique to a device ID. The access authority **150** then communicates the challenge response in association with the secondary ID back to the authentication authority **130** over the communications network **116**.

[0071] Upon receipt of the challenge response and the secondary ID, the authentication authority **130** retrieves, based on the secondary ID, both the PIN of the authorized user **210** and the first key of the asymmetric key pair of the authentication authority **130** for that secondary ID. The authentication authority **130** then reconstructs the challenge response based on the retrieved PIN and first key as well as, inter alia, the challenge itself, and compares the reconstructed challenge response to the challenge response that was received. The secondary ID is authenticated upon the successful matching of the received challenge response with the reconstructed challenge response by the authentication authority **130**. The authentication authority **130** then communicates an indication of the result of the challenge response comparison to the access authority **150** over the communications network **116**.

[0072] The key pair of which the first key is utilized in constructing the challenge response preferably is generated by the authentication authority **130** during the registration process. In particular, the first key of the key pair is communicated by the authentication authority **130** to the authorized user **210** during registration process **400** as illustrated in FIG. 4. As will be apparent from a comparison of FIGS. 2 and 4, the registration processes **200,400** are identical except for the additional inclusion of this first key with the registration code in its encrypted communication over the communications network **112** to the authorized user **210**.

[0073] Turning now to FIG. 5, steps of a preferred method **500** of the multi-factor authentication system of FIG. 1 are illustrated, wherein a suspect user requests a passcode to obtain access to a network resource. The suspect user preferably initiates the method **500** when he or she executes a passcode request application on a device of the suspect user. Preferably, the device is a personal communication device of the suspect user. When executed, the application prompts the suspect user to identify (Step **504**) the network resource(s) to which access is desired by selecting a domain for the network resource(s). Upon selection of the domain, the application prompts the suspect user to input (Step **506**) the PIN previously registered by the authorized user of the device and associated with the selected domain, as discussed hereinafter with regard to FIG. 6.

[0074] The application then creates (Step **508**) a passcode request containing the primary ID and the PIN input by the suspect user (i.e., the "suspect PIN"). As stated previously, in preferred embodiments, the primary ID includes the

device ID of the device possessed by the suspect user. If there is more than one domain for a network resource to which the authorized user is entitled to access, then the primary ID also includes a domain ID (or "domain designation") associated with the domain selected by the suspect user which identifies an access authority for that domain to the authentication authority.

[0075] Furthermore, the PIN is encrypted using a first key (e.g., "public key") of an asymmetric key pair of the authentication authority prior to its inclusion in the passcode request. The passcode request then is communicated (Step 512) over the ancillary communications network to the authentication authority.

[0076] The authentication authority receives the passcode request, decrypts (Step 514) the PIN and compares (Step 516) the decrypted suspect PIN with the PIN of the authorized user that is retrieved based on the primary ID of the passcode request. If the suspect PIN matches the retrieved PIN of the authorized user in Step 516, then the authentication authority generates (Step 518) a passcode. Preferably, the passcode is time stamped (Step 520) and then recorded (Step 522) in association with the primary ID in a computer-readable storage medium. The authentication authority then encrypts (Step 524) the time-stamped passcode using the first key ( $K^1$ ) of an asymmetric key pair of the authorized user and communicates (Step 526) the encrypted passcode over the ancillary communications network to the suspect user. On the other hand, if the suspect PIN does not match in Step 516 the retrieved PIN of the authorized user, then the authentication authority generates and returns (Step 519) an error message to the suspect user indicating that the PIN input by the suspect user is invalid or was incorrectly input into the device.

[0077] The suspect user decrypts (Step 528) the encrypted passcode using the device and, specifically, using the second key ( $K^2$ ) of the asymmetric key pair of the authorized user, which is preferably stored within the device. The suspect user then communicates (Step 530) the passcode, which is still considered a "suspect passcode" at this point, and a user ID of the authorized user over the communications network to the access authority.

[0078] Upon receipt of the suspect passcode and user ID, the access authority communicates (Step 532) the suspect passcode to the authentication authority for authentication. If the suspect passcode does not already serve as a secondary ID to identify the suspect user (and potentially also the access authority), then the secondary ID is also communicated in Step 532 with the suspect passcode.

[0079] The access authority then authenticates the secondary ID of the suspect user by comparing (Step 534) the suspect passcode associated with the secondary ID (as received from the access authority) to the previously generated passcode associated with the primary ID. Preferably, a time stamp associated with the passcode is also used for validation of the suspect passcode.

[0080] If the suspect passcode matches the previously generated passcode in Step 534, then the authentication authority indicates (Step 537) to the access authority an indication of the successful authentication of the secondary ID, upon which the access authority then grants (Step 538) access to the requested network resource to the now autho-

rized user. On the other hand, if the suspect passcode does not match the previously generated passcode in Step 534, then the authentication authority communicates (Step 536) back to the access authority an indication of the unsuccessful authentication of the secondary ID, upon which the access authority then denies (Step 539) access to the requested network resource to the suspect user.

[0081] Turning now to FIG. 6, steps of a method 600 of the preferred user registration system of FIG. 2 are illustrated in which an authorized user registers with the authentication authority for the purpose of later being able to request and obtain a passcode for access to a network resource.

[0082] In this regard, to ensure that communications between the authorized user and authentication authority are secure, it is desirable as a preliminary matter for the authorized user to obtain a first key (e.g., public key) of an asymmetric key pair of the authentication authority, whereby communications from the authorized user sent to the authentication authority may be encrypted.

[0083] The method begins when the authorized user executes (Step 602) a registration request application on a device of the authorized user. Upon execution, the application creates (Step 604) a registration request containing the primary ID, which preferably includes the device ID of the device and the domain ID for the relevant domain for which registration is being requested, and the first key ( $K^1$ ) of an asymmetric key pair of the authorized user, which key pair is stored on and is previously generated within the device. For security purposes, the registration request is encrypted using the first key of the authentication authority and then communicated (Step 606) to the authentication authority over the ancillary communications network.

[0084] The authentication authority decrypts the encrypted registration request and stores (Step 608) the primary ID and first key ( $K^1$ ) in a computer-readable storage medium such that the first key is subsequently retrievable based on the primary ID. The authentication authority then generates a PIN request that is communicated (Step 610) to the authorized user over the ancillary communications network.

[0085] In response thereto, the device receives the PIN request and the registration request application then prompts the authorized user to input a PIN for use with the device when requesting a passcode for access to the network resource(s) of the identified domain. In response thereto, the authorized user inputs the PIN into the device in conventional manner (e.g., by inputting the PIN twice to ensure no typographical errors between the two entries). The primary ID and PIN are then communicated (Step 612) to the authentication authority over the ancillary communications network (again encrypted again using the first key of the authentication authority).

[0086] In response thereto, the authentication authority decrypts the encrypted primary ID and PIN and stores (Step 614) the PIN in the computer-readable storage medium such that the PIN is subsequently retrievable based on the primary ID. The authentication authority then generates (Step 616) a registration code (reg code), which is encrypted (Step 618) using the first key ( $K^1$ ) of the device, and then communicated (Step 620) to the authorized user over the ancillary communications network.

[0087] Upon receipt thereof, the authorized user decrypts (Step 622) the encrypted registration code using the second key of the asymmetric key pair that is stored within the device. The authorized user then communicates (Step 624) the unencrypted registration code together with a user ID to the access authority over the communications network. Other credentials of the authorized user preferably are also communicated with the user ID and registration code in Step 624 for authentication (Step 626) of the user ID in accordance with the then-current authentication system that is utilized by the access authority.

[0088] Upon authentication of the user ID in Step 626 using the user credentials, the access authority communicates (Step 628) to the authentication authority the registration code considered by the access authority to be suspect. A secondary ID also is sent with the suspect registration code for purposes of later identifying the authorized user to the authentication authority based thereon. If the user ID is not authenticated with the credentials, then an error is indicated (Step 630) and the method ends.

[0089] Upon receipt of the secondary ID and suspect registration, the authentication authority first confirms (Step 632) that the suspect registration code matches a valid registration code (i.e., one that was previously encrypted and communicated to an authorized user). If so, then the authentication authority associates (Step 634) the secondary ID of the authorized user with the primary ID of the authorized user in the computer-readable storage medium such that any subsequent passcode assigned to or otherwise associated with the primary ID is subsequently retrievable based on receipt of the secondary ID. If the suspect registration code does not match a valid registration code in Step 632, then no association is made between the secondary ID of the authorized user with the primary ID of the authorized user in the computer-readable storage medium.

[0090] The authentication authority also communicates (Steps 636, 640) an indication of the result of the registration code comparison back to the access authority. The access authority, in turn, enables (Step 638) the authorized user for authentication by way of the system 100 if the indicated result from the authentication authority is a successful match.

[0091] Turning now to FIG. 7, steps of the preferred method 300 of the multi-factor authentication system of FIG. 3 are illustrated. The steps shown begin with a request (Step 702) for a challenge code that is made to the authentication authority by the access authority. In response, the authentication authority generates (Step 704) a challenge code that is then communicated (Step 706) via the access authority to the suspect user seeking access from the access authority to a network resource. The user receives the challenge code and enters (Step 708) the challenge code into the device of the user together with the PIN of the authorized user. The device then computes a challenge response (Step 710) based on a key of an asymmetric key pair of the authentication authority, PIN of the authorized user, and challenge code. The device then displays the resulting challenge response to the user. The challenge response is preferably of manageable size for display and manual reading and entering on a keypad. The user reads the challenge response from a display of the device and communicates (Step 712) it back to the access authority, which

in turn communicates it back to the authentication authority with the secondary ID. The authentication authority then authenticates (Step 714) the secondary ID based on the challenge response by reconstructing it. If the challenge response from the suspect user matches in Step 716 the reconstructed challenge response, i.e., the response is valid, then access is granted (Step 718) by the access authority, and if the challenge response from the suspect user does not match in Step 716 the reconstructed challenge response, i.e., the response is invalid, then access is denied (Step 720) by the access authority.

[0092] FIG. 8 illustrates a flowchart of certain steps of the preferred registration process 400 of FIG. 4. As set forth above, the registration process 400 is generally the same as the registration process 200 described above, with the additional steps as identified in FIG. 8. In this regard, these additional steps include: generating a pair of asymmetric encryption keys of the authentication authority (Step 815) which is generally unique to the device of the authorized user that is registering; encrypting (Step 817) the first key, of this secondary together with the registration code that is sent to the authorized user, i.e., encrypting the first key of the secondary pair with the first key of the asymmetric key pair of the authorized user that is received from the authorized user during registration; sending (Step 819) the encrypted first key of the secondary pair and the registration code to the user via the ancillary communications network; decrypting (Step 821) the first key of the secondary pair and the registration code using the second key of the asymmetric key pair of the authorized user; and storing (Step 823) the first key of the secondary pair within the device and using it for computation of a challenge response in accordance with an aspect of the present invention. Because the first key of the secondary pair of the authentication authority preferably is not used but for computation of the challenge response, and because this key is safely stored on the device of the user, matching a received challenge response with a reconstructed challenge response by the authentication entity results in the strong indication that the device of the authorized user actually computed the challenge response.

#### DETAILED DESCRIPTION OF PREFERRED COMMERCIAL EMBODIMENTS OF THE INVENTION

[0093] Commercial embodiments of the present multi-factor authentication system are designed to be commercially viable as a strong multi-factor security system. The commercial wireless authentication system employs new application ready wireless devices as an out-of-band method for receiving passcodes into intranets, virtual private networks (VPNs), highly secured websites, and other access restricted systems. The system utilizes a wireless device as a passcode reception device to gain access on a secure wired network.

[0094] The wireless authentication system is designed to be as secure as existing two-factor security systems with significantly less costs to implement and maintain. Like existing two-factor authentication methods, the present commercial wireless authentication system requires the passcodes to be derived and verified in two separate network channels: the wireless network, and the wired, network service. Through verification of the validity of the device and optional triangulation, the passcodes are authenticated

and matched against a named user. However, the present authentication system differs from other two-factor systems in several key ways:

- [0095] 1) The intelligence of the passcode generation is not within the client device, preventing theft and reverse engineering;
- [0096] 2) The system is not 100% counter/time/algorithm-based (as are most competing systems), preventing the existence of N+1 and N-1 valid codes as the single-use devices age and lose synchronization;
- [0097] 3) The system generates a code only when requested, not continuously when not needed, which would open the system to algorithm analysis or cracking;
- [0098] 4) The system employs no single-use devices, which eliminates the expenditure for and investment in short-life devices; and
- [0099] 5) The system can support multiple security domains both on the client, to reduce the need for multiple single use devices, and on the server, to enforce flexible security policies.

[0100] Instead, the present wireless system uses a portable, multi-function wireless device that is increasingly present in both personal and business environments. Thus, the present wireless authentication system uses a single device for accessing all subscribed systems and enjoys the ultimate portability while avoiding the need for users to install software on each system that they use. Furthermore, the system adds unified identification to the user's existing wireless device providing a versatile multifunction capability and increasing the convenience for the user.

[0101] Wireless devices have encapsulated strong unique identification principles and secure protocols for device to server communications. A server based authentication model may be constructed to that equates the unique identification of the wireless device to the unique persona of the device operator. Using shared secrets and secure communication methods, access to the wireless device and the knowledge of user application credentials, a real-time token generation system can be deployed which will provide an extremely secure identification and authentication system.

[0102] The present wireless authentication system is based on the unique properties of a wireless device that allows and ensures that transmissions are routed to the correct device. In the attempt to avoid fraudulent use of wireless networks, an infrastructure has been created that when coupled with the various inventions of the present system allows for strong identification and authentication of a user in a system or network environment.

[0103] Turning now back to the figures, FIG. 9 provides an overview of the operation of a commercial wireless authentication system 900. As illustrated, the wireless authentication system 900 entails a passcode to be derived and verified in two separate network channels. The passcode is derived over the mobile network 914, while verified over a wired network 914.

[0104] A wireless personal communication device 922 is the client platform for the identification of the individual

user 914 and utilized for the provision of passcodes. The wireless authentication system 900 supports application ready wireless devices 922 such as RIM BLACKBERRY devices, java-enabled telephones, personal digital assistants (PDAs), WINDOWS CE clients, PALM devices, and the like. In order to utilize the wireless authentication system, a small client application is installed on the wireless device 922. The application manages several processes including key generation, registration, passcode requests, passcode reception, and offline passcode verification, all of which are discussed in greater detail in connection with the following figures.

[0105] As previously stated, the wireless device 922 is utilized to obtain a passcode to access a wired authentication server (WAS) 930. The WAS 930 can be configured to operate with any operating system. However, one commercial embodiment runs a hardened version of Linux 2.4.18. The operating system running on the WAS appliance can be hardened in the following ways:

- [0106] 1) The engineering staff applies security kernel patches, system patches and application patches.
- [0107] 2) All processes run under an unprivileged user, including application processes, application server processes, protocol modules and database server processes.
- [0108] 3) All unnecessary services, including network services such as telnet, ftp, line printer, etc. are removed from the system, if possible, or disabled.
- [0109] 4) A netfilter IP-tables firewall process is created and configured to remove access to unwanted and unneeded processes, applications and ports.
- [0110] 5) Access to any process—most importantly the terminal services, file transfer services and database administration services—are conducted over an encrypted connection (SSH2) and negotiated through public key exchange.
- [0111] 6) Additionally, inherently non-encrypted services (like database administration services) are conducted over a SSH2 tunneled connection.
- [0112] 7) All internal services are conducted over an access controlled loop back service.
- [0113] 8) All file system, application and system services are set to deny access by default.
- [0114] 9) All elements within the file system are set to read-only and accessed by an unprivileged user.
- [0115] 10) Buffer overruns, unchecked variables and other application weaknesses are protected.
- [0116] 11) Access to the cryptographic keys and database passwords is via a protected process. The keys and passwords never appear in plain text on the file system.

[0117] Additionally, in this embodiment, the WAS 930 uses mainly JAVA-based server components and application components. The underlying database 935 is an embedded version of Sybase, which is self-contained and does not require database administration. The WAS database 935 is a database of domains, devices, users, and protocol modules.

[0118] In order for the WAS 930 to communicate with network clients 950, the WAS 930 has installed the appropriate protocol modules. One embodiment supports Remote Authentication Dial In User Service (RADIUS) and a proprietary wireless authentication system protocol.

[0119] RADIUS is a standard TCP/IP based service for authorization and access control. The RADIUS protocol is detailed within the Internet Engineering Taskforce RFC 2865 with additional information provided by RFC's 2866 to 2869. The RADIUS protocol can be less secure than proprietary protocols since it utilizes a MAC encoding of the packets within the protocol exchange. Consequently, it is normally utilized on trusted networks, e.g., corporate Intranets, or to support standard VPN and dial-in clients. RADIUS is supported by Microsoft's RAS, Cisco's routing and firewall software as well as by most of the terminal and PPP device makers. The WAS 930 can support fully RADIUS authentication and less fully RADIUS accounting and proxy features.

[0120] The proprietary protocol is encrypted for the verification of passcodes from certain network clients 950. The proprietary protocol can be more secure than RADIUS since it can utilize full asymmetric payload and transport encryption, but it requires use of an application component to be implemented within a network client 950. Typically, the component is a JAVA bean that can be integrated into a website, a web application, a client-server application or as a forwarding service within an LDAP service.

[0121] In addition, the WAS 930 can offer a web-based administrative utility for the management of the server components. The WAS 930 can provide a fully web-enabled administration utility to create, modify, enable and disable each of the components utilized. Most of the WAS 930 administration is completed using an administration application. This entirely web-based system provides administration of wireless devices 922, security domains, users 910, protocol modules, network clients 950 and preferences. In addition, the application provides access to logs, reports, statistics and help.

[0122] Network clients 950 provide network services on the wired network channel 914. They can vary greatly in their implementation, depending on the requirements of the organization that deploys the wireless authentication system 900. For example, a network client 950 can be a firewall that provides VPN services to a partner extranet (via RADIUS) or a private website that provides sales support services (via a proprietary protocol over SSL). The options are limitless as long as the network client implements either RADIUS (as most network devices), a proprietary protocol through an application component, or other future standard protocols adopted for authentication or access control.

[0123] The network clients 950 are accessed by users 914 desiring access to a network service on a wired network 914. The WAS 930 employs the mobile network 912 for receiving the passcodes for authorization into intranets, VPNs, and highly secure websites. The passcode reception process and passcode provision process are conducted over two separate and distinct channels. One channel is the untrusted wireless network 912 (or trusted private wireless network for tele-coms), while the other is an untrusted or trusted wired network 914. Strong encryption should be utilized when transmission takes place on an untrusted network. In short,

the passcode is received on one hand by the wireless device 922 and provided on another by any separate computing device 926 that can access the wired network 914. The transfer between the bands is accomplished manually by the user 910.

[0124] In order to gain access to a secure network resource, the user 910 initiates a passcode request by selecting a domain and entering a PIN for the selected domain. The PIN was created during a registration process discussed later in greater detail. The wireless device application generates the passcode request. The passcode request consists of payload that includes a device identification (device ID), the PIN, and a server identification (server ID) encrypted with general server key provided in the registration process. The passcode request is transmitted to the wireless authentication server (ONAS) 930 over an encrypted SSL connection.

[0125] After receiving the passcode request, the WAS 930 decrypts the request with its local server key. The server looks up in an associated database 935 the requesting wireless device for the selected domain using the device ID and verifies the PIN.

[0126] In addition, the WAS 930 may use location information as part of the authentication process. A wireless network 912 can provide geographic location information by using triangulation of the originating communication. The triangulation can be accomplished by the signal strengths received at various network towers 990 in the wireless network system 912. Furthermore, many wireless devices include built in GPS location service that using the known GPS system 980. Consequently, these enabled wireless devices 922 can provide exact location information. A user 910 can specify valid geographic boundaries for the origination of a passcode request such as an office, residence, airport, city, state, or other geographic area. Likewise a user 910 can specify time ranges for a valid request such as weekdays during normal work hours. Clearly, geographic location and a time range can be merged such that a valid request can be from an office during normal work hours and a residence during off hours. Furthermore, usage patterns can be tracked and deviations from a pattern can trigger additional security requirements.

[0127] If the authenticating information is validated, the WAS 930 creates a passcode that is encrypted with the general device key. The passcode is time stamped and valid for only a predetermined time period based upon the security requirements of the domain. Typically, a passcode is valid only for 60 seconds or 90 second. However, it is conceivable passcodes could be valid up to a month or more depending on the sensitivity of the network resource. The WAS 930 returns the passcode to the wireless device 922 via SSL.

[0128] When the passcode is received, the message is decrypted with the device local key. This key is unique to the domain and has never been transmitted from the device 922. The passcode is displayed on the device 922 and the user 910 can use the passcode to gain access to the network service 950.

[0129] Before a wireless device 922 can communicate with the WAS 930, the device 922 is first registered within the WAS 930 and associated with a security domain. In this commercial embodiment, each supported security domain requires approximately 1200 bytes of storage on the wireless device 922. There are two main methods for registering a device 922:



[0130] If the domain is configured for auto-registration, the wireless device 922 can request registration through the client application. First, the user 910 uses the client application to request that the device 922 be added to the WAS 930 and security domain in question. A server code is entered by the user 910. This server code can be provided by a technical security staff or automatically displayed to the user 910 upon successful entry into an existing security system. Once this 12-digit server code has been entered into the device 922, the user 910 establishes a PIN for the domain connection. A separate PIN can be provided for each domain, and it is recommended that the user 910 establish unique PINs for each domain. At this point in the process, the general device key that was generated in the key generation process is provided to the WAS 930. The WAS 930 will then record the cryptographic key and provide the domain's general key, a unique identifier for the instance of the device within the security domain and a large registration code. Additionally, the server 930 will generate a second set of keys unique for that particular client device 922 in the security domain for offline passcode verification.

[0131] The registration code is a one-use temporary element. It is not a passcode or password and cannot be used for access into a network resource 950. Instead, the registration code is used to associate the wireless device 922 with a known user 910 within a trusted system. It is possible that the association can take place outside of the wireless authentication system 900; however, in most cases, it will be on a registration website within the administration system. When the user 910 goes to the registration website (or other registration system), the user 910 may be required to enter an existing user ID, identifying information, and the registration code. The identifying information is the credentials that are acceptable to the network client for validating a user 910. This process associates the wireless device 922 with the user 910, verifies the wireless device 922 as valid within the security domain and activates the wireless device 922 within the security domain.

[0132] If the domain is not configured for auto-registration, much of the auto-registration process is still followed. The key exchange is same. One major difference is in the final registration step. Instead of the user 910 completing this step, the administrator of the WAS 930 would associate the wireless device 922 with the user ID and security domain and enable it. The manual process can be used when an existing user 910 joins the system 900 and continuity with the existing system is desired.

[0133] The WAS 930 stores named users and associates each user 910 with a device 922 and a security domain. This process allows for login within a network service, whether it is via a RADIUS-based VPN, secure website, or any other service that is provided by a network client 950.

[0134] The WAS 930 contains a database 935 of domains, devices, users, and protocol modules. Additionally, the WAS 930 also offers a web-based administrative utility for the management of these components. Each instance of authorization, the WAS 930 runs under a particular security domain. The security domain is intended to segregate users 910 with respect to access and services. For example, Intranet access may be provided with one domain, partner extranet access with another, and public Internet (Website) access with a third. Separate security policies can be pro-

vided for each domain and access can be granted on a device/individual user basis. Unlike other systems, the client for each domain (the wireless device 922) is the same. Upon creation, each domain generates a key pair for payload encryption within the passcode request/passcode reception process. These keys are the domain local key and the domain general key and are exchanged in the registration process.

[0135] The cryptographic signature or device profile for each wireless device 922 is stored within the WAS 930 and associated with a domain 950 and user 922. In the case of encrypted mode (recommended since the wireless network 912 is untrusted), the cryptographic signature is a 1024 bit-equivalent general device key as generated in the registration. This strong, asymmetric encryption key is generated on the device 922 and serves to identify a valid device 922 within the security domain and to provide payload security during the reception of passcodes. The device 922 also receives, stores and utilizes the public key of the WAS 930, which is provided by the server 930 during the registration process. Once these keys are exchanged and the device-domain PIN established, the wireless device 922 becomes a registered or trusted device.

[0136] When the application is started for the first time, the application automatically generates a key pair: a local device key and a general device key. These keys are used for the decryption of the payload from the WAS 930 and identification of the device 922. The keys are asymmetric, and the strength of the key pair is approximately equivalent to RSA1024 bits. The time for the key generation process averages 14 seconds.

[0137] The commercial embodiment uses the NTRU algorithm from NTRU Cryptosystems, Inc. for this key generation and in turn for the payload encryption. It is generally accepted that the encryption strength of the NTRU modified lattice algorithm is approximately the same as existing elliptical curve or RSA asymmetric algorithms. However, with the inferior computing power of wireless devices 922, the NTRU algorithm is superior because it is much, much faster when running on the device 922. For security reasons, it is preferred that the key generation be completed on the device 922, not on a PC 926 or server and transferred to the device 922. In this way the local device key never leaves the device 922 and is not subject to interception, electronic copying or redistribution. Thus, the wireless device 922 functions similarly to a smart card. But unlike a smart card, it does not require a wired reader, which greatly reduces the cost of implementation and greatly increases portability.

[0138] When a security domain is created within the WAS 930, two keys are generated for the domain: 1) the server local key  $\{SK^1\}$  and the general server key  $\{SK^2\}$ , these keys roughly relate to the security domain's public and private key respectively; however, terminology used by the NTRU algorithm does not match RSA's terminology precisely. At the initiation of the client applications the device creates a key pair the local device key  $\{CK^1\}$  and the general device key  $\{CK^2\}$ .

[0139] When communication is initiated by an unregistered device 922, the device 922 communicates with the WAS 930 based on the "server code" $\{SC\}$  entered by the user 910. This code is either a zero-padded IP address representing the address on the Internet or a 12-digit alias within the systems net namespace (for ASP services). After

resolving the address {RA} of the target, the devices will request the following URL and POST {CK<sup>2</sup>} to <stdin> via https:

[0140] https://<{SC}{RA}/wikid/servlet/InitDeviceS?a=0&S={SC}

[0141] The server 930 expects exactly 255 bytes for the {CK<sup>2</sup>}. The server 930 will encrypt the following message:

[0142] CK<sup>2</sup>{[UTF encoded string][int][long][int][bytes]}

[0143] Corresponding to:

[0144] CK<sup>2</sup>{[domain name][minPIN][PIN TTL][device ID({DID})][SK<sup>2</sup>length][{SK<sup>2</sup>}]}

[0145] The typical length of the reply (after expansion) is approximately 3526 bytes depending on configuration and length of {SK<sup>2</sup>}. The device should decrypt string with {CK<sup>1</sup>} and prompt for PIN, utilizing the minPIN. The PIN selection is then encrypted with {SK<sup>2</sup>} and POSTed to:

[0146] https://<{SC}{RA}/wikid/servlet/InitDevicesS?a=1&d={DID}&s={SC}

[0147] The server will expect 251 bytes on <stdin>. The server decrypts with {SK<sup>1</sup>} and verifies. Then, the server replies with the following encrypted message:

[0148] CK<sup>2</sup>{[reg code {RC}]}

[0149] Typical length is 263 bytes (251 bytes+[http overhead]). The device should enable and display the domain name. In order to increase the system security, the PIN and {RC} are not stored on the device in case of theft. The wireless device 922 is not enabled until the registration is complete on the second, wired channel network 914. The remainder of the registration generally takes place within the wired channel network 914.

[0150] Without strong encryption, the system 900 would not be as secure as current two-factor systems. Simply put, the weakness of using an untrusted network channel, namely the wireless network, is significant without strong cryptography. Therefore, the client software employs standard 128-bit SSL for transport security. In addition, the wireless authentication system 900 encrypts the payload of the passcode request and passcode reception as previously noted. This allows for process-to-process encryption in addition to the application-to-network service encryption provided by SSL. On the Java phones SSL is supported by the MIDP system; on the BLACKBERRY it is accomplished with a proprietary MOBIBTEXT gateway.

[0151] Network clients 950 provide network services on the wired network channel 914. They can vary greatly in their implementation, depending on the requirements of the organization that deploys the wireless authentication system 900. For example, a network client 950 can be a firewall that provides VPN services to a partner extranet (via RADIUS) or a private website that provides sales support services (via a proprietary protocol over SSL). Those skilled in the art will acknowledge that the options are limitless. However, for a network client 950 to become active within the WAS security domain, it is first registered. The registration of network clients is accomplished through the administration system.

[0152] In the commercial embodiment, it is the responsibility of the network client 950 to provide passcodes via a

computer network 916 for verification by the WAS 930. Typically, the network client 950 will provide to the WAS 930 the passcode and the user ID. The network client 950 does not verify the code itself; instead it provides the code to the WAS 930 through the chosen protocol. When the result (acceptance or denial) of the code is returned from the WAS 930 via the computer network 916, the network client 950 acts upon the acceptance (or denial). In the case of RADIUS devices, the network devices 950 are by design programmed to act on the acceptance or denial of the code. In the case of network clients 950 using a proprietary protocol, the appropriate access granting action should also be taken.

[0153] Turning to FIG. 10, illustrated is a commercial embodiment for offline passcode verification. Offline passcode verification is utilized when the wireless network 1012 is not accessible. This state may be due to the user 1010 being out-of-range of wireless network 1012 or for other reasons.

[0154] When the WAS 1030 can not be reached by a wireless device 1022, the offline verification process can be instituted by the network client 1050. Based on the user's action, the network client can request a challenge code from the WAS 1030, rather than requesting a passcode verification. This action can be taken in response to the user 1010, not providing any response to a passcode input field over a computer network 1014 from a computing device 1026.

[0155] Upon receiving a null code for the passcode, the WAS 1030 provides a large (usually 12 digit) code for the challenge code to the network client 1050 over a computer network 1016. The network client 1050, in turn, displays the challenge code to the user 1010.

[0156] The user 1010 runs a client application on the wireless device 1022 in offline mode and enters the challenge code into the device 1022. The device 1022 assembles the following message: [general device key|PIN for domain|challenge code] (separators are shown for readability) and encrypts it with a secondary general server key used only for offline verification. This key pair is specific to the wireless client 1022 and the security domain. The encrypted payload is hashed with SHA1 producing a 20 byte string of ASCII characters. The string is base62 encoded and displayed to the user 1010.

[0157] The user 1010 then returns to the process associated with the network client 1050, such as web page login or terminal server login, and enters the resulting message as an answer to the challenge.

[0158] The challenge answer is provided by the network client 1050 to the WAS 1030 over an encrypted (or in the case of RADIUS encoded and through CHAP) connection 1016. The WAS 1030 decrypts the message with the server local key for offline verification, repeats the message creation above and compares the SHA1 hash. The result of the challenge verification is returned to the network client 1050. Based upon the result, the network 1050 can grant or deny access.

[0159] In view of the foregoing detailed description of preferred embodiments of the present invention, it readily will be understood by those persons skilled in the art that the present invention is susceptible of broad utility and application. While various aspects have been described in par-

icular contexts of use, the aspects may be useful in other contexts as well. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the foregoing description thereof, without departing from the substance or scope of the present invention. Furthermore, any sequence(s) and/or temporal order of steps of various processes described and claimed herein are those considered to be the best mode contemplated for carrying out the present invention. It should also be understood that, although steps of various processes may be shown and described as being in a preferred sequence or temporal order, the steps of any such processes are not limited to being carried out in any particular sequence or order, absent a specific indication of such to achieve a particular intended result. In most cases, the steps of such processes may be carried out in various different sequences and orders, while still falling within the scope of the present inventions. Accordingly, while the present invention has been described herein in detail in relation to preferred embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made merely for purposes of providing a full and enabling disclosure of the invention. The foregoing disclosure is not intended nor is to be construed to limit the present invention or otherwise to exclude any such other embodiments, adaptations, variations, modifications and equivalent arrangements, the present invention being limited only by the claims appended hereto and the equivalents thereof.

What is claimed is:

1. In a system wherein both a PIN of a user authorized to access a network resource and a first key of an asymmetric key pair of the authorized user are maintained in association with a first primary identification by an authentication authority such that each of the PIN and the first key are retrievable based on the first primary identification, a method performed by the authentication authority whereby the authorized user gains access to the network resource from an access authority with a passcode, the method comprising the steps of:

- (a) receiving the first primary identification and a suspect PIN from a suspect user;
- (b) authenticating the first primary identification by considering at least one authentication factor, including comparing the suspect PIN with the PIN of the authorized user maintained in association with the first primary identification by the authentication authority; and
- (c) following a successful authentication of the first primary identification,
  - (i) generating the passcode,
  - (ii) encrypting the passcode using the first key of the asymmetric key pair of the authorized user, and
  - (iii) communicating the encrypted passcode to the suspect user for subsequent decryption and presentation to the access authority.

2. The method of claim 1, further comprising the steps of:

- (a) receiving a suspect passcode from the access authority;

- (b) comparing the suspect passcode with the passcode that was encrypted and communicated to the suspect user by the authentication authority; and

- (c) communicating an indication of a result of the comparison to the access authority.

3. The method of claim 2, wherein the passcode must be received within a predetermined amount of time after being generated in order to gain access to the network resource.

4. The method of claim 3, wherein the predetermined period of time is less than ninety seconds.

5. The method of claim 3, wherein the predetermined period of time is arbitrarily configurable by an administrator of the authentication authority.

6. The method of claim 1, wherein the authorized user gains access to the network resource over a communications network and wherein said step of receiving the first primary identification and suspect PIN includes receiving the first primary identification and suspect PIN over an ancillary communications network.

7. The method of claim 6, wherein the communications network is the Internet.

8. The method of claim 6, wherein the communications network is an intranet.

9. The method of claim 6, wherein the communications network is an untrusted network.

10. The method of claim 6, wherein the communications over the communications network are encrypted.

11. The method of claim 6, wherein the ancillary communications network is a telecommunications network.

12. The method of claim 6, wherein the ancillary communications network is a trusted network.

13. The method of claim 1, wherein biometric information of the authorized user further is maintained in association with the first primary identification such that the biometric information is retrievable based on the first primary identification, and wherein said step of considering at least one authentication factor by the authentication authority further includes comparing suspect biometric information received with the first primary identification with the biometric information of the authorized user maintained in association with the first primary identification by the authentication authority.

14. The method of claim 13, wherein the biometrical information represents a physical characteristic of the authorized user.

15. The method of claim 14, wherein the biometric information represents a voice pattern of the user.

16. The method of claim 14, wherein the biometric information represents a retina pattern of the user.

17. The method of claim 14, wherein the biometric information represents a fingerprint of the user.

18. The method of claim 1, wherein a geographical location for the authorized user is maintained in association with the first primary identification such that the geographical location is retrievable based on the first primary identification, and wherein said step of considering at least one authentication factor by the authentication authority further includes comparing a geographical location identified as the origin of communication of the suspect PIN with the geographic location maintained in association with the first primary identification by the authentication authority.

19. The method of claim 1, wherein a time range for the authorized user is maintained in association with the first primary identification such that the time range is retrievable

based on the first primary identification, and wherein said step of considering at least one authentication factor by the authentication authority further includes comparing with the time range with a time of receipt of the first primary authentication and the suspect PIN.

20. The method of claim 1, wherein the first primary identification comprises a device ID.

21. The method of claim 20, wherein the device ID is an identification of a personal communications device.

22. The method of claim 21, wherein the personal communications device comprises a PDA.

23. The method of claim 21, wherein the personal communications device comprises a wireless device.

24. The method of claim 21, wherein the personal communications device comprises a GPS device.

25. The method of claim 21, wherein the personal communications device comprises a JAVA-enabled device.

26. The method of claim 21, wherein the personal communications device comprises a mobile phone.

27. The method of claim 21, wherein the personal communications device comprises a two-way pager device.

28. The method of claim 1, wherein the first primary identification includes a domain ID.

29. The method of claim 1, wherein the first primary identification comprises a combination of a device ID and a domain ID.

30. The method of claim 29, wherein the suspect PIN is received encrypted with a first key of an asymmetric key pair of the authentication authority, the key pair of the authentication authority being generally unique to the domain ID.

31. The method of claim 29, wherein the passcode communicated to the suspect user is further maintained by the authentication authority such that the passcode is retrievable based on a first secondary identification.

32. The method of claim 31, wherein the first secondary identification comprises the combination of (i) a user ID that represents an identification of the authorized user to the access authority and (ii) the domain ID.

33. The method of claim 29, wherein the authorized user is additionally authorized to access a second network resource, and wherein both a second PIN of the authorized user and a first key of a second asymmetric key pair of the authorized user are maintained by the authentication authority in association with a second primary identification such that each of the second PIN and the first key of the second key pair of the authorized user are retrievable based on the second primary identification.

34. The method of claim 33, wherein a first key of a second asymmetric key pair of the authentication authority is maintained by the authentication authority in association with a second domain ID such that the first key of the second asymmetric key pair of the authentication authority is retrievable based on the second ID, the second key pair of the authentication authority being generally unique to the second domain ID.

35. The method of claim 33, further comprising the steps of,

- (a) receiving the second primary identification and a suspect second PIN;
- (b) authenticating the second primary identification by considering at least one authentication factor, including comparing the suspect second PIN with the second PIN

of the authorized user maintained in association with the second primary identification by the authentication authority; and

(c) following a successful authentication of the second primary identification,

(i) generating a second passcode,

(ii) encrypting the second passcode using the first key of the second asymmetric key pair of the authorized user, and

(iii) communicating the encrypted second passcode to the suspect user for subsequent decryption.

36. The method of claim 33, wherein the second primary identification comprises a combination of the device ID and the second domain ID.

37. The method of claim 33, wherein the second passcode communicated to the suspect user is further maintained by the authentication authority such that the second passcode is retrievable based on a second secondary identification.

38. The method of claim 37, wherein the second secondary identification comprises a combination of (i) a second user ID that represents an identification of the authorized user to an access authority with respect to the second network resource, and (ii) the second domain ID.

39. Compute-readable medium having computer-executable instructions for performing the steps of claim 1.

40. Compute-readable medium having computer-executable instructions for performing the steps of claim 2.

41. Computer-readable medium having computer-executable instructions that perform a method comprising the steps of:

- (a) maintaining a PIN of an authorized user of a network resource and a first key of an asymmetric key pair of the authorized user in association with a primary identification such that each of the PIN and the first key are retrievable based on the primary identification;
  - (b) retrieving the PIN of the authorized user based on the primary identification received over an ancillary communications network and comparing the retrieved PIN with a suspect PIN also received over the ancillary communications network with the primary identification;
  - (c) generating a passcode and encrypting the passcode using the first key of the asymmetric key pair of the authorized user for communicating back over the ancillary communications network;
  - (d) maintaining the passcode in association with a secondary identification such that the passcode is retrievable based on the secondary identification; and
  - (e) retrieving the generated passcode based on the secondary identification that is received and comparing the retrieved passcode with a suspect passcode also received with the secondary identification.
42. The computer-readable medium of claim 40, wherein the method further includes the step of communicating an indication of a result of the passcode comparison.
43. The computer-readable medium of claim 40, wherein the method further includes the step of receiving the secondary identification and suspect passcode from an access authority that grants to a suspect user access to the network resource based on the passcode comparison.

44. The computer-readable medium of claim 40, wherein the ancillary communications network is a telecommunications network.

45. The computer-readable medium of claim 40, wherein the ancillary communications network is a trusted network.

46. The computer-readable medium of claim 40, wherein the method further comprises the steps of maintaining biometric information of the authorized user in association with the primary identification such that the biometric information is retrievable based on the primary identification, and comparing suspect biometric information received with the primary identification over the communications medium with the biometric information of the authorized user maintained in association with the first primary identification.

47. The computer-readable medium of claim 40, wherein the method further comprises the steps of maintaining geographical location for the authorized user in association with the primary identification such that the geographical information is retrievable based on the primary identification, and comparing a geographical location identified as the origin of communication of the suspect PIN received with the primary identification with the geographic location maintained in association with the primary identification.

48. The computer-readable medium of claim 40, wherein the method further comprises the step of maintaining a second PIN of the authorized user and a first key of another asymmetric key pair of the authorized user in association with a second primary identification such that each of the second PIN and the first key of the second pair are retrievable based on the second primary identification.

49. A computer system including the computer-readable medium of claim 40.

50. In a system wherein both a PIN of a user authorized to access a network resource and a first key of an asymmetric key pair generally unique to a personal communications device of the authorized user are maintained by an authentication authority in association with an identifier such that each of the PIN and the first key are retrievable based on the identifier, a method performed by the authentication authority whereby the authorized user gains access to the network resource from an access authority, the method comprising the steps of:

- (a) with respect to a suspect user seeking to gain access to the network resource from the access authority, receiving a challenge request from the access authority in association with an identifier;
- (b) in response to the challenge request, communicating a challenge to the access authority;
- (c) receiving from the access authority a challenge response and the identifier; and
- (d) authenticating the identifier by comparing the challenge response to a function of,
  - (i) the challenge;
  - (ii) the PIN maintained by the authentication authority in association with the identifier; and
  - (iii) the first key maintained by the authentication authority in association with the identifier.

51. The method of claim 51, wherein the key pair is generated by the authentication authority and the first key of

the key pair is communicated by the authentication authority to the personal communications device of the authorized user.

52. The method of claim 51, wherein the first key is communicated to the personal communications device of the authorized user upon initial receipt of the PIN from the authorized user for maintaining in association with the identifier.

53. The method of claim 51, wherein the function includes hashing of the (i) challenge, (ii) PIN, and (iii) first key of the asymmetric pair that is generally unique to the user device and that was provided by the authentication authority, as well as (i) a first key of an asymmetric key pair that is generally unique to the user device but that was generated within the device and not provided by the authentication authority.

54. The method of claim 51, wherein the identifier includes a user ID that identifies the authorized user to the access authority.

55. The method of claim 51, wherein the identifier comprises (i) a user ID that identifies the authorized user to the access authority, and (ii) a domain ID that identifies the access authority to the authentication authority.

56. The method of claim 51, wherein the personal communications device comprises a PDA.

57. The method of claim 51, wherein the personal communications device comprises a wireless device.

58. The method of claim 51, wherein the personal communications device comprises a GPS device.

59. The method of claim 51, wherein the personal communications device comprises a JAVA-enabled device.

60. The method of claim 51, wherein the personal communications device comprises a mobile phone.

61. The method of claim 51, wherein the personal communications device comprises a two-way pager device.

62. The method of claim 51, wherein the first key is communicated over an ancillary communications network and the challenge request is received over a communications network.

63. The method of claim 62, wherein the communications network comprises the Internet.

64. The method of claim 62, wherein the communications network comprises an intranet.

65. The method of claim 62, wherein the communications network comprises an untrusted network.

66. The method of claim 62, wherein communications over the communications network are encrypted.

67. The method of claim 62, wherein the ancillary communications network comprises a telecommunications network.

68. The method of claim 62, wherein the ancillary communications network is a trusted network.

69. Computer-readable medium having computer-executable instructions for performing the steps of claim 51.

70. A method for gaining access by a user to a network resource, comprising the steps of:

- (a) communicating a PIN and a first primary identification over an ancillary communications network to an authentication authority;
- (b) receiving an encrypted passcode over the ancillary communications network from the authentication authority;

- (c) decrypting the passcode using a key of an asymmetric key pair; and
- (d) communicating the passcode and a user ID over a communications network to an access authority.
71. The method of claim 70, further comprising the step of communicating biometric information in addition to the PIN and first primary identification over the ancillary communications network.
72. The method of claim 70, wherein the communications network comprises the Internet.
73. The method of claim 70, wherein the communications network comprises an intranet.
74. The method of claim 70, wherein the communications network comprises an untrusted network.
75. The method of claim 70, wherein communications over the communications network are encrypted.
76. The method of claim 70, wherein the ancillary communications network is a telecommunications network.
77. The method of claim 70, wherein the ancillary communications network is a trusted network.
78. The method of claim 70, wherein the PIN and first primary identification are communicated over the ancillary communications network using a personal communications device.
79. The method of claim 78, wherein the personal communications device comprises a PDA.
80. The method of claim 78, wherein the personal communications device comprises a wireless device.
81. The method of claim 78, wherein the personal communications device comprises a GPS device.
82. The method of claim 78, wherein the personal communications device comprises a JAVA-enabled device.
83. The method of claim 78, wherein the personal communications device comprises a mobile phone.
84. The method of claim 78, wherein the personal communications device comprises a two-way pager device.
85. The method of claim 78, further comprising the step of manually entering the PIN into the personal communications device for communicating the PIN over the ancillary communications network to the authentication authority.
86. The method of claim 78, wherein the first primary identification includes a device ID of the personal communications device.
87. The method of claim 78, wherein the first primary identification comprises (i) a device ID of the personal communications device and (ii) a domain ID that identifies the access authority to the authentication authority.
88. The method of claim 78, wherein the encrypted passcode is received and decrypted by the personal communications device.
89. The method of claim 78, wherein the key with which the passcode is decrypted is stored within and generally unique to the personal communications device.
90. The method of claim 78, wherein the passcode and user ID are communicated over the communications network using another device different from the personal communications device.
91. The method of claim 90, wherein the other device is a computer of a computer network.
92. The method of claim 90, further comprising the step of manually reading the passcode from a display of the personal communications device for communicating the passcode over the communications network.
93. The method of claim 70, further comprising the steps of:
- communicating a second PIN and a second primary identification over the ancillary communications network to the authentication authority;
  - receiving a second encrypted passcode over the ancillary communications network from the authentication authority;
  - decrypting the second passcode using a key of a second asymmetric key pair; and
  - communicating the second passcode and a second user ID over the communications network to another access authority.
94. The method of claim 93, wherein the second PIN and second primary identification are communicated over the ancillary communications network using a personal communications device.
95. The method of claim 94, wherein the second primary identification comprises (i) a device ID of the personal communications device and (ii) a second domain ID.
96. Computer-readable medium having computer-executable instructions that perform the method of claim 70.
97. Computer-readable medium having computer-executable instructions that perform a method comprising the steps of:
- generating an asymmetric key pair generally unique to a domain ID;
  - communicating a first key of the asymmetric key pair in association with a device ID to an authentication authority over an ancillary communications network;
  - receiving a PIN from a user through user-input of the device;
  - communicating the PIN and a first primary identification over the ancillary communications network to the authentication authority;
  - receiving an encrypted passcode over the ancillary communications network from the authentication authority;
  - decrypting the passcode using the second key of the asymmetric key pair, and
  - displaying the passcode to the user.
98. The computer-readable medium of claim 97, wherein the first primary identification comprises the device ID and the domain ID.
99. The computer-readable medium of claim 97, wherein the method includes the further steps of:
- generating a second asymmetric key pair generally unique to a second domain ID;
  - communicating a first key of the second asymmetric key pair in association with the device ID to the authentication authority over the ancillary communications network;
  - receiving a second PIN from a user through user-input of the device;
  - communicating the second PIN and a second primary identification over the ancillary communications network to the authentication authority;

- (e) receiving an encrypted second passcode over the ancillary communications network from the authentication authority;
- (f) decrypting the second passcode using the second key of the second asymmetric key pair; and
- (g) displaying the second passcode to the user.

**100.** The computer-readable medium of claim 99, wherein the second primary identification comprises the device ID and the second domain ID.

**101.** Computer-readable medium having computer-executable instructions that perform a method comprising the steps of, during registration of an authorized user with respect to a network resource:

- (a) generating a first asymmetric key pair generally unique to a domain ID;
- (b) communicating a first key of the first asymmetric key pair in association with a device ID of a device to an authentication authority over an ancillary communications network;
- (c) receiving a first key of an asymmetric key pair of the authentication authority over the ancillary communications network;
- (d) receiving a PIN from a user through user-input of the device;
- (e) encrypting the PIN using the first key of the asymmetric key pair of the authentication authority;
- (f) communicating the encrypted PIN over the ancillary communications network to the authentication authority in association with the device ID;
- (g) receiving an encrypted registration code over the ancillary communications network from the authentication authority;
- (h) decrypting the registration code using the second key of the first asymmetric key pair, and
- (i) displaying the registration code to the user.

**102.** The computer-readable medium of claim 101, wherein the method further comprises the steps of, following registration of the authorized user:

- (a) receiving a suspect PIN from a suspect user through the user-input of the device;
- (b) communicating the suspect PIN and a first primary identification over the ancillary communications network to the authentication authority;
- (c) receiving an encrypted passcode over the ancillary communications network from the authentication authority;
- (d) decrypting the passcode using the second key of the first asymmetric key pair; and
- (e) displaying the passcode to the suspect user.

**103.** The computer-readable medium of claim 102, wherein the first primary identification comprises the device ID and the domain ID.

**104.** The computer-readable medium of claim 101, wherein the method further comprises the steps of, during registration of the authorized user with respect to a second network resource:

- (a) generating a second asymmetric key pair generally unique to a second domain ID;
- (b) communicating a first key of the second asymmetric key pair in association with the device ID to the authentication authority over the ancillary communications network;
- (c) receiving a first key of a second asymmetric key pair of the authentication authority over the ancillary communications network;
- (d) receiving a second PIN from the user through user-input of the device;
- (e) encrypting the second PIN using the first key of the second asymmetric key pair of the authentication authority;
- (f) communicating the encrypted PIN over the ancillary communications network to the authentication authority in association with the device ID;
- (g) receiving an encrypted second registration code over the ancillary communications network from the authentication authority;
- (h) decrypting the second registration code using the second key of the second asymmetric key pair; and
- (i) displaying the second registration code to the user.

**105.** The computer-readable medium of claim 104, wherein the method further comprises the steps of, following registration of the authorized user with respect to the second network resource:

- (a) receiving a suspect second PIN through the user-input of the device;
- (b) communicating the suspect second PIN and a second primary identification over the ancillary communications network to the authentication authority;
- (c) receiving an encrypted second passcode over the ancillary communications network from the authentication authority;
- (d) decrypting the second passcode using the second key of the second asymmetric key pair; and
- (e) displaying the second passcode.

**106.** The computer-readable medium of claim 105, wherein the second primary identification comprises the device ID and the second domain ID.

**107.** The computer-readable medium of claim 101, wherein the method further comprises the steps of,

- (a) during registration of the authorized user, receiving a first key of a secondary asymmetric key pair of the authentication authority over the ancillary communications network; and
- (b) after registration of the authorized user,
  - (i) receiving a challenge from an access authority from which access to the network resource is sought;
  - (ii) receiving a suspect PIN from a suspect user through the user-input of the device;
  - (iii) calculating a challenge response as a function of the challenge, the suspect PIN, and the first key of the secondary key pair of the authentication authority; and

(iv) displaying the challenge response to the suspect user.

108. The method of claim 107, wherein the challenge is received through the user-input of the device.

109. The method of claim 107, wherein the function comprises hashing the challenge, suspect PIN, and first key of the secondary key pair of the authentication authority.

110. A method for registering for access by an authorized user with respect to a network resource, comprising the steps of:

- (a) generating a first asymmetric key pair generally unique to a device of the authorized user,
- (b) communicating in association with a device ID of the device to an authentication authority over an ancillary communications network both a first key of the first asymmetric key pair and a PIN of the authorized user;
- (c) receiving an encrypted registration code over the ancillary communications network from the authentication authority;
- (d) decrypting the registration code using the second key of the first asymmetric key pair of the device; and
- (e) communicating the registration code to an access authority over a communications network in association with a user ID that identifies the authorized user to the access authority.

111. The method of claim 110, wherein the PIN is not stored within the device following its encryption and communication to the authentication authority and wherein the second key of the key pair of the device is not exported from the device.

112. A system in which an authorized user is registered with an authentication authority for later authenticating of a suspect user seeking to gain access from an access authority to a network resource, comprising the steps of:

- (a) generating within a device of the authorized user a first asymmetric key pair of the authorized user that is generally unique to the device, and
- (b) communicating with the device a first key of the first asymmetric key pair in association with a device ID of the device to the authentication authority over an ancillary communications network;

(c) by the authentication authority,

- (i) receiving and maintaining the first key in association with the device ID, and
- (ii) communicating to the device of the authorized user over the ancillary communications network a first key of a first key asymmetric key pair of the authentication authority that is unique to a domain ID;

(d) by the authorized user,

- (i) encrypting with the device using the first key of the asymmetric key pair of the authentication authority a PIN of the authorized user that is entered into the device, and
- (ii) communicating the encrypted PIN in association with the device ID to the authentication authority over the ancillary communications network;

(e) by the authentication authority,

- (i) decrypting the PIN and maintaining the PIN in association with the device ID and the domain ID,
- (ii) encrypting using the first key associated with the device ID a registration code, and
- (iii) communicating the registration code to the device of the authorized user over the ancillary communications network;

(f) by the authorized user,

- (i) decrypting within the device the encrypted registration code using the second key of the first asymmetric key pair of the authorized user, and
- (ii) communicating over a communications network the registration code to an access authority in association with a user ID identifying the authorized user to the access authority; and

(g) comparing the registration code received with the user ID with the registration code encrypted and sent to the authorized user.

113. The method of claim 112, wherein the PIN is not stored within the device following its encryption and communication to the authentication authority and wherein the second key of the key pair of the device is not exported from the device.

114. The system of claim 112, wherein the first asymmetric key pair of the authorized user in combination with the device ID is further unique to the domain ID.

115. The system of claim 112, further comprising the step of communicating by the access authority the user ID and the registration code to the authentication authority.

116. The system of claim 112, wherein said step of comparing the registration code received with the user ID with the registration code encrypted and sent to the user is performed by the authentication authority.

117. The system of claim 112, further comprising the step of communicating over the communications network the device ID with the registration code to the access authority.

118. The system of claim 117, further comprising the step of communicating the device ID with the registration code and user ID to the authentication authority.

119. The system of claim 93, further comprising maintaining the user ID in association with the device ID such that a passcode maintained in association with the device ID is retrievable based on the user ID.

120. A method of granting access to a suspect user seeking to access a network resource, comprising the steps of:

(a) first,

- (i) maintaining credentials of the authorized user such that the credentials are retrievable based on the user ID,
- (ii) receiving a user ID, registration code, and suspect credentials,

(iii) comparing the suspect credentials with the credentials maintained in association with the user ID, and

(iv) upon a successful authentication of the user ID by matching the suspect credentials with the maintained credentials, communicating the user ID and registration code to an authentication authority; and



- (b) thereafter, granting access to the network resource to a suspect user upon,
  - (i) receiving a user ID and passcode from the suspect user,
  - (ii) communicating the user ID and passcode to the authentication authority, and
  - (iii) receiving an indication of a successful passcode comparison by the authentication authority.

**121.** The method of claim 120, further comprising the steps of,

- (a) additionally receiving suspect credentials with the user ID and passcode,
- (b) comparing the suspect credentials with the credentials maintained in association with the user ID, and
- (c) communicating the user ID to the authentication authority only upon a successful match of the suspect credentials with the maintained credentials.

**122.** Computer-readable medium having computer-executable instructions for performing the method of claim 120.

**123.** A computer system including the computer-readable medium of claim 122.

**124.** A method of upgrading a single-factor authentication system to a multi-factor authentication system wherein a suspect user seeks access to a network resource, the single-factor authentication system including the binding of a user ID with credentials of an authorized user, the method comprising the steps of:

- (a) initially,
  - (i) binding a device ID of a device with a PIN,
  - (ii) binding the device ID with a private key of the device, and
  - (iii) binding the device ID with the user ID, including authenticating the user ID with the credentials; and

- (b) thereafter,
  - (i) authenticating the device ID including, as part thereof, communicating from the device the device ID and the PIN over an ancillary communications network,
  - (ii) authenticating the device including, as part thereof, communicating to the device a passcode encrypted with the public key corresponding to the device private key and decrypting the passcode using the device private key, and

- (iii) communicating the unencrypted passcode over a communications network with the user ID.

**125.** The method of claim 124, wherein the device ID is communicated over the ancillary communications network to an authentication authority and the unencrypted passcode is communicated over the communications authority to an access authority.

**126.** The method of claim 125, wherein the unencrypted passcode is subsequently communicated to the authentication authority for comparison with the passcode sent encrypted to the device.

**127.** The method of claim 124, wherein the passcode must be received over the communications network within a predetermined amount of time after being communicated encrypted to the device in order to gain access to the network resource.

**128.** The method of claim 127, wherein the predetermined period of time is less than ninety seconds.

**129.** The method of claim 127, wherein the predetermined period of time is less than a hour.

**130.** The method of claim 124, wherein the communications network is the Internet.

**131.** The method of claim 124, wherein the communications network is an intranet.

**132.** The method of claim 124, wherein the communications network is an untrusted network.

**133.** The method of claim 124, wherein communications over the communications network are encrypted.

**134.** The method of claim 124, wherein the ancillary communications network is a telecommunications network.

**135.** The method of claim 124, wherein the ancillary communications network is a trusted network.

**136.** The method of claim 124, wherein the device is a personal communications device.

**137.** The method of claim 136, wherein the personal communications device comprises a PDA.

**138.** The method of claim 136, wherein the personal communications device comprises a wireless device.

**139.** The method of claim 136, wherein the personal communications device comprises a GPS device.

**140.** The method of claim 136, wherein the personal communications device comprises a JAVA-enabled device.

**141.** The method of claim 136, wherein the personal communications device comprises a mobile phone.

**142.** The method of claim 136, wherein the personal communications device comprises a two-way pager device.

\* \* \* \* \*



US 20060130135A1

03 Jul 2012

2012100462

(19) **United States**  
 (12) **Patent Application Publication** (10) **Pub. No.: US 2006/0130135 A1**  
**Krstulich et al.** (43) **Pub. Date: Jun. 15, 2006**

(54) **VIRTUAL PRIVATE NETWORK CONNECTION METHODS AND SYSTEMS** (52) **U.S. Cl. .... 726/15**

(75) **Inventors: Zlatko Krstulich, Ottawa (CA); Cheng-Yln Lee, Ottawa (CA)** (57) **ABSTRACT**

**Correspondence Address:**  
**ECKERT SEAMANS CHERIN & MELLOTT, LLC.**  
**US STEEL TOWER**  
**600 GRANT STREET, 44TH FLOOR**  
**PITTSBURGH, PA 15219-2788 (US)**

A method and system for connecting a customer equipment (CE) communication device to a virtual private network (VPN) is provided. A virtual private network membership signal is generated at the customer equipment and transmitted to service provider equipment. The signal includes an identifier which identifies the customer equipment as a member of the virtual private network. On receiving the signal, service provider equipment such as a network element verifies that the customer equipment belongs to the virtual private network based on the customer identifier and only connects the customer equipment to the VPN if the verification is successful. The membership signal may be generated by a customer identification device distributed to the customer and installed in customer equipment to be connected to a virtual private network.

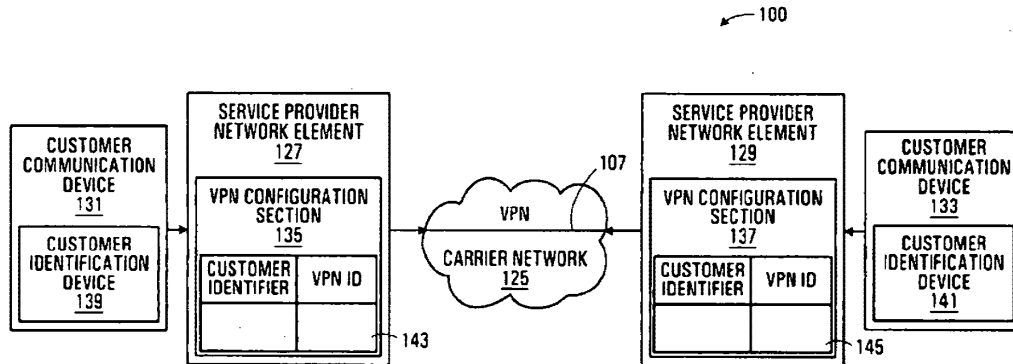
(73) **Assignee: ALCATEL**

(21) **Appl. No.: 11/009,917**

(22) **Filed: Dec. 10, 2004**

**Publication Classification**

(51) **Int. Cl. G06F 15/16 (2006.01)**



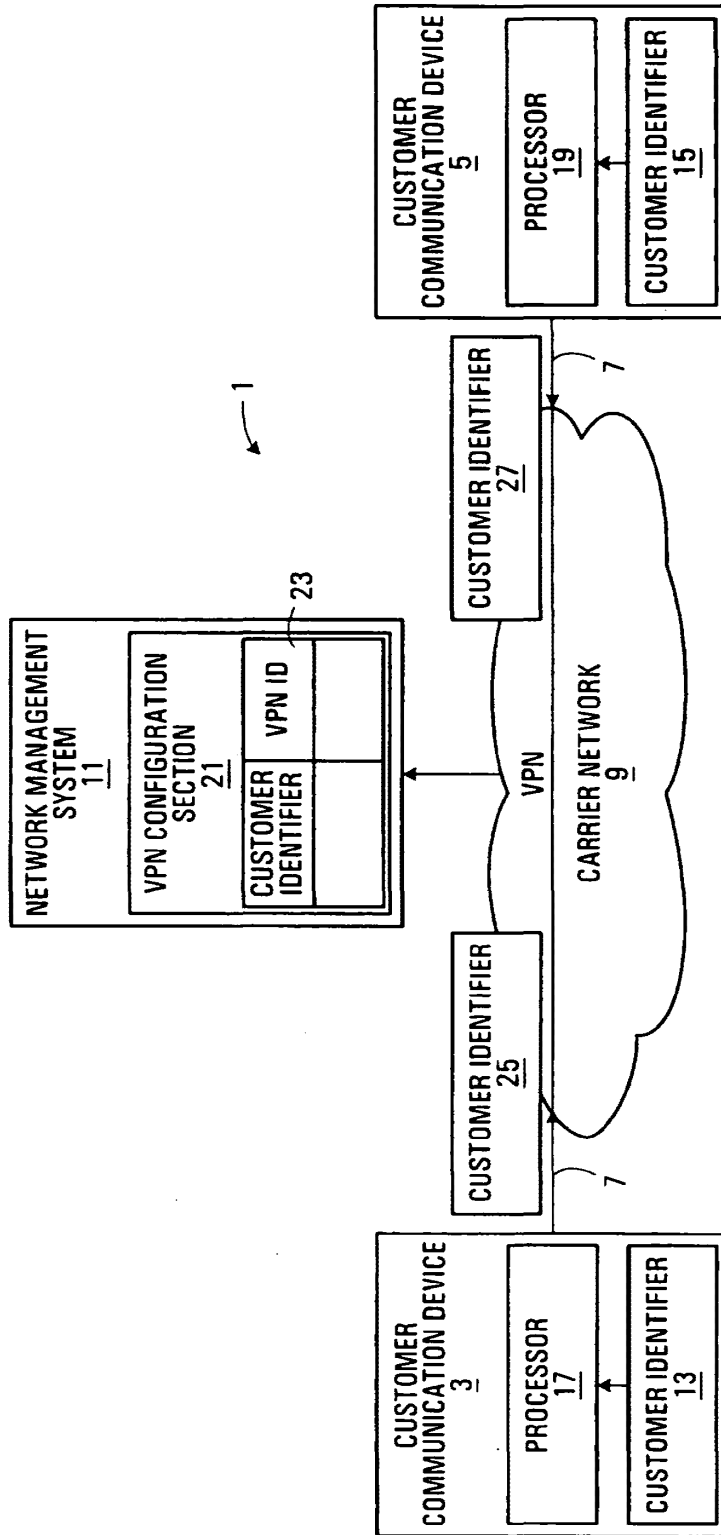
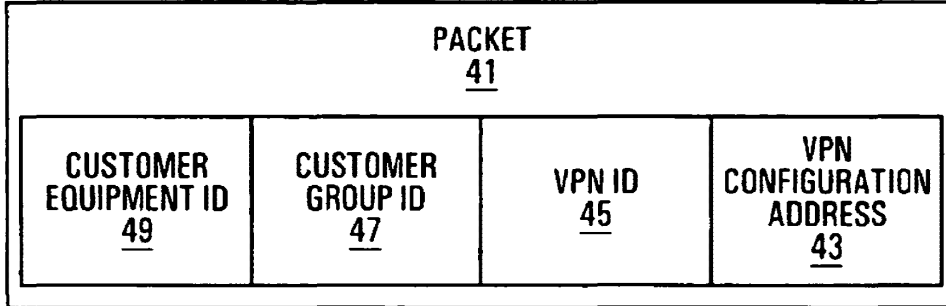


FIG. 1

2012100462 03 Jul 2012



**FIG. 2**

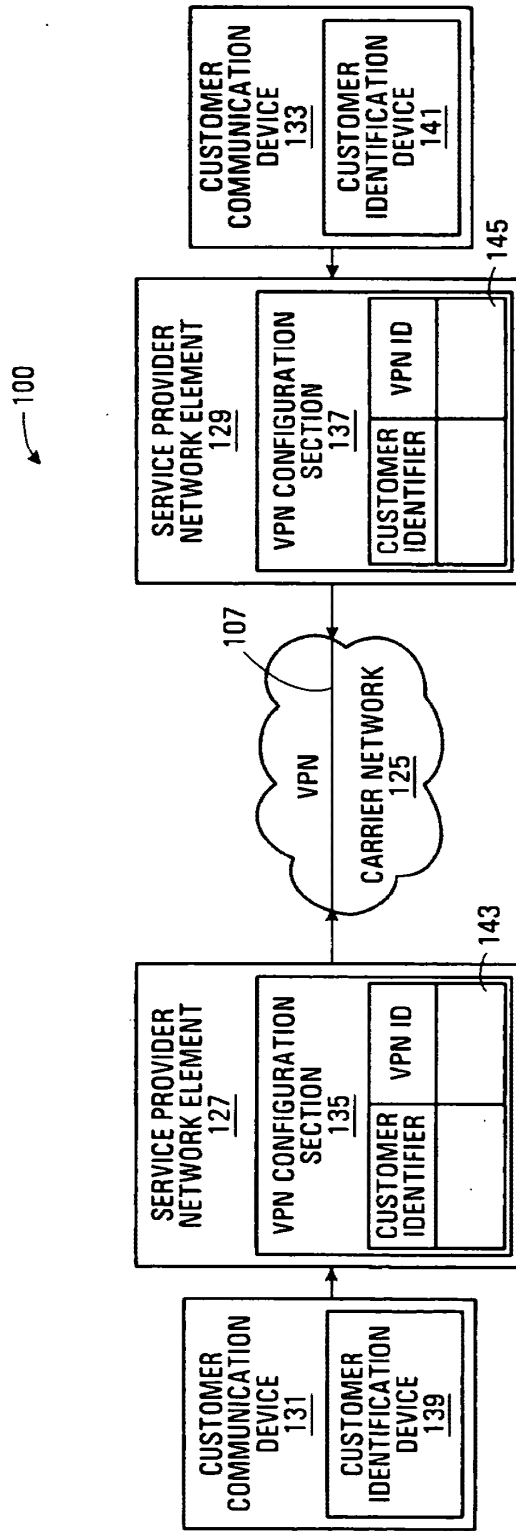


FIG. 3

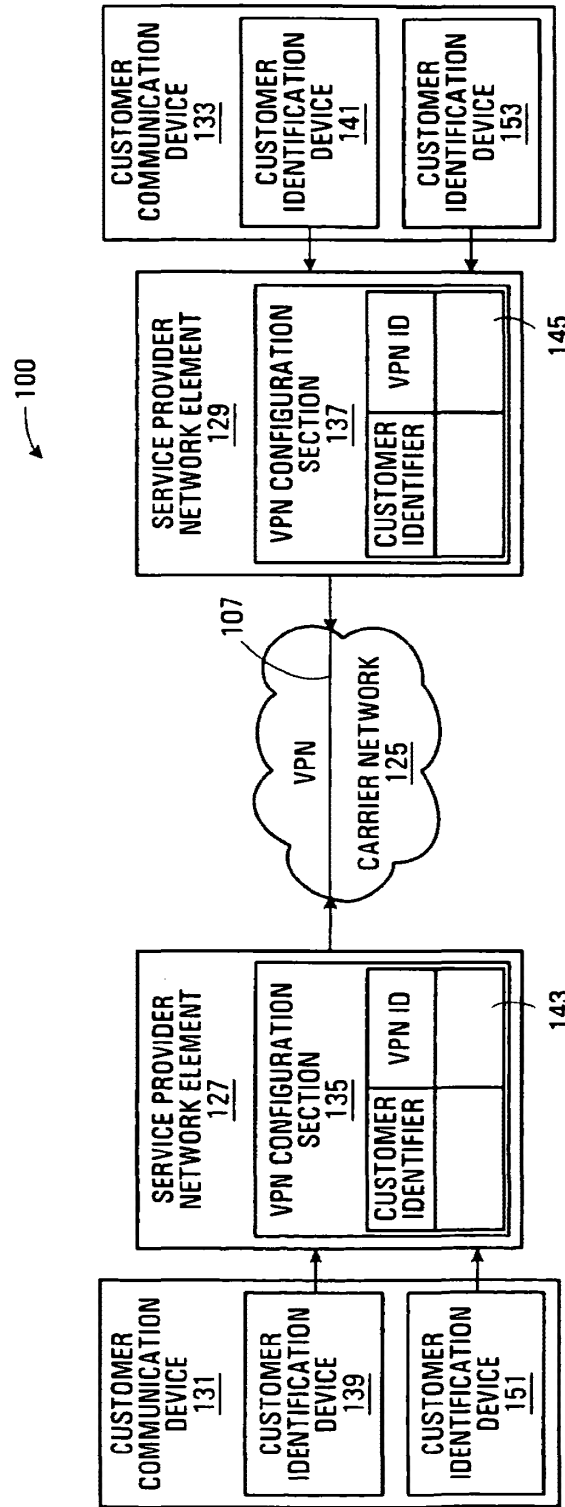
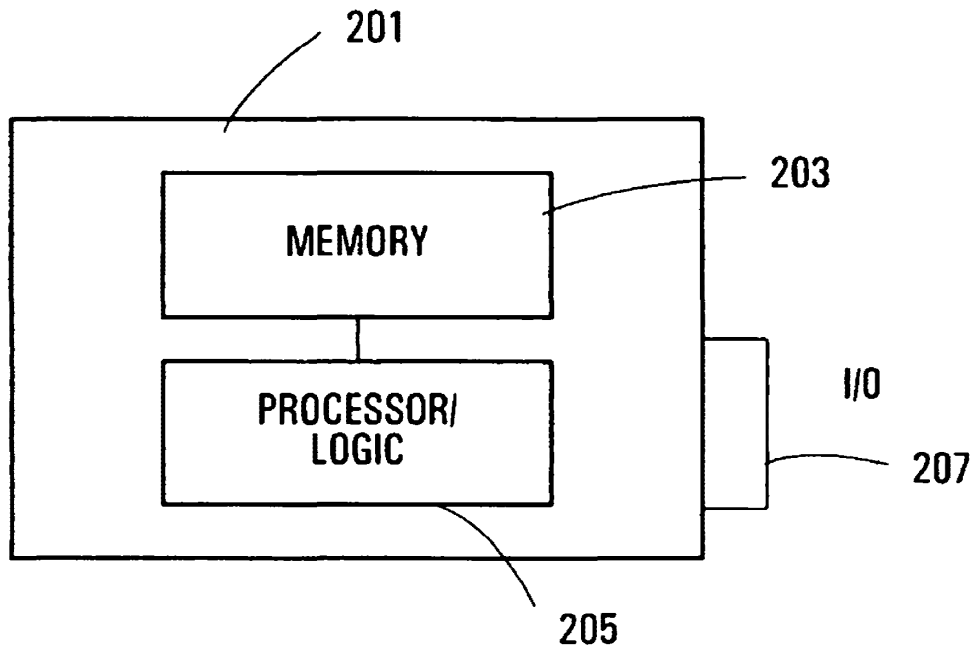


FIG. 4

2012100462 03 Jul 2012



**FIG. 5**

## VIRTUAL PRIVATE NETWORK CONNECTION METHODS AND SYSTEMS

### FIELD OF THE INVENTION

[0001] The present invention relates to methods and systems for connecting customer communication devices to a virtual private network and in particular, but not limited to, methods and systems for connecting communication devices to a multi-point virtual private network (mpVPN).

### BACKGROUND OF THE INVENTION

[0002] Virtual private networks allow predefined customer communication devices to be interconnected across a public network to enable private communication between devices which belong to the same VPN. Virtual private networks can be configured and implemented in a variety of different ways. For example, VPNs may be implemented using a link layer protocol such as TDM, FR (frame relay) or ATM (asynchronous transfer mode). These protocols allow point-to-point connectivity between two customer communication devices by forming a direct private connection or dedicated virtual private circuit (VPC) between the two devices, each connection being configured manually. However, VPNs based on these protocols are not generally implemented to allow multi-point connections, i.e. direct connections between all devices on the same virtual private network, with the service provider providing meshed connectivity.

[0003] A multi-point VPN is a service that implements an Ethernet LAN over a virtual layer 2 or layer 3 VPN in the carrier's domain, and typically connects numerous end-customer sites.

[0004] When configuring a virtual private network, it is important to ensure that only the intended subscriber equipment is connected to the VPN so that the network privacy and security of each customer is maintained. VPNs based on TDM, FR or ATM are less vulnerable to improper connection or misconfiguration as they are mostly point-to-point in nature and typically involve uniquely configured or custom data equipment at the customer premises. This implies that random misconnections would not result in an operational link and would very likely result in network alarms or "trouble tickets".

[0005] In contrast, configuring multi-point VPNs correctly and maintaining the configuration as customer drops are added and removed from the VPN instance can be error prone as it involves a number of configuration steps on carrier equipment that is shared across multiple end users, both at the physical layer (shared CPE or data terminating equipment) and the Operational Support System (OSS). The new generation of Ethernet/IP mpVPNs that interconnect customer CPE equipment utilize widely used and well standardized protocols and interfaces so that unwanted connections or "joins" to an mpVPN could easily go undetected and could provide a viable connection to an unintended party. Since the service provider would likely offer mpVPN services to a great number of clients such as enterprises and institutions, the risk and adverse consequences of inadvertently connecting the host node of one client to another client's mpVPN cannot be overlooked.

[0006] U.S. Patent Application Publication No. 2004/0093492 describes generating a digital certificate defining a

VPN by aggregating configuration parameters from both a service provider and the customer. The digital certificate is used by the VPN service provider or the VPN customer to verify the VPN configuration or associated configuration logs by comparing information contained in the certificate with data stored at a customer workstation or in the service provider database.

[0007] When a customer communication device is to be connected to a VPN, there is a possibility that the physical connection of the device interface and the provider edge node will be incorrectly implemented so that for example the customer device becomes connected to the VPN of another customer. Although the methods discussed above may allow such a misconfiguration to be detected, none of these methods prevent a customer communication device from being initially connected to an incorrect VPN to thereby prevent any communication between the device and the incorrect VPN.

[0008] U.S. Patent Application Publication No. 2004/0088542 (Daude et al.) describes a method for interconnecting different VPNs. An interconnection device analyzes information contained in digital certificates to identify VPN properties of a device being connected and compares these properties to those contained in another digital certificate of another VPN.

[0009] The interconnection device implements the VPN rules from one or both of the interconnecting VPNs which are necessary to establish a secure interconnection. The interconnection device implements secure interconnection between VPNs without the need for a completely centralized decision-making process.

[0010] Draft-IETF-BONICA-13VPN-AUTH-03.txt "CE to CE Authentication from Layer 3 VPNs", June 2002, and Draft-IETF-13VPN-13VPN-AUTH-00.txt "CE to CE Member Verification for Layer 3 VPNs" September, 2003, are concerned with the problem of VPN misconfigurations. A customer equipment-based verification mechanism is proposed in which each customer VPN site sends a "magic cookie" or token to the provider edge (PE) router that supports it. Upon receiving the token, the PE router connects the site to the VPN and distributes the token to other customer sites on the VPN, which verify the validity of the token. If the token is not valid, an alarm is raised at the customer VPN sites, and in this way misconfigurations are detected and indicated to the customer. As an optional variant, the first of these references describes an authentication process in which a PE router that receives a magic cookie from a CE transmits an authentication request which includes the magic cookie to a customer controlled server. If the server explicitly rejects the authentication request, the PE router terminates the authentication process and will neither accept traffic from the CE nor send traffic to the CE. However, if the customer controlled server cannot be contacted or sends no response at all, the PE router nevertheless joins the CE to the VPN. On the other hand, in the CE to CE based verification method disclosed in the second of these two references, there is no customer controlled authentication server and the PE simply connects the site to the VPN and immediately distributes tokens to other customer sites on the VPN.

[0011] A shortcoming of both of these proposals is that they are incapable of ensuring that a connection of non-VPN



member equipment to a VPN is always prevented. Instead, they allow misconfigurations to be detected, and require customer interaction to rectify a carrier error.

#### SUMMARY OF THE INVENTION

[0012] According to one aspect of the present invention, there is provided a customer equipment communication device comprising signal forming means adapted to form a virtual private network membership signal for transmission to and use by service provider equipment, wherein the signal includes an identifier for identifying said customer equipment as a member of a predetermined virtual private network, and is conditioned to cause said service provider equipment to verify that said communication device is a member of said predetermined virtual private network.

[0013] According to another aspect of the present invention, there is provided an apparatus for controlling connection of a customer communication device to a virtual private communication network, comprising means for receiving a signal from a customer communication device, determining means for determining from the signal whether or not the customer communication device is a member of a predetermined virtual private communication network, and controlling means for controlling connection of the customer communication device to the predetermined virtual private network based on the determination made by the determining means.

[0014] According to another aspect of the present invention, there is provided a method of controlling connection of a customer communication device to a virtual private communication network, comprising the steps of receiving at service provider equipment a signal from a customer communication device, determining at the service provider equipment whether or not the customer communication device is a member of a predetermined virtual private communication network based on information contained in the signal, and controlling connection of the customer communication device to the virtual private network based on the result of the determination.

[0015] Advantageously, in this arrangement, a customer communication device, such as a switch, router or host transmits a signal containing a customer identifier to service provider equipment responsible for configuring one or more virtual private networks. The configuration section of the service provider equipment determines from the customer identifier contained in the signal whether or not the customer device is a member of a predetermined virtual private network before connecting the communication device to the VPN. Advantageously, this arrangement enables an incorrect physical connection of a customer communication device at a provider edge node to be detected before data communication between the device and the virtual private network is enabled.

[0016] Furthermore, as the authentication process is performed by equipment under the control of the service provider, rather than requiring a customer controlled authentication server, a customer identifier belonging to one VPN is not passed to the customer of another VPN, so that each customer identifier can remain secret as between one customer and another.

[0017] Moreover, this arrangement allows the service provider equipment to verify whether or not customer equip-

ment should be connected to a VPN so that, unlike the prior art methodologies, the service provider equipment can always ensure that a connection is prevented if the authentication process fails.

[0018] In one embodiment, the authentication process is performed autonomously by the service provider network elements, for example, provider edge nodes, which are connected directly to customer equipment from which the VPN request is transmitted. Advantageously, this arrangement removes the need for element, network, or OSS management systems to participate in or orchestrate the authentication process thereby removing the need for modifying element, network or OSS systems to conform to a specific implementation of the authentication process. The simplification provided by this embodiment thereby makes the authentication process more robust and reliable.

[0019] According to another aspect of the present invention, there is provided a method of requesting connection of a customer equipment communication device to a predetermined virtual private network, comprising the steps of: forming at said customer equipment, a virtual private network membership signal for transmission to and use by service provider equipment, wherein the signal includes an identifier for identifying said customer equipment as a member of said predetermined virtual private network and is conditioned to cause said service provider equipment to verify that said communication device is a member of said predetermined virtual private network, and transmitting said signal from said customer equipment communication device to said service provider equipment.

[0020] According to another aspect of the present invention, there is provided a method of detecting member equipment of a virtual private network comprising the steps of: receiving signals which originate from customer equipment communication devices, the signals each containing a customer identifier and a virtual private network identifier, detecting the identifiers in the signals and recording information based on each detected identifier.

[0021] According to another aspect of the present invention, there is provided a method of controlling connection of customer communication equipment to a virtual private network, comprising the steps of: receiving at service provider equipment a predetermined customer identifier associated with a virtual private network from a customer equipment communication device, subsequently receiving another customer identifier, determining whether the other customer identifier is sufficiently similar to said predetermined customer identifier that both identifiers belong to the same customer, and controlling connection of service provider equipment based on the result of said determining step.

[0022] According to another aspect of the present invention, there is provided an apparatus for controlling connections to one or more virtual private networks, comprising receiving means for receiving from a customer equipment communication device a predetermined customer identifier associated with a virtual private network, and for receiving subsequent to receipt of said predetermined customer identifier, another customer identifier, and verification means for verifying whether the other customer identifier is sufficiently similar to said predetermined customer identifier that both identifiers belong to the same customer, and connection control means for controlling connection of customer com-

munication equipment to said virtual private network based on the result of the verification by said verification means.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0023] Examples of embodiments of the present invention will now be described with reference to the drawings in which:

[0024] FIG. 1 shows a schematic diagram of a communication network in which an embodiment of the present invention is implemented;

[0025] FIG. 2 shows an example of a customer identification packet according to an embodiment of the present invention;

[0026] FIG. 3 shows a communication network in which another embodiment of the present invention is implemented;

[0027] FIG. 4 shows a communication network in which another embodiment of the present invention is implemented; and

[0028] FIG. 5 shows an embodiment of a customer identification device according to an embodiment of the present invention.

#### DESCRIPTION OF EMBODIMENTS

[0029] FIG. 1 shows a schematic diagram of a communication network in which an embodiment of the present invention is implemented. In particular, FIG. 1 shows first and second customer communication devices 3, 5 which are to be connected to a virtual private network 7 over a carrier network 9 which is managed by a network management system 11. The customer communication devices may comprise any communication device connectable to a network, for example, a workstation, a host computer, a switch or a router. A device 13, 15 is connected to each customer communication device which contains an identifier for the customer. The identifier is transmitted from the customer communication device to the carrier network 9 and is used by the carrier network to verify that the customer communication device is a member of the virtual private network 7.

[0030] In one implementation, the carrier network 9 is adapted to verify, using the customer identifier transmitted from the communication device, that the communication device is a member of the VPN before the carrier network connects the customer communication device 3, 5 to the VPN 7. Alternatively, or in addition, the customer identifier may be transmitted from the customer communication device to the carrier network after the customer communication device has been connected to the VPN to verify that the communication device is an authorized member of the VPN, and the signal may be transmitted periodically.

[0031] The customer identification device 13, 15 may comprise any suitable device that can be connected to the customer communication device for transmitting, or causing the customer communication device to transmit, a customer identifier to the carrier network. The device may include a memory for storing the customer identifier and may further include a signal generator for generating a signal which includes the customer identifier for transmission to the carrier network. Alternatively, the customer identification device may be adapted to transmit the customer identifier to

a data communications processor 17, 19 of the customer communication device and the processor may generate a signal containing the customer identifier for transmission to the carrier network.

[0032] In this embodiment, the network management system 11 includes a virtual private network configuration section 21 which is responsible for the connection of customer communication devices to one or more virtual private networks. The VPN configuration section 21 includes a table 23 containing customer identifiers and an identification of each virtual private network with which they are associated.

[0033] In one implementation, a message or packet (or token) 25, 27 addressed to the VPN configuration section of the carrier network is formed at the customer communication device, which includes the customer identifier recorded in the customer identification device 13, 15, and is transmitted from the customer communication device to the network management system 11. On receiving the message, the VPN configuration section 21 checks the customer identifier against the list of customer identifiers stored in the table 23, and if a match is found, the VPN configuration section permits the customer communication device identified in the message to be connected to the VPN associated with the customer identifier. However, if the customer identifier in the message does not match any customer identifiers contained in the table 23, the VPN configuration section prohibits connection of the customer communication device to any VPN.

[0034] In another implementation, the packet 25, 27 transmitted from the customer communication device may contain a request for the customer communication device to be connected to a particular VPN. In this case, the packet contains the VPN identifier identifying the VPN to which the customer communication device is to be connected, and the customer identifier which may include a group identifier and/or an identification of the customer communication device, such as its network address. On receiving the request packet, the VPN configuration section 21 checks the VPN ID and the customer identifier contained in the packet with those stored in the table 23 and if a match of both parameters is found, the VPN configuration section 21 allows the customer communication device 3 to be connected to the VPN, otherwise connection to the VPN is denied.

[0035] Advantageously, this arrangement, in which an authentication signal is transmitted from a customer communication device to a carrier network, allows the carrier network to verify reliably whether or not the customer communication device is a member of a predetermined virtual private network before the device is connected to the VPN, and therefore prevents VPN misconfigurations. Furthermore, the customer communication device may be adapted to periodically transmit similar packets containing the customer ID to the carrier network to enable the carrier network to periodically check that the customer communication device continues to be a member of the virtual private network after being connected thereto.

[0036] In one embodiment, if a customer communication device becomes disconnected from the VPN, and its reconnection to the VPN is subsequently required, the customer communication device transmits a reconnection request and the customer ID (either separately or together) to the carrier network equipment responsible for VPN membership veri-

fication and connection. On detecting the request and customer ID, the carrier network equipment authenticates the customer equipment as belonging to the VPN using the customer ID before allowing reconnection.

[0037] The customer identifier may comprise any suitable identifier and may include several parts. In one embodiment, the customer identifier may simply comprise the name of the customer or another identifier which is unique to the customer. The customer identifier may comprise a common or group customer identifier which is used by customer communication devices all belonging to the same customer, and a second identifier which additionally identifies the particular customer communication device. The customer identifier may or may not also be encrypted.

[0038] An example of a VPN membership verification packet is shown in FIG. 2. The membership verification packet 41 includes a destination address which enables the packet to be transmitted to the VPN configuration section of the carrier network. The packet also includes a number of fields 45, 47, 49 which, in this embodiment contain the VPN identifier, a group identifier for the customer, and an identifier identifying the particular communication device to be connected to the VPN. Together with an appropriate query (e.g. one or more commands) the customer communication device will transmit an appropriate response containing the verification packet as shown in FIG. 2 enabling the customer communication device to be verified by the service provider.

[0039] In other embodiments of the present invention, authentication of a customer communication device to be connected to a particular VPN may be performed by network devices of the carrier network other than the network management system. For example, authentication may be performed by network elements or nodes of the network such as a provider edge (PE) node of the carrier network. An example of such an implementation is described below with reference to FIG. 3.

[0040] Referring to FIG. 3, a carrier network 125 includes a plurality of PE nodes 127, 129, each of which serves as both ingress and egress nodes to customer communication devices 131, 133 connected thereto. Each PE node 127, 129 includes a VPN configuration section 135, 137 for configuring one or more virtual private networks and which also authenticates customer identification devices to be connected (or reconnected) or which are already connected to a particular VPN.

[0041] Each customer communication device 131, 133 includes a customer identification device 139, 141 connected thereto which transmits or causes transmission of a customer identifier from the customer communication device to a PE node of the carrier network 125.

[0042] When first configuring a new VPN 107, a record identifying the VPN and a customer identifier associated with the VPN is created and stored in the VPN configuration section of a PE node of the carrier network 125. This record may be created in response to a VPN configuration request transmitted from one of the customer communication devices to be connected to the VPN. The request may include the customer identifier and also a VPN identifier which is to be created. Alternatively, the VPN identifier may be determined by the carrier network and transmitted to the

customer communication device. On receipt of the request, which includes the customer identifier, the PE node stores the customer identifier together with the VPN identifier and transmits both parameters to one or more other PE nodes of the carrier network 125.

[0043] Each additional customer communication device which is connected to the VPN is provided with a customer identification device which causes a message or packet containing the customer identifier to be transmitted to the PE node of the carrier network to which it is connected to enable the PE node to authenticate the customer communication device as a member of the VPN. The customer identification device connected to each customer communication device may be similar to any of the embodiments described above in connection with FIG. 1 and may operate in a similar manner.

[0044] The customer identifier generally includes an identifier which is common to all members of the VPN and may also include an additional identifier which uniquely identifies the particular customer communication device. The customer identifier signal transmitted from each customer communication device enables the PE node to which it is connected to verify that the customer device is a member of the VPN group before allowing the connection, and this arrangement therefore prevents incorrect communication devices from being connected to the VPN. Furthermore, this arrangement uses PE nodes to verify whether or not a particular customer communication device should be connected to a VPN without involving the element management, network management, or the Operational Support System (OSS), and therefore does not involve and is independent of higher layers of software applications. This arrangement is also more robust as it does not rely upon the success of communications to and from the OSS or upon the OSS operating properly, or to have been so modified, to provide the required verification. This arrangement also does not require any pre-configuration regarding the association of a group customer identification to a specific VPN.

[0045] Customer identification devices may be provided to the customer for connection to the customer communication devices when the customer subscribes to a virtual private network service. For example, a quantity of customer identification devices may be issued to the customer by the service provider of the virtual private network service and distributed to each customer site which is to be connected to the service. A customer identification device is connected by authorized personnel such as IT staff, to customer equipment at each site that is to be connected to the VPN service. Each customer identification device causes a customer ID signal to be transmitted to the VPN configuration application or process of the carrier network, which can then verify that the customer equipment at each site should be connected to the VPN before allowing the connection.

[0046] In an alternative embodiment, customer identification devices may be preinstalled in the customer communication devices, for example by the manufacturer or system integrator, rather than at a later time after the communication devices have been installed at the customer site. When a VPN service is required, the customer identification devices could be activated to transmit or cause transmission of the customer ID to the configuration process of the carrier network. Knowledge of the customer ID is independently

passed to the configuration process of the carrier network to allow verification that customer equipment should be connected to a VPN.

[0047] Since, in this embodiment, the group identification may be known to a third party, i.e. the manufacturer of the communication device with the preinstalled customer identification device, the customer identification signal may be suitably secured by any appropriate technique such as encryption techniques, of which public key infrastructure (PKI) techniques are one example. In this case, a key or customer signature is provided to the carrier network to allow the carrier network to read and authenticate the customer ID contained in the signal. If the customer key or signature matches, the configuration process of the carrier network allows the connection and enables data communication, otherwise the connection is denied.

[0048] Preinstallation of customer identification devices in customer equipment advantageously eliminates the need to separately distribute special ID devices that are limited to one customer, thereby reducing inventory and distribution concerns.

[0049] In another embodiment of the present invention, the customer may provide the service provider with information that enables the service provider to query and uniquely identify valid equipment before allowing connection to the mpVPN. For example, the carrier network may be provided with the MAC (Media Access Control) addresses of each customer communication device to be connected to a specific VPN instance, together with an appropriate query (e.g. one or more commands) which causes the customer communication device to transmit an appropriate response containing data which enables the customer communication device to be verified by the service provider as a valid member of that specific VPN. The response signal may contain a unique customer identifier and optionally other identifiers such as the VPN identifier to which the communication device is to be connected. In addition, the response signal may be secured, for example, by encryption. On receipt of the response signal by the VPN configuration process of the carrier network, the configuration process uses the signal to verify against its own verification data whether to connect the communication device to the VPN instance and permit data communication.

[0050] In other embodiments of the present invention, when commissioning a new virtual private network for the first time, the service provider equipment (e.g. network management system and/or network elements) may be arranged to connect the customer communication device to the virtual private network from which the customer identifier associated with that VPN is first received by the customer equipment. Advantageously, in this arrangement, the customer equipment needs no prior knowledge of the customer identifier associated with the VPN. On receiving subsequent requests from customer equipment to be connected to that VPN, the VPN configuration section of the service provider equipment simply verifies whether the subsequently received IDs match the first received customer ID and, if so, the connection is allowed, otherwise the connection is denied.

[0051] When a new VPN is first commissioned, the VPN configuration section may record the first received customer ID for future use in verifying subsequently requested con-

nections. The record may be stored permanently or temporarily for a limited time and then deleted. In cases where no record of the customer ID is retained by the service provider equipment, and a connection to the VPN is subsequently requested, the service provider equipment may be adapted to request the customer communication device from which the customer ID was first received, to retransmit the customer ID to enable the VPN configuration section to compare this with the customer ID in the subsequent request to determine whether to allow the new requested connection.

[0052] Alternatively, the customer communication device first connected to the VPN may repeatedly transmit the customer identifier to the service provider equipment to enable the VPN configuration section to use the retransmitted customer ID in verifying a subsequently requested connection.

[0053] Advantageously, either of these two arrangements obviates the need for the service provider equipment to maintain a record of the customer identifier or even needing to know what the customer ID is, thereby significantly reducing the risk of the customer identifier being revealed to unauthorized parties through the service provider equipment.

[0054] The above-described VPN connection verification process is based on a comparison of customer identifiers received from customer equipment communication devices, rather than with any record of a customer identifier maintained by the service provider. The customer identifier may be generated either by the customer or the service provider. Advantageously, if the customer identifier is generated by the customer, the customer identifier need never be retained by the service provider equipment, as the service provider equipment simply performs an equivalency check between two customer identifiers it receives. This also assists in making the customer ID inaccessible to service provider personnel.

[0055] In any of the embodiments described above, the customer identifier may comprise a plurality of characters in which the range of characters from which each character can be selected and/or the total number of characters in the customer identifier is sufficiently large that it would be improbable for any other VPN customer of the same service provider to choose the same customer ID. For example, the range or number of characters can be selected so that the probability is less than at least 1 in 50, preferably less than at least 1 in 1000 and more preferably less than 1 in a million. This allows the customer ID to be selected by the customer, rather than by the service provider, in a similar manner to selecting a PIN (Personal Identification Number) or password.

[0056] In any of the embodiments described herein, the customer ID may comprise several parts, including a predetermined field which is common to all equipment of the same customer to be connected to a particular VPN. In this case, the service provider equipment may only need to compare this predetermined field of one customer identifier with the corresponding field of another customer identifier. In this way, the customer equipment need only check that two customer identifiers are sufficiently similar to one another, and there is no requirement for the whole customer identifier to be the same as another nor any need to check equivalency of the whole customer identifier. The field or

portion of the customer ID selected for comparison should be that portion which is unique to each customer. If the customer ID is selected by the service provider, or otherwise verified as unique, the field may be relatively short. If the characters of the field are selected by the customer, the field should be sufficiently long to ensure its uniqueness, as described above.

[0057] In embodiments of the invention, more than one customer identification device may be connected to or installed in a customer communication device to provide redundancy in case one customer ID device fails. This is particularly beneficial when the continuation of an allowed connection of a customer communication device to a VPN, once a connection has been established, is dependent on the continued transmission of the customer identification signal from the customer equipment to the carrier network. In this case, where failure to send the signal would otherwise cause the carrier network to disconnect the customer equipment from the VPN, the provision of one or more additional customer identification devices would allow continued transmission of the signal and thereby prevent disconnection of the customer equipment should one customer ID device fail. Transmission of the signal may be monitored by the CPE equipment so that failures can be detected and the auxiliary or backup customer identification device activated, as necessary.

[0058] FIG. 4 shows an example of a communication network in which a customer communication device has a plurality of customer identification devices to provide redundancy. The components of FIG. 4 are similar to those shown in FIG. 3, and like parts are designated by the same reference numerals. In this embodiment, each customer communication device 131, 133 comprises a first customer identification device 139, 141 and a second customer identification device 151, 153. The first customer identification device may constitute the normally active device which provides the customer identifier to the service provider network, and the second customer identification device may constitute the redundant device which is activated if the first customer identification device fails.

[0059] FIG. 5 shows a schematic diagram of a customer identification device according to an embodiment of the present invention. The communication device 201 comprises a memory 203 (e.g. a non-volatile memory) which stores the customer identifier used by the service provider equipment to authenticate whether the customer equipment is member equipment of a predetermined virtual private network. The memory may also contain other data such as an identification of the virtual private network to which the customer belongs and/or the address of the service provider equipment which controls authentication and connection to VPNs. The customer identification device may also comprise a processor 205 for generating a packet or other signal containing the customer identifier used for authentication. A communication port 207 is also provided to connect the customer identification device to customer communication equipment at a customer site so that the signal generated by the customer identification device is transmitted to the service provider network. The port may comprise a uni-directional output port or a bi-directional input/output port. The customer identification device may be powered by either an internal or external power source, and in the case

of an external power source, the customer identification device may be provided with suitable power receiving terminals and connectors.

[0060] Another embodiment of the customer identification device may comprise simply a memory storing the customer ID, and possibly other data as indicated above, and a suitable port for connection to customer equipment. The memory may comprise a non-volatile memory, so that data can be held therein without the need for a power source. In this case, the customer equipment is adapted to generate a suitable packet (or other signal) containing the customer ID for transmission to the service provider network.

[0061] Advantageously, the embodiments described herein enable a physical connection of a customer communication device to a virtual private network to be detected before data communication between the device and the VPN is enabled. For example, an incorrect connection may occur when VPN provider personnel physically connect a customer communication device intended to be connected to that customer's VPN to the VPN of another customer, by for example, connecting the communication link to an incorrect port. However, before data communication is enabled, the VPN configuration section checks whether the customer identifier transmitted from the customer communication device corresponds to the customer identifier for the VPN associated with that port, and as the customer communication device is connected to the incorrect port, the verification section will deny the connection, and may also provide an indication of the denied connection to the VPN provider personnel so that the misconfiguration can be rectified.

[0062] Changes and modifications to the embodiments described herein will be apparent to those skilled in the art.

1. A customer equipment communication device comprising signal forming means adapted to form a virtual private network membership signal for transmission to and use by service provider equipment, wherein the signal includes an identifier for identifying said customer equipment as a member of a predetermined virtual private network and is conditioned to cause said service provider equipment to verify that said communication device is a member of said predetermined virtual private network.

2. A communication device as claimed in claim 1, wherein said identifier comprises at least one of an identifier uniquely identifying said customer equipment and an identifier used to identify a group of equipment belonging to said virtual private network.

3. A communication device as claimed in claim 2, wherein at least one of said unique identifier and said group identifier is encrypted.

4. A communication device as claimed in claim 1, wherein said identifier includes an identifier of said customer equipment and an identifier of said predetermined virtual private network.

5. A communication device as claimed in claim 1, wherein said signal forming means is arranged to condition said signal for transmission to service provider equipment adapted to configure said virtual private network.

6. A communication device as claimed in claim 5, wherein said service provider equipment comprises at least one of a service provider network management system and a network element at the edge of said service provider network.

7. A communication device as claimed in claim 1, wherein said signal forming means is adapted to form said signal at least one of before and after said communication device is connected to said virtual private network by said service provider.

8. A communication device as claimed in claim 1, comprising signal transmission means for transmitting said signal to said service provider equipment.

9. A communication device as claimed in claim 8, wherein said signal transmission means is adapted to transmit said signal at least one of before and after said customer communication device is connected to said virtual private network.

10. A communication device as claimed in claim 8, wherein said signal transmission means is adapted to repeatedly transmit said signal periodically.

11. A communication device as claimed in claim 1, further comprising a second signal forming means adapted to form said virtual private network membership signal.

12. A communication device as claimed in claim 11, further comprising detection means for detecting a failure of transmission of said virtual private network membership signal from said customer communication device and for causing a virtual private network membership signal to be formed by said second signal forming means in response to said detected failure.

13. A communication device as claimed in claim 8, further comprising second signal transmission means for transmitting said virtual private network membership signal to said service provider.

14. A communication device as claimed in claim 13, further comprising detection means for detecting failure of transmission of said signal by said signal transmission means and means for causing said signal to be transmitted by said second transmission means in response to detection of said failure.

15. A communication device as claimed in claim 1, wherein said signal forming means is one of (1) preinstalled in said customer equipment communication device before said communication device is first delivered to said customer and (2) connected to said customer equipment communication device after said communication device is first delivered to said customer.

16. A communication device as claimed in claim 1, wherein said signal forming means comprises a customer identification device which contains said customer identifier.

17. A communication device as claimed in claim 1, further comprising receiving means for receiving a predetermined signal from service provider equipment and wherein said communication device is adapted to transmit said virtual private network membership signal to said service provider equipment in response to said predetermined signal.

18. A method of requesting connection of a customer equipment communication device to a predetermined virtual private network, comprising the steps of:

forming at said customer equipment, a virtual private network membership signal for transmission to and use by service provider equipment, wherein the signal includes an identifier for identifying said customer equipment as a member of said predetermined virtual private network and is conditioned to cause said service provider equipment to verify that said communication device is a member of said predetermined virtual private network, and transmitting said signal from said

customer equipment communication device to said service provider equipment.

19. A method as claimed in claim 18, further comprising the step of connecting a customer identification device to said communication device to form said virtual private network membership signal.

20. A method of controlling connection of a customer communication device to a virtual private communication network comprising the steps of:

receiving at service provider equipment a signal from a customer communication device,

determining at said service provider equipment whether or not said customer communication device is a member of a predetermined virtual private communication network based on information contained in said signal, and

controlling connection of said customer communication device to said virtual private network based on the result of said determination.

21. A method as claimed in claim 20, wherein said customer communication device initially is not connected to said virtual private communication network, and wherein the step of controlling connection comprises enabling connection of the customer communication device to said virtual private communication network if, by said determining step, the customer communication device is determined to be a member of the virtual private communication network.

22. A method as claimed in claim 21, wherein said customer communication device is previously connected to said predetermined virtual private communication network, and the step of controlling connection comprises permitting continued enablement of said connection if, by said determination step, the customer device is determined to be a member of the predetermined virtual private communication network.

23. A method as claimed in claim 21, wherein said customer communication device initially is not connected to said predetermined virtual private communication network, and the step of controlling comprises prohibiting a connection of said customer communication device to said predetermined virtual private communication network, if by said determining step, the customer communication device is determined not to be a member of said virtual private communication network.

24. A method as claimed in claim 21, further comprising the step of monitoring at said service provider equipment receipt of a subsequent predetermined signal from said customer communication device, and controlling connection of said customer communication device to said virtual private communication network in response to said monitoring.

25. A method as claimed in claim 24, wherein the step of controlling said connection in response to said monitoring comprises disabling said connection if said further signal is not received within a predetermined time.

26. A method as claimed in claim 25, further comprising the step of monitoring at said service provider equipment receipt of a subsequent predetermined signal from said customer communication device, and controlling connection of said customer communication device to said virtual private communication network in response to said monitoring.

27. A method as claimed in claim 26, wherein the step of controlling said connection in response to said monitoring comprises disabling said connection if said further signal is not received within a predetermined time.

28. A method as claimed in claim 20, wherein said service provider equipment comprises at least one of a network management system and a provider edge network element.

29. A method as claimed in claim 20, further comprising the step of transmitting from said service provider equipment a customer identifier identifying said customer and a VPN identifier identifying said predetermined virtual private network to one or more provider edge network elements if, by said determining step, said customer communication device is determined to be a member of said predetermined virtual private network.

30. A method as claimed in claim 20, wherein said determining step is performed as part of a virtual private network configuration process in said service provider equipment.

31. A method as claimed in claim 20, comprising receiving at said service provider equipment a signal requesting reconnection of a previously connected but subsequently disconnected customer communication device, and subsequently performing said determining and controlling steps in response to said signal containing said information.

32. A method as claimed in claim 20, further comprising the step of providing said customer with a customer identification device for use in generating said signal from said customer communication device.

33. A method as claimed in claim 18, further comprising providing first and second independently operable customer identification devices each capable of forming said virtual private network membership signal, monitoring said first customer identification device from said virtual private network membership signal if said first customer identification device fails.

34. A method of controlling connection of a customer communication device to a virtual private communication network comprising:

monitoring at service provider equipment, receipt of a predetermined signal from a customer communication device, and

controlling connection of said customer communication device to a predetermined virtual private communication network based on whether or not said predetermined signal is received at said service provider equipment within a predetermined time.

35. A method as claimed in claim 34, wherein a connection between said customer communication device and said virtual private communication network is previously established, and the step of controlling comprises disabling said connection if said signal is not received within said predetermined time.

36. A method as claimed in claim 34, wherein a connection between said customer communication device and said virtual private communication network is previously established, and the step of controlling comprises continuing to enable the established connection if said signal is received within said predetermined time.

37. A method as claimed in claim 35, wherein said controlling is performed as part of a virtual private network configuration process at said service provider equipment.

38. An apparatus for controlling connection of a customer communication device to a virtual private communication network comprising:

means for receiving a signal from a customer communication device,

determining means for determining from information in said signal whether or not said customer communication device is a member of a predetermined virtual private communication network, and

controlling means for controlling connection of said customer communication device to said predetermined virtual private network based on the determination made by said determining means.

39. An apparatus as claimed in claim 38, wherein said controlling means is adapted to enable connection of said customer communication device to said predetermined virtual private network if said determining means determines that the customer communication device is a member of said predetermined virtual private communication network.

40. An apparatus as claimed in claim 38, wherein said controlling means is adapted to prohibit connection of the customer communication device to said predetermined virtual private network if said determining means determines that said customer communication device is not a member of said predetermined virtual private network.

41. An apparatus as claimed in claim 38, wherein said information comprises a customer identifier.

42. An apparatus as claimed in claim 41, wherein said information includes an identifier identifying said predetermined virtual private communication network.

43. An apparatus for controlling connection of a customer communication device to a virtual private communication network comprising:

monitoring means for monitoring receipt of a predetermined signal from a customer communication device, and

controlling means for controlling connection of said customer communication device to a predetermined virtual private communication network based on whether or not said predetermined signal is received within a predetermined time.

44. An apparatus as claimed in claim 43, wherein said controlling means is adapted to disable a previously established connection of said customer communication device to said virtual private network if said predetermined signal is not received within said predetermined time.

45. An apparatus as claimed in claim 43, wherein said controlling means is adapted to permit a previously established connection between a customer communication device and said predetermined virtual private network to continue if said predetermined signal is received within said predetermined time.

46. An apparatus as claimed in claim 43, further comprising indicator means for providing an indication to an operator if said predetermined signal is not received within said predetermined time.

47. A customer identification device comprising:

a non-volatile memory for storing a customer identifier, signal forming means for forming a signal conditioned for transmission to a virtual private network configuration section of a predetermined carrier network and

for causing said configuration section to verify that said device is a member of a predetermined virtual private network, the signal containing said customer identifier, and

connection means for connecting said device to a customer communication device.

48. A method of controlling connection of customer communication equipment to a virtual private network, comprising the steps of:

receiving at service provider equipment a predetermined customer identifier associated with a virtual private network from a customer equipment communication device,

subsequently receiving another customer identifier,

determining whether the other customer identifier is sufficiently similar to said predetermined customer identifier that both identifiers belong to the same customer, and

controlling connection of service provider equipment based on the result of said determining step.

49. A method as claimed in claim 48, wherein said predetermined customer identifier is the first customer identifier associated with said virtual private network to be received, and connecting the customer equipment communication device from which said first customer identifier is received to said virtual private network.

50. A method as claimed in claim 49, wherein said other customer identifier is received from another customer equipment communication device, and connecting said other customer equipment communication device to said virtual private network if said other customer identifier is determined to be sufficiently similar to said predetermined customer identifier.

51. A method as claimed in claim 49, wherein said other customer identifier is received from another customer equipment communication device, and denying connection of said other customer equipment communication device to said virtual private network if the other customer identifier is determined to be insufficiently similar to said predetermined customer identifier.

52. A method as claimed in claim 48, further comprising requesting the customer equipment communication device from which said predetermined customer identifier is received to send said predetermined customer identifier to said service provider equipment again in response to said service provider equipment receiving said other customer identifier, and wherein said determining step is performed based on the retransmitted predetermined customer identifier.

53. A method as claimed in claim 48, comprising repetitively receiving said predetermined customer identifier which is retransmitted from said customer equipment communication device and wherein said determining step is performed based on a retransmitted predetermined customer identifier.

54. A method as claimed in claim 48, wherein said predetermined customer identifier includes a field of characters which is common to all customer equipment of a predetermined customer to be connected to a predetermined VPN.

55. A method as claimed in claim 54, wherein the characters of said field are selected by said customer.

56. A method as claimed in claim 54, wherein at least one of (a) the range of characters from which each character in said field can be selected and (b) the number of characters in said field is sufficient to cause the probability of any other customer selecting the same sequence of characters to be less than a predetermined value.

57. A method as claimed in claim 56, wherein said predetermined value is 1 in a million.

58. A method as claimed in claim 54, wherein said determining step comprises comparing said field with a field contained in said other customer identifier.

59. Apparatus for controlling connections to one or more virtual private networks, comprising receiving means for receiving from a customer equipment communication device a predetermined customer identifier associated with a virtual private network, and for receiving subsequent to receipt of said predetermined customer identifier, another customer identifier, and verification means for verifying whether the other customer identifier is sufficiently similar to said predetermined customer identifier that both identifiers belong to the same customer, and connection control means for controlling connection of customer communication equipment to said virtual private network based on the result of the verification by said verification means.

60. An apparatus as claimed in claim 59, wherein said connection control means is adapted to connect to said virtual private network the customer equipment communication device from which a customer identifier associated with said virtual private network is first received by said apparatus.

61. An apparatus as claimed in claim 60, wherein said connection control means is adapted to connect a customer equipment communication device from which said other customer identifier is received if said verification means determines that the other customer identifier is sufficiently similar to said first received customer identifier.

62. An apparatus as claimed in claim 61, further comprising transmitting means for transmitting to said first connected customer communication device a request for said predetermined customer identifier in response to receiving said subsequent customer identifier and wherein said verification means is adapted to verify whether said other customer identifier is sufficiently similar to said predetermined customer identifier transmitted from said customer equipment in response to said request.

63. An apparatus as claimed in claim 59, wherein said customer identifier comprises a field of characters which is common to all customer equipment of a predetermined customer to be connected to said virtual private network.

64. An apparatus as claimed in claim 63, wherein the characters of said field are selected by said customer.

65. An apparatus as claimed in claim 63, wherein at least one of (a) the range of characters from which each character can be selected and (b) the number of characters in said field is sufficient to cause the probability of any virtual private network customer of said service provider selecting the same sequence of characters to be less than a predetermined value.

66. An apparatus as claimed in claim 65, wherein said predetermined value is 1 in a million.

\* \* \* \* \*





US 20100281261A1

2012100462 03 Jul 2012

(19) **United States**  
 (12) **Patent Application Publication** (10) **Pub. No.: US 2010/0281261 A1**  
**Razzell** (43) **Pub. Date: Nov. 4, 2010**

(54) **DEVICE AND METHOD FOR NEAR FIELD COMMUNICATIONS USING AUDIO TRANSDUCERS**

**Publication Classification**

(51) **Int. Cl.**  
*H04L 29/06* (2006.01)  
*H04B 5/00* (2006.01)  
*H04L 9/00* (2006.01)  
*H04K 1/00* (2006.01)

(75) **Inventor:** Charles Razzell, Pleasanton, CA (US)

**Correspondence Address:**  
 NXP, B.V.  
 NXP INTELLECTUAL PROPERTY & LICENSING  
 M/S41-SJ, 1109 MCKAY DRIVE  
 SAN JOSE, CA 95131 (US)

(52) **U.S. Cl.** ..... 713/171; 455/41.1; 713/168; 380/270

(57) **ABSTRACT**

Secure wireless communication links are established between proximately-located devices, each of which includes respective audio transmitters and audio receivers. The audio transmitter of the first device can be used to transmit a device-dependent authentication key, which is received by the audio receiver of the second device. The audio transmitter of the second device can be used to transmit an acknowledgement, which is received at the audio receiver of the first device. The round-trip time from transmitting the authentication key from the first device to receiving the acknowledgement at the first device can be determined, and the decision of whether to establish the secure wireless communication link can be based on the determined round-trip time. In certain embodiments, these steps can be repeated starting with the second device to establish a two-way trust between the devices.

(73) **Assignee:** NXP B.V., Eindhoven (NL)

(21) **Appl. No.:** 12/743,425

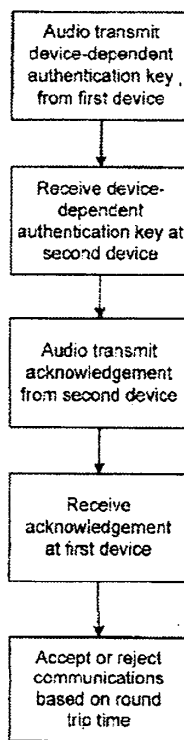
(22) **PCT Filed:** Nov. 13, 2008

(86) **PCT No.:** PCT/IB2008/054765

§ 371 (c)(1),  
 (2), (4) **Date:** May 18, 2010

(30) **Foreign Application Priority Data**

Nov. 21, 2007 (US) ..... 60/989547



This data, for application number 2012100462, is current as of 2012-12-28 22:09 AEST

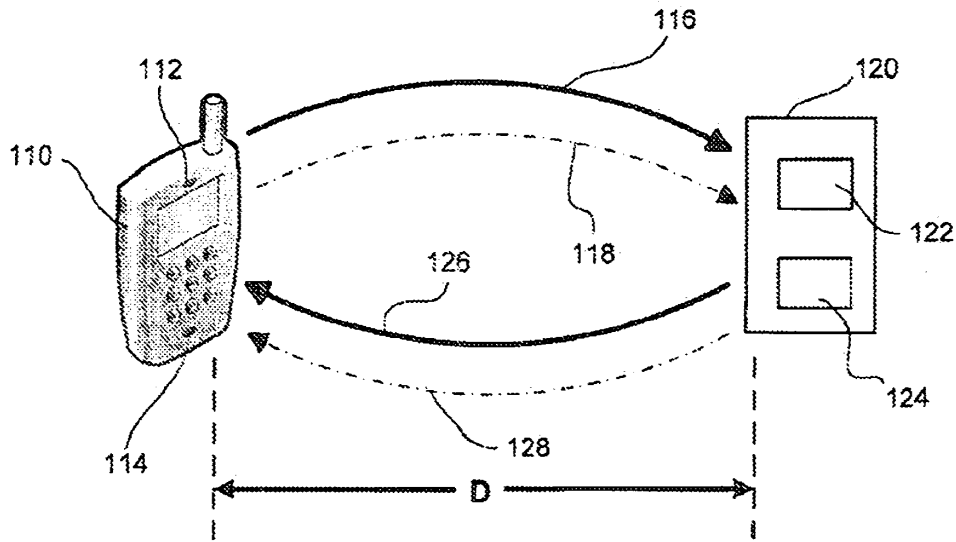
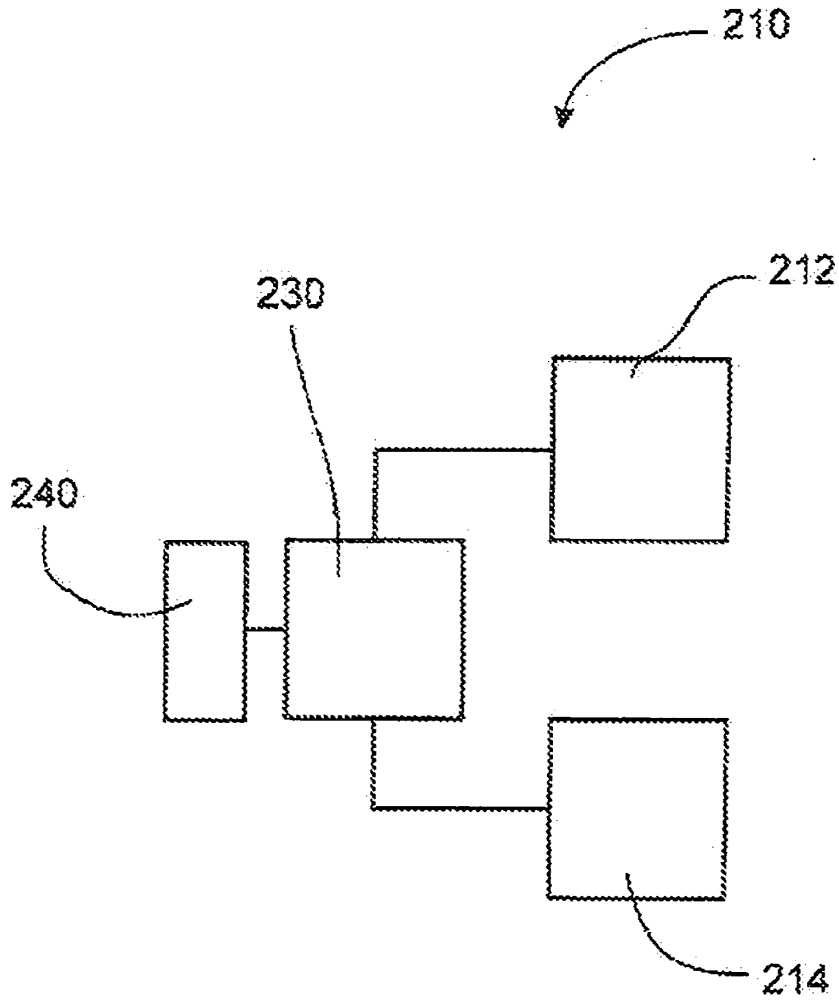
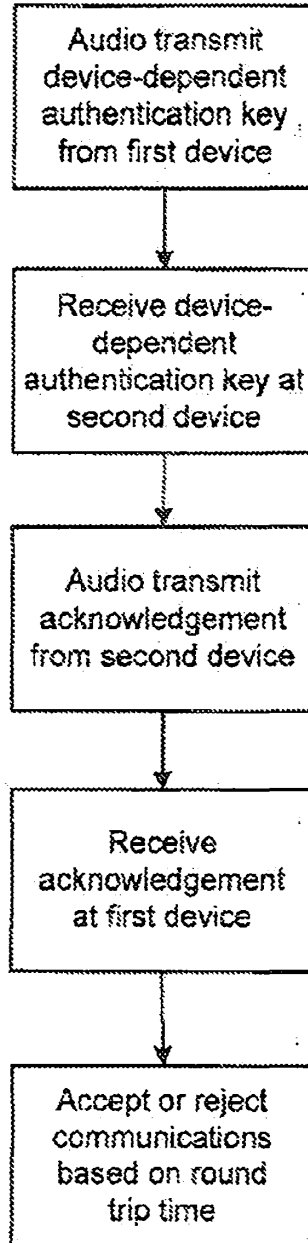


FIG. 1



**FIG. 2**



**FIG. 3**

## DEVICE AND METHOD FOR NEAR FIELD COMMUNICATIONS USING AUDIO TRANSDUCERS

### FIELD OF THE INVENTION

[0001] The present invention relates generally to wirelessly exchanging data between devices over short distances, and particularly to using acoustic signals to exchange data between devices over short distances, for example to establish a secure communications link.

### BACKGROUND

[0002] Near Field Communication (NFC) is a short-range wireless communication technology that provides for the exchange of data between devices distances typically up to about 20 cm. NFC technology is based on RFID, and works by magnetic field induction using relatively low data rates (specified speeds are 106 kbit/s, 212 kbit/s and 424 kbit/s). NFC technology is primarily used with mobile phones, and can be used to provide services such as: card emulation, in which the NFC-enabled device behaves like an existing contactless card; RFID reader, in which the NFC-enabled device is active and reads a passive RFID tag, for example for interactive advertising; and communications mode, in which two NFC-enabled devices exchange information.

[0003] NFC and Bluetooth are both short-range communication technologies which have recently been integrated into mobile phones. The significant advantage of NFC over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify Bluetooth devices, the connection between two NFC-enabled devices is established immediately (<0.1 s). To avoid the complicated configuration process, NFC can be used to set up the Bluetooth link.

### SUMMARY

[0004] Various aspects of the present invention are directed to methods for establishing a secure wireless communication link between first and second proximately-located devices, each of which includes respective audio transmitters and audio receivers. The methods can include using the audio transmitter of the first device to transmit a device-dependent authentication key, receiving the transmitted authentication key at the audio receiver of the second device and using the audio transmitter of the second device to transmit an acknowledgement, receiving the acknowledgement at the audio receiver of the first device, determining the round-trip time from transmitting the authentication key from the first device to receiving the acknowledgement at the first device, and determining whether to establish the secure wireless communication link based on the determined round-trip time. In certain embodiments, these steps can be repeated starting with the second device to establish a two-way trust between the devices.

[0005] Consistent with example embodiments, the present invention is directed mobile communications devices that include an audio transmitter, an audio receiver, and circuitry adapted to send audio data packets via the audio transmitter, receive audio data packets via the audio receiver, calculate round-trip times between sending audio data packets and receiving audio acknowledgements, and validate audio communications based on the calculated round-trip times.

[0006] Consistent with example embodiment, the present invention is further directed to methods for use with a mobile

communications device having an audio transmitter, an audio receiver, and a processor adapted to send audio data packets via the audio transmitter and receive audio data packets via the audio receiver. The methods can include adapting the mobile communications device to establish secure communication links by uploading a program to the mobile communications device, the program being executable by the processor to calculate round-trip times between sending audio data packets and receiving audio acknowledgements, and to validate audio communications based on the calculated round-trip times.

[0007] The above summary is not intended to describe each embodiment or every implementation of the present disclosure. The figures and detailed description that follow more particularly exemplify various embodiments.

### BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The invention may be more completely understood in consideration of the following detailed description of various embodiments of the invention in connection with the accompanying drawings, in which:

[0009] FIG. 1 illustrates establishing a communications link between proximately-located devices via acoustic signals in accordance with embodiments of the present invention;

[0010] FIG. 2 illustrates circuitry for use in a device for establishing communications links with proximately-located devices via acoustic signals in accordance with embodiments of the present invention; and

[0011] FIG. 3 illustrates steps that can be performed in accordance with embodiments of the present invention.

[0012] While the invention is amenable to various modifications and alternative forms, specifics thereof have been shown by way of example in the drawings and will be described in detail. It should be understood, however, that the intention is not to limit the invention to the particular embodiments described. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the scope of the invention including aspects defined by the appended claims.

### DETAILED DESCRIPTION

[0013] Embodiments of the present invention relate to using acoustic signals, for example airborne acoustic signals, to exchange data between proximately-located devices. The acoustic signals can be transmitted and received using audio transducers, for example a speaker and microphone of a mobile phone. As such, embodiments of the present invention can advantageously utilize existing audio transducers as the means of out-of-band communications. For example, the audio transducers already existing in mobile phone devices, along with voiceband modem technology, can be used to establish communications links with other proximately-located devices without the need for adding the hardware required with typical NFC techniques. At the same time, all the services normally provided by NFC can still be provided.

[0014] As discussed, NFC operates over short distances and enables electronic devices such as cell phones and PDAs to connect with each other and share information simply by being positioned close together. While NFC has been purported to have a great number of potential applications, the cost, size and integration difficulties may limit widespread adoption in mass-market mobile phones. NFC transducers

are not small and are difficult to integrate into typical cell-phone case mechanics, especially when using metalized parts, which can detune or block the NFC transducers. Acoustic data exchange to establish secure links between proximately-located devices can overcome the difficulties of common NFC techniques by providing an easily integrated solution that is not prone to interference and that can provide the same functionality.

**[0015]** In various embodiments of the present invention, the round-trip flight time between sending acoustic data and receiving acoustic acknowledgements can be measured in an effort to provide communications security. For example, a deliberate upper bound on the operating distance can be implemented by rejecting all communications for which the round-trip time is greater than a specified maximum. This can help reduce the possibility of eavesdropping. In addition, robust communication can be obtained in the presence of ambient acoustic noise by using appropriate filtering, extra error correction coding, and lower data rate. The various embodiments of the present disclosure are independent of modem speed and modulation technique.

**[0016]** FIG. 1 illustrates an example of a communications link between a first device 110 and a second device. As shown, first device 110 is a mobile device such as a cell phone, PDA, media player, or the like, although it will be appreciated that any suitable device can be used. Second device 120 can be a stationary device such as a ticketing or electronic banking kiosk, fixed points in a building such as limited access doors or security checkpoints, and the like, or can be another mobile device. Device 110 is equipped with an audio transmitter 112, such as a speaker, and an audio receiver 114, such as a microphone. While audio transmitter 112 and audio receiver 114 are shown separately, they can be provided in any suitable manner. Preferably, the audio transducers already used in the device are used as the audio transmitter and receiver. Device 120 is likewise equipped with an audio transmitter 122 and an audio receiver 124.

**[0017]** In an example embodiment, when device 110 is brought into proximity with device 120, the audio transmitter 112 can be used to send an audio data message 116. The message 116 can include an identifier, or device-dependent authentication key. The identifier can be randomly generated to promote additional security. The message 116 can also include a timestamp indicating the time at which the message 116 was sent. Message 116 can be received at the audio receiver 124 of device 120. Once received, the message 116 can be subject to an immediate acknowledgement message 126 sent by the audio transmitter 122 of device 120. Acknowledgement 126 can include the identifier from message 116, along with a timestamp indicating when message 116 was received and/or when acknowledgement 126 was sent. Upon receiving acknowledgement 126 at audio receiver 114, device 110 can compute the round-trip time from sending audio message 116 to receiving audio acknowledgement 126. Using the determined round-trip time, and knowing the speed of sound in the propagation medium (e.g., air), the distance  $D$  between the devices can be determined. A maximum round-trip time can be set to place a limit on  $D$ . This provides a certain measure of security. As a further security measure, the timestamps can be used to determine whether the first leg of the round-trip communication (time from sending message 116 from device 110 to receiving message 116 at device 120) matches the second leg of the round-trip communication

(time from sending acknowledgement 126 from device 120 to receiving acknowledgement 126 at device 110).

**[0018]** Once the devices 110 and 120 are securely paired, desired communications can take place. For example, pairing of devices 110 and 120 by acoustic communications can be used as an out-of-band method of exchanging encryption keys that are used for secure in-band communications. The pairing can also be used to quickly link the devices for Bluetooth communications. As will be appreciated, any suitable procedures for device pairing can be used, for example Diffie-Hellman key agreement methods.

**[0019]** Referring back to FIG. 1, if two-way mutual trust is desired, device authentication can optionally take place from device 120 to device 110 in a similar ping-and-echo fashion as from device 110 to device 120. For example, message 128 can be sent acoustically from the audio transmitter 122 of device 120, where message 128 includes an identifier (for example a randomly generated authentication key specific to device 120) and optionally a timestamp. When message 128 is received by audio receiver 114 of device 110, an acknowledge message 118 can be sent back from the audio transmitter 112 of device 110. The acknowledge 118 can include the identifier sent in message 128, along with a timestamp indicating when acknowledge 118 was sent and/or when message 128 was received. Device 120 receives the acknowledge message 118 at audio receiver 124. Round-trip time for the communication can be determined and used as described above to establish a mutual trust pairing.

**[0020]** A datagram, for example containing a unique, random identifier, can be sent from device A, and subject to an immediate acknowledgement upon its receipt at device B. In its acknowledgement, device B can echo the identifier supplied by device A, and can also supply a unique identifier specific to device B. The round-trip delay from device A to device B and back to device A can establish a proximity trust relationship, and can prevent a distant intercept device from acting as man-in-the-middle. If mutual trust, rather than one-way trust, is desired the ping-and-echo response can be repeated starting with device B initiating the ping.

**[0021]** FIG. 2 schematically illustrates a circuit 210 for sending a receiving audio data messages using audio transmitter 212 and audio receiver 214, and for determining round-trip times of acoustic communications. A processor unit 230 can be connected to the transmitter 212 and receiver 214 to send and receive audio communications in a suitable manner. In the case of a mobile phone equipped with speaker phone capabilities, the processor unit 230 can be used to send and receive acoustic messages in a manner similar to transmitting and receiving voice signals during a phone call. Processor 230 can be adapted to determine round-trip times so that a secure communications link can be established as described above. Processor 230 can include or be connected to an internal memory 240, for example a non-volatile memory, that stores a program for generating and decoding audio messages and for determining round-trip times so that secure communications links between proximately-located devices can be established. As such, existing devices can be enabled to perform methods of the present disclosure by storing such a program, for example as firmware, in a non-volatile memory on the device so that it can be accessed by the processing unit.

**[0022]** As discussed, in certain embodiments secure communications can be established by limiting the distance over which replies are considered valid. Considering that the speed of sound in air is 344 m/s, each millisecond of round-trip time

for a message can be considered as representing 17 cm of distance between the two devices. If device separations are limited to 0.5 m, the maximum round-trip can therefore be set at 6 ms. To help ensure reliability, turnaround times for the immediate acknowledge should be specified as low enough so that no allowance for turn-around time need be made in computing the round-trip time, and thus the distance between devices. For example, allowing turn-around times of 3 ms creates a device-to-device uncertainty of 0.5 m, allowing a rogue device capable of an instant turn-around to eavesdrop on communications and be up to 0.5 m farther away.

[0023] In addition to the round-trip time limitations, acoustic power levels can be kept to a minimum to reduce the probability of discrete interception. Note that a potential eavesdropping device located a large distance away must transmit loudly enough to be heard by the devices at that distance, and as such risks being detected by human ears that are in the vicinity. Embodiments of the present invention contemplate using any desired acoustic frequency, including audible frequencies as well as ultrasonic sound. However, if ultrasonic frequencies are used, ultrasonic transducers would likely be required rather than being able to utilize the existing audio transducers found in mobile phones. Using ultrasonic frequencies can reduce the likelihood of unauthorized human intercept.

[0024] By way of summary, FIG. 3 illustrates steps that can be performed in embodiments of the present invention. These steps include acoustically transmitting a device-dependent authentication key from a first device. The acoustic message bearing the device-dependent authentication key can then be received at a second device. The second device generates an acknowledgement message, which is transmitted acoustically and received back at the first device. A communications link can be established or rejected based on the time for round-trip acoustic communication, and therefore proximity of the devices.

[0025] Applications of embodiments of the present invention include: mobile ticketing in public transportation (e.g., ticket validation and fare collection terminals); mobile payment (the mobile phone acts as a debit/credit payment card); Bluetooth pairing; electronic ticketing; electronic money; travel cards; identity documents; mobile commerce; electronic keys (home, office, hotel). Embodiments of the present invention can be particularly suited for application with portable devices that may benefit from a low-cost means of out-of-band communication, for example to set up cryptographic keys, to enable secure transactions at point-of-sale, ticket validation, and the like.

[0026] The various embodiments described above and shown in the figures are provided by way of illustration only and should not be construed to limit the invention. Based on the above discussion and illustrations, those skilled in the art will readily recognize that various modifications and changes may be made to the present invention without strictly following the exemplary embodiments and applications illustrated and described herein. For instance, one or more of the above example embodiments may be implemented with a variety of approaches, including digital and/or analog circuitry and/or software-based approaches. The above example embodiments and implementations may also be integrated with a variety of circuits, devices, systems and approaches. Such modifications and changes do not depart from the true scope of the present invention that is set forth in the following claims.

What is claimed is:

1. A method for establishing a secure wireless communication link between first and second proximately-located devices, each of which includes respective audio transmitters and audio receivers, the method comprising:

using the audio transmitter of the first device to transmit a device-dependent authentication key;  
receiving the transmitted authentication key at the audio receiver of the second device, and using the audio transmitter of the second device to transmit an acknowledgement;  
receiving the acknowledgement at the audio receiver of the first device;  
determining the round-trip time from transmitting the authentication key from the first device to receiving the acknowledgement at the first device; and  
determining whether to establish the secure wireless communication link based on the determined round-trip time.

2. The method of claim 1, further comprising limiting the proximity of communications by rejecting any acknowledgement received at the first device after a threshold response time has elapsed from the time of transmitting the authentication key.

3. The method of claim 2, wherein the threshold response time corresponds to a distance between devices of 1 m or less.

4. The method of claim 1, wherein the second device transmits a further device-dependent authentication key that is received by the first device along with the acknowledgement.

5. The method of claim 4, further comprising transmitting a further acknowledgement from the first device in response to the further device-dependent authentication key, and receiving the further acknowledgement at the second device.

6. The method of claim 5, further comprising determining a further round-trip time from transmitting the further authentication key from the second device to receiving the further acknowledgement at the second device.

7. The method of claim 6, wherein the communication link is established only if the round-trip time determined at the first device sufficiently matches the further round-trip time determined at the second device.

8. The method of claim 1, wherein acoustic communications take place using an audible frequency range.

9. The method of claim 1, wherein acoustic communications take place using a frequency just outside of the audible range.

10. The method of claim 1, wherein acoustic communications take place using an ultrasonic frequency range.

11. The method of claim 1, wherein the secure communication link is used to exchange an encryption key used for further communications between the first and second devices.

12. A mobile communications device comprising:

an audio transmitter;

an audio receiver;

circuitry adapted to send audio data packets via the audio transmitter, receive audio data packets via the audio receiver, calculate round-trip times between sending audio data packets and receiving audio acknowledgements, and validate audio communications based on the calculated round-trip times.

13. The device of claim 12, wherein the audio transmitter is a speaker.

14. The device of claim 12, wherein the audio transmitter is a microphone.

15. The device of claim 12, wherein the device is a cell phone.

16. A method for use with a mobile communications device having an audio transmitter, an audio receiver, and a processor adapted to send audio data packets via the audio transmitter and receive audio data packets via the audio receiver, the method comprising adapting the mobile communications device to establish secure communication links by:

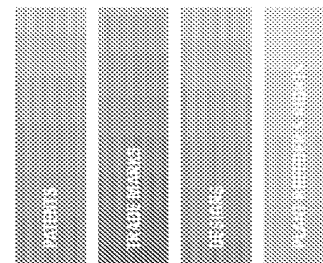
storing a program in a memory location of the mobile communications device, the program being executable by the processor to calculate round-trip times between sending audio data packets and receiving audio acknowledgements, and to validate audio communications based on the calculated round-trip times.

\* \* \* \* \*





**Australian Government**  
**IP Australia**



ABN 98 113 072 716

Discovery House, Phillip ACT 2606  
 PO Box 200, Woden ACT 2606  
 Australia

P 1300 851 010  
 +61 2 6283 2999 (International)  
 F +61 2 6283 7999  
 E assist@ipaustralia.gov.au  
 ipaustralia.gov.au

**Address:** Madderns Patent & Trade Mark Attorneys  
 GPO Box 2752  
 Adelaide SA 5001  
 Australia

**Date of issue:** 8 August 2012

## Innovation Patent Examination Report No. 2

### Application Details

**Patent Application No.:** 2012100462  
**Applicant(s):** Uniloc USA, Inc.  
**Applicant reference:** 40665 AAL:KR  
**Earliest Priority Date:** 06 February 2012  
**Examination Request Date:** 24 April 2012  
**Examination Requested By:** Madderns Patent & Trade Mark Attorneys  
**Third Party Reference** 40665 AAL:KR

Your application has been examined under Section 101B of the Patents Act 1990. I consider that the application does not meet the requirements of the Act for the reasons indicated below.

### Actions you can take

You have until 21 November 2012 to remove all grounds of revocation otherwise your Innovation Patent will cease.

### Basis of the report

Last proposed amendment item no. 2

In examining your application I have taken into account:

- the specification as filed
- the proposed amendments under S104 filed on 03 July 2012



*Robust intellectual property rights delivered efficiently*



This data, for application number 2012100462, is current as of 2012-12-28 22:09 AEST

## Statement of Novelty, Innovative Step and Patentable Subject Matter

<b>Novelty/Innovative Step</b>	Claim No. 1 - 5 Claim No. NONE	<b>Yes</b> <b>No</b>
<b>Patentable Subject Matter</b>	Claim No. 1 - 5 Claim No. NONE	<b>Yes</b> <b>No</b>

## Section 40 (Fair Basis, Full Description, Clarity, Lack of Unity)

- 2 Claim 1 is not clear because said claim is directed to "authentication of sources" but it is unclear how the method steps of claim 1 relate to authenticating said sources. From reading said claim it is unclear whether the method steps of claim 1 are performed by the sources to authenticate itself or performed by the audio transceiver computing device. It should also be noted that if the method steps of claim 1 are not performed by the sources then it is unclear as to how the method steps of claim 1 authenticate the sources. Applicant is requested to clarify the matter.

## Documents Cited or Considered Relevant

D6 : US 2010/0281261 A1 (RAZZELL) 04 November 2010 ^  
Category: A Claims: 1 - 5

^ Document provided by the applicant with the response of 3 July 2012 and listed as D6.

### Special categories of cited documents (based on PCT standard):

A: Document defining the general state of the art which is not considered to be of particular relevance.

## Other Issues

I apologise for any inconvenience resulting from your application not being considered within the time limit set out in our Customer Service Charter.


## How to contact us

<b>Examiner:</b>	Anish Singh Patent Examination B C3 - Electronics and Communications (02) 6283 7915	<b>Corporate Telephone</b>	1300 651 010 (9am-5pm Mon- Fri)
		<b>Fax:</b>	(02) 6283 7999
<b>Mail:</b>	IP Australia PO Box 200 Woden, ACT 2606	<b>Email:</b>	<a href="mailto:assist@ipaustralia.gov.au">assist@ipaustralia.gov.au</a>
		<b>Website:</b>	<a href="http://www.ipaustralia.gov.au">www.ipaustralia.gov.au</a>



Website QR code

View your application in AusPat by going to <http://www.ipaustralia.gov.au/auspat/> and entering your application number.

 Australian Government IP Australia		<b>Search Information Statement (SIS)</b>				
		<b>Application Number</b>	2012100462			
<b><u>A. Search Details</u></b>						
<b>Additional Members of the Search Team (if convened):</b>	T. Thanabalasingham, S. Kumar	<b>Earlier Search Results available</b>	Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
		<b>Current SIS Completion Date</b>	08 August 2012			
<b><u>B. Search Strategy</u></b>						

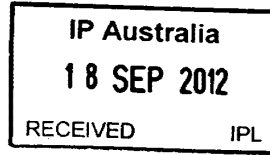
Databases : EPODOC, WPI

SS Results

- 1 67252 NEAR\_FIELD OR BLUETOOTH OR WI\_FI OR NFC
- 2 67252 ..LIM 1
- 3 354 (FREE OR UNUSED OR SENS+ OR SCAN+) 3D (FREQUENC+ OR BANDWIDTH)
- 4 354 ..LIM 3
- 5 134 BIOMETRIC OR IDENT+ OR FINGER\_PRINT+ OR AUTHENTICAT+ OR CERTIF+
- 6 268 CONTENT OR MESSAG+ OR INFORMATION OR DATA OR SIGNAL+ OR WAVE
- 7 107 5 AND 6

Results of search statement 7 were viewed.

[www.freepatentsonline.com](http://www.freepatentsonline.com): nfc, near field, bluetooth, free, unused, frequency, bandwidth, biometric, identity, identification, fingerprint, content, message, signal and similar terms.



Level 4, 19 Gouger Street  
Adelaide SA 5000 Australia  
GPO Box 2752  
Adelaide SA 5001 Australia  
Phone: +61 8 8311 8311  
Fax: +61 8 8311 8300  
mail@madderns.com.au  
www.madderns.com.au  
ABN: 98 056 210 140

18 September 2012

The Commissioner of Patents  
P O Box 200  
WODEN ACT 2606

MA SPEED DIAL 534

Dear Sir/Madam

**Australian Innovation Patent No 2012100462  
NEAR FIELD AUTHENTICATION THROUGH  
COMMUNICATION OF ENCLOSED CONTENT SOUND  
WAVES**

**Uniloc USA, Inc.**

**Examiner: Anish Singh**

Our Ref: 40665 AAL:JAL

We refer to the Examiner's Second Report dated 8 August 2012 and **enclose** amendments as set forth in the accompanying Schedule of Proposed Amendments.

Regarding item 2 the Report, Claim 1 has been amended to recite in relevant part "a method for near field authentication of a source, *the source* using an audio transceiver device". The claim then goes onto state the various steps of the invention. We respectfully submit that it would be immediately apparent to one of ordinary skill in the art that it is source that is authenticating itself using an audio transceiver computing device and request that the objection be withdrawn.

Favourable reconsideration of the application is respectfully requested.

Yours faithfully  
MADDERNS

ANTHONY LEE

Enc

**Partners**  
Craig Vinall  
BE (Mech)  
Bill McFarlane  
BSc (Physics) MIEAust  
Grad Dip ElecSys  
Tom Melville  
BE (Mech) MBA  
Alun Thomas  
BAppSc (App Chem)  
Notary Public  
Martin Pannall  
BE (Elec) (Hons)  
Mark O'Donnell  
BSc (Hons)  
Anthony Lee  
PhD LLB (Hons) CPEng  
Louise Emmett  
LLM LLB/LP (Hons) BA  
**Professionals**  
Megan Ryder  
LLB (Hons) GDLP BA  
Grad Dip IP Law  
(Senior Associate)  
Jeff Holman  
PhD BSc (Hons)  
(Senior Associate)  
Stephen O'Brien  
BE (Elec) (Hons)  
(Senior Associate)  
Stephen Worthley  
BSc LLB (Hons) MIP  
(Associate)  
Lucy Deane  
LLB (Hons) BA (Hons)  
(Associate)  
Phillip Boehm  
BE (Mech) (Hons) MIP  
(Associate)  
Irena Fizulic  
BBus (CommLaw)  
Grad Cert TMLP  
Karen Heilbronn Lee  
PhD BSc (Hons) MIP  
Christopher Wilkinson  
PhD BSc (Hons) MIP  
Kin Seong Leong  
PhD BE (Elec) (Hons) MIP  
**Professional Support**  
Nick McLeod  
BE (Mech) (Hons)  
BMA&CompSci  
Greg Maloney  
BE (Elec)  
Richard Catt  
1949 - 2007

2012100462 18 Sep 2012

**AUSTRALIA**

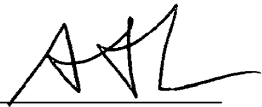
Patents Act 1990

**SECOND SCHEDULE OF PROPOSED AMENDMENTS**

**Agent Name:** MADDERNS Patent & Trade Mark Attorneys  
**Agent Address:** GPO Box 2752, Adelaide, South Australia, 5001, Australia  
**Agent Reference:** 40665 AAL:JAL  
**Application No:** 2012100462  
**Applicant:** Uniloc USA, Inc.  
**Report No:** 2  
**Report Date:** 8 August 2012

---

3. Cancel existing claim page 18 (claims 1 to 5) as currently on file and substitute in place thereof new claim page 18 (claims 1 to 5) as attached hereto.



Date: 18 September 2012

ANTHONY LEE  
MADDERNS

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for near field authentication of <sup>a</sup>source<sub>1</sub> using an audio transceiver computing <sup>the source</sup> <sub>2</sub> No  
device comprising:
  - scanning a plurality of predetermined frequencies for a free frequency;
  - selecting the free frequency from the plurality of predetermined frequencies;
  - generating a periodic enclosed content message;
  - generating a modulated carrier wave representing the periodic enclosed content message;and
  - transmitting the modulated carrier wave at the free frequency;
  - wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and
  - wherein the content includes at least one of biometric data, or device identification data.
  
2. The method of claim 1 further comprising:
  - displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and
  - responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.
  
3. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.
  
4. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.
  
5. The method of any one of claims 1 to 4 wherein the modulated carrier wave comprises a sound wave.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for near field authentication of a source, the source using an audio transceiver computing device comprising:
  - scanning a plurality of predetermined frequencies for a free frequency;
  - selecting the free frequency from the plurality of predetermined frequencies;
  - generating a periodic enclosed content message;
  - generating a modulated carrier wave representing the periodic enclosed content message; and
  - transmitting the modulated carrier wave at the free frequency;wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and  
wherein the content includes at least one of biometric data, or device identification data.
2. The method of claim 1 further comprising:
  - displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and
  - responsive to receiving the biometric data, generating the periodic enclosed content message,wherein the content in each period of the periodic enclosed content message includes the biometric data.
3. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.
4. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.
5. The method of any one of claims 1 to 4 wherein the modulated carrier wave comprises a sound wave.



Australian Government  
IP Australia

LETTERS PATENT

# INNOVATION PATENT CERTIFICATE OF EXAMINATION

I, Robyn Foster, the Commissioner of Patents,  
hereby certify that I have examined the complete specification relating to

## **Innovation Patent**

2012100462

granted to

Uniloc USA, Inc. of 2151 Michelson Drive, Suite 100, Irvine, California, 92612, United States of  
America

for the Innovation Patent titled

Near field authentication through communication of enclosed content sound waves

invented by Etchegoyen, Craig S.;

Harjanto, Dono and

Burdick, Sean D..

in accordance with the requirements of the Patents Act 1990 for examination and certification of  
an innovation patent and decided a ground for the revocation of the innovation patent has not  
been made out, or that any such ground has been removed.



Signed at  
Canberra in the Australian Capital Territory  
This 25<sup>th</sup> Day of October 2012

*RE Foster*  
Robyn Foster  
Commissioner of Patents

PATENTS ACT 1990



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appl. no.: 13/734,178

Conf. no. 3155

Applicant: Craig ETCHEGOYEN

Art Unit:

Filed: January 4, 2013

Examiner: (Not Yet Assigned)

Title: **NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED  
CONTENT SOUND WAVES**

**TRANSMITTAL LETTER AND APPLICANT REMARKS  
FOR PPH REQUEST**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir,

Applicant respectfully requests participation in the Patent Prosecution Highway (PPH) for the above-referenced patent application. The following documents are submitted herewith:

- 1) Request for Participation in the Patent Prosecution Highway (PPH) Pilot Program Between IP Australia (IPAU) and the USPTO [Form PTO/SB/20AU];
- 2) Copy of AU Innovation Patent No. 2012100462, which has identical claims to those submitted for the above-referenced patent application;
- 3) Copy of the IPAU Examiner's First Report and substantive examination dated May 21, 2012 for AU Innovation Patent No. 2012100462;
- 4) Copy of Applicant's response dated July 3, 2012 to the Examiner's First Report and substantive examination;
- 5) Copy of the IPAU Examiner's Second Report and substantive examination dated August 8, 2012 for AU Innovation Patent No. 2012100462;

13/734,178

1

- 6) Copy of Applicant's response dated September 18, 2012 to the Examiner's Second Report and substantive examination;
- 7) List of References (Form PTO/SB08) submitted with the referenced AU application and cited in the Second Examination Report.
- 8) Copy of the Certificate of Examination for Australian Innovation Patent AU 2012100462 dated October 25, 2012, indicating that all grounds for revocation of the patent have been removed.

In view of all of the above, Applicant respectfully requests that this application be accepted for examination along the Patent Prosecution Highway.

Respectfully Submitted,



Sean D. Burdick  
Reg. No. 51,513

Uniloc USA, Inc.  
Legacy Towne Center  
7160 N. Dallas Parkway  
Suite 380  
Plano, TX 75024  
972 905 9580 x227

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.

<b>REQUEST FOR PARTICIPATION IN THE PATENT PROSECUTION HIGHWAY (PPH) PILOT PROGRAM BETWEEN IP AUSTRALIA (IPAU) AND THE USPTO</b>			
Application No.:	13/734,178	Filing Date:	January 4, 2013
First Named Inventor:	Craig S. Etchegoyen		
Attorney Docket No.:	UN-NP-SC-085		
Title of the Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		
THIS REQUEST FOR PARTICIPATION IN THE PPH pilot PROGRAM ALONG WITH THE REQUIRED DOCUMENTS MUST BE SUBMITTED VIA EFS-WEB. INFORMATION REGARDING EFS-WEB IS AVAILABLE AT <a href="http://www.uspto.gov/ebc/efs_help.html">HTTP://WWW.USPTO.GOV/EBC/EFS_HELP.HTML</a> .			
<b>APPLICANT HEREBY REQUESTS PARTICIPATION IN THE PATENT PROSECUTION HIGHWAY (PPH) PILOT PROGRAM AND PETITIONS TO MAKE THE ABOVE-IDENTIFIED APPLICATION SPECIAL UNDER THE PPH PILOT PROGRAM.</b>			
The above-identified application (1) validly claims priority under 35 U.S.C. 119(a) and 37 CFR 1.55 to one or more corresponding IPAU application(s) or to a PCT application that does not contain any priority claim, or (2) is a national stage entry of a PCT application that does not contain any priority claim.			
The IPAU/PCT application number(s) is/are: AU2012100462			
The filing date of the IPAU/PCT application(s) is/are: April 24, 2012			
<b>I. List of Required Documents:</b>			
a. <b>A copy of all IPAU office actions which are relevant to patentability in the above-identified IPAU application(s)</b>			
<input checked="" type="checkbox"/> Is attached.			
b. <b>A copy of all claims which were determined to be patentable by IPAU in the above-identified IPAU application(s)</b>			
<input checked="" type="checkbox"/> Is attached.			
c. <b>(1) An information disclosure statement listing the documents cited in the IPAU office actions</b>			
<input checked="" type="checkbox"/> Is attached.			
<input type="checkbox"/> Has already been filed in the above-identified U.S. application on _____			
<b>(2) Copies of all documents (except for U.S. patents or U.S. patent application publications)</b>			
<input type="checkbox"/> Are attached.			
<input type="checkbox"/> Have already been filed in the above-identified U.S. application on _____			

[Page 1 of 2]

This collection of information is required by 35 U.S.C. 119, 37 CFR 1.55, and 37 CFR 1.102(d). 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 1.11 and 1.14. This collection is estimated to take 2 hours 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, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.



## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant ( *i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	14620245
<b>Application Number:</b>	13734178
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3155
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN
<b>Customer Number:</b>	96051
<b>Filer:</b>	Sean Dylan Burdick
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	UN-NP-SC-085
<b>Receipt Date:</b>	08-JAN-2013
<b>Filing Date:</b>	
<b>Time Stamp:</b>	13:13:17
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	SC-085_IDS_List.pdf	27301 <small>72b6f0969ef579f91c9dcaed07cfea12d4359885</small>	no	1

### Warnings:

### Information:

This is not an USPTO supplied IDS fillable form					
2	Miscellaneous Incoming Letter	AU_2012100462.pdf	3251218 01247499357161628895a3019e2859631a536bd9	no	29
<b>Warnings:</b>					
<b>Information:</b>					
3	Examination support document	AU_2012100462_Examination_Report_1.pdf	50743 96e73b6e72e21a0301f24c5c74435ed141c172bf	no	1
<b>Warnings:</b>					
<b>Information:</b>					
4	Miscellaneous Incoming Letter	AU_2012100462_Resp_Exam_Report_1.pdf	6557302 19b59f5d56ce880c19813081bbc4c090fa1549e	no	110
<b>Warnings:</b>					
<b>Information:</b>					
5	Examination support document	AU_2012100462_Examination_Report_2.pdf	403820 e4609ab261eedff6165c87688e5b400d554bb68bd	no	3
<b>Warnings:</b>					
<b>Information:</b>					
6	Miscellaneous Incoming Letter	AU_2012100462_Resp_Exam_Report_2.pdf	118388 5dc23d62e2b75282ae5853b984c735433d2f8675	no	4
<b>Warnings:</b>					
<b>Information:</b>					
7	Miscellaneous Incoming Letter	AU_2012100462_Patent_Certificate.pdf	2046705 e0b7ee3a7b2dde7f909369404eed6bce2f54d4b6	no	1
<b>Warnings:</b>					
<b>Information:</b>					
8	Transmittal Letter	UN-NP-SC-085_PPH_Transmittal_Form.pdf	33174 1214aec54d5639a24b8162960d74671009122e21	no	2
<b>Warnings:</b>					
<b>Information:</b>					
9	Petition to make special under Patent Prosecution Hwy	SC-085_sb0020au_fill.pdf	168083 e82372611f450c1c7e9c96007bd9b52e9e43cd0c	no	3
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			12656734		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number 13/734,178
---	--

APPLICATION AS FILED - PART I			SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	(Column 1)	(Column 2)					
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	98		N/A	
SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	7	minus 20 = *	x 31 =	0.00	OR		
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	1	minus 3 = *	x 125 =	0.00			
APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>				230			
			TOTAL	763		TOTAL	

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

APPLICATION AS AMENDED - PART II					SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	x	=	OR	x	=
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	x	=	OR	x	=
	Application Size Fee <small>(37 CFR 1.16(s))</small>						OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	x	=	OR	x	=
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	x	=	OR	x	=
	Application Size Fee <small>(37 CFR 1.16(s))</small>						OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L 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 found in the appropriate box in column 1.



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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/734,178, 01/04/2013, 2668, 533, UN-NP-SC-085, 5, 1

CONFIRMATION NO. 3155

FILING RECEIPT



96051
Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

Date Mailed: 02/05/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s)

Craig S. ETCHEGOYEN, Newport Beach, CA;
Dono HARJANTO, Irvine, CA;
Sean D. BURDICK, Dallas, TX;

Applicant(s)

UNILOC LUXEMBOURG S.A., Luxembourg, LUXEMBOURG

Assignment For Published Patent Application

UNILOC LUXEMBOURG S.A., Luxembourg, LUXEMBOURG

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/595,599 02/06/2012

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

AUSTRALIA 2012100462 04/24/2012

Permission to Access - A proper Authorization to Permit Access to Application by Participating Offices (PTO/SB/39 or its equivalent) has been received by the USPTO.

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to Retrieve Electronic Priority Application(s) (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

**If Required, Foreign Filing License Granted:** 01/31/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/734,178**

**Projected Publication Date:** 08/08/2013

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT  
SOUND WAVES

**Preliminary Class**

382

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



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

Table with 4 columns: APPLICATION NUMBER (13/734,178), FILING OR 371(C) DATE (01/04/2013), FIRST NAMED APPLICANT (Craig S. ETCHEGOYEN), ATTY. DOCKET NO./TITLE (UN-NP-SC-085)

CONFIRMATION NO. 3155

FORMALITIES LETTER



96051
Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

Date Mailed: 02/05/2013

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing.

Applicant is given TWO MONTHS from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of \$ 230 as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
• A surcharge (for late submission of the basic filing fee, search fee, examination fee or inventor's oath or declaration) as set forth in 37 CFR 1.16(f) of \$ 65 for a small entity in compliance with 37 CFR 1.27, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within TWO MONTHS from the date of this Notice is \$ 295 for a small entity

- \$ 65 Surcharge.
• Total additional claim fee(s) for this application is \$ 230
• \$ 230 for multiple dependent claim surcharge.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
All
Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.

<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

*/aabranos/*

---

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

<b>MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET</b>  Substitute for Form PTO-1360 (For use with Form PTO/SB/06)	Application Number <b>13734178</b>	Filing Date
Applicant(s) <b>Craig ETCHEGOYEN</b>		

\* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT		*	*	*
	Indep	Depend	Indep	Depend	Indep	Depend			

1	1								
2		1							
3		2							
4		2							
5		(1)							
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									
Total Indep	1		0		0				
Total Depend	6	↙	0	↙	0	↙			
Total Claims	7		0		0				

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									

UNITED STATES PATENT AND TRADEMARK OFFICE  
COMMISSIONER FOR PATENTS  
P.O. BOX 1450  
ALEXANDRIA VA 22313-1451

PRESORTED  
FIRST-CLASS MAIL  
U.S. POSTAGE PAID  
POSTEDIGITAL  
NNNNN

Uniloc USA Inc.  
Legacy Town Center  
7160 Dallas Parkway  
Suite 380  
Plano, TX 75024



**Courtesy Reminder for  
Application Serial No: 13/734,178**

Attorney Docket No: UN-NP-SC-085  
Customer Number: 96051  
Date of Electronic Notification: 02/05/2013

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

sean.burdick@unilocusa.com  
amanda.ivey@unilocusa.com  
lfrancis@unilocusa.com

To view your correspondence online or update your email addresses, please visit us anytime at <https://sportal.uspto.gov/secure/myportal/privatepair>. If you have any questions, please email the Electronic Business Center (EBC) at [EBC@uspto.gov](mailto:EBC@uspto.gov) or call 1-866-217-9197.



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appl. no.:	13/734,178	Conf. no.	3155
Inventor:	Craig S. ETCHEGOYEN	Art Unit:	2668
Filed:	January 4, 2013	Examiner:	not yet assigned
Title:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		

**PRELIMINARY AMENDMENT  
IN RESPONSE TO NOTICE TO FILE MISSING PARTS**

Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir,

In response to the Notice to File Missing Parts mailed February 5, 2013, please amend the present application as follows:

**Amendments to the Claims** are shown on page 2.

**Remarks** begin on page 4.

## CLAIMS

What is claimed is:

1. (original) A method for near field authentication of a source the source using an audio transceiver computing device comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message;

and

transmitting the modulated carrier wave at the free frequency.

2. (original) The method of claim 1 further comprising

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (currently amended) The method of claim 1 ~~or 2~~, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. (currently amended) The method of claim 1 ~~or 2~~, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (currently amended) The method of claim 1 ~~to~~4 wherein the modulated carrier wave comprises a sound wave.
6. (new) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.
7. (new) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.
8. (new) The method of claim 4 wherein the modulated carrier wave comprises a sound wave.

**REMARKS**

The Notice to File Missing Parts identified a fee deficiency arising from applicant's omission of the \$230 multiple dependent claim fee applicable to claims 3, 4, and 5.

In response, applicant submits herewith a Preliminary Amendment that divides multiple-dependent claim 4 into three separate dependent claims. There are now seven total claims – two independent and five dependent, with no multiple dependent claims. Applicant believes that the \$533 filing fee is sufficient for the current set of claims.

Applicant respectfully requests entry of the Preliminary Amendment, withdrawal of the Notice to File Missing Parts, and approval of the PPH request.

Respectfully Submitted,



Sean D. Burdick  
Reg. No. 51,513

Uniloc USA, Inc.  
7160 N. Dallas Parkway, Suite 380  
Plano, TX 75024  
(972) 905-9580 x227

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13734178			
<b>Filing Date:</b>	04-Jan-2013			
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES			
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN			
<b>Filer:</b>	Sean Dylan Burdick/Amanda Ivey			
<b>Attorney Docket Number:</b>	UN-NP-SC-085			
Filed as Small Entity				
<b>Utility under 35 USC 111(a) Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
Late Filing Fee for Oath or Declaration	2051	1	70	70
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>70</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15331531
<b>Application Number:</b>	13734178
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3155
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN
<b>Customer Number:</b>	96051
<b>Filer:</b>	Sean Dylan Burdick/Amanda Ivey
<b>Filer Authorized By:</b>	Sean Dylan Burdick
<b>Attorney Docket Number:</b>	UN-NP-SC-085
<b>Receipt Date:</b>	22-MAR-2013
<b>Filing Date:</b>	04-JAN-2013
<b>Time Stamp:</b>	13:54:59
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$70
RAM confirmation Number	162
Deposit Account	506053
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

<b>File Listing:</b>					
<b>Document Number</b>	<b>Document Description</b>	<b>File Name</b>	<b>File Size(Bytes)/ Message Digest</b>	<b>Multi Part /.zip</b>	<b>Pages (if appl.)</b>
1	Preliminary Amendment	UN-NP-SC-085_Preliminary_Amendme nt.pdf	33382 cae7bfe6e55801623b34a73d53838e2c21fae20c	no	4
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (SB06)	fee-info.pdf	30361 00f1d6973e0368e76c89335922a6a949c76fec7f	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			63743		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					



**PATENT ASSIGNMENT**

Electronic Version v1.1  
 Stylesheet Version v1.1

<b>SUBMISSION TYPE:</b>	NEW ASSIGNMENT
<b>NATURE OF CONVEYANCE:</b>	ASSIGNMENT
<b>CONVEYING PARTY DATA</b>	
<b>Name</b>	<b>Execution Date</b>
Craig S. ETCHEGOYEN	01/15/2013
Dono Harjanto	03/04/2013
Sean D. Burdick	03/16/2013
<b>RECEIVING PARTY DATA</b>	
<b>Name:</b>	UNILOC LUXEMBOURG S.A.
<b>Street Address:</b>	15, Rue Edward Steichen
<b>City:</b>	Luxembourg
<b>State/Country:</b>	LUXEMBOURG
<b>Postal Code:</b>	L-2450
<b>PROPERTY NUMBERS Total: 1</b>	
<b>Property Type</b>	<b>Number</b>
<b>Application Number:</b>	13734178
<b>CORRESPONDENCE DATA</b>	
<b>Fax Number:</b> <i>Correspondence will be sent via US Mail when the fax attempt is unsuccessful.</i>	
<b>Email:</b>	amanda.ivey@unilocusa.com
<b>Correspondent Name:</b>	Amanda Ivey
<b>Address Line 1:</b>	7160 Dallas Parkway
<b>Address Line 2:</b>	Suite 380
<b>Address Line 4:</b>	Plano, TEXAS 75024
<b>ATTORNEY DOCKET NUMBER:</b>	UN-NP-SC-085
<b>NAME OF SUBMITTER:</b>	Amanda Ivey
<b>Signature:</b>	/Amanda Ivey/
<b>Date:</b>	04/03/2013

CH \$40.00 13734178

This document serves as an Oath/Declaration (37 CFR 1.63).

**Total Attachments: 4**

source=SC-085\_Executed\_Assign\_Decl\_Craig#page1.tif

source=SC-085\_Executed\_Assign\_Decl\_Craig#page2.tif

source=SC-085\_Executed\_Assign\_Decl\_Dono\_Seal#page1.tif

source=SC-085\_Executed\_Assign\_Decl\_Dono\_Seal#page2.tif

## Combined Declaration and Assignment for Utility Patent and Design Patent Applications

### DECLARATION

As a below named inventor, I hereby declare that:

I believe I am the original inventor or an original joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

Insert Title:

NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT  
SOUND WAVES

the application of which is attached hereto unless the following is checked

was filed on January 4, 2013 as United States Application Number 13/734,178 and was amended on \_\_\_\_\_ (if applicable).

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this declaration is punishable under section 1001 of title 18 by fine or imprisonment of not more than 5 years, or both.

### ASSIGNMENT

FOR GOOD AND VALUABLE CONSIDERATION, the adequacy and receipt of which is hereby acknowledged by the undersigned inventor(s) (hereinafter ASSIGNOR) by

Insert Assignee(s)  
Name/Address:

UNILOC LUXEMBOURG S.A.  
15, Rue Edward Steichen, L-2450  
Luxembourg, Grand-Duchy of Luxembourg

(hereinafter ASSIGNEE), the undersigned ASSIGNOR hereby sells, assigns and transfers to ASSIGNEE the entire and exclusive right, title and interest to the above-identified application (e.g., provisional or non-provisional) and all Letters Patent of the United States to be obtained therefore on said application or any continuation, divisional, substitute, reissue, reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof for the full term or terms for which the same may be granted.

The ASSIGNOR agrees to execute all papers necessary in connection with the application and any continuation, divisional, reissue, reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof and also to execute separate assignments in connection with such applications as the ASSIGNEE may deem necessary or expedient.

The ASSIGNOR agrees to execute all papers necessary in connection with any interference, litigation, or other legal proceeding which may be declared concerning this application or any continuation, divisional, reissue or reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof or Letters Patent or reissue patent issued thereon and to cooperate with the ASSIGNEE in every way possible in obtaining and producing evidence and proceeding with such interference, litigation, or other legal proceeding.

The ASSIGNOR sells, assigns and transfers to said ASSIGNEE the entire and exclusive right, title and interest to the application(s) and the invention(s) disclosed therein for the United States of America and all countries foreign to the United States and do hereby authorize said ASSIGNEE to apply for patents therefore in its own name in countries where such procedure is proper and to claim the priority right under the International Convention and agrees to execute all papers

necessary in connection with applications for such patents and any continuation, divisional, substitute, reissue or reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof and also execute separate assignments in connection with such applications as the ASSIGNEE may deem necessary or expedient.

Hereby executed by the undersigned on the date opposite the undersigned name:

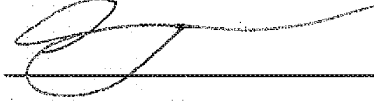
Legal Name  
of inventor ⇨

Craig S. ETCHEGOYEN

Date:

1-15-13

Inventor's  
Signature ⇨



## Combined Declaration and Assignment for Utility Patent and Design Patent Applications

### DECLARATION

As a below named inventor, I hereby declare that:

I believe I am the original inventor or an original joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

Insert Title:

NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT  
SOUND WAVES

the application of which is attached hereto unless the following is checked

was filed on **January 4, 2013** as United States Application Number **13/734,178** and was amended on \_\_\_\_\_ (if applicable).

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this declaration is punishable under section 1001 of title 18 by fine or imprisonment of not more than 5 years, or both.

### ASSIGNMENT

FOR GOOD AND VALUABLE CONSIDERATION, the adequacy and receipt of which is hereby acknowledged by the undersigned inventor(s) (hereinafter ASSIGNOR) by

Insert Assignee(s)  
Name/Address:

UNILOC LUXEMBOURG S.A.  
15, Rue Edward Steichen, L-2450  
Luxembourg, Grand-Duchy of Luxembourg

(hereinafter ASSIGNEE), the undersigned ASSIGNOR hereby sells, assigns and transfers to ASSIGNEE the entire and exclusive right, title and interest to the above-identified application (e.g., provisional or non-provisional) and all Letters Patent of the United States to be obtained therefore on said application or any continuation, divisional, substitute, reissue, reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof for the full term or terms for which the same may be granted.

The ASSIGNOR agrees to execute all papers necessary in connection with the application and any continuation, divisional, reissue, reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof and also to execute separate assignments in connection with such applications as the ASSIGNEE may deem necessary or expedient.

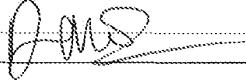
The ASSIGNOR agrees to execute all papers necessary in connection with any interference, litigation, or other legal proceeding which may be declared concerning this application or any continuation, divisional, reissue or reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof or Letters Patent or reissue patent issued thereon and to cooperate with the ASSIGNEE in every way possible in obtaining and producing evidence and proceeding with such interference, litigation, or other legal proceeding.

The ASSIGNOR sells, assigns and transfers to said ASSIGNEE the entire and exclusive right, title and interest to the application(s) and the invention(s) disclosed therein for the United States of America and all countries foreign to the United States and do hereby authorize said ASSIGNEE to apply for patents therefore in its own name in countries where such procedure is proper and to claim the priority right under the International Convention and agrees to execute all papers

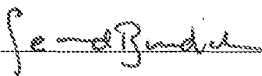
necessary in connection with applications for such patents and any continuation, divisional, substitute, reissue or reexamination, supplemental examination, inter partes review, post grant review, or other procedures thereof and also execute separate assignments in connection with such applications as the ASSIGNEE may deem necessary or expedient.

Hereby executed by the undersigned on the date opposite the undersigned name:

Legal Name of inventor ⇨ Dono HARJANTO Date: 03/04/2013

Inventor's Signature ⇨ 

Legal Name of inventor ⇨ Sean D. BURDICK Date: 3/6/13

Inventor's Signature ⇨ 



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	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085

**CONFIRMATION NO. 3155**

96051  
Uniloc USA Inc.  
Legacy Town Center  
7160 Dallas Parkway  
Suite 380  
Plano, TX 75024

**NOTICE**



Date Mailed: 04/05/2013

**INFORMATIONAL NOTICE TO APPLICANT**

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):  
all  
Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number 13/734,178
---	--

APPLICATION AS FILED - PART I			SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	(Column 1)	(Column 2)					
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	70		N/A	
SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	8	minus 20 = *	x 40 =	0.00	OR		
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	1	minus 3 = *	x 210 =	0.00			
APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II					SMALL ENTITY		OR	OTHER THAN SMALL ENTITY		
	(Column 1)	(Column 2)	(Column 3)							
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)		
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	x	=	OR	x	=
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee <small>(37 CFR 1.16(s))</small>									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>									
				TOTAL ADD'L FEE		TOTAL ADD'L FEE				
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)		
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	x	=	OR	x	=
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee <small>(37 CFR 1.16(s))</small>									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>									
				TOTAL ADD'L FEE		TOTAL ADD'L FEE				
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.</p>										





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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/734,178, 01/04/2013, 2668, 603, UN-NP-SC-085, 8, 1

CONFIRMATION NO. 3155

UPDATED FILING RECEIPT



OC000000060182441

96051
Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

Date Mailed: 04/05/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s)

Craig S. ETCHEGOYEN, Newport Beach, CA;
Dono HARJANTO, Irvine, CA;
Sean D. BURDICK, Dallas, TX;

Applicant(s)

UNILOC LUXEMBOURG S.A., Luxembourg, LUXEMBOURG

Assignment For Published Patent Application

UNILOC LUXEMBOURG S.A., Luxembourg, LUXEMBOURG

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/595,599 02/06/2012

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

AUSTRALIA 2012100462 04/24/2012 No Access Code Provided

Permission to Access - A proper Authorization to Permit Access to Application by Participating Offices (PTO/SB/39 or its equivalent) has been received by the USPTO.

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to Retrieve Electronic Priority Application(s) (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

**If Required, Foreign Filing License Granted:** 01/31/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/734,178**

**Projected Publication Date:** 08/08/2013

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT  
SOUND WAVES

**Preliminary Class**

382

**Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:**

### **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

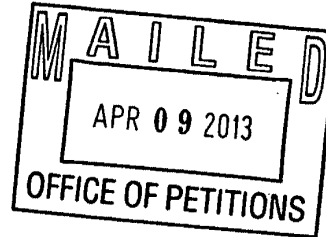
---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNILOC USA, INC.  
LEGACY TOWN CENTER  
7160 DALLAS PARKWAY  
SUITE 380  
PLANO, TX 75024



In re Application of  
Craig S. Etchegoyen, et al.  
Application No.: 13/734,178  
Filed: 04 January 2013  
Attorney Docket No.: UN-NP-SC-085  
For: NEAR FIELD AUTHENTICATION  
THROUGH COMMUNICATION OF  
ENCLOSED CONTENT SOUND  
WAVES

: DECISION ON REQUEST TO  
: PARTICIPATE IN THE PATENT  
: PROSECUTION HIGHWAY  
: PROGRAM AND PETITION  
: TO MAKE SPECIAL UNDER  
: 37 CFR 1.102(a)

This is a decision on the request to participate in the Patent Prosecution Highway (PPH) pilot program and the petition under 37 CFR 1.102(a), filed 08 January 2013, to make the above-identified application special.

The request and petition are **DISMISSED**.

#### DISCUSSION

A grantable request to participate in the PPH program and petition to make special require:

1. The U.S. application must validly claim priority under 35 U.S.C. 119(a) to one or more applications filed in the IPAU, note where the IPAU application with similar claims is not the same application from which the U.S. application claims priority then the applicant must identify the relationship between the IPAU application with similar claims and the IPAU priority application;
2. Applicant must submit a copy of:
  - a. The allowable/patentable claim(s) from the IPAU application(s) or if a copy of the allowable/patentable claims is available via the Dossier Access System (DAS) applicant may request the USPTO obtain a copy from the DAS, however if the USPTO is unable to obtain a copy from the DAS the applicant will be required to submit a copy;

- b. An English translation of the allowable/patentable claim(s) and
  - c. A statement that the English translation is accurate;
3. Applicant must
    - a. Ensure all the claims in the U.S. application must sufficiently correspond or be amended to sufficiently correspond to the allowable/patentable claim(s) in the IPAU application(s) and
    - b. Submit a claims correspondence table in English;
  4. Examination of the U.S. application has not begun;
  5. Applicant must submit:
    - a. Documentation of prior office action:
      - i. a copy of the office action(s) just prior to the "Decision to Grant a Patent" from each of the IPAU application(s) containing the allowable/patentable claim(s) or
      - ii. if the allowable/patentable claims(s) are from a "Notification of Reasons for Refusal" then the Notification of Reasons for Refusal or
      - iii. if the IPAU application is a first action allowance then no office action from the IPAU is necessary should be indicated on the request/petition form;Further, if a copy of the documents from a or b above is available via the Dossier Access System (DAS) applicant may request the USPTO obtain a copy from the DAS, however if the USPTO is unable to obtain a copy from the DAS the applicant will be required to submit a copy;
    - b. An English language translation of the IPAU Office action from (5)(a)(i)-(ii) above
    - c. A statement that the English translation is accurate;
  6. Applicant must submit:
    - a. An IDS listing the documents cited by the IPAU examiner in the IPAU office action (unless already submitted in this application)
    - b. Copies of the documents except U.S. patents or U.S. patent application publications (unless already submitted in this application);

Conditions (1-2) and (4-6) above are considered to have been met. However, the request to participate in the PPH pilot program and petition fails meet condition (3).

Regarding the requirement of condition (3), applicant has failed to ensure that all the claims filed in the preliminary amendment filed in the US application sufficiently correspond to the filed in the foreign application.

Applicant is given **ONE** opportunity within a time period of **ONE MONTH or THIRTY DAYS**, whichever is longer, from the mailing date of this decision to correct the deficiencies. **NO EXTENSION OF TIME UNDER 37 CFR 1.136 IS PERMITTED.** If the deficiencies are not corrected with the time period given, the application will await action in its regular turn.

Response must be filed via the Electronic Filing System (EFS) using the document description: Petition to make special under Patent Pros Hwy. Any preliminary amendments and IDS submitted with the PPH documents must be separately indexed as a preliminary amendment and IDS, respectively.

Telephone inquiries concerning this decision should be directed to April M. Wise at (571) 272-1642.

All other inquiries concerning the examination or status of the application is accessible in the PAIR system at <http://www.uspto.gov/ebc/index.html>.

/dab/  
David Bucci  
Petitions Examiner  
Office of Petitions

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.

<b>REQUEST FOR PARTICIPATION IN THE PATENT PROSECUTION HIGHWAY (PPH) PILOT PROGRAM BETWEEN IP AUSTRALIA (IPAU) AND THE USPTO</b>			
Application No.:	13/734,178	Filing Date:	January 4, 2013
First Named Inventor:	Craig S. Etchegoyen		
Attorney Docket No.:	UN-NP-SC-085		
Title of the Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES		
THIS REQUEST FOR PARTICIPATION IN THE PPH pilot PROGRAM ALONG WITH THE REQUIRED DOCUMENTS MUST BE SUBMITTED VIA EFS-WEB. INFORMATION REGARDING EFS-WEB IS AVAILABLE AT <a href="http://www.uspto.gov/EBC/EFS_HELP.HTML">HTTP://WWW.USPTO.GOV/EBC/EFS_HELP.HTML</a> .			
<b>APPLICANT HEREBY REQUESTS PARTICIPATION IN THE PATENT PROSECUTION HIGHWAY (PPH) PILOT PROGRAM AND PETITIONS TO MAKE THE ABOVE-IDENTIFIED APPLICATION SPECIAL UNDER THE PPH PILOT PROGRAM.</b>			
The above-identified application (1) validly claims priority under 35 U.S.C. 119(a) and 37 CFR 1.55 to one or more corresponding IPAU application(s) or to a PCT application that does not contain any priority claim, or (2) is a national stage entry of a PCT application that does not contain any priority claim.			
The IPAU/PCT application number(s) is/are: AU2012100462			
The filing date of the IPAU/PCT application(s) is/are: April 24, 2012			
<b>I. List of Required Documents:</b>			
a. <b>A copy of all IPAU office actions which are relevant to patentability in the above-identified IPAU application(s)</b>			
<input checked="" type="checkbox"/> Is attached.			
b. <b>A copy of all claims which were determined to be patentable by IPAU in the above-identified IPAU application(s)</b>			
<input checked="" type="checkbox"/> Is attached.			
c. <b>(1) An information disclosure statement listing the documents cited in the IPAU office actions</b>			
<input checked="" type="checkbox"/> Is attached.			
<input type="checkbox"/> Has already been filed in the above-identified U.S. application on _____			
<b>(2) Copies of all documents (except for U.S. patents or U.S. patent application publications)</b>			
<input type="checkbox"/> Are attached.			
<input type="checkbox"/> Have already been filed in the above-identified U.S. application on _____			

[Page 1 of 2]

This collection of information is required by 35 U.S.C. 119, 37 CFR 1.55, and 37 CFR 1.102(d). 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 1.11 and 1.14. This collection is estimated to take 2 hours 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, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.





## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant ( *i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15724387
<b>Application Number:</b>	13734178
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3155
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN
<b>Customer Number:</b>	96051
<b>Filer:</b>	Sean Dylan Burdick/Amanda Ivey
<b>Filer Authorized By:</b>	Sean Dylan Burdick
<b>Attorney Docket Number:</b>	UN-NP-SC-085
<b>Receipt Date:</b>	09-MAY-2013
<b>Filing Date:</b>	04-JAN-2013
<b>Time Stamp:</b>	08:42:30
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	SC-085_Request_Reconsideration.pdf	33112 <small>7b02eeda3a050d005aef1d57fdc038d9c8d dfaeb</small>	no	2

### Warnings:

### Information:

2	Petition to make special under Patent Prosecution Hwy	SC-085_sb0020au.pdf	1017560 <small>b5e0ead83d695ee366f5259d5c302e99195846ca</small>	no	3
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				1050672	
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appl. no.: 13/734,178

Conf. no. 3155

Applicant: Craig S. Etchegoyen

Art Unit: 2649

Filed: January 4, 2013

Examiner: Not Yet Assigned

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF  
ENCLOSED CONTENT SOUND WAVES

**REQUEST FOR RECONSIDERATION OF PETITION TO MAKE SPECIAL UNDER  
THE PATENT PROSECUTION HIGHWAY PILOT PROGRAM**

Mail Stop Petition  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir,

Applicant submits this Request in response to the DECISION ON REQUEST TO PARTICIPATE IN PATENT PROSECUTION HIGHWAY PROGRAM AND PETITION TO MAKE SPECIAL, mailed April 9, 2013, dismissing applicant's Request to participate in the Patent Prosecution Highway (PPH) pilot program.

Applicant requests reconsideration of the PPH Request in view of the remarks herein.

**REMARKS**

On January 8, 2013, Applicant complied with every requirement for a grantable request to participate in the PPH program as set forth in 1329 OG 165 "Patent Prosecution Highway Program between the United States Patent and Trademark Office and IP Australia", with the exception of Requirement 3(a) Ensure all in the U.S. application must sufficiently correspond or be amended to sufficiently correspond to the allowable/patentable claim(s) in the IPAU application(s).

Applicant has since corrected this deficiency by submitting a corrected "Request for Participation In The Patent Prosecution Highway (PPH) Pilot Program Between IP Australia and the USPTO" (Form PTO/SB/20AU). The correction is on II. Claims Correspondence Table, indicating the correct claims under Claims in US Application.

Applicant believes that all grounds for participation in the PPH have now been met, and respectfully requests that the Request be reconsidered and granted.

Respectfully Submitted,



Sean D. Burdick

Reg. No. 51,513

Uniloc USA, Inc.  
7160 N. Dallas Parkway, Suite 380  
Plano, TX 75024  
(972) 905-9580 x227



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

Table with 4 columns: APPLICATION NUMBER (13/734,178), FILING OR 371(C) DATE (01/04/2013), FIRST NAMED APPLICANT (Craig S. ETCHEGOYEN), ATTY. DOCKET NO./TITLE (UN-NP-SC-085)

CONFIRMATION NO. 3155

96051
Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

PUBLICATION NOTICE



Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

Publication No. US-2013-0203350-A1
Publication Date: 08/08/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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.

**POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO**

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

Practitioners associated with Customer Number:

96051

**OR**

Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

The address associated with Customer Number:

**OR**

<input type="checkbox"/>	Firm or Individual Name			
	Address			
	City	State	Zip	
	Country			
	Telephone	Email		

Assignee Name and Address: Uniloc Luxembourg S.A.  
75, Boulevard Grande Duchesse Charlotte  
Luxembourg, Luxembourg L-1331**A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.****SIGNATURE of Assignee of Record**

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	/Alexander H. Good/	Date	06-13-2013
Name	Alexander H. Good	Telephone	
Title	Director A		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 1.11 and 1.14. This collection is estimated to take 3 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, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



**GENERAL POWER OF ATTORNEY TO PROSECUTE PATENT APPLICATIONS**

The undersigned representative(s) of Uniloc Luxembourg S.A., a public limited liability company (*société anonyme*), incorporated under the laws of the Grand Duchy of Luxembourg, with registered office at 75, bld Grande Duchesse Charlotte, L-1331 Luxembourg, Grand Duchy of Luxembourg and registered with the Luxembourg Register of Commerce and Companies (R.C.S. Luxembourg) under number B 159.161 ("Uniloc Luxembourg S.A."), for and on behalf of Uniloc Luxembourg S.A. and not in their individual capacities, hereby appoint:

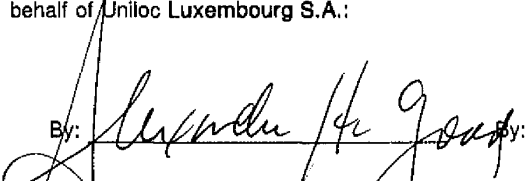
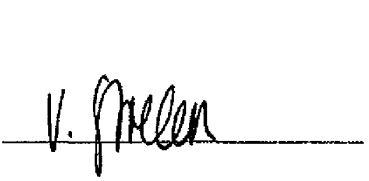
Uniloc USA, Inc.

as Uniloc Luxembourg S.A.'s agent authorized to represent Uniloc Luxembourg S.A. in a capacity limited to representation before the United States Patent and Trademark Office (USPTO) in connection with the prosecution or management of any and all patent applications, reexamination proceedings, and related matters involving any patent properties that are owned by or assigned to Uniloc Luxembourg S.A.

This Power of Attorney further authorizes the appointed agent to engage, on behalf of Uniloc Luxembourg S.A., other patent attorneys, patent agents, or patent prosecution firms, located throughout the world, in a capacity limited to the representation of Uniloc Luxembourg S.A. before the USPTO in connection with the prosecution or management of any patent applications, reexamination proceedings, and related matters involving any patent properties that are owned by or assigned to Uniloc Luxembourg S.A. during the term of this General Power of Attorney to Prosecute Patent Applications.

**SIGNATURE OF UNILOC LUXEMBOURG S.A.**

The individuals whose signatures and titles are shown below are authorized to act on behalf of Uniloc Luxembourg S.A.:

By: 	By: 
Name: <u>Alexander H. Good</u>	Name: <u>Virginia Strelan</u>
Title: <u>Director A</u>	Title: <u>Director B</u>
Date: <u>June 17, 2013</u>	Date: <u>June 11, 2013</u>

**STATEMENT UNDER 37 CFR 3.73(c)**Applicant/Patent Owner: Uniloc Luxembourg, S. A.Application No./Patent No.: 13/734,178 Filed/Issue Date: January 4, 2013Titled: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVEUniloc Luxembourg, S. A., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1.  The assignee of the entire right, title, and interest.
2.  An assignee of less than the entire right, title, and interest (check applicable box):
- The extent (by percentage) of its ownership interest is \_\_\_\_\_%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3.  The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4.  The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A.  An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 030140, Frame 0048, or for which a copy thereof is attached.

- B.  A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at

Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

2. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at

Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). 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 1.11 and 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, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**STATEMENT UNDER 37 CFR 3.73(c)**

3. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

4. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

5. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

6. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

Additional documents in the chain of title are listed on a supplemental sheet(s).

As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Alexander H. Good/

Signature

Alexander H. Good

Printed or Typed Name

August 8, 2013

Date

Director A

Title or Registration Number

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	16532600
<b>Application Number:</b>	13734178
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3155
<b>Title of Invention:</b>	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
<b>First Named Inventor/Applicant Name:</b>	Craig S. ETCHEGOYEN
<b>Customer Number:</b>	96051
<b>Filer:</b>	Sean Dylan Burdick/Amanda Ivey
<b>Filer Authorized By:</b>	Sean Dylan Burdick
<b>Attorney Docket Number:</b>	UN-NP-SC-085
<b>Receipt Date:</b>	08-AUG-2013
<b>Filing Date:</b>	04-JAN-2013
<b>Time Stamp:</b>	09:56:46
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	aia0080.pdf	80103 <small>c4003d74ddada97b1b7e429a69e7810140f21fb6</small>	no	2

### Warnings:

### Information:

2	Power of Attorney	Lux_General_POA_USPTO.pdf	27704 e2845b0b7215d2d03e0c1bcc34d8526b7f37c327	no	1
<b>Warnings:</b>					
<b>Information:</b>					
3	Assignee showing of ownership per 37 CFR 3.73.	SC-085_aia0096.pdf	118153 d112790ae8548939296f49042e79e2f4be600259	no	3
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				225960	
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO (modified by Applicant)  <b>INFORMATION DISCLOSURE          STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>				<b>Complete if Known</b>		
				Application Number	13/734,178	
				Filing Date	January 4, 2013	
				First Named Inventor	Craig S. ETCHEGOYEN	
				Art Unit	2649	
				Examiner Name	Yuwen Pan	
Sheet	1	of	5	Attorney Docket Number	UN-NP-SC-085	

U. S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code <small>(if known)</small>			
		US-4,200,770	04/29/1980	Hellman et al.	
		US-4,218,582	08/19/1980	Hellman et al.	
		US-4,323,921	04/06/1982	Guillou	
		US-4,337,483	06/29/1982	Guillou	
		US-4,405,829	09/20/1983	Rivest et al.	
		US-4,450,535	05/22/1984	de Pommery et al.	
		US-4,633,036	12/30/1986	Hellman et al.	
		US-4,652,990	03/24/1987	Pailen et al.	
		US-4,672,572	06/09/1987	Alsberg, Peter	
		US-4,747,139	05/24/1988	Taafe, James L.	
		US-4,868,877	09/19/1989	Fischer, Addison M.	
		US-4,977,594	12/11/1990	Shear, Victor H.	
		US-5,005,200	04/02/1991	Fischer, Addison M.	
		US-5,048,085	09/10/1991	Abraham et al.	
		US-5,050,213	09/17/1991	Shear, Victor H.	
		US-5,123,045	06/16/1992	Ostrovsky et al.	
		US-5,144,667	09/01/1992	Pogue, Jr. et al.	
		US-5,148,481	09/15/1992	Abraham et al.	
		US-5,155,680	10/13/1992	Wiedemer, John D.	
		US-5,162,638	11/10/1992	Diehl et al.	
		US-5,191,611	03/02/1993	Lang, Gerald s.	
		US-5,204,901	04/20/1993	Hershey et al.	
		US-5,231,668	07/27/1993	Kravitz, David W.	
		US-5,349,643	09/20/1994	Cox et al.	
Examiner Signature				Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute for form 1449/PTO (modified by Applicant)  <b>INFORMATION DISCLOSURE          STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>				<b>Complete if Known</b>		
				Application Number	13/734,178	
				Filing Date	January 4, 2013	
				First Named Inventor	Craig S. ETCHEGOYEN	
				Art Unit	2649	
				Examiner Name	Yuwen Pan	
Sheet	2	of	5	Attorney Docket Number	UN-NP-SC-085	

U. S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code <small>(if known)</small>			
		US-5,418,854	05/03/1995	Kaufman et al.	
		US-5,606,614	02/25/1997	Brady et al.	
		US-6,098,053	08/01/2000	Slater, Alan	
		US-6,163,843	12/09/2000	Inoue et al.	
		US-6,681,017	01/20/2004	Matias et al.	
		US-6,880,079	04/12/2005	Kefford et al.	
		US-7,032,110	04/18/2006	Su et al.	
		US-7,032,242	04/18/2006	Grabelsky et al.	
		US-7,310,813	12/18/2007	Lin et al.	
		US-7,444,508	10/28/2008	Karjala et al.	
		US-7,506,056	03/17/2009	Satish et al.	
		US-7,599,303	10/06/2009	Nadeau et al.	
		US-7,739,401	06/15/2010	Goyal, Pawan	
		US-7,739,402	06/15/2010	John Roesse	
		US-7,852,861	12/14/2010	Wu et al.	
		US-2002/0010864	01/24/2002	Safa, John Aram	
		US-2002/0099952	07/25/2002	Lambert et al.	
		US-2002/0112171	08/15/2002	Ginter et al.	
		US-2003/0063750	04/03/2003	Medvinsky et al.	
		US-2003/0149777	08/07/2003	Adler, Micah	
		US-2003/0190046	10/09/2003	Kammerman et al.	
		US-2003/0204726	10/30/2006	Kefford et al.	
		US-2003/0212892	11/13/2003	Oishi, Kazuomi	
		US-2003/0217263	11/20/2003	Sakai, Tsutomu	
Examiner Signature				Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.



Substitute for form 1449/PTO (modified by Applicant)  <b>INFORMATION DISCLOSURE          STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>				<b>Complete if Known</b>		
				Application Number	13/734,178	
				Filing Date	January 4, 2013	
				First Named Inventor	Craig S. ETCHEGOYEN	
				Art Unit	2649	
				Examiner Name	Yuwen Pan	
Sheet	3	of	5	Attorney Docket Number	UN-NP-SC-085	

U. S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code <small>(if known)</small>			
		US-2003/0237004	12/25/2003	Okamura, Mine	
		US-2004/0030912	02/12/2004	Merkle et al.	
		US-2004/0143746	07/22/2004	Ligeti et al.	
		US-2004/0145773	07/29/2004	Oakeson et al.	
		US-2005/0033957	02/10/2005	Enokida, Tomoaki	
		US-2005/0169271	08/04/2005	Janneteau et al.	
		US-2005/0187890	08/25/2005	Sullivan, Bryan	
		US-2006/0095454	05/04/2006	Shankar et al.	
		US-2006/0161914	07/20/2006	Morrison et al.	
		US-2006/0271485	11/30/2006	McKenzie et al.	
		US-2006/0280207	12/14/2006	Guarini et al.	
		US-2007/0005974	01/04/2007	Kudou, Yoshiyuki	
		US-2007/0055853	03/08/2007	Hatasaki et al.	
		US-2007/0079365	04/05/2007	Ito et al.	
		US-2007/0219917	09/20/2007	Liu et al.	
		US-2008/0022103	01/24/2008	Brown et al.	
		US-2008/0028114	01/31/2008	Mun, Kui-Yon	
		US-2008/0040785	02/14/2008	Shimada, Katsuhiko	
		US-2008/0049779	02/28/2008	Hopmann et al.	
		US-2008/0052775	02/28/2008	Sandhu et al.	
		US-2008/0076572	03/27/2008	Nguyen et al.	
		US-2008/0082813	04/03/2008	Chow et al.	
		US-2008/0098471	04/24/2008	Ooi et al.	
		US-2008/0244739	10/02/2008	Liu et al.	
Examiner Signature				Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute for form 1449/PTO (modified by Applicant)  <b>INFORMATION DISCLOSURE          STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>				<b>Complete if Known</b>		
				Application Number	13/734,178	
				Filing Date	January 4, 2013	
				First Named Inventor	Craig S. ETCHEGOYEN	
				Art Unit	2649	
				Examiner Name	Yuwen Pan	
Sheet	4	of	5	Attorney Docket Number	UN-NP-SC-085	

U. S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code <small>(if known)</small>			
		US-2008/0298595	12/04/2008	Narayanan et al.	
		US-2008/0311994	12/18/2008	Amaitis et al.	
		US-2009/0003600	01/01/2009	Chen et al.	
		US-2009/0006861	01/01/2009	ven Bommel, Jeroen	
		US-2009/0016264	01/15/2009	Hirano et al.	
		US-2009/0113088	04/30/2009	Illowsky et al.	
		US-2009/0158426	06/18/2009	Yoon et al.	
		US-2010/0034207	02/11/2010	Mcgrew et al.	
		US-2010/0164720	07/01/2010	Kore, Vinayak	
		US-2010/0211795	08/19/2010	Brown et al.	
		US-2011/0026529	02/03/2011	Majumdar et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		Country Code – Number – Kind Code				
		JP 4 117 548	04/17/1992	Fujitsu Ltd		
		WO 2001/009756	02/08/2001	Safewww, Inc.		
		WO 2008/034900	03/27/2008	Boesgaard Sorensen		
		WO 2008/052310	05/8/2008	PGMX, Inc.		

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO (modified by Applicant)  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>				<b>Complete if Known</b>		
				Application Number	13/734,178	
				Filing Date	January 4, 2013	
				First Named Inventor	Craig S. ETCHEGOYEN	
				Art Unit	2649	
				Examiner Name	Yuwen Pan	
Sheet	5	of	5	Attorney Docket Number	UN-NP-SC-085	
<b>NON PATENT LITERATURE DOCUMENTS</b>						
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.			T	
		Housley et al., "Internet x.509 Public Key Infrastructure Certificate and CRL Profile," <u>The Internet Society</u> , Network Working Group, Sept. 1999, 75 pages. [RFC 2459]				
		Wikipedia: "Software Extension," May 28, 2009, Internet Article retrieved on October 11, 2010. XP002604710				
		H. Williams, et al., "Web Database Applications with PHP & MySQL", Chapter 1, "Database Applications and the Web", ISBN 0-596-00041-3, O'Reilly & Associates, Inc., March 2002, avail. at: <a href="http://docstore.mik.ua/orelly/webprog/webdb/ch01_01.htm">http://docstore.mik.ua/orelly/webprog/webdb/ch01_01.htm</a> . XP002603488				
		Zhu, Yunpu, "A New Architecture for Secure Two-Party Mobile Payment Transactions," Submitted to the School of Graduate Studies of the University of Lethbridge, Master of Science, 2010, 240 pages.				
		Ylonen et al., "The Secure Shell (SSH) Authentication Protocol," <u>Network Working Group</u> , January 2006, 17 pages. RFC-4252.				
		Nesi, et al., "A Protection Processor for MPEG-21 Players," In Proceedings of ICME, 2006, pp.1357-1360.				

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平4-117548

⑬ Int. Cl.<sup>5</sup>

G 06 F 15/00  
9/06

識別記号

3 3 0 Z  
4 5 0 P  
4 5 0 Z

庁内整理番号

7218-5L  
7927-5B  
7927-5B

⑭ 公開 平成4年(1992)4月17日

審査請求 未請求 請求項の数 1 (全6頁)

⑮ 発明の名称 プログラムの不正使用防止方式

⑯ 特 願 平2-238301

⑰ 出 願 平2(1990)9月7日

⑱ 発 明 者 黒 住 弘 明 神奈川県川崎市中原区上小田中1015番地 富士通株式会社  
内

⑲ 出 願 人 富 士 通 株 式 会 社 神奈川県川崎市中原区上小田中1015番地

⑳ 代 理 人 弁 理 士 穂 坂 和 雄 外2名

明 細 書

1. 発明の名称

プログラムの不正使用防止方式

2. 特許請求の範囲

汎用パーソナル・コンピュータから通信回線を介してセンタに接続して取引処理を行うシステムにおけるプログラムの不正使用防止方式であって、

センタに対し取引処理を行うプログラムの一部を含むパッケージを汎用パーソナル・コンピュータに備え、

該取引処理を行うプログラムの残りの部分は該パーソナル・コンピュータがセンタにアクセスすると動作するセンタのローディング手段によりロードされ、

該取引処理用のプログラム中の所定間隔において設けられたタイマのセット及びリセット指示により制御されるタイマ手段を備え、

該タイマ手段のタイムオーバー出力により取引処

理のプログラムエリアを消去することを特徴とするプログラムの不正使用防止方式。

3. 発明の詳細な説明

[概要]

汎用パーソナル・コンピュータから通信回線を介してセンタに接続して処理を行うシステムにおけるプログラムの不正使用防止方式であって、

在宅からセンタにアクセスして取り引きを行う等の処理を汎用パソコンで行う場合に処理ソフトの解析やデータ変造ができないプログラムの不正使用防止方式を提供することを目的とし、

センタに対し取引処理を行うプログラムの一部を含むパッケージを汎用パーソナル・コンピュータに備え、取引処理を行うプログラムの残りの部分は該パーソナル・コンピュータがセンタにアクセスすると動作するセンタのローディング手段によりロードされ、取引処理用のプログラム中の所定間隔において設けられたタイマのセット及びリセット指示により制御されるタイマ手段を備え、

タイマ手段のタイムオーバー出力により取引処理のプログラムエリアを消去するよう構成する。

〔産業上の利用分野〕

本発明は汎用パーソナル・コンピュータから通信回線を介してセンタに接続して処理を行うシステムにおけるプログラムの不正使用防止方式に関する。

近年、在宅において種々の予約や、取り引きを行うことが可能になった。例えば、PB信号式の電話機により列車予約や、馬券の投票が行われているが、これらの処理を自宅のパーソナル・コンピュータを操作して実行したいという要望がある。

〔従来の技術〕

従来は、電話で行う場合、センタのオペレータに対して口頭で自分の識別番号(秘密番号)や、銀行の口座番号等を通知して本人の確認をして、購入する対象を知らせると、オペレータが端末を操作して取り引きが実行される方法や、顧客が電

用パーソナル・コンピュータ(以下、汎用パソコンという)を用いて投票等の処理を可能にすることが望まれている。ところが、在宅で自分が所有するパソコンからセンタにアクセスして処理を行う場合には、そのような処理を行うためのプログラムが必要となる。

ところが、そのためのアプリケーションプログラムをフロッピィまたはROMのような形で利用者に提供することは可能であるが、第1にパソコンによる投票の場合、データの送受信が行われるだけなので、取り引きの証拠が確実に残らないという問題がある。この点、従来は音声や、PB信号が介在する取引は全て録音され、万一トラブルが発生した場合その録音内容が証拠として利用された。

また、プログラムを利用者に提供した場合、取り引きの処理プログラムを利用者が分析することが可能となり、悪意がある場合、自分に都合が良いように内容を改造したり、いたずらでセンタに取り引きを申し込んだり(他人名義等)、データ

話をするときセンタの自動応対装置に接続され、センタからのアナウンスにより指示があると、それに対応した情報(数字)を電話のキーを操作することにより通知され、それをセンタで受信すると確認のアナウンスが顧客に送られる。それを聞いて確認することにより取り引きが成立するという方法が採られている。

このような取引の場合、後でトラブル(取引をした覚えがない、注文したものが違う、数量が違う等)が発生するのを防止するために、取引時のやりとりを全て(音声やPB信号等)録音する方法が採用されている。

〔発明が解決しようとする課題〕

上記のような電話による取り引きまたは投票(馬券等)では、音声と電話のキーによるやりとりが行われるので、目によって確認することができないし、センタが持っている関係情報を知ることができないという問題があった。

これに対し、遠隔の利用者が自宅にいながら汎

の変更、破壊等が発生することが予想される。すなわち、汎用パソコンの場合、利用者から一方的にデータを入力するだけでなく、センタが持つデータを知らせて(例えば、馬券の場合現在のオッズをセンタから送信してパソコンの表示装置に表示する等)、選択させる等のサービスが当然予想され、センタのデータにアクセスするプログラムがアプリケーションプログラムに含まれるからである。

本発明は在宅からセンタにアクセスして取引処理を汎用パソコンで行う場合に処理ソフトの解析やデータ変造ができないプログラムの不正使用防止方式を提供することを目的とする。

〔課題を解決するための手段〕

第1図は本発明の原理構成図である。

第1図において、10はセンタシステム、101はローディング手段、11は通信回線、12は家庭等の宅内に設けられたパーソナル・コンピュータ(パソコン)、13はパソコン内の取引処理

用プログラムが格納されたメモリ、131は処理プログラムの中の利用者が保持するパッケージからローディングされたプログラム、132はセンタからローディングされたプログラム、14はタイマ手段、15はメモリ消去手段である。

本発明はパソコンで使用する取引処理用ソフトの一部を除いた部分は利用者が保持しているが、キーとなる部分をセンタシステムからIPLにより使用する度に供給し、プログラムを実行した時に、実行を停止した場合には停止状態を検出してメモリ消去を行うことにより、ソフトウェアの解析やデータの変造を防止するものである。

#### 【作用】

利用者が自宅等に設置したパソコン12に対し、自分が保持する取引処理用のパッケージをローディングすることによりメモリ13内に一部が欠けた形のプログラム131が格納される。

次に利用者がパソコン12から通信回線11を介してセンタシステム10にアクセスして在宅シ

を繰り返す。しかし、利用者がプログラムを停止させて内容を解析しようとしたり、プログラムに含まれたデータを改変しようとする時、タイマ手段14がタイムオーバー出力を発生する。

このようにして、取引処理用のプログラムの内容の解析を防止し、取引により発生するデータ(取引の証憑)の保証が可能となる。

#### 【実施例】

第2図は実施例の構成図、第3図は実施例による取引処理のフローチャート、第4図はタイマ制御のタイミングチャート、第5図は取引処理の例を示す図である。

第2図において、20は投票センターシステム20は、例えば馬券等の投票の集計や、売上、配当等の各種のデータ収集や処理結果の出力等を実行する機能を備えている投票センターシステム、21は公衆網を介する通信回線、22はパーソナル・コンピュータ(パソコン)を表す。

パソコン22内において、23はCPU、24

システムからの取引の要求を行う。これに対し、センタシステム10では、ローディング手段101が起動して取引処理用のプログラムのキーとなる部分をパソコン12に対して送出する。パソコン12ではこれを受け取ると、メモリ13内の所定のエリアにセンタシステム10から送られたプログラムを格納する。これにより取引処理用のプログラムの全体がロードされた状態となる。

この後、当該取引処理用のプログラムを起動すると、この取引処理用のプログラム中に一定間隔で設けられたタイマのセット、リセット指令が発生する。この指令により制御されるタイマ手段14は、一定時間内にリセット指令が発生しないとタイムオーバー出力を発生し、その出力によりメモリ消去手段15が駆動される。メモリ消去手段15は駆動されるとメモリ13の内容を消去して、取引処理用のプログラムの全体を消去する。

すなわち、利用者が取引処理プログラムを実行している間は、タイマ手段14はセットされた後タイムオーバーとなる前にリセットされ、その動作

はROM、25は通信制御部、26はディスク装置、27はメモリ(RAM)、28はディスプレイ、29はキーボード、30はフロッピーディスク、1Fはインタフェース回路を表す。

第3図に示す取引処理のフローチャートを参照しながら実施例の動作を説明する。

利用者は投票処理を行うためのプログラムが格納されたフロッピーディスク30を保持しており、利用者が投票処理を行う場合、ディスク装置26にフロッピーディスク30を装着して、イニシャルプログラムローディング(IPL)を実行する(第3図の31)し、メモリ27にロードされる。メモリ27にロードされたプログラムは、第1図について説明したようにプログラムのキーとなる部分(図の斜線で示す)が欠けている。次にパソコン利用者が投票センターシステム20に対し接続する(同32)。この場合、パソコン22の通信制御部25、通信回線21を介して投票センターシステム20と接続され、確認等の処理を行い投票センターシステム20が、当該パソ

コンを識別すると、予め備えられた取引処理用のプログラムのキーとなる部分を取り出して、部分IPLによりパソコン22のメモリ27の一部(斜線で表示)にローディングする(同33)。

こうして、メモリ27上に取引処理用のソフトウェアの全体が完成すると、プログラムが起動され、タイマ1(メモリ上のエリアを使用する)をセットする(同34)。以後、タイマ1はクロックにより自律的にカウントする。

次に、利用者が、センターとのやりとりによる投票処理を開始する(同35)。この後、タイマ1はリセットされ、直ぐにタイマ1はセットされる(同36、37)。この後データ入力が行われると(同38)、タイマ1はリセットされ続いてセットが行われる(同39、40)。

その後終了か否かが判断され、終了しないとデータ入力が行われ、終了の場合、投票センターシステム20にデータ送信が行われる(同42)。次にタイマリセットが行われて(同43)、続いてタイマ1がセットされ(同44)、タイムオー

バによりセンターIPLのメモリが消去される。

また、上記のフローの中で、タイマ1セットの動作が行われた後(第3図の34、37、40等)、タイマ1リセットが発生しない場合(プログラムを停止した場合)、タイマ1のタイムオーバーによる割り込みが発生し、センターからIPLした内容がメモリから消去され、異常終了となる(同46、47)。

このフローでは、タイマ1割込によりセンターからIPLした内容だけメモリ27から消去するが、取引処理のプログラム全体を消去してもよい。上記のタイマ制御の動作を第4図のタイミングチャートに示す。

図に示すように、ロー(LOW)レベルの処理であるプログラムによる定期タイマ(上記タイマ1)制御においてセット・リセットを行い、もしタイマがタイムオーバーになると、割込が発生する。この割込は解析処理されてタイマ割込であることが解析されると、ハイ(HIGH)レベルのプログラム処理によりメモリ消去が実行される。

パソコンによりセンタにアクセスして行われる取引処理の例を第5図により説明する。

パソコンを所有している加入者Aが予め銀行Bに自分の口座を開設し、投票センタとその口座を用いた取引を行う契約を結んでおく。その加入者Aがパソコンから通信回線を介して投票センターシステムに接続する。この時、上記した本発明により投票センタシステムから取引処理プログラムの一部がIPLによりローディングされ、続いて、加入者がデータ入力(例えば、特定の馬券を指定して数量等を入力)することにより投票の取引処理が行われる。

投票センタシステムはその投票を受けると銀行の当該加入者の口座から取引金額を引き落とす(銀行からの残高通知により残高が無いと取引は成立しない)。投票に対する配当の支払いは、銀行の該当口座への振込処理により行う。

#### [発明の効果]

本発明によれば今後増大すると予想される汎用

のパーソナル・コンピュータによるセンタシステムとの在宅取引処理において、ソフトウェアの解析を困難にして処理データの信頼性向上を達成することができ、更にデータの変造ができないので契約処理(取引の証拠)の保証を可能とすることができる。

#### 4. 図面の簡単な説明

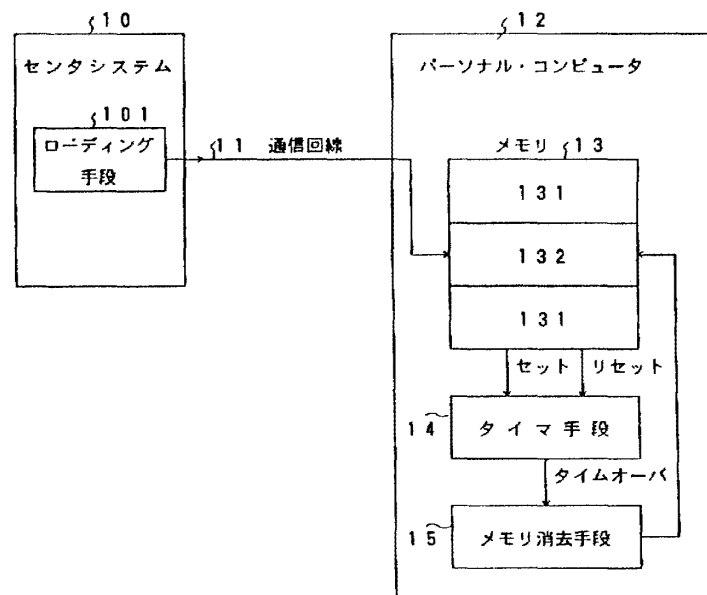
第1図は本発明の原理構成図、第2図は実施例の構成図、第3図は実施例による取引処理のフローチャート、第4図はタイマ制御のタイミングチャート、第5図は取引処理の例を示す図である。

第1図中、

- 10: センタシステム
- 101: ローディング手段
- 11: 通信回線
- 12: パーソナル・コンピュータ(パソコン)
- 13: メモリ
- 131: パッケージからローディングされた

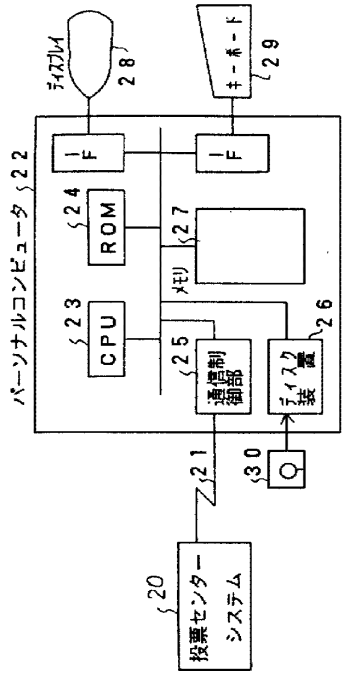
- プログラム、  
 132: センタからローディングされた  
 プログラム  
 14: タイマ手段  
 15: メモリ消去手段

特許出願人 富士通株式会社  
 代理人弁理士 穂坂 和雄(外2名)

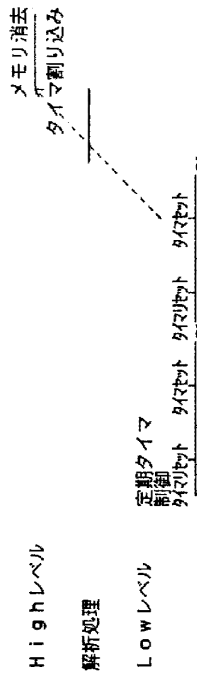


本発明の原理構成図  
 第1図

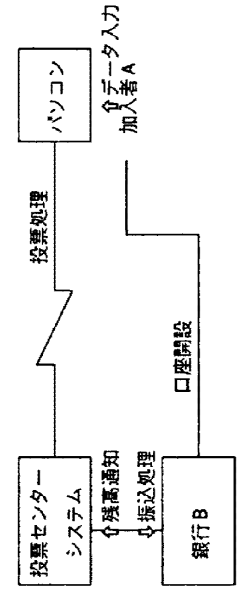




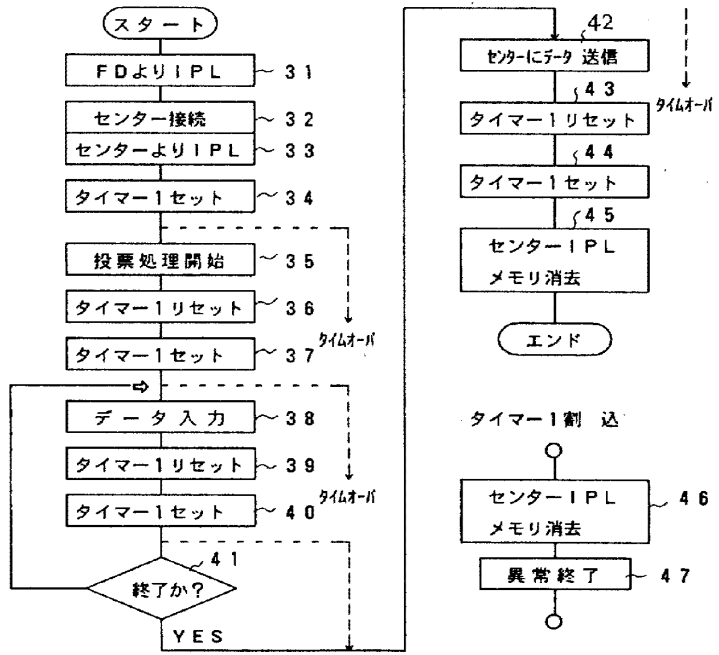
実施例の構成図  
第 2 図



タイマ制御のタイミングチャート  
第 4 図



取引処理の例を示す図  
第 5 図



実施例による取引処理のフローチャート  
第 3 図



Espacenet

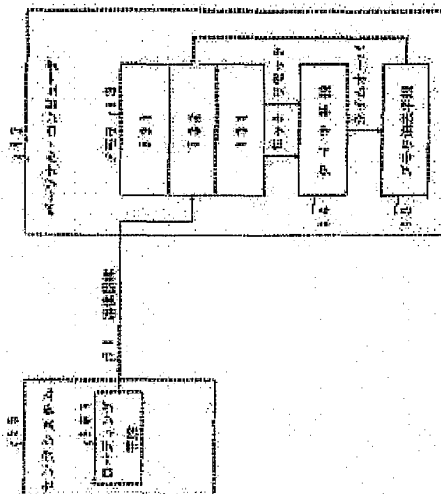
**Bibliographic data: JP4117548 (A) — 1992-04-17****PREVENTION SYSTEM FOR ILLICIT USE OF PROGRAM****Inventor(s):** KUROZUMI HIROAKI ± (KUROZUMI HIROAKI)**Applicant(s):** FUJITSU LTD ± (FUJITSU LTD)**Classification:** - international: **G06F12/14; G06F15/00; G06F21/00; G06F21/22; G06F21/24; G06F9/06;** (IPC1-7): G06F15/00; G06F9/06

- European:

**Application number:** JP19900238301 19900907**Priority number (s):** JP19900238301 19900907**Also published as:** JP3014130 (B2)**Abstract of JP4117548 (A)**

**PURPOSE:** To prevent the alteration of the data as well as the analysis of software by detecting the stop state of a program and erasing the contents of a memory when the execution of the program is discontinued.

**CONSTITUTION:** When a transaction processing program is started, the set/reset commands are produced for the timers provided at a fixed interval into the program. A timer means 14 which is controlled by the set/reset commands produces the time-over output when no reset command is produced within a fixed time. A memory erasing means 15 is driven by the time-over output. Thus the means 15 erases the contents of a memory 13 and then erases the entire program for transaction processing. Then the analysis of the program contents can be prevented.



CORRECTED VERSION

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
8 February 2001 (08.02.2001)

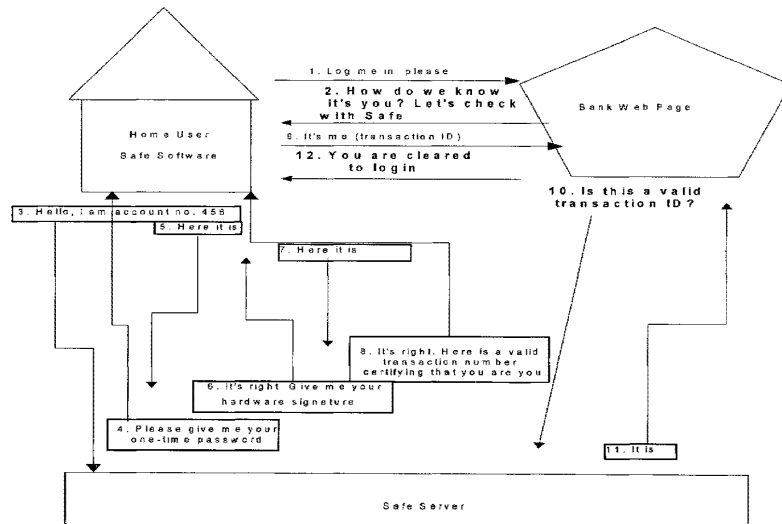
PCT

(10) International Publication Number  
WO 01/009756 A3

- (51) International Patent Classification<sup>7</sup>: G07C 9/00, EGI INTERNET LTD. [IL/IL]; John Eliasov, Haminhara Street 14, 46586 Herzliya (IL).  
G07F 7/10, G06F 17/60
- (21) International Application Number: PCT/US00/21058
- (22) International Filing Date: 31 July 2000 (31.07.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
  - 60/146,628 30 July 1999 (30.07.1999) US
  - 60/167,352 24 November 1999 (24.11.1999) US
  - 09/500,601 8 February 2000 (08.02.2000) US
  - 09/523,902 13 March 2000 (13.03.2000) US
  - 09/564,660 4 May 2000 (04.05.2000) US
- (71) Applicants (for all designated States except US): SAFEWWW, INC. [US/US]; John Eliasov, 50 Charles Lindbergh Blvd., Suite 400, Uniondale, NY 11553 (US).
- (72) Inventor: SANCHO, Enrique, David [IL/IL]; P.O. Box 1151, 30900 Zichron Yaacov (IL).
- (74) Agent: CHIRNOMAS, Morton; Shibolet H Yisraeli Roberts Zisman & Co., 350 Fifth Avenue, 60th Floor, New York City, NY 10118 (US).
- (81) Designated States (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, 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

[Continued on next page]

(54) Title: A SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING



(57) Abstract: A system for permitting a secure electronic purchase transaction on a public computer network, said network comprising a user's computer, a vendor's server, a creditor's server, and further comprising a toolbox server for providing third-party verification of user's identity, whereby in response to a request by said vendor's server said toolbox server positively identifies user's computer, requests a confirmation from said user's computer of said transaction and upon receiving said confirmation provides vendor's server with a gatepass for receiving a payment commitment from said creditor server.



WO 01/009756 A3



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, GW, ML, MR, NE, SN, TD, TG).

**(48) Date of publication of this corrected version:**

12 September 2002

**Published:**

— *with international search report*

**(15) Information about Correction:**

see PCT Gazette No. 37/2002 of 12 September 2002, Section II

**(88) Date of publication of the international search report:**

26 April 2001

*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.*

**A SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING**Cross-Reference To Related Applications

The present application claims the priority of the following US Patent Applications: U.S.  
5 Application Serial No. 09/564,660, filed 4 May, 2000, which is a continuation in part of U.S.  
Application Serial No. 09/523,902, filed March 13, 2000, which is a continuation in part of  
U.S. Application Serial No. 09/500,601 filed February 8, 2000 and claims the benefit of  
priority to U.S. Provisional application SN 60/167,352, filed November 24, 1999 and U.S.  
Provisional application SN 60/146,628, filed July 30, 1999. The specifications of these  
10 applications are hereby incorporated herein by reference in their entireties.

Field And Background Of The Invention

The present invention relates to systems and methods for implementing secure purchases  
over a computer network. More particularly, the methods relate to a system which permits  
15 purchases of merchandise to be made over a computer network, whereby the purchaser may  
feel confident that personal credit card information is not at risk of being diverted,  
misappropriated or stolen and the vendor may be more confident that the purchaser is bona  
fide.

20 It is well known for users of merchandise to access the global client/server network  
commonly referred to as the Internet, a part of which is the World Wide Web, for the purpose  
of searching for and purchasing merchandise from on-line vendors selling wares ranging  
from travel services and investment services to buying CD recordings, books, software,  
computer hardware and the like.

25 Numerous patents teach methods or systems purporting to secure commercial credit card  
transactions carried out over the Internet. Examples of such patents include US Patent Nos.  
5,671,279 to Elgamal, 5,727,163 to Bezos, 5,822,737 to Ogram, 5,899,980 to Wilf et al. and  
US Patent Nos. 5,715,314 and US 5,909,492, both to Payne, et al., the disclosures of which  
30 are incorporated by reference herein for providing background.

SUBSTITUTE SHEET (RULE 26)

Most of the disclosed systems have the disadvantage that they rely on the transmission of sensitive information over unsecured network routes and lines for each transaction. Although practically speaking, the systems which rely solely on encryption are fairly safe, there is still  
5 some risk of credit card misappropriation and there is little psychological comfort given to potential users by their knowing that encryption is being used.

Generally speaking, the Internet is a network of computers, remote from one another, linked by a variety of communications lines including telephone lines, cable television lines, satellite  
10 link-ups and the like. Internet service providers (hereinafter "ISPs") provide the link to the main backbone of the Internet for small end users. The account for the end user is established in the normal manner usually by providing credit card information to the ISP by conventional means, such as by voice telephony, fax transmission or check. In most ISP-end user relationships, the ISP has been given credit card or other credit account information,  
15 which information is on file with the ISP and available to the ISP's computers. In return for receiving payment, the ISP provides a gateway to the Internet for the end-user's use. The end-user (or user) is provided with identification codes for dialling directly into the ISP's computers and software means (for example, dialler software, browser software, electronic mail software, and the like) for doing so if necessary.

20

Most purchases are conducted in the following manner: a purchaser using a browser application on his local client computer connects via his computer's modem to a dial-up Internet Service Provider (hereinafter "ISP") and makes connections therethrough to various Web sites, i.e. Internet server locations assigned a URL (Uniform Resource Locator)  
25 address. The purchaser selects his merchandise and the vendor usually requests payment by one of several methods, one of which usually includes payment by providing credit card information.

According to surveys and other marketing data, there always has been and there still exists a  
30 high percentage of the population which is deterred from purchasing merchandise directly

over the Internet. This large percentage of the population apparently fears that, despite all the efforts at security and cryptography promised by the vendors, there still exists the possibility that their credit account information will be intercepted on-line by a third party computer hacker and used illegally, at great expense and trouble for the cardholder.

5

An additional anxiety-inducing factor related to merchandising over the Internet, or e-commerce, is that the vendor cannot always be certain that just because he has obtained credit card or account information, that he will actually be paid for the merchandise he ships. After all, credit card fraud and/or theft occurs regularly and may not be caught in time to stop the order from being shipped. When the cardholder discovers the theft and stops the card, it may be too late for the vendor to recover his property. At the very least, this situation leads to unnecessary aggravation and wasted resources for the vendor, credit card company and cardholder.

15 Summary And Objects Of The Invention

Thus, it is an objective of the present invention to provide a system and method for potential on-line purchasers of merchandise marketed over the Internet to pay for those purchases with minimized exposure to the risk of credit card theft by electronic interception.

20 It is a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence of the consuming public in the safety of such transactions.

It is still a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence with which vendors may ship the purchased product or deliver the purchased service without fear of the payment being provided fraudulently.

25 It is yet a further object of the present invention to provide a site-specific and computer-specific identification confirmation system for use in a secure electronic purchasing system, or other secure electronic transaction systems like authenticatin, access permission,

30

etc.

It is indeed a further object of the present invention to provide a method for encoding downloadable content files, such as MP3 music files, graphic files, e-books and the like so  
5 that the files can only be accessed by the actual purchaser of the file and preferably only from the computer to which they were downloaded, or to a limitable number of secondary authorized devices.

These objectives and others not specifically enumerated herein are achieved by the invention  
10 disclosed herein which comprises a system and method for providing a trustworthy commitment for payment to an on-line vendor for services or goods provided to an on-line user, without having credit card information passing over the public and unsecured Internet. The system and method of the present invention provides added security and comfort by providing, among other features, the comfort of knowing that an independent, uninterested  
15 third-party is confirming the identities of the parties involved and the validity of each and every transaction, in real time, and the further security of knowing that at no time is the user's credit card information being exposed over the World Wide Web.

In one exemplary embodiment, the method takes advantage of the existing business  
20 relationships between the end user with the owners of member computers/servers who give access to the backbone structure of the Internet. As explained hereinabove, the Internet is a network of servers, remote from one another, linked by a variety of communications lines including telephone lines, cable television lines, satellite link-ups and the like. Internet service providers (hereinafter "ISPs") provide the link to the main backbone of the Internet for  
25 small end users. The account for the end user is established in the normal manner usually by providing credit card information to the ISP by conventional means, such as by voice telephony, fax transmission or check. In most ISP-end user relationships, the ISP has been given credit card or other credit account information, which information is on file with the ISP and available to the ISP's computers. In return for receiving payment, the ISP provides a  
30 gateway to the Internet for the end-user's use. The end-user (or subscriber) is provided with



identification codes for dialing directly into the ISP's computers and software means (for example, dialer software, browser software, electronic mail software, and the like) for doing so if necessary.

5 Each time a user signs in to the ISP's computers for an on-line session, the user is assigned an Internet Protocol (hereinafter "IP") address. The user's computer transmits messages which are received by the ISP computer and relayed through the IP address and out onto the Internet to the ultimate intended recipient computer. During the entire time the on-line session in progress, the IP address does not change and is thus available as identifying  
10 information. By monitoring and occasionally re-verifying that the user's computer is still on-line at the assigned IP address, the ISP can confirm that certain activities could be attributed to the user.

This embodiment of the present invention takes advantage of the intimate relationship which  
15 is re-created every time an Internet user's computer goes online and signs into his ISP's computer by assigning to the ISP computer the function of clearinghouse and active intermediary between the user's computer and the vendor's computer. A user computer signs in to the ISP computer system and is recognized and assigned an IP address. When the user identifies merchandise or services at a vendor's website which he wishes to  
20 purchase, he sends programming to the website which selects the items and instructs the vendor's computer to generate a purchase authorization request which is sent to the ISP computer. The purchase authorization request contains information about the merchandise to be purchased, identifying information about the proposed purchaser, some of which is the identifying information assigned by the ISP to the user. The ISP confirms internally that the  
25 user is still signed in to the ISP computer system by verifying the identity of the computer currently actively communicating through the IP address. When satisfied that the user is still online, the ISP computer generates and sends a message to the user's computer requesting confirmation of the order for the merchandise. Upon receipt from the user's computer of the confirmation, the ISP generates and transmits to the vendor's computer a message  
30 confirming the order and providing a confirmation number, agreeing to pay the invoice which

the vendor's computer subsequently generates and presents to the ISP computer. The ISP computer then uses the user's credit card information and presents an invoice against the credit card account to be sent through normal channels.

5 In another exemplary embodiment of the present invention, the ISP does not serve as the credit giver or transaction verifier/guarantor. This function is provided by a bank or vendor with whom the user already has a credit account, and who has an online presence, i.e. has a transaction server connected to the Internet which can participate in the transaction as it is carried out by the user/consumer.

10

Another aspect of the present invention lies in the security provided by employing a method for verifying that the system is only usable by computers specifically registered with the system. More particularly, the method for identifying a registered computer, i.e. one which can be used for making a purchase transaction, or other electronic transaction and/or  
15 request, on the system of the invention, is constructed such that if a hacker were to try to "pretend" that his computer was in fact the registered computer of a bona fide user, the codes detect that they are no longer in their originally installed environment and the system becomes inoperable. The system can only be reactivated by reregistering the machine.

20 In another aspect of the present invention, the system is configured such that the request for a confirmation of a purchase transaction, or other electronic transaction, is forwarded in the form of an SMS (short message system) note to a user's cellular communications device, such as a cellular phone, alphanumeric pager or modem-equipped handheld computer. Thus, if the user was not sitting at the system registered computer, he can still be advised  
25 instantly that someone else, perhaps illegally, is attempting to fraudulently use his account or even his computer to make a purchase. This feature of the invention can contribute to deterring such computer fraud.

#### Brief Description Of The Drawings

30 For a better understanding of the invention, the following drawings are included for

consideration in combination with the detailed specification which follows:

Fig. 1 shows a user computer in communication with a vendor computer via the ISP computer, wherein user computer is initiating a purchase transaction;

5

Fig. 2 shows the vendor computer communicating with the ISP computer to request authorization to complete user's requested transaction;

Fig. 3 shows the ISP computer confirming that correct IP address is active with user's computer and requesting confirmation of user's transaction;

10

Fig. 4 shows users computer responding to ISP computer's request for confirmation;

Fig. 5 shows ISP computer's transmission of a confirmation code and invoicing instructions to vendor's computer;

15

Fig. 6 shows a block diagram illustrating another exemplary embodiment of the present invention;

Fig. 7 shows a block diagram illustrating another exemplary embodiment of the present invention;

20

Fig. 8 shows a block diagram illustrating another exemplary embodiment of the present invention;

Fig. 9 shows a block diagram illustrating the handshake and priming process of the system of the present invention;

25

Fig. 10 shows a user reacting remotely to fraudulent use of his PC;

Fig. 11 shows a user computer in simultaneous communication with a vendor computer and

30

the AA computer, wherein user computer is initiating a purchase transaction; and

Fig. 12 shows a block diagram illustrating another exemplary embodiment of the present invention.

5

#### Detailed Description Of The Exemplary Embodiments

In all of the exemplary embodiments which will be described hereinbelow, there are certain common features which, together with reference to the drawings, will be described once here  
10 to provide the reader with an easily understood framework.

As was discussed hereinabove, the present invention is designed to reduce compromising the security of one's credit account information which can be caused by transmitting the information over the unsecured World Wide Web. Additionally, the invention  
15 helps to ascertain that the parties participating in a transaction are who they purport to be.

The exemplary embodiments assume the following arrangement of the parties to a transaction: [a] a user is connected via his PC or client to the Internet through telephone, cable TV, satellite or data lines, usually through a modem and the user's client PC has  
20 installed therein a browser program, such as Microsoft Corporation's Internet Explorer or Netscape Corporation's Navigator or Communicator, an instance of which has been activated prior to the transaction; [b] a vendor has a server in communication with the Internet which constitutes or communicates a Website accessible to users' browser; [c] a security administration system operates via a security server, or toolbox (hereinafter "TB"), the  
25 physical location of which can vary as will be discussed hereinbelow; and [d] a creditor or payment guarantor has a payment server, although this function may optionally be performed by the security server. In the context of the present application, it should be understood that reference to a client or PC expressly includes any browser-equipped telecommunications device which gives the user the ability to access and interface with remote servers, and in  
30 particular Web sites on the Internet. Thus, such devices include browser-equipped cellular

phones, personal digital assistants, palm held computers, laptop computers, and desktop PCs, though not exclusively.

Additionally, it should be noted here that, rather than being a vendor of merchandise,  
5 vendor might simply be a provider of an information or financial service, as example. Thus  
vendor might be using the present invention to ensure that access to secured databases is  
only to properly authorized and duly-identified persons.

All of the four components of the system employ a combination of security measures,  
10 for instance, all transmissions take place in an encrypted environment, such as RSA, Triple  
DES, etc., using encryption tables which are replaceable by the security server or by a  
central system administrator server at random intervals.

The systems are of two general kinds; where the ISP will participate in the system,  
15 giving the highest possible level of security, and where the ISP is not a participant in the  
system. Where the ISP is a participant, it can participate in two aspects; [1] the ISP can serve  
as the physical host of the TB and [2] the ISP can be the creditor or payment guarantor, since  
the ISP already has an ongoing service agreement with the user. Where the ISP is not a  
participant as a creditor or payment guarantor, this function can be served by another party.  
20 The advantage to having the ISP as participant wherein the TB is physically at the site of the  
ISP has been alluded to hereinabove. That advantage lies in the fact that since most users  
dial into an ISP's modem basket over copper phone lines, the only way for a hacker to get  
between the ISP server (and the TB if installed piggyback to the ISP server) and the user is to  
physically tap into a phone company junction box, something that most hackers would not  
25 ever do. Even if the TB is at another physical location, the system still retains effectiveness  
but the fewer areas open for hacker attack, the better. If the ISP is not a participant, insofar  
as being a creditor or payment guarantor, this function can be fulfilled by the  
Internet-accessible payment servers of such business entities as online banks, merchants  
which give their customers credit accounts and other credit-providing institutions. In such a  
30 case, the TB might be located at the site of the credit institution, or in fact a single server

could act as the TB as well as the payment server. In another case, the TB and the payment server might be at completely different locations.

5 Before a transaction can take place, the components of the system need to be programmed and/or installed as follows:

The TB is a series of at least two servers, in addition to a Firewall Server, which includes therein a database containing the identification data of the security system's user participants. Additionally, TB can include programming to check and update the user's software version,, and encryption tables and instructions to either update those tables as  
10 needed, mark them for future updating or to direct user's browser to the URL of an appropriate server, such as the central administrator server for downloading updated tables.

The vendor server is modified such that a button or other directing device is added to the purchase initiating software that gets downloaded to a user's browser from the vendor server when a user indicates readiness to pay for a transaction. The added button tells a  
15 user to click on it if payment by the secured system of the invention is desired. By clicking the button, the user initiates a series of events which will be described further hereinbelow.

The creditor server is provided with programming directing it how to respond to the request from a vendor server for payment on a transaction that is accompanied by a Gatepass code, which the vendor receives from the TB.  
20

TB records all transaction data and assigns a unique transaction ID (UTID) to the record and further marks the record as "not yet confirmed". TB records the transaction data received from the vendor server and puts it under a URL. TB then commands  
25 User's waiting thread to come and retrieve the page at the URL on the TB and show it to User. The shown page is the Confirmation Request page which appears to user on client PC as a Pop Up window.

In the Pop Up window, User sees certain details of the transaction and text to the following effect: "We have been asked to pay a vendor \$17.20 for an order from you. Do you approve

the transaction?". To approve the transaction, User is instructed to input his System password (selected in the registration process) and click the OK button.

- a) If User clicks Reject or does not respond within a predetermined time frame then the order is deemed not accepted and TB rejects Vendor's request for payment URL.
- 5 b) If User accepts the transaction by entering his System password into the appropriate field and clicking the OK button, it closes the Confirmation Request Page window and sends the password back to the Wallet which encrypts the password and sends it back to the TB.
- c) In one exemplary embodiment of the present invention, the User can elect to  
10 additionally receive notice on his cellular phone or other cellular-enabled communication device (such as an alphanumeric beeper or an Internet-ready personal digital assistant or PDA) of the transmission of a Confirmation Request page to his PC. When User has elected this service, the transmission to his PC of a Confirmation Request page is accompanied by the simultaneous transmission of an  
15 SMS (Short Message System) message to his cellular device, thereby advising him that someone is operating his PC and conducting a purchase transaction. Using this follow-me technology, a user might then use his cellular device to respond to the SMS message with a message to cancel the transaction and/or initiate a trace of the fraudulent purchase request.

20

The transaction continues as follows in the embodiment wherein the Toolbox is located at the vendor or at the secure administration site, for example.

Physical Placement of TB In an exemplary embodiment of the invention, the TB is at the  
25 secure administration site or at the vendor site. In the case of the TB being at the vendor site, the TB is at the service provider's server. The user is not necessarily purchasing merchandise, but, for example, is making a request to the vendor server for access to secured databases contained therein or protected thereby. Thus, in order to be certain that the user has permission to access the secured databases, the vendor's server, in response to

user's selecting a button indicating participation in the system of the invention, takes the information forwarded with user's selection and creates an identity verification from the TB server. The rest of the procedure is substantially the same as described hereinabove. TB receives the identification verification request, undergoes the double ping handshake procedure and upon receiving the appropriate responses from user's client PC, sends a Gatepass response incorporating the UTID back to vendor's server. At this point, vendor's server can admit user into the desired secured database. As an additional layer of protection, vendor's server might undergo a double ping handshake procedure with TB to ensure the source of the Gatepass.

10

As noted hereinabove, rather than being a vendor of merchandise, vendor might simply be a provider of an information or financial service, as example. Thus vendor might be using the present invention to ensure that access to secured databases is only to properly authorized and duly-identified persons. For example, a bank might want identity verification before permitting a customer access to his account information or to use financial services. As another example, a large corporation might use the present invention to give third-party verification of an employee's or outside contractor's identity before permitting them access to secured databases which might not otherwise be available via the Internet.

15

The TB is essentially a mini-server, dedicated to the security tasks assigned to it. The TB is provided with programming which, when activated, sends, receives and verifies the proper forms and/or data to either a participating home user, ISP server or vendor in order to carry out the proposed transaction.

20

The authentication agent (hereinafter "AA") is software downloaded into the client computer. AA, which will be further described hereinbelow, performs the same function as a magnetic strip on a plastic card, e.g., a credit card. This enables the AA to be employed in Internet generated automatic teller machine (ATM) applications, such as fund transfers, credit card or debit card credits or debits, without the need for physical access to the ATM.

25  
30



The procedure described in this embodiment hereinabove is modified as follows:

1) In one embodiment of the present invention, AA sends SIMULTANEOUS messages to vendor and TB, so that the TB is expecting a certain message from the vendor.

5

2) The AA's action is described hereinbelow. In the present embodiment the AA is a COM object which creates a "digital fingerprint" consisting of various identifying hardware characteristics which it collects from the user's PC, as well as passwords (to be described further). Activation of the account initiates a process by which the TB records a fingerprint for the user, which the AA has derived, including a unique identification ("UID") for the user, using the identifying characteristics of user's PC (e.g. CPU ID number, hard disk serial number, amount of RAM, BIOS version and type, etc.).

10

3) When a transaction starts, the user's AA, which is a simple DLL, is activated by the vendor script. The AA sends a message to the Toolbox server, using the server's public key. If the server answers the AA, the home user's computer knows that it is talking to the correct server, since only the Toolbox has the private key that can decrypt the message sent with its public key. The Toolbox server now sends the user half of a new Triple DES key that it has generated so that the home user can communicate with it securely. Next the TB asks for the user's OTP (one time password) which is stored on a configuration file in the home user's computer. This configuration file can only be opened by a combination of personal password and CPU id. If the home user's computer responds with the correct password, the TB knows it is talking to the correct user. Once the TB has verified that it is talking to the correct user, the TB sends a dynamically generated smart DLL to collect the computer's hardware signature, verifying that it is also talking to the correct machine. The TB also records the number of encounters with the user. Any hacker who manages access probably fails this check, and is thereby discovered. The configuration file, which contains the account ID, machine ID, and a replaceable one-time password, among other items, can be stored optionally on user's computer's registry, or on the hard drive or on a removable floppy, i.e., the configuration file can be removed and taken away from the proximity of the user's computer, thereby

15

20

25

30

disabling the user's access to the account from that computer.

When registering for the first time, and also when authenticating a user, the simple DLL loads itself into memory, and calls a "smart" DLL, from a collection of thousands of continuously regenerated smart DLL's, which collects a large number of different parameters, for example  
5 12, identifying the user's computer. A simple example of an authentication transaction is now described using two machine parameters. the DLL applies an algorithm such that if the disk serial number is 1 and is multiplied by 1; and if the CPU serial number is 2 and is multiplied by 2, the resulting string is their sum, or "5". Thus,  $1(1) + 2(2) = 5$ . This information is  
10 hashed by the DLL according to that DLL's hashing programming, then encrypted, and the encrypted hash is sent back to the TB. The order of the parameters and the algorithm used can change each time. Furthermore, the actual information is further interspersed with "garbage" code, expected by the TB, every time. The server receives the hashed and encrypted result from the smart DLL, and compares it to the result which it expects to receive.  
15 This is done by the TB by calculating the expected result by running it's own copy of the unique DLL on the user's identifying parameters that it has stored in the database. It then hashes the result, and compares its hash to the deencrypted hash string it received from the user.

20 .  
An exemplary embodiment of the present invention, more specifically uses a 2048 bit RSA key to initiate the handshake, and thereafter moves to Triple DES encryption. The Public Key is distributed to all the end-users with the Agent and the Private Key(s) are held by the AA Server. There is a different set of Keys for different Providers, i. e., Credit Card  
25 Companies, Banks, etc.

The TB can be used to verify a digital fingerprint in various forms of Internet transactions, for example:

#### Banking and Financial Services

A bank or financial institution can use digital fingerprints to provide customers with secure access to their accounts for stock transactions and account management. Customers can use their digital fingerprints as a universal log-in at the bank's Web site for quick access to their account information without having to remember a unique log-in name and password. To further enhance each user's experience, the bank can provide targeted content and services to its customers based on the registration information contained in their digital fingerprints. The bank can also use digital fingerprints to send secure e-mail, allowing it to proactively send private account information to its customers.

#### Retail

A manager of a online retail store can watch customers browse merchandise, identify purchase patterns, observe the behavior of casual visitors, and set up accounts for purchases. A manager of a retail Internet site can perform these same functions online by using digital fingerprints. By implementing client authentication with digital fingerprints, the retail site can analyze customer interests and behaviors, track and compare the profiles of visitors who browse and those who actually place orders, and perform market analysis and segmentation based on information presented in its customers' digital fingerprints. The site can extend the power of digital fingerprints by linking the ID to information in its existing customer database (e.g. customer's account, order status, or purchase history).

Additionally, by using the one-step registration feature of digital fingerprints, the site can quickly find out information about first-time visitors to the site. The site can use this information to provide relevant content to these visitors, thus capturing their interest and increasing the likelihood that they will become customers.

The authentication and security associated with digital fingerprints can allow the site to verify the identity of a customer, eliminating consumer misrepresentation and false orders. Additionally, consumers will have more confidence in conducting transactions on the Internet.

5 Publishing and Subscription

An online newspaper depends on advertising and subscription revenues. Digital fingerprints can allow this site to use basic registration information that is in a digital fingerprint - country, zip-code, age and gender - to understand the profile of its visitor population, thereby increasing the value of the advertisement placement and the amount that can be charged for  
10 the advertisement.

The site can use the universal log-in feature of digital fingerprints for identifying its site subscribers. Site visitors no longer need to remember unique log-in names and passwords for the site, and the site no longer needs to maintain a costly log-in and password database.

15 By understanding the profile of its first-time customers, and providing tailored information based on the basic registration information in a digital fingerprint, the site can use digital fingerprints to help it acquire new customers.

Services

20 A service company, such as a delivery company, can use digital fingerprints to provide secure access to its Web site, allowing customers to track their shipments without having to enter user names or specific tracking information. Digital fingerprints can allow this site to provide a highly customized experience to its visitors, for example, by providing specific delivery rates based on the geographic location of the customer. Digital fingerprints can also enable the site  
25 to send secure e-mail with billing information to its customers.

#### Business-to-Business

With the level of authentication provided by digital fingerprints, a manufacturing company can allow portions of its Internet site to be updated by its business partners and accessed by its customers. The manufacturing company's suppliers can update their product availability and scheduled shipping date in the manufacturer's database, providing a more efficient means for inventory management. Additionally customers can track order status through the same online database. These types of transactions would not be possible on the public Internet without the use of digital fingerprints to authenticate the identity of the company's suppliers and customers.

#### Music, Picture, Video, or e-Book File Sale and Download

Another possible application for the unique hardware fingerprint is to use it as a lock and key for preventing unauthorized downloading, copying and playback of content files, such as MP3 music files, e-book files, graphic files, etc. The fingerprint could be associated with the downloaded file and attempting to open the file on a machine which does not bear the fingerprint results in the file being permanently locked, unusable or somehow otherwise disabled. The fingerprint coding can determine whether the downloaded file can be copied to and played on a limited number of secondary machines. In fact, the encoding could initially be used to determine that the person downloading the file is the person even entitled to do so.

The examples discussed herein and demonstrated by the Figures are merely for illustrative purposes only. Variations and modifications of the disclosed invention in a manner well within the skill of the man of average skill in the art are contemplated and are intended to be encompassed within the scope and spirit of the invention as defined by the claims which follow.

For example, in another exemplary embodiment the ISP is not the site where the Toolbox

resides. With reference to Fig. 7, The Toolbox could be physically located at the site of the credit provider ("Creditor"), e.g. online-enabled bank, credit card provider or other affinity-card or charge account provider (including brick-and-mortar retailer's with an online presence such as Macy's) and in communication through normal channels with Creditor's transactional server. In this case, the ISP would not be an active part of the purchase transaction, other than in the usual known way by giving User access to the Internet. Generally, except as specified hereinbelow, the rest of the process proceeds substantially as described hereinbelow. Specifically, in this exemplary embodiment, the account is set up as follows:

10

## Installation Process:

- 1) A user requests to join the system, via an ASP page on a web server, over an HTTPS connection.
- 15 2) The applicant receives an account ID, and his application information is stored in an applicant's database on an application and database server, behind a firewall. The system owner, which can be an ISP, bank or other financial provider accesses this database from another web page, located on a Web server behind a firewall on an internal LAN.
- 20 3) When the system owner approves the user's application, the system automatically sends the user an email containing a link to a unique URL where he can begin the registration process. It also generates a one-time activation key linked to the user's account. The system owner must give this one-time activation key to the user in a secure way (for example, in person, or via a printout from his automatic teller).
- 25 Possession of the one-time activation key constitutes proof that the user is who he purports to be during the activation stage.
- 4) When the user goes to the URL, and presses the "Activate" button, the activation process begins by downloading a DLL containing a COM object to his computer. Dynamic Link Library (DLL) refers to the ability in Windows and OS/2 for executable memory to call software libraries (i.e., subroutines, or code for accomplishing specific
- 30

functions) not previously linked to the executable. The executable is compiled with a library of "stubs" which allow link errors to be detected at compile-time. Then, at run-time, either the system loader or the task's entry code must arrange for library calls to be patched with the addresses of the real shared library routines, possibly via a jump table.

5

5) This COM object relays the user's account ID (which it knows because he has been directed to a unique URL) to a "listener." This listener contains a proprietary communication protocol to enable the authentication web servers in the DMZ to communicate securely with the authentication application server and database server behind the firewall. The listener asks the applicant database behind the firewall to validate that the account ID it has been given is legal, and not yet activated. If so, the listener tells the COM object to send a pop-up to the user, to collect the one-time activation key. If not, the activation process stops. De-Militarized Zone (DMZ) is from the military term for an area between two opponents, where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. External DMZ Ethernets link regional networks with routers to internal networks. Internal DMZ Ethernets link local nodes with routers to the regional networks.

10

15

6) If the key collected by the popup matches what is stored in the database for the user's account, the DLL proceeds to collect the user's hardware signature (12 parameters including CPU ID, BIOS ID, disk volume information, various serial numbers etc.) and send it back to the database. If the key does not match, or the user does not answer within a set time limit, the activation process stops. After a set number of failed tries, the user's account is disabled.

20

7) If the key matched, the DLL then returns a seed for an encrypted one-time password (OTP) for use during the next encounter. Another pop-up is sent to collect a personal password chosen by the user, which is known only to the user, and not stored anywhere.

25

8) After the personal password has been collected, a configuration file containing, among other things, the OTP, which has just been exchanged, is encrypted. The account is then marked as active. On the next encounter, the one-time password just

30

exchanged will be used as part of the authentication process. The key to opening the configuration file is the user's personal password together with parts of his computer's hardware.

- 5 Once the installation has been completed, the software components remaining on the home user's computer are the configuration file and the DLL containing the COM object.

The COM object contains a self-validation routine, which lets it make sure that it has not been tampered with when it is loaded into memory, and a routine to establish a secure  
10 communication channel after it has made sure that it is intact. The secure communication channel is used to call a dynamically generated DLL from the server. In all future encounters, this dynamically generated DLL does most of the work in collecting information for the authentication process.

- 15 The other components of the COM object are a locator, a profile manager and a payment method manager.

The locator ensures that the latest version of the software is installed, and locates the profile manager and the payment method manager for a home user.

20

The locator has two interfaces implemented via the `agentClassId` property and the `agentCodeBase` property.

`AgentClassId` specifies which payment method manager and which profile manager to use.

- 25 `AgentCodeBase` specifies which server holds the most updated version of the software, and compares what is installed to latest version. If the latest version is not installed, `agentCodeBase` installs it automatically. (This feature is supported under Internet Explorer, versions 4 and 5 and Netscape 5). This enables us to control what information is supplied to vendors while allowing vendors to code one standard line of code that never changes.

30



AgentClassId has five methods: get attribute, set attribute, set parameter, stop payment, and pay.

*Get attribute* is a method to get non-sensitive information such as name, shipping information, etc.

5 *Set attribute* helps a browser page put this information into the user's computer.

*Set parameter* helps configure the profile.

*Stop payment* lets the user stop in the middle of a transaction, once the pay method has been invoked.

*Pay* is responsible for establishing a secure communications channel, and returning the  
10 buyer's hardware signature and password on that channel.

The Payment Method Manager enables the choice of more than one payment option.

The profile manager allows different people to use the same hardware. One account may have multiple users, with multiple shipping addresses or billing addresses. A user may also  
15 choose to use billing information from a previously existing wallet such as Microsoft wallet, via the profile manager.

Transaction Cycle

*Step 1 - Customer Starts the Login Process at a Bank or Vendor*

The first step occurs when the customer contacts a bank or vendor with vendor script installed  
20 and attempts to log in. This activates script, which was copied and pasted into the bank or vendor's ecommerce application.

*Step 2 - The Customer Contacts the TB*

The script activates code, which contacts the DLL installed with the buyer's home software, and tries to load the COM object into memory. When the COM object is loaded into memory it  
25 runs an integrity test to make sure that it has not been tampered with. If the checksum is correct, it leaves the result in memory, so it can pass it later to the authentication server. Otherwise, it returns an error that disables the user's account and stops working.

If the COM object succeeds in verifying that it is intact, Pay attempts to contact a "listener" on the TB and establish a secure TCP/IP communication channel. It contacts the TB using the

TB's public RSA key, passing to it the user's account and machine IDs. The listener sends a request to validate the customer's account number and machine ID number to the application database, where the user's installation parameters are recorded. If they are valid, the listener asks the COM object for an encrypted one-time password. This password is generated from a seed that was stored in a configuration file on the user's computer and in the TB's user database during the last exchange between them. This one-time password is "unlocked" for use by the user's personal password, known only to him, and stored only in his mind, and by the CPU Id of his computer. (When the transaction is an installation, and there has been no prior exchange, a first time activation key received from the owner system takes the place the place of the one-time password.)

If the numbers do not match, or if the user does not answer within a set time limit, the home user software sends back an error message, the account is temporarily disabled, and a log is created.

If the numbers match, the COM object knows that it is talking to the TB, since only the TB can decrypt messages sent with its public key, and the TB knows that it is talking to the right person since only he can "unlock" the one-time password. Using RSA encryption, a shared secret key is now exchanged using a Diffie-Helman key exchange on this channel, and the encryption method switches to triple-DES. (In triple DES encryption, the encryption keys change several times during the transmission.)

### 20 *Step 3 - The TB Authenticates the Customer*

Now that a secure channel exists, the listener on the TB sends a dynamically generated DLL to collect the home user's hardware signature information. This DLL is unique to each transaction. It returns signature in a string which is uniquely scrambled for each transaction and encrypted.

25 If all of the parameters match, the TB's authentication server can be sure it is talking to the correct customer, who is communicating from the correct computer. The TB returns a valid transaction ID to the customer, who passes it to the bank or vendor. In the bank model, the thread is closed, and an object on the server waits for the bank to inquire about the transaction.

In the ISP or ecommerce model, the thread remains open, waiting for an order to issue a pop-up window to the user to validate purchase details for the transaction.

*Step 4 - The Bank or Vendor Contacts the TB to Verify the Transaction*

5 Bank or Pure Authentication Model

The bank or other vendor passes customer's account ID, machine ID, Listener ID, Provider ID and transaction ID to the TB. If these match what was stored in the database when the customer was authenticated, in the pure authentication model, the process ends here. A log-in transaction is validated and the customer continues on to carry out his transactions using the owner's proprietary system, whatever that may be.

10

Optionally, the TB may send the customer an SMS message notifying him of the transaction

ISP or Ecommerce Models

In the ISP and other Ecommerce models, payment details and credit availability must be validated in addition to user identity. In addition to the customer's account ID, machine ID, Listener ID, provider ID and transaction ID mentioned above, the Vendor passes the payment details (invoice number, invoice amount, currency) to the TB's authentication server. A new pop-up window is sent to the user on the secure channel previously established by Pay, asking him to authorize the invoice details. (As noted above, if the user does not answer within the set period of time, or rejects the transaction, the process is stopped and the thread dies). If the user accepts the transaction by clicking on the "Accept" button, TB's authentication server contacts a Payment server, and verifies that the user has credit available. If so, a transaction debiting the user and crediting the vendor is issued to the customer's chosen financial provider.

20

25 Lastly, the TB notifies the vendor that the transaction is valid and the customer that a successful transaction has been completed. Optionally, the TB may send the customer an SMS message notifying him of the transaction.

With reference to FIG. 7, it can be seen that a typical purchasing session in this exemplary

embodiment proceeds as follows:

- 5 a) User PC goes online and user points his browser to the Website of a Vendor server using any Web Browser Program; downloads files depicting merchandise for sale and selects merchandise to purchase which generates a purchase request to Vendor's server, all in a manner well known in the art.
- 10 b) Vendor's server sends back to user PC an order page or pages which typically includes a transaction number, the value of the order, and asks for billing information, shipping information. At some point, user is offered to indicate her desired method of payment and selects option button which designates the AA payment plan of the present invention, e.g. "AA OPTION".
- 15 c) Selection of the "AA Option" generates a message back to Vendor's server which includes user's IP address and instructs Vendor's server to forward a request to Creditor's Toolbox to confirm that the user at the IP address provided is (a) actually and actively online and trying to make this purchase, and (b) that the user at the IP address has the necessary credit to make such a purchase.
- 20 d) Upon receipt of the request from Vendor's server, Toolbox immediately sends a transmission to the IP address provided by Vendor's server. The transmission includes files which (a) search for, decrypt and read the UID files in user's PC to see who it is, (if the PC is a machine registered in the system) and (b) which generate a Pop-up message on the registered user's browser to make sure that the transaction is desired by the AA system registered user. The message advises that a transaction having a particular value is being requested and asks for confirmation or rejection of the transaction. To reject the transaction, user can actively Reject by pressing a Reject button or simply by not responding within a pre-determined default time.. To
- 25 accept the transaction, the user must provide his user password and submit the form back to the Toolbox. The form is accompanied transparently by the fingerprint file containing the UID and other machine identifying information decrypted and extracted

from user's PC by the transmission from the Toolbox.

5 e) If accepted by user, then Toolbox checks database to make sure user's credit limit is not exceeded and sends a coded confirmation to Vendor's server that the transaction is confirmed and will be paid for by Creditor on behalf of user. Vendor then sends HTML message to advise user that the identified transaction has been successfully processed.

10 f) As described hereinabove, if user either actively Rejects or fails to respond to the Pop-up message in a predetermined time period, for example, 2 minutes, the Pop-up message disappears and Toolbox advises Vendor's server that the transaction is not accepted. Optionally, provision can be made where user can label a tendered transaction as "suspicious" and reject an order with prejudice, thus alerting both Toolbox and Security Program Manager, and therefore Vendor, that some attempt was made to defraud Vendor.. Obviously, this knowledge can provide great benefits in aiding to track down cyber credit frauds and inhibit criminal activity.

15 In yet another exemplary embodiment, the Creditor server is also an ISP server, or at least they are at the same location and being serviced by the same modem basket. The Toolbox is still situated at that location as well. Thus, a bank which offers ISP services to it's on-line customers can also offer them the safety of the AA transaction system and method, which is carried out by the Toolbox right on the bank's/ISP's premises.

20 The transaction continues as follows in the embodiment wherein the Toolbox is located at the ISP, hereinafter the ISP-Toolbox Model.

25 As was mentioned hereinabove, TB receives the encrypted password from the wallet if user accepted. TB can further have the ISP server verify that the IP address of the user has not changed during the course of the transaction. TB uses the encrypted password to change mark on transaction record from "not yet confirmed" to "Confirmed". The transaction

record, was assigned a unique ID number (UTID) which also serves as the Gatepass number and which is now sent to the vendor server.

Vendor server receives the Gatepass number and forwards it to creditor or payment server ("PS"), together with the amount to be paid and a vendor-assigned purchase transaction number.

For extra security, it is preferable that PS confirm the Gatepass with TB using the double handshake and priming routine with TB, similar to that performed between TB and user's client PC. PS sends 2 ping numbers (first ping number was previous payment transaction's second ping number and present second ping number will be used as first ping number in next payment transaction), repeats sending both ping numbers, then, when TB responds by sending back second ping number, PS sends Gatepass received from Vendor together with transaction information. Optionally, when PS is registered as a participant in the security program, similar software agents and wallets could be installed on the PS so that TB can confirm PS identity after the handshake process using hardware fingerprints.

TB checks TB server database and if Gatepass and transaction information match the transaction record, then TB sends response to PS indicating that user has confirmed the desire to close the transaction and PS is authorized to charge User's account for the order. TB records on the transaction record that the payment request has been tendered and approved.

#### Physical Placement of TB

In one exemplary embodiment, the TB is located at the physical site of the ISP, optimally connected to the phone or communication lines coming into the ISP server directly from users on one side of ISP server. The TB is also connected to lines going out to the Internet (via the modem basket) from the ISP server. The TB does not interact directly with the ISP server. For the most part, it monitors incoming and outgoing traffic, waiting to take over those communications should a security related transaction be called for by a home user.

The following scenario describes an exemplary embodiment of the process initiated when a request for a security related transaction is detected by the TB located at the ISP.. As will be further described hereinbelow, in another exemplary embodiment, the Toolbox might not be located at the ISP but at the site of another credit provider.

- a) User directs his browser to the URL of a vendor server and selects merchandise to purchase.
- b) User is offered methods of payment and selects option button for "SECURITY PROGRAM MANAGER" or "AA PAY OPTION".
- c) In an Autofetch process, an OnChange script handler in User's software prepares and sends request to central system administrator server for Session User Identity.
- d) Central system administrator server redirects request to user's TB equipped ISP.
- e) TB searches its files and returns user's identity..
- f) A user form is generated by user's computer and populated with user information including identity returned in step (e) from ISP TB.
- g) The form is submitted, together with a challenge which is forwarded to the vendor server.
- h) Vendor server runs a script that calls the central system administrator server's getGatePass.asp, thereby transmitting the Session User Identity, IP (user's current IP address), Sum of the transaction and the challenge.
- i) The central system administrator server redirects the vendor server's call to the ISP identified by the IP while the user stands by.

j) The TB at the ISP receives the getGatePass.asp and runs a check of the IP provided as part of the vendor server's call against the internally known IP to make the sure that is where the user really is logged in. If the IP test fails, the vendor server receives a rejection notification from the ISP server and the transaction is terminated.

k) If the IP test succeeds (i.e. the user really is connected to the correct IP address) then the ISP challenges the home listener .

Figure 10 illustrates a situation where client 204 is located remotely from his PC 212, for example driving his car 206. An intruder 208 has gained access to his PC 212, and has fraudulently attempted a secure transaction. The AA communicates a message accordingly to client 204 via the Internet 220. The client can be remotely contacted, for example, through his cellphone 230, his pager 240 or his PDA 210. Client 204 is shown receiving the message through his cellphone 230.

Figure 11 illustrates client 302 sending a simultaneous message 304 to AA 306 and vendor 308.

The fingerprint mechanism of the present invention can be adapted for use to ensure ownership rights in downloaded copyrighted material, such as content files which includes MP3 music files, e-books, graphic files, and the like. In the event a content file is to be purchased by a user, for example, if a user orders an MP3 file, the user is directed to a URL address for downloading the file. The digital fingerprint provided by the smart DLL in the user's PC is incorporated into code in the content file itself. Thus, the file is only downloadable if the fingerprint information encoded into the file matches that of the user's PC. Additionally, the content file can be encoded to limit how and where the downloaded file can be accessed and operated. The encoding can determine whether or not the file can be transferred to a limited number of other PC. Alternatively, the ID is associated with a diskette, as described hereinabove, and may be transferred to a limited number of PC's or perhaps



only to one other MP3 player (or PDAs in the case of an e-book).

It will be appreciated that the preferred embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both  
5 combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description, and which are not disclosed in the prior art.

What is claimed is:

- 1) A system for permitting a secure electronic purchase transaction on a public computer network, said network comprising a user's computer, a vendor's server, a creditor's server, and further comprising a toolbox server for providing third-party verification of user's identity, whereby in response to a request by said vendor's server said toolbox server positively identifies user's computer, requests a confirmation from said user's computer of said transaction and upon receiving said confirmation provides vendor's server with a gatepass for receiving a payment commitment from said creditor server.
- 2) A system in accordance with claim 1, wherein said toolbox server positively identifies user's computer by first accessing said user's computer via a gatekeeper.
- 3) A system in accordance with claim 2, wherein said toolbox server transmits to said gatekeeper a pair of identification numbers, wherein the first of said identification numbers is for gaining admittance and the second of said identification numbers is for priming said gatekeeper for admittance on a subsequent occasion.
- 4) In a computer network, a system for performing a secured transaction between a user's computer, a vendor's server, a creditor server and a toolbox server, wherein said user's computer has received fingerprint programming from said toolbox server for creating a digital fingerprint for use by said toolbox server to identify said user's computer.

- 5) A method for performing secure electronic transactions on a computer network, said network comprising a user's computer, a vendor server, a creditor server and a toolbox server, said user's computer having a gatekeeper and digital fingerprint stored therein, including the steps of:
- 5           i)       said user computer sending a purchase request to said vendor server to pay for a purchase, which purchase request includes a user identification number associated with said user computer and known to said toolbox server, said request initiating the transmission of a confirmation request from said vendor server to said toolbox server to
- 10           confirm said user computer's identity;
- ii)       said confirmation request causing said toolbox server to send a pre-arranged handshake and primer to said gatekeeper, whereupon said gatekeeper allows said toolbox server to request confirmation of said digital fingerprint.
- 15
- 6) A method in accordance with claim 5, wherein said primer comprises a pre-arranged handshake for the next succeeding occurrence of a transaction confirmation operation.
- 20       7) A method in accordance with claim 5, wherein said digital fingerprint is internally confirmed by said user's computer when said purchase request is initiated.
- 8) A method in accordance with claim 5, wherein said user's purchase request
- 25       is sent to said vendor simultaneously with said confirmation request, which is sent directly from said user computer to said toolbox server.
- 9) A system for verifying the identity of a client computer requesting access to
- 30       a secured database via a public computer network, said network comprising a

user's computer, a vendor's server, and further comprising a toolbox server for providing third-party verification of user's identity, whereby in response to a request by said vendor's server said toolbox server positively identifies user's computer, requests a confirmation from said user's computer of said request  
5 for access and upon receiving said confirmation provides vendor's server with a gatepass for permitting said client computer access to said secured database.

10) A system for permitting a secure electronic purchase transaction on a public  
10 computer network without passing credit account information over said public computer network, said network comprising a user's computer, a vendor's server, a creditor's server, and further comprising a toolbox server for providing third-party verification of user's identity, whereby in response to a request by said vendor's server said toolbox server positively identifies user's computer,  
15 requests a confirmation from said user's computer of said transaction and upon receiving said confirmation provides vendor's server with a gatepass for receiving a payment commitment from said creditor server.

11) A system for copy-protecting content files downloadable from a computer  
20 network, said network including a user's computer, a vendor's server, and a toolbox, wherein said user's computer has received fingerprint programming from said toolbox for creating a digital fingerprint for use by said toolbox to identify said user's computer, and further comprising said vendor server encoding said digital fingerprint into said content files, whereby said  
25 downloaded files will only be downloadable by said user.

12) A system for copy-protecting content files downloadable from a computer  
network in accordance with claim 11, wherein said downloaded files can only  
be played on a user computer having the digital fingerprint encoded into said  
30 file by said vendor server.

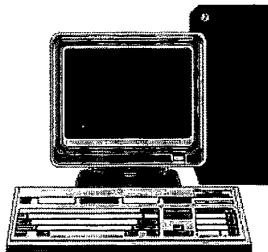
13) A system for copy-protecting content files downloadable from a computer network in accordance with claim 11, wherein said downloaded files can only be copied a limitable number of times directly from said user's computer onto  
5 other secondary devices, said limitable number being determined by said digital fingerprint encoding.

14) A system in accordance with claim 1, wherein a said confirmation request is contemporaneously sent to a cellular device.

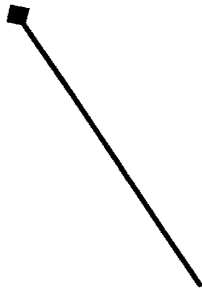
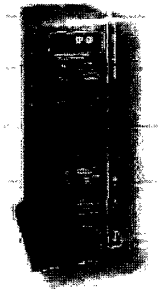
10

FIG. 1

Amazon Shop (Vendor)



Internet Service Provider (ISP)

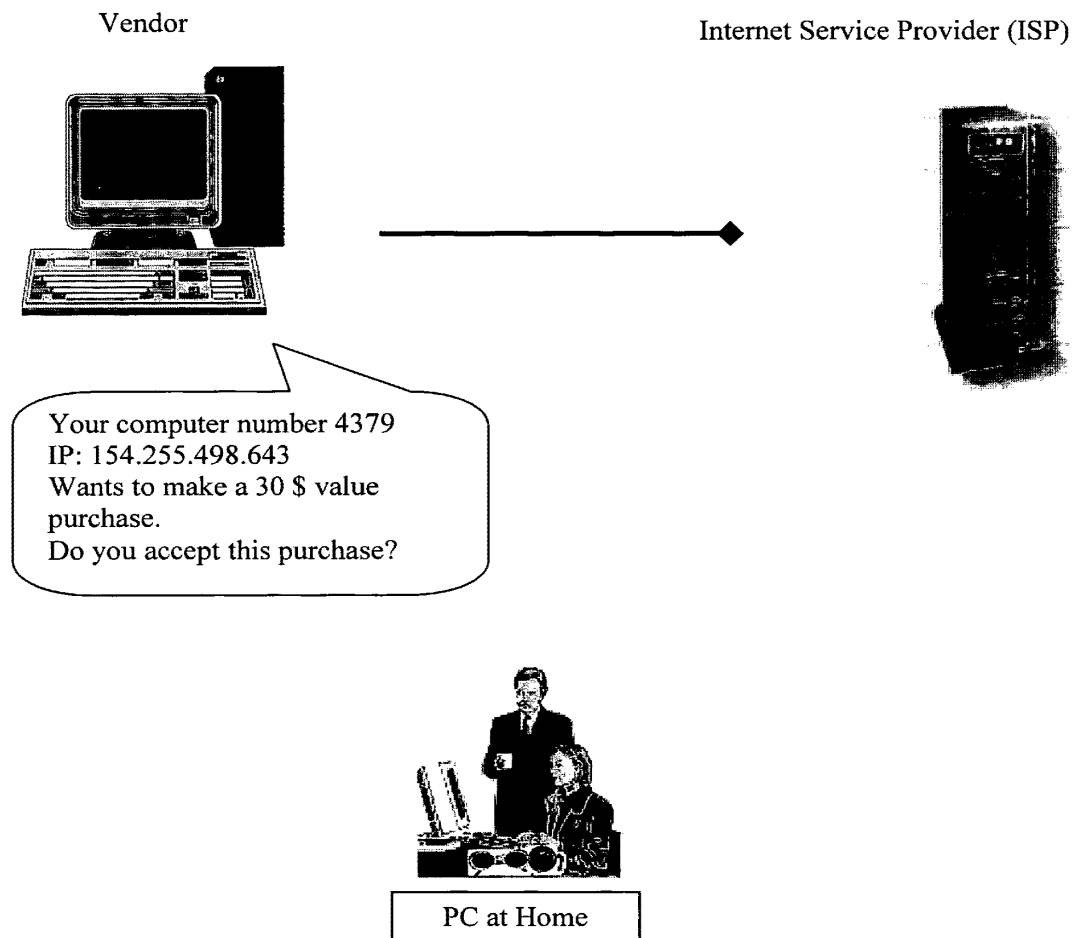


PC at Home

I am Mr. Smith  
ID # 16495358-4379  
HP: 154.255.498.643  
Purchase a Beatles Book, Item  
number 6546/12  
Price 30 \$

2/12

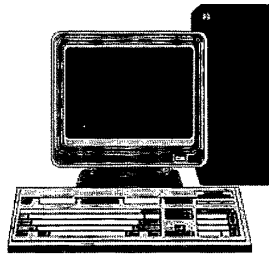
FIG. 2



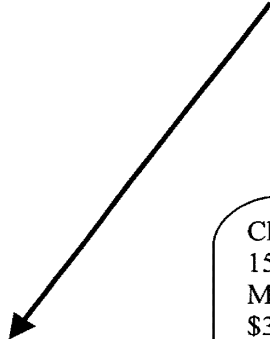
3/12

FIG. 3

Amazon Shop (Vendor)



Internet Service Provider (ISP)



PC at Home

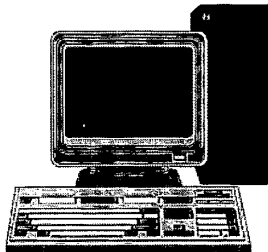
Checking IP:.....  
154.255.498.643  
Mr. Smith do you accept a  
\$30  
Value purchase that you  
made in the Amazon Book  
Shop?  
If yes enter your password.



4/12

FIG. 4

Amazon Shop (Vendor)



Internet Service Provider (ISP)



PC at Home

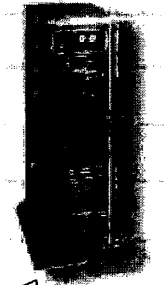
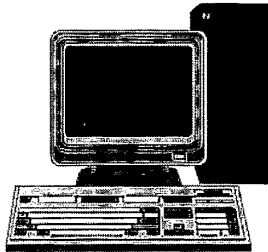
I do accept a 30 \$ value purchase that I made in the Amazon Book Shop.  
My password is \*\*\*\*\*

5/12

FIG. 5

Amazon Shop (Vendor)

Internet Service Provider (ISP)



Confirm transaction # 123456789  
Send invoice to ISP # 16495358



PC at Home

FIG. 6

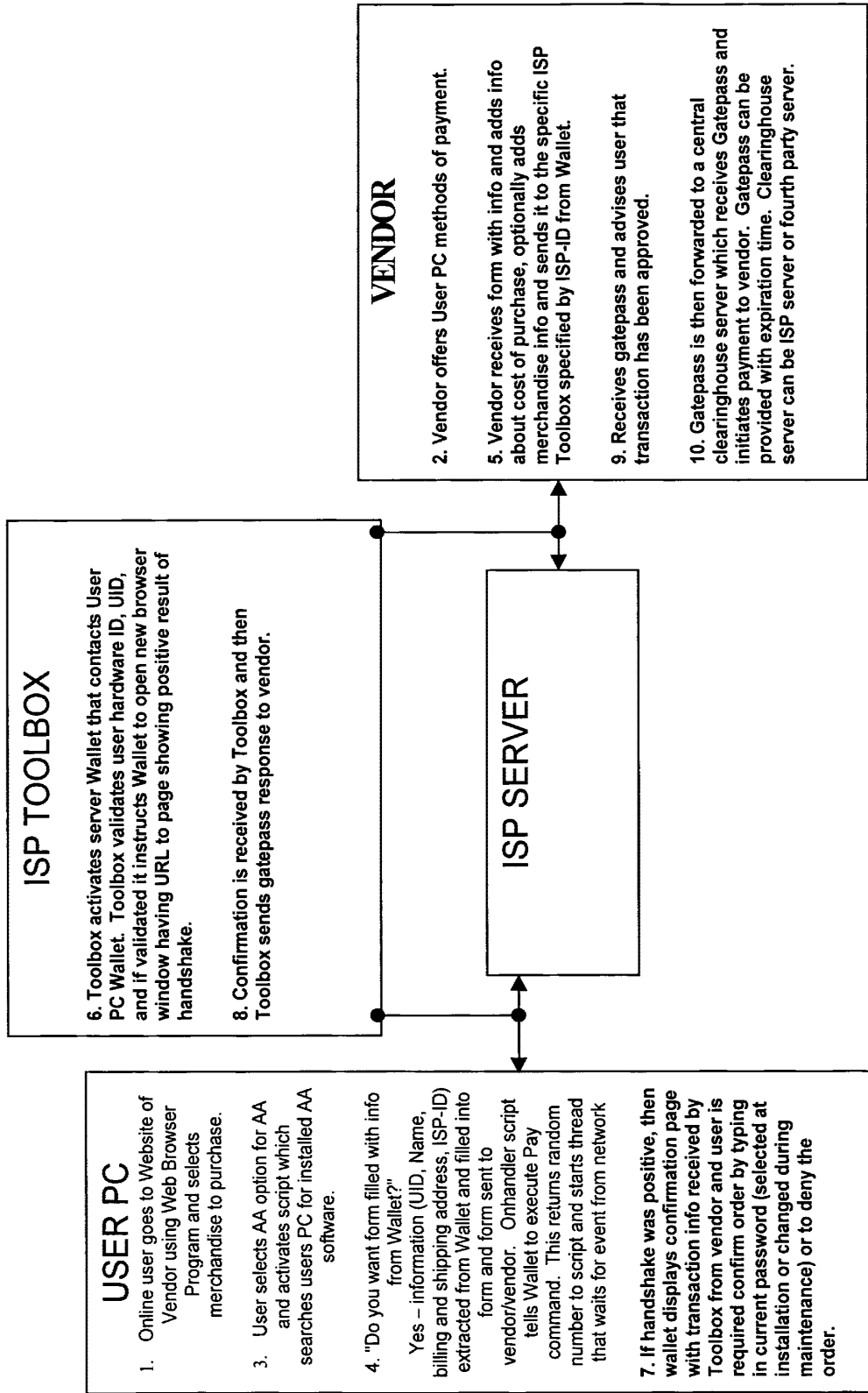


FIG. 7

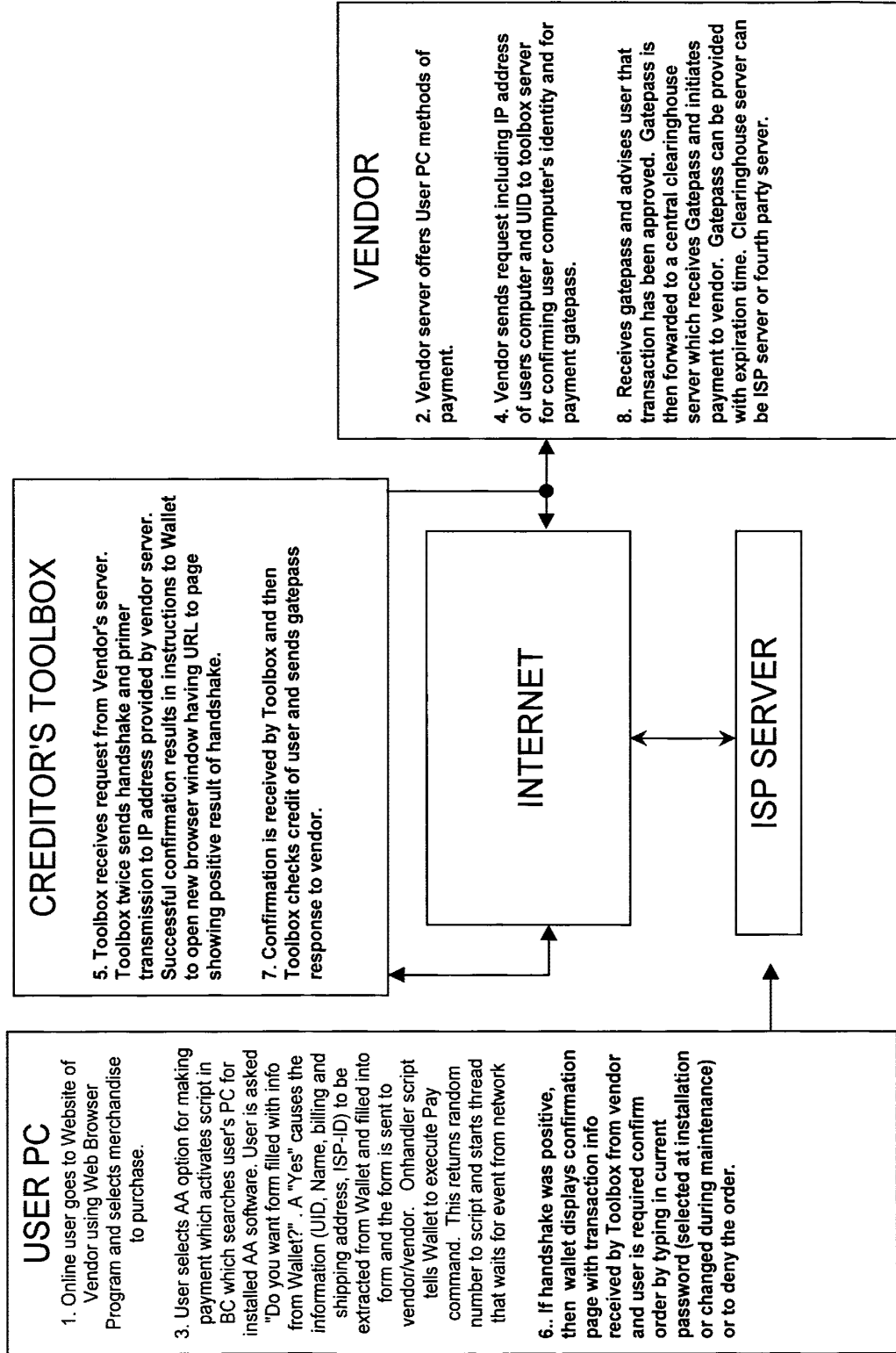
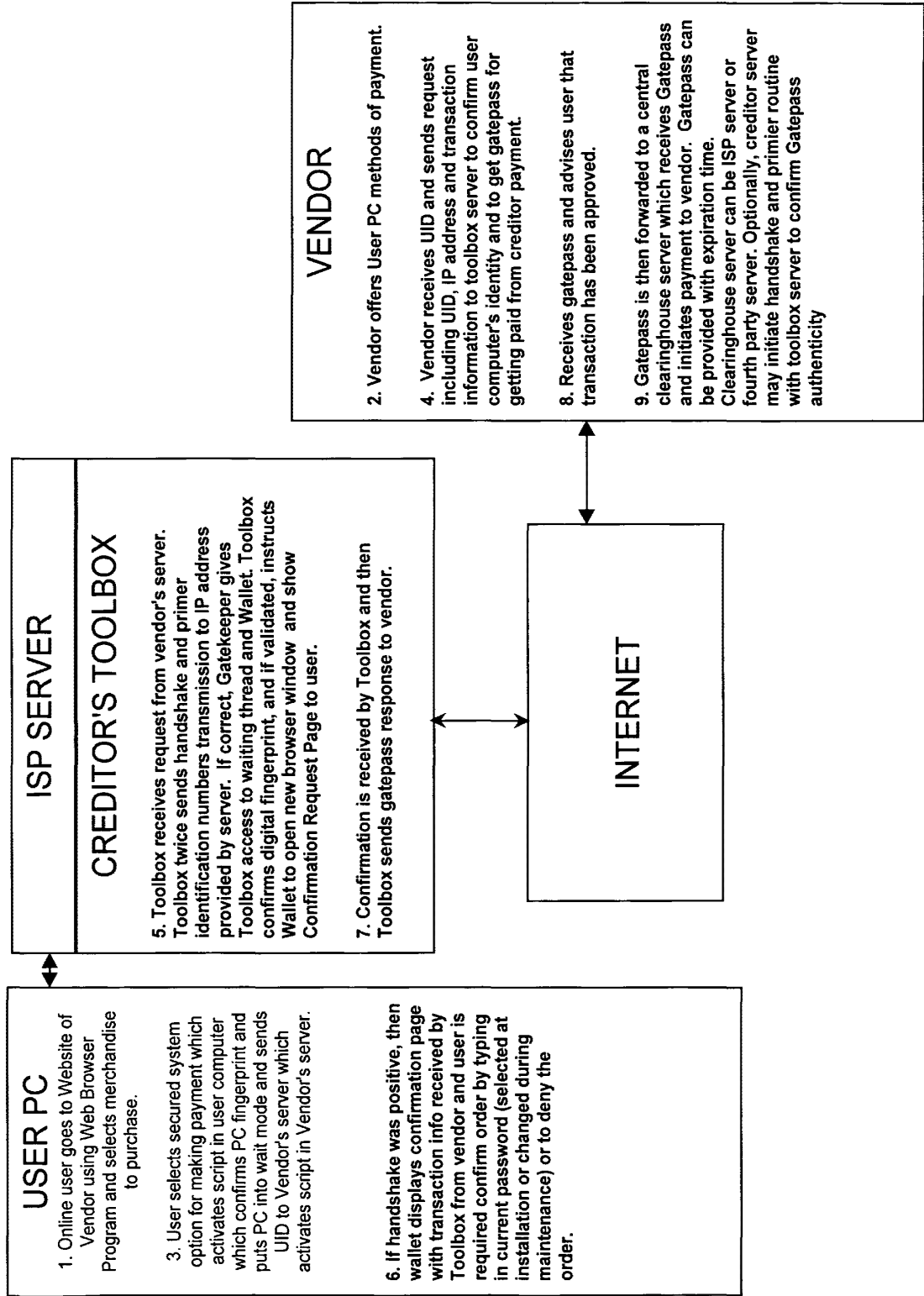


FIG. 8



9/12

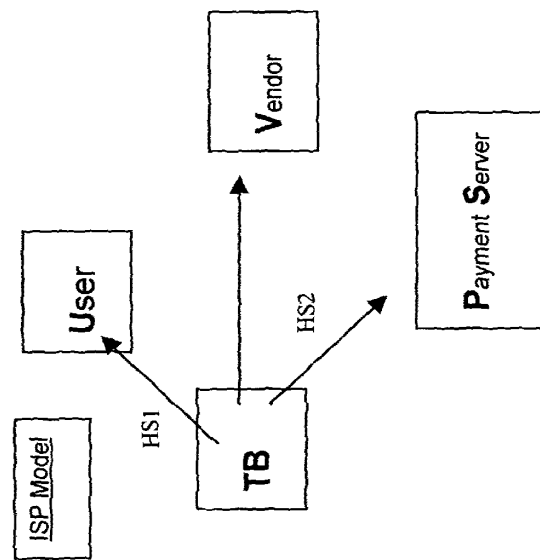


FIG. 9

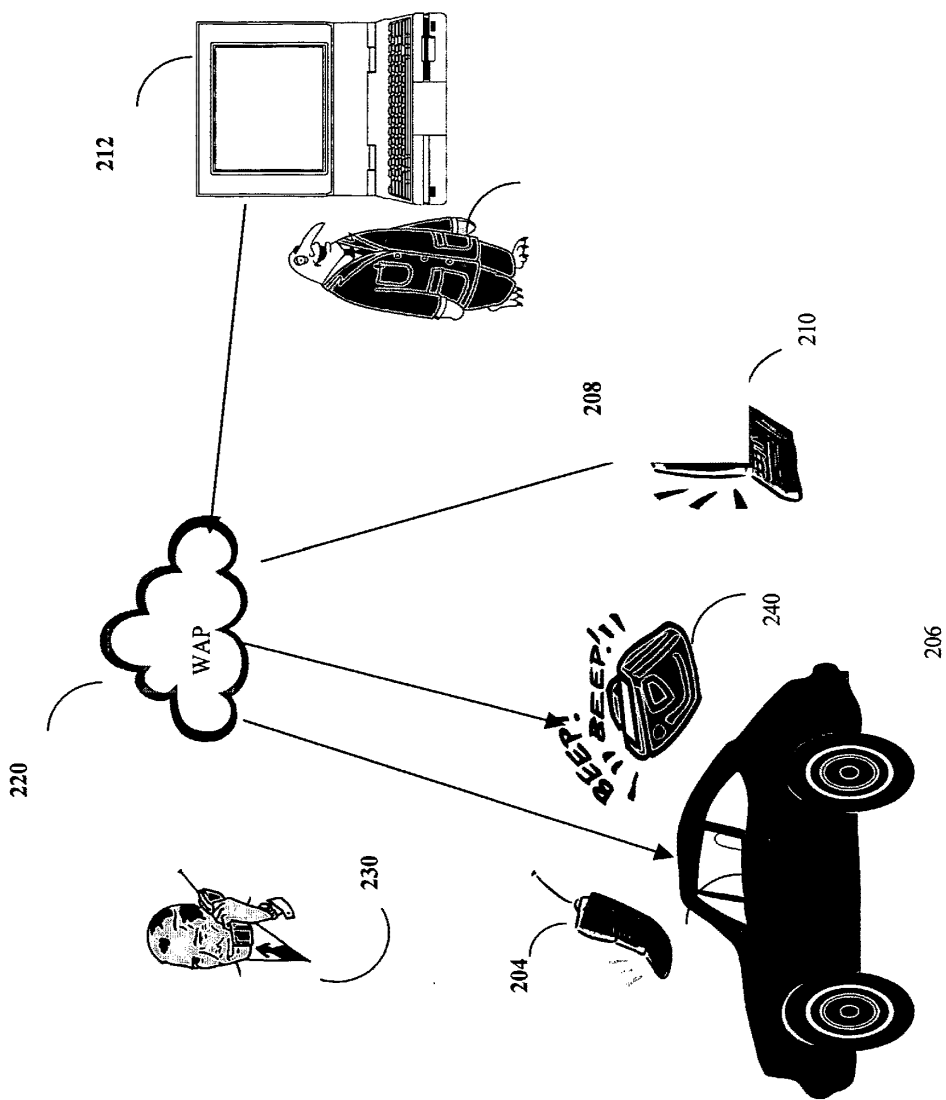
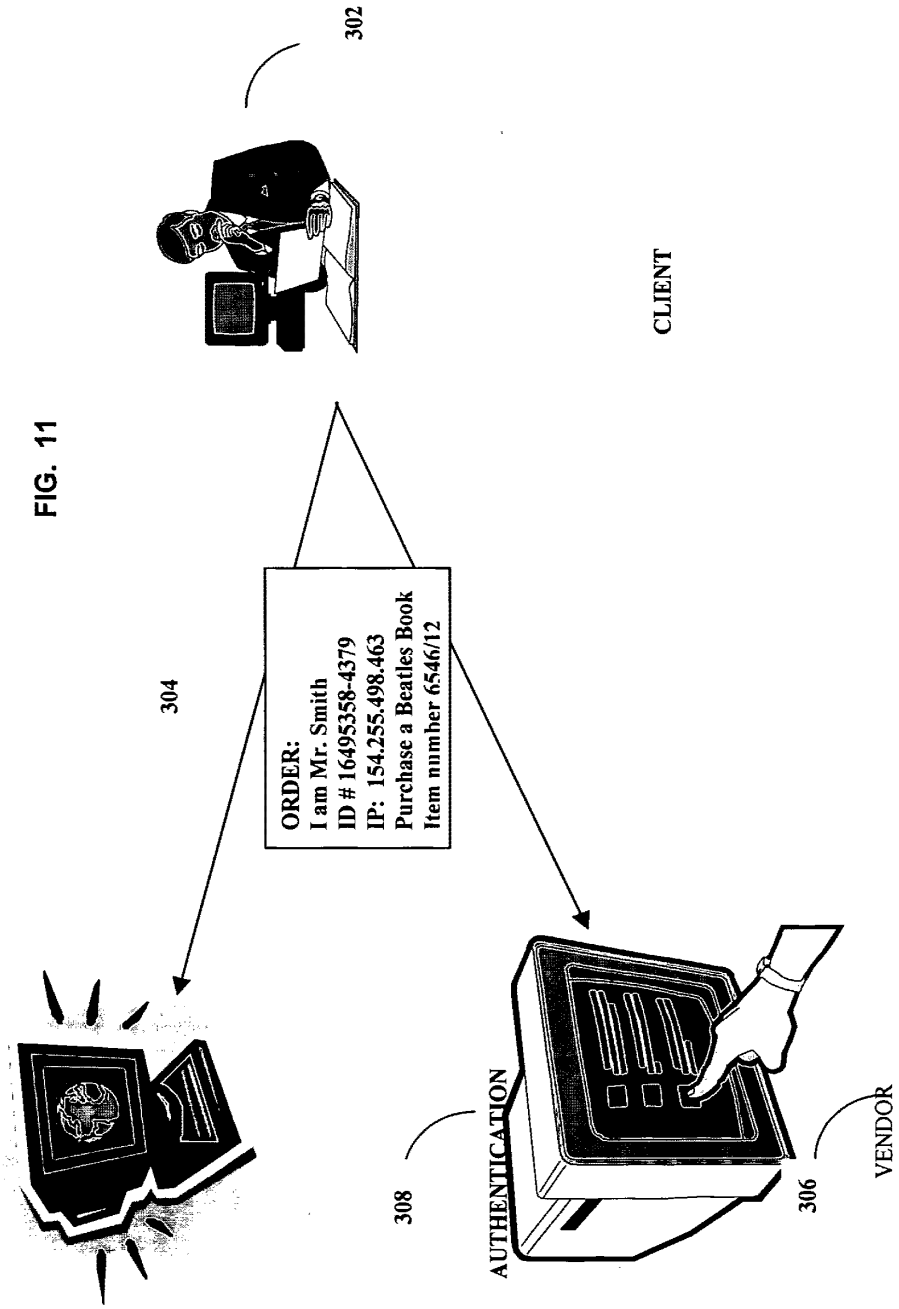


FIG. 10

11/12

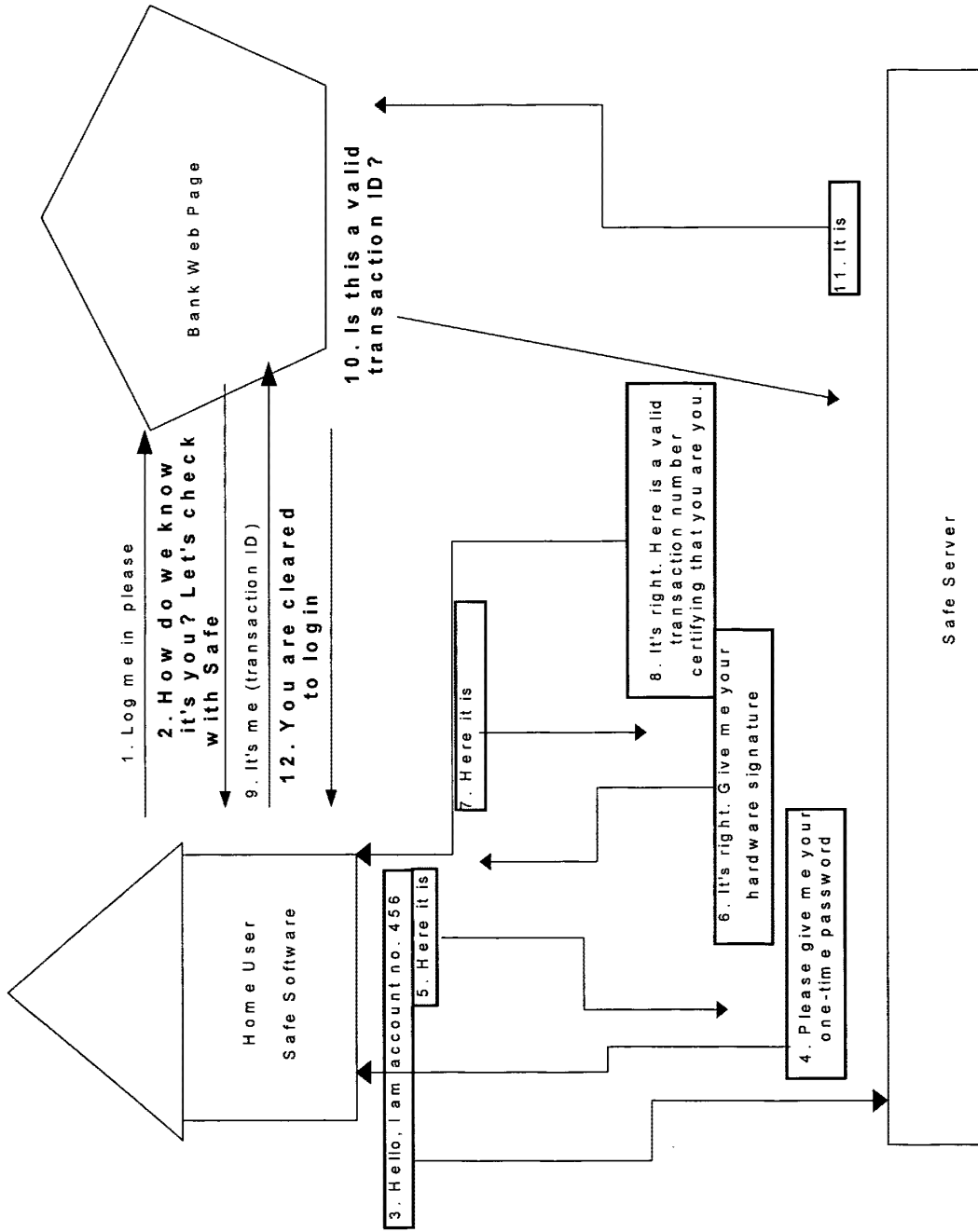


SUBSTITUTE SHEET (RULE 26)



12/12

FIG. 12



SUBSTITUTE SHEET (RULE 26)

**INTERNATIONAL SEARCH REPORT**

Internat'l Application No  
PCT/US 00/21058

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
IPC 7	G07C9/00	G07F7/10 G06F17/60
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols)		
IPC 7 G07F G06F G07C		
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		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 899 980 A (RUVIO GUY ET AL) 4 May 1999 (1999-05-04)	1,2,9,10
Y	column 1, line 55 -column 4, line 51 column 5, line 58 -column 7, line 20 column 11, line 10 -column 12, line 5; figures	4,5
X	WO 98 47116 A (ERICSSON TELEFON AB L M) 22 October 1998 (1998-10-22)	1,14
Y	column 2, line 25 -column 3, line 7 column 8, line 20 -column 9, line 29 column 12, line 26 -column 13, line 16 column 16, line 14 -column 17, line 26; figures 3A-3C,5A-5C	11-13
X	US 5 794 221 A (EGENDORF ANDREW) 11 August 1998 (1998-08-11)	1,9,10
A	the whole document	6
	--- -/--	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> 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. *Z* document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
18 January 2001		29/01/2001
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  Paraf, E

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

INTERNATIONAL SEARCH REPORT

International Application No  
PCT/US 00/21058

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 648 648 A (CHOU KEN W ET AL) 15 July 1997 (1997-07-15) column 1, line 57 -column 3, line 25; claim 5; figure 1 ----	4,5
Y	US 5 907 617 A (RONNING JOEL A) 25 May 1999 (1999-05-25) column 1, line 35 -column 2, line 40; claim 1; figure 1 ----	11-13
A	WO 99 31610 A (BRITISH TELECOMM ;LEVERIDGE PHILIP CHARLES (GB)) 24 June 1999 (1999-06-24) page 3 -page 5; figures ----	1,5,9
A	US 5 852 812 A (REEDER MARY) 22 December 1998 (1998-12-22) abstract; claim 7; figures 1-3 ----	1,9
A	WO 98 59455 A (PERETTI GIULIO) 30 December 1998 (1998-12-30) page 2, line 25 -page 5; figure 1 -----	1,9

Form PCT/SA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/21058

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5899980     A	04-05-1999	AU 8644298 A	01-03-1999
		BR 9814041 A	03-10-2000
		CN 1270682 T	18-10-2000
		EP 1031106 A	30-08-2000
		WO 9908218 A	18-02-1999
		NO 20000563 A	11-04-2000
WO 9847116     A	22-10-1998	AU 7094398 A	11-11-1998
		BR 9808534 A	23-05-2000
		CN 1260895 T	19-07-2000
		EP 0976116 A	02-02-2000
		NO 995031 A	16-12-1999
US 5794221     A	11-08-1998	AU 5986596 A	10-02-1997
		CA 2226253 A	30-01-1997
		EP 0845125 A	03-06-1998
		JP 2000505568 T	09-05-2000
		WO 9703410 A	30-01-1997
US 5648648     A	15-07-1997	NONE	
US 5907617     A	25-05-1999	AU 6269796 A	30-12-1996
		CA 2223409 A	19-12-1996
		EP 0870381 A	14-10-1998
		WO 9641449 A	19-12-1996
WO 9931610     A	24-06-1999	AU 1570399 A	05-07-1999
		EP 1040437 A	04-10-2000
US 5852812     A	22-12-1998	NONE	
WO 9859455     A	30-12-1998	IT T0970546 A	23-12-1998
		AU 7917398 A	04-01-1999
		EP 0996939 A	03-05-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 March 2008 (27.03.2008)

PCT

(10) International Publication Number  
**WO 2008/034900 A1**

- (51) International Patent Classification:  
**G06F 21/22** (2006.01)
- (21) International Application Number:  
PCT/EP2007/060056
- (22) International Filing Date:  
21 September 2007 (21.09.2007)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
- |               |                                |    |
|---------------|--------------------------------|----|
| PA 2006 01221 | 21 September 2006 (21.09.2006) | DK |
| 60/874,955    | 15 December 2006 (15.12.2006)  | US |
| 60/907,465    | 3 April 2007 (03.04.2007)      | US |
| PA 2007 01237 | 30 August 2007 (30.08.2007)    | DK |
| 60/935,769    | 30 August 2007 (30.08.2007)    | US |

(74) Agent: INSPICOS A/S; P.O. Box 45, Bøge Allé 5, DK-2970 Hørsholm (DK).

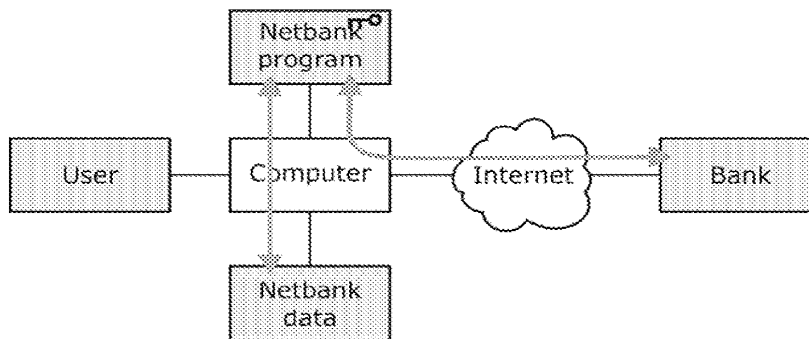
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant and  
(72) Inventor: **BOESGAARD SØRENSEN, Hans Martin**  
[DK/DK]; Ulrikkenborg 10A, 1., DK-2800 Lyngby (DK).

Published:  
— with international search report

(54) Title: FABRICATION OF COMPUTER EXECUTABLE PROGRAM FILES FROM SOURCE CODE



WO 2008/034900 A1

(57) Abstract: A method for protecting a computer program against manipulation and for shielding its communication with other programs against eavesdropping and modification is presented. The method comprises the creation of individualized program copies to different groups of users, the insertion of or the derivation of individual cryptographic keys from the program code, the obfuscation of the program code, and the self-authentication of the program towards other programs. The method is suitable for the protection of online banking, online investment, online entertainment, digital rights management, and other electronic commerce applications.

## FABRICATION OF COMPUTER-EXECUTABLE PROGRAM FILES FROM SOURCE CODE

FIELD OF THE INVENTION

- 5 The present invention is generally concerned with securing computer programs, network communication, and stored data against attacks.

BACKGROUND OF THE INVENTION

- 10 The increase in electronic commerce in recent years has also led to a rapid growth in computer crime. In particular, authenticating transactions over computer networks proved to be a major target of attacks, using a variety of techniques such as phishing. As an example, at the time of this writing, almost all major banks worldwide are under attack by various forms of identity theft, and while the financial losses are significant, the more important  
15 danger is that of bank users losing confidence in online banking.

- It has become clear that the old recipes for protecting client-server connections over insecure networks (as e.g. user passwords or their combination with one-time passwords) no longer provide the necessary level of security. Attackers use a combination of more and more  
20 advanced techniques, such as man-in-the-middle attacks, phishing, DNS spoofing, and malware (viruses, Trojan horses). In this context, new protection techniques are required to secure financial online transactions.

- The present invention can prevent most man-in-the-middle, phishing, and malware attacks  
25 on for example online banking applications, online investment applications, and online entertainment applications.

SUMMARY OF THE INVENTION

- 30 *Nomenclature*

Some of the terms used in this document are described in the following:

- Argument: An input, e.g. to a function, a server, or a HTTP request  
35 Asymmetric key: A cryptographic key to be used in an asymmetric algorithm.  
Asymmetric algorithm: An algorithm using one key for encryption and another key for decryption or an algorithm using one key for signing and another key for verifying the signature, Can for example be RSA or ECC.  
Authentication tag: See tag.

SUBSTITUTE SHEET (RULE 26)

- Block cipher: An encryption/decryption algorithm operating on plaintext / ciphertext blocks of fixed length. Can for example be AES or 3DES. Also see [Sc96] pp. 4 and 189-211.
- Cipher: See encryption / decryption algorithm.
- 5 Ciphertext: An encrypted string.
- Client application: A computer program that can connect to a server application. An application being a client towards a server might also be a server towards another client.
- 10 Composition: In this text, the composition of a function or algorithm that is different for each copy denotes the functionality of the specific function or algorithm in a specific copy. For example, one composition can be  $f(x) = 3x + 4$  and another composition can be  $f(x) = 7x - 2$ .
- Computer-executable program file: For example an .exe, .dll, .ocx, .class, or .jar file.
- 15 Copy: Two different copies of a computer program have the same overall features but may have different internal functions, e.g. key generators.
- Cryptographic algorithm / function: In this text, this denotes a mathematical function (or its implementation) that is used for communication or storage in the presence of an adversary. Examples include encryption / decryption algorithms, message authentication codes (MAC), or hash functions.
- 20 Digital document: Includes HTML, XHTML, XML, PDF, word process files, and spread sheet files.
- Encryption / decryption algorithm: An encryption algorithm encodes data under a key such that it cannot be distinguished from random data. A decryption algorithm reverses the encryption algorithm and restores the original data, using a key. Can e.g. be a block cipher, a stream cipher or an asymmetric cipher. Also see [Sc96] pp. 1-5.
- 25 Hash function: A function that takes a string of any length as input and returns a string of fixed length as output. The function achieves a strong mixing of the string, and its output can be used as a short identifier for the input. Examples are collision resistant hash functions, one-way functions, or any family of pseudo-random functions). Also see [Sc96] pp. 30-31.
- 30 IV: Initialization vector. A publicly known string that is used to avoid that a cryptographic algorithm always produces the same output.
- Key: A string usually known only by some parties. Keys are used as input to cryptographic algorithms. Also see [Sc96] p. 3.
- 35 MAC function: A message authentication code (or MAC) takes a key and a data string as input and produces an authentication tag as output. If the key is a secret shared by sender and receiver and if the tag is appended to the message,

the receiver can re-run the MAC to verify that the data has not modified since it was written. Also see [Sc96] p. 31.

One-time password (OTP) or one-time key (OTK): A key or password used only once, e.g. for authenticating a user.

- 5 Plaintext: An un-encrypted string.
- PRNG: A pseudo-random number generator (or PRNG) takes a seed as input and generates an output string of arbitrary length. If the key is not known, the output string cannot be distinguished from random. Also see "pseudorandom sequence generator" in [Sc96] pp. 44-45.
- 10 Seed: Input to a PRNG.
- Server application: A computer program that can receive connections from a client application and/or provide services to a client application.
- Server: Software (i.e. server application), hardware, or combination thereof that can receive connections from a client application and/or provide services to a client application.
- 15 Source code: For example the content of a .java, .c, .cpp, .h, or .pas file.
- Stream cipher: An encryption/decryption algorithm operating on streams of plaintext or ciphertext. Also see [Sc96] pp. 4, 189, and 197-199.
- String: A block of data. Can be a text string (a set of characters) or a binary string (a set of bits).
- 20 Symmetric key: A cryptographic key to be used in a symmetric algorithm.
- Symmetric algorithm: An algorithm using the same key for both encryption and decryption or for both creating an authentication tag and verifying an authentication tag. Can for example be a block cipher, a stream cipher, or a MAC function.
- 25 Tag: Output of a MAC function.
- Time stamp: A string containing information about date and/or time of day.
- Version: Two different versions of a computer program have different features. Usually, a new version has more or better features than the previous version.
- 30 XOR: Binary operation often denoted by  $\oplus$ .  $0 \oplus 0 = 0$ ,  $0 \oplus 1 = 1$ ,  $1 \oplus 0 = 1$ , and  $1 \oplus 1 = 0$ .

[Sc96]: Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996.

### 35 *Introduction*

In a first aspect, the invention provides a method of fabricating computer-executable program files from a source code, the method comprising the step of embedding, in each of the fabricated computer-executable program files, at least one value or means for generating



at least one value, said value being uniquely selected or generated for each of the fabricated computer-executable program files, whereby all of the fabricated computer-executable program files are capable of carrying out instructions defined by the source code, and whereby each individual computer-executable program file is capable of generating a unique  
5 output, which depends on said uniquely selected or uniquely generated value.

It will hence be appreciated that the method of the first aspect of the present invention fabricates unique copies of a computer program (computer-executable program file), i.e. copies that are all capable of carrying out the same instructions to perform identical  
10 operations in terms of overall functionality. However, the copies fabricated by the method of the first aspect of the invention all differ from each other in that each copy is capable of generating a unique output.

It will be understood that, in embodiments of the method according to the present invention,  
15 the at least one value may be embedded as a static value. Alternatively, the at least one value may be generatable by the means for generating the value. The means for generating the value may be generated at the stage of fabricating the computer-executable program files. The means for generating the value are preferably adapted to generate the value at runtime of the computer-executable program files.

20

The unique output is normally generated at runtime of the computer-executable program files, but may also be embedded as a static value, which is generated at the fabrication stage.

25 In preferred embodiments of the invention, the means for generating the at least one value may comprise computer program functionality, such as source code, e.g. in macro or script language, or compiled code capable of generating the value.

The unique output is preferably reproducible by another program or accessible by another  
30 program. For example, different copies of the computer-executable program files fabricated by the present method may be distributed to different users, such as users in a computer network, such as online banking users. The other program capable of reproducing or accessing the unique output may, for example, be running on a server in the computer network, such as a server run by a bank. Hence, the unique output may be used as a  
35 common secret or used to generate a common secret, such as one or more encryption keys.

Whereas it has hitherto been a paradigm in the art of computer programming that all copies of a program were identical in all respects, the present invention relies on the fundamental principle that all copies are deliberately made non-identical. This brings about the advantage

that it is rendered impossible to design a hacking tool capable of generally attacking the computer-executable program files fabricated by the present invention. For example, if an encryption key is hacked, this key is of no use if applied in a copy of the program different from the original unique copy of the program.

5

Preferably, the unique outputs of two copies of the computer program are uncorrelated, i.e. with the knowledge of one output, one cannot predict the unique output provided by another copy of the computer program.

- 10 For example, the computer-executable program files fabricated may be capable of carrying out online banking transactions. Hence, all copies of the program files will appear identical to users, i.e. all user interfaces are identical, and the programs carry out identical operations, except with regard to the unique output, which is different between different copies of the program files. The operations carried out by all copies of the computer program may e.g.
- 15 include prompting for user id and password, offering various functionalities, such as money transactions, account inquiries, etc.

- In most envisaged embodiments of the invention, the unique output produced by each individual copy of the program files is preferably not visible to or accessible by users. Such
- 20 embodiments include, in particular, most online banking applications, media players, anti virus programs, other security programs, financial programs, games, distributed computing applications, DRM applications. However, the unique output may for certain applications be made visible to or accessible by users. For example, the output may be made available to users for debugging purposes.

25

The method according to the first aspect of the invention is preferably carried out on a device capable of automatically carrying out instructions as provided in a program. Preferably, the method is implemented on an electronic device including an electronic processor, such as a computer including a CPU.

30

From the above description, it will be appreciated that each user or group of users preferably uses (is provided with) a different copy of the computer-executable program file. Whereas for certain applications it may be acceptable that the same copy is provided to two different users among many users, it is usually preferred that a copy provided to a user is not re-used,

35 i.e. is not provided to another user.

The embedded means for generating the at least one value may depend on at least one embedded value. The means for generating the at least one value may, for example, include a key generator for generating an encryption key, which is unique in respect of a particular

copy of the program. The key generated by the key generator may depend from a value, which is specific for one single copy of the program file, and which has been embedded at the fabrication stage. In preferred embodiments, key generators of different copies of the program use different arithmetic functions as well as different embedded values to enhance security.

The process of fabricating computer-executable program files from a source code may be divided into at least two steps. In a first step, which is performed once, source code is converted into at least one intermediate file, such as a machine-code or object file. In a second, subsequent step, the at least one intermediate file and optionally other files are converted into the computer-executable program file. The second step is performed for each computer-executable program file. Thereby, fabrication is facilitated, as the first fabrication step, which is common to all copies, is only performed once.

At least a part of the source code used as input to the fabrication process may be evaluated to determine if it meets one or more predefined criteria for being equipped with the at least one embedded value or means for generating the at least one value. For example, at the step of fabricating, it may be determined if the computer-executable program file(s) to be used as input is intended to be capable of exposing confidential data. If this is the case, the fabrication software may be setup to deny fabrication.

The embedded means for generating the at least one unique value may comprise at least one extractor subfunction, as described in further detail below. The extractor subfunction(s) may be uniquely selected for each computer-executable program file.

As discussed, the unique output may be used to generate a cryptographic key, or used itself as a cryptographic key. Such key may e.g. be used to generate an authentication tag for authenticating data or for authenticating the program itself or other programs, or for authenticating the execution environment, in which the program is run. The execution environment to be authenticated may e.g. include an operating system, internet browser, or external software components.

The at least one embedded value or means for generating at least one value may be used as a serial number or to derive a serial number that can be used, e.g. by server software, to identify the copy of the computer program. For example, the server may include a database, from which the internal structure of the specific copy of the program can be derived, e.g. to reconstruct a key generator. In other words, information about how a computer-executable program file is generated can be stored, such that the computer-executable program file can

be reproduced or its functionality or part thereof can be reproduced or simulated, for example by a server.

5 The at least one embedded value or the means for generating the value may be constructed by an algorithm using a pseudo-random number generator (PRNG). Hence, the fabrication method may include the following steps:

1. choosing a PRNG seed,
2. generating a string of pseudo-random bits from the PRNG seed using a pseudo-random number generator,
- 10 3. using the string of pseudo-random bits to determine at least one embedded value or how to construct the embedded means for generating at least one value.

Hence, if the PRNG seeds and the serial numbers of the individual copies of the program are stored, the embedded value or means for generating the value, e.g. a key generator, may be reproduced at a later stage, e.g. by a server.

15

To enhance security, the computer-executable program files may be obfuscated. More specifically, obfuscation renders it more difficult to extract, for example, a key generator from the fabricated program files, and patching of the fabricated program files is also rendered difficult.

20

The obfuscation method may depend random or pseudo-random data, so that its output varies in accordance with that data. Hence the obfuscation output may vary to further enhance security. Thus, if the obfuscation method is applied more than once to the same input (such as e.g. a source code or a compiled version of a program), the two obfuscated outputs will not be identical.

25

At least a part of the computer-executable program file may be stored in encrypted form and may be decrypted at runtime. For example, an unencrypted part of the program file may be used to initiate operation or setup of the program, e.g. to contact a server with a request for a decryption key for decrypting the remaining part(s) of the program file. The decryption key provided by the server may be provided in encrypted form and may be decrypted by the program file, using a cryptographic key derived from the unique output.

30

The fabricated computer-executable program file including the at least one embedded value or embedded means for generating at least one value may contain program code that can read profile data, such as:

35

- brand, type, version, or serial number of a hardware component,
- brand, type, version, or serial number of a software component,
- software or hardware configuration data,

- network configuration data, and
- identity of the user

where the profile data is used as input to the means for generating at least one value. It may thereby be ensured that the program is not executable on any other system (or in any other  
5 environment) than the one, at which it is intend to run. Alternatively, the program may include functionality allowing the profile data to be submitted to a server to allow the server to determine if the program is executed in an allowable environment.

As described further below in connection with Fig. 14, data may be sent in encrypted or  
10 authenticated form between a first and a second program (programs *C* and *D* in Fig. 14). The encryption/decryption key or authentication key may be derived from the at least one embedded value or means for generating the at least one value in the first program program *C*. The encryption/decryption key or authentication key may be derived in the second  
15 program *D* from knowledge about the at least one embedded value or means for generating at least one value in the first program *C*.

As described further below in connection with Fig. 15, data may be sent in encrypted or  
authenticated form between third and fourth programs, *G* and *H* in Fig. 15. The programs *G*  
20 and *H* both communicate securely with server *I* using cryptographic keys derived from *G*'s and *H*'s at least one embedded value or means for generating the at least one value. The server *I* provides at least one cryptographic key to *G* and *H* to be used to encrypt/decrypt or  
authenticate at least a part of the data sent between *G* and *H*.

The present invention further provides a server from which computer-executable program  
25 files fabricated according to the fabrication method described above can be downloaded. Further, the invention provides a server communicating with a computer-executable program file fabricated according to the present fabrication method.

The invention further provides a document into which at least one computer-executable  
30 program file fabricated according to the present invention is embedded. Further, the invention provides a computer on which at least one computer-executable program file fabricated according to the present invention is stored or executed. Further, the invention provides a computer program for fabricating computer-executable program files from source  
35 code, the computer program comprising means for performing the fabrication method according to the present invention. Further, the invention provides a computer-readable data medium comprising such a computer program, and a computer loaded with the computer program. Further, the invention provides a computer-executable program file fabricated by the fabrication method of the present invention.

Still further, the present invention provides a computer program comprising a computer-executable program file fabricated from a source code, the computer program including, in said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the  
5 computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value.

The computer program may include functionality, i.e. program code, to carry out all method  
10 steps described above in connection with the fabrication method of the first aspect of the invention.

The present invention further provides a computer network comprising a server and a plurality of clients, wherein each client is loaded with a copy of a first computer program, and  
15 wherein the server is loaded with a second computer program, each copy of the first computer program comprising:

- a computer-executable program file fabricated from a source code, which is common to all copies of the first computer program;
- at least one embedded value or means for generating at least one value, said value or  
20 said means being included in said computer-executable program file, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the common source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value; the computer  
25 network being programmed to communicate said unique output from each of the clients to the server, so as to enable the second computer program to authenticate each copy of the first computer program based on said output.

Each copy of the first computer program may include functionality, i.e. program code, to  
30 carry out all method steps described above in connection with the fabrication method of the first aspect of the invention.

The invention also provides a server for use in the above-described computer network, the server being suited for communication with said plurality of clients via the computer network,  
35 said second computer program being adapted to authenticate each copy of said first computer program based on said unique output.

The invention further provides a server communicating with a client computer program comprising a computer-executable program file fabricated from a source code, the computer

program including, in said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of  
5 generating a unique output, which depends from said uniquely selected or uniquely generated value.

The computer-executable program file may include functionality, i.e. program code, to carry out all method steps described above in connection with the fabrication method of the first  
10 aspect of the invention.

The server may include functionality that allows it to recreate at least one of

- at least one of the at least one embedded values, and
- at least a part of the embedded means for generating at least one value

15 as is embedded in a client program.

The server may further include functionality allowing it to load, from a database or file, at least one of

- at least one of the at least one embedded values, and
- at least a part of the embedded means for generating at least one value

20 as is embedded in a Client Program.

Using a online banking application as example, figure 1 shows an attack scenario. In the top, we have the bank, which is considered secure. Below that, we have the Internet which  
25 connects the users' computers to the bank. From left, we have three legal users, who want to use the online banking application to conduct transactions. But at the right, we have an attacker who wants to make money by modifying other users' transactions or by fabricating transactions that to the bank look like transactions authorized by other users.

30 Figure 2 shows the components involved in online banking. The user and the bank are considered secure, but the online banking program, the computer, the data stored on the user's computer by the online banking program, and the Internet can be under control of an attacker. This can be used by the attacker to trick the user and/or the bank to modify or make transactions in the attackers favor.

35 Figure 3 shows how the present invention can improve the security of online banking. By inserting a key generator in the online banking program ("netbank program" in the figure), the online banking program's authenticity can be verified by the banking. Thus, the online banking program will be secure. Using this key generator, a secure link can be established to

the banking (illustrated by the green arrow between the online banking program and the bank), and finally, online banking data stored on the user's computer can be protected (illustrated by the green arrow between the online banking program and the online banking data ("netbank data" in the figure). This solution leaves only one weakness: the link between  
5 the user and the online bank program (i.e. the user interface).

*Key generator*

10 In one embodiment of the present invention, a key extractor is embedded into a computer-executable program file. This key extractor may take an extractor IV as input and generates an extracted key as output (see left part of figure 4). The extracted keys can for example be used as key in cryptographic functions.

15 In one embodiment of the present invention, computer-executable program files are generated in a way such that one or more unique strings are embedded into each copy. These one or more unique strings can for example be used as parameters to a key extractor in order to generate keys that are unique for each copy, as serial numbers, or as keys in cryptographic functions.

20 In one embodiment of the present invention, the extractor function always returns a constant string. Thus, the extracted key is a constant.

In one embodiment of the present invention, the extractor function is build as shown in figure 5:

- 25
- The function has a number of inner state words (their initial values are  $W_1$ ,  $W_2$ ,  $W_3$ , and  $W_4$  in the figure).
  - A number of extractor subfunctions ( $F_1$ ,  $F_2$ , ...  $F_n$  in the figure) are manipulating the inner state words.
  - The resulting inner state words are manipulated (the L function in the figure) in order  
30 to generate the extracted key.

Each extractor subfunctions can take one or more inner state words as input and can change the value of one or more inner state words. One or more of the initial values of the inner state words ( $W_1$ ,  $W_2$ ,  $W_3$ , and  $W_4$  in the figure) may be derived from an extractor IV. There can be one or more inner state words. One or more of the extractor subfunctions may  
35 depend on an extractor IV or value derived thereof. One or more of the extractor subfunctions may depend on a constant value.

In one embodiment of the present invention, extractor subfunctions are chosen from a set of available extractor subfunctions when the computer-executable program file containing an



extractor function is generated. The set of available extractor subfunctions can be defined in the program generating the computer-executable program files containing an extractor function.

- 5 The function combining the inner state words into the extracted key (the L function in figure 5) can for example consist of one or more of:
- A concatenation of the inner state words.
  - A hash function
  - A MAC function
  - 10 • An encryption function; e.g. one block cipher operation for each state words using the state word as key, forwarding the output (ciphertext) to the next as input (plaintext). The output of the last operation is the extracted key.

In one embodiment of the present invention, the extractor function is build as shown in figure 15 6:

- Initial values of the inner state words are generated from the extractor IV by a function (the J function in the figure).
- A number of extractor subfunctions are manipulating the inner state words ( $F_1, F_2, \dots F_n$  in the figure).
- 20 • Parameters for the extractor subfunctions are generated from the extractor IV by a function (illustrated by the K function in the figure).
- Constants for the extractor subfunctions ( $C_1, C_2, \dots C_n$  in the figure) are embedded in the computer-executable program file.
- The resulting inner state words are processed by a function to generate the extracted key (the L function in the figure).
- 25

Each extractor subfunction can take one or more inner state words as input and can change the value of one or more inner state words.

- 30 In one embodiment of the present invention, the extractor subfunctions produces a balanced output, are non-linear, and/or are correlation-resistant.

In one embodiment of the present invention, the extractor subfunctions relies on bijective function (e.g. addition, subtraction, xor, or rotating) or on table lookups (e.g. the s-boxes from the encryption algorithm AES).

35

In one embodiment of the present invention, extractor functions have jump instructions. These jump instructions may for example be conditional. The conditional jumps can for example depend on one or more of:

- One or more inner state words.

- The extractor IV.
- A constant value.

5 In one embodiment of the present invention, an extracted key or one or more unique strings are used as input to a blender function (see right part of figure 4). This blender function also takes a blender IV as input and generates a purpose key as output.

10 In one embodiment of the present invention, the output from a key generator (an extracted key) is used as input to a blender function (see figure 4).

In one embodiment of the present invention, a unique key generator function is embedded into each computer-executable program file. The extractor function is or is not different for each copy. The blender function is or is not different for each copy.

15 In one embodiment of the present invention, a blender function relies on cryptographic functions to generate the purpose key from its inputs.

20 In one embodiment of the present invention, a blender function concatenates the blender IV and the extracted key and processes the resulting string (or a string derived thereof) by a hash function. The output from the hash function or a string derived thereof is used as purpose key.

25 In one embodiment of the present invention, a blender function uses the blender IV (or a string derived thereof) as message and the extracted key (or a string derived thereof) as key to a MAC function. The output of the MAC function (or a string derived thereof) is used as purpose key.

30 In one embodiment of the present invention, a blender function uses the blender IV (or a string derived thereof) as plaintext and the extracted key (or a string derived thereof) as key to a block cipher. The output of the block cipher (or a string derived thereof) is used as purpose key.

35 In one embodiment of the present invention, a blender function uses the blender IV (or a string derived thereof) as key and the extracted key (or a string derived thereof) as plaintext to a block cipher. The output of the block cipher (or a string derived thereof) is used as purpose key.

In one embodiment of the present invention, the key generator consists of a constant string that directly or after manipulation is used as key for a block cipher. The generator IV (or a

string derived thereof) is used as plaintext and the cipher text output (or a string derived from it) is used purpose key.

5 In one embodiment of the present invention, the key generator consists of a constant string that is concatenated with the generator IV or by other means combined with the generator IV. The resulting string is hashed and the resulting string (or something derived from it) is used as purpose key.

10 In one embodiment of the present invention, an extractor IV and/or a blender IV are derived from a key generator IV.

In one embodiment of the present invention, a key generator IV is derived from a counter value.

15 In one embodiment of the present invention, a key generator IV is derived from a time stamp.

In one embodiment of the present invention, several purpose keys are generated from one key generator IV. This can be achieved in several ways, for example:

- 20
- By manipulating the key generator IV before calling the key generator.
  - By manipulating the extractor IV.
  - By manipulating the blender IV.
  - By manipulating the extracted key, e.g. appending a string to it.
  - By manipulating the purpose key returned by the key generator.
- 25
- By manipulating the purpose key returned by the key generator and sending the manipulated key through a cryptographic function, e.g. a hash function.
  - By using different key generator functions (completely different or with just one or more components different).

30 In one embodiment of the present invention, a purpose key is used as at least one of:

- An encryption key.
- A decryption key.
- An authentication key.
- An authentication value (i.e. a value that can be used to confirm that a computer-executable program file contains a given key generator).

35

In one embodiment of the present invention, data from the user, data about the user, or data from something in the user's possession is included in the key generation process. In this way, user authentication can be embedded into the key generation. Data from the user can

for example be a password, an account number, or a user name. Data about the user can for example be biometric data. Data from something in the user's possession can for example be a one-time password or a short-time password (e.g. from a password generator device) or a key stored in a file on a devices (e.g. a hard disk or a USB memory stick).

5

In one embodiment of the present invention, a computer-executable program file has several key generators.

10 In one embodiment of the present invention, one computer program has a key generator embedded into its program code. Another computer program has knowledge about the composition of the key generator and can, based on this knowledge, reproduce the key generator's functionality and thus its output.

15 In one embodiment of the present invention, the process of generating a computer-executable program file with a key generator comprises generating a random or unique seed string. This seed string is expanded to a longer string using a PRNG. This string (or something derived from it) is divided into substrings used for constructing the extractor function. These substrings can for example choose which extractor subfunctions to use, on which inner state words they operate, or be used as constants given to the subfunctions (e.g. 20  $C_1, C_2, \dots, C_n$  in figure 6). If all non-static information needed to construct an extractor function is derived from the expanded string (and thus from the seed string), knowledge of the seed string is enough to reproduce the complete key generator.

25 In one embodiment of the present invention, computer-executable program files with unique key generators are given unique serial numbers. This serial number can for example be used to look up the copy's PRNG seed in a table or a database. If a party knows the PRNG seeds used to generate a program with a given serial number, that party can reproduce the key generator and thus produce the same keys as the computer-executable program file. The serial numbers can for example be consecutive, random, or encrypted consecutive numbers.

30

In one embodiment of the present invention, a computer-executable program file with a key generator is embedded or included in another file, for example a java archive file (.jar file), an archive file (e.g. a .tar file), a compressed file (e.g. a .gz file), a compressed archive file (e.g. a .zip file), or an install file.

35

#### *Client and server*

In one embodiment of the present invention, a client program has a key generator embedded into its program code and a server has knowledge about the composition of the key

generator. Thus, the client program and the server program can generate the same purpose key given the same key generator IV.

5 In one embodiment of the present invention, client programs with embedded key generators are communicating with one or more server programs. Figure 7 shows an example. The client program generator is a program that can generate client programs with unique embedded key generators. For each client program it has generated, it stores the generated program in a program file database and the program's serial number and PRNG seed in a seed database. The client program can for example be distributed to users via a web server or on optical  
10 media via retail stores or by mail. When the user uses the client program, the client program can communicate with a transaction server using purpose keys generated by the key generator if the transaction server has access to the seed database, since it using the program's serial number (sent from the client program to the server) can find the client program's seed in the seed database and using the seed can reproduce the client program's  
15 key generator.

In one embodiment of the present invention, client programs with embedded key generators are communicating with one or more server programs. The client program generator stores the generated client programs in a program file database and stores the program's serial  
20 number with a program containing only the key generator as embedded in the generated client program in a key generator database. When the user uses the client program, the client program can communicate with a transaction server using keys generated by the key generator if the transaction server has access to the key generator database, since the key generator program can generate the same keys as the client program's key generator.

25 In one embodiment of the present invention, client programs with embedded key generators are communicating with one or more server programs. The client program generator generates client programs with unique key generators on-demand when a user requests a program. When a client program is generated, the serial number and PRNG seed is stored in a seed database. Alternatively, serial number and key generator is stored in a key generator  
30 database.

In one embodiment of the present invention, HTTP caching e.g. by proxy servers is prevented by giving unique names to each computer-executable program file, e.g. by adding a  
35 argument string (e.g. "?rand\_id=0x5E9A005F") to the file name URL, where the hexadecimal number is unique for each user (e.g. stored on user PC in cookie) or unique in general.

*Obfuscation*

In one embodiment of the present invention, the generated computer-executable program file or a part thereof is obfuscated. This obfuscation may make it harder to derive information on how the key generator function is build and/or to make it harder to reverse-engineer the program in general. Furthermore, the obfuscation may make it harder to produce a computer  
5 program that can automatically patch (i.e. modify) the computer-executable program file.

The obfuscation process can for example comprise one or more of the following techniques:

- Replacing a program instruction or a set of program instructions with another program instruction or set of program instructions with equivalent functionality.
- 10 • Reallocate registers, i.e. change the use of processor or co-processor registers.
- Change the order of the program instructions.
- Change the order of functions or program instruction blocks.
- Change loop structure, e.g. inline functions, add meaningless jumps, or replace loop with post-evaluation of condition with loop with pre-evaluation of condition.
- 15 • Inserting useless data or program instructions.
- Interleaving one or more program sequences.
- Reordering of static data.
- Reordering of runtime data.
- Encryption of program instructions.
- 20 • Encryption of static data.
- Replace constant values with code generating the constant values.
- Move static or runtime data between stack, heap, and registers.
- Use several stacks.
- Use several stack pointers to the same stack.
- 25 • Make the program code self-modifying.
- Mix data with program code.
- Rename classes, functions, or variables. (e.g. exported function and variables)
- Rename files or modules.

30 In one embodiment of the present invention, byte code (e.g. Java code) can be obfuscated by removing the structure of the compiled byte code. After normal compilation, source code files (e.g. .java files) are compiled into output files (e.g. .class files). The output files contain information about the program code's interface etc. A group of output files is often combined in an archive file (e.g. a .jar file). These output files are linked together at runtime. The  
35 problem is that all this structure of the compiled code makes the code easier to analyze and reverse-engineer. This structure can, however, be removed by restructuring the code in a way such that functionality from a number of output files is combined into one output file. This may require that the program code can handle some tasks that are normally handled by

the system, e.g. assigning and freeing memory, handling stack, and handling error situations.

5 In one embodiment of the present invention, byte code representing more than one class or more than one function is combined into byte code representing one class or one function. Figure 13 illustrates an example. On the left side, the function A contains program code (the lines with aa, bb, cc, and dd). A also contains a call to the function B and a return statement that returns from the function A. The function B also contains program code (the lines with ee, ff, gg, and hh), a call to the function C, and a return statement. The function C contains  
10 program code (the line with ii) and a return statement. On the right side of the figure, the functions A and B are combined. The combined function is called A and still has all the functionality of the original function A but has the functionality of the function B embedded into it. The beginning of the new function A is similar to the original function A except that the call to B is now a local *jsr* (jump to subroutine) The code from the original function B is  
15 inserted hereafter, but before the original B code, functionality to allocate temporary memory to be used by the functionality of B is added (in the original code this was handled automatically by the runtime environment or operating system as B was a separate function). Similarly, functionality to free temporary memory is added in the end of the original B code. Also, the "return from function" statement is replaced by a local *ret* (retturn from subroutine)  
20 statement. The call to C is unchanged. Also the function C itself is unchanged.

In one embodiment of the present invention, obfuscation methods are used that confuse debugging tools or disassembler / decompiler tools, e.g. adding program code between  
25 functions that is never called but confuses a disassembler to decode the code with wrong alignment or use of software interrupts.

*Table with program parameters*

30 In one embodiment of the present invention, destination addresses for jump instructions and/or parameters to instructions are read from a table. The table or part thereof might be provided in the computer-executable program file, eventually in encrypted form to be decrypted at runtime. The decryption key used to decrypt the encrypted table entries might be generated by a key generator, read from a file or downloaded from a server. The table or  
35 part thereof might be downloaded or updated with records downloaded from a server.

In one embodiment of the present invention, a table as described above is given to a client application to allow it to be executed as part of an anti-piracy scheme. This table can for example be given when the user has registered his copy and/or typed in his copy's serial

number. This table can for example be stored on disk in encrypted form when is has been received by the client application.

*Check program before fabrication*

5

In one embodiment of the present invention, a source code file or an intermediate file derived from a source code file is evaluated before being processed in order to determine if it meets certain criteria before the source code converted into a computer-executed program file and is equipped with a key generator. These criteria might be defined by the same organization as developed the source code. A description of these criteria might be distributed along with the computer-executable program file.

10

In one embodiment of the present invention, the criteria used to evaluate a source code file or intermediate file are defines such that the evaluated program cannot export data, access data, create data, or manipulate data in a way not wanted by the entity defining the criteria. A criteria file can be a manifest file as e.g. used in Java.

15

In one embodiment of the present invention, a criteria file associated to a computer-executable program file is evaluated before the computer program is executed to determine if the criteria meets the policies defined for the computer or environment it is about to be executed on.

20

*Hardware binding*

In one embodiment of the present invention, a computer program collects data that can be used to identify the computer it runs on (also called hardware profile data). This data can for example be any of:

25

- Brand, type, version, or serial number of hardware components.
- Brand, type, version, or serial number of operating system.
- Brand, type, version, or serial number of hardware drivers.
- Brand, type, version, or serial number of software components.
- Software configuration data.
- Hardware configuration data.
- Identity (e.g. user name or e-mail address) of the user.

30

35

- MAC number, IP number, DNS settings, or other network configuration data.

In one embodiment of the present invention, a server application collects data about the computer a client application runs on without involving the client application. This data can for example be any of:



- IP number.
- Brand, type, or version of browser.
- Operating system details.

5 In one embodiment of the present invention, a server application uses hardware profile data (collected by client program and/or server program) to detect if a client program runs on the correct computer.

10 In one embodiment of the present invention, hardware profile data collected by a client application is combined in groups of strings. These strings are hashed, and the resulting strings are sent to the server. This can anonymize the user's data but still allow the server application to detect changes in the hardware profile. A string unique for the given user or client application can for example be added to the hardware profile data strings before hashing. This will ensure that even if two users have the same hardware components, the  
15 server cannot detect it as the hash strings will be different.

*Program authentication*

In one embodiment of the present invention, the generated computer-executable program file can be authenticated to detect if it is authentic. This authentication can for example be performed by the program itself, by another program, or by a hardware device. This  
20 authentication can for example be based on a purpose key generated by a key generator.

Figure 8 shows a method for authenticating a computer-executable program file. A purpose key is generated by the key generator (KG in the figure) from a key generator IV. The program file may be pre-processed by a function (F in the figure). The program file or the  
25 pre-processed program file is then processed by a MAC function taking the generated purpose key as its key. The output of the MAC function is the authentication tag used to authenticate the program. The pre-processor might be individual for each program copy.

In one embodiment of the present invention, a method for authenticating the computer-executable program file is to process the file, a part thereof, or something derived thereof by  
30 a hash function to obtain a hash value representing the content of the file. Another method is to process several parts of the computer-executable program file or something derived thereof to obtain several hash values as illustrated in figure 9. These parts may overlap and parts may be left out. This processing might be individual for each copy of the computer-executable program file. Instead of hash functions, other cryptographic functions, e.g. MAC  
35 functions can be used to obtain a value with similar properties as a hash value. The one or more hash values can for example be processed by a MAC function where the MAC function is given a purpose key from a key generator (KG in the figure) as key.

In one embodiment of the present invention, the authenticity of a computer-executable program file can be verified by calculating the expected MAC value and compare it with the MAC value generated by the program. If these are equal, the computer-executable program file is considered authentic. For example, a server might generate a random key generator IV value and send it to a client program. The client program then generates the MAC value over its own computer-executable program file using the key generator IV as input to the key generator. The generated MAC value is returned to the server. The server already knows the hash value(s), generates the MAC key, and calculates the MAC value. If the server's calculated MAC value is equal to the MAC value received from the client, the client is considered authentic.

In one embodiment of the present invention, a part of the computer-executable program file is not authenticated. This can for example allow for patching and updating without changing data on the server.

In one embodiment of the present invention, a part of a computer-executable program file is updated. The hash value(s) on the server for the parts of the file that is updated are updated to allow the server to verify the authenticity of the new computer-executable program file.

In one embodiment of the present invention, a computer-executable program consists of several files. All or some of these files are included in the authentication process.

In one embodiment of the present invention, a computer-executable program file authenticates itself towards another computer-executable program file. This allows for example sub-modules to authenticate themselves towards a main module.

In one embodiment of the present invention, a computer-executable program file is authenticated towards on or more of:

- Another computer-executable program file (e.g. running on the same computer or on another computer).
- A security-related hardware component (e.g. a Trusted Platform Module (TPM), a smartcard, or a smartcard reader).
- An input-output device (e.g. a graphics adaptor, a screen, a keyboard, a keyboard adaptor, a mouse, a mouse adaptor, a sound card, a speaker, or a microphone).
- A communication device (e.g. a network adaptor, a modem, a switch, a router, or a firewall)
- A network (e.g. towards a switch, a router, or a firewall).
- A storage device (e.g. a hard drive, a storage adaptor, a raid adaptor, a storage-area network (SAN), or a network-attached storage (NAS))

- Another kind of hardware module.
- A program running on another hardware device (e.g. another computer or a server).

5 In one embodiment of the present invention, the generated authentication tag is used as a key. Different keys can for example be generated by appending different strings to the input to the MAC function.

10 In one embodiment of the present invention, an execution environment in which a computer-executable program file is executed is authenticated. This authentication can for example be performed by hashing some or all of the program code, computer-executable program files, and data files of the execution environment. The generated hash value can for example be compared with a list of known hash values of authentic or accepted execution environments stored in the program calculating the hash value or sent to a server that can compare it with a list of authentic or accepted hash values.

15

*Secure communication link*

In one embodiment of the present invention, a purpose key generated by a key generator is used to encrypt data to be transmitted or to decrypt data that has been transmitted.

20

In one embodiment of the present invention, a purpose key generated by a key generator is used to generate an authentication tag on data to be transmitted or data that has been transmitted. This tag can for example be transmitted along with the data. The transmitted tag can for example be compared with the tag generated by the receiver to verify if the transmitted data is authentic.

25

In one embodiment of the present invention, a secure communication link is established between a server application and a client application by using the shared knowledge of the client's key generator.

30

An example of a procedure for establishing a secure communication link:

- The client application connects to the server application.
- The server generates one or more random key generator IVs and sends them to the client application.
- 35 • Using the key generator IVs, one or more keys are generated by both the client application and the server application.
- Using the one or more keys, data sent between the client application and the server application is encrypted and/or authenticated.

In one embodiment of the present invention, a program authenticity check is built into setting up the link encryption/authentication keys. For example, the key generator IV generated by the server is used to generate an authentication tag authenticating the computer-executable program file. This tag can for example be used as key or one or more  
5 keys can be derived from the tag. Keys can be derived for example by appending a string to the authentication tag and hashing it. This hash value is then used e.g. as encryption key. Append another string to the tag and hash it. This second hash value is used e.g. as authentication key. See figure 10. Another example is to use the authentication tag as key and encrypt one string using an encryption algorithm to obtain an encryption key and to  
10 encrypt another string to obtain an authentication key.

In one embodiment of the present invention, the key generator IV is generated from a string generated by the server application and a string generated by the client application. These two strings can for example be combined by means of a hash function.

15

In one embodiment of the present invention, individual messages are protected. An example:

- The sending party generates a key generator IV.
- Using the key generator IV, an encryption key and an authentication key are generated by a key generator.
- 20 • The payload string is encrypted and authenticated using the keys.
- The protected payload string and the key generator IV are sent to the recipient.
- The recipient generates the two keys using the key generator IV.
- The recipient verifies the authenticity and decrypts the payload string.

Two key generator IVs may be generated and used instead of one to generate the two keys.

25

In one embodiment of the present invention, request and response messages are protected.

An example:

- The requesting party generates a key generator IV.
- Using the key generator IV, an encryption key and an authentication key are generated by a key generator.
- 30 • The request payload string is encrypted and authenticated using the keys.
- The protected request string and the key generator IV are sent to the responding party.
- The responding party generates keys using the key generator IV.
- 35 • The protected request string is verified and decrypted by the responding party.
- The response payload string is encrypted and authenticated using the keys.
- The protected response payload is sent to the requesting party.
- The protected response payload is verified and decrypted by the requesting party.

For increased security, the requesting party and the responding party may use different IVs for encryption and authentication or use different keys, e.g. using a derived key generator IV for generating keys for protecting the response payload or using different generator IVs each way. The derived key generator IV may consist of the original key generator IV combined  
5 with a key generator IV chosen by the responding party. The responding party's key generator IV may be unique for each message and may be sent with the message to the requesting party. The combination can for example be achieved by XOR'ing the key generator IVs, by concatenating them and hashing the result, or by a block cipher by using the requesting party's key generator IV as plaintext and the responding party's key generator IV  
10 as key.

In one embodiment of the present invention, communication link sessions are protected. The communication link may be used to transmit data synchronous or asynchronous. An example:

- 15 • The client application connects to the server application.
- The server application generates a key generator IV and sends it to the client application.
- Server and client generate encryption and authentication keys based on the key generator IV.
- 20 • All sub-sequent messages are protected using these keys.

For increased security, different IVs or different keys could be used for encrypting and/or authenticating each message. The generator IV can for example be a combination of a string generated by the server and a string generated by the client. An example of an application using asynchronous transmission is AJAX (Asynchronous JAVa XML).

25 For some applications, it might be relevant to use only encryption or only authentication. In that case, the above mentioned embodiment can for example be modified by omitting the unneeded key.

30 In one embodiment of the present invention, the server application and the client application are communicating by means of at least one of:

- A TCP/IP socket.
- A modem.
- An xDSL connection.
- 35 • A VPN connection.
- A SSL or TLS connection.
- A web browser (e.g. using HTTP or HTTPS), for example via
  - Cookies.
  - Arguments sent to server by GET or POST commands.

- Data embedded into HTML, XHTML, or XML.
- Data returned by GET or POST commands.
- HTTP headers.
- E-mail.
- 5 • Instant messaging applications.
- Files.
- SMS (e.g. on GSM phones).

In one embodiment of the present invention, the transmitted data protected is payment data.  
10 Payment data can for example comprise a credit card number, a password, or a one-time password.

*Communication scenarios*

15 In one embodiment of the present invention, two computer programs communicate with each other protected by cryptographic key(s) downloaded from a server. The communication with said server might be encrypted using a purpose key. The communication with said server might be authenticated using a purpose key. The downloaded might be symmetric or  
asymmetric.

20 In one embodiment of the present invention, a first client application communicated with a server protected by purpose keys. The first client application communicates with a second client application protected by purpose keys generated by the second client application's key generator. The first client application gets the keys needed to communicate with the second  
25 client application from a server knowing how the key generator of the second client application is constructed.

In one embodiment of the present invention, a program communicates with a second  
30 program; the two programs verifies if they run on the same computer by sending profile data or something derived thereof to each other.

*Inner key exchange*

35 In one embodiment of the present invention, a secure communication channel is established between a client application and a server application. Through this channel, a key exchange protocol is executed to establish an exchanged set of keys. The key exchange protocol might be based on the Diffie-Hellman protocol. The exchanged set of keys might be used to encrypt and/or authenticate data sent between the client applications and the server application.

In one embodiment of the present invention, a secure channel is established between two computer programs; at least one of them has an embedded key generator. Through this channel, a key exchange protocol is executed to establish an exchanged set of keys. The key exchange protocol might be based on the Diffie-Hellman protocol. The exchanged set of keys  
5 might be used to encrypt and/or authenticate data sent between the client applications and the server application.

In one embodiment of the present invention, a secure communication channel is established between a server application and a client application. Through this channel, a public  
10 asymmetric key is sent. The party sending the public key has the corresponding private key. One party generates a cryptographic key and encrypts it using one of the asymmetric keys; the encrypted key is sent to the other party which decrypts it using the other asymmetric key. The algorithm used to perform the encryption/decryption might be RSA or ECC.

15 *Secure storage*

In one embodiment of the present invention, a purpose key generated by a key generator is used to encrypt data to be stored or to decrypt data that has been stored.

20 In one embodiment of the present invention, a purpose key generated by a key generator is used to generate an authentication tag on data to be stored or data that has been stored. A tag can for example be written along with the data. A read tag may be compared with the tag generated by the reader to verify if the stored data is authentic.

25 In one embodiment of the present invention, an encrypted file is created by the following procedure:

- A random key generator IV is chosen.
- The key generator IV is stored in the file.
- Using a key generator, two purpose keys are generated; one key for encryption and  
30 one for authentication.
- Payload is encrypted and authenticated using the generated keys and stored in the file.
- The generated authentication tag is stored in the file.

The file can then be read using the following procedure:

- Read the key generator IV.
- Generate encryption key and authentication key.
- Read encrypted payload from the file
- Calculate an authentication tag over the encrypted payload using the authentication  
35 key. If the tag matches the tag read from the file, the content is authentic.
- The payload is decrypted using the encryption key.

Encryption or authentication may be omitted if desired. Two key generator IV's may be used instead of one.

5 In one embodiment of the present invention, stored data is encrypted and/or authenticated with a key that depends on hardware profile data. This makes the files unreadable by a computer with another hardware profile than the one that wrote the file.

In one embodiment of the present invention, an encrypted file is created by the following procedure:

- 10
- Two random key generator IVs are chosen.
  - The key generator IVs are stored in the file.
  - Using a key generator, two purpose keys are generated.
  - A random encryption key and a random authentication key are chosen.
  - Using the two purpose keys, the two random keys are encrypted (e.g. using XOR or an

15 encryption algorithm). The encrypted keys are stored in the file.

  - Payload is encrypted and authenticated using the random keys and stored in the file.
  - The generated authentication tag is stored in the file.

The file can then be read using the following procedure:

- 20
- Read the key generator IVs.
  - Generate the two purpose keys using a key generator.
  - Decrypt the two read keys using the two generated purpose keys.
  - Authenticate and decrypt the payload using the two decrypted keys.

Encryption or authentication (and their keys) may be omitted if desired. One purpose key may be used instead of two (also if both encryption and authentication is used; both keys

25 may be encrypted using the same key). One key generator IV may be used instead of two.

In one embodiment of the present invention, an encrypted file is created by the following procedure (also see figure 11):

- 30
- A random key generator IV is chosen.
  - The key generator IV is stored in the file.
  - A random encryption key is chosen.
  - A purpose key is generated by the key generator (KG in the figure) using the key generator IV.
  - A program authentication tag is created (by MAC in the figure) using the purpose key as MAC key.

35

  - Hardware profile data is read. The hardware profile data is collected in groups. For each group
    - The authentication tag and the hardware parameter group data string are hashed (by upper H in the figure).



- The output from the hash function is XOR'ed with the encryption key (this way, the key is encrypted). The resulting string is stored in the file.
  - The output from the hash function is hashed again (by lower H in the figure). This second-order hash string is stored in the file.
- 5     • The payload is encrypted using the encryption key. The encrypted string is stored in the file.

The file can be decrypted using the following procedure:

- Read the generator IV.
- A purpose key is generated by the key generator using the key generator IV.
- 10   • A program authentication tag is created using the purpose key as MAC key.
- Hardware profile data is read. The hardware profile data is collected is the same groups as when encrypting the file. For each group:
  - The authentication tag and the hardware parameter group data string are hashed.
  - The output from the hash function is hashed again. The output is compared to the
  - 15   second-order hash strings in the file.
  - If a matching second-order hash string is found in the file, the corresponding XOR'ed key is read. This key is XOR'ed with the original hash string (first-order hash string) to obtain the encryption key.
- The encrypted payload is decrypted using the found encryption key.

- 20   If program integrity is not needed, the MAC function is removed and the purpose key is used directly as part of the input to the first (upper) hash function. If hardware binding is not needed, the output from the MAC function is used as encryption key; no hash strings or encrypted keys are stored in the file. Hardware parameter data may be manipulated prior to the first hashing. If just one hardware profile group is used, just use the output from the first
- 25   hash function as key (no hash strings or keys are stored) or use it to encrypt the key (no hash strings are stored but the encrypted key is stored). If no key generator is present, the purpose key may be replaced by a constant or the MAC function used in generating the authentication tag may be replaced by a hash function or the authentication tag may be omitted as input to the first hash function (i.e. only hardware profile data is input). The key
- 30   generator IV, second-order hash strings, and/or encrypted keys may be stored in the same file as the (encrypted) payload or in one or more other files. If the file is also to be authenticated, a second random key is chosen in the file generation step and two encrypted keys are stored instead of one for each second-order hash. The encrypted keys may be encrypted by other functions than xor; for example by an encryption algorithm. If more keys
- 35   are generated for the same hardware profile, the input to the first hash function may be manipulated in different ways (e.g. by appending different strings) to obtain different hash strings for each key. Several encrypted keys for each second-order hash may be stored, allowing to decrypt (or verify authenticity of) several files or parts of files. Different files or parts of files encrypted using different keys may be decrypted by knowing different hardware

profile data (e.g. more secret data may require more correct hardware parameters than less secret data).

- 5 In one embodiment of the present invention, a file encrypted by one copy of a client program can be re-encrypted to be accessible by another copy of a client program. For example, if the file is encrypted using a key generated by the first copy's key generator, the file can be sent to the server, the server (knowing how both the first copy's and the second copy's key generator's compositions) can generate the keys needed to decrypt the file and encrypt it again for the second copy. As another example, if the file's encryption key is encrypted using
- 10 a key generated by the first copy's key generator, the encrypted key can be sent to the server, the server (knowing how both the first copy's and the second copy's key generator's compositions) can generate the keys needed to decrypt the key and encrypt it again for the second copy
- 15 In one embodiment of the present invention, a key generator is used to encrypt/decrypt and/or authenticate a cookie (e.g. used in a web browser or a web server).

*Version update*

- 20 In one embodiment of the present invention, a new version of a copy of a computer-executable program file is generated such that the new version has a key generator equivalent to the one of the old version.
- In one embodiment of the present invention, an old version of a computer-executable
- 25 program file downloads a new version with a key generator equivalent to the one of the old version.
- In one embodiment of the present invention, an old version of a computer-executable
- 30 program file in the form of an embedded object in a home page receives a message from a server application telling it to forward the browser to another page using an argument given by the server application. This other page combined with the given arguments allows the web server to send a new version of the computer-executable program file with a key generator equivalent to the one of the old version.
- 35 In one embodiment of the present invention, a database containing at least two of: user ID, client program serial numbers, client program version number, and client program PRNG seeds is maintained. When a new version of the client program is sent to a user, the database is updated accordingly.

In one embodiment of the present invention, a client program is updated if certain criteria are fulfilled. For example, when a client program connects to a server, the client program sends an identification string to the server (e.g. containing its serial number). If the server decides that the client program needs to be updated, it sends a message to the client  
5 program saying that it should update itself. If the client program is a program embedded into a homepage, the auto update may be initialized by forwarding the containing page to another URL, the other URL initiates the update.

Before a client program embedded into a home page is started, the browser (or another  
10 component on the client computer) will usually check if a newer version of the client program is available. The check is usually performed by contacting a server using HTTP or HTTPS. In one embodiment of the present invention, the server decides if a newer version should be downloaded to the user based on at least one of: the content of a cookie, arguments given to the referrer site (can be detected through the "referrer" header line), or the "last-modified"  
15 header line.

#### *Digital rights management*

In one embodiment of the present invention, a key generator is used to generate keys to  
20 decrypt and/or verify the authenticity of digital content, for example video, music, computer programs, or computer games.

In one embodiment of the present invention, a playback device (e.g. a media player or a gaming console) has an embedded key generator. This key generator can for example  
25 generate keys that can decrypt and/or verify the authenticity of digital content or generate keys that can decrypt keys that can be used to decrypt and/or verify the authenticity of digital content.

In one embodiment of the present invention, a distributor of digital content encrypts or  
30 generates an authentication tag using a random key. This key is encrypted using a key generated by a server knowing how the user's application's key generator is constructed. The protected content and the encrypted key are sent to the user, who can play it using his client application. If the user also wants to play the content on another playback device, he can apply (e.g. the content owner) for the key encrypted for the other device.  
35

In one embodiment of the present invention, digital content is protected and distributed as illustrated on figure 12. The user acquires a playback device (e.g. a media player) from a player vendor. This playback device has an embedded key generator. The player vendor informs a license manager about how the key generator is constructed such that the license

manager can reproduce it. The content is stored by the content vendor. When a user wants to download (or in another way acquire) content, the content is encrypted and/or an authentication tag is generated (alternatively, this process can be performed ahead of the user's request). The content is sent to the user e.g. over the Internet (or another network, a satellite link, a radio link, or on a media, e.g. a DVD). The content can for be stored on the user's storage for later use or can be processed by the playback device right away. To use the content, the playback device acquires a key from the license manager (e.g. in encrypted form such that it can be decrypted using the playback device's key generator). This key can be stored for later use or can be used right away.

5

In one embodiment of the present invention, each copy or set of copies of a digital content is encrypted using a unique key. Optionally, a serial number, a product number, and/or another form of identification may be embedded into the encrypted content. When a user wants to use the content, he contacts a server and requests a key for that copy of that content (may be downloaded in encrypted form) to become able to decrypt the content..

10

In one embodiment of the present invention, all copies of a digital content are encrypted using the same key. Optionally, a product number and/or another form of identification may be embedded into the content. When a user wants to use the content, he contacts a server and requests a key for that content (may be downloaded in encrypted form) to become able to decrypt the content.

15

In one embodiment of the present invention, the playback device acquires keys (e.g. using the internet, a satellite link, or a radio link) for each playback of the content.

20

In one embodiment of the present invention, the playback device acquires keys that a stored and used for several playbacks of the content.

25

In one embodiment of the present invention, digital content is acquired; decrypted if it was acquired in encrypted form; and encrypted using a purpose key generated by a key generator.

30

#### *User and transaction authentication*

In one embodiment of the present invention, a key generator is embedded into an authentication token (like e.g. RSA SecureID). This authentication token can for example generate one-time passwords used to authenticate a user.

35

In one embodiment of the present invention, a key generator is used to periodically generate new master keys in an authentication token.

5 In one embodiment of the present invention, the output of an authentication token is derived from a purpose key generated by a key generator.

#### *Authenticate boot image*

10 In one embodiment of the present invention, a key generator is embedded into a device (e.g. a cell phone, a PDA, a gaming console, or a set top box), for example in the boot-strap code of the device. Using this key generator, data (e.g. program code or content) can be authenticated. For example, a boot image stored in flash memory can be verified by boot-strap code stored in read-only memory to verify if the boot image is authentic and intact. This can for example be achieved by appending a MAC tag to the boot image that can be  
15 verified using the key generator in the boot strap code. This MAC tag can be generated by a server that knows how the key generator in the specific device is constructed.

In one application of the present invention, a key generator is embedded into a device. Using this key generator, data can be decrypted or encrypted. For example, a boot image can be  
20 decrypted as part of the installation process, such that a user can download an encrypted boot image over the internet, this boot image can only be decrypted by a device having a given key generator.

25 In one embodiment of the present invention, a key generator embedded into a device is used to generate keys to secure a network link, secure stored data, or access digital content.

#### *Hardware key generators*

30 In one embodiment of the present invention, a key generator (or part thereof) is embedded into a hardware device or an electronic chip (e.g. a programmable electronic chip).

#### *Applications*

The present invention can for example be used in one of:

- 35
- A financial application (e.g. an online banking application, an online investment application, a payment site, or an automatic teller machine).
  - A computer game (e.g. an online game, e.g. online poker).
  - A DRM application (e.g. license manager or a media player).

- A security application (e.g. a VPN client, a remote desktop application, or an anti-virus application).
- A distributed computing application (e.g. to verify authenticity of client applications).

5 *Unique and random*

When the term "unique" is used in this document on number or strings, it may include randomly chosen numbers or strings (e.g. generated by a PRNG) even though these can collide (i.e. there is a certain chance that the same number can be drawn more than once).

10

It should be understood that the method steps, structural details, functionalities and any other feature of any of the methods, computers, computer programs, servers, clients and any other invention described and embodied herein, may be fully or partially applied in any other method, computer, computer program, server, client and any other invention described and embodied herein, unless otherwise stated. Hence, all possible combinations of the presently embodied and described inventions are within the scope of the present specification and embodiments.

15

DESCRIPTION OF THE DRAWINGS

20

Figure 1 illustrates three customers communicating with their bank over the Internet using their computers. The fourth user is an attacker. In a worst-case scenario, the attacker has full control over the Internet and the users' computers.

25

Figure 2 illustrates the components involved in the communication between the user and the bank (i.e. the bank's internal computer systems). The user and the bank are considered secure, but all other components can be under the influence of an attacker.

30

Figure 3 illustrates how the online banking program (the "netbank program") can be secured by the present invention by having an embedded value or key generator. This value or key generator is used to authenticate the online banking program towards the bank, whereby the bank can make sure that the online banking program is authentic. The value or key generator may also be used to create a secure communication link between the program and the bank even if the computer or the Internet is compromised by an attacker. Finally, the value or key generator may be used to encrypt/decrypt data stored locally (the "netbank data"), again even if the computer is compromised.

35

Figure 4 illustrates a key generator. Internally, it consists of two sub-functions: An extractor and a blender. The extractor takes an extractor IV as input and generates an extracted key.

The extractor is usually unique for each copy of a program. The blender takes an extracted key and a blender IV and generates a purpose key.

5 Figure 5 illustrates an extractor.  $W_1$ ,  $W_2$ ,  $W_3$ , and  $W_4$  represents the initial values of the inner state words, which are being processed by  $n$  generator subfunction,  $F_1$ ,  $F_2$ , ...  $F_n$ . The resulting values of the inner state words are processed by a function  $L$  to generate an extracted key.

10 Figure 6 illustrates an extractor. An extractor IV is used to generate four initial values of the inner state words by the  $K$  function. The extractor IV is also used to generate parameters for the generator subfunctions by the  $J$  function. The generator subfunctions,  $F_1$ ,  $F_2$ , ...  $F_n$ , manipulates the inner state words and uses each a constant,  $C_1$ ,  $C_2$ , ...  $C_n$ . The resulting inner state words are processed by the  $L$  function to obtain an extracted key.

15 Figure 7 illustrates a client-server setup. Client programs are generated by a client program generator. The client generator stores the generated program files in a program file database and stores the generated program's serial number and PRNG seed in a SN/Seed database. When a user downloads a copy of the program from web server, the web server fetches one of the programs in the program database. When the client program communicates with a transaction server, the transaction server can look up the PRNG seed using the programs  
20 serial number as key. Using the PRNG seed, the transaction server can reproduce the functionality of the key generator embedded into the client program.

25 Figure 8 illustrates a method for authenticating a computer-executable program file. A key generator IV is sent to a key generator (KG), to obtain a purpose key. The client program is processed by a function ( $F$ ) and the resulting string is sent through a MAC function where the generated purpose key is used as MAC key. The resulting MAC tag is used as an authentication tag.

30 Figure 9 illustrates a method for authenticating a computer-executable program file. A key generator IV is sent to a key generator (KG), to obtain a purpose key. The client program is divided into substrings. Each substring is processed by a hash function. The outputs from the hash functions are sent through a MAC function where the generated purpose key is used as MAC key. The resulting MAC tag is used as an authentication tag.

35 Figure 10 illustrates a method for generating an encryption key and an authentication key. A key generator IV is sent to a key generator (KG), to obtain a purpose key. The client program is divided into substrings. Each substring is processed by a hash function. The outputs from the hash functions are sent through a MAC function where the generated purpose key is used as MAC key. One string is appended to the output of the MAC function

and the resulting string is hashed. The result of this hash operation is used as an encryption key. Another string is appended to the output of the MAC function and the resulting string is hashed. The result of this hash operation is used as an authentication key.

- 5 Figure 11 illustrates a method for storing a file encryption key. A key generator IV is stored in a file and is sent to a key generator (KG), to obtain a purpose key. The computer-executable program file is processed by a MAC function where the generated purpose key is used as MAC key. Hardware profile data is read on the computer the program runs on. This data is grouped. Each hardware profile group is processed with the output of the MAC
- 10 function by a first hash function (upper H). The output from the first hash function is hashed again and the result is stored in the file. The output from the first hash function is also used to encrypt a key. The encrypted key is also stored in the file. An encrypted key and an output of the second hash function (lower H) are stored for each hardware profile group.
- 15 Figure 12 illustrates a DRM system where a user acquires a playback device with an embedded key generator from a player vendor. The player vendor sends information about the key generator to a license manager such that the license manager can reproduce the key generator's functionality. Content is encrypted and/or authenticated and sent to the user. The user downloads an encrypted key from the license manager. This key can be decrypted
- 20 by the playback device in order to achieve the key(s) needed to decrypt or verify authenticity of the content.
- Figure 13 illustrates two functions (A and B) in a being merged into one. The call from the code of the original function A to the code from the original function B is changed to a local
- 25 call. In the same way, the return from the code of the original function B is replaced by a local return statement. Furthermore, extra functionality is embedded into the resulting function in order to handle tasks previously handled by the runtime environment or operating system, e.g. allocating and freeing memory for temporary variables.
- 30 Figure 14 illustrates a computer program (C) and a server (D). C has an embedded key generator (KG). D has a key generator emulator (KGE). If D knows the identity of C (e.g. knows its serial number), it can look up the seed value used to generate the key generator embedded into C from the serial number and seed database. This knowledge can be used by D's key generator emulator to emulate C's key generator. Thus, C and D can generate the
- 35 same keys. These keys can be used to send data in protected form between C and D. This protection can consist of the data being encrypted and/or authenticated using key generated by C's KG and D's KGE.



Figure 15 illustrates two computer programs (G and H) and a server (I). G and H each have an embedded unique key generator (KG). I has a key generator emulator (KGE). The key generator emulator can generate the same keys as the key generators in G and H provided that I knows the identity of G and H (e.g. by knowing their serial numbers). The key generator emulator can look up the seed values used to generate the key generators in G and H in the serial number / seed database. I can create a cryptographic key that can be sent in protected form (e.g. encrypted form) to both G and H (i.e. encrypted using keys that can be generated by the key generators of G and H respectively). When G and H shares the same key, they can send protected data between each other where this data is encrypted and/or authenticated using the shared key.

It should be understood that the present invention is not limited to the subject-matter of the appended claims. In particular, the embodiments outlined below form part of the present invention:

1. A method of fabricating computer-executable program files from a source code, the method comprising the step of embedding, in each of the fabricated computer-executable program files, at least one value or means for generating at least one value, said value being uniquely selected or generated for each of the fabricated computer-executable program files, whereby all of the fabricated computer-executable program files are capable of carrying out instructions defined by the source code, and whereby each individual computer-executable program file is capable of generating a unique output, which depends on said uniquely selected or uniquely generated value.
2. A method according to embodiment 1 where each user or group of users uses a different copy of the computer-executable program file.
3. A method according to embodiment 1 or 2 where the embedded means for generating at least one value depends on at least one embedded value.
4. A method according to any of embodiments 1 – 3 where the process of fabricating computer-executable program files from a source code is divided into at least two steps; a first step of converting source code into at least one intermediate file is performed once and a later step of converting at least one intermediate file and optionally other files into a computer-executable program file is performed for each computer-executable program file.
5. A method according to embodiment 4 where at least one of the intermediate files is a computer-executable program file, an object file, or a source code file.

6. A method according to any of the preceding embodiments where at least a part of the source code is evaluated to determine if it meets one or more predefined criteria for being equipped with the embedded at least one value or means for generating at least one value.
- 5 7. A method according to embodiment 4 or 5 where at least one of the intermediate files is evaluated to determine if it meets one or more predefined criteria for being equipped with the embedded at least one value or means for generating at least one value.
- 10 8. A method according to embodiment 6 or 7 where the criteria are defined by the organization providing the source code.
9. A method according to any of embodiments 6 – 8 where the criteria are defined such that the program cannot export sensitive data in an unprotected form.
- 15 10. A method according to any of embodiments 6 – 9 where the criteria are defines such that the program cannot manipulate sensitive data.
- 20 11. A method according to any of embodiments 6 – 10 where information about the criteria is distributed along with the fabricated computer-executable program file who's functionality is evaluated according to the criteria.
- 25 12. A method according to any of embodiments 1 – 11 where the embedded means for generating at least one value comprises at least one extractor subfunctions, the extractor subfunctions have been selected from a set of available extractor subfunctions.
13. A method according to embodiment 12 where the extractor subfunctions are uniquely selected for each computer-executable program file.
- 30 14. A method according to embodiment 12 or 13 where at least one extractor subfunctions depend on at least one inner state word and generate at least one inner state word.
15. A method according to any of embodiments 1 – 11 where the embedded means for generating at least one value comprises at least one extractor subfunction.
- 35 16. A method according to embodiment 15 where at least one of the extractor subfunctions is uniquely selected for each computer-executable program file.
17. A method according to embodiment 15 or 16 where at least one of the extractor subfunctions is selected from a set of available extractor subfunctions.

18. A method according to any of embodiments 15 – 17 where at least one of the extractor subfunctions depend on at least one inner state word and generate at least one inner state word.

5

19. A method according to any of embodiments 12 – 18 where at least one extractor subfunction depends on a value derived from a key generator initialization vector (key generator IV) where the key generator IV is given as argument to the embedded means for generating at least one value.

10

20. A method according to any of embodiments 12 – 19 where at least one extractor subfunction depends on at least one embedded value.

21. A method according to any of embodiments 12 – 20 where at least one extractor subfunction comprises at least one of:

15

- a bijective operation,
- an arithmetical operation,
- a logical operation,
- a table lookup, and

20

- an embedded value.

22. A method according to any of embodiments 12 – 21 where the initial value of at least one inner state word depends on a key generator IV.

25

23. A method according to any of embodiments 12 – 22 where the output from at least one extractor subfunction or a value derived thereof is used as input to a cryptographic function.

24. A method according to embodiment 23 where the cryptographic function is a hash function.

30

25. A method according to embodiment 24 where the hash function also depends on at least a part of the key generator IV.

26. A method according to any of embodiments 12 – 25 where the output from at least one extractor subfunction or a value derived thereof is used as a cryptographic key.

35

27. A method according to any of embodiments 1 – 26 where the embedded at least one value or means for generating at least one value is used to derive a cryptographic key.

28. A method according to any of embodiments 1 – 27 where an embedded value, a value derived thereof, a value generated by means for generating at least one value, or a value derived thereof is used as input to a cryptographic algorithm where the output of the cryptographic algorithm is used as a cryptographic key.

5

29. A method according to any of embodiments 1 – 28 where the embedded at least one value or means for generating at least one value is used to authenticate a computer program.

10

30. A method according to any of embodiments 1 – 29 where the embedded at least one value or means for generating at least one value is used as a serial number or to derive a serial number that can be used to identify the copy of the computer program.

15

31. A method according to any of embodiments 1 – 26 where the embedded at least one value or output from means for generating at least one value is combined with at least one of:

- data from the user,
- data about the user,
- data from something the user possesses, and
- data from the computer the program runs on

20

to obtain a resulting value.

32. A method according to any of embodiments 1 – 26 where the means for generating at least one value depends on at least one of:

25

- data from the user,
- data about the user,
- data from something the user possesses, and
- data from the computer that program runs on

in order to generate a resulting value.

30

33. A method according to embodiment 31 or 32 where the resulting value is used as a cryptographic key or to obtain a cryptographic key.

35

34. A method according to any of embodiments 26, 27, 28, or 33 where the cryptographic key is used to encrypt or decrypt data.

35. A method according to embodiment 34 where the cryptographic key is used to encrypt data to be stored or to decrypt data that has been stored.

36. A method according to embodiment 34 where the cryptographic key is used to encrypt data to be transmitted or to decrypt data that has been transmitted.
37. A method according to any of embodiments 26, 27, 28, or 33 where the cryptographic  
5 key is used to generate an authentication tag.
38. A method according to embodiment 37 where the authentication tag is appended to data to be stored or is extracted from data that has been stored.
- 10 39. A method according to embodiment 37 where the authentication tag is used to authenticate stored data.
40. A method according to embodiment 37 where the authentication tag is appended to data to be transmitted or is extracted and from data that has been transmitted.  
15
41. A method according to embodiment 37 where the authentication tag is used to authenticate transmitted data.
42. A method according to any of embodiments 37 – 41 where the authentication tag is used  
20 to authenticate at least a part of a computer program.
43. A method according to any of embodiments 37 – 42 where the correctness of the authentication tag is verified by a server.
- 25 44. A method according to any of embodiments 37 – 43 where the correctness of the authentication tag is verified by a hardware device.
45. A method according to any of the preceding embodiments where information about how a computer-executable program file is generated is stored such that the computer-executable  
30 program file can be reproduced or its functionality or part thereof can be reproduced or simulated.
46. A method according to embodiment 45, wherein the stored information about the computer-executable program file is used in a computer program and/or hardware device to  
35 reproduce at least a part of the at least one embedded value or to simulate at least a part of the embedded means for generating at least one value.
47. A method of fabricating computer-executable program files according to any of the preceding embodiments comprising the following steps:

1. choosing a PRNG seed,
  2. generating a set of pseudo-random values from the PRNG seed using a pseudo-random number generator,
  3. using the set of pseudo-random values to determine at least one embedded value or  
5 how to construct the embedded means for generating at least one value.
48. A method of fabricating computer-executable program files according to any of the preceding embodiments comprising the following steps:
1. choosing a PRNG seed,
  - 10 2. generating a string of pseudo-random bits from the PRNG seed using a pseudo-random number generator,
  3. using the string of pseudo-random bits to determine at least one embedded value or how to construct the embedded means for generating at least one value.
- 15 49. A method according to embodiment 47 or 48 where the PRNG seed is stored for later use.
50. A method according to any of embodiments 47 – 49 where the PRNG seed is used to generate the set of pseudo-random values again; the set of value is used to recreate at least one embedded value or the embedded means for generating at least one value.
- 20 51. A method according to any of embodiments 47 – 50 where the PRNG seed is used to generate the string of pseudo-random bits again; the string of bits is used to recreate at least one embedded value or the embedded means for generating at least one value.
- 25 52. A method according to any of embodiments 47 to 51 where the PRNG seed is used to allow a computer program or a hardware device to create the same cryptographic key as a computer-executable program file being executed; the PRNG seed is used to reproduce the embedded at least one value or means for generating at least one value embedded into the  
30 computer executable program file on the computer program or hardware device such that both parties can generate the same cryptographic keys derived from the embedded at least one value or means for generating at least one value.
53. A method according to any of the preceding embodiments where a new version of a computer-executable program file is sent to a user; the new version has the same embedded  
35 at least one value or means for generating at least one value as the previous version.
54. A method according to any of the preceding embodiments where a computer-executable program file with an embedded at least one value for means for generating at least one value

downloads or in another way acquires another computer-executable program file with the same embedded at least one value for means for generating at least one value.

5 55. A method according to any of the preceding embodiments where the embedded at least one value or means for generating at least one value is copied from one computer-executable program file to another computer-executable program file.

10 56. A method according to any of the preceding embodiments where information about program file's embedded at least one value or means for generating at least one value is stored; when a computer-executable program file is updated, this information is updated.

15 57. A method according to any of the preceding embodiments where information about a program file's embedded at least one value or means for generating at least one value is stored; when the computer-executable program file is updated, this information is updated.

20 58. A method according to any of the preceding embodiments where information about a program file's embedded at least one value or means for generating at least one value is stored in a database; when the computer-executable program file is updated, its record in the database is updated.

25 59. A method according to any of the preceding embodiments where the computer-executable program files are obfuscated.

30 60. A method according to embodiment 59 where the obfuscation method comprises means for at least one of:

- replacing a program instruction or a set of program instructions with at least one new program instruction with equivalent functionality,
- reallocating registers,
- reordering program instructions,
- 35 • adding or removing jump instructions,
- inserting useless data or program instructions into the computer program,
- interleaving at least two program sequences,
- reordering static data, and
- reordering runtime data.

61. A method according to any of the preceding embodiments where at least a part of the computer-executable program file is stored in encrypted form and is decrypted at runtime.

62. A method according to embodiment 61 where the key to decrypt the encrypted at least a part of the computer-executable program code is downloaded from a server.
- 5 63. A method according to embodiment 62 where the encrypted part of the computer-executable program file is decrypted using a cryptographic key derived from the embedded at least one value or means for generating at least one value.
- 10 64. A method according to any of the preceding embodiments where a computer-executable program file with embedded at least one value or means for generating at least one value decrypts another computer-executable program file.
65. A method according to any of the preceding embodiments where the destination address of at least one jump instruction in the computer-executable program file is read from a table.
- 15 66. A method according to any of the preceding embodiments where at least one parameter to at least one instruction in the computer-executable program file is read from a table.
- 20 67. A method according to embodiment 65 or 66 where the at least one entry in the table has a pre-defined value stored in the computer-executable file.
68. A method according to any of embodiments 65 – 67 where at least one entry in the table is downloaded from a server.
- 25 69. A method according to any of embodiments 65 – 68 where at least one entry in the table is decrypted at runtime.
- 70 A method according to embodiment 68 or 69 where at least one downloaded or decrypted value replaces at least one pre-defined value in the table.
- 30 71. A method according to embodiment 69 or 70 where the decryption key is derived from the embedded at least one value or means for generating at least one value.
72. A method according to embodiment 69 or 70 where the decryption key is derived from a string downloaded from a server.
- 35 73. A method according to any of the preceding embodiments where a computer-executable program file with at least one embedded value or embedded means for generating at least one value contains program code that can read profile data, the profile data comprises at least one of:



- brand, type, version, or serial number of a hardware component,
  - brand, type, version, or serial number of a software component,
  - software or hardware configuration data,
  - network configuration data, and
- 5       • identity of the user.
74. A method according to embodiment 73 where profile data is used as input to the means for generating at least one value.
- 10       75. A method according to any of the preceding embodiments where a computer program (*A*) communicating with a computer-executable program file with at least one embedded value or embedded means for generating at least one value (*B*); *A* can read profile data related to *B*, the computer *B* runs on, or the user using *B*.
- 15       76. A method according to any of embodiments 73 – 75 where profile data is used to detect if the computer-executable program file runs on the right computer.
77. A method according to any of the preceding embodiments where data sent between program *C* and *D* is encrypted/decrypted; the encryption/decryption key is derived from the embedded at least one value or means for generating at least one value in program *C*; the encryption/decryption key is derived from knowledge about the embedded at least one value or means for generating at least one value in *C* by program *D*.
- 20
78. A method according to any of the preceding embodiments where data is sent in encrypted form between programs *C* and *D*; the encryption/decryption key is derived from the embedded at least one value or means for generating at least one value in program *C*; the encryption/decryption key is derived in program *D* from knowledge about the embedded at least one value or means for generating at least one value in *C*.
- 25
79. A method according to any of the preceding embodiments where data sent between program *E* and *F* is authenticated; the authentication key is derived from the embedded at least one value or means for generating at least one value in program *E*; the authentication key is derived from knowledge about the embedded at least one value or means for generating at least one value in *E* by program *F*.
- 30
80. A method according to any of embodiments 77 – 79 where one party in a communication selects a key generator *IV*; the key generator *IV* is sent to the other party; both parties uses the key generator *IV* to derive a key that can be used for encryption/decryption or authentication.
- 35

81. A method according to any of embodiments 77 – 79 where both parties in a communication selects a part of a key generator IV; the parts are communicated; a key generator IV is derived in both ends from the parts; both parties uses the constructed key generator IV to derived a key that can be used for encryption/decryption or authentication.

82. A method according to any of the preceding embodiments where data is sent in encrypted form between programs *G* and *H* where *G* and *H* both communicates securely with server *I* using cryptographic keys derived from *G*'s and *H*'s embedded at least one value or means for generating at least one value; the server *I* provides at least one cryptographic key to *G* and *H* to be used to encrypt/decrypt at least a part of the data sent between *G* and *H*.

83. A method according to any of the preceding embodiments where data is sent in authenticated form between programs *J* and *K* where *J* and *K* both communicates securely with server *L* using cryptographic keys derived from *J*'s and *K*'s embedded at least one value or means for generating at least one value; the server *L* provides at least one cryptographic key to *J* and *K* to be used to authenticate at least a part of the data sent between *J* and *K*.

84. A method according to any of the preceding embodiments where at least one cryptographic key is negotiated between programs *M* and *N* where *M* and *N* both communicates securely with server *O* using cryptographic keys derived from *M*'s and *N*'s embedded at least one value or means for generating at least one value

85. A method according to embodiment 84 where *O* provides the same cryptographic key to *M* and *N*.

86. A method according to embodiment 84 or 85 where at least one of the at least one cryptographic keys is used to encrypt/decrypt data sent between *M* and *N*.

87. A method according to any of embodiments 84 – 86 where at least one of the at least one cryptographic keys is used to authenticate data sent between *M* and *N*.

88. A method according to any of embodiments 1 – 81 where data is sent in encrypted form between programs *P* and *Q*; *P* derives the encryption/decryption key from its embedded at least one value or means for generating at least one value; *Q* receives the encryption/decryption key from a server.

89. A method according to any of embodiments 1 – 81 where data sent between programs *R* and *S* is authenticated; *R* derives the authentication key from its embedded at least one

value or means for generating at least one value; S receives the authenticate key from a server.

5 90. A method according to any of embodiments 82 – 89 where the two programs run on the same computer.

91. A method according to embodiment 90 where the two programs read profile data and compare these to verify that they run on the same computer.

10 92. A method according to any of embodiments 82 – 89 where the two programs run on different computers.

15 93. A method according to any of the preceding embodiments where key exchange protocol data is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value.

20 94. A method according to any of the preceding embodiments where key exchange protocol data is authenticated using a cryptographic key derived from an embedded at least one value or means for generating at least one value.

95. A method according to embodiment 93 or 94 where the key exchange protocol is the Diffie-Hellman protocol.

25 96. A method according to any of embodiments 93 – 95 where the key exchange protocol is used to derive a symmetrical cryptographic key.

97. A method according to any of the preceding embodiments where an asymmetric key is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value.

30 98. A method according to any of the preceding embodiments where an asymmetric key is authenticated using a cryptographic key derived from an embedded at least one value or means for generating at least one value.

35 99. A method according to embodiment 97 or 98 where the asymmetric key is a public RSA key or a private RSA key.

100. A method according to embodiment 97 or 98 where the asymmetric key is a public ECC key or a private ECC key.

101. A method according to any of embodiments 97 – 100 where the asymmetric key is used to derive a symmetrical cryptographic key.

5 102. A method according to embodiment 96 or 101 where the symmetrical key is used to encrypt or decrypt data.

103. A method according to any of embodiments 96, 101, and 102 where the symmetrical key is used to authenticate data.

10

104. A method according to any of the preceding embodiments where data to be stored is encrypted or data that has been stored is decrypted; the encryption/decryption key is derived from the embedded at least one value or means for generating at least one value.

15 105. A method according to any of the preceding embodiments where data to be stored or that has been stored is processed in order to generate an authentication tag; the authentication key is derived from the embedded at least one value or means for generating at least one value.

20 106. A method according to embodiment 104 or 105 where a key generator IV is used to derive the encryption/decryption key or authentication key; the key generator IV is stored with the data.

25 107. A method according to embodiment 104 or 105 where a value stored with the data is hashed with profile data to obtain a key generator IV used to derive the encryption/decryption key or authentication key.

30 108. A method according to any of the preceding embodiments where a cryptographic key is stored in encrypted form; the decryption key to be used to decrypt the cryptographic key is derived from the embedded at least one value or means for generating at least one value.

35 109. A method according to any of the preceding embodiments where a cryptographic key is stored in encrypted form; the decryption key to be used to decrypt the cryptographic key is downloaded from a server.

110. A method according to any of the preceding embodiments where a computer program or a computer-executable program file is authenticated using an authentication key derived from the embedded at least one value or means for generating at least one value.

111. A method according to embodiment 110 where a computer program or a computer-executable program file is authenticated towards another computer program or a hardware device.

5 112. A method according to embodiment 110 or 111 where a computer program is calculating an authentication tag on itself.

10 113. A method according to any of the preceding embodiments where an authentication tag is calculated on a computer program, a computer-executable program file, or a data file; the authentication key is derived from an embedded at least one value or means for generating at least one value, the authentication tag is compared to one stored with the program or data to verify if the program or data is authentic and if the stored tag was generated by someone with knowledge about the embedded at least one value or means for generating at least one value.

15 114. A method according to embodiment 113 where the embedded at least one value or means for generating at least one value is stored on a device and the program or file to be authenticated is a program the be executed or accessed on that device.

20 115. A method according to embodiment 113 or 114 where the stored authentication tag is generated with knowledge about the embedded at least one value or means for generating at least one value.

25 116. A method according to any of the preceding embodiments where a computer-executable program file with the embedded at least one value or means for generating at least one value is used to play back digital content.

30 117. A method according to any of the preceding embodiments where digital content is distributed in encrypted form; the encrypted content is decrypted by a computer-executable program file with an embedded at least one value or means for generating at least one value in order to play back the digital content.

35 118. A method of generating a media player with at least one uniquely selected value or at least one value generated by uniquely selected means is used to play back digital content produced by a method according to any of the preceding embodiments.

119. A method of distributing a decryption key for digital content to a playback device; the playback device is constructed by a method according to any of the preceding embodiments.

120. A method according to any of the preceding embodiments where the fabricated computer-executable program file is tested to verify if it works as intended.

5 121. A method according to any of the preceding embodiments where at least one fabricated computer-executable program file is inserted into another file.

122. A server from which computer-executable program files fabricated according to any of the preceding embodiments can be downloaded.

10 123. A server communicating with a computer-executable program file fabricated according to any of the preceding embodiments.

124. A file written by a computer-executable program file fabricated according to any of the preceding embodiments.

15

125. An file encrypted using a key; the decryption key can be derived or decrypted using at an embedded at least one value or means for generating at least one value in a computer-executable program file fabricated according to any of the preceding embodiments.

20 126. Data sent over a network; the data is encrypted by a computer-executable program file fabricated according to any of embodiments any of the preceding embodiments.

25 127. Data sent over a network; the data is encrypted using a key; the decryption key can be derived or decrypted using an embedded at least one value or means for generating at least one value in a computer-executable program file fabricated according to any of embodiments any of the preceding embodiments.

30 128. Data sent over a network; the data is authenticated by a computer-executable program file fabricated according to any of the preceding embodiments.

30

129. Data sent over a network; the data is authenticated using a key; the decryption key can be derived or decrypted using an embedded at least one value or means for generating at least one value in a computer-executable program file fabricated according to any of the preceding embodiments.

35

130. A document into which at least one computer-executable program file fabricated according to any of the preceding embodiments is embedded.

131. A computer on which at least one computer-executable program file fabricating according to any of the preceding embodiments is stored or executed.

5 132. A computer program for fabricating computer-executable program files from source code, the computer program comprising means for performing the method of any of the preceding embodiments.

10 133. A computer-readable data medium comprising a computer program according to embodiment 132.

134. A computer loaded with a computer program according to embodiment 132.

15 135. A computer-executable program file fabricated by a method according to any of embodiments 1 – 121.

136. A method according to any of the preceding embodiments of fabricating computer-executable program files according to any of embodiments 137 - 300.

20 137. A computer program comprising a computer-executable program file fabricated from a source code, the computer program including, in said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of generating a unique output, which depends from said uniquely selected or  
25 uniquely generated value.

138. A computer program according to embodiment 137, wherein the computer-executable program file is fabricated by a method according to any of embodiments 1 – 136.

30 139. A computer-readable data medium comprising a computer program according to embodiment 137 or 138.

140. A computer loaded with a computer program according to embodiment 139.

35 141. A computer program according to any of embodiments 137 – 140 where the embedded means for generating at least one value comprises at least one extractor subfunction.

142. A computer program according to embodiment 141 where at least one of the extractor subfunctions is uniquely selected for each computer-executable program file.

143. A computer program according to embodiment 141 or 142 where at least one of the extractor subfunctions is selected from a set of available extractor subfunctions.

5 144. A computer program according to any of embodiments 141 – 143 where at least one of the extractor subfunctions depends on at least one inner state word and generates at least one inner state word.

10 145. A computer program according to any of embodiments 141 – 144 where at least one of the extractor subfunctions depends on a value derived from a key generator initialization vector (key generator IV) where the key generator IV is given as argument to the embedded means for generating at least one value.

15 146. A computer program according to any of embodiments 141 – 145 where at least one of the extractor subfunctions depends on at least one embedded value.

147. A computer program according to any of embodiments 141 – 146 where at least one of the extractor subfunctions comprises at least one of:

- a bijective operation,
- 20 • an arithmetical operation,
- a logical operation,
- a table lookup, and
- an embedded value.

25 148. A computer program according to any of embodiments 141 – 147 where the initial value of at least one of the inner state word depends on a key generator IV.

30 149. A computer program according to any of embodiments 141 – 148 where the output from at least one of the extractor subfunction or a value derived thereof is used as input to a cryptographic function.

150. A computer program according to embodiment 149 where the cryptographic function is a hash function.

35 151. A computer program according to embodiment 150 where the hash function also depends on at least a part of the key generator IV.



152. A computer program according to any of embodiments 141 – 149 where the output from at least one of the extractor subfunction or a value derived thereof is used as a cryptographic key.
- 5 153. A computer program according to any of embodiments 137 – 152 where at least one embedded value is changed at runtime.
154. A computer program according to any of embodiments 137 – 153 where at least one of the at least one embedded uniquely selected values is changed at runtime.
- 10 155. A computer program according to embodiment 153 or 154 where the new value of an embedded value is read from a file.
156. A computer program according to any of embodiments 153 – 155 where the new value of an embedded value is received from a server.
- 15 157. A computer program according to any of embodiments 137 – 156 where at least one embedded value is replaced with a value obtained from a cryptographic function.
- 20 158. A computer program according to embodiment 157 where the cryptographic function is a pseudo-random number generator.
159. A computer program according to 137 – 158 where at least one embedded value is encrypted or decrypted using a cryptographic algorithm.
- 25 160. A computer program according to embodiment 158 or 159 where the PRNG seed or cryptographic key is read from a file.
161. A computer program according to embodiment 158 or 159 where the PRNG seed or cryptographic key is received from a server.
- 30 162. A computer program according to any of embodiments 137 – 161 where the embedded at least one value or means for generating at least one value is used to derive a cryptographic key.
- 35 163. A computer program according to any of embodiments 137 – 162 where an embedded value, a value derived thereof, a value generated by means for generating at least one value, or a value derived thereof is used as input to a cryptographic algorithm where the output of the cryptographic algorithm is used as a cryptographic key.

164. A computer program according to any of embodiments 137 – 163 where the embedded at least one value or means for generating at least one value is used to authenticate a computer program.

5

165. A computer program according to any of embodiments 137 – 164 where the embedded at least one value or means for generating at least one value is used as a serial number or to derive a serial number that can be used to identify the copy of the computer program.

10

166. A computer program according to any of embodiments 137 – 165 where the embedded at least one value or output from means for generating at least one value is combined with at least one of:

- data from the user,
- data about the user,
- 15 • data from something the user possesses, and
- data from the computer the program runs on

to obtain a resulting value.

20

167. A computer program according to any of embodiments 137 – 166 where the means for generating at least one value depends on at least one of:

- data from the user,
- data about the user,
- data from something the user possesses, and
- data from the computer that program runs on

25

in order to generate a resulting value.

168. A computer program according to embodiment 137 or 167 where the resulting value is used as a cryptographic key or to obtain a cryptographic key.

30

169. A computer program according to any of embodiments 152, 162, 163, or 168 where the cryptographic key is used to encrypt or decrypt data.

170. A computer program according to embodiment 169 where the cryptographic key is used to encrypt data to be stored or to decrypt data that has been stored.

35

171. A computer program according to embodiment 169 where the cryptographic key is used to encrypt data to be transmitted or to decrypt data that has been transmitted.

172. A computer program according to any of embodiments 152, 162, 163, or 168 where the cryptographic key it used to generate an authentication tag.
- 5 173. A computer program according to embodiment 172 where the authentication tag is appended to data to be stored or is extracted from data that has been stored.
174. A computer program according to embodiment 172 where the authentication tag is used to authenticate data that has been stored.
- 10 175. A computer program according to embodiment 172 where the authentication tag is appended to data to be transmitted or is extracted and from data that has been transmitted.
176. A computer program according to embodiment 172 where the authentication tag is used to authenticate data that has been transmitted.
- 15 177. A computer program according to any of embodiments 172 – 176 where the authentication tag is used to authenticate at least a part of a computer program.
178. A computer program according to any of embodiments 172 – 177 where the correctness of the authentication tag is verified by a server.
- 20 179. A computer program according to any of embodiments 172 – 178 where the correctness of the authentication tag is verified by a hardware device.
- 25 180. A computer program according to any of embodiments 137 – 179 where a check sum is calculated on a software module; the check sum is compared to an expected value to determine of the software module is authentic.
- 30 181. A computer program according to embodiment 180 where the check sum is calculated by a cryptographic function.
182. A computer program according to embodiment 181 where the cryptographic functions is a hash function.
- 35 183. A computer program according to any of embodiments 137 – 182 where a new version of a computer-executable program file is sent to a user; the new version has the same embedded at least one value or means for generating at least one value as the previous version.

184. A computer program according to any of embodiments 137 – 183 where a computer-executable program file with an embedded at least one value for means for generating at least one value downloads or in another way acquires another computer-executable program file with the same embedded at least one value for means for generating at least one value.
- 5
185. A computer program according to any of embodiments 137 – 184 where the embedded at least one value or means for generating at least one value is copied from one computer-executable program file to another computer-executable program file.
- 10
186. A computer program according to any of embodiments 137 – 185 where information about a program file's embedded at least one value or means for generating at least one value is stored; when the computer-executable program file is updated, this information is updated.
- 15
187. A computer program according to any of embodiments 137 – 185 where information about a program file's embedded at least one value or means for generating at least one value is stored in a database; when the computer-executable program file is updated, its record in the database is updated.
- 20
188. A computer program according to any of embodiments 137 – 187 where the computer program is obfuscated.
189. A computer program according to embodiment 188 where the obfuscation method comprises means for at least one of:
- 25
- replacing a program instruction or a set of program instructions with at least one new program instruction with equivalent functionality,
  - reallocating registers,
  - reordering program instructions,
  - adding or removing jump instructions,
- 30
- inserting useless data or program instructions into the computer program,
  - interleaving at least two program sequences,
  - reordering static data, and
  - reordering runtime data.
- 35
190. A computer program according to any of embodiments 137 – 189 where at least a part of the computer-executable program file is stored in encrypted form and is decrypted at runtime.

191. A computer program according to embodiment 190 where the key to decrypt the encrypted at least a part of the computer-executable program code is downloaded from a server.
- 5 192. A computer program according to embodiment 190 where the encrypted part of the computer-executable program file is decrypted using a cryptographic key derived from the embedded at least one value or means for generating at least one value.
- 10 193. A computer program according to any of embodiments 137 – 192 where a computer-executable program file with embedded at least one value or means for generating at least one value decrypts another computer-executable program file.
- 15 194. A computer program according to any of embodiments 137 – 193 where the destination address of at least one jump instruction in the computer-executable program file is read from a table.
195. A method according to any of embodiments 137 – 194 where at least one parameter to at least one instruction in the computer-executable program file is read from a table.
- 20 196. A computer program according to embodiment 194 or 195 where the at least one entry in the table has a pre-defined value stored in the computer-executable file.
197. A computer program according to any of embodiments 194 – 196 where at least one entry in the table is downloaded from a server.
- 25 198. A computer program according to any of embodiments 194 – 197 where at least one entry in the table is decrypted at runtime.
199. A computer program according to embodiment 197 or 198 where at least one downloaded or decrypted value replaces at least one pre-defined value in the table.
- 30 200. A computer program according to embodiment 198 or 199 where the decryption key is derived from the embedded at least one value or means for generating at least one value.
- 35 201. A computer program according to embodiment 198 or 199 where the decryption key is downloaded from a server.
202. A computer program according to any of embodiments 137 – 201 capable of reading profile data, the profile data comprises at least one of:

- brand, type, version, or serial number of a hardware component,
  - brand, type, version, or serial number of a software component,
  - software or hardware configuration data,
  - network configuration data, and
- 5     • identity of the user.

203. A computer program according to embodiment 202 where profile data is used as input to the means for generating at least one value.

- 10    204. A computer program according to embodiment 202 or 203 where profile data is used to detect if the computer program runs on the right computer.

205. A computer program according to any embodiments 137 – 204 where data sent between program *C* and *D* is encrypted/decrypted; the encryption/decryption key is derived from the embedded at least one value or means for generating at least one value in program *C*; the encryption/decryption key is derived from knowledge about the embedded at least one value or means for generating at least one value in *C* by program *D*.
- 15

206. A computer program according to embodiments 137 – 205 where data is sent in encrypted form between programs *C* and *D*; the encryption/decryption key is derived from the embedded at least one value or means for generating at least one value in program *C*; the encryption/decryption key is derived from knowledge about the embedded at least one value or means for generating at least one value in *C* by program *D*.
- 20

207. A computer program according to embodiments 137 – 206 where data sent between program *E* and *F* is authenticated; the authentication key is derived from the embedded at least one value or means for generating at least one value in program *E*; the authentication key is derived from knowledge about the embedded at least one value or means for generating at least one value in *E* by program *F*.
- 25

208. A computer program according to any of embodiments 205 – 207 where one party in a communication selects a key generator *IV*; the key generator *IV* is sent to the other party; both parties uses the key generator *IV* to derive a key that can be used for encryption/decryption or authentication.
- 30

209. A computer program according to any of embodiments 205 – 207 where both parties in a communication selects a part of a key generator *IV*; the parts are communicated; a key generator *IV* is derived in both ends from the parts; both parties uses the constructed key generator *IV* to derived a key that can be used for encryption/decryption or authentication.
- 35

210. A computer program (*G*) according to any of embodiments 137 – 209 where data is sent in encrypted form between programs *G* and *H* where *G* and *H* both communicates securely with server *I* using cryptographic keys derived from *G*'s and *H*'s embedded at least one value or means for generating at least one value; the server *I* provides at least one cryptographic key to *G* and *H* to be used to encrypt/decrypt at least a part of the data sent between *G* and *H*.
211. A computer program (*J*) according to any of embodiments 137 – 210 where data is sent in authenticated form between programs *J* and *K* where *J* and *K* both communicates securely with server *L* using cryptographic keys derived from *J*'s and *K*'s embedded at least one value or means for generating at least one value; the server *L* provides at least one cryptographic key to *J* and *K* to be used to authenticate at least a part of the data sent between *J* and *K*.
212. A computer program (*M*) according to any of embodiments 137 – 211 where at least one cryptographic key is negotiated between programs *M* and *N* where *M* and *N* both communicates securely with server *O* using cryptographic keys derived from *M*'s and *N*'s embedded at least one value or means for generating at least one value
213. A computer program according to embodiment 212 where *O* provides the same cryptographic key to *M* and *N*.
214. A computer program according to embodiment 212 or 213 where at least one of the at least one cryptographic keys is used to encrypt/decrypt data sent between *M* and *N*.
215. A computer program according to any of embodiments 212 – 214 where at least one of the at least one cryptographic keys is used to authenticate data sent between *M* and *N*.
216. A computer program (*P*) according to any of embodiments 137 – 209 where data is sent in encrypted form between programs *P* and *Q*; *P* derives the encryption/decryption key from its embedded at least one value or means for generating at least one value; *Q* receives the encryption/decryption key from a server.
217. A computer program (*Q*) according to any of embodiments 137 – 209 where data is sent in encrypted form between programs *P* and *Q*; *P* derives the encryption/decryption key from its embedded at least one value or means for generating at least one value; *Q* receives the encryption/decryption key from a server.

218. A computer program (*R*) according to any of embodiments 137 – 209 where data sent between programs *R* and *S* is authenticated; *R* derives the authentication key from its embedded at least one value or means for generating at least one value; *S* receives the authenticate key from a server.

5

219. A computer program (*S*) according to any of embodiments 137 – 209 where data sent between programs *R* and *S* is authenticated; *R* derives the authentication key from its embedded at least one value or means for generating at least one value; *S* receives the authenticate key from a server.

10

220. A computer program according to any of embodiments 210 – 219 where the two communicating programs run on the same computer.

221. A computer program according to embodiment 220 where the two communicating programs read profile data and compare these to verify that they run on the same computer.

15

222. A computer program according to any of embodiments 210 – 219 where the two communicating programs run on different computers.

20

223. A computer program according to any of embodiments 202 – 222 where the two computer programs communicating is a computer program and a software module loaded by the computer program.

224. A computer program according to embodiment 223 where the software module is a .dll file.

25

225. A computer program according to any of embodiments 137 – 224 where key exchange protocol data is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value.

30

226. A computer program according to any of embodiments 137 – 225 where key exchange protocol data is authenticated using a cryptographic key derived from an embedded at least one value or means for generating at least one value.

35

227. A compute program according to embodiment 225 or 226 where the key exchange protocol is the Diffie-Hellman protocol.

228. A computer program according to any of embodiments 225 – 227 where the key exchange protocol is used to derive a symmetrical cryptographic key.



229. A computer program according to any of embodiments 137 – 228 where an asymmetric key is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value.
- 5
230. A computer program according to any of embodiments 137 – 229 where an asymmetric key is authenticated using a cryptographic key derived from an embedded at least one value or means for generating at least one value.
- 10
231. A computer program according to embodiment 229 or 230 where the asymmetric key is a public RSA key or a private RSA key.
232. A computer program according to embodiment 229 or 230 where the asymmetric key is a public ECC key or a private ECC key.
- 15
233. A computer program according to any of embodiments 229 – 232 where the asymmetric key is used to derive a symmetrical cryptographic key.
234. A computer program according to embodiment 228 or 233 where the symmetrical key is used to encrypt or decrypt data.
- 20
235. A computer program according to any of embodiments 228, 233, and 234 where the symmetrical key is used to authenticate data.
- 25
236. A computer program according to any of embodiments 137 – 235 where data to be stored is encrypted or data that has been stored is decrypted; the encryption/decryption key is derived from the embedded at least one value or means for generating at least one value.
- 30
237. A computer program according to any of embodiments 137 – 236 where data to be stored or that has been stored is processed in order to generate an authentication tag; the authentication key is derived from the embedded at least one value or means for generating at least one value.
- 35
238. A computer program according to embodiment 236 or 237 where a key generator IV is used to derive the encryption/decryption key or authentication key; the key generator IV is stored with the data.

239. A computer program according to embodiment 236 or 237 where a value stored with the data is hashed with profile data to obtain a key generator IV used to derive the encryption/decryption key or authentication key.
- 5 240. A computer program according to any of embodiments 138 – 239 where a cryptographic key is stored in encrypted form; the decryption key to be used to decrypt the cryptographic key is derived from the embedded at least one value or means for generating at least one value.
- 10 241. A computer program according to any of embodiments 137 – 240 where a cryptographic key is stored in encrypted form; the decryption key to be used to decrypt the cryptographic key is downloaded from a server.
- 15 242. A computer program according to any of embodiments 137 – 241 where credit card information is encrypted or decrypted using a cryptographic key derived from the embedded at least one value or means for generating at least one value.
- 20 243. A computer program according to any of embodiments 137 – 242 where payment authorization data is encrypted or decrypted using a cryptographic key derived from the embedded at least one value or means for generating at least one value.
244. A computer program according to embodiment 243 where the payment authorization data comprises a credit card number.
- 25 245. A computer program according to embodiment 243 or 244 where the payment authorization data comprises a one-time password or one-time key.
246. A computer program according to any of embodiments 137 – 245 inserted into a file.
- 30 247. A server from which computer programs according to any of embodiments 137 – 246 can be downloaded.
- 35 248. A server according to embodiment 247 which has different versions of the computer program to be downloaded; the server decides which one to send according to predefined criteria.
249. A server according to embodiment 248 where the decision depends on knowledge about the computer downloading the computer program.

250. A server communicating with at computer program according to any of embodiments 137 – 246.
251. A file written by computer program according to any of embodiments 137 – 246.
- 5
252. An file encrypted using a key; the decryption key can be derived or decrypted using at an embedded at least one value or means for generating at least one value in a computer program according to any of embodiments 137 – 246.
- 10
253. Data sent over a network; the data is encrypted by a computer program according to any of embodiments 137 – 246.
254. Data sent over a network; the data is encrypted using a key; the decryption key can be derived or decrypted using an embedded at least one value or means for generating at least
- 15
- one value in a computer program according to any of embodiments 137 – 246.
255. Data sent over a network; the data is authenticated by a computer program according to any of embodiments 137 – 246.
- 20
256. A document into which at least one computer program according to any embodiments 137 – 246 is embedded.
257. A computer on which at least one computer program according to any of embodiments 137 – 246 is stored or executed.
- 25
258. A method of generating a one-time password, the method including the steps of any of embodiments 137 – 257.
259. A method of generating a one-time password in a device comprising a computer-executable program file fabricated from a source code, the computer program including, in
- 30
- said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of generating a unique output,
- 35
- which depends from said uniquely selected or uniquely generated value, the method further comprising the step of processing said unique output to generate said one-time password.
260. A method according to embodiment 294 or 259 where the one-time password is derived from an embedded at least one value or means for generating at least one value.

261. A method according to embodiment 294 or 259 where the one-time password is derived from a master key; the master key is derived from an embedded at least one value or means for generating at least one value.

5

262. A method according to any of embodiments 294 – 261 where the one-time password is derived from a counter value; the counter is increased each time a one-time password is generated.

10

263. A method according to any of embodiments 294 – 262 where the one-time password is derived from a time stamp.

264. A device containing a one-time password generator constructed according to any of embodiments 294 – 263.

15

265. A computer network comprising a server and a plurality of clients, wherein each client is loaded with a copy of a first computer program, and wherein the server is loaded with a second computer program, each copy of the first computer program comprising:

20

- a computer-executable program file fabricated from a source code, which is common to all copies of the first computer program;
- at least one embedded value or means for generating at least one value, said value or said means being included in said computer-executable program file, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the common source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value; the computer network being programmed to communicate said unique output from each of the clients to the server, so as to enable the second computer program to authenticate each copy of the first computer program based on said output.

25

30

266. A computer network according to embodiment 265, wherein each computer-executable program file is fabricated by a method according to any of embodiments 1 – 136.

35

267. A server for use in a computer network according to embodiment 265 or 266, the server being suited for communication with said plurality of clients via the computer network, said second computer program being adapted to authenticate each copy of said first computer program based on said unique output.

268. A method of generating a combined software component, comprising:

- providing at least two non-combined software components, which are intended to be combined by an operating system at runtime or in a runtime environment;
  - combining said at least two non-combined software components into a pre-combined software component before runtime;
- 5     • adding, to said pre-combined software component, functionality for performing operations that would have been performed by the operating system or the runtime environment, if the non-combined software components were combined at runtime, to thereby generate said combined software component.
- 10   269. A method according to embodiment 268 where at least one of the software components is a function implementations, a class, a library file, or a program file.
270. A method according to embodiment 268 or 269 where at least one of the software components is a Java .class files, a Java .java files, or a function implementation is such files.
- 15   271. A method according to any of embodiments 268 – 270 where at least one of the software components is a .dll file or a function in such file.
272. A method according to embodiment 268, 269, or 271 where an .exe or a .dll file is derived from resulting software component.
- 20   273. A method according to any of embodiments 268 – 272 where at least one of the added means for handling tasks that otherwise would be handled by the runtime environment or operating system is means for handling memory allocation, stack operations, or errors.
- 25   274. A method according to any of embodiments 268 – 273 where the destination address of at least one jump instruction in the combined software component is read from a table.
275. A method according to any of embodiments 268 – 274 where at least one parameter to at least one instruction in the combined software component is read from a table.
- 30   276. A method according to embodiment 274 or 275 where at least a part of the table is downloaded from a server.
- 35   277. A method according to embodiment 276 where the at least a part of the table have a pre-defined value that is used until the at least a part of the table is downloaded from a server.

278. A method according to any of embodiments 274 – 277 where at least a part of the table is decrypted at runtime.
279. A method according to embodiment 278 where the decryption key is derived from the embedded at least one value or means for generating at least one value.
280. A method according to embodiment 278 where the decryption key is downloaded from a server.
281. A software component combined according to any of embodiments 268 – 280.
282. A computer-readable data medium comprising a software component according to embodiment 281.
283. A computer loaded with a software component according to embodiment 281.
284. A number of software components, which at runtime are linked together, at least one of the software components is a resulting software component or is derived from a resulting software component according to any of embodiments 268 - 280.
285. A method of fabricating a computer program according to any of embodiments 268 - 280 with an embedded at least one value or means for generating at least one value according to any of embodiments 1 – 136.
286. A computer program according to any of embodiments 268 - 280 with an embedded at least one value or means for generating at least one value according to any of embodiments 137 – 264.
287. A server communicating with a client computer program comprising a computer-executable program file fabricated from a source code, the computer program including, in said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value.
288. A server according to embodiment 287 with functionality that allows it to recreate at least one of
- at least one of the at least one embedded values, and

- at least a part of the embedded means for generating at least one value as is embedded in a Client Program.

289. A server according to embodiment 287 that can load from a database or file at least one  
5 of

- at least one of the at least one embedded values, and
- at least a part of the embedded means for generating at least one value as is embedded in a Client Program.

10 290. A server according to any of embodiments 287 – 289 that can load from a database or file the PRNG seed that was used to generate the string of pseudo-random bits that determined at least one of

- at least one of the at least one embedded values, and
  - how to construct at least a part of the embedded means for generating at least one  
15 value
- when a Client Program file was fabricated.

291. A server according to embodiment 287 that can load and use a software module containing at least one of:

- at least one of the at least one embedded values, and
  - at least a part of the embedded means for generating at least one value.
- 20

292. A server according to embodiment 291 where the loaded software module is stored in a file with program code that is linked with the server's program code at runtime.

25

293. A server according to embodiment 292 where the loaded software module is stored in a .dll file.

294: A server according to any of embodiments 287 – 293 where the recreated or loaded at  
30 least one value or means for generating at least one value is kept ready-to-use for a certain period of time after the session with the relevant program has ended such that the recreated or loaded at least one value or means for generating at least one value is ready for use in case of the given program connects to the server again within the given period of time.

35 295. A server according to any of embodiments 287 – 294 having a list of which rights are assigned to which types of Client Programs.

296. A server according to any of embodiments 287 – 295 having a list of which rights are assigned to which copies of the Client Program.

297. A server according to embodiment 295 or 296 where the assigned rights relate to which data types Client Program may read or write.
- 5 298. A server according to embodiment 295 or 296 where the assigned rights relate to which instances of data Client Program may read or write.
299. A server according to embodiment 295 or 296 where the assigned rights relates to who are allowed to execute Client Program.
- 10 300. A server according to embodiment 295 or 296 where the assigned rights relates to when a Client Program is allowed to be executed.
301. A server according to embodiment 295 or 296 where the assigned rights relates to when a Client Program is allowed to access which data.
- 15 302. A server according to any of embodiments 295 – 301 where a Client Program connects to the server to download information about its rights.
- 20 303. A server according to embodiment 302 where the downloaded information about the Client Programs rights is stored on disk by the Client Program.
304. A server according to any of embodiments 295 – 303 where a Client Program connects to the server to download cryptographic keys that can be used to encrypt, decrypt, or
- 25 authenticate data.
305. A server according to embodiment 304 that refuses to provide keys to access types of data or copies of data that the Client Program is not allowed to access.
- 30 306. A server according to any of embodiments 295 – 305 where a log file is maintained with information about which Client Programs have been given which rights.
307. A server according to any of embodiments 295 – 306 where a log file is maintained with information about which Client Programs have been given which cryptographic keys.
- 35 308. A server according to any of embodiments 287 – 307 where key exchange protocol data communicated with a Client Program is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value in the Client Program.



- 5 309. A server according to any of embodiments 287 – 307 where key exchange protocol data communicated with a Client Program is authenticated using a cryptographic key derived from an embedded at least one value or means for generating at least one value in the Client Program.
310. A server according to embodiment 308 or 309 where the key exchange protocol is the Diffie-Hellman protocol.
- 10 311. A server according to any of embodiments 308 – 310 where the key exchange protocol is used to derive a symmetrical cryptographic key.
- 15 312. A server according to any of embodiments 287 – 311 where an asymmetric key is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value in the Client Program.
- 20 313. A server according to any of embodiments 287 – 312 where an asymmetric key is authenticated using a cryptographic key derived from an embedded at least one value or means for generating at least one value in the Client Program.
314. A server according to embodiment 312 or 313 where the asymmetric key is a public RSA key or a private RSA key.
- 25 315. A server according to embodiment 312 or 313 where the asymmetric key is a public ECC key or a private ECC key.
316. A server according to any of embodiments 312 – 315 where the asymmetric key is used to derive a symmetrical cryptographic key.
- 30 317. A server according to embodiment 312 or 316 where the symmetrical key is used to encrypt or decrypt data.
318. A server according to any of embodiments 311, 316, and 317 where the symmetrical key is used to authenticate data.
- 35 319. A server according to any of embodiments 287 – 318 where Client Programs with functionality for sending e-mail, sending instant messages, or conducting phone calls connecting to the server are authenticated.

320. A server according to embodiment 319 where Client Programs with functionality for sending e-mail, sending instant messages, or conducting phone calls that cannot authenticate themselves are rejected.

5 321. A server according to embodiment 319 or 320 that adds special headers to e-mails, instant messages, or phone calls received from an authenticated Client Program.

322. A server according to any of embodiments 319 – 320 that signs e-mails, instant messages, or phone calls received from an authenticated Client Program.

10

323. A server according to any of embodiments 319 – 322 maintaining a list of black-listed Client Programs.

15 324. A server according to any of embodiments 287 – 323 where credit card information is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value in the Client Program.

20 325. A server according to any of embodiments 287 – 324 where payment authorization data is encrypted or decrypted using a cryptographic key derived from an embedded at least one value or means for generating at least one value in the Client Program.

326. A server according to embodiment 325 where the payment authorization data comprises a credit card number.

25 327. A server according to embodiment 325 or 326 where the payment authorization data comprises a one-time password or one-time key.

328. A computer program communicating with a server according to any of embodiments 287 – 327.

30

329. A file encrypted by a server according to any of embodiments 287 – 327.

330. Data sent over a network; the data is encrypted by a server according to any of embodiments 287 – 327.

35

331. Data sent over a network; the data is authenticated by a server according to any of embodiments 287 – 327.

332. A computer-readable data medium comprising server software according to any of embodiments 287 – 327.

5 333. A computer program communicating with a server according to any of embodiments 287 – 327.

334. A device communicating with a server according to any of embodiments 287 – 327.

## CLAIMS

1. A method of fabricating computer-executable program files from a source code, the  
5 method comprising the step of embedding, in each of the fabricated computer-executable  
program files, at least one value or means for generating at least one value, said value being  
uniquely selected or generated for each of the fabricated computer-executable program files,  
whereby all of the fabricated computer-executable program files are capable of carrying out  
10 instructions defined by the source code, and whereby each individual computer-executable  
program file is capable of generating a unique output, which depends on said uniquely  
selected or uniquely generated value.
2. A method according to claim 1 wherein each user or group of users uses a different copy  
15 of the computer-executable program file.
3. A method according to claim 1 or 2 wherein the embedded means for generating at least  
one value depends on at least one embedded value.
4. A method according to any of the preceding claims wherein the process of fabricating  
20 computer-executable program files from a source code is divided into at least two steps; a  
first step of converting source code into at least one intermediate file is performed once, and  
a later step of converting at least one intermediate file and optionally other files into a  
computer-executable program file is performed for each computer-executable program file.
- 25 5. A method according to any of the preceding claims wherein at least a part of the source  
code is evaluated to determine if it meets one or more predefined criteria for being equipped  
with the embedded at least one value or means for generating at least one value.
6. A method according to any of the preceding claims wherein the embedded means for  
30 generating at least one value comprises at least one extractor subfunction.
7. A method according to claim 6 wherein the at least one extractor subfunction is uniquely  
selected for each computer-executable program file.
- 35 8. A method according to any of the preceding claims wherein the embedded at least one  
value or means for generating at least one value is used to derive a cryptographic key.
9. A method according to claim 8 wherein the cryptographic key is used to generate an  
authentication tag.

10. A method according to any of the preceding claims wherein the embedded at least one value or means for generating at least one value is used to authenticate a computer program.
- 5
11. A method according to any of the preceding claims wherein the embedded at least one value or means for generating at least one value is used as a serial number or to derive a serial number that can be used to identify the copy of the computer program.
- 10
12. A method according to any of the preceding claims wherein information about how a computer-executable program file is generated is stored such that the computer-executable program file can be reproduced or its functionality or part thereof can be reproduced or simulated.
- 15
13. A method of fabricating computer-executable program files according to any of the preceding claims comprising the following steps:
1. choosing a PRNG seed,
  2. generating a string of pseudo-random bits from the PRNG seed using a pseudo-random number generator,
  - 20 3. using the string of pseudo-random bits to determine at least one embedded value or how to construct the embedded means for generating at least one value.
14. A method according to claim 13 wherein the PRNG seed is stored for later use.
- 25
15. A method according to claim 13 or 14 wherein the PRNG seed is used to generate at least a part of the string of pseudo-random bits again, and wherein the string of bits is used to recreate at least one embedded value or the embedded means for generating at least one value.
- 30
16. A method according to any of claims 13 to 15 wherein the PRNG seed is used to allow a computer program or a hardware device to create the same cryptographic key as a computer-executable program file being executed; the PRNG seed is used to reproduce the embedded at least one value or means for generating at least one value embedded into the computer executable program file on the computer program or hardware device such that
- 35
- two parties can generate the same cryptographic keys derived from the embedded at least one value or means for generating at least one value.
17. A method according to any of the preceding claims wherein the computer-executable program files are obfuscated.

18. A method according to claim 17, wherein obfuscation uses a random or pseudo-random input, so that the obfuscated computer-executable program file varies in accordance with the random or pseudo-random input.

5

19. A method according to any of the preceding claims wherein at least a part of the computer-executable program file is stored in encrypted form and is decrypted at runtime.

20. A method according to claim 19 wherein the key to decrypt the encrypted at least a part of the computer-executable program code is downloaded from a server.

10

21. A method according to any of the preceding claims wherein a computer-executable program file with at least one embedded value or embedded means for generating at least one value contains program code that can read profile data, the profile data comprises at least one of:

15

- brand, type, version, or serial number of a hardware component,
- brand, type, version, or serial number of a software component,
- software or hardware configuration data,
- network configuration data, and
- identity of the user

20

wherein the profile data is used as input to the means for generating at least one value.

22. A method according to any of the preceding claims wherein data is sent in encrypted or authenticated form between programs *C* and *D*; the encryption/decryption key or authentication key is derived from the embedded at least one value or means for generating at least one value in program *C*; the encryption/decryption key or authentication key is derived in program *D* from knowledge about the embedded at least one value or means for generating at least one value in *C*.

25

23. A method according to any of the preceding claims wherein data is sent in encrypted or authenticated form between programs *G* and *H* where *G* and *H* both communicates securely with server *I* using cryptographic keys derived from *G*'s and *H*'s embedded at least one value or means for generating at least one value, and wherein the server *I* provides at least one cryptographic key to *G* and *H* to be used to encrypt/decrypt or authenticate at least a part of the data sent between *G* and *H*.

30

35

24. A server from which computer-executable program files fabricated according to any of the preceding claims can be downloaded.

25. A server communicating with a computer-executable program file fabricated according to any of the preceding claims.
26. A document into which at least one computer-executable program file fabricated according to any of the preceding claims is embedded.
27. A computer on which at least one computer-executable program file fabricated according to any of the preceding claims is stored or executed.
28. A computer program for fabricating computer-executable program files from source code, the computer program comprising means for performing the method of any of the preceding claims.
29. A computer-readable data medium comprising a computer program according to claim 28.
30. A computer loaded with a computer program according to claim 28.
31. A computer-executable program file fabricated by a method according to any of claims 1 – 23.
32. A computer program comprising a computer-executable program file fabricated from a source code, the computer program including, in said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value.
33. A computer program according to claim 32, wherein the computer-executable program file is fabricated by a method according to any of claims 1 – 23.
34. A computer network comprising a server and a plurality of clients, wherein each client is loaded with a copy of a first computer program, and wherein the server is loaded with a second computer program, each copy of the first computer program comprising:
- a computer-executable program file fabricated from a source code, which is common to all copies of the first computer program;
  - at least one embedded value or means for generating at least one value, said value or said means being included in said computer-executable program file, said value being

5 uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the common source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value; the computer network being programmed to communicate said unique output from each of the clients to the server, so as to enable the second computer program to authenticate each copy of the first computer program based on said output.

10 35. A computer network according to claim 34, wherein each computer-executable program file is fabricated by a method according to any of claims 1 – 23.

15 36. A server for use in a computer network according to claim 34 or 35, the server being suited for communication with said plurality of clients via the computer network, said second computer program being adapted to authenticate each copy of said first computer program based on said unique output.

20 37. A server communicating with a client computer program comprising a computer-executable program file fabricated from a source code, the computer program including, in said computer-executable program file, at least one embedded value or means for generating at least one value, said value being uniquely selected or uniquely generated for the computer-executable program file, whereby the computer-executable program file is capable of carrying out instructions provided by the source code and of generating a unique output, which depends from said uniquely selected or uniquely generated value.

25 38. A server according to claim 37 with functionality that allows it to recreate at least one of

- at least one of the at least one embedded values, and
- at least a part of the embedded means for generating at least one value

as is embedded in a Client Program.

30 39. A server according to claim 37 that can load from a database or file at least one of

- at least one of the at least one embedded values, and
- at least a part of the embedded means for generating at least one value

as is embedded in a Client Program.



1/8

Figure 1

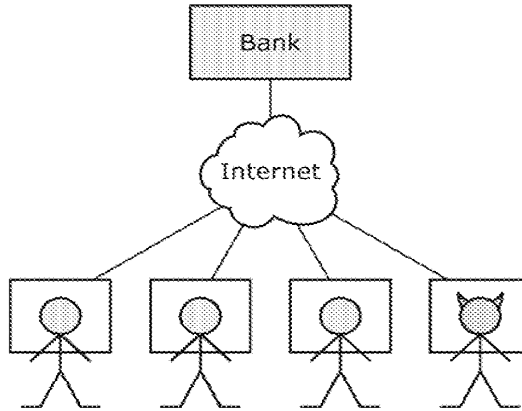


Figure 2

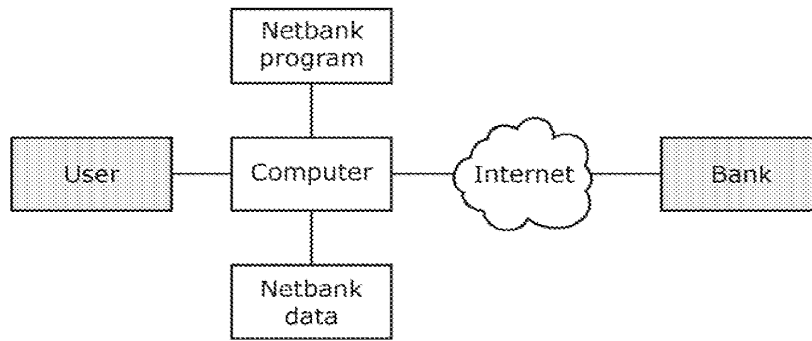
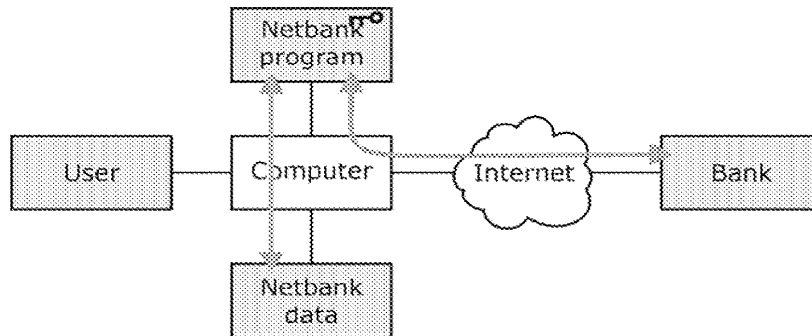


Figure 3



2/8

Figure 4

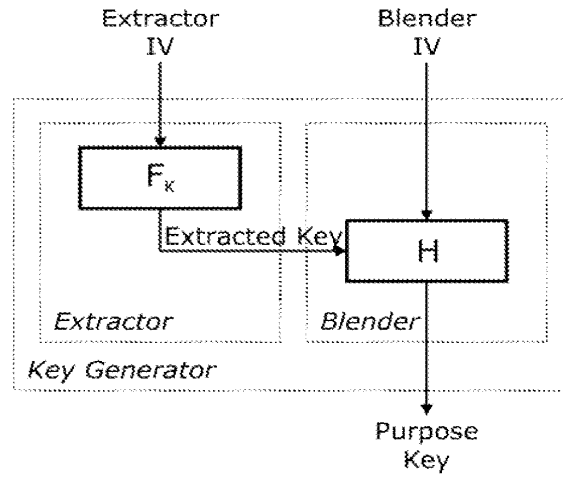
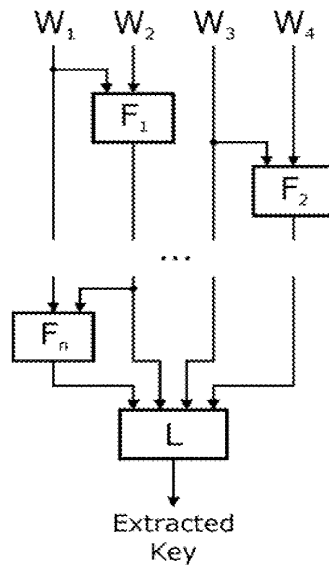


Figure 5



3/8  
Figure 6

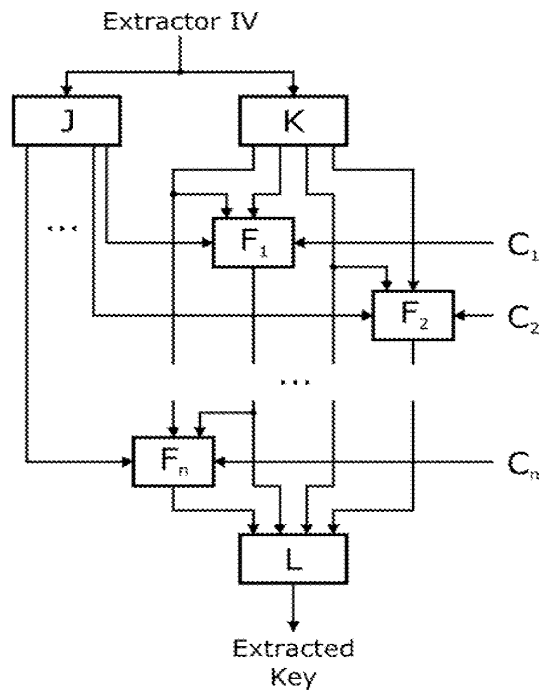
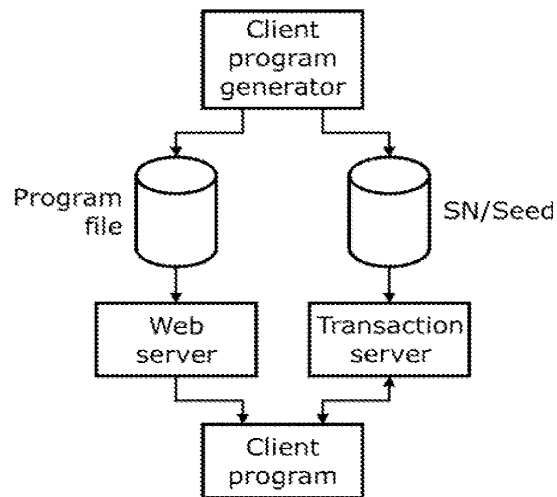


Figure 7



4/8

Figure 8

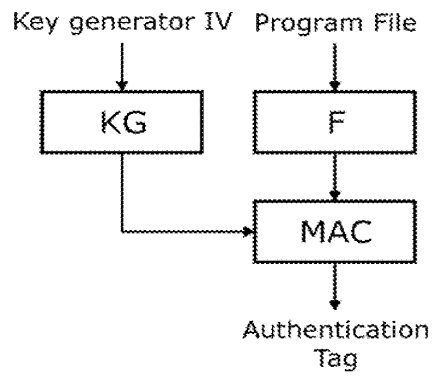
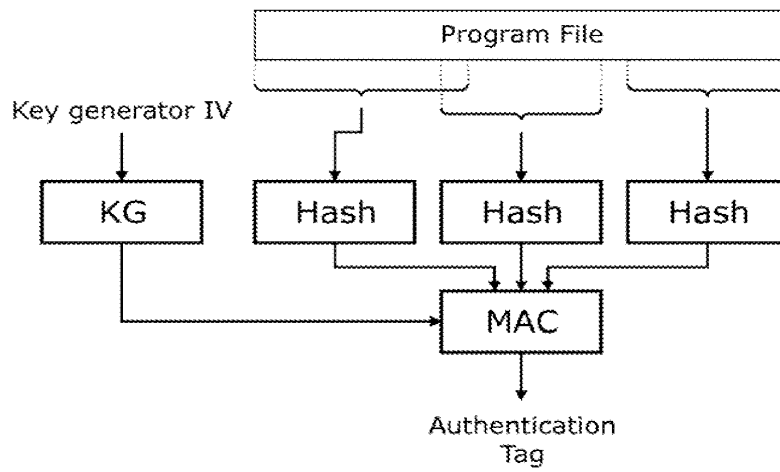


Figure 9



5/8  
Figure 10

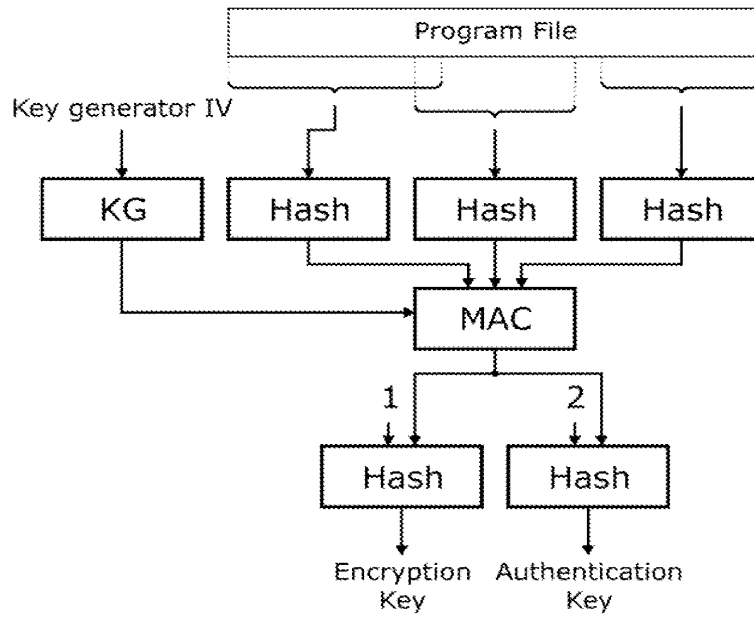
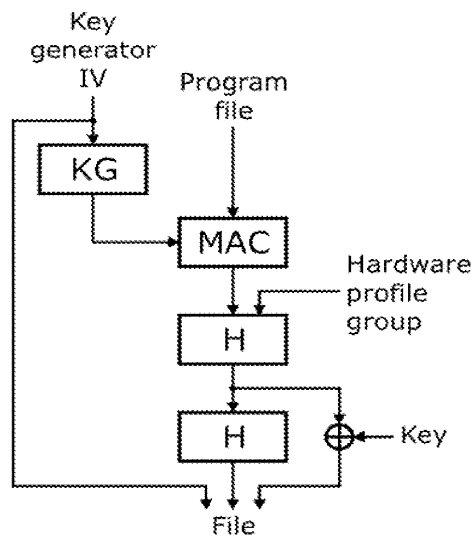
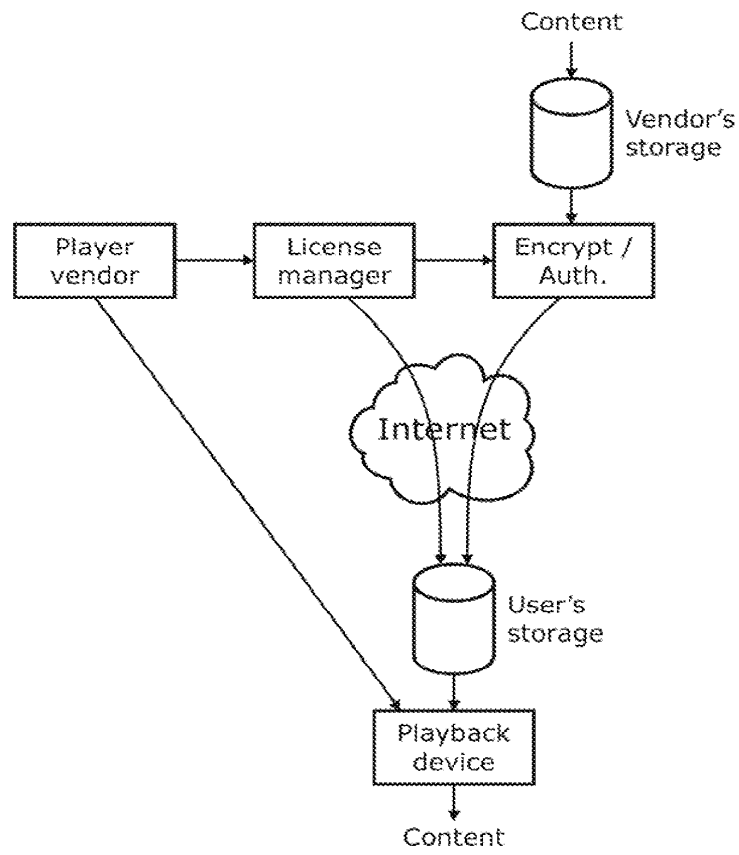


Figure 11



6/8  
Figure 12



7/8  
Figure 13

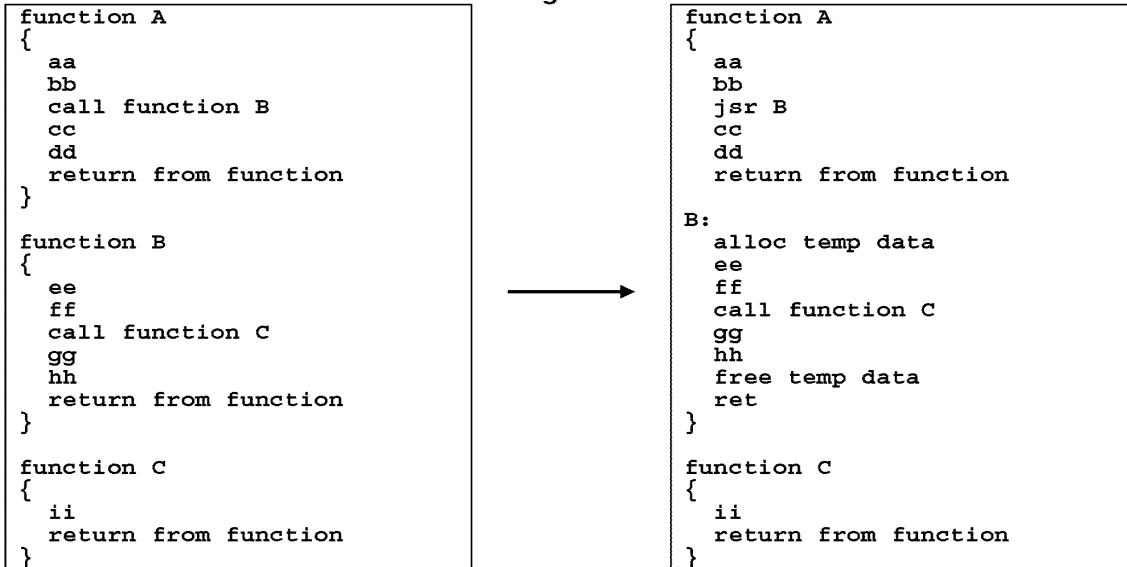
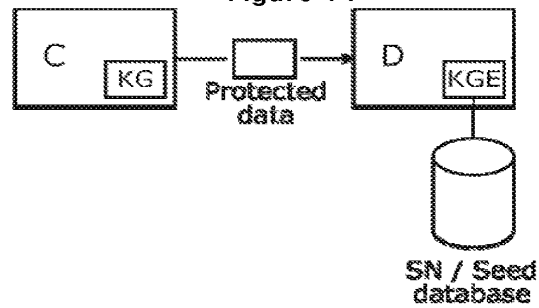
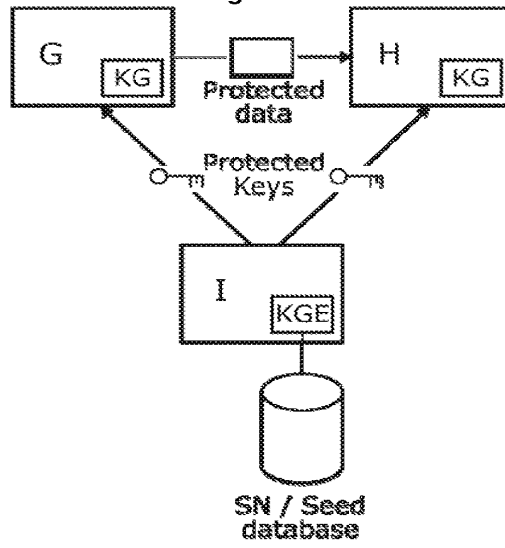


Figure 14



8/8  
Figure 15





**INTERNATIONAL SEARCH REPORT**

International application No  
PCT/EP2007/060056

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> INV. G06F21/22		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols) 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, WPI Data		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 513 113 A1 (FRANCE TELECOM [FR]) 9 March 2005 (2005-03-09) the whole document	1-39
X	US 2001/051928 A1 (BRODY MOSHE [IL]) 13 December 2001 (2001-12-13)  paragraph [0130] - paragraph [0191]	1,2,4, 10,11, 19,24-33
A	US 6 668 325 B1 (COLLBERG CHRISTIAN SVEN [NZ] ET AL) 23 December 2003 (2003-12-23) column 1, line 1 - column 37, line 9	17,18
A	column 37, line 10 - line 62	34-36
A	WO 99/18490 A (I P R CO 21 LIMITED [GB]; JAMIESON ANGUS LAMBERTON [GB]) 15 April 1999 (1999-04-15) page 3, line 3 - page 4, line 29	21
	-/--	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family 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  19 December 2007		Date of mailing of the international search report  02/01/2008
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  Segura, Gustavo

INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2007/060056

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 006 328 A (DRAKE CHRISTOPHER NATHAN [AU]) 21 December 1999 (1999-12-21) column 5, line 35 - column 6, line 16 column 13, line 55 - column 18, line 6 figures 6,10-13 -----	19,20
A	US 2005/188214 A1 (WORLEY JOHN S [US] ET AL) 25 August 2005 (2005-08-25) abstract paragraph [0048] - paragraph [0056] -----	10
A	BELLARE M ET AL INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH: "KEYING HASH FUNCTIONS FOR MESSAGE AUTHENTICATION" 18 August 1996 (1996-08-18), ADVANCES IN CRYPTOLOGY - CRYPTO '96. 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, PAGE(S) 1-15 , XP000626584 ISBN: 3-540-61512-1 paragraph [01.1] -----	9

Form PCT/ISA/210 (continuation of second sheet) (Apr. 2005)

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No

PCT/EP2007/060056

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1513113	A1	09-03-2005	AT 332549 T 15-07-2006
			CN 1617492 A 18-05-2005
			DE 60306648 T2 21-06-2007
			ES 2268296 T3 16-03-2007
			JP 2005080315 A 24-03-2005
			US 2005086479 A1 21-04-2005
US 2001051928	A1	13-12-2001	NONE
US 6668325	B1	23-12-2003	AU 7957998 A 25-01-1999
			CA 2293650 A1 14-01-1999
			CN 1260055 A 12-07-2000
			EP 0988591 A1 29-03-2000
			JP 2002514333 T 14-05-2002
			WO 9901815 A1 14-01-1999
WO 9918490	A	15-04-1999	AU 9275098 A 27-04-1999
US 6006328	A	21-12-1999	NONE
US 2005188214	A1	25-08-2005	NONE

Form PCT/ISA/210 (patent family annex) (April 2005)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
8 May 2008 (08.05.2008)

PCT

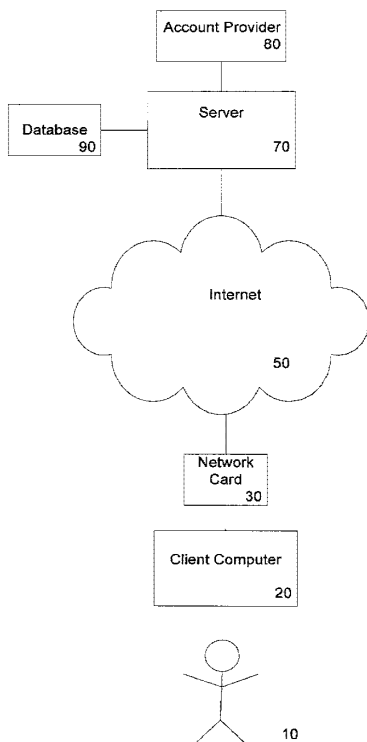
(10) International Publication Number  
**WO 2008/052310 A1**

- (51) **International Patent Classification:**  
*H04L 9/32* (2006.01) *G06Q 20/00* (2006.01)
- (21) **International Application Number:**  
PCT/CA2007/001767
- (22) **International Filing Date:** 4 October 2007 (04.10.2007)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**  
60/849,008 4 October 2006 (04.10.2006) US
- (71) **Applicant (for all designated States except US):** **PGMX, INC.** [US/US]; 1134 Glen Road, Lafayette, California 94549 (US).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** **BARTLETT, Rob** [CA/CA]; 3248 Stonegate Court, Westbank, British Columbia V4T 1A7 (CA). **KHARE, Anuj** [IN/IN]; E-146 Ashok Vihar-1, Delhi 110052 (IN). **KHARE, Rajat** [IN/IN]; E-146 Ashok Vihar-1, Delhi 110052 (IN). **WIG,**

- Tarun** [IN/IN]; A 2/24 Shakti Nagar Extn, Delhi 110052 (IN). **MALHOTRA, Dheeraj** [IN/IN]; 126/39, Block-G, Govind Nagar, Kapnpur 208006 UP (IN).
- (74) **Agent:** **INGALLS, Doran;** c/o Fasken Martineau Du-Moulin, 2100 - 1075 West Georgia Street, Vancouver, British Columbia V6E 3G2 (CA).
- (81) **Designated States (unless otherwise indicated, for every kind of national protection available):** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States (unless otherwise indicated, for every kind of regional protection available):** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) **Title:** METHOD AND SYSTEM OF SECURING ACCOUNTS



(57) **Abstract:** A method and system of securing account is provided. When a client computer requests access to an account accessible via a server, the server determines a mac address associated with the client computer and compares it to a mac address associated with the account. If the mac address of the client computer is not the same as the mac address associated with the account, the server initially denies access to the client computer, but may allow access after verification of the client computer by the user associated with the account.

WO 2008/052310 A1



ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IS, IT, LI, LU, LV, MC, MT, NL, PL,  
PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM,  
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— *with international search report*

## METHOD AND SYSTEM OF SECURING ACCOUNTS

This application claims the benefit of U.S. Provisional Patent Application No. 60/849,008, filed October 4, 2006, which is hereby incorporated by reference.

### FIELD OF THE INVENTION

- 5 This invention relates to methods and systems of conducting secure transactions over a computer network, and more particularly to securing authentication systems used in such transactions.

### BACKGROUND OF THE INVENTION

- 10 Networks, particularly the global computer network known as the Internet, are now used for many purchases and other business transactions, usually by means such as a credit card. A key component of these credit card transactions is the ability to authenticate the holder of the credit card, as the absence of signatures and face-to-face contact between the transacting parties makes authentication of the credit card holder difficult.

- 15 At present, malicious users can gain unauthorized access to online accounts and/or credit cards of account users by hacking, or stealing or phishing passwords or personal info. These accounts may include game accounts, bank accounts, and online payment processing systems like those offered by PayPal™ or credit card processors. Currently, the preferred way to offer significant security online is to request additional security questions from the user, which is an inconvenience to the user, and possibly a further security risk. Most online authentication systems therefore trade convenience for security.

- 20 Online banking tends to have significantly better security compared to payment systems for other account providers such as PayPal, or accounts for online games. This is because if a malicious user gains access to an online bank account, they can do a significant amount of damage, and the bank may be liable (they have no merchants on whom to offload the liability). Therefore, it is in the bank's best interest to ensure that it is difficult to access an online bank account. Some banks use  
25 cookies and additional security questions to secure their systems, but, as described above, this is an inconvenience to clients.

Most account providers, such as game companies and payment processors, have relatively weak authentication systems. Once a password is known, a malicious user may access accounts and misuse such accounts, usually from any computer. The account provider and/or the account user must take steps to protect their account. As an example, PayPal requests an account user to verify their account and address at registration, but once that is completed, only a single password is needed to allow access to the account.

Credit card processors typically ask account users for address verification and the Credit Card Verification (CCV) number on the back of the card; and may also ask account users for a password. If a malicious user accesses this information, they may make fraudulent orders with the credit card. Therefore, it is up to the merchant accepting the credit card to protect themselves against malicious users as the credit card payment processor will not usually take the necessary steps to do so (for example by comparing the Internet Protocol (IP) address of the client computer operated by the credit card user to the region in which the order is being made, or calling the credit card user).

Internet service providers (ISPs) may restrict access of users to the Internet, often based on the Media Access Control (MAC) address of the computer being used. If a user tries to connect a new computer to the ISP using an Internet connection, they may have to register the new MAC address with the ISP before receiving permission. The MAC address of a computer is a unique identifier that can correctly identify a particular computer on a local area network. It is possible to spoof or change a MAC address, but typically it is only possible to discover the MAC address of a computer from the same local area network.

Some account providers, such as online banks, use improved security systems which are cookie based. These systems ask an account user to “remember this computer” or “remember this password” after asking one or two security questions. Once the computer is registered, these extra questions are not asked again unless the cookies are deleted from the computer. A deficiency of this system is that it requires the use of cookies, which is not permitted by all account users and many account users do not want to provide answers to additional security questions to access their account.

There have been various attempts in the prior art to solve this account user authentication issue, including U.S. Patent Publication No. 2004/0117321 to Sancho, for a system and method for secure network purchasing. Sancho discloses that once a merchant/client transaction is initiated, that it can be traced back to the originating computer using the IP address of that computer, which does not  
5 change during the transaction.

U.S. Patent Publication No. 2005/0177442 to Sullivan et al., for a method and system for performing a retail transaction using a wireless device, discloses a method of identifying a wireless Internet connection for an online purchase, and matching a customer account with transaction data. This system is dependent on a customer account registered with the wireless device, and requires  
10 the computer to already have a registered customer account.

U.S. Patent Publication No. 2005/0033653 to Eisenberg et al., for an electronic mail card purchase verification, discloses a method of looking for additional information about the purchaser to verify that the transaction is not suspicious. This application discloses an automation process for standard security checks known in the art.

U.S. Patent Publication No. 2004/0243832 to Wilf et al., for a verification of a personal identifier received online, discloses a method of ensuring secure communication between two computers over  
15 a connection.

PCT Patent Application No. WO 2004/027620 to Freidman et al., for an authentication system and method, discloses an authentication system with proprietary identification codes, which must be  
20 installed on the client/authenticating computers. The MAC address of the computer is used along with other system details to produce a unique identifier for the client computer that is software dependent. A system that requires such a software installation may be difficult to implement (and account users may not want to install additional software). Such systems also limit the account user to a single computer, and must be reinstalled when making a purchase or accessing an account from  
25 a new computer. If any system is too complicated, while it may be secure, it may not practical in application. This is a reason why most current authentication systems (with the exception of bank accounts and very secure sites) are poor, as they trade convenience for security.