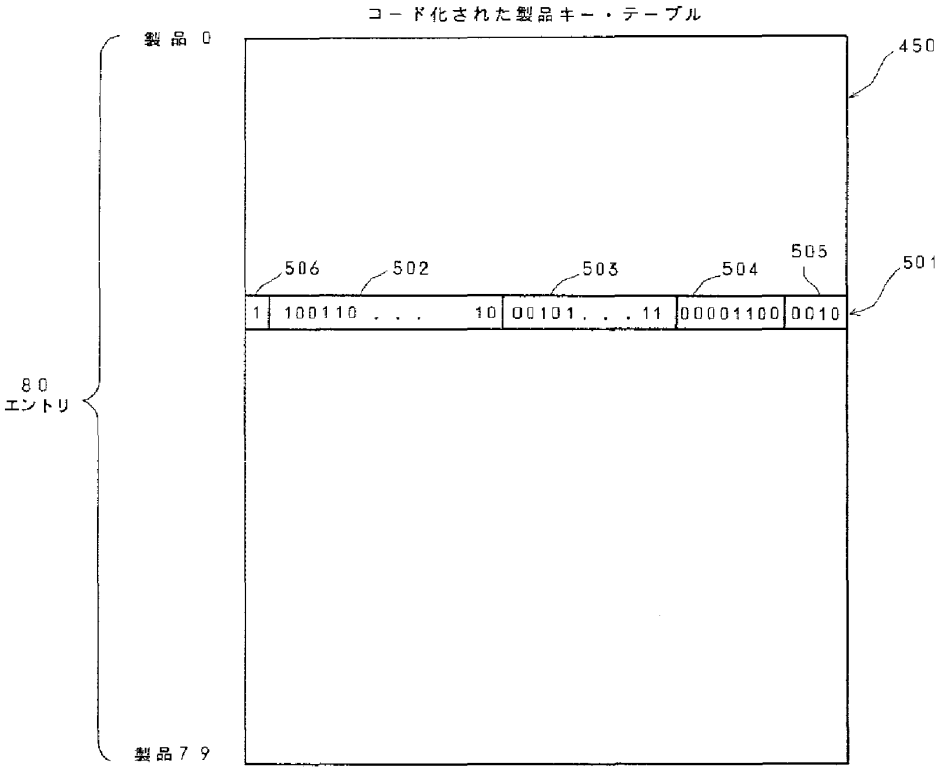
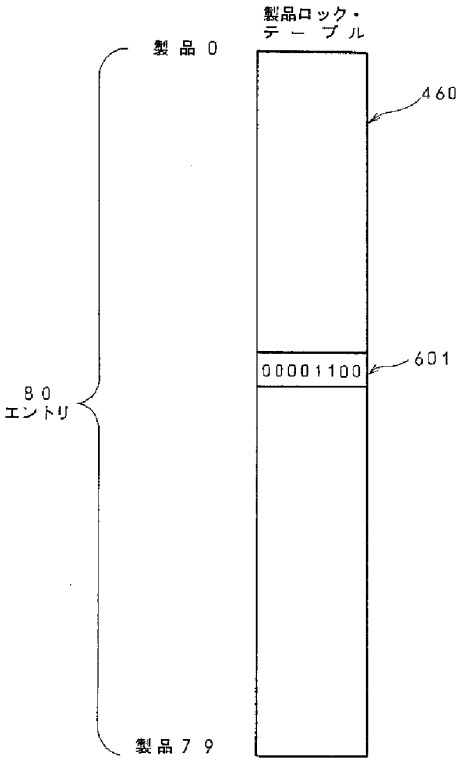
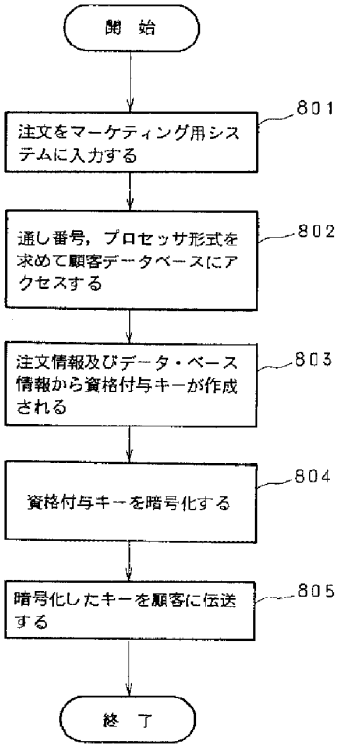
【図5】


コード化された製品キー・テーブル
製品 0
450
506
502
503
504
505
501
1
100110 . . .
10
00101. . .11
00001100
0010
80
エントリ
製品79

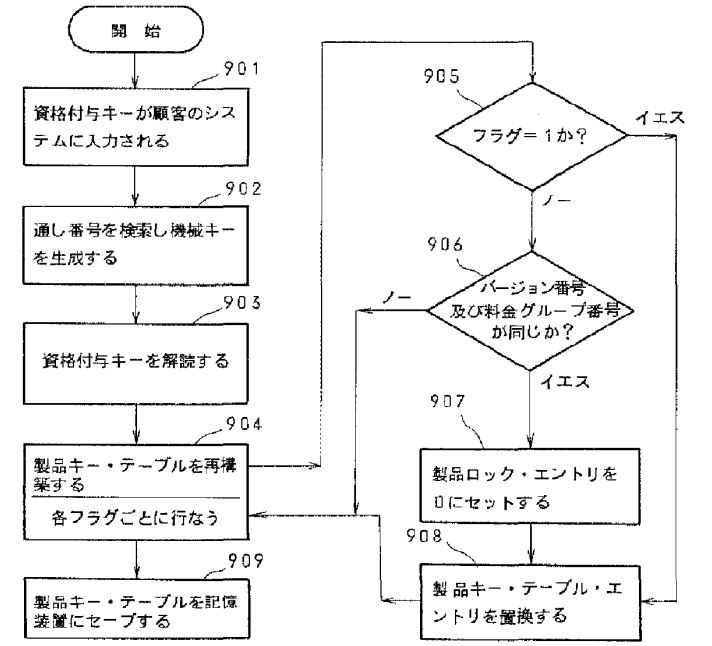
【図6】


製品ロック・
テーブル
製品０
460
00001100
601
８０
エントリ
製品７９

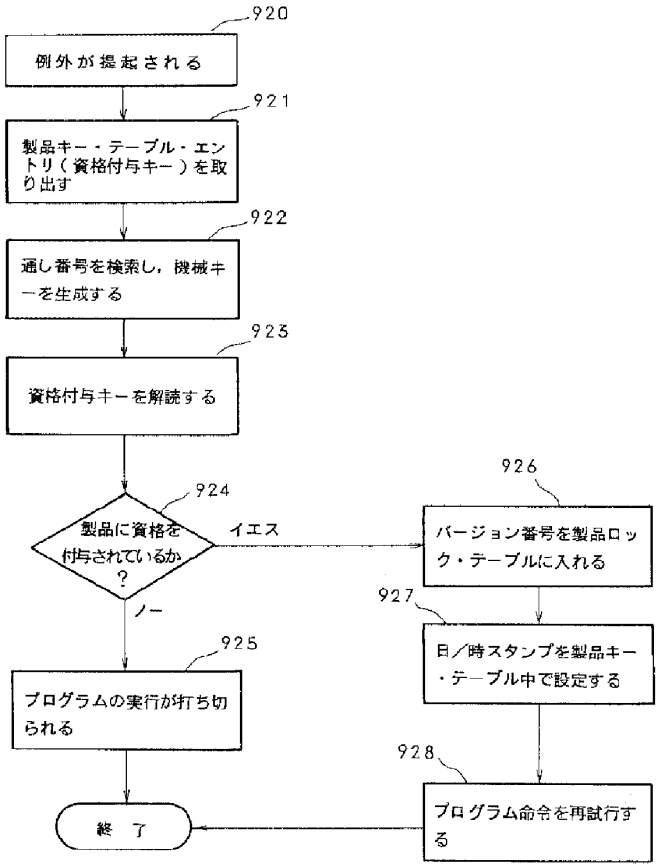
【図8】


開始
注文をマーケティング用システムに入力する
801
通し番号，プロセッサ形式を求めて顧客データベースにアクセスする
802
注文情報及びデータ・ベース情報から資格付与キーが作成される
803
資格付与キーを暗号化する
804
暗号化したキーを顧客に伝送する
805
終了

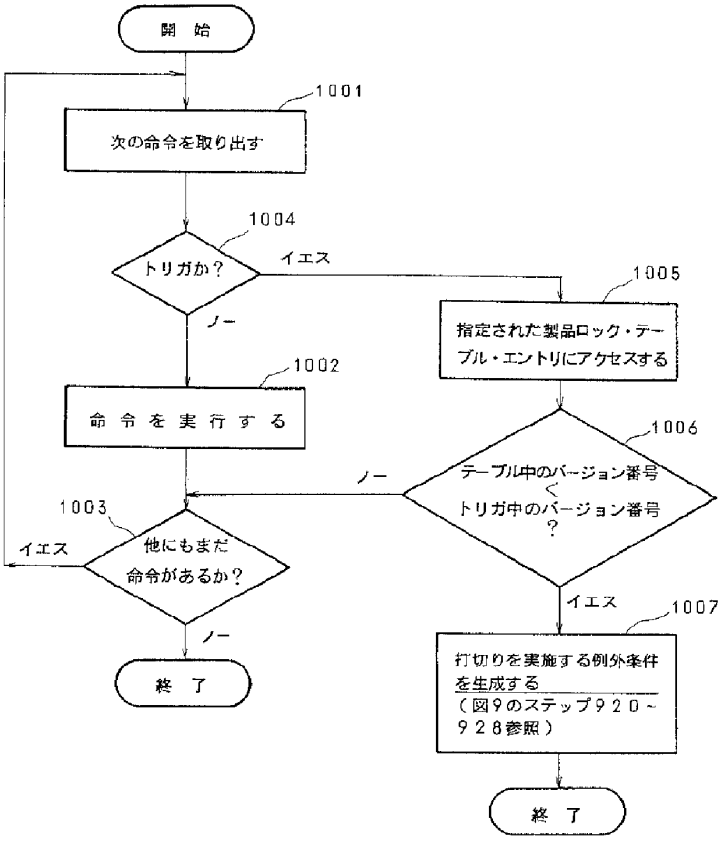
【図9ａ】


開　始
901
資格付与キーが顧客のシステムに入力される
902
通し番号を検索し機械キーを生成する
903
資格付与キーを解読する
904
製品キー・テーブルを再構築する
各フラグごとに行なう
909
製品キー・テーブルを記憶装置にセーブする
905
フラグ＝１か？
イエス
ノー
906
バージョン番号及び料金グループ番号が同じか？
ノー
イエス
907
製品ロック・エントリを０にセットする
908
製品キー・テーブル・エントリを置換する

【図9b】


920
例外が提起される
921
製品キー・テーブル・エントリ（資格付与キー）を取り出す
922
通し番号を検索し，機械キーを生成する
923
資格付与キーを解読する
924
製品に資格を付与されているか？
イエス
ノー
926
バージョン番号を製品ロック・テーブルに入れる
927
日／時スタンプを製品キー・テーブル中で設定する
928
プログラム命令を再試行する
925
プログラムの実行が打ち切られる
終　了

【図10】



フロントページの続き

(72)発明者　マイケル・ジョーゼフ・コリガン
アメリカ合衆国55906、ミネソタ州ロチェスター、20番アベニュー、ノース・イースト　1510番地

(72)発明者　フランシス・ジョーゼフ・リアドン・ジュニア
アメリカ合衆国55901、ミネソタ州ロチェスター、シャトー・ロード、ノース・ウェスト　5685番地

(72)発明者　ジェームズ・ウィリアム・モラン
アメリカ合衆国55934、ミネソタ州エヨタ　チェスター・ロード、サウス・イースト　3221番地

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G11B 20/00 — A2

(11) International Publication Number: WO 97/43761

(43) International Publication Date: 20 November 1997 (20.11.97)

(21) International Application Number: PCT/US97/08192

(22) International Filing Date: 15 May 1997 (15.05.97)

(30) Priority Data:

60/017,722	15 May 1996 (15.05.96)	US
60/018,132	22 May 1996 (22.05.96)	US
08/689,606	12 August 1996 (12.08.96)	US
08/689,754	12 August 1996 (12.08.96)	US
08/699,712	12 August 1996 (12.08.96)	US
PCT/US96/14262	4 September 1996 (04.09.96)	WO
(34) Countries for which the regional or international application was filed:		US et al.
60/037,931	14 February 1997 (14.02.97)	US

(71) Applicant *(for all designated States except US)*: INTERTRUST TECHNOLOGIES CORP. [US/US]; 460 Oakmead Parkway, Sunnyvale, CA 94086 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SHEAR, Victor, H. [US/US]; 5203 Battery Lane, Bethesda, MD 20814 (US). SIBERT, Olin, W. [US/US]; 30 Ingleside Road, Lexington, MA 02173-2522 (US). VANWIE, David, M. [US/US]; Apartment 216, 965 E. El Camino Real, Sunnyvale, CA 94087 (US). WEBER, Robert, P. [US/US]; 215 Waverley Street #4, Menlo Park, CA 94025 (US).

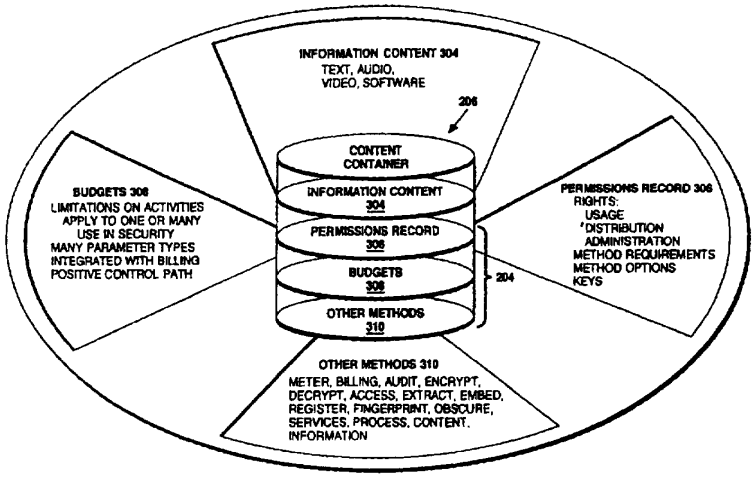
(74) Agent: FARIS, Robert, W.; Nixon & Vanderhye P.C., 8th floor, 1100 North Glebe Road, Arlington, VA 22201-4714 (US).

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

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

(54) Title: CRYPTOGRAPHIC METHODS, APPARATUS AND SYSTEMS FOR STORAGE MEDIAELECTRONIC RIGHTS MANAGEMENT IN CLOSED AND CONNECTED APPLIANCES

(57) Abstract



A rights management arrangement for storage media such as optical digital video disks (DVDs, also called digital versatile disks) provides adequate copy protection in a limited, inexpensive mass-produceable, low-capability platform such as a dedicated home consumer disk player and also provides enhanced, more flexible security techniques and methods when the same media are used with platforms having higher security capabilities. A control object (or set) defines plural rights management rules for instance, price for performance or rules governing redistribution. Low capability platforms may enable only a subset of the control rules such as controls on copying or marking of played material. Higher capability platforms may enable all (or different subsets) of the rules. Cryptographically strong security is provided by encrypting at least some of the information carried by the media and enabling decryption based on the control set and/or other limitations. A secure "software container" can be used to protectively encapsulate (e.g., by cryptographic techniques) various digital property content (e.g., audio, video, game, etc.) and control object (i.e., set of rules) information. A standardized container format is provided for general use on/with various mediums and platforms. In addition, a special purpose container may be provided for DVD medium and appliances (e.g., recorders, players, etc.) that contains DVD program content (digital property) and DVD medium specific rules. The techniques, systems and methods disclosed herein are capable of achieving compatibility with other protection standards, such as for example, CGMA and Matsushita data protection standards adopted for DVDs. Cooperative rights management may also be provided, where plural networked rights management arrangements collectively control a rights management event on one or more of such arrangements.

DISH-Blue Spike 842
Exhibit 1005, Page 0938

FOR THE PURPOSES OF INFORMATION ONLY

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

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

DISH-Blue Spike 842
Exhibit 1005, Page 0939

CRYPTOGRAPHIC METHODS, APPARATUS AND SYSTEMS FOR STORAGE MEDIA ELECTRONIC RIGHTS MANAGEMENT IN CLOSED AND CONNECTED APPLIANCES

Cross-Reference to Related Applications and Patents

The specifications and drawings of the following prior, commonly assigned published patent specifications are incorporated by reference into this patent specification:

PCT Publication No. WO 96/27155 dated 6 September 1996 entitled "Systems And Methods For Secure Transaction Management And Electronic Rights Protection", which is based on PCT application no. PCT/US96/02303 filed 13 February 1996 and U.S. patent application serial no. 08/388,107 of Ginter et al. entitled filed on February 13, 1995 (hereinafter "Ginter et al");

U.S. Patent No 4,827,508 entitled "Database Usage Metering and Protection System and Method" dated May 2, 1989;

U.S. Patent No. 4,977,594 entitled "Database Usage Metering and Protection System and Method" dated December 11, 1990;

U.S. Patent No. 5,050,213 entitled "Database Usage Metering and Protection System and Method" dated September 17, 1991; and

U.S. Patent No. 5,410,598 entitled "Database Usage Metering and Protection System and Method" dated April 25, 1995; and

European Patent No.EP 329681 entitled "Database Usage Metering and Protection System and Method" dated January 17, 1996.

In addition, the specifications and drawings of the following commonly-assigned prior-filed patent specifications are incorporated by reference into this patent application:

PCT Application No. PCT/US96/14262 filed 4 September 1996 entitled "Trusted Infrastructure Support Systems, Methods And Techniques For Secure Electronic Commerce, Electronic Transactions, Commerce Process Control And Automation, Distributed Computing, And Rights Management," which corresponds to U.S. patent application serial no. 08/699,712 filed on August 12, 1996 (hereinafter "Shear et al.");

PCT Application No. _____ filed _____, 1997 entitled "Steganographic Techniques For Securely Delivering Electronic Digital Rights Management Control Information Over Insecure Communications Channels," which corresponds to U.S. patent application serial no. 08/689,606 of Van Wie and Weber filed on August 12, 1996 (hereinafter "Van Wie and Weber"); and

PCT Application No. _____ filed _____, 1997 based on U.S. Patent Application serial no.08/689,754 entitled "Systems and Methods Using Cryptography To Protect Secure Computing Environments," of Sibert and Van Wie filed on August 12, 1996 (hereinafter "Sibert and Van Wie").

FIELD OF THE INVENTION

This invention relates to information protection techniques using cryptography, and more particularly to techniques using cryptography for managing rights to information stored on portable media -- one example being optical media such as Digital Video Disks (also known as "Digital Versatile Disks" and/or "DVDs"). This invention also relates to information protection and rights management techniques having selectable applicability depending upon, for example, the resources of the device being

used by the consumer (e.g., personal computer or standalone player), other attributes of the device (such as whether the device can be and/or typically is connected to an information network ("connected" versus "unconnected")), and available rights. This invention further relates, in part, to cooperative rights management -- where plural networked rights management arrangements collectively control a rights management event on one or more of such arrangements. Further, important aspects of this invention can be employed in rights management for electronic information made available through broadcast and/or network downloads and/or use of non-portable storage media, either independent of, or in combination with portable media.

BACKGROUND OF THE INVENTION

The entertainment industry has been transformed by the pervasiveness of home consumer electronic devices that can play video and/or audio from pre-recorded media. This transformation began in the early 1900s with the invention of the phonograph—which for the first time allowed a consumer to listen to his or her favorite band, orchestra or singer in his or her home whenever he or she wishes. The availability of inexpensive video

cassette recorders/players beginning in the early 1980s brought about a profound revolution in the movie and broadcast industries, creating an entirely new home consumer market for films, documentaries, music videos, exercise videos, etc.

The entertainment industry has long searched for optimal media for distributing content to home consumers. The original phonograph cylinders distributed by Thomas Edison and other phonograph pioneers had the advantage that they were difficult to copy, but suffered from various disadvantages such as high manufacturing costs, low resistance to breakage, very limited playback time, relatively low playback quality, and susceptibility to damage from wear, scratching or melting. Later-developed wax and vinyl disks could hold more music material but suffered from many of the same disadvantages. Magnetic tapes, on the other hand, could be manufactured very inexpensively and could hold a large amount of program material (e.g., 2, 4 or even 6 hours of video and/or audio). Such magnetic tapes could reproduce program material at relatively high quality, and were not as susceptible to damage or wearing out. However, despite the many clear advantages that magnetic tape provides over other media, the

entertainment industry has never regarded it as an ideal or optimum medium because of its great susceptibility to copying.

Magnetic tape has the very flexible characteristic that it can be relatively easily recorded on. Indeed, the process for recording a magnetic tape is nearly as straightforward as that required for playing back pre-recorded content. Because of the relative ease by which magnetic tape can be recorded, home consumer magnetic tape equipment manufacturers have historically provided dual mode equipment that can both record and play back magnetic tapes. Thus, home audio and video tape players have traditionally had a "record" button that allows a consumer to record his or her own program material on a blank (un-recorded) magnetic tape. While this recording ability has given consumers additional flexibility (e.g., the ability to record a child's first words for posterity, and the ability to capture afternoon soap operas for evening viewing), it has unfortunately also been the foundation of an illegal multi-billion dollar content pirating industry that produces millions of illegal, counterfeit copies every year. This illegal pirating operation—which is international in scope—leeches huge amounts of revenue every year from the world's major

entertainment content producers. The entertainment industry must pass along these losses to honest consumers—resulting in higher box office prices, and higher video and audio tape sales and rental prices.

In the mid 1980s, the audio entertainment industry developed the optical compact disk as an answer to some of these problems. The optical compact disk—a thin, silvery plastic platter a few inches in diameter—can hold an hour or more of music or other audio programming in digital form. Such disks were later also used for computer data. The disk can be manufactured very inexpensively, and provides extremely high quality playback that is resistant to noise because of the digital techniques used to record and recover the information. Because the optical disk can be made from plastic, it is light weight, virtually unbreakable, and highly resistant to damage from normal consumer handling (unlike the prior vinyl records that were easily scratched or worn down even by properly functioning phonographs). And, because recording on an optical disk is, so far, significantly more difficult than playing back an optical disk, home consumer equipment providing both recording and playback capabilities is unlikely, in

the near future, to be as cost-effective as play-only equipment—greatly reducing the potential for illicit copying. Because of these overwhelming advantages, the music industry has rapidly embraced the new digital compact disk technology—virtually replacing older audio vinyl disk media within the space of a few short years.

Indeed, the threat of widespread and easy unauthorized copying in the absence of rights management technologies apparently has been an important contributing factor to the demise of digital audio tape (DAT) as a media for music distribution and, more importantly, home audio recording. Rightsholders in recorded music vigorously opposed the widespread commercialization of inexpensive DAT technology that lacked rights management capabilities since the quality of the digital recording was completely faithful to the digital source on, for example, music CDs. Of course, the lack of rights management was not the only factor at work, since compared with optical media, tape format made random access difficult, for example, playing songs out of sequence.

The video entertainment industry is on the verge of a revolution similar to that wrought by music CDs based on movies in digital format distributed on high capacity read-only optical media. For example, digital optical disk technology has advanced to the point where it is now possible to digitally record, among other things, a full length motion picture (plus sound) on one side of a 5" plastic optical disk. This same optical disk can accommodate multiple high-quality digital audio channels (e.g., to record multi-channel "sensurround" sound for home theaters and/or to record film dialog in multiple different languages on the same disk). This same technology makes it possible to access each individual frame or image of a movie for still image reproduction or—even more exciting—to provide an unprecedented "random access" playback capability that has never before existed in home consumer equipment. This "random access" playback could be used, for example, to delete violence, foul language or nudity at time of playback so that parents could select a "PG" playback version of an "R" rated film at the press of a button. The "random access" capability also has exciting possibilities in terms of allowing viewers to interact with the pre-recorded content (e.g.,

allowing a health enthusiast to select only those portions of an exercise video helpful to a particular day's workout). See, for example, "Applications Requirements for Innovative Video Programming," DVD Conference Proceedings (Interactive Multimedia Association, 19-20 October 1995, Sheraton Universal Hotel, Universal City, California).

Non-limiting examples of the DVD family of optical media include:

- DVD (Digital Video Disk, Digital Versatile Disk), a non-limiting example of which includes consumer appliances that play movies recorded on DVD disks;
- DVD-ROM (DVD-Read Only Memory), a non-limiting example of which includes a DVD read-only drive and disk connected to a computer or other appliance;
- DVD-RAM (DVD Random Access Memory), a non-limiting example of which includes a read/write drive and optical media in, for example, consumer appliances for home recording and in a computer or other appliance

DISH-Blue Spike 842
Exhibit 1005, Page 0949

for the broadest range of specific applications; and

- Any other high capacity optical media presently known or unknown.

"DVDs" are, of course, not limited to use with movies. Like CDs, they may also be used for other kinds of information, for example:

- sound recordings
- software
- databases
- games
- karaoke
- multimedia
- distance learning
- documentation
- policies and manuals

- any kind of digital data or other information
- any combination of kinds of digital data or other information
- any other uses presently known or unknown.

The broad range of DVD uses presents a technical challenge: how can the information content distributed on such disks, which might be any kind or combination of video, sound, or other data or information broadly speaking, be adequately protected while preserving or even maximizing consumer flexibility? One widely proposed requirement for the new technology(mainly within the context of video), is, to the extent copying is permitted at all, to either: (a) allow a consumer to make a first generation copy of the program content for their own use, but prevent the consumer from making "copies of copies", or multi-generational copies of a given property (thus keeping honest people honest); or (b) to allow unlimited copying for those properties that rightsholders do not wish to protect against copying, or which consumers have made themselves.

However, providing only such simplistic and limited copy protection in a non-extensible manner may turn out to be extremely shortsighted—since more sophisticated protection and/or rights management objectives (e.g., more robust and selective application of copy protection and other protection techniques, enablement of pay-per-view models, the ability of the consumer to make use of enhanced functionality such as extracting material or interactivity upon paying extra charges, and receiving credit for redistribution, to name a few) could be very useful now or in the future. Moreover, in optimally approaching protection and rights management objectives, it is extremely useful to take differing business opportunities and threats into account that may relate to information delivered via DVD media, for example, depending upon available resources of the device and/or whether the device is connected or unconnected.

More sophisticated rights management capabilities will also allow studios and others who have rights in movies and/or sound recordings to better manage these important assets, in one example, to allow authorized parties to repurpose pieces of digital film, video and/or audio, whether specific and/or arbitrary pieces,

F033_WO1997043761_Intertrust Page 15 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 0952

to create derivative works, multimedia games, in one non-limiting example. Solutions proposed to date for protecting DVD content have generally focused solely on limited copy protection objectives and have failed to adequately address or even recognize more sophisticated rights management objectives and requirements. More specifically, one copy protection scheme for the initial generation of DVD appliances and media is based on an encryption method developed initially by Matsushita and the simple CGMA control codes that indicate permitted copying: a one-generation copy, no copies, or unlimited copying.

SUMMARY OF THE INVENTIONS

Comprehensive solutions for protecting and managing information in systems that incorporate high capacity optical media such as DVD require, among other things, methods and systems that address two broad sets of problems: (a) digital to analog conversion (and vice versa); and (b) the use of such optical media in both connected and unconnected environments. The inventions disclosed herein address these and other problems. For example, in the context of analog to digital conversion (and vice versa), it is contemplated that, in accordance with the present

inventions, at least some of the information used to protect properties and/or describe rights management and/or control information in digital form could also be carried along with the analog signal. Devices that convert from one format and/or medium to another can, for example, incorporate some or all of the control and identifying information in the new context(s), or at least not actively delete such information during the conversion process. In addition, the present inventions provide control, rights management and/or identification solutions for the digital realm generally, and also critically important technologies that can be implemented in consumer appliances, computers, and other devices. One objective of the inventions is to provide powerful rights management techniques that are useful in both the consumer electronics and computer technology markets, and that also enable future evolution of technical capabilities and business models. Another non-limiting objective is to provide a comprehensive control, rights management and/or identification solution that remains compatible, where possible, with existing industry standards for limited function copy protection and for encryption.

The present inventions provide rights management and protection techniques that fully satisfy the limited copy protection objectives currently being voiced by the entertainment industry for movies while also flexibly and extensibly accommodating a wide range of more sophisticated rights management options and capabilities.

Some important aspects of the present inventions (that are more fully discussed elsewhere in this application) include:

- Selection of control information associated with information recorded on DVD media (for example, rules and usage consequence control information, that comprise non-limiting example elements of a Virtual Distribution Environment (VDE)) that is based at least in part on class of appliance, for example, type of appliance, available resources and/or rights;

- Enabling such selected control information to be, at least in part, a subset of control information used on other appliances and/or classes of appliance, or completely different control information;

- Protecting information output from a DVD device, such as applying rights management techniques disclosed in Ginter et al. and the present application to the signals transmitted using an IEEE 1394 port (or other serial interface) on a DVD player;

- Creation of protected digital content based on an analog source;

- Reflecting differing usage rights and/or content availability in different countries and/or regions of the world;

- Securely managing information on DVD media such that certain portions may be used on one or more classes of appliance (e.g., a standalone DVD player), while other portions may be used on the same or different classes of appliance (e.g., a standalone DVD player or a PC);

- Securely storing and/or transmitting information associated with payment, auditing, controlling and/or otherwise managing content recorded on DVD media, including techniques related to those disclosed in Ginter et al. and in Shear et al.;

- Updating and/or replacing encryption keys used in the course of appliance operation to modify the scope of information that may be used by appliances and/or classes of appliances;

- Protecting information throughout the creation, distribution, and usage process, for example, by initially protecting information collected by a digital camera, and continuing protection and rights management through the editing process, production, distribution, usage, and usage reporting.

- Allowing "virtual rights machines," consisting of multiple devices and/or other systems that participate and work together in a permanently or in a temporarily connected network to share some or all of the rights management for a single and/or multiple nodes including, for example, allowing resources available in plural such devices and/or other systems, and/or rights associated with plural parties and/or groups using and/or controlling such devices and/or other systems, to be employed in concert (according to rights related rules and controls) so as to govern one or more electronic

events on any one or more of such devices and/or other systems, such event governance including, for example: viewing, editing, subsetting, anthologizing, printing, copying, titling, extracting, saving, and/or redistributing rights protected digital content.

- Allowing for the exchange of rights among peer-to-peer relating devices and/or other systems, wherein such devices and/or other systems participate in a temporary or permanently connected network, and wherein such rights are bartered, sold for currency, and/or otherwise exchanged for value and/or consideration where such value and/or consideration is exchanged between such peer-to-peer participating commercial and/or consumer devices and/or other systems.

General Purpose DVD/Cost-effective Large Capacity Digital Media Rights Protection and Management

The inventions described herein can be used with any large capacity storage arrangement where cost-effective distribution media is used for commercial and/or consumer digital information delivery and DVD, as used herein, should be read to include any such system.

Copy protection and rights management are important in practical DVD systems and will continue to be important in other large capacity storage, playback, and recording systems, presently known or unknown, in the future. Protection is needed for some or all of the information delivered (or written) on most DVD media. Such protection against copying is only one aspect of rights management. Other aspects involve allowing rightsholders and others to manage their commercial interests (and to have them enforced, potentially at a distance in time and/or space) regardless of distribution media and/or channels, and the particular nature of the receiving appliance and/or device. Such rights management solutions that incorporate DVD will become even more significant as future generations of recordable DVD media and appliances come to market. Rightsholders will want to maintain and assert their rights as, for example, video, sound recordings, and other digital properties are transmitted from one device to another and as options for recording become available in the market.

The apparent convergence between consumer appliances and computers, increasing network and modem speeds, the declining cost of computer power and bandwidth, and the

increasing capacity of optical media will combine to create a world of hybrid business models in which digital content of all kinds may be distributed on optical media played on at least occasionally connected appliances and/or computers, in which the one-time purchase models common in music CDs and initial DVD movie offerings are augmented by other models, for example, lease, pay per view, and rent to own, to name just few. Consumers may be offered a choice among these and other models from the same or different distributors and/or other providers. Payment for use may happen over a network and/or other communications channel to some payment settlement service. Consumer usage and audit information may flow back to creators, distributors, and/or other participants. The elementary copy protection technologies for DVD now being introduced cannot support these and other sophisticated models.

As writable DVD appliances and media become available, additional hybrid models are possible, including, for example, the distribution of digital movies over satellite and cable systems. Having recorded a movie, a consumer may elect a lease, rental, pay-per-view, or other model if available. As digital television

comes to market, the ability of writable DVDs to make faithful copies of on-air programming creates additional model possibilities and/or rights management requirements. Here too, simplistic copy protection mechanisms currently being deployed for the initial read-only DVD technologies will not suffice.

Encryption Is A Means, Not An End

Encryption is useful in protecting intellectual properties in digital format, whether on optical media such as DVD, on magnetic media such as disk drives, in the active memory of a digital device and/or while being transmitted across computer, cable, satellite, and other kinds of networks or transmission means. Historically, encryption was used to send secret messages. With respect to DVD, a key purpose of encryption is to require the use of a copy control and rights management system in order to ensure that only those authorized to do so by rightsholders can indeed use the content.

But encryption is more of a means, rather than an end. A central issue is how to devise methods for ensuring, to the maximal extent possible, that only authorized devices and parties can decrypt the protected content and/or otherwise use information

only to the extent permitted by the rightsholder(s) and/or other relevant parties in the protected content.

The Present Inventions

The present inventions provide powerful right management capabilities. In accordance with one aspect provided by the present invention, encrypted digital properties can be put on a DVD in a tamper-resistant software "container" such as, for example, a "DigiBox" secure container, together with rules about "no copy" and/or "copy" and/or "numbers of permitted copies" that may apply and be enforced by consumer appliances. These same rules, and/or more flexible and/or different rules, can be enforced by computer devices or other systems that may provide more and/or different capabilities (e.g., editing, excerpting, one or more payment methods, increased storage capability for more detailed audit information, etc.). In addition, the "software container" such as for example, a "DigiBox" secure container, can store certain content in the "clear" (that is, in unencrypted form). For example, movie or music titles, copyright statements, audio samples, trailers, and/or advertising can be stored in the clear and/or could be displayed by any appropriate application or

device. Such information could be protected for authenticity (integrity) when available for viewing, copying, and/or other activities. At the same time, valuable digital properties of all kinds-film, video, image, text, software, and multimedia— may be stored at least partially encrypted to be used only by authorized devices and/or applications and only under permitted, for example rightsholder-approved, circumstances.

Another aspect provided in accordance with the present invention (in combination with certain capabilities disclosed in Ginter et al.) is that multiple sets of rules could be stored in the same "container" on a DVD disk. The software then applies rules depending on whether the movie, for example, was to be played by a consumer appliance or computer, whether the particular apparatus has a backchannel (e.g., an on-line connection), the national and/or other legal or geographic region in which the player is located and/or the movie is being displayed, and/or whether the apparatus has components capable of identifying and applying such rules. For example, some usage rules may apply when information is played by a consumer device, while other rules may apply when played by a computer. The choice of rules

may be left up to the rightsholder(s) and/or other participants-- or some rules may be predetermined (e.g., based on the particular environment or application). For example, film rightsholders may wish to limit copying and ensure that excerpts are not made regardless of the context in which the property is played. This limitation might be applied only in certain legal or geographic areas. Alternatively, rightsholders of sound recordings may wish to enable excerpts of predetermined duration (e.g., no more than 20 seconds) and that these excerpts are not used to construct a new commercial work. In some cases, governments may require that only "PG" versions of movies and/or the equivalent rating for TV programs may be played on equipment deployed in their jurisdiction, and/or that the applicable taxes, fees and the like are automatically calculated and/or collected if payments related to content recorded on DVD is requested and/or performed (e.g., pay-per-use of a movie, game, database, software product, etc.; and/or orders from a catalog stored at least in part on DVD media, etc.).

In a microprocessor controlled (or augmented) digital consumer appliance, such rules contemplated by the present

inventions can be enforced, for example, without requiring more than a relatively few additions to a central, controlling microprocessor (or other CPU, a IEEE 1394 port controller, or other content handling control circuitry), and/or making available some ROM or flash memory to hold the necessary software. In addition, each ROM (or flash or other memory, which such memory may be securely connected to, or incorporated into, such control circuitry in a single, manufactured component) can, in one example, contain one or more digital documents or "certificate(s)" that uniquely identifies a particular appliance, individual identity, jurisdiction, appliance class(es), and/or other chosen parameters. An appliance can, for example, be programmed to send a copy of a digital property to another digital device only in encrypted form and only inside a new, tamper-resistant "software container." The container may also, for example, carry with it a code indicating that it is a copy rather than an original that is being sent. The device may also put a unique identifier of a receiving device and/or class of devices in the same secure container. Consequently, for example, in one particular arrangement, the copy may be playable only on the intended receiving device,

class(es) of devices, and/or devices in a particular region in one non-limiting example and rights related to use of such copy may differ according to these and/or other variables.

The receiving device, upon detecting that the digital property is indeed a copy, can, for example, be programmed not to make any additional copies that can be played on a consumer device and/or other class(es) of devices. If a device detects that a digital property is about to be played on a device and/or other class(es) of devices other than the one it was intended for, it can be programmed to refuse to play that copy (if desired).

The same restrictions applied in a consumer appliance can, for example, be enforced on a computer equipped to provide rights management protection in accordance with the present inventions. In this example, rules may specify not to play a certain film and/or other content on any device other than a consumer appliance and/or classes of appliances, for example. Alternatively, these same powerful capabilities could be used to specify different usage rules and payment schemes that would apply when played on a computer (and/or in other appliances and/or classes of appliances), as the rightsholder(s) may desire, for example,

different pricing based upon different geographic or legal locales where content is played.

In addition, if "backchannels" are present—for example, set-top boxes with bi-directional communications or computers attached to networks—the present inventions contemplate electronic, independent delivery of new rules if desired or required for a given property. These new rules may, for example, specify discounts, time-limited sales, advertising subsidies, and/or other information if desired. As noted earlier, determination of these independently delivered rules is entirely up to the rightsholder(s) and/or others in a given model.

The following are two specific examples of a few aspects of the present invention discussed above:

1. An Analog To Digital Copying Example

a) Bob has a VHS tape he bought (or rented) and wants to make a copy for his own use. The analog film has copy control codes embedded so that they do not interfere with the quality of the signal. Bob has a writable DVD appliance

that is equipped to provide rights management protection in accordance with the present invention. Bob's DVD recorder detects the control codes embedded in the analog signal (for example, such recorder may detect watermarks and/or fingerprints carrying rights related control and/or usage information), creates a new secure container to hold the content rules and describe the encoded film, and creates new control rules (and/or delivers to a secure VDE system for storage and reporting certain usage history related information such as user name, time, etc.) based on the analog control codes and/or other information it detected and that are then placed in the DigiBox and/or into a secure VDE installation data store such as a secure data base. Bob can play that copy back on his DVD appliance whenever he chooses.

b) Bob gives the DVD disk he recorded to Jennifer who wishes to play it on computer that has a DVD drive. Her computer is equipped to provide rights management protection in accordance with the present invention. Her computer opens the "DigiBox," detects that this copy is being used on a device different from the one that recorded it (an unauthorized device) and refuses to play the copy.

c) Bob gives the DVD disk to Jennifer as before, but now Jennifer contacts electronically a source of new rules and usage consequences, which might be the studio, a distributor, and/or a rights and permissions clearinghouse, (or she may have sufficient rights already on her player to play the copy). The source sends a DigiBox container to Jennifer with rules and consequences that permit playing the movie on her

computer while at the same time charging her for use, even though the movie was recorded on DVD by Bob rather than by the studio or other value chain participant.

2. A Digital To Analog Copying Example

a) Jennifer comes home from work, inserts a rented or owned DVD into a player connected to, or an integral part of her TV, and plays the disk. In a completely transparent way, the film is decrypted, the format is converted from digital to analog, and displayed on her analog TV.

b) Jennifer wishes to make a copy for her own use. She plays the film on an DVD device incorporating rights management protection in accordance with the present invention, that opens the DigiBox secure container, accesses the control information, and decrypts the film.

She records the analog version on her VCR which records a high-quality copy.

c) Jennifer gives the VCR copy to Doug who wishes to make a copy of the analog tape for his own use, but the analog control information forces the recording VCR to make a lower-quality copy, or may prevent copying. In another non-limiting example, more comprehensive rights management information may be encoded in the analog output using the methods and/or systems described in more detail in the above referenced Van Wie and Weber patent application.

In accordance with one aspect provided by this invention, the same portable storage medium, such as a DVD, can be used with a range of different, scaled protection environments providing different protection capabilities. Each of the different environments may be enabled to use the information carried by the portable storage medium based on rights management techniques and/or capabilities supported by the particular environment. For

example, a simple, inexpensive home consumer disk player may support copy protection and ignore more sophisticated and complex content rights the player is not equipped to enable. A more technically capable and/or secure platform (e.g., a personal computer incorporating a secure processing component possibly supported by a network connection, or a "smarter" appliance or device) may, for example, use the same portable storage medium and provide enhanced usage rights related to use of the content carried by the medium based on more complicated rights management techniques (e.g., requiring payment of additional compensation, providing secure extraction of selected content portions for excerpting or anthologizing, etc.). For example, a control set associated with the portable storage medium may accommodate a wide variety of different usage capabilities—with the more advanced or sophisticated uses requiring correspondingly more advanced protection and rights management enablement found on some platforms and not others. Lower-capability environments can, as another example, ignore (or not enable or attempt to use) rights in the control set that they don't understand, while higher-capability environments (having awareness of the

overall capabilities they provide), may, for example, enable the rights and corresponding protection techniques ignored by the lower-capability environments.

In accordance with another aspect provided by the invention, a media- and platform-independent security component can be scaled in terms of functionality and performance such that the elementary rights management requirements of consumer electronics devices are subsets of a richer collection of functionality that may be employed by more advanced platforms. The security component can be either a physical, hardware component, or a "software emulation" of the component. In accordance with this feature, an instance of medium (or more correctly, one version of the content irrespective of media) can be delivered to customers independently of their appliance or platform type with the assurance that the content will be protected. Platforms less advanced in terms of security and/or technical capabilities may provide only limited rights to use the content, whereas more advanced platforms may provide more expansive rights based on correspondingly appropriate security conditions and safeguards.

In accordance with a further aspect provided by the present invention, mass-produced, inexpensive home consumer DVD players (such as those constructed, for example, with minimum complexity and parts count) can be made to be compatible with the same DVDs or other portable storage media used by more powerful and/or secure platforms (such as, for example, personal computers) without degrading advanced rights management functions the storage media may provide in combination with the more powerful and/or secure platforms. The rights management and protection arrangement provided and supported in accordance with this aspect of the invention thus supports inexpensive basic copy protection and can further serve as a commercial convergence technology supporting a bridging that allows usage in accordance with rights of the same content by a limited resource consumer device while adequately protecting the content and further supporting more sophisticated security levels and capabilities by (a) devices having greater resources for secure rights management, and/or (b) devices having connectivity with other devices or systems that can supply further secure rights management resources. This aspect of the invention allows

multiple devices and/or other systems that participate and work together in a permanently or temporarily connected network to share the rights management for at least one or more electronic events (e.g., managed through the use of protected processing environments such as described in Ginter et al.) occuring at a single, or across multiple nodes and further allows the rights associated with parties and/or groups using and/or controlling such multiple devices and/or other systems to be employed according to underlying rights related rules and controls, this allowing, for example, rights available through a corporate executive's device to be combined with or substitute for, in some manner, the rights of one or more subordinate corporate employees when their computing or other devices of these parties are coupled in a temporary networking relationship and operating in the appropriate context. In general, this aspect of the invention allows distributed rights management for DVD or otherwise packaged and delivered content that is protected by a distributed, peer-to-peer rights management.Such distributed rights management can operate whether the DVD appliance or oth- electronic information usage device is participatin,

permanently or temporarily connected network and whether or not the relationships among the devices and/or other systems participating in the distributed rights management arrangement are relating temporarily or have a more permanent operating relationship. In this way, the same device may have different rights available depending on the context in which that device is operating (e.g., in a corporate environment such as in collaboration with other individuals and/or with groups, in a home environment internally and/or in collaboration with external one or more specified individuals and/or other parties, in a retail environment, in a classroom setting as a student where a student's notebook might cooperate in rights management with a classroom server and/or instructor PC, in a library environment where multiple parties are collaboratively employing differing rights to use research materials, on a factory floor where a hand held device works in collaboration with control equipment to securely and appropriately perform proprietary functions, and so on).

For example, coupling a limited resource device arrangement, such as a DVD appliance, with an inexpensive network computer (NC), or a personal computer (PC), may allow

an augmenting (or replacing) of rights management capabilities and/or specific rights of parties and/or devices by permitting rights management to be a result of a combination of some or all of the rights and/or rights management capabilities of the DVD appliance and those of an Network or Personal Computer (NC or PC). Such rights may be further augmented, or otherwise modified or replaced by the availability of rights management capabilities provided by a trusted (secure) remote network rights authority.

These aspects of the present invention can allow the same device, in this example a DVD appliance, to support different arrays, e.g., degrees, of rights management capabilities, in disconnected and connected arrangements and may further allow available rights to result from the availability of rights and/or rights management capabilities resulting from the combination of rights management devices and/or other systems. This may include one or more combinations of some or all of the rights available through the use of a "less" secure and/or resource poor device or system which are augmented, replaced, or otherwise modified through connection with a device or system that is

"more" or "differently" secure and/or resource rich and/or possesses differing or different rights, wherein such connection employs rights and/or management capabilities of either and/or both devices as defined by rights related rules and controls that describe a shared rights management arrangement.

In the latter case, connectivity to a logically and/or physically remote rights management capability can expand (by, for example, increasing the available secure rights management resources) and/or change the character of the rights available to the user of the DVD appliance or a DVD appliance when such device is coupled with an NC, personal computer, local server, and/or remote rights authority. In this rights augmentation scenario, additional content portions may be available, pricing may change, redistribution rights may change (e.g., be expanded), content extraction rights may be increased, etc.

Such "networking rights management" can allow for a combination of rights management resources of plural devices and/or other systems in diverse logical and/or physical relationships, resulting in either greater or differing rights through the enhanced resources provided by connectivity with one or more

"remote" rights authorities. Further, while providing for increased and/or differing rights management capability and/or rights, such a connectivity based rights management arrangement can support multi-locational content availability, by providing for seamless integration of remotely available content, for example, content stored in remote, Internet world wide web-based, database supported content repositories, with locally available content on one or more DVD discs.

In this instance, a user may experience not only increased or differing rights but may use both local DVD content and supplementing content (i.e., content that is more current from a time standpoint, more costly, more diverse, or complementary in some other fashion, etc.). In such an instance, a DVD appliance and/or a user of a DVD appliance (or other device or system connected to such appliance) may have the same rights, differing, and/or different rights applied to locally and remotely available content, and portions of local and remotely available content may themselves be subject to differing or different rights when used by a user and/or appliance. This arrangement can support an overall, profound increase in user content opportunities that are seamlessly

integrated and efficiently available to users in a single content searching and/or usage activity by exploiting the rights management and content resources of plural, connected arrangements.

Such a rights augmenting remote authority may be directly coupled to a DVD appliance and/or other device by modem, or directly or indirectly coupled through the use of an I/O interface, such as a serial 1394 compatible controller (e.g., by communicating between a 1394 enabled DVD appliance and a local personal computer that functions as a smart synchronous or asynchronous information communications interface to such one or more remote authorities, including a local PC or NC or server that serves as a local rights management authority augmenting and/or supplying the rights management in a DVD appliance).

In accordance with yet another aspect provided by this invention, rights provided to, purchased, or otherwise acquired by a participant and/or participant DVD appliance or other system can be exchanged among such peer-to-peer relating devices and/or other systems through the use of one or more permenantly or temporarily networked arrangments. In such a case, rights may be

bartered, sold, for currency, otherwise exchanged for value, and/or loaned so long as such devices and/or other systems participate in a rights management system, for example, such as the Virtual Distribution Environment described in Ginter, et al., and employ rights transfer and other rights management capabilities described therein. For example, this aspect of the present invention allows parties to exchange games or movies in which they have purchased rights. Continuing the example, an individual might buy some of a neighbor's usage rights to watch a movie, or transfer to another party credit received from a game publisher for the successful superdistribution of the game to several acquaintances, where such credit is transferred (exchanged) to a friend to buy some of the friend's rights to play a different game a certain number of times, etc.In accordance with yet another aspect provided by this invention, content carried by a portable storage medium such as a DVD is associated with one or more encryption keys and a secure content identifier. The content itself (or information required to use the content) is at least partially cryptographically encrypted—with associated decryption keys being required to decrypt the content before the content can be

used. The decryption keys may themselves be encrypted in the form of an encrypted key block. Different key management and access techniques may be used, depending on the platform.

In accordance with still yet another aspect provided by this invention, electronic appliances that "create" digital content (or even analog content) —e.g., a digital camera/video recorder or audio recorder—can be readily equipped with appropriate hardware and/or software so as to produce content that is provided within a secure container at the outset. For example, content recorded by a digital camera could be immediately packaged in a secure container by the camera as it is recording. The camera could then output content already packaged in a secure container(s). This could preclude the need to encapsulate the content at a later point in time or at a later production stage, thus, saving at least one production-process step in the overall implementation of electronic rights management in accordance with the present invention. Moreover, it is contemplated that the very process of "reading" content for use in the rights management environment might occur at many steps along a conventional production and distribution process (such as during editing and/or

the so called "pressing" of a master DVD or audio disk, for example). Accordingly, another significant advantage of the present invention is that rights management of content essentially can be extended throughout and across each appropriate content creation, editing, distribution, and usage stages to provide a seamless content protection architecture that protects rights throughout an entire content life cycle.

In one example embodiment, the storage medium itself carries key block decryption key(s) in a hidden portion of the storage medium not normally accessible through typical access and/or copying techniques. This hidden key may be used by a drive to decrypt the encrypted key block—such decrypted key block then being used to selectively decrypt content and related information carried by the medium. The drive may be designed in a secure and tamper-resistant manner so that the hidden keys are never exposed outside of the drive to provide an additional security layer.

In accordance with another example embodiment, a video disk drive may store and maintain keys used to decrypt an encrypted key block. The key block decryption keys may be

stored in a drive key store, and may be updatable if the video disk drive may at least occasionally use a communications path provided, for example, by a set top box, network port or other communications route.

In accordance with a further example embodiment, a virtual distribution environment secure node including a protected processing environment such as a hardware-based secure processing unit may control the use of content carried by a portable storage medium such as a digital video disk in accordance with control rules and methods specified by one or more secure containers delivered to the secure node on the medium itself and/or over an independent communications path such as a network.

Certain conventional copy protection for DVD currently envisions CGMA copy protection control codes combined with certain encryption techniques first proposed apparently by Matsushita Corporation. Notwithstanding the limited benefits of this approach to digital property protection, the present invention is capable of providing a supplementary, compatible, and far more comprehensive rights management system while also providing

additional and/or different options and solutions. The following are some additional examples of advantageous features provided in accordance with the inventions:

- Strong security to fully answer content supplier needs.

- Value chain management automation and efficiencies including distributed rights protection, "piece of the tick" payment disaggregation to value chain participants, cost-effective micro-transaction management, and superdistribution, including offline micropayment and microtransaction support for at least occasionally connected devices.

- Simplified, more efficient channel management including support for the use of the same content deliverable on limited resource, greater resource, standalone, and/or connected devices.

- Can be used with any medium and application type and/or all forms of content and content models -- not just compressed video and sound as in some prior techniques and supports the use of copies of the same or materially the

same content containers across a wide variety of media delivery systems (e.g., broadcast, Internet repository, optical disc, etc) for operation on a wide variety of different electronic appliances (e.g., digital cameras, digital editing equipment, sound recorders, sound editing equipment, movie theater projectors, DVD appliances, broadcast tape players, personal computers, smart televisions, etc).

- Asset management and revenue and/or other consideration maximizing through important new content revenue and/or other consideration opportunities and the enhancement of value chain operating efficiencies.

- Is capable of providing 100% compatibility with the other protection techniques such as, for example, CGMA protection codes and/or Matsushita data scrambling approaches to DVD copy protection.

- Can be employed with a variety of existing data scrambling or protection systems to provide very high degrees of compatibility and/or level of functionality.

- Allows DVD technology to become a reusable, programmable, resource for an unlimited variety of entertainment, information commerce, and cyberspace business models.

- Enables DVD drive and/or semiconductor component manufacturers and/or distributors and/or other value adding participants to become providers of, and rights holders in, the physical infrastructure of the emerging, connected world of the Internet and Intranets where they may charge for the use of a portion (e.g., a portion they provided) of the distributed, physical infrastructure as that portion participates in commercial networks. Such manufacturers and/or distributors and/or other value adding participants can enjoy the revenue benefits resulting from participation in a "piece of the tick" by receiving a small portion of the revenue received as a result of a participating transaction.

- Provides automated internationalization, regionalization, and rights management in that:

-- DVD content can be supplied with arrays of different rule sets for

automatic use depending on rights and identity of the user; and

-- Societal rights, including taxes, can be handled transparently.

In addition, the DVD rights management method and apparatus of the present invention provides added benefits to media recorders/publishers in that it:

- Works with a current "keep honest people honest" philosophy.
- Can provide 100% compatibility with other protection schemes such as for example, Matsushita data scrambling and/or CGMA encoded discs.
- Can work with and/or supplement other protection schemes to provide desired degree and/or functionality, or can be used in addition to or instead of other approaches to provide additional and/or different functionality and features.

- Provides powerful, extensible rights management that reaches beyond limited copy protection models to rights management for the digitally convergent world.

- Empowers recording/publishing studios to create sophisticated asset management tools.

- Creates important business opportunities through controlled use of studio properties in additional multimedia contexts.

- Uniquely ties internationalization, regionalization, superdistribution, repurposing, to content creation processes and/or usage control.

Other aspects of the present invention provide benefits to other types of rightsholders, such as for example:

- Persistent, transparent protection of digital content—globally, through value chain and process layers.

- Significant reduction in revenue loss from copying and pass-along.

- Converts "pass-along," copying, and many forms of copyright infringement from a strategic business threat to a fundamental business opportunity.

- A single standard for all digital content regardless of media and/or usage locality and other rights variables.

- Major economies of scale and/or scope across industries, distribution channels, media, and content type.

- Can support local usage governance and auditing within DVD players allowing for highly efficient micro-transaction support, including multiparty microtransactions and transparent multiparty microtransactions.

- Empowers rightsholders to employ the broadest range of pricing, business models, and market strategies—as they see fit.

Further aspects of the present invention which may prove beneficial to DVD and other digital medium appliance manufacturers are:

- Capable of providing bit for bit compatibility with existing discs.

- Content type independent.

- Media independent and programmable/reusable.

- Highly portable transition to next generation of appliances having higher density devices and/or a writable DVD and/or other optical media format(s).

- Participation in revenue flow generated using the appliance.

- Single extensible standard for all digital content appliances.

- Ready for the future "convergent" world in which many appliances are connected in the home using, as one example, IEEE 1394 interfaces or other means (e.g., some appliances will be very much like computers and some computers will be very much like appliances).

Aspects of the present inventions provide many benefits to computer and OS manufacturers such as for example:

- Implementation in computers as an extension to the operating system, via for example, at least one transparent plug-in, and does not require modifications to computer hardware and/or operating systems.

- Easy, seamless integration into operating systems and into applications.

- Extremely strong security, especially when augmented with "secure silicon" (i.e., hardware/firmware protection apparatus fabricated on chip).

- Transforms user devices into true electronic commerce appliances.

- Provides a platform for trusted, secure rights management and event processing.

- Programmable for customization to specialized requirements.

Additional features and advantages provided in accordance with the inventions include, for example:

- Information on the medium (for example, both properties and metadata) may be encrypted or not.

- Different information (for example, properties, metadata) may be encrypted using different keys. This provides greater protection against compromise, as well as supporting selective usage rights in the context of a sophisticated rights management system.

- There may be encrypted keys stored on the medium, although this is not required. These keys may be used to decrypt the protected properties and metadata. Encrypted keys are likely to be used because that allows more keying material for the information itself, while still keeping access under control of a single key.

- Multiple sets of encrypted keys may be stored on the medium, either to have different sets of keys associated with different information, or to allow multiple control regimes to use the

same information, where each control regime may use one or more different keys to decrypt the set of encrypted keys that it uses.

- To support the ability of the player to access rights managed containers and/or content, a decryption key for the encrypted keys may be hidden on the medium in one or more locations that are not normally accessible. The "not normally accessible" location(s) may be physically enabled for drives installed in players, and disabled for drives installed in computers. The enablement may be different firmware, a jumper on the drive, etc.

- The ability of the player to access rights managed containers and/or content may also be supported by one or more stored keys inside the player that decrypts certain encrypted keys on the medium.

- Keys in a player may allow some players to play different properties than others. Keys could be added to, and/or deleted from the player by a network connection (e.g., to a PC, a cable system, and/or a modem connection to a source of new and/or additional keys and/or

key revocation information) or automatically loaded by "playing" a key distribution DVD.

- Controlling computer use may be supported by some or all of the same techniques that control player use of content and/or rights managemnt information.

- Controlling computer use of content and/or rights management information may be supported by having a computer receive, through means of a trusted rights management system, one or more appropriate keys.

- A computer may receive additional keys that permit decryption of certain encrypted keys on the medium.

- A computer may receive additional keys that permit decryption of one or more portions of encrypted data directly. This may permit selective use of information on the medium without disclosing keys (e.g., a player key that decrypts any encrypted keys).

In accordance with further aspects provided by the present invention, a secure "software container" is provided that allows:

- Cryptographically protected encapsulation of content, rights rules, and usage controls.

- Persistent protection for transport, storage, and value chain management.

- Sophisticated rules interface architecture.

Elements can be delivered independently, such as new controls, for example, regarding discount pricing (e.g. sale pricing, specific customer or group discounts, pricing based on usage patterns, etc.) and/or other business model changes, can be delivered after the property has been distributed (this is especially beneficial for large properties or physical distribution media (e.g., DVD, CD-ROM) since redistribution costs may be avoided and consumers may continue to use their libraries of discs). In addition, encrypted data can be located "outside" the container. This can allow, for example, use of data stored independently from the controls and supports "streaming" content as well as "legacy" systems (e.g., CGMS).

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages provided in accordance with these inventions may be better and more completely understood by referring to the following detailed description of presently preferred examples in conjunction with the drawings, of which:

Figure 1A shows example home consumer electronics equipment for using portable storage media such as digital video disks;

Figure 1B shows example secure node equipment for using the same portable storage media but providing more advanced rights management capabilities;

Figure 1C shows an example process for manufacturing protected optical disks;

Figure 2A shows an example architecture of the Figure 1A consumer electronics equipment;

Figure 2B shows an example architecture for the Figure 1B secure node equipment;

Figure 3 shows example data structures used by the Figure 1A equipment;

Figure 3A and 3B show example control set definitions;

Figures 4A and 4B show example usage techniques provided by the Figure 1A appliance;

Figure 5 shows example data structures used by the Figure 1B secure node for accessing information on the storage medium;

Figure 6 shows an example usage technique performed by the Figure 1B secure node;

Figure 7 is a block diagram illustrating an example of a special secure software container contained on a DVD;

Figure 8 is a block diagram illustrating an example of a secure container along with the video property content stored on a DVD medium;

Figure 9 is a block diagram illustrating another example of a standard container stored on a DVD medium including an additional container having a more complex rule arrangement for use, for example, with a secure node;

Figure 10 shows an example use of a DVD having a container (i.e., stored on the medium) with a DVD player provided with a secure rights management node, and also shows use of the same DVD with a DVD player that does not have a secure rights management node;

Figure 11 is a block diagram illustrating use of a DVD that does not have a container on a DVD player that is provided with rights management secure node in accordance with the present invention as compared with use of the same DVD with a DVD player that does not have a secure node;

Figures 12-14 show example network configurations; and

Figures 15A-15C show an example virtual rights process.

DETAILED DESCRIPTION OF PRESENTLY PREFERRED EXAMPLE EMBODIMENTS

Overall Example Digital Video Disk Usage System

Figure 1A shows example inexpensive mass-produced home consumer electronics equipment 50 for using information stored on a storage medium 100 such as a portable digitally-encoded optical disk (e.g., a digital video disk or "DVD").

Consumer equipment 50 includes a dedicated disk player 52, that in some embodiments, may also have the capability to write optical media (writeable DVD disks, or "DVD-RAM") for example) as well, connected to a home color television set 54. A remote control unit 56 may be used to control the disk player 52 and/or television set 54.

In one example, disk 100 may store a feature length motion picture or other video content. Someone wishing to watch the content stored on disk 100 may purchase or rent the disk, insert the disk into player 52 and use remote control 56 (and/or controls 58 that may be provided on player 52) to control the player to play back the content via home television set 54.

In some embodiments, remote control 56 (and/or controls 58 that may be provided on device 52) may be used to control the recording of a movie, for example. Player 52 reads the digitized video and audio information carried by disk 100, converts it into signals compatible with home color television set 54, and provides those signals to the home color television set.

In some embodiments, television set 54 (and/or a set top box) provide the video signals to be recorded by device 52 on writable optical media, DVD-RAM in one non-limiting example. Television set 54 produces images on screen 54a and produces sounds through loudspeakers 54b based on the signals player 52 provides to the television set.

The same disk 100 may be used by a more advanced platform 60 shown in Figure 1B. Platform 60 may include, for example, a personal computer 62 connected to a display monitor 64, a keyboard 66, a mouse pointing device 68, and a loudspeaker 70. In this example, platform 60 may be able to play back the content stored on disk 100 in the same way as dedicated disk player 52, but may also be capable of more sophisticated and/or advanced uses of the content as enabled by the presence of secure node 72 within the platform. (In some embodiments, platform 60 may also be able to record content on writable optical media, DVD-RAM, in one non-limiting example.) For example, it may be possible, using platform 60 and its secure node 72, to interactively present the motion picture or other content such that the user may input choices via keyboard 66 and/or mouse pointing device 68

that, in real time, change the presentation provided via display 64 and loudspeaker 60.

As one example, the platform 60 user selects from options displayed on display 64 that cause the content presentation sequence to change (e.g., to provide one of a number of different endings, to allow the user to interactively control the flow of the images presented, etc.). Computer 62 may also be capable of using and manipulating digital data including for example computer programs and/or other information stored on disk 100 that player 52 cannot handle.

Secure node 72 provides a secure rights management facility that may, for example, permit more invasive or extensive use of the content stored on disk. For example, dedicated player 52 may prevent any copying of content stored by disk 100, or it may allow the content to be copied only once and never again. Platform 60 including secure node 72, on the other hand, may allow multiple copies of some or all of the same content—but only if certain conditions are met (e.g., the user of equipment 60 falls within a certain class of people, compensation at an agreed on rate is securely provided for each copy made, only certain excerpts of

the content are copied, a secure audit trail is maintained and reported for each copy so made, etc.). (In some embodiments, dedicated player 52 may send protected content only to devices authenticated as able to enforce securely rights management rules and usage consequences. In some embodiments, devices may authenticate using digital certificates, one non-limiting example being certificates conforming to the X.509 standard.) Hence, platform 60 including secure node 72 can, in this example, use the content provided by disk 100 in a variety of flexible, secure ways that are not possible using dedicated player 52—or any other appliance that does not include a secure node.

Example Secure Disk Creation and Distribution Process

Figure 1C shows an example secure process for creating a master multimedia DVD disk 100 for use with players 50, 60. In this example, a digital camera 350 converts light images (i.e., pictures) into digital information 351 representing one or a sequence of images. Digital camera 350 in this example includes a secure node 72A that protects the digital information 351 before it leaves camera 350. Such protection can be accomplished, for

example, by packaging the digital information within one or more containers and/or associating controls with the digital information.

In this example, digital camera 350 provides the protected digital image information 351 to a storage device such as, for example, a digital tape recorder 352. Tape recorder 352 stores the digital image information 351 (along with any associated controls) onto a storage medium such as magnetic tape cartridge 354 for example. Tape recorder 352 may also include a secure node 72B. Secure node 72B in this example can understand and enforce the controls that the digital camera secure node 72A applies to and/or associated with the digital information 351, and/or it may apply its own controls to the stored information.

The same or different tape recorder 352 may play back protected digital information 351 to a digital mixing board 356. Digital mixing board 356 may mix, edit, enhance or otherwise process the digital information 351 to generate processed digital information 358 representing one or a sequence of images. Digital mixing board 356 may receive additional inputs from other devices such as for example other tape recorders, other digital cameras, character generators, graphics generators, animators, or

any other image-based devices. Any or all of such devices may also include secure nodes 72 to protect the information they generate. In some embodiments, some of the digital information can be derived from equipment including a secure node, and other digital information can be derived from equipment that has no secure node. In still other embodiments, some of the digital information provided to digital mixer 356 is protected and some is not protected.

Digital mixing board 356 may also include a secure node 72C in this example. The digital mixing board secure node 72C may enforce controls applied by digital camera secure node 72A and/or tape recorder secure node 72B, and/or it may add its own protections to the digital information 358 it generates.

In this example, an audio microphone 361 receives sound and converts the sound into analog audio signals. The audio signals in this example are inputted to a digital audio tape recorder 362. In the example shown, tape recorder 362 and audio mixer 364 are digital devices. However, in other embodiments, one, the other or both of these devices may operate in the analog domain. In the example shown, digital audio tape recorder 362 converts the

analog audio signals into digital information representing the sounds, and stores the digital information (and any associated controls) onto a tape 362.

In this example, audio tape recorder 362 includes a secure node 72E that may associate controls with the information stored on tape 363. Such controls may be stored with the information on the tape 363. In another embodiment, microphone 361 may include its own internal secure node 72 that associates control information with the audio information (e.g., by steganographically encoding the audio information with control information). The tape recorder 362 may enforce such controls applied by microphone 361.

Alternatively, microphone 361 may operate in the digital domain and provide digital representations of audio, perhaps including control information supplied by secure node 72 optionally incorporated in microphone 361, directly to connected devices such as audio tape recorder 362. Digital representations may optionally be substituted for analog representations of any signals between the devices in the example Figure 1C.

The same or different tape recorder 362 may play back the information recorded on tape 363, and provide the information 366 to an audio mixer 364. Audio mixer 364 may edit, mix, or otherwise process the information 366 to produce information 368 representing one or a sequence of sounds. Audio mixer 364 may also receive inputs from other devices such as for example other tape recorders, other microphones, sound generators, musical synthesizers, or any other audio-based devices. Any or all of such devices may also include secure nodes 72 to protect the information they generate. In some embodiments, some of the digital information is derived from equipment including a secure node, and other digital information is derived from equipment that has no secure node. In still other embodiments, some of the digital information provided to audio mixer 364 is protected and some is not protected.

Audio mixer 364 in this example includes a secure node 72F that enforces the controls, if any, applied by audio tape recorder secure node 72E; and/or applies its own controls.

Digital image mixer 356 may provide digital information 358 to "DVD-RAM" equipment 360 that is capable of writing to

master disks 100 and/or to disks from which master dicks may be created Similarly, audio mixer 364 may provide digital information 368 to equipment 360. Equipment 360 records the image information 358 and audio information 368 onto master disk 100. In this example, equipment 360 may include a secure node 72D that enforces controls applied by digital camera secure node 72A, tape recorder secure node 72B, digital mixer secure node 72C audio tape recorder secure node 72E and/or audio mixer secure node 72F; and/or it may add its own protections to the digital information 358 it writes onto master disks 100. A disk manufacturer can then mass-produce disks 100(1)-100(N) based on the master disk 100 using conventional disk mass-production equipment for distribution through any channels (e.g., video and music stores, websites, movie theaters, etc.). Consumer appliances 50 shown in Figures 1A and 1B may play back the disks 100 – enforcing the controls applied to the information stored on the disks 100. Secure nodes 72 thus maintain end-to-end, persistent secure control over the images generated by digital camera 350 and the sounds generated by microphone 361 during the entire process of making, distributing and using disks 100.

In the Figure 1C example shown, the various devices may communicate with one another over so-called "IEEE 1394" high-speed digital serial busses. In this context, "IEEE 1394" refers to hardware and software standards set forth in the following standards specification incorporated by reference herein: 1394-1995 IEEE Standard for a High Performance Serial Bus, No. 1-55937-583-3 (Institute of Electrical and Electronics Engineers 1995). This specification describes a high-speed memory mapped digital serial bus that is self-configuring, hot pluggable, low cost and scalable. The bus supports isochronous and asynchronous transport at 100, 200 or 400 Mbps, and flexibly supports a number of different topologies. The specification describes a physical level including two power conductors and two twisted pairs for signalling. The specification further describes physical, link and transaction layer protocols including serial bus management. Alternatively, any other suitable electronic communication means may be substituted for the "IEEE 1394" medium shown in Figure 1C, including other wired media (e.g., Ethernet, universal serial bus), and/or wireless media based on radio-frequency (RF)

transmission, infra-red signals, and/or any other means and/or types of electronic communication.

Example Dedicated Player Architecture

Figure 2A shows an example architecture for dedicated player 52. In this example, player 52 includes a video disk drive 80, a controller 82 (e.g., including a microprocessor 84, a memory device such as a read only memory 86, and a user interface 88), and a video/audio processing block 90. Video disk drive 80 optically and physically cooperates with disk 100, and reads digital information from the disk. Controller 82 controls disk drive 80 based on program instructions executed by microprocessor 84 and stored in memory 86 (and further based on user inputs provided by user interface 88 which may be coupled to controls 58 and/or remote control unit 56). Video/audio processing block 90 converts digital video and audio information read by disk drive 80 into signals compatible with home color television set 54 using standard techniques such as video and audio decompression and the like. Video/audio processing block 90 may also insert a visual marking indicating the ownership and/or protection of the video program. Block 90 may also

introduce a digital marking indicating to a standard recording device that the content should not be recorded.

Example Secure Node Architecture

Figure 2B shows an example architecture for platform 60 shown in Figure 1B—which in this example is built around a personal computer 62 but could comprise any number of different types of appliances. In this example, personal computer 62 may be connected to an electronic network 150 such as the Internet via a communications block 152. Computer equipment 62 may include a video disk drive 80' (which may be similar or identical to the disk drive 80 included within example player 52). Computer equipment 62 may further include a microprocessor 154, a memory 156 (including for example random access memory and read only memory), a magnetic disk drive 158, and a video/audio processing block 160. Additionally, computer equipment 62 may include a tamper-resistant secure processing unit 164 or other protected processing environment. Secure node 72 shown in Figure 1B may thus be provided by a secure processing unit 164, software executing on microprocessor 154, or a combination of

the two. Different embodiments may provide secure node 72 using software-only, hardware-only, or hybrid arrangements.

Secure node 72 in this example may provide and support a a general purpose Rights Operating System employing reusable kernel and rights language components. Such a commerce-enabling Rights Operating System provides capabilities and integration for advanced commerce operating systems of the future. In the evolving electronic domain, general purpose, reusable electronic commerce capabilities that all participants can rely on will become as important as any other capability of operating systems. Moreover, a rights operating system that provides, among other things, rights and auditing operating system functions can securely handle a broad range of tasks that relate to a virtual distribution environment. A secure processing unit can, for example, provide or support many of the security functions of the rights and auditing operating system functions. The other operating system functions can, for example, handle general appliance functions. The overall operating system may, for example, be designed from the beginning to include the rights and auditing operating system functions plus the other operating

system functions, or the rights and auditing operating system functions may, in another example, be an add-on to a preexisting operating system providing the other operating system functions. Any or all of these features may be used in combination with the invention disclosed herein.

Example Disk Data Structures and Associated Protections

Figure 3 shows some example data structures stored on disk 100. In this example, disk 100 may store one or more properties or other content 200 in protected or unprotected form. Generally, in this example, a property 200 is protected if it is at least in part encrypted and/or associated information needed to use the property is at least in part encrypted and/or otherwise unusable without certain conditions having being met. For example, property 200(1) may be completely or partially encrypted using conventional secure cryptographic techniques. Another property 200(2) may be completely unprotected so that it can be used freely without any restriction. Thus, in accordance with this example, disk 100 could store both a movie as a protected property 200(1) and an unprotected interview with the actors and producers or a

"trailer" as unprotected property 200(2). As shown in this example, disk 100 may store any number of different properties 200 in protected or unprotected form as limited only by the storage capacity of the disk.

In one example, the protection mechanisms provided by disk 100 may use any or all of the protection (and/or other) structures and/or techniques described in the above-referenced Shear patents. The Shear patents describe, by way of non-exhaustive example, means for solving the problem of how to protect digital content from unauthorized use. For example, the Shear patent specifications describe, among other things, means for electronically "overseeing" -- through distributed control nodes present in client computers -- the use of digital content. This includes means and methods for fulfilling the consequences of any such use.

Non-limiting examples of certain elements described in the Shear patent specifications include:

(a) decryption of encrypted information,

(b) metering,

(c) usage control in response to a combination of derived metering information and rules set by content providers,

(d) securely reporting content usage information,

(e) use of database technology for protected information storage and delivery,

(f) local secure maintenance of budgets, including, for example, credit budgets,

(g) local, secure storage of encryption key and content usage information,

(h) local secure execution of control processes, and

(i) in many non-limiting instances, the use of optical media.

Any or all of these features may be used in combination in or with the inventions disclosed herein.

Certain of the issued Shear patents' specifications also involve database content being local and remote to users.

Database information that is stored locally at the end-user's system and complemented by remote, "on-line" database information, can, for example, be used to augment the local information, which in one example, may be stored on optical media (for example, DVD and/or CD-ROM). Special purpose semiconductor hardware can, for example, be used to provide a secure execution environment to ensure a safe and reliable setting for digital commerce activities.

The Shear patents also describe, among other things, database usage control enabled through the use of security, metering, and usage administration capabilities. The specifications describe, *inter alia*, a metering and control system in which a database, at least partially encrypted, is delivered to a user (e.g., on optical media). Non-limiting examples of such optical media may, for example, include DVD and CD-ROM. Subsequent usage can, for example, be metered and controlled in any of a variety of ways, and resulting usage information can be transmitted to a responsible party (as one example).

The Shear patent specifications also describe the generation of a bill in response to the transmitted information. Other

embodiments of the Shear patents provide, for example, unique information security inventions which involve, for example, digital content usage being limited based on patterns of usage such as the quantity of particular kinds of usage. These capabilities include monitoring the "contiguousness," and/or "logical relatedness" of used information to ensure that the electronic "conduct" of an individual does not exceed his or her licensed rights. Still other aspects of the Shear patents describe, among other things, capabilities for enabling organizations to securely and locally manage electronic information usage rights. When a database or a portion of a database is delivered to a client site, some embodiments of the Shear patents provide, for example, optical storage means (non-exhaustive examples of which include DVD and CD-ROM) as the mechanism of delivery. Such storage means can store, for example, a collection of video, audio, images, software programs, games, etc., in one example, on optical media, such as DVD and/or CD-ROM, in addition to other content such as a collection of textual documents, bibliographic records, parts catalogs, and copyrighted or uncopyrighted materials of all kinds.

Any or all of these features may be used in the embodiments herein.

One specific non-limiting embodiment could, for example, involve a provider who prepares a collection of games. The provider prepares a database "index" that stores information pertaining to the games, such as for example, the name, a description, a creator identifier, the billing rates, and the maximum number of times or total elapsed time each game may be used prior to a registration or re-registration requirement. Some or all of this information could be stored in encrypted form, in one example, on optical media, non-limiting examples of which include DVD and CD-ROM. The provider may then encrypt some or all portions of the games such that a game could not be used unless one or more encrypted portions were decrypted. Typically, decryption would not occur unless provider specified conditions were satisfied, in one example, unless credit was available to compensate for use and audit information reflecting game usage was being stored. The provider could determine, for example: which user activities he or she would allow, whether to meter such activities for audit and/or control purposes, and what, if any, limits

would be set for allowed activities. This might include, for example, the number of times that a game is played, and the duration of each play. Billing rates might be discounted, for example, based on total time of game usage, total number of games currently registered for use, or whether the customer was also registered for other services available from the same provider, etc.

In the non-limiting example discussed above, a provider might, for example, assemble all of the prepared games along with other, related information, and publish the collection on optical media, non-limiting examples of which include CD-ROM and/or DVD. The provider might then distribute this DVD disk to prospective customers. The customers could then select the games they wish to play, and contact the provider. The provider, based on its business model, could then send enabling information to each authorized customer, such as for example, including, or enabling for use, decryption keys for the encrypted portion of the selected games (alternatively, authorization to use the games may have arrived with the DVD and/or CD-ROM disk, or might be automatically determined, based on provider set criteria, by the

user's secure client system, for example, based on a user's participation in a certified user class). Using the user's client decryption and metering mechanism the customer could then make use of the games. The mechanism might then record usage information, such as for example, the number of times the game was used, and, for example, the duration of each play. It could periodically transmit this information the game provider, thus substantially reducing the administration overhead requirements of the provider's central servers. The game provider could receive compensation for use of the games based upon the received audit information. This information could be used to either bill their customers or, alternatively, receive compensation from a provider of credit.

Although games provide one convenient, non-limiting example, many of these same ideas can be easily applied to all kinds of content, all kinds of properties, including, by way of non-limiting examples:

- video,
- digitized movies,

- audio,
- images,
- multimedia,
- software,
- games,
- any other kind of property
- any combination of properties.

Other non-limiting embodiments of the Shear patent specifications support, for example, securely controlling different kinds of user activities, such as displaying, printing, saving electronically, communicating, etc. Certain aspects further apply different control criteria to these different usage activities. For example, information that is being browsed may be distinguished from information that is read into a host computer for the purpose of copying, modifying, or telecommunicating, with different cost rates being applied to the different activities (so that, for example,

the cost of browsing can be much less than the cost of copying or printing).

The Shear patent specifications also, for example, describe management of information inside of organizations by both publishers and the customer. For example, an optional security system can be used to allow an organization to prevent usage of all or a portion of an information base unless the user enters his security code. Multiple levels of security codes can be supported to allow restriction of an individual's use according to his security authorization level. One embodiment can, for example, use hardware in combination with software to improve tamper resistance, and another embodiment could employ an entirely software based system. Although a dedicated hardware/software system may under certain circumstances provide assurance against tampering, techniques which may be implemented in software executing on a non-dedicated system may provide sufficient tamper resistance for some applications. Any or all of these features may be used in combination with the technology disclosed in this patent specification.

Figures 3 Disks May Also Store Metadata, Controls and Other Information

In this example, disk 100 may also store "metadata" in protected and/or unprotected form. Player 52 uses metadata 202 to assist in using one or more of the properties 200 stored by disk 100. For example, disk 100 may store one metadata block 202(1) in unprotected form and another metadata block 202(2) in protected form. Any number of metadata blocks 202 in protected and/or unprotected form may be stored by disk 100 as limited only by the disk's storage capacity. In this example, metadata 202 comprises information used to access properties 200. Such metadata 202 may comprise, for example, frame sequence or other "navigational" information that controls the playback sequence of one or more of the properties 200 stored on disk 100. As one example, an unprotected metadata block 202 may access only selected portions of a protected property 200 to generate an abbreviated "trailer" presentation, while protected metadata block 202 may contain the frame playback sequence for the entire video presentation of the property 200. As another example, different metadata blocks 202 may be provided for different "cuts" of the

same motion picture property 200 (e.g., an R-rated version, a PG-rated version, a director's cut version, etc.).

In this example, disk 100 may store additional information for security purposes. For example, disk 100 may store control rules in the form of a control set 204—which may be packaged in the form of one or more secure containers 206. Commerce model participants can securely contribute electronic rules and controls that represent their respective "electronic" interests. These rules and controls extend a "Virtual Presence™" through which the commerce participants may govern remote value chain activities according to their respective, mutually agreed to rights. This Virtual Presence may take the form of participant specified electronic conditions (e.g., rules and controls) that must be satisfied before an electronic event may occur. These rules and controls can be used to enforce the party's rights during "downstream" electronic commerce activities. Control information delivered by, and/or otherwise available for use with, VDE content containers may, for example, constitute one or more "proposed" electronic agreements which manage the use and/or consequences of the use of such content and which can enact the

terms and conditions of agreements involving multiple parties and their various rights and obligations.

The rules and controls from multiple parties can be used, in one example, to form aggregate control sets ("Cooperative Virtual Presence™") that ensure that electronic commerce activities will be consistent with the agreements amongst value chain participants. These control sets may, for example, define the conditions which govern interaction with protected digital content (disseminated digital content, appliance control information, etc.). These conditions can, for example, be used to control not only digital information use itself, but also the consequences of such use. Consequently, the individual interests of commerce participants are protected and cooperative, efficient, and flexible electronic commerce business models can be formed. These models can be used in combination with the present invention.

Disks May Store Encrypted Information

Disk 100 may also store an encrypted key block 208. In this example, disk 100 may further store one or more hidden keys 210. In this example, encrypted key block 208 provides one or more cryptographic keys for use in decrypting one or more properties

200 and/or one or more metadata blocks 202. Key block 208 may provide different cryptographic keys for decrypting different properties 200 and/or metadata blocks 202, or different portions of the same property and/or metadata block. Thus, key block 208 may comprise a large number of cryptographic keys, all of which are or may be required if all of the content stored by disk 100 is to be used. Although key block 208 is shown in Figure 3 as being separate from container 206, it may be included within or as part of the container if desired.

Cryptographic key block 208 is itself encrypted using one or more additional cryptographic keys. In order for player 52 to use any of the protected information stored on disk 100, it must first decrypt corresponding keys within the encrypted key block 208—and then use the decrypted keys from the key block to decrypt the corresponding content.

In this example, the keys required to decrypt encrypted key block 208 may come from several different (possibly alternative) sources. In the example shown in Figure 3, disk 100 stores one or more decryption keys for decrypting key block 208 on the medium itself in the form of a hidden key(s) 210. Hidden key(s) 210 may

be stored, for example, in a location on disk 100 not normally accessible. This "not normally accessible" location could, for example, be physically enabled for drives 80 installed in players 52 and disabled for drives 80' installed in personal computers 62. Enablement could be provided by different firmware, a jumper on drive 80, etc. Hidden key(s) 210 could be arranged on disk 100 so that any attempt to physically copy the disk would result in a failure to copy the hidden key(s). In one example a hidden key(s) could be hidden in the bit stream coding sequences for one or more blocks as described by J. Hogan (Josh Hogan, "DVD Copy Protection," presentation to DVD copy protect technical meeting #4, 5/30/96, Burbank, CA.)

Alternatively, and/or in addition, keys required to decrypt encrypted key block 208 could be provided by disk drive 80. In this example, disk drive 80 might include a small decryption component such as, for example, an integrated circuit decryption engine including a small secure internal key store memory 212 having keys stored therein. Disk drive 80 could use this key store 212 in order to decrypt encrypted key block 208 without exposing either keys 212 or decrypted key block 208—and then use the

decrypted key from key block 208 to decrypt protected content 200, 202.

Disks May Store and/or Use Secure Containers

In yet another example, the key(s) required to decrypt protected content 200, 202 is provided within secure container 206. Figure 3A shows a possible example of a secure container 206 including information content 304 (properties 200 and metadata 202 may be external to the container—or alternatively, most or all of the data structures stored by video disk 100 may be included as part of a logical and/or actual protected container). The control set 204 shown in Figure 3 may comprise one or more permissions record 306, one or more budgets 308 and/or one or more methods 310 as shown in Figure 3A. Figure 3B shows an example control set 204 providing one or more encryption keys 208, one or more content identifiers 220, and one or more controls 222. In this example, different controls 222 may apply to different equipment and/or classes of equipment such as player 52 and/or computer equipment 62 depending upon the capabilities of the particular platform and/or class of platform. Additionally, controls 220 may apply to different ones of properties 200 and/or

different ones of metadata blocks 202. For example, a control 222(1) may allow property 200(1) to be copied only once for archival purposes by either player 52 or computer equipment 62. A control 222(2) (which may be completely ignored by player 52 because it has insufficient technical and/or security capabilities but which may be useable by computer equipment 62 with its secure node 72) may allow the user to request and permit a public performance of the same property 200(1) (e.g., for showing in a bar or other public place) and cause the user's credit or other account to be automatically debited by a certain amount of compensation for each showing. A third control 222(3) may, for example, allow secure node 72 (but not player 52) to permit certain classes of users (e.g., certified television advertisers and journalists) to extract or excerpt certain parts of protected property 200(1) for promotional uses. A further control 222(4) may, as another example, allow both video player 52 and secure node 72 to view certain still frames within property 200(1)—but might allow only secure node 72 to make copies of the still frames based on a certain compensation level.

Example Disks and/or System May Make Use of Trusted Infrastructure

Controls 222 may contain pointers to sources of additional control sets for one or more properties, controls, metadata, and/or other content on the optical disk. In one example, these additional controls may be obtained from a trusted third party, such as a rights and permissions clearinghouse and/or from any other value chain participant authorized by at least one rightsholder to provide at least one additional control set. This kind of rights and permissions clearinghouse is one of several distributed electronic administrative and support services that may be referred to as the "Distributed Commerce Utility," which, among other things, is an integrated, modular array of administrative and support services for electronic commerce and electronic rights and transaction management. These administrative and support services can be used to supply a secure foundation for conducting financial management, rights management, certificate authority, rules clearing, usage clearing, secure directory services, and other transaction related capabilities functioning over a vast electronic network such as the Internet and/or over organization internal Intranets, or even in-home networks of electronic appliances. Non-

limiting examples of these electronic appliances include at least occasionally connected optical media appliances, examples of which include read-only and/or writable DVD players and DVD drives in computers and convergent devices, including, for example, digital televisions and settop boxes incorporating DVD drives.

These administrative and support services can, for example, be adapted to the specific needs of electronic commerce value chains in any number of vertical markets, including a wide variety of entertainment applications. Electronic commerce participants can, for example, use these administrative and support services to support their interests, and/or they can shape and reuse these services in response to competitive business realities. Non-exhaustive examples of electronic commerce participants include individual creators, film and music studios, distributors, program aggregators, broadcasters, and cable and satellite operators.

The Distributed Commerce Utility can, for example, make optimally efficient use of commerce administration resources, and can, in at least some embodiments, scale in a practical fashion to

optimally accommodate the demands of electronic commerce growth.

The Distributed Commerce Utility may, for example, comprise a number of Commerce Utility Systems. These Commerce Utility Systems can provide a web of infrastructure support available to, and reusable by, the entire electronic community and/or many or all of its participants. Different support functions can, for example, be collected together in hierarchical and/or in networked relationships to suit various business models and/or other objectives. Modular support functions can, for example, be combined in different arrays to form different Commerce Utility Systems for different design implementations and purposes. These Commerce Utility Systems can, for example, be distributed across a large number of electronic appliances with varying degrees of distribution.

The "Distributed Commerce Utility" provides numerous additional capabilities and benefits that can be used in conjunction with the particular embodiments shown in the drawings of this application, non-exhaustive examples of which include:

- Enables practical and efficient electronic commerce and rights management.

- Provides services that securely administer and support electronic interactions and consequences.

- Provides infrastructure for electronic commerce and other forms of human electronic interaction and relationships.

- Optimally applies the efficiencies of modern distributed computing and networking.

- Provides electronic automation and distributed processing.

- Supports electronic commerce and communications infrastructure that is modular, programmable, distributed and optimally computerized.

- Provides a comprehensive array of capabilities that can be combined to support services that perform various administrative and support roles.

- Maximizes benefits from electronic automation and distributed processing to produce optimal allocation and use of resources across a system or network.

- Is efficient, flexible, cost effective, configurable, reusable, modifiable, and generalizable.

- Can economically reflect users' business and privacy requirements.

- Can optimally distribute processes -- allowing commerce models to be flexible, scaled to demand and to match user requirements.

- Can efficiently handle a full range of activities and service volumes.

- Can be fashioned and operated for each business model, as a mixture of distributed and centralized processes.

- Provides a blend of local, centralized and networked capabilities that can be uniquely shaped and reshaped to meet changing conditions.

- Supports general purpose resources and is reusable for many different models; in place infrastructure can be reused by different value chains having different requirements.

- Can support any number of commerce and communications models.

- Efficiently applies local, centralized and networked resources to match each value chain's requirements.

- Sharing of common resources spreads out costs and maximizes efficiency.

- Supports mixed, distributed, peer-to-peer and centralized networked capabilities.

- Can operate locally, remotely and/or centrally.

- Can operate synchronously, asynchronously, or support both modes of operation.

- Adapts easily and flexibly to the rapidly changing sea of commercial opportunities, relationships and constraints of "Cyberspace."

Any or all of these features may be used in combination with the inventions disclosed herein.

The Distributed Commerce Utility provides, among other advantages, comprehensive, integrated administrative and support services for secure electronic commerce and other forms of electronic interaction. These electronic interactions supported by the Distributed Commerce Utility may, in at least some embodiments, entail the broadest range of appliances and distribution media, non-limiting examples of which include networks and other communications channels, consumer appliances, computers, convergent devices such as WebTV, and optical media such as CD-ROM and DVD in all their current and future forms.

Example Access Techniques

Figures 3, 4A and 4B show example access techniques provided by player 52. In this example, upon disk 100 being loaded into player disk drive 80 (Figure 4A, block 400), the player controller 82 may direct drive 80 to fetch hidden keys 210 from disk 100 and use them to decrypt some or all of the encrypted key block 208 (Figure 4A, block 402). In this example, drive 80 may

store the keys so decrypted without exposing them to player controller 82 (e.g., by storing them within key store 212 within a secure decryption component such as an integrated circuit based decryption engine) (Figure 4A, block 404). The player 52 may control drive 80 to read the control set 204 (which may or may not be encrypted) from disk 100 (Figure 4A, block 406). The player microprocessor 82 may parse control set 204, ignore or discard those controls 222 that are beyond its capability, and maintain permissions and/or rights management information corresponding to the subset of controls that it can enforce (e.g., the "copy once" control 222(1)).

Player 52 may then wait for the user to provide a request via control inputs 58 and/or remote control unit 56. If the control input is a copy request ("yes" exit to Figure 4A, decision block 408), then player microprocessor 84 may query control 222(1) to determine whether copying is allowed, and if so, under what conditions (Figure 4A, decision block 410). Player 52 may refuse to copy the disk 100 if the corresponding control 222(1) forbids copying ("no" exit to Figure 4A, decision block 410), and may allow copying (e.g., by controlling drive 80 to sequentially access

all of the information on disk 100 and provide it to an output port not shown) if corresponding control 222(1) permits copying ("yes" exit to Figure 4A, decision block 410; block 412). In this example, player 52 may, upon making a copy, store an identifier associated with disk 100 within an internal, non-volatile memory (e.g., controller memory 86) or elsewhere if control 222(1) so requires. This stored disk identifier can be used by player 52 to enforce a "copy once" restriction (i.e., if the user tries to use the same player to copy the same disk more than once or otherwise as forbidden by control 222(1), the player can deny the request).

If the user requests one of properties 200 to be played or read ("yes" exit to Figure 4A, decision block 414), player controller 82 may control drive 80 to read the corresponding information from the selected property 200 (e.g., in a sequence as specified by metadata 202) and decrypt the read information as needed using the keys initially obtained from key block 208 and now stored within drive key storage 212 (Figure 4A, block 416).

Figure 4B is a variation on the Figure 4A process to accommodate a situation in which player 52 itself provides decryption keys for decrypting encrypted key block 208. In this

example, controller 82 may supply one or more decryption keys to drive 80 using a secure protocol such a Diffie-Hellman key agreement, or through use of a shared key known to both the drive and some other system or component to which the player 52 is or once was coupled (Figure 4B, block 403). The drive 80 may use these supplied keys to decrypt encrypted key block 208 as shown in Figure 4A, block 404, or it may use the supplied keys to directly decrypt content such as protected property 200 and/or protected metadata 202(2).

As a further example, the player 52 can be programmed to place a copy it makes of a digital property such as a film in encrypted form inside a tamper-resistant software container. The software container may carry with it a code indicating that the digital property is a copy rather than an original. The sending player 52 may also put its own unique identifier (or the unique identifier of an intended receiving device such as another player 52, a video cassette player or equipment 50) in the same secure container to enforce a requirement that the copy can be played only on the intended receiving device. Player 52 (or other receiving device) can be programmed to make no copies (or no

additional copies) upon detecting that the digital property is a copy rather than an original. If desired, a player 52 can be programmed to refuse to play a digital property that is not packaged with the player's unique ID.

Example Use of Analog Encoding Techniques

In another example, more comprehensive rights management information may be encoded by player 52 in the analog output using methods for watermarking and/or fingerprinting.Today, a substantial portion of the "real world" is analog rather than digital. Despite the pervasiveness of analog signals, existing methods for managing rights and protecting copyright in the analog realm are primitive or non-existent. For example:

- Quality degradation inherent in multigenerational analog copying has not prevented a multi-billion dollar pirating industry from flourishing.

- Some methods for video tape copy and pay per view protection attempt to prevent any copying at all of commercially released content, or allow only one

generation of copying. These methods can generally be easily circumvented.

- Not all existing devices respond appropriately to copy protection signals.

- Existing schemes are limited for example to "copy/no copy" controls.

- Copy protection for sound recordings has not been commercially implemented.

A related problem relates to the conversion of information between the analog and digital domains. Even if information is effectively protected and controlled initially using strong digital rights management techniques, an analog copy of the same information may no longer be securely protected.

For example, it is generally possible for someone to make an analog recording of program material initially delivered in digital form. Some analog recordings based on digital originals are of quite good quality. For example, a Digital Versatile Disk

("DVD") player may convert a movie from digital to analog format and provide the analog signal to a high quality analog home VCR. The home VCR records the analog signal. A consumer now has a high quality analog copy of the original digital property. A person could re-record the analog signal on a DVD-RAM. This recording will in many circumstances have substantial quality – and would no longer be subject to "pay per view" or other digital rights management controls associated with the digital form of the same content.

Since analog formats will be with us for a long time to come, rightsholders such as film studios, video rental and distribution companies, music studios and distributors, and other value chain participants would very much like to have significantly better rights management capabilities for analog film, video, sound recordings and other content. Solving this problem generally requires a way to securely associate rights management information with the content being protected.

In combination with other rights management capabilities, watermarking and/or fingerprinting, may provide "end to end"

secure rights management protection that allows content providers and rights holders to be sure their content will be adequately protected -- irrespective of the types of devices, signaling formats and nature of signal processing within the content distribution chain. This "end to end" protection also allows authorized analog appliances to be easily, seamlessly and cost-effectively integrated into a modern digital rights management architecture.

Watermarking and/or fingerprinting may carry, for example, control information that can be a basis for a Virtual Distribution Environment ("VDE") in which electronic rights management control information may be delivered over insecure (e.g., analog) communications channels. This Virtual Distribution Environment is highly flexible and convenient, accommodating existing and new business models while also providing an unprecedented degree of flexibility in facilitating ad hoc creation of new arrangements and relationships between electronic commerce and value chain participants -- regardless of whether content is distributed in digital and/or analog formats.

Watermarking together with distributed, peer-to-peer rights management technologies providers numerous advantages, including, but not limited to:

- An indelible and invisible, secure technique for providing rights management information.

- An indelible method of associating electronic commerce and/or rights management controls with analog content such as film, video, and sound recordings.

- Persistent association of the commerce and/or rights management controls with content from one end of a distribution system to the other -- regardless of the number and types of transformations between signaling formats (for example, analog to digital, and digital to analog).

- The ability to specify "no copy/ one copy/ many copies" rights management rules, and also more

complex rights and transaction pricing models (such as, for example, "pay per view" and others).

- The ability to fully and seamlessly integrate with comprehensive, general electronic rights management solutions.

- Secure control information delivery in conjunction with authorized analog and other non-digital and/or non-secure information signal delivery mechanisms.

- The ability to provide more complex and/or more flexible commerce and/or rights management rules as content moves from the analog to the digital realm and back.

- The flexible ability to communicate commerce and/or rights management rules implementing new, updated, or additional business models to authorized analog and/or digital devices.

Any or all of these features may be used in combination in and/or with the inventions disclosed in the present specification.

Briefly, watermarking and/or fingerprinting methods may, using "steganographical" techniques, substantially indelibly and substantially invisibly encode rights management and/or electronic commerce rules and controls within an information signal such as, for example, an analog signal or a digitized (for example, sampled) version of an analog signal, non-limiting examples of which may include video and/or audio data, that is then decoded and utilized by the local appliance. The analog information and stenographically encoded rights management information may be transmitted via many means, non-limiting examples of which may include broadcast, cable TV, and/or physical media, VCR tapes, to mention one non-limiting example. Any or all of these techniques may be used in combination in accordance with the inventions disclosed herein.

Watermarking and/or fingerprinting methods enable at least some rights management information to survive transformation of the video and/or other information from analog to digital and from

digital to analog format. Thus in one example, two or more analog and/or digital appliances may participate in an end-to-end fabric of trusted, secure rights management processes and/or events.

Example, More Capable Embodiments

As discussed above, the example control set shown in Figure 3B provides a comprehensive, flexible and extensible set of controls for use by both player 52 and computer equipment 62 (or other platform) depending upon the particular technical, security and other capabilities of the platform. In this example, player 52 has only limited technical and security capabilities in order to keep cost and complexity down in a mass-produced consumer item, and therefore may essentially ignore or fail to enable some or all of the controls 222 provided within control set 204. In another example, the cost of memory and/or processors may continue to decline and manufacturers may choose to expand the technical and security capabilities of player 52. A more capable player 52 will provide more powerful, robust, and flexible rights management capabilities.

Figure 5 shows an example arrangement permitting platform 60 including secure node 72 to have enhanced and/or different capabilities to use information and/or rights management information on disk 100, and Figure 6 shows an example access technique provided by the secure node. Referring to Figure 5, secure node 72 may be coupled to a network 150 whereas player 52 may not be—giving the secure node great additional flexibility in terms of communicating security related information such as audit trails, compensation related information such as payment requests or orders, etc. This connection of secure node 72 to network 150 (which may be replaced in any given application by some other communications technique such as insertion of a replaceable memory cartridge) allows secure node 72 to receive and securely maintain rights management control information such as an additional container 206' containing an additional control set 204'. Secure node 72 may use control set 204' in addition or in lieu of a control set 204 stored on disk 100. Secure node 72 may also maintain a secure cryptographic key store 212 that may provide cryptographic keys to be used in lieu of or in addition to any keys 208, 210 that may be stored on disk 100.

Because of its increased security and/or technical capabilities, secure node 72 may be able to use controls 222 within control set 204 that player 52 ignores or cannot use—and may be provided with further and/or enhanced rights and/or rights management capabilities based on control set 204' (which the user may, for example, order specially and which may apply to particular properties 200 stored on disk 100 and/or particular sets of disks).

Example Secure Node Access Techniques

The Figure 6 example access technique (which may be performed by platform 60 employing secure node 72, for example) involves, in this particular example, the secure node 72 fetching property identification information 220 from disk 100 (Figure 6, block 502), and then locating applicable control sets and/or rules 204 (which may be stored on disk 100, within secure node 72, within one or more repositories the secure node 72 accesses via network 150, and/or a combination of any or all of these techniques) (Figure 6, block 504). Secure node 72 then loads the necessary decryption keys and uses them to decrypt information as required (Figure 6, block 506). In one example, secure node 72 obtains the necessary keys from secure containers 206 and/or 206'

and maintains them within a protected processing environment such as SPU 164 or a software-emulated protected processing environment without exposing them externally of that environment. In another example, the secure node 72 may load the necessary keys (or a subset of them) into disk drive 82' using a secure key exchange protocol for use by the disk drive in decrypting information much in the same manner as would occur within player 52 in order to maintain complete compatibility in drive hardware.

Secure node 72 may monitor user inputs and perform requested actions based on the particular control set 204, 204'. For example, upon receiving a user request, secure node 72 may query the control set 204, 204' to determine whether it (they) permits the action the user has requested (Figure 6, block 508) and, if permitted, whether conditions for performing the requested operation have been satisfied (Figure 6, block 510). In this example, secure node 72 may effect the operations necessary to satisfy any such required conditions such as by, for example, debiting a user's locally-stored electronic cash wallet, securely requesting an account debit via network 150, obtaining and/or

checking user certificates to ensure that the user is within an appropriate class or is who he or she says he is, etc.—using network 150 as required (Figure 6, block 510). Upon all necessary conditions being satisfied, secure node 72 may perform the requested operation (and/or enable microprocessor 154 to perform the operation) (e.g., to release content) and may then generate secure audit records which can be maintained by the secure node and/or reported at the time or later via network 150 (Figure 6, block 512).

If the requested operation is to release content (e.g., make a copy of the content), platform 60 (or player 52 in the example above) may perform the requested operation based at least in part on the particular controls that enforce rights over the content. For example, the controls may prevent platform 60 from releasing content except to certain types of output devices that cannot be used to copy the content, or they may release the content in a way that discourages copying (e.g., by "fingerprinting" the copy with an embedded designation of who created the copy, by intentionally degrading the released content so that any copies made from it will be inferior, etc.). As one specific example, a

video cassette recorder (not shown) connected to platform 60 may be the output device used to make the copy. Because present generations of analog devices such as video cassette recorders are incapable of making multigenerational copies without significant loss in quality, the content provider may provide controls that permit content to be copied by such analog devices but not by digital devices (which can make an unlimited number of copies without quality loss). For example, platform 60 may, under control of digital controls maintained by secure node 72, release content to the video cassette recorder only after the video cassette recorder supplies the platform a digital ID that designates the output device as a video cassette recorder -- and may refuse to provide any output at all unless such a digital ID identifying the output device as a lower quality analog device is provided. Additionally or in the alternative, platform 60 may intentionally degrade the content it supplies to the video cassette recorder to ensure that no acceptable second -generation copies will be made. In another example, more comprehensive rights management information may be encoded by platform 60 in the analog output using watermarking and/or fingerprinting.

Additional Examples of Secure Container Usage

Figure 7 shows a basic example of a DVD medium 700 containing a kind of secure container 701 for use in DVDs in accordance with the present invention. As shown in this example, container 701 ("DigiBox for DVDs") could be a specialized version of a "standard" container tailored especially for use with DVD and/or other media, or it could, alternatively (in an arrangement shown later in Figure 8), be a fully "standard" container. As shown in this example, the specialized container 701 incorporates features that permit it to be used in conjunction with content information, metadata, and cryptographic and/or protection information that is stored on the DVD medium 700 in the same manner as would have been used had container 701 not been present. Thus, specialized container 701 provides compatibility with existing data formats and organizations used on DVDs and/or other media. In addition, a specialized container 701 can be tailored to support only those features necessary for use in support of DVD and/or other media, so that it can be processed and/or manipulated using less powerful or less expensive computing resources than would be required for complete support of a "standard" container object.

In this example, specialized "DVD only" container 701 includes a content object (a property) 703 which includes an "external reference" 705 to video title content 707, which may be stored on the DVD and/or other medium in the same manner as would have been used for a medium not including container 701. The video title content 707 may include MPEG-2 and/or AC-3 content 708, as well as scrambling (protection) information 710 and header, structure and/or meta data 711. External reference 705 contains information that "designates" (points to, identifies, and/or describes) specific external processes to be applied/executed in order to usecontent and other information not stored in container 701. In this example, external reference 705 designates video title content 707 and its components 708, 710, and 711. Alternatively, container 701 could store some or all of the video title content in the container itself, using a format and organization that is specific to container 701, rather than the standard format for the DVD and/or other medium 700.

In this example, container 701 also includes a control object (control set) 705 that specifies the rules that apply to use of video title content 707. As indicates by solid arrow 702, control object

705 "applies to" content object (property) 703. As shown in this example, rule 704 can specify that protection processes, for example CGMA or the Matsushita data scrambling process, be applied, and can designate, by external reference 709 contained in rule 704, data scrambling information 710 to be used in carrying out the protection scheme. The shorthand "do CGMA" description in rule 704 indicates that the rule requires that the standard CGMA protection scheme used for content on DVD media is to be used in conjunction with video title content 707, but a different example could specify arbitrary other rules in control object 705 in addition to or instead of the "do CGMA" rule, including other standard DVD protection mechanisms such as the Matsushita data scrambling scheme and/or other rights management mechanisms. External reference 709 permits rule 704 to be based on protection information 710 that is stored and manipulated in the same format and manner as for a DVD medium that does not incorporate container 701 and/or protection information that is meaningful only in the context of processing container 701.

Figure 8 shows a example of a DVD medium 800 containing a "standard" secure container 801. In this example, the

"standard" container provides all of the functionality (if desired) of the Figure 7 container, but may offer additional and/or more extensive rights management and/or content use capabilities than available on the "DVD only" container (e.g., the capacity to operate with various different platforms that use secure nodes).

Figure 9 shows a more complex example of DVD medium 800 having a standard container 901 that provides all of the functionality (if desired) of the Figure 7 container, and that can function in concert with other standard containers 902 located either on the same DVD medium or imported from another remote secure node or network. In this example, standard container 902 may include a supplementary control object 904 which applies to content object 903 of standard container 901. Also in this example, container 902 may provide an additional rule(s) such as, for example, a rule permitting/extending rights to allow up to a certain number (e.g., five) copies of the content available on DVD 900. This arrangement, for example, provides added flexibility in controlling rights management of DVD content between multiple platforms via access through "backchannels" such as via a set-top

box or other hardware having bi-directional communications capabilities with other networks or computers.

Additional Use of A DVD Disk With A Secure Container

Figure 10 illustrates the use of a "new" DVD disk—i.e., one that includes a special DVD secure container in the medium. This container may, in one example, be used or two possible use scenarios: a first situation in which the disk is used on an "old" player (DVD appliance, i.e., a DVD appliance that is not equipped with a secure node to provide rights management in accordance with the present invention; and a second situation in which the disk is used on a "new" player—i.e., a DVD appliance which is equipped with a secure node to provide rights management in accordance with the present invention. In this example, a secure node within the "new" player is configured with the necessary capabilities to process other copy protection information such as, for example, CGMA control codes and data scrambling formats developed and proposed principally by Matsushita.

For example, in the situation shown in Figure 10, the "new" player (which incorporates a secure node in accordance with the

present invention) can recognize the presence of a secure container on the disk. The player may then load the special DVD secure container from the disk into the resident secure node. The secure node opens the container, and implements and/or enforces appropriate rules and usage consequences associated with the content by applying rules from the control object. These rules are extremely flexible. In one example, the rules may, for example, call for use of other protection mechanisms (such as, for example, CGMA protection codes and Matsushita data scrambling) which can be found in the content (or property) portion of the container.

In another example shown in Figure 10, the special DVD container on the disk still allows the "old" player to use to a predetermined limited amount content material which may be used in accordance with conventional practices.

Example Use of A DVD Disk With No Secure Container

Referring now to Figure 11, a further scenario is discussed. Figure 11 illustrates use of an "old" DVD disk with two possible use examples: a first example in which the disk is used on an "old" player—i.e., a DVD appliance that is not equipped with a secure

node for providing rights management in accordance with the present invention—and a second example in which the disk is used on a "new" player (i.e., equipped with a secure node).

In the first case, the "old" player will play the DVD content in a conventional manner. In the second scenario, the "new" player will recognize that the disk does not have a container stored in the medium. It therefore constructs a "virtual" container in resident memory of the appliance. To do this, it constructs a container content object, and also constructs a control object containing the appropriate rules. In one particular example, the only applicable rule it need apply is to "do CGMA" -- but in other examples, additional and/or different rules could be employed. The virtual container is then provided to the secure node within the "new" player for implementing management of use rights in accordance with the present invention. Although not shown in Figures 10 and 11, use of "external references" may also be provided in both virtual and non-virtual containers used in the DVD context.

Example Illustrative Arrangements for Sharing, Brokering and Combining Rights When Operating in At Least Occasionally Connected Scenarios

As described above, the rights management resources of several different devices and/or other systems can be flexibly combined in diverse logical and/or physical relationships, resulting for example in greater and/or differing rights. Such rights management resource combinations can be effected through connection to one or more remote rights authorities. Figures 12-14 show some non-limiting examples of how rights authorities can be used in various contexts.

For example, Figure 12 shows a rights authority broker 1000 connected to a local area network (LAN) 1002. LAN 1002 may connect to wide area network if desired. LAN 1002 provides connectivity between rights authority broker 1000 and any number of appliances such as for example a player 50, a personal computer 60, a CD "tower" type server 1004. In the example shown, LAN 1002 includes a modem pool (and/or network

protocol server, not shown)1006 that allows a laptop computer 1008 to connect to the rights authority broker 1000 via dial-up lines 1010. Alternatively, laptop 1008 could communicate with rights authority broker 1000 using other network and/or communication means, such as the Internet and/or other Wide Area Networks (WANs). A disk player 50A may be coupled to laptop 1008 at the laptop location. In accordance with the teachings above, any or all of devices shown in Figure 12 may include one or more secure nodes 72.

Rights authority broker 1000 may act as an arbiter and/or negotiator of rights. For example, laptop 1008 and associated player 50A may have only limited usage rights when operating in a stand-alone configuration. However, when laptop 1008 connects to rights authority broker 1000 via modem pool 1006 and LAN 1002 and/or by other communication means, the laptop may acquire different and/or expanded rights to use disks 100 (e.g., availability of different content portions, different pricing, different extraction and/or redistribution rights, etc.) Similarly, player 50, equipment 60 and equipment 1004 may be provided with an enhanced and/or different set of disk usage rights through

communication with rights authority broker 1000 over LAN 1002. Communication to and from rights authority broker 1000 is preferably secured through use of containers of the type disclosed in the above-referenced Ginter et al. patent specification.

Figure 13 shows another example use of a rights authority broker 1000 within a home environment. In this example, the laptop computer 1008 may be connected to a home-based rights authority broker 1000 via a high speed serial IEEE 1394 bus and/or by other electronic communication means. In addition, rights authority broker 1000 can connect with any or all of:

- a high definition television 1100,
- one or more loudspeakers 1102 or other audio transducers,
- one or more personal computers 60,
- one or more set-top boxes 1030,
- one or more disk players 50,
- one or more other rights authority brokers 1000A-1000N and

- any other home or consumer equipment or appliances.

Any or all of the equipment listed above may include a secure node 72.

Figure 14 shows another example use of a rights authority broker 1000. In this example, rights authority broker 1000 is connected to a network 1020 such as a LAN, a WAN, the Internet, etc. Network 1020 may provide connectivity between rights authority broker 1000 and any or all of the following equipment:

- one or more connected or occasionally connected disk players 50A, 50B;
- one more networked computers 1022;
- one or more disk reader towers/servers 1004;
- one or more laptop computers 1008;
- one or more Commerce Utility Systems such as a rights and permissions clearinghouse 1024 (see Shear et al., "Trusted Infrastructure..." specification referenced above);

- one or more satellite or other communications uplinks 1026;
- one or more cable television head-ends 1028;
- one or more set-top boxes 1030 (which may be connected to satellite downlinks 1032 and/or disk players 50C);
- one or more personal computer equipment 60;
- one or more portable disk players 1034 (which may be connected through other equipment, directly, and/or occasionally unconnected;
- one or more other rights authority brokers 1000A-1000N; and
- any other desired equipment.

Any or all of the above-mentioned equipment may include one or more secure nodes 72. Rights authority broker 1000 can distribute and/or combine rights for use by any or all of the other components shown in Figure 14. For example, rights authority broker 100 can supply further

F033_WO1997043761_Intertrust Page 127 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1064

secure rights management resources to equipment connected to the broker via network 1020. Multiple equipment shown in Figure 14 can participate and work together in a permanently or temporarily connected network 1020 to share the rights management for a single node. Rights associated with parties and/or groups using and/or controlling such multiple devices and/or other systems can be employed according to underlying rights related rules and controls. As one example, rights available through a corporate executive's laptop computer 1008 might be combined with or substituted for, in some manner, the rights of one or more subordinate corporate employees when their computing or other devices 60 are coupled to network 1020 in a temporary networking relationship. In general, this aspect of the invention allows distributed rights management for DVD or otherwise packaged and delivered content that is protected by a distributed, peer-to-peer rights management. Such a distributed rights management can operate whether the DVD appliance or other content usage device is participating in a permanently or temporarily

connected network 1020, and whether or not the relationships among the devices and/or other systems participating in the distributed rights management arrangement are relating temporarily or have a more permanent operating relationship.

For example, laptop computer 1008 may have different rights available depending on the context in which that device is operating. For example, in a general corporate environment such as shown in Figure 12, the laptop 1008 may have one set of rights. However, the same laptop 1008 may be given a different set of rights when connected to a more general network 1020 in collaboration with specified individuals and/or groups in a corporation. The same laptop 1008 may be given a still different set of rights when connected in a general home environment such as shown by example in Figure 13. The same laptop 1008 could be given still different rights when connected in still other environments such as, by way of non-limiting example:

- a home environment in collaboration with specified individuals and/or groups,

- a retail environment,
- a classroom setting as a student,
- a classroom setting in collaboration with an instructor, in a library environment,
- on a factory floor,
- on a factory floor in collaboration with equipment enabled to perform proprietary functions, and so on.

As one more particular example, coupling a limited resource device arrangement such as a DVD appliance 50 shown in Figure 14 with an inexpensive network computer (NC) 1022 may allow an augmenting (or replacing) of rights management capabilities and/or specific rights of parties and/or devices by permitting rights management to be a result of a combination of some or all of the rights and/or rights management capabilities of the DVD appliance and those of an Network or Personal Computer (NC or PC). Such rights may be further augmented, or otherwise modified or replaced by the availability of rights management capabilities provided by a trusted (secure) remote network rights authority 1000.

The same device, in this example a DVD appliance 50, can thus support different arrays, e.g., degrees, of rights management capabilities, in disconnected and connected arrangements and may further allow available rights to result from the availability of rights and/or rights management capabilities resulting from the combination of rights management devices and/or other systems. This may include one or more combinations of some or all of the rights available through the use of a "less" secure and/or resource poor device or system which are augmented, replaced, or otherwise modified through connection with a device or system that is "more" or "differently" secure and/or resource rich and/or possesses differing or different rights, wherein such connection employs rights and/or management capabilities of either and/or both devices as defined by rights related rules and controls that describe a shared rights management arrangement.

In the latter case, connectivity to a logically and/or physically remote rights management capability can expand (by, for example, increasing the available secure rights management resources) and/or change the character of the rights available to the user of the DVD appliance 50 or a DVD appliance when such

device is coupled with an NC 1022, personal computer 60, and/or remote rights authority 1000. In this rights augmentation scenario, additional content portions may be available, pricing may change, redistribution rights may change (e.g., be expanded), content extraction rights may be increased, etc.

Such "networking rights management" can allow for a combination of rights management resources of plural devices and/or other systems in diverse logical and/or physical relationships, resulting in either greater or differing rights through the enhanced resources provided by connectivity with one or more "remote" rights authorities. Further, while providing for increased and/or differing rights management capability and/or rights, such a connectivity based rights management arrangement can support multi-locational content availability, by providing for seamless integration of remotely available content, for example, content stored in remote, Internet world wide web-based, database supported content repositories, with locally available content on one or more DVD discs 100.

In this instance, a user may experience not only increased or differing rights but may be able to use to both local DVD content

and supplementing content (i.e., content that is more current from a time standpoint, more costly, more diverse, or complementary in some other fashion, etc.). In such an instance, a DVD appliance 50 and/or a user of a DVD appliance (or other device or system connected to such appliance) may have the same rights, differing, and/or different rights applied to locally and remotely available content, and portions of local and remotely available content may themselves be subject to differing or different rights when used by a user and/or appliance. This arrangement can support an overall, profound increase in user content opportunities that are seamlessly integrated and efficiently available to users in a single content searching and/or usage activity.

Such a rights augmenting remote authority 1000 may be directly coupled to a DVD appliance 50 and/or other device by modem (see item 1006 in Figure 12) and/or directly or indirectly coupled through the use of an I/O interface, such as a serial 1394 compatible controller (e.g., by communicating between a 1394 enabled DVD appliance and a local personal computer that functions as a smart synchronous or asynchronous information communications interface to such one or more remote authorities,

including a local PC 60 or NC 1022 that serves as a local rights management authority augmenting and/or supplying the rights management in a DVD appliance) and/or by other digital communication means such as wired and/or wireless network connections.

Rights provided to, purchased, or otherwise acquired by a participant and/or participant DVD appliance 50 or other system can be exchanged among such peer-to-peer relating devices and/or other systems so long as they participate in a permanently or temporarily connected network. 1020. In such a case, rights may be bartered, sold, for currency, otherwise exchanged for value, and/or loaned so long as such devices and/or other systems participate in a rights management system, for example, such as the Virtual Distribution Environment described in Ginter, et al., and employ rights transfer and other rights management capabilities described therein. For example, this aspect of the present invention allows parties to exchange games or movies in which they have purchased rights. Continuing the example, an individual might buy some of a neighbor's usage rights to watch a movie, or transfer to another party credit received from a game

publisher for the successful superdistribution of the game to several acquaintances, where such credit is transferred (exchanged) to a friend to buy some of the friend's rights to play a different game a certain number of times, etc.

Example Virtual Rights Process

Figures 15A-15C shows an example of a process in which rights management components of two or more appliances or other devices establish a virtual rights machine environment associated with an event, operation and/or other action. The process may be initiated in a number of ways. In one example, an appliance user (and/or computer software acting on behalf of a user, group of users, and/or automated system for performing actions) performs an action with a first appliance (e.g., requesting the appliance to display the contents of a secure container, extract a portion of a content element, run a protected computer program, authorize a work flow process step, initiate an operation on a machine tool, play a song, etc.) that results in the activation of a rights management component associated with such first appliance (Figure 15A, block 1500). In other examples, the process may get started in response to an automatically generated event (e.g., based

on a time of day or the like), a random or pseudo-random event, and/or a combination of such events with a user-initiated event.

Once the process begins, a rights management component such as a secure node 72 (for example, an SPE and/or HPE as disclosed in Ginter et al.) determines which rights associated with such first appliance, if any, the user has available with respect to such an action (Figure 15A, block 1502). The rights management component also determines the coordinating and/or cooperating rights associated with such an action available to the user located in whole or in part on other appliances (Figure 15A, block 1502).

In one example, these steps may be performed by securely delivering a request to a rights authority server 1000 that identifies the first appliance, the nature of the proposed action, and other information required or desired by such a rights authority server. Such other information may include, for example:

- the date and time of the request,
- the identity of the user,
- the nature of the network connection,

- the acceptable latency of a response, etc.), and/or
- any other information.

In response to such a request, the rights authority server 1000 may return a list (or other appropriate structure) to the first appliance. This list may, for example, contain the identities of other appliances that do, or may, have rights and/or rights related information relevant to such a proposed action.

In another embodiment, the first appliance may communicate (e.g., poll) a network with requests to other appliances that do, or may, have rights and/or rights related information relevant to such proposed action. Polling may be desirable in cases where the number of appliances is relatively small and/or changes infrequently. Polling may also be useful, for example, in cases where functions of a rights authority server 1000 are distributed across several appliances.

The rights management component associated with the first appliance may then, in this example, check the security level(s) (and/or types) of devices and/or users of other appliances that do, or may, have rights and/or rights related information relevant to

such an action (Figure 15A, block 1506). This step may, for example, be performed in accordance with the security level(s) and/or device type management techniques disclosed in Sibert and Van Wie, and the user rights, secure name services and secure communications techniques disclosed in Ginter et al. Device and/or user security level determination may be based, for example, in whole or in part on device and/or user class.

The rights management component may then make a decision as to whether each of the other appliance devices and/or users have a sufficient security level to cooperate in forming the set of rights and/or rights related information associated with such an action (Figure 15A, block 1508). As each appliance is evaluated, some devices and/or users may have sufficient security levels, and others may not. In this example, if a sufficient security level is not available ("No" exit to decision block 1508), the rights management component may create an audit record (for example, an audit record of the form disclosed in Ginter et al.) (Figure 15A, block 1510), and may end the process (Figure 15A, block 1512). Such audit record may be for either immediate transmission to a responsible authority and/or for local storage and later

transmission, for example. The audit recording step may include, as one example, incrementing a counter that records security level failures (such as the counters associated with summary services in Ginter et al.)

If the devices and/or users provide the requisite security level ("Yes" exit to block 1508), the rights management component in this example may make a further determination based on the device and/or user class(es) and/or other configuration and/or characteristics (Figure 15B, block 1514). Such determination may be based on any number of factors such as for example:

- the device is accessible only through a network interface that has insufficient throughput;
- devices in such a class typically have insufficient resources to perform the action, or relevant portion of the action, at all or with acceptable performance, quality, or other characteristics;

- the user class is inappropriate due to various conditions (e.g., age, security clearance, citizenship, jurisdiction, or any other class-based or other user characteristic); and/or
- other factors.

In one example, decision block 1514 may be performed in part by presenting a choice to the user that the user declines.

If processes within the rights management component determines that such device and/or user class(es) are inappropriate("No" exit to block 1514), the rights management component may write an audit record if required or desired (Figure 15B, block 1516) and the process may end (Figure 15B, block 1518).

If, on the other hand, the rights management component determines that the device and/or user classes are appropriate to proceed ("Yes" exit to block 1514), the rights management component may determine the rights and resources available for performing the action on the first appliance and the other appliances acting together (Figure 15B, block 1520). This step may be performed, for example, using any or all of the method

processing techniques disclosed in Ginter et al. For example, method functions may include event processing capabilities that formulate a request to each relevant appliance that describes, in whole or in part, information related to the action, or portion of the action, potentially suitable for processing, in whole or in part, by such appliance. In this example, such requests, and associated responses, may be managed using the reciprocal method techniques disclosed in Ginter et al. If such interaction requires additional information, or results in ambiguity, the rights management component may, for example, communicate with the user and allow them to make a choice, such as making a choice among various available, functionally different options, and/or the rights management component may engage in a negotiation (for example, using the negotiation techniques disclosed in Ginter et al.) concerning resources, rights and/or rights related information.

The rights management component next determines whether there are sufficient rights and/or resources available to perform the requested action (Figure 15B, decision block 1522). If there are insufficient rights and/or resources available to perform the action ("No" exit to block 1522), the rights management component may

write an audit record (Figure 15B, block 1524), and end the process (Figure 15B, block 1526).

In this example, if sufficient rights and/or resources are available ("Yes" exit to block 1522), the rights management component may make a decision regarding whether additional events should be processed in order to complete the overall action (Figure 15B, block 1528). For example, it may not be desirable to perform only part of the overall action if the necessary rights and/or resources are not available to complete the action. If more events are necessary and/or desired ("Yes" exit to block 1528), the rights management component may repeat blocks 1520, 1522 (and potentially perform blocks 1524, 1526) for each such event.

If sufficient rights and/or resources are available for each of the events ("No" exit to block 1528), the rights management component may, if desired or required, present a user with a choice concerning the available alternatives for rights and/or resources for performing the action (Figure 15B, block 1530). Alternatively and/or in addition, the rights management component may rely on user preference information (and/or defaults) to "automatically" make such a determination on behalf

of the user (for example, based on the overall cost, performance, quality, etc.). In another embodiment, the user's class, or classes, may be used to filter or otherwise aid in selecting among available options. In still another embodiment, artificial intelligence (including, for example, expert systems techniques) may be used to aid in the selection among alternatives. In another embodiment, a mixture of any or all of the foregoing (and/or other) techniques may be used in the selection process.

If there are no acceptable alternatives for rights and/or resources, or because of other negative aspects of the selection process (e.g., a user presses a "Cancel" button in a graphical user interface, a user interaction process exceeds the available time to make such a selection, etc.), ("No" exit to block 1530) the rights management component may write an audit record (Figure 15B, block 1532), and end the process (Figure 15B, block 1534).

On the other hand, if a selection process identifies one or more acceptable sets of rights and/or resources for performing the action and the decision to proceed is affirmative ("Yes" exit to block 1530), the rights management component may perform the proposed action using the first appliance alone or in combination

with any additional appliances (e.g., a rights authority 1000, or any other connected appliance) based on the selected rights and/or resources (Figure 15C, block 1536). Such cooperative implementation of the proposed actions may include for example:

- performing some or all of the action with the first appliance;
- performing some or all of the action with one or more appliances other than the first appliance (e.g., a rights authority 1000 and/or some other appliance);
- performing part of the action with the first appliance and part of the action with one or more other appliances; or
- any combination of these.

For example, this step may be performed using the event processing techniques disclosed in Ginter et al.

As one illustrative example, the first appliance may have all of the resources necessary to perform a particular task (e.g., read certain information from an optical disk), but may lack the rights necessary to do so. In such an instance, the first appliance may

obtain the additional rights it requires to perform the task through the steps described above. In another illustrative example, the first appliance may have all of the rights required to perform a particular task, but it may not have the resources to do so. For example, the first appliance may not have sufficient hardware and/or software resources available to it for accessing, processing or otherwise using information in certain ways. In this example, step 1536 may be performed in whole or in part by some other appliance or appliances based in whole or in part on rights supplied by the first appliance. In still another example, the first appliance may lack both rights and resources necessary to perform a certain action, and may rely on one or more additional appliances to supply such resources and rights.

In this example, the rights management component may, upon completion of the action, write one or more audit records (Figure 15C, block 1538), and the process may end (Figure 15C, block 1540).

* * * * * *

An arrangement has been described which adequately satisfies current entertainment industry requirements for a low cost, mass-produceable digital video disk or other high capacity disc copy protection scheme but which also provides enhanced, extensible rights management capabilities for more advanced and/or secure platforms and for cooperative rights management between devices of lessor, greater, and/or differing rights resources. While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the invention.

We Claim:

1. An electronic appliance including:

a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

a secure node coupled to the disk use arrangement, the secure node providing at least one rights management process.

2. An electronic appliance including:

a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

at least one processing arrangement coupled to the disk use arrangement, the processing arrangement selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.

3. A system as in claim 2 wherein the processing arrangement selects a subset of control information used on another appliance and/or class of appliance.

4. A system as in claim 2 wherein the processing arrangement selects different control information from the information selected by another appliance and/or class of appliance.

5. A system as in claim 2 wherein at least some of the control information comprises an analog signal.

6. A system as in claim 2 wherein at least some of the control information comprises digitally encoded information.

7. In an appliance capable of using digital versatile disks, a method including the following steps:

at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.

8. A method as in claim 7 wherein the selecting step includes the step of selecting a subset of control information used on another appliance and/or class of appliance.

9. A method as in claim 7 wherein the selecting step includes the step of selecting, from control information stored on the storage medium, a different set of control information than the control information selected by another appliance and/or class of appliance.

10. An electronic appliance including:

a disk use arrangement for reading information from a digital versatile disk optical storage medium; and

at least one processing arrangement coupled to the disk use arrangement, the processing arrangement protecting information read from the storage medium.

11. An appliance as in claim 10 wherein the processing arrangement includes a rights management arrangement that applies at least one rights management technique to the read information.

12. An appliance as in claim 10 wherein the appliance further includes at least one port compliant at least in part with the IEEE 1394-1995 high speed serial bus standard, and the processing arrangement couples the protected information to the port.

13. In an electronic appliance, a method including the following steps:

reading information from a digital versatile disk optical storage medium; and

protecting the information read from the optical storage medium.

14. A method as in claim 13 wherein the protecting step includes the step of applying at least one rights management technique to the read information.

15. A method as in claim 13 further including the step of sending the protected information to an IEEE 1394 port.

16. An electronic appliance including:

a disk use arrangement for using information stored, or to be stored, on a digital versatile disk optical storage medium; and

at least one protecting arrangement coupled to the disk use arrangement and also coupled to receive at least one analog signal, the protecting arrangement creating protected digital information based at least in part on the analog signal.

17. In an electronic appliance, a method including the following steps:

receiving at least one analog signal; and

creating protected digital content based at least in part on the analog signal for storage on a digital versatile disk.

18. In an electronic appliance, a method including the following steps:

reading at least one analog signal from a digital versatile disk;

creating protected digital content based at least in part on the analog signal; and

outputting the protected digital content.

19. An electronic appliance including:

a disk use arrangement for using information stored, or to be stored, on a digital versatile disk optical storage medium; and

at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement treating the storage medium and/or information obtained from the storage medium differently depending on the geographical and/or jurisdictional context of the appliance.

20. In an electronic appliance, a method including the steps of:

reading information from at least one digital versatile disk; and

performing at least one rights management operation based at least in part on the geographical and/or jurisdictional context of the appliance.

21. An electronic appliance including:

a disk use arrangement for using at least one secure container stored on a digital versatile disk optical storage medium; and

at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement processing the secure container.

22. In an electronic appliance, a method including the following steps:

reading at least one secure container from at least one digital versatile disk; and

performing at least one rights management operation on the secure container.

23. An electronic appliance including:

at least one rights management arrangement for generating and/or modifying at least one secure container for storage onto a digital versatile disk optical storage medium.

24. In an electronic appliance, a method including the step of performing at least one rights management operation on at least one secure container for storage onto a digital versatile disk optical storage medium.

25. A digital versatile disk use system and/or method characterized in that the system and/or method uses at least one secure container.

26. A digital versatile disk use system and/or method characterized in that the system and/or method uses at least one

secure container of the type disclosed in PCT Publication No. WO 96/27155.

27. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and

a secure arrangement that securely manages information on the storage medium such that at least a first portion of the information may be used on at least a first class of appliance while at least a second portion of the information may be used on at least a second class of appliance

28. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium;

using at least a first portion of the information on at least a first class of appliance; and

using at least a second portion of the information on at least a second class of appliance.

29. A system including first and second classes of electronic appliances each including a secure processing arrangement, the first appliance class secure arrangement securely managing and/or using at least a first portion of the information, the second appliance class secure arrangement securely managing and/or using at least a second portion of the information.

30. A system as in claim 29 wherein the first and second information portions are different, and the second appliance class secure arrangement does not use the first information portion.

31. A system as in claim 29 wherein the first appliance class does not use the second information portion.

32. In a system including first and second classes of electronic appliances each including a secure arrangement, a method comprising:

(a) securely managing and/or using at least a first portion of the information with the first appliance class secure arrangement, and

(b) securely managing and/or using at least a second portion of the information with the second appliance class secure arrangement.

33. A method as in claim 32 wherein the first and second information portions are different, and step (b) does not use the first information portion.

34. A method as in claim 32 wherein step (a) does not use the second information portion.

35. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and

a secure arrangement that securely stores and/or transmits information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.

36. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium; and

securely storing and/or transmitting information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.

37. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium;

a cryptographic engine coupled to the disk use arrangement, the engine using at least one cryptographic key; and

a secure arrangement that securely updates and/or replaces at least one cryptographic key used by the cryptographic engine to at least in part modify the scope of information usable by the appliance.

38. A method of operating an electronic appliance including:

writing information onto and/or reading information from a digital versatile disk optical storage medium;

using at least one cryptographic key in conjunction with said information; and

securely updating and/or replacing at least one cryptographic key used by the cryptographic engine to at least in part modify the scope of information useable by the appliance.

39. A digital versatile disk appliance characterized in that at least one cryptographic key used by the appliance is securely updated and/or replaced to at least in part modify the scope of information that can be used by the appliance.

40. An appliance as in claim 39 further characterized in that the key updating and/or replacing is based on class of appliance.

41. An electronic appliance having a class associated therewith, characterized in that at least one cryptographic key set used by the appliance class is selected to help ensure security of information released from at least one digital versatile disk.

42. A digital camera for generating at least one image to be written onto a digital versatile disk optical storage medium, characterized in that the camera includes at least one information protecting arrangement that at least in part protects the image so that the information is persistently protected through subsequent processes such as editing, production, writing onto a digital versatile disk, and/or reading from a digital versatile disk.

43. A digital camera for generating image information that can be written onto a digital versatile disk optical storage medium, a method comprising:

capturing at least one image with a digital camera; and

protecting information provided by the digital camera so that the information is selectively persistently protected through subsequent processes such as distribution, editing and/or production, writing onto the digital versatile disk optical storage medium, and/or reading from the digital versatile disk optical storage medium.

44. In an electronic appliance including a disk use arrangement, a method comprising:

reading information from at least one digital versatile disk optical storage medium; and

persistently protecting at least some of the read information through at least one subsequent editing and/or production process.

45. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium; and

securely managing information on the storage medium, including the step of using at least a first portion of the information on at least a first class of appliance, and using at least a second portion of the information on at least a second class of appliance.

46. A method of providing copy protection and/or use rights management of at least one digital property content and/or secure container to be stored and/or distributed on a digital versatile disk medium, comprising the step(s) of:

providing a set of use control(s) within a cryptographically encapsulated data structure having a predetermined format, the data structure format defining at least one secure software container for providing use rights information for digital property content to be stored on the digital versatile disk medium.

47. A method as in claim 46 further including the step of using at least one digital property content stored on an optical disk in accordance with the use controls, including the step of using a prescribed secure cryptographic key or set of cryptographic keys for using rights information.

48. A method as in claim 46 further including the step of decrypting control rules and/or other selected encrypted

information content encapsulated in the software container using at least one set of cryptographic keys.

49. A method as in claim 46 further including the step of applying decrypted control rules to regulate use in accordance with control information contained within said control rules, so as to facilitate management of a diverse set of use and distribution rights which may be specific to different users and/or optical disk appliances.

50. A method of providing rights management of digital property stored on digital versatile disk according to claim 46 wherein said secure container data structure comprises:

one or more content objects comprising digital property content; and

one or more control objects comprising a set of control rules defining copy protection, use and distribution rights to digital property content stored on the optical disk.

51. A method of providing rights management of digital property stored on a digital versatile disk according to claim 46, wherein a content object further comprises one or more reference pointers to digital property content stored elsewhere on the digital versatile disk.

52. A method of providing rights management of digital property stored on a digital versatile disk according to claim 46, wherein a control object further comprises one or more reference pointers to control information stored elsewhere on the digital versatile disk.

53. A method of providing rights management of digital property stored on digital versatile disk according to claim 46, wherein digital information stored on said optical disk includes one or more metadata blocks comprising further information used in conjunction with the control rules to use digital property content stored elsewhere on the optical disk.

54. A method of providing rights management of digital property stored on digital versatile disk according to claim 46, wherein a metablock may be either of a protected type or of an unprotected type.

55. An arrangement for implementing a rights management system for controlling copy protection, use and/or distribution rights to multi-media digital property content stored or otherwise contained on a digital versatile disk, comprising:

an encrypted data structure defining a secure information container stored on an optical disk medium, the encrypted data structure including and/or referencing at least one content object and at least one control object associated with the content object, said content object comprising digital property content and said control object comprising rules defining use rights to the digital property content.

56. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a content object further comprises one or more reference pointers to digital property content stored elsewhere on the digital versatile disk.

57. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises one or more reference pointers to control information stored elsewhere on the digital versatile disk.

58. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein an control object further comprises information for controlling various operations of an optical disk appliance or computer.

59. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises information for controlling various operations of an optical disk appliance or computer.

60. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises a rule specifying decoding and/or enforcement of CGMA encoded copy protection rules associated with the digital content property.

61. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises a rule specifying at least one content scrambling system compatible encoding/decoding of digital property content.

62. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein said optical disk contains a block of stored information comprising encrypted keys used for decryption of said encrypted data structure.

63. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein said optical disk contains a block of stored information comprising hidden keys used for decryption of said encrypted keys.

64. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a content object further comprises one or more reference pointers to digital property content stored on a separate storage medium.

65. A rights management system for providing copy protection, use and/or distribution rights management for multi-media digital property content stored or otherwise contained on a digital versatile disk for access by an optical disk player device that uses digital property content stored on said optical disk medium, wherein said appliance includes a microprocessor controller for decrypting and using control rules and other selected encrypted information content encapsulated in the secure container by using a prescribed cryptographic key and applying said decrypted control rules to regulate use in accordance with control information contained within said control rules, so as to facilitate management of a diverse set of use and/or distribution rights which may be specific to different users and/or optical disk appliances, the system including:

an optical disk medium having stored thereon an encrypted data structure defining a secure information container, the encrypted data structure comprising and/or referencing at least one content object and at least one control object, said content object comprising digital property content, said control object

comprising rules defining use rights associated with the digital property.

66. A method for providing copy protection, use and distribution rights management of multi-media digital property stored on and/or distributed via digital versatile disk, said optical disk medium having stored thereon an encrypted data structure defining a secure container for housing rights and/or copy protection information pertaining to digital property content stored on the optical disk, wherein an optical disk player appliance for using digital property content stored on an optical disk must utilize a prescribed secure cryptographic key or set of keys to use the secure container, said data structure comprising one or more content objects comprising digital property content and one or more control objects comprising a set of rules defining use rights to digital property, comprising the steps of:

(a) decrypting control rules and other selected encrypted information content encapsulated in the secure container using one or more cryptographic keys; and

(b) applying decrypted control rules to regulate use and/or distribution of digital property content stored on the optical disk in accordance with control information contained within the control rules, so as to provide customized use and/or distribution rights that are specific to different optical disk user platforms and/or optical disk appliances.

67. A rights management system for providing copy protection, use and/or distribution rights management of digital property stored or otherwise contained on a digital versatile disk, comprising:

a secure container means provided on an optical disk medium for cryptographically encapsulating digital property content stored on the optical disk, said container means comprising a content object means for containing digital property content and a control object means for containing control rules for regulating use and/or distribution of said digital property content stored on the optical disk.

68. The rights management system of claim 67 wherein an optical disk player appliance for using information stored on an optical disk comprises a secure node means for using said secure container means provided on an optical disk and implementing said control rules to control operation of said player appliance to regulate use of said digital property content.

69. In a system including plural electronic appliances at least temporarily connected to one another, a rights authority broker that determines what appliances are connected and specifies at least one rights management context depending on said determination.

70. An electronic appliance at least temporarily connected to a rights authority broker, the electronic appliance receiving at least one rights context from the rights authority broker when the device is connected to the rights authority broker.

71. A first electronic appliance at least temporarily connected to a second electronic appliance, the first

electronic appliance selecting between at least first and second rights management contexts depending at least in part on whether the first appliance is connected to the second electronic appliance.

72. In a system including first and second electronic appliances that may be selectively coupled to communicate with one another, an arrangement for defining at least one different rights management control based at least in part on whether the first and second electronic appliances are connected.

73. A method of defining at least one rights management context comprising:

(a) determining whether a first electronic appliance is present; and

(b) defining at least one rights management control set based at least in part on the determining step (a).

74. A method of defining at least one rights management context including:

(a) coupling an optical disk storing information to an electronic appliance that can be selectively connected to a rights management broker;

(b) determining whether the electronic appliance is currently coupled to a rights management broker; and

(c) conditioning at least one aspect of use of at least some of the information stored on the optical disk based on whether the electronic appliance is coupled to the rights management broker.

75. A method as in claim 74 wherein step (c) includes the step of obtaining at least one rights management context from the rights management broker.

76. A method as in claim 74 wherein step (c) includes the step of obtaining at least one combined control set from the rights management broker.

77. A method of defining at least one rights management context including:

(a) coupling an optical disk storing information to an electronic appliance;

(b) using at least some of the information stored on the optical disk based on a first rights management context;

(c) coupling the electronic appliance to a rights management broker; and

(d) concurrently with step (c), using at least some of the information stored on the optical disk based on a second rights management context different from the first rights management context

78. An electronic appliance include a secure node and an optical disk reader, the electronic appliance applying different rights management contexts to protected information stored on an optical disk coupled to the optical disk reader depending at least in part on whether the electronic appliance is coupled to at least one additional secure node.

79. An electronic appliance including:

an optical disk reading and/or writing arrangement;

a secure node coupled to the optical disk reading and/or writing arrangement, the secure node performing at least one rights management related function with respect to at least some information read by the optical disk reading and/or writing arrangement; and

at least one serial bus port coupled to the secure node, the serial bus port for providing any or all of the functions, structures, protocols and/or methods of IEEE 1394-1995.

80. A digital versatile disk appliance including:

means for watermarking content; and

serial bus means for communicating the watermarked content,

wherein the serial bus means complies with IEEE 1394-1995.

81. An optical disk reading and/or writing device including:

at least one secure node capable of watermarking content and/or processing watermarked content; and

an IEEE 1394-1995 serial bus port.

82. An optical disk using device comprising:

a secure processing unit; and

an IEEE 1394-1995 serial bus port.

83. A device as in claim 82 wherein the secure processing unit includes a channel manager.

84. A device as in claim 82 wherein the secure processing unit executes a rights operating system in whole or in part.

85. A device as in claim 82 wherein the secure processing unit includes a tamper-resistant barrier.

86. A device as in claim 82 wherein the secure processing unit includes an encryption/decryption engine.

87. A rights cooperation method comprising:

(a) connecting an appliance to at least one further appliance;

(b) determining whether the first and/or further appliance and/or user(s) of said first and/or further appliance have appropriate rights and/or resources for performing an action; and

(c) selectively performing the action based at least in part on the determination.

88. A rights cooperation method comprising:

(a) connecting an appliance to at least one further appliance;

(b) determining whether the first and/or further appliance and/or user(s) of said first and/or further appliance have appropriate security for performing an action; and

(c) cooperating between the first and further appliance to selectively perform the action.

89. A cooperative rights management arrangement comprising:

a communications arrangement that allows at least first and second appliances to communicate; and

an arrangement that processes at least one event based at least in part on assessing and/or pooling rights and/or resources between the first and second appliances.

90. An optical disk using system and/or method including at least some of the elements shown in Figure 1A.

91. An optical disk using system and/or method including at least some of the elements shown in Figure 1B.

92. An optical disk using system and/or method including at least some of the elements shown in Figure 1C.

93. An optical disk using system and/or method including at least some of the elements shown in Figure 2A.

94. An optical disk using system and/or method including at least some of the elements shown in Figure 2B.

95. An optical disk using system and/or method including at least some of the elements shown in Figure 3.

96. An optical disk using system and/or method using at least some of the elements shown in Figure 3A.

97. An optical disk using system and/or method using at least some of the control set elements shown in Figure 3B.

98. An optical disk using system and/or method using at least some of the elements shown in Figure 4A.

99. An optical disk using system and/or method using at least some of the elements shown in Figure 4B.

100. An optical disk using system and/or method using at least some of the elements shown in Figure 5.

101. An optical disk using system and/or method using at least some of the elements shown in Figure 6.

102. An optical disk using system and/or method using at least some of the elements shown in Figure 7.

103. An optical disk using system and/or method using at least some of the elements shown in Figure 8.

104. An optical disk using system and/or method using at least some of the elements shown in Figure 9.

105. An optical disk using system and/or method using at least some of the elements shown in Figure 10.

106. An optical disk using system and/or method using at least some of the elements shown in Figure 11.

107. An optical disk using system and/or method including at least some of the elements shown in Figure 12.

108. An optical disk using system and/or method including at least some of the elements shown in Figure 13.

109. An optical disk using system and/or method including at least some of the elements shown in Figure 14.

110. A system and/or method including some or all of the elements shown in Figures 15A-15C.

111. A system and/or method as in any one of the preceding claims, further including, in combination, any element described in any one of the following prior patent specifications:

PCT Publication No. WO 96/27155;

European Patent No. EP 329681;

PCT Application No. PCT/US96/14262;

U.S. Patent Application Serial No. 08/689,606; and/or

U.S. Patent Application Serial No. 08/689,754.

112. A system or process as in any of the preceding claims wherein the phrase "high capacity optical disk" is substituted for "digital versatile disk."

113. A method of clearing or otherwise processing information resulting at least in part from one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

114. A system and/or method for defining rules for use in one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

115. A system and/or method for defining rules and associated content for use in one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

116. A system and/or method for producing an optical disk for use with one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

117. A system and/or method for clearing audit information from one or more appliances and/or methods as defined in any of the preceding claims.

118. In an network including at least one electronic appliance that reads information from and/or writes information to at least one digital versatile disk optical storage medium, and securely communicates information associated with at least one of

payment, auditing, usage, access, controlling and/or otherwise managing content recorded on the storage medium, a method of processing said communicated information including the step of generating at least one payment request and/or order based at least in part on the information.

119. A method of defining at least one control set for storage on a high capacity optical disk that can storage images, audio, text and/or other information, the high capacity optical disk for use by any of plural different electronic appliance types, the method including the step of specifying at least one control that provides different conditions and/or consequences depending upon at least one of the following:

electronic appliance class;

electronic appliance security;

electronic appliance user class;

electronic appliance connectivity;

electronic appliance resources;

electronic appliance access to resources; and

rights management cooperation between plural electronic appliances.

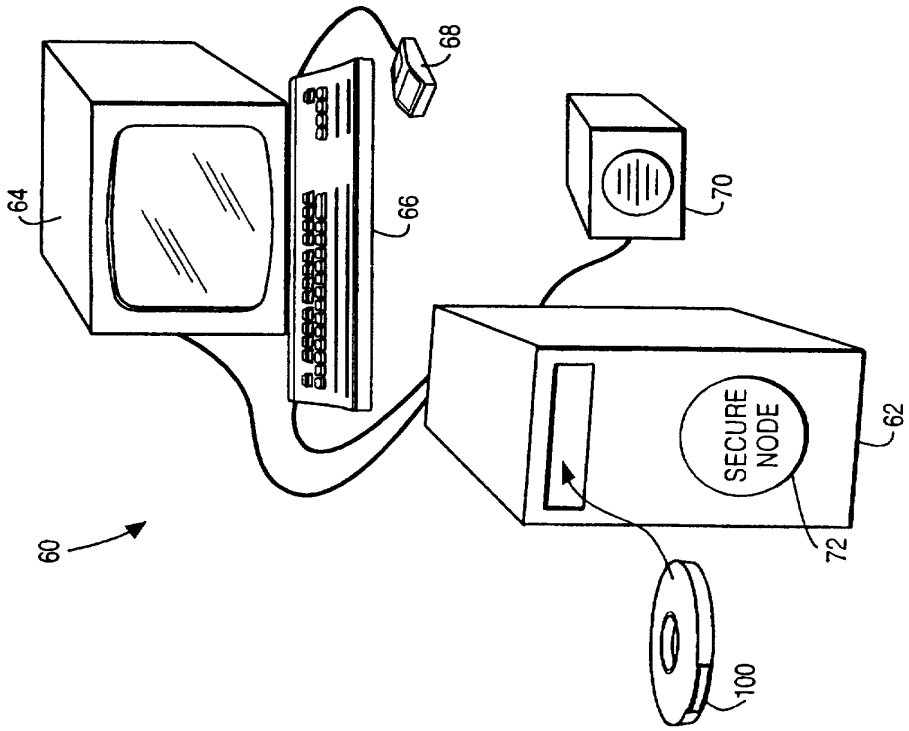


Fig.1B

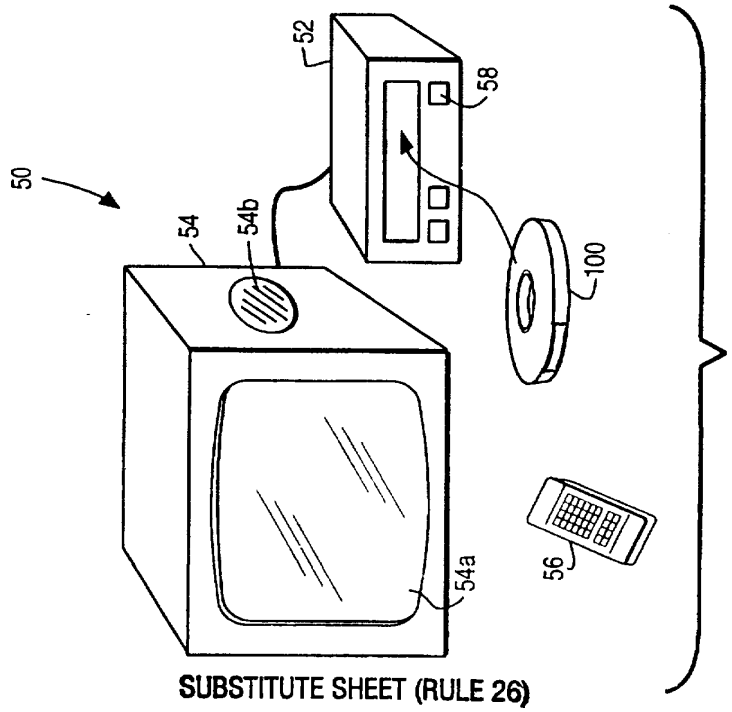


Fig.1A

DISH-Blue Spike 842
Exhibit 1005, Page 1127

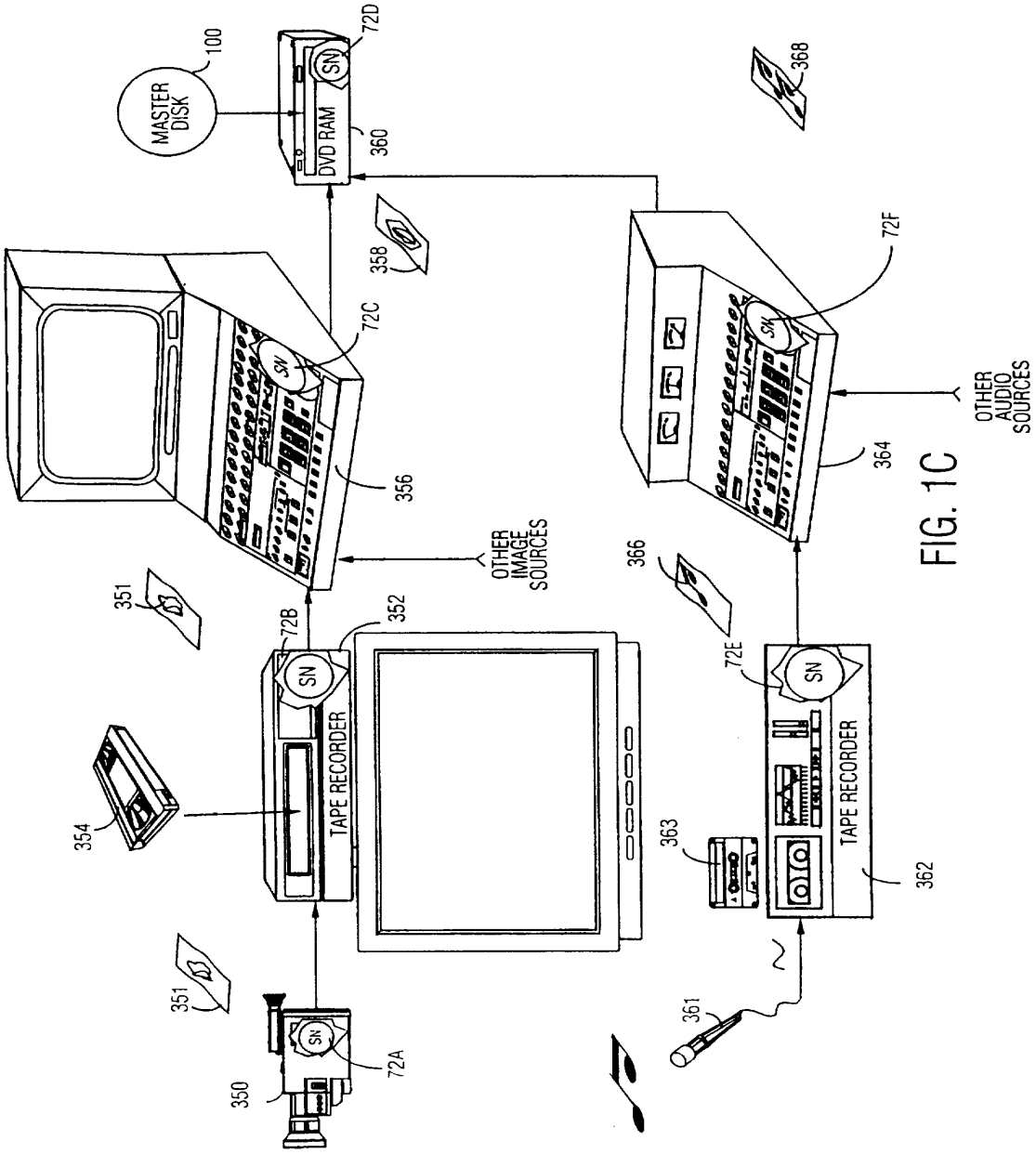


FIG. 1C

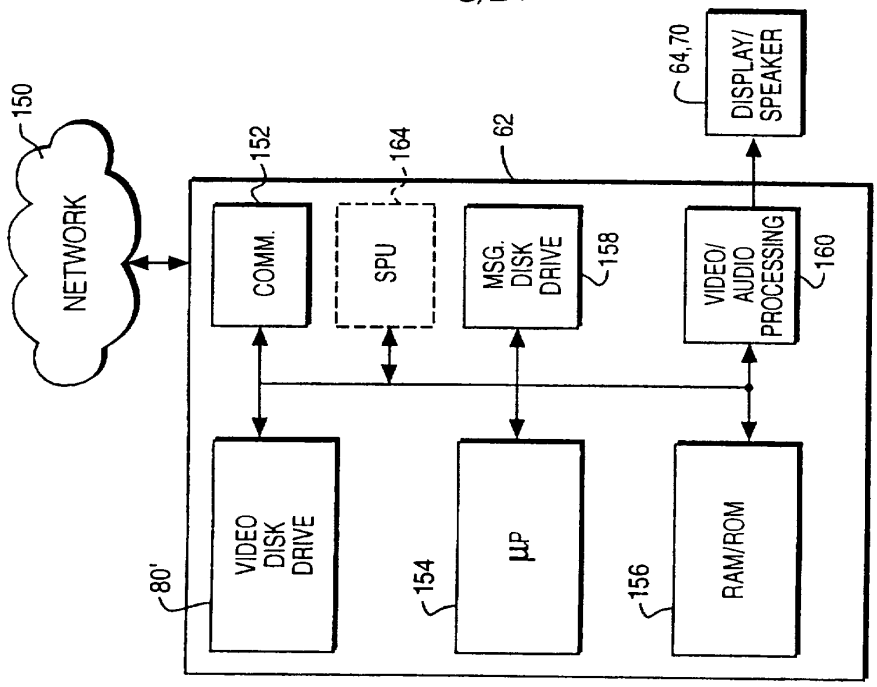


Fig.2B

EXAMPLE SECURE NODE ARCHITECTURE

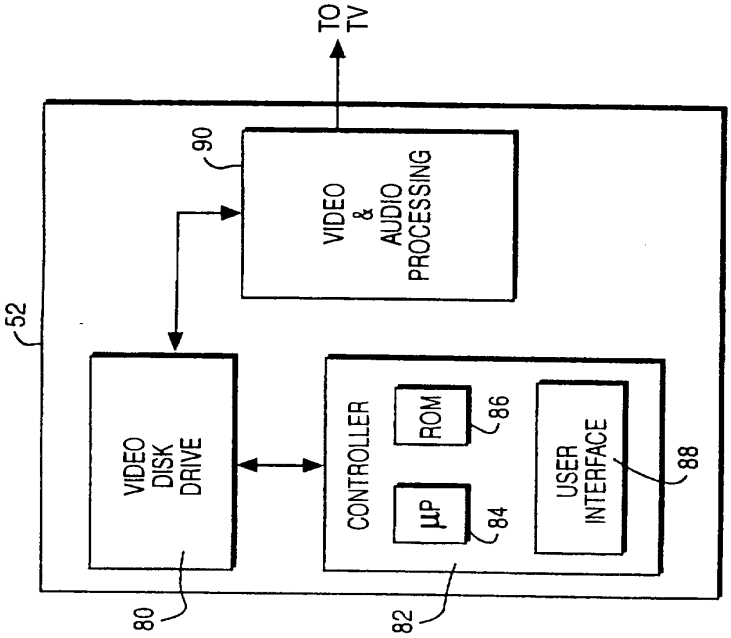


Fig.2A

EXAMPLE PLAYER ARCHITECTURE

DISH-Blue Spike 842
Exhibit 1005, Page 1128

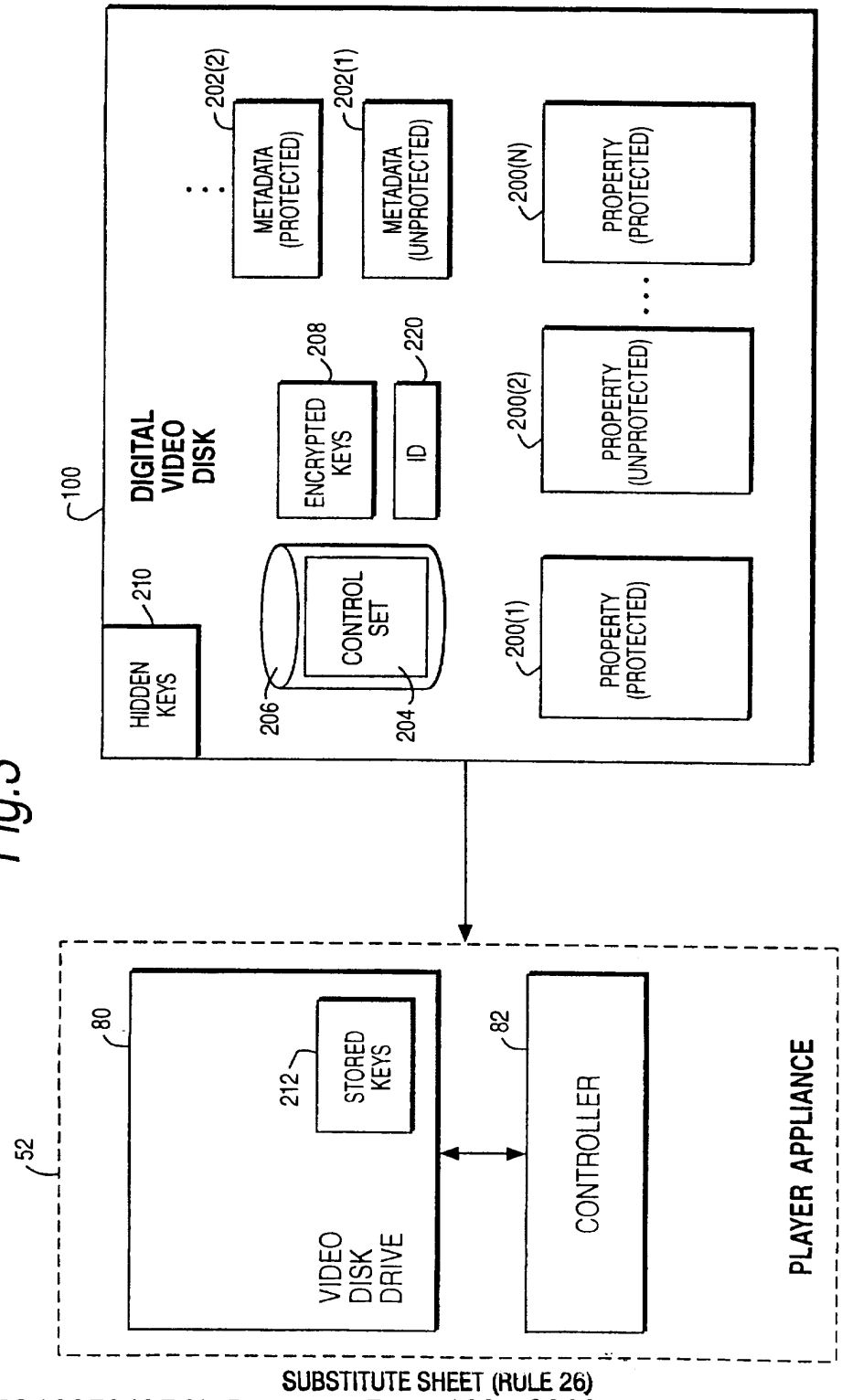


Fig.3

F033_WO1997043761_Intertrust Page 192 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1129

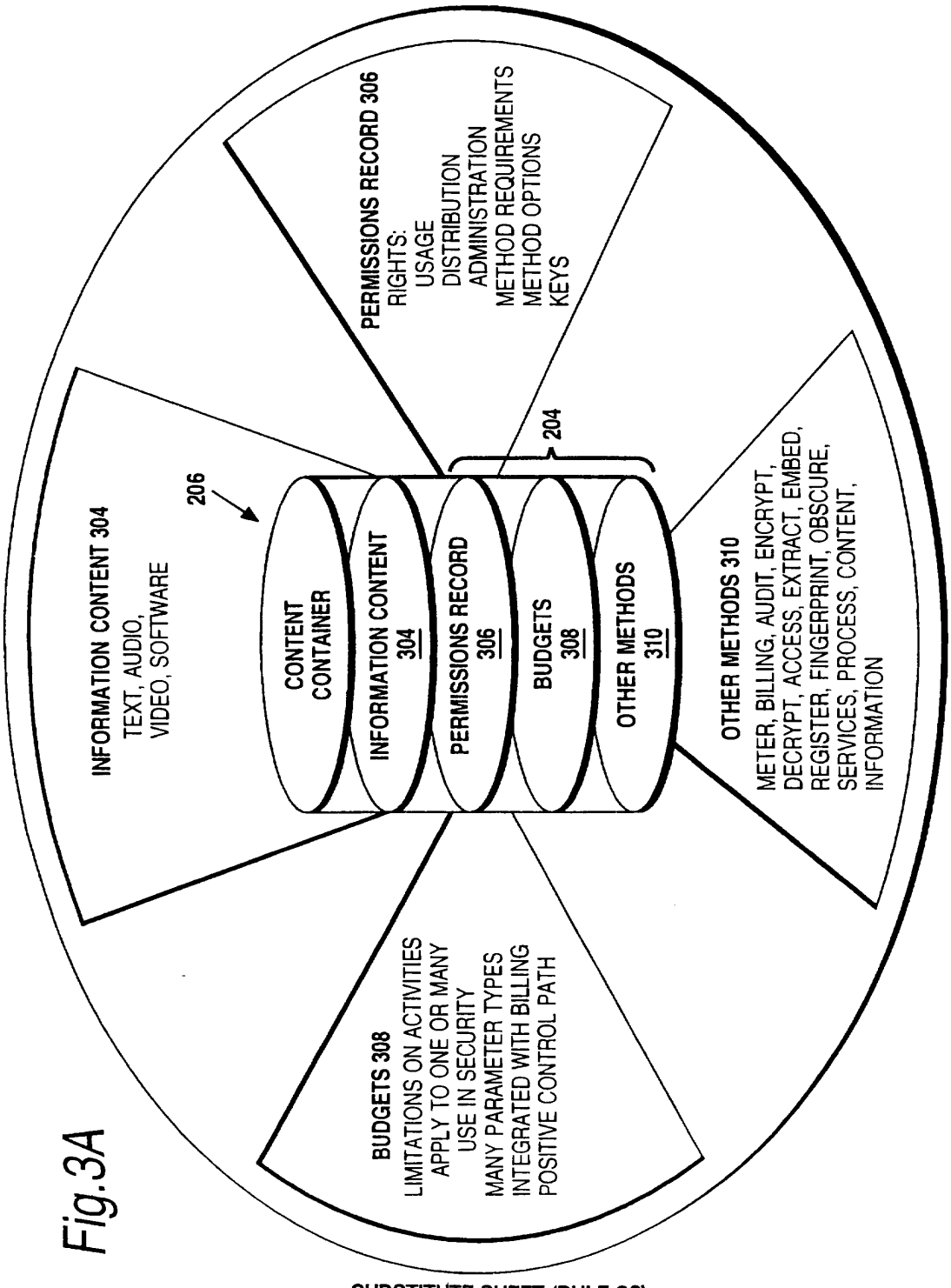


Fig.3A

DISH-Blue Spike 842
Exhibit 1005, Page 1130

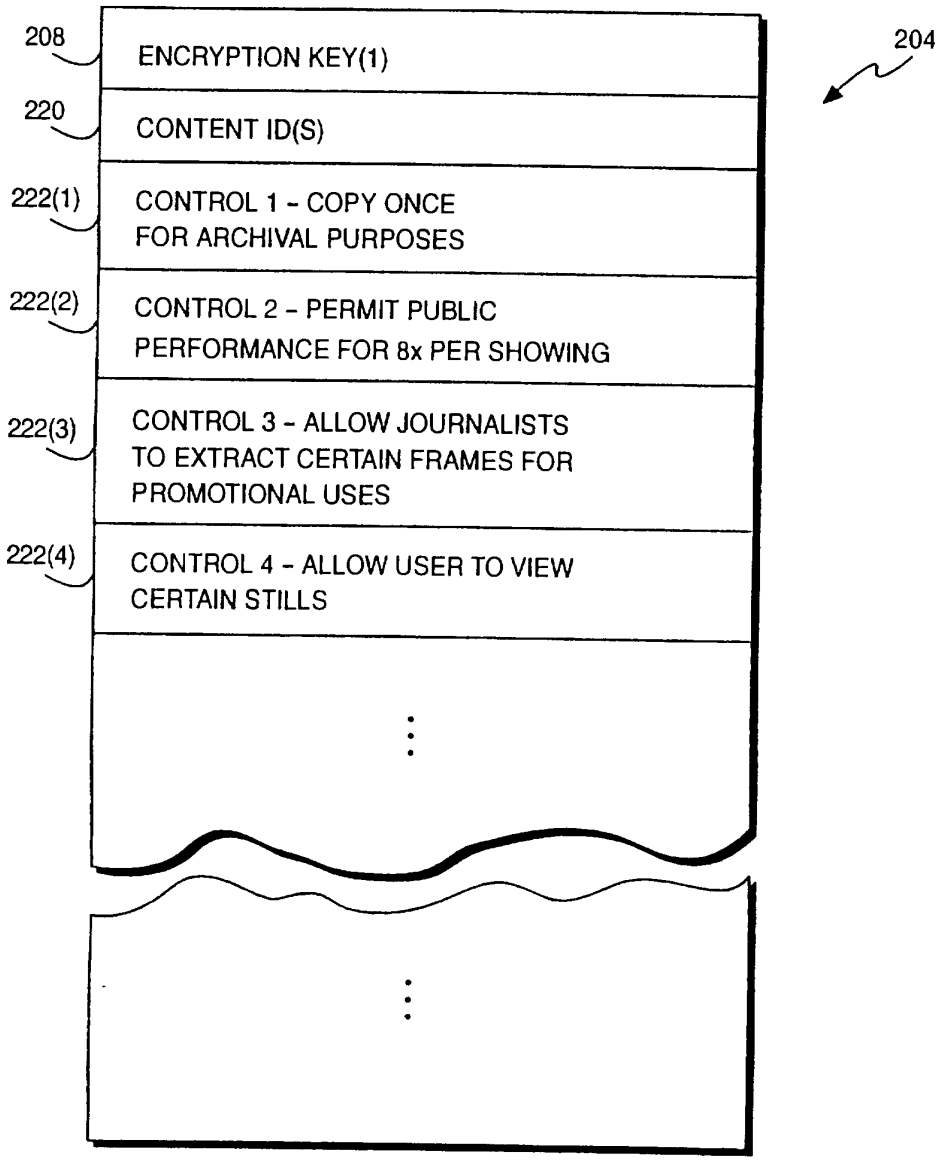


Fig.3B

EXAMPLE CONTROL SET

Fig.4A
EXAMPLE PLAYER STEPS

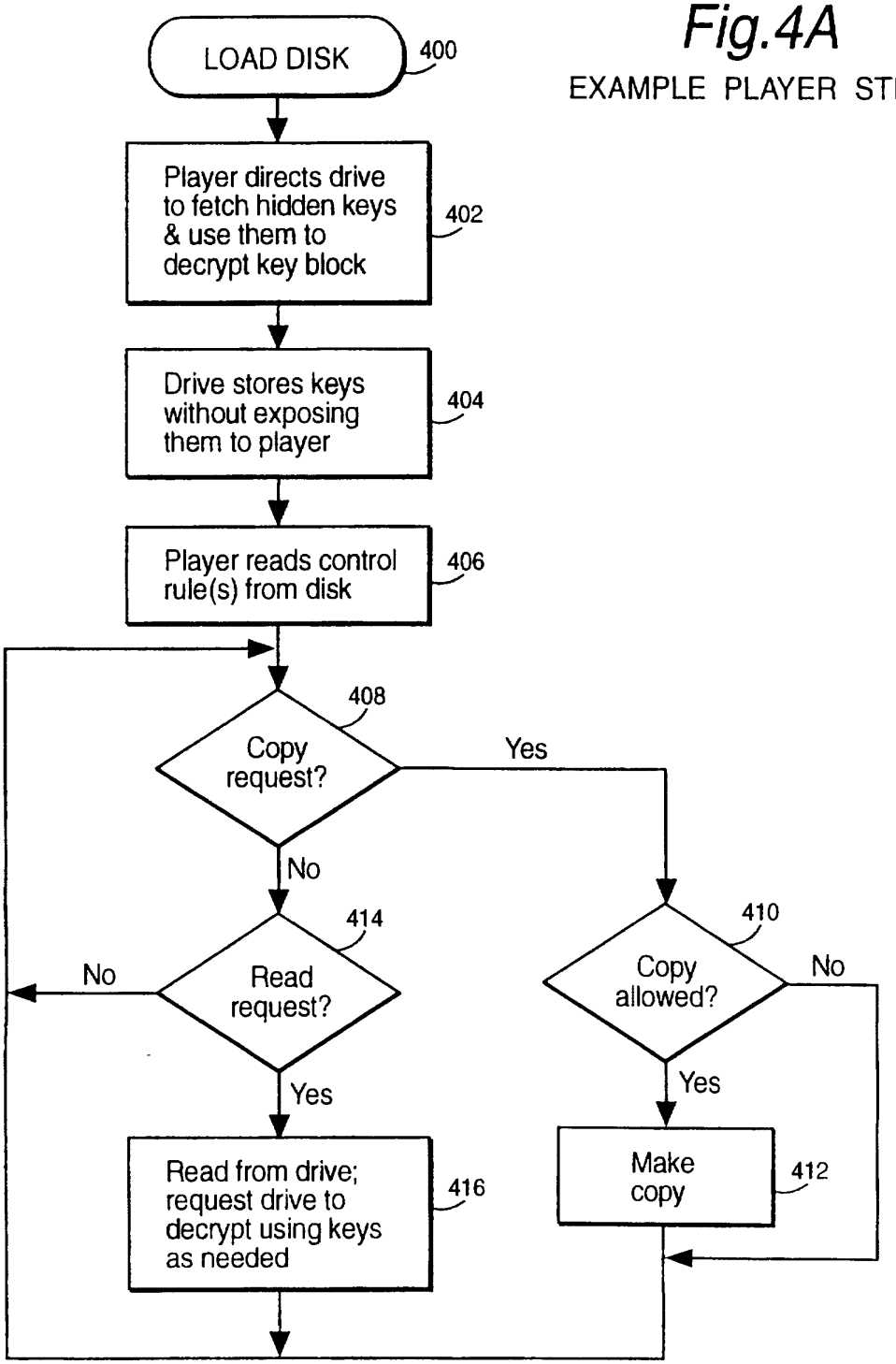
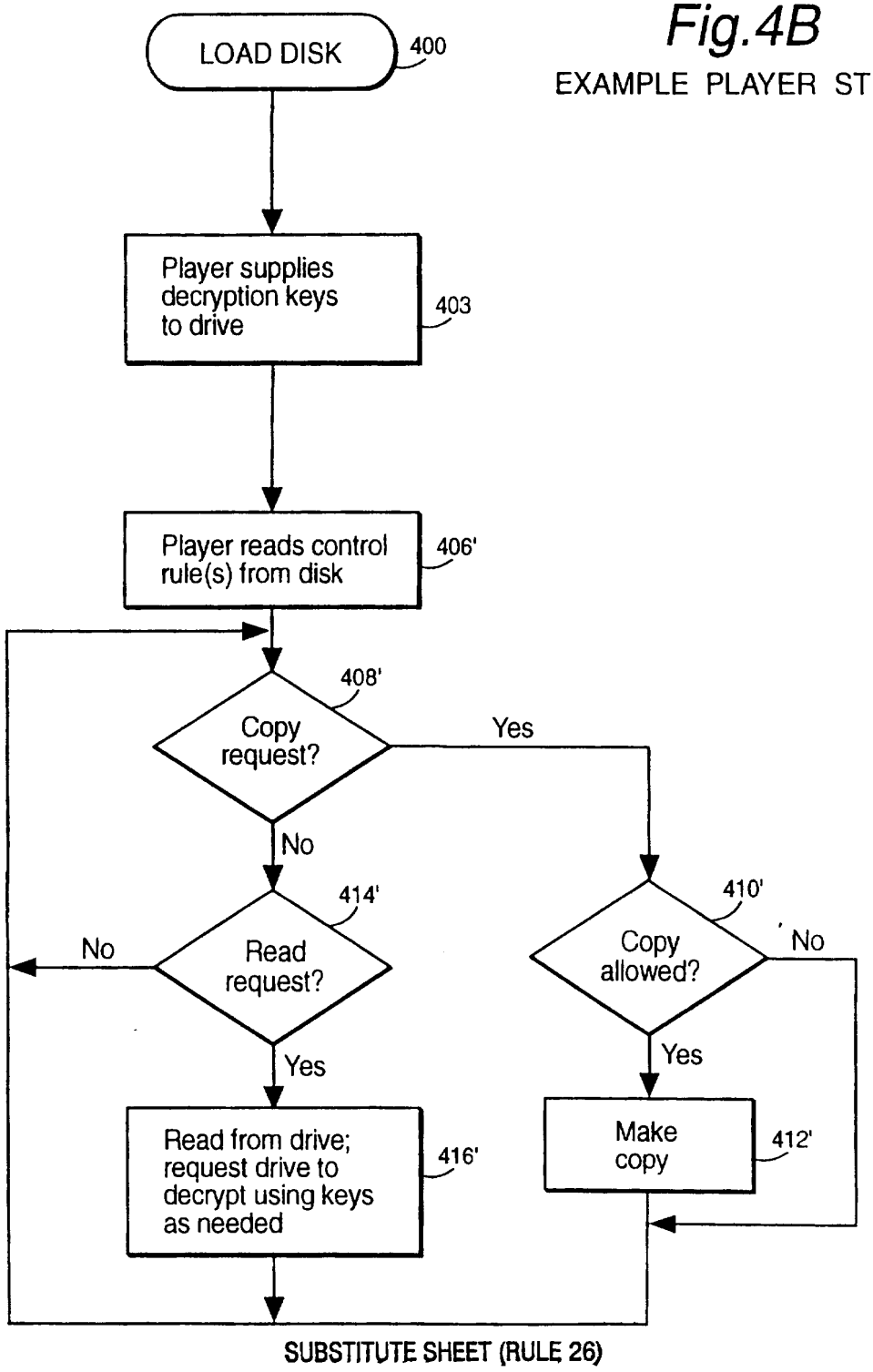


Fig.4B
EXAMPLE PLAYER STEPS



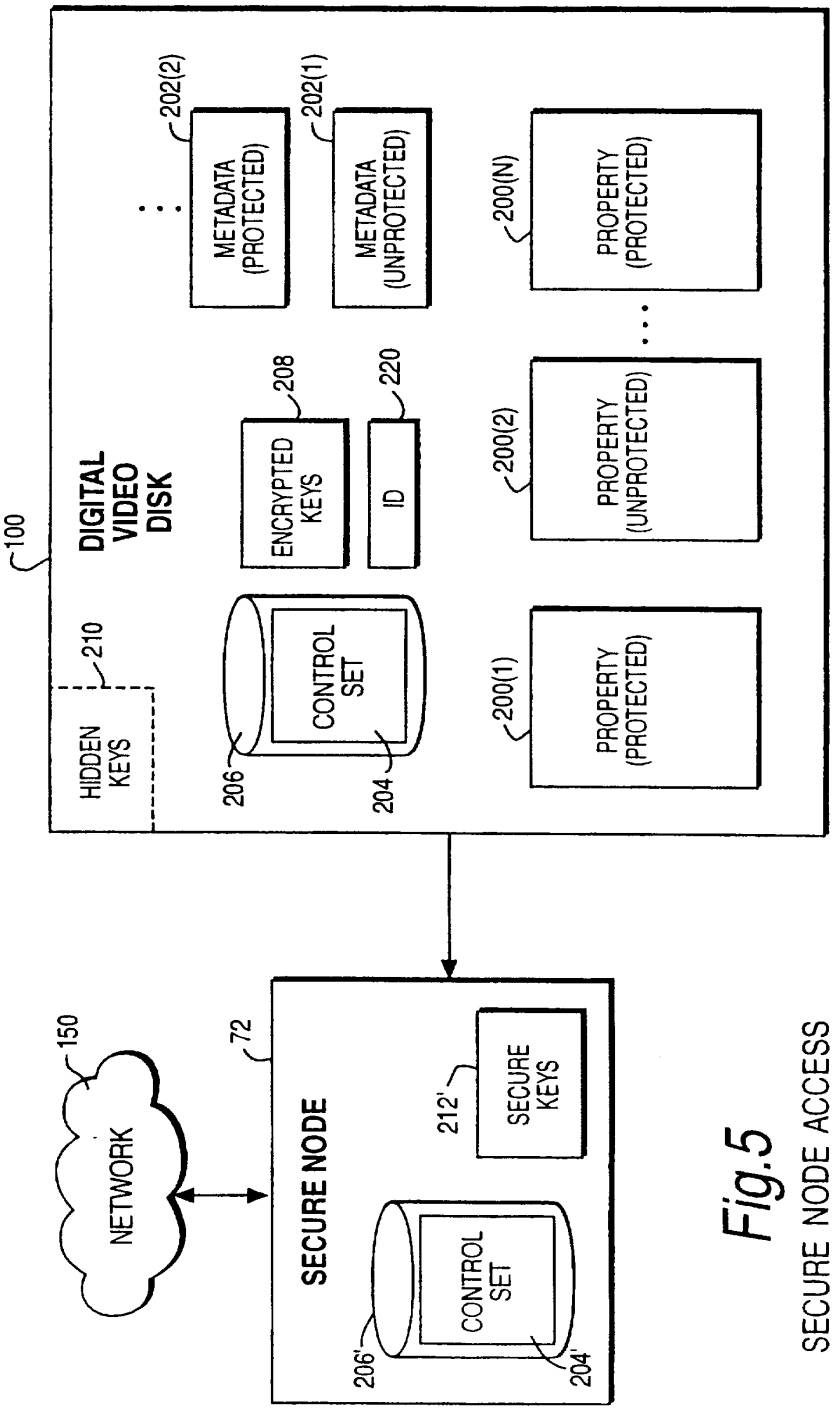


Fig.5
SECURE NODE ACCESS

F033_WO1997043761_Intertrust Page 197 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1134

Fig.6

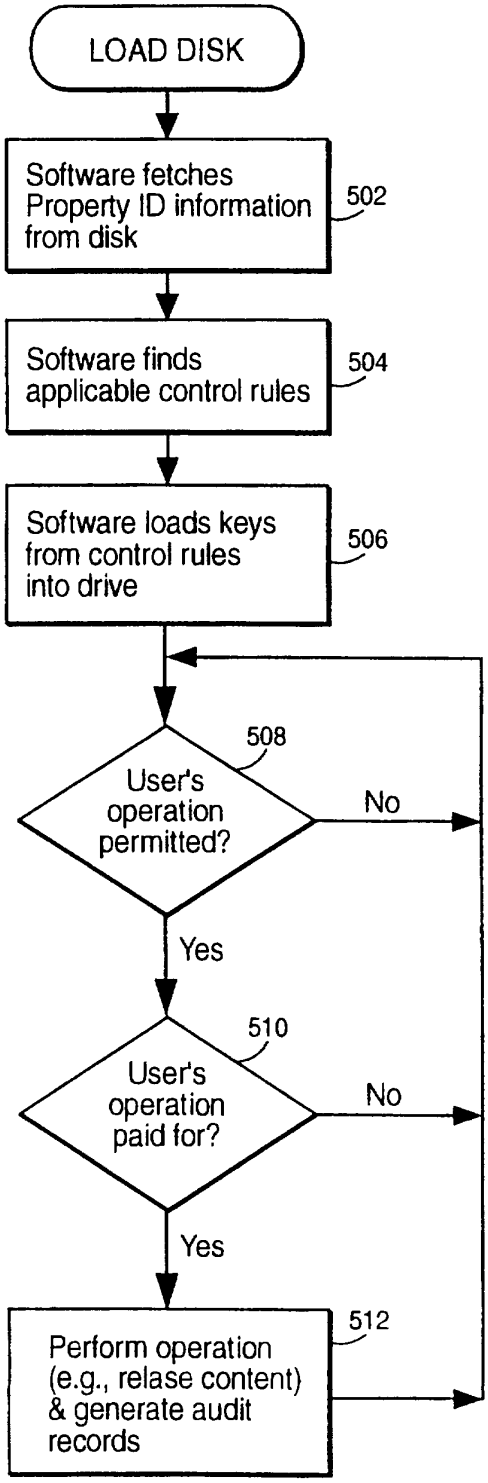

LOAD DISK
Software fetches Property ID information from disk
502
Software finds applicable control rules
504
Software loads keys from control rules into drive
506
508
User's operation permitted?
No
Yes
510
User's operation paid for?
No
Yes
512
Perform operation (e.g., relase content) & generate audit records

FIG. 7

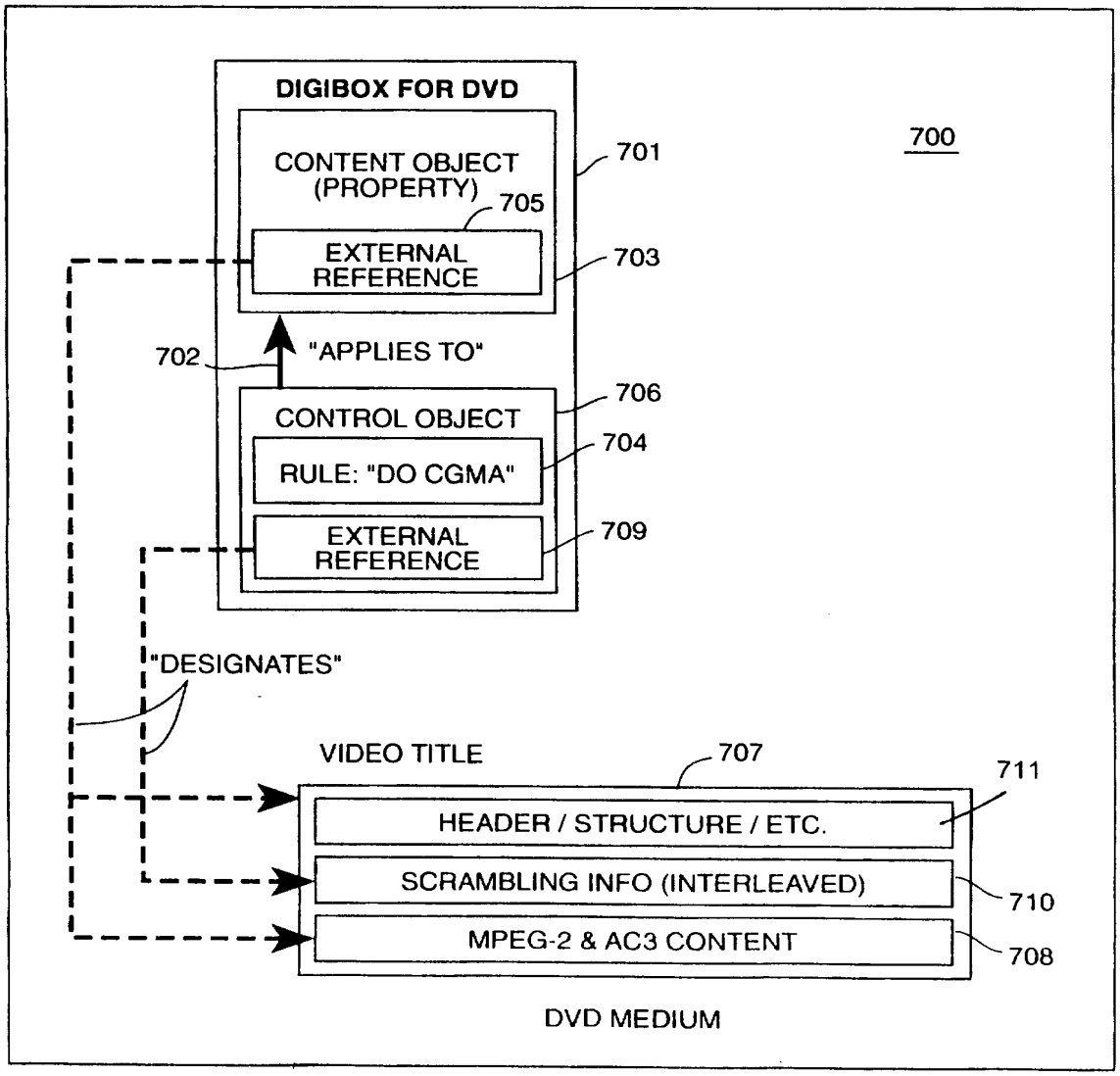
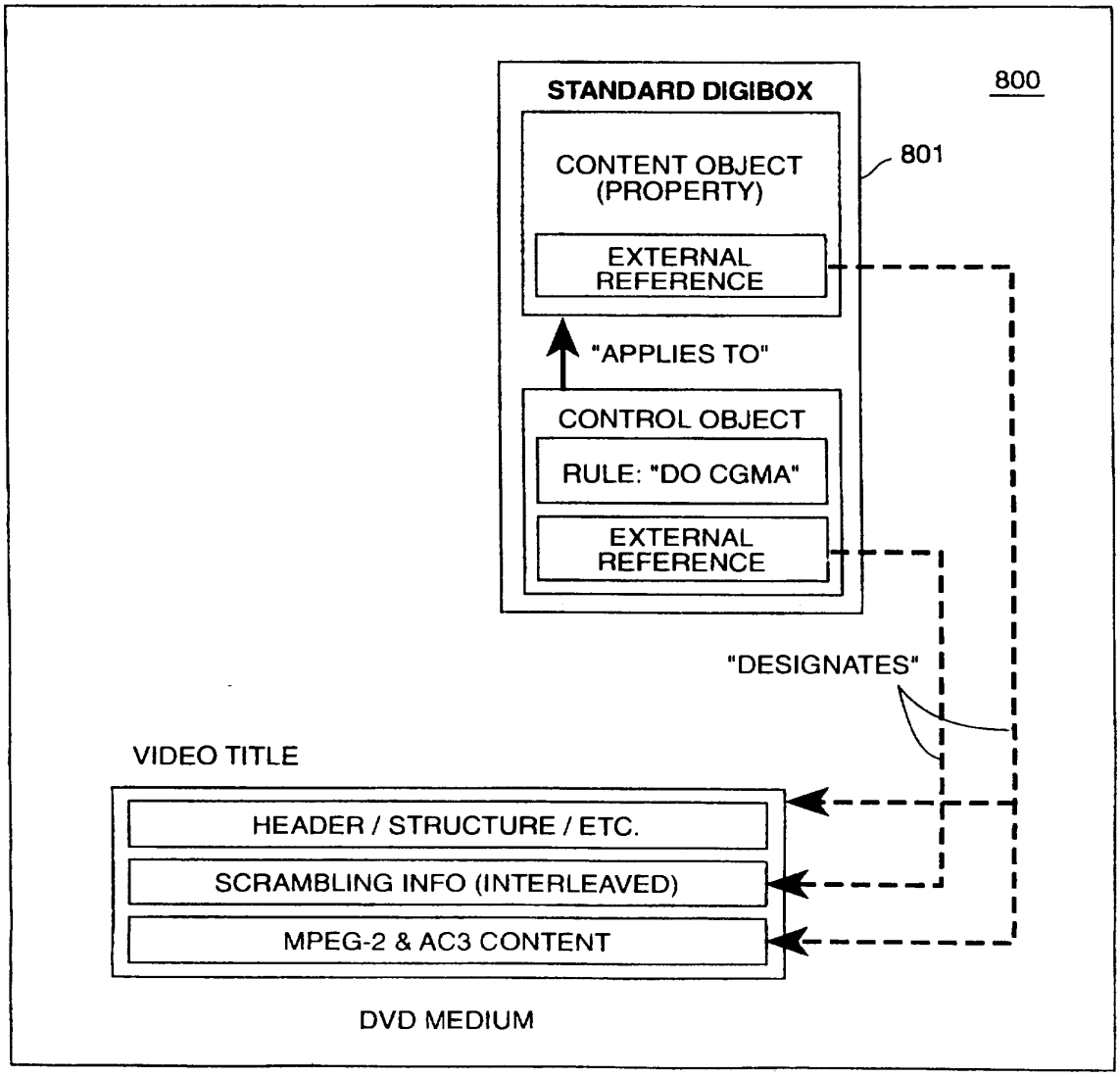

DIGIBOX FOR DVD
CONTENT OBJECT (PROPERTY)
EXTERNAL REFERENCE
"APPLIES TO"
CONTROL OBJECT
RULE: "DO CGMA"
EXTERNAL REFERENCE
"DESIGNATES"
VIDEO TITLE
HEADER / STRUCTURE / ETC.
SCRAMBLING INFO (INTERLEAVED)
MPEG-2 & AC3 CONTENT
DVD MEDIUM
700
701
703
705
702
706
704
709
707
711
710
708

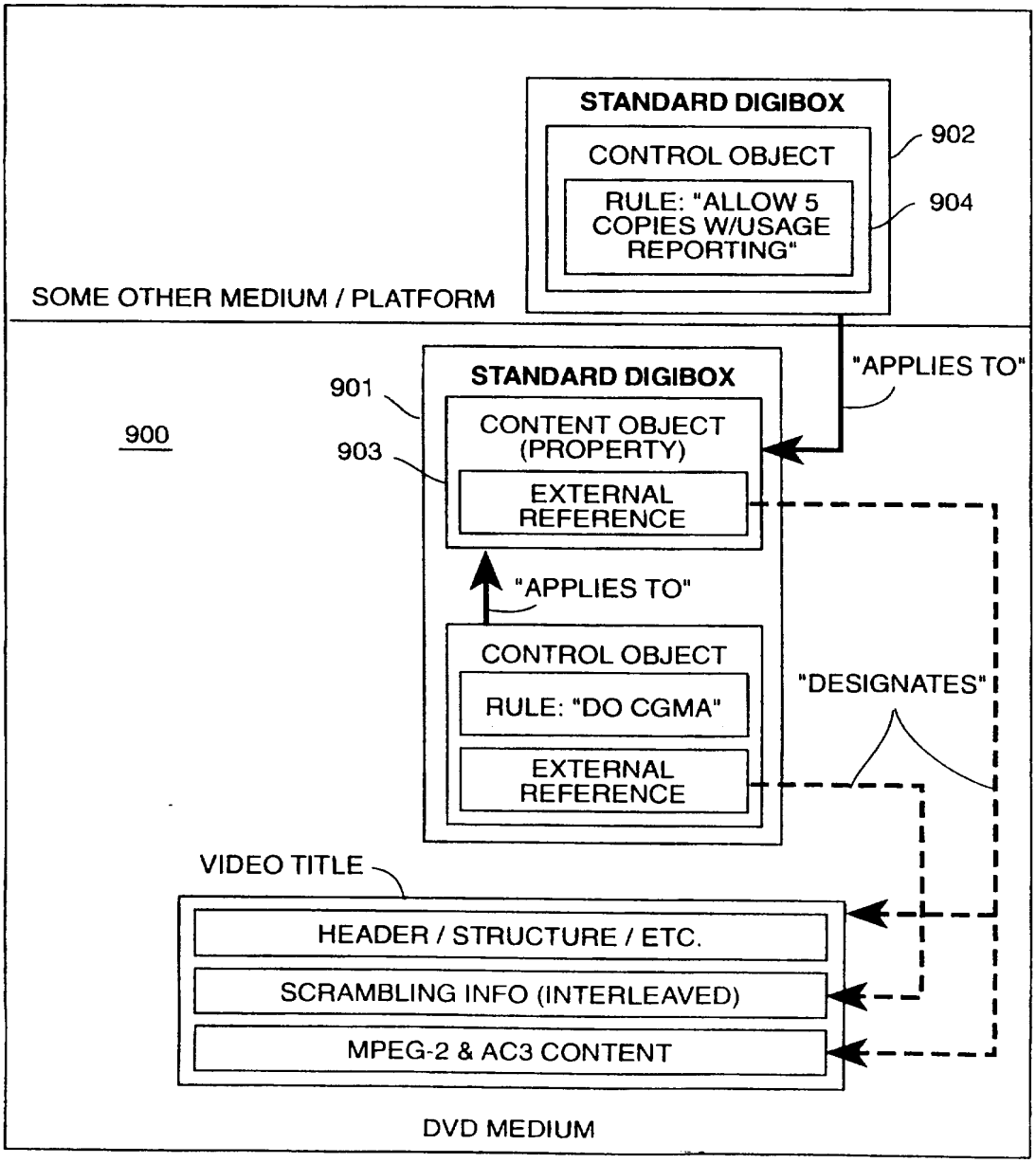
FIG. 8



F033_WO1997043761_Intertrust Page 200 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1137

FIG. 9



F033_WO1997043761_Intertrust Page 201 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1138

FIG. 10

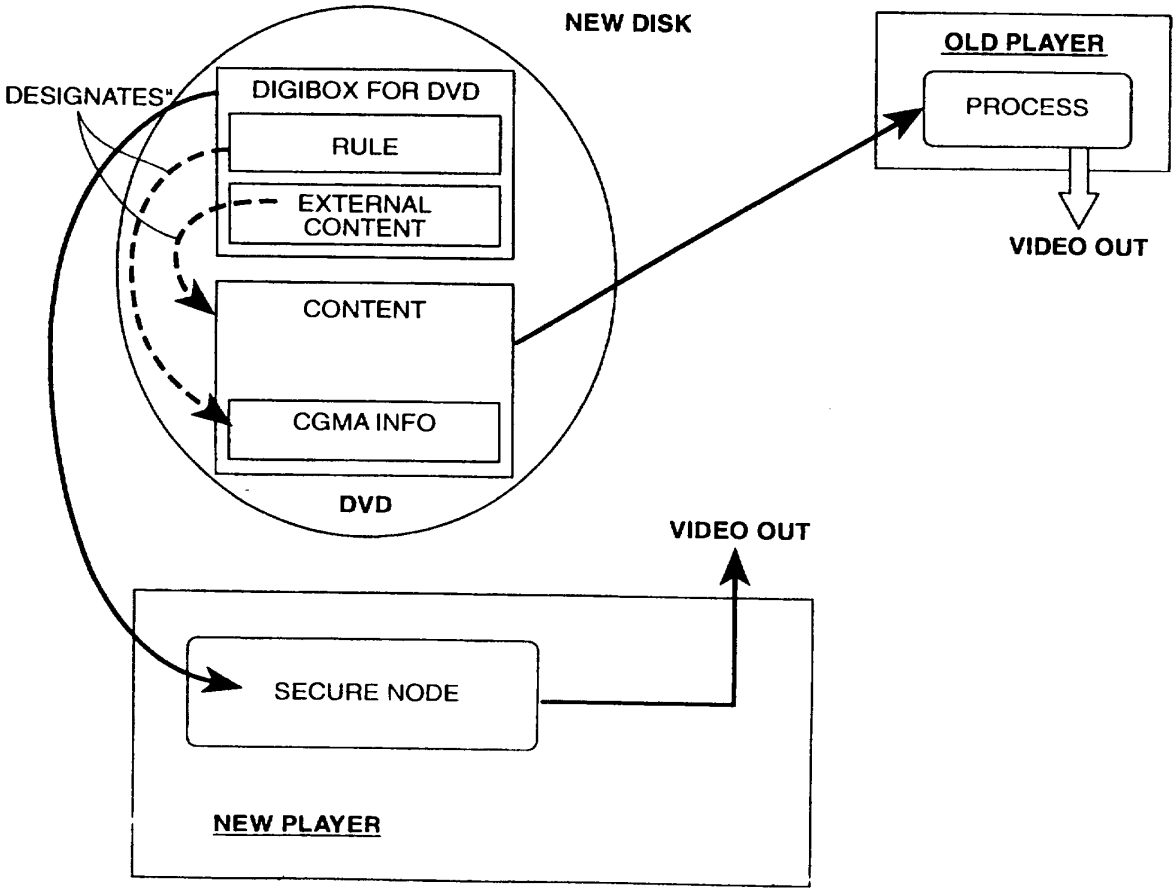
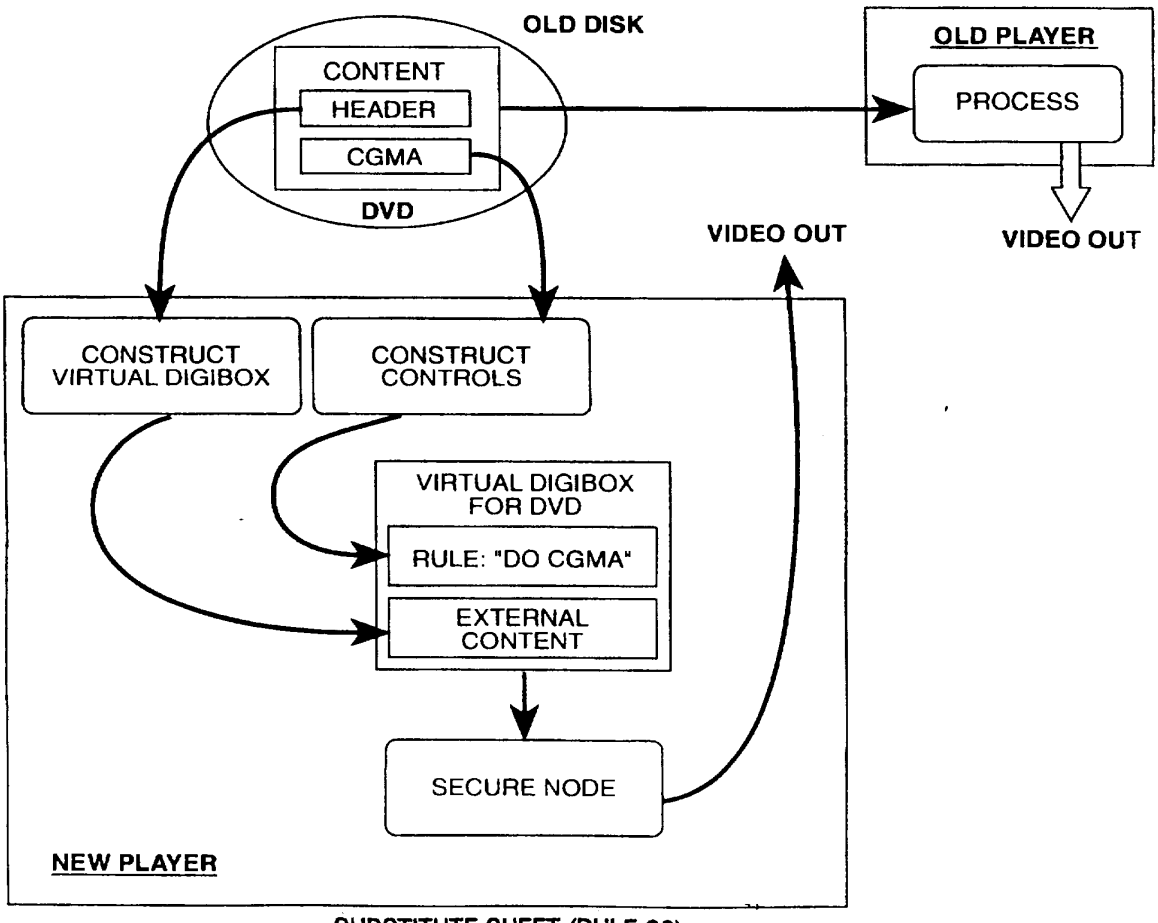

NEW DISK
DESIGNATES"
DIGIBOX FOR DVD
RULE
EXTERNAL CONTENT
CONTENT
CGMA INFO
DVD
OLD PLAYER
PROCESS
VIDEO OUT
VIDEO OUT
SECURE NODE
NEW PLAYER

FIG. 11



F033_WO1997043761_Intertrust Page 203 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1140

DISH-Blue Spike 842
Exhibit 1005, Page 1141

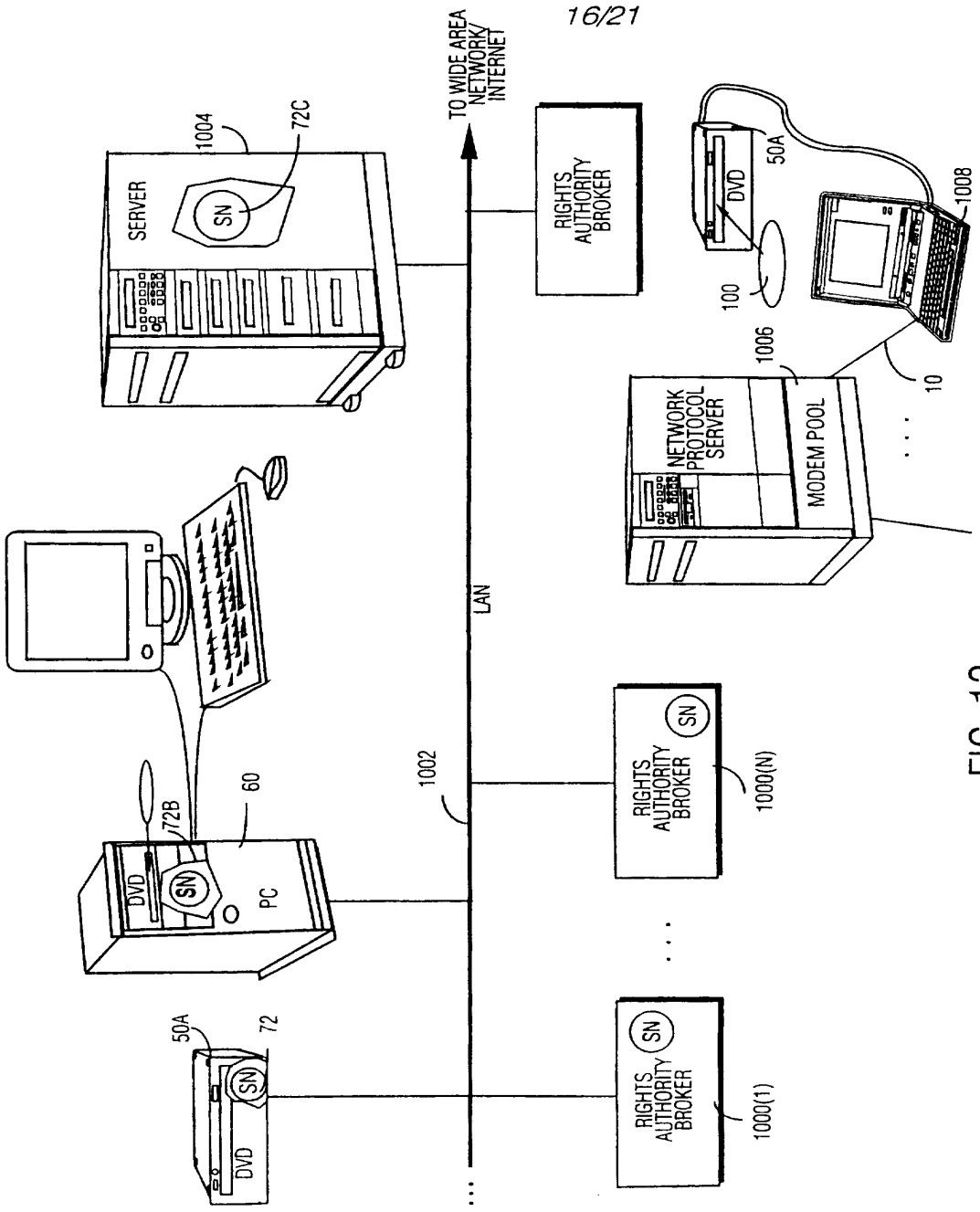


FIG. 12

F033_WO1997043761_Intertrust Page 204 of 209

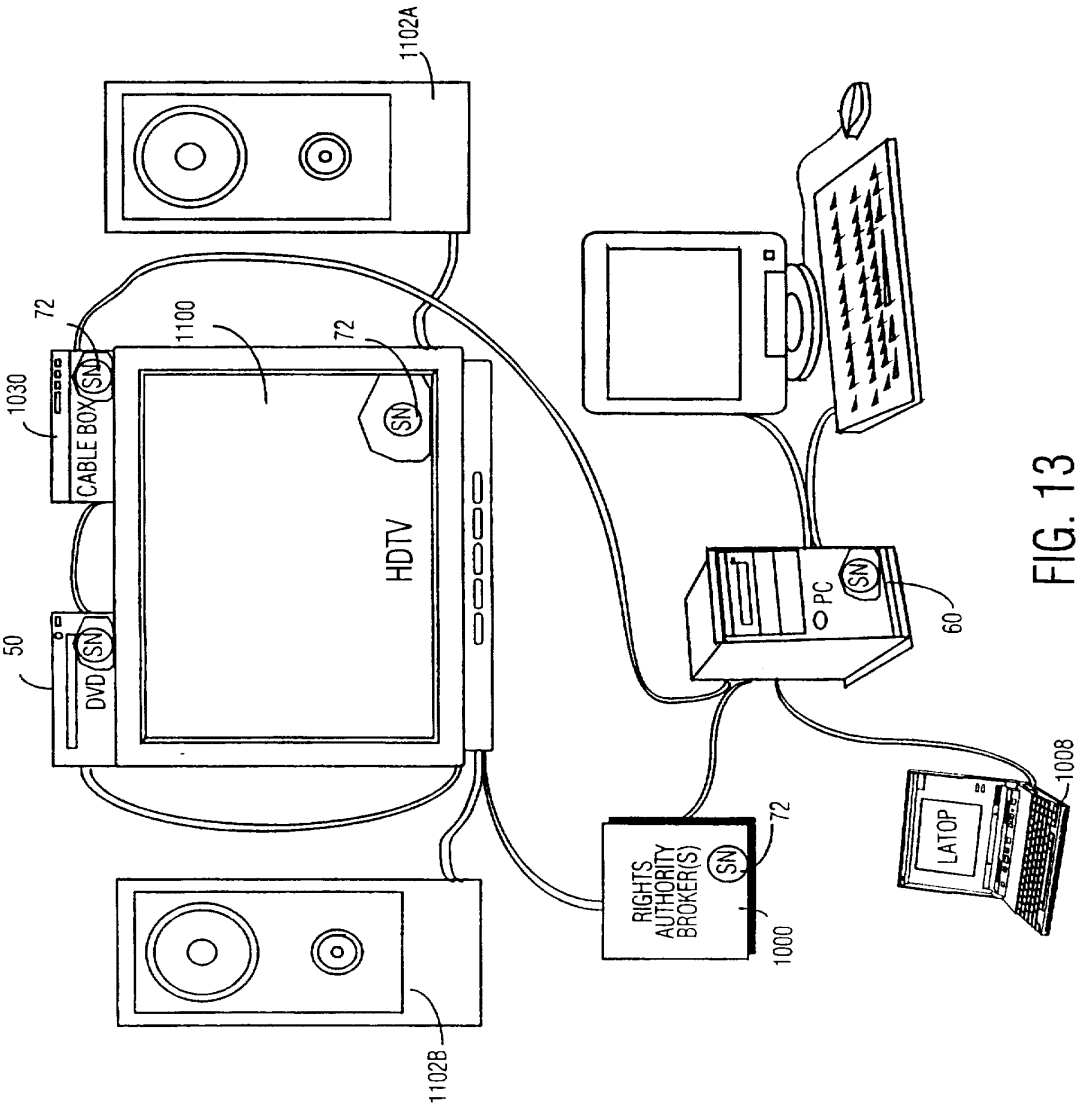


FIG. 13

F033_WO1997043761_Intertrust Page 205 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1142

DISH-Blue Spike 842
Exhibit 1005, Page 1143

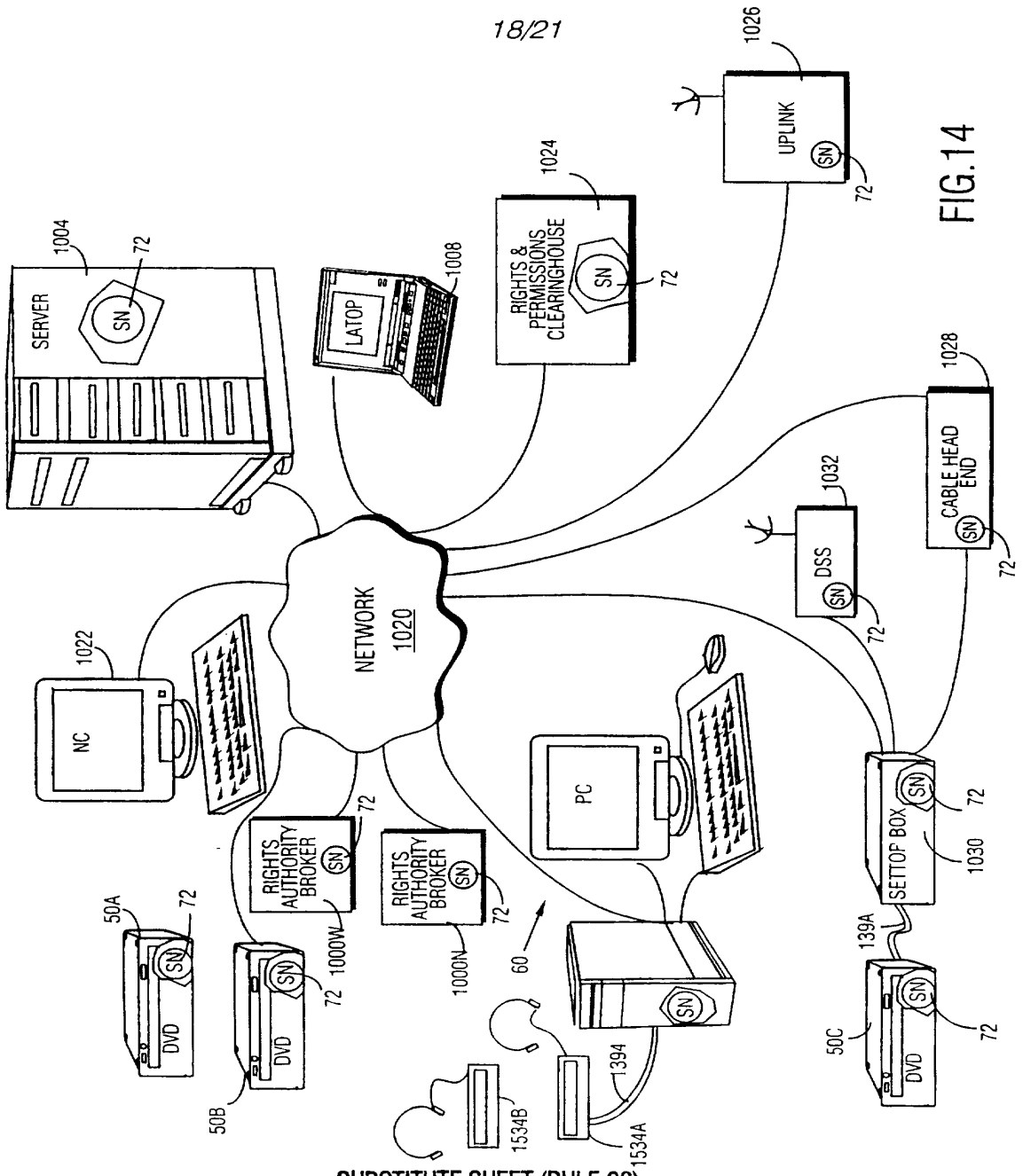


FIG.14

F033_WO1997043761_Intertrust Page 206 of 209

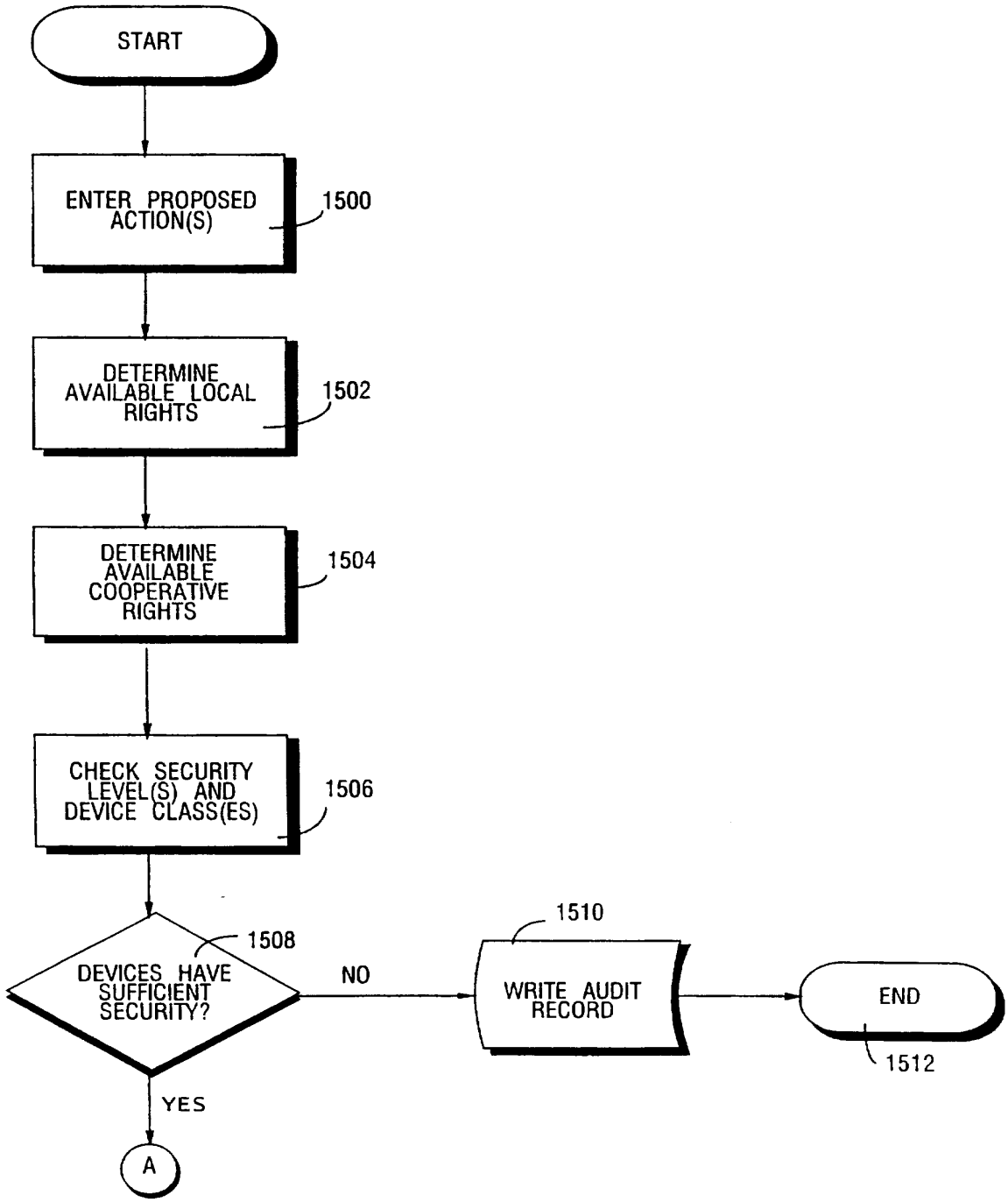


FIG.15A

DISH-Blue Spike 842
Exhibit 1005, Page 1144

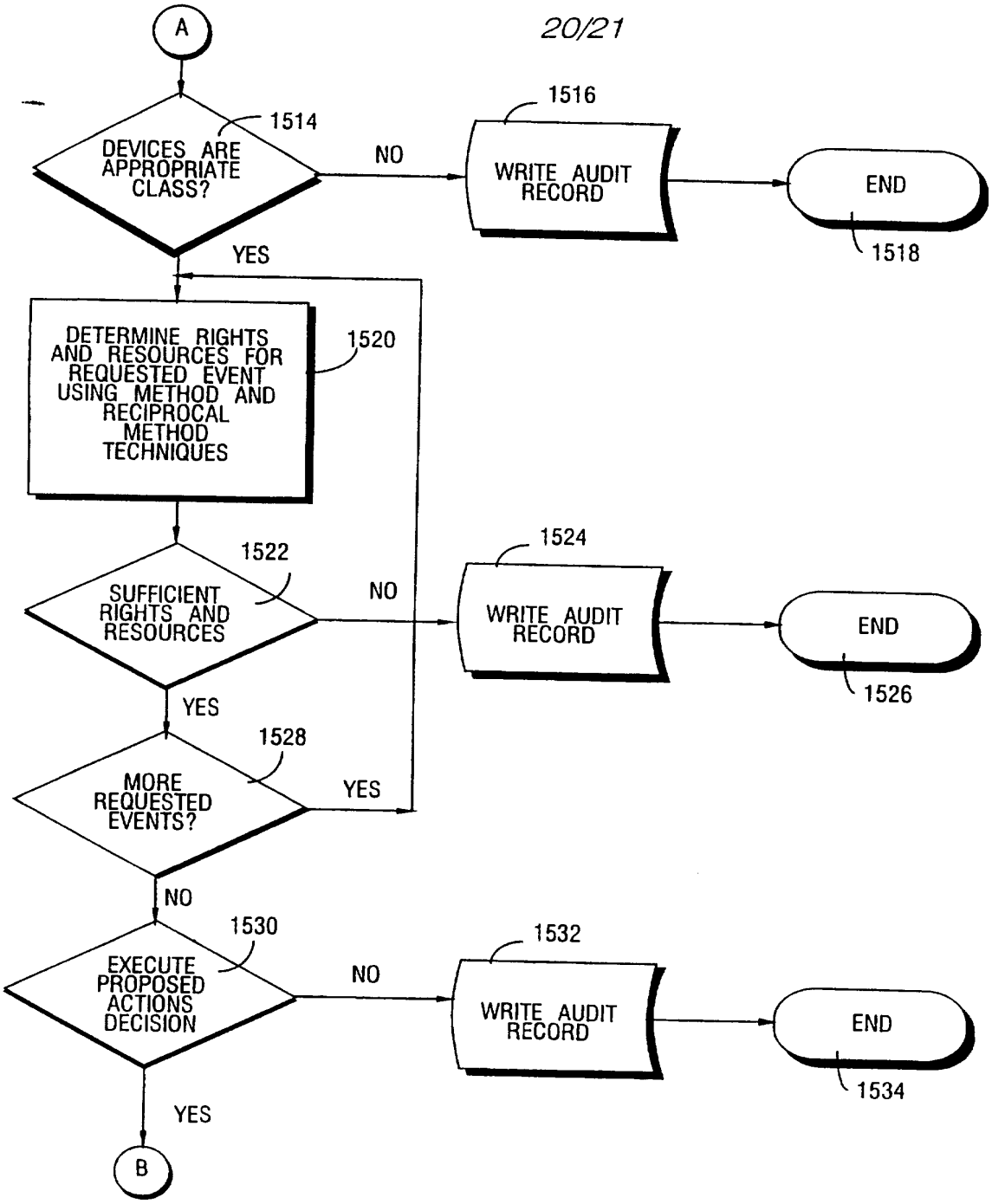
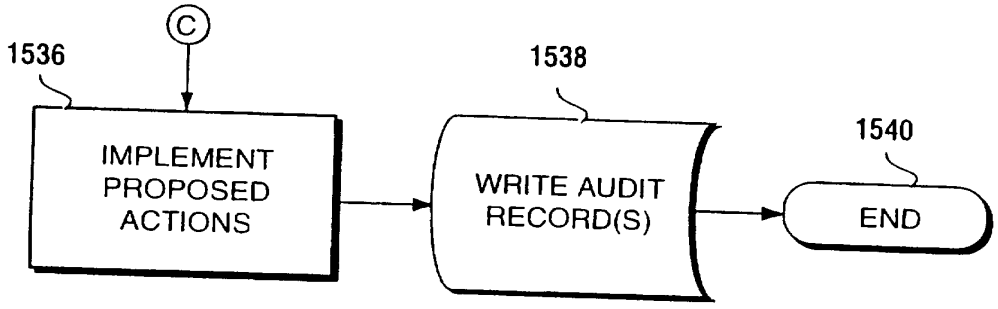


FIG.15B

F033_WO1997043761_Intertrust Page 208 of 209

DISH-Blue Spike 842
Exhibit 1005, Page 1145

FIG. 15C


C
1536
IMPLEMENT PROPOSED ACTIONS
1538
WRITE AUDIT RECORD(S)
1540
END

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 028 401 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
16.08.2000 Bulletin 2000/33

(51) Int. Cl.[7]: **G07F 19/00**, G07F 7/08

(21) Application number: **00200448.9**

(22) Date of filing: **10.02.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.02.1999 US 119818 P**
21.07.1999 US 144927 P

(71) Applicant: **CITIBANK, N.A.**
New York, New York 10043 (US)

(72) Inventors:
- **Schutzer, Dan**
  New York 10583 (US)
- **Slater, Alan**
  East Brunswick, New Jersey 08816 (US)
- **Cirillo, Thomas**
  Greenwich, Connecticut 06830 (US)
- **Derodes, Robert**
  Peachtree City, Georgia 30269 (US)
- **Dancanet, Lucien**
  Los Angeles, Califonia 90045 (US)

(74) Representative: **Hynell, Magnus**
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) Method and system for performing a bankcard transaction

(57) A method and system for performing a bankcard transaction provides a transaction card system for use, for example, on the Internet that allows a transaction card user to input authentication information to a transaction card issuer, which generates an anonymous or alternate card number and maintains a link between the anonymous or alternate card number and the transaction card user's transaction card number. An alternate aspect makes use, for example, of software on a local computing device, such as the transaction card user's personal computer or a point of sale terminal, which authenticates the transaction card user and generates the anonymous or alternate card number in sequence synchronization with the transaction card issuer's server.

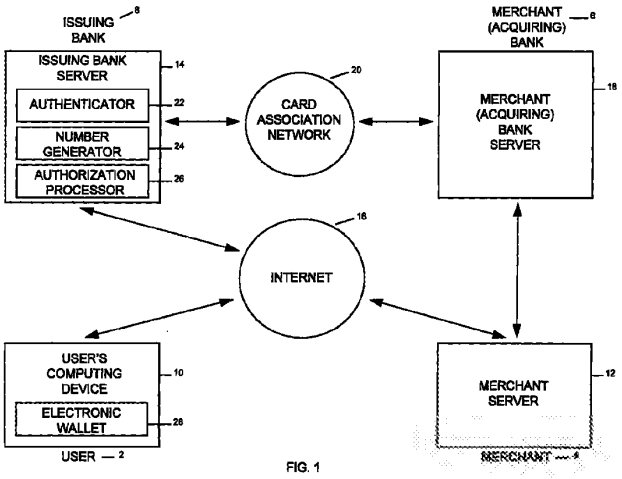


FIG. 1

Apple 1115

EP 1 028 401 A2

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.8

DISH-Blue Spike 842
Exhibit 1005, Page 1147

Description

Cross-Reference to Related Applications

[0001] This application claims priority to applicant's co-pending application having U.S. Serial No. 60/119,818 filed February 12, 1999 and applicant's co-pending application having U.S. Serial No. 60/144,927 filed July 21, 1999.

Field of the Invention:

[0002] The present invention relates generally to the field of bankcard transactions and more particularly to a method and system for securely performing a bankcard transaction utilizing an anonymous or alternate card number.

Background of the Invention

[0003] Transaction card transactions that occur over the Internet today utilizing the transaction card infrastructure are most commonly performed, for example, by a cardholder transmitting his or her credit or debit card number over an encrypted link, using a standard universally available web browser and server capability such as Secure Sockets Layer (SSL) to the merchant server. The link between the cardholder and the merchant must be encrypted to prevent the card number from being intercepted and fraudulently read by an unauthorized third party. This type of fraud is sometimes referred to as the man-in-the-middle attack. The link is encrypted so that no eavesdropper can listen in and steal the card number. However, this method has a number of disadvantages.

[0004] For example, the cardholder must trust the merchant with safeguarding the card number. This leaves the cardholder vulnerable to a risk of fraud by a merchant or its employees or a merchant who is honest but who is nevertheless negligent in maintaining the merchant's web site against break-ins. This risk is great enough to discourage customers from giving their card numbers to merchant web sites over the Internet whom they do not know or with whom they have no previous experience.

[0005] The particular risk is limited with credit cards and debit cards by consumer protection laws and association rules to a maximum exposure, such as $50 limit. Further, the cardholder has an opportunity, for example, with a credit card to dispute a charge before it is actually deducted from the cardholder's account. However, it is still a nuisance and a risk, and in the event of fraud, it may be necessary for the cardholder to be issued a new card and card number. The risk is greater with debit cards, because the limitation of liability is not as clear, and the charge is deducted from the cardholder's account before he or she is informed. Thus, with a debit card, the cardholder is placed in the position of having to dispute the deduction in order to regain his or her stolen funds.

[0006] Another disadvantage, for example, is that when a merchant accepts a card number from a customer over the Internet, the merchant has no way of authenticating that the customer making the purchase is the actual cardholder. The transaction is treated as a Mail Order/Telephone Order (MOTO) transaction, also known as a "card not present" transaction. In such a transaction, the merchant's transaction cost and exposure is much greater than when a customer is physically present at the point-of-sale. If the customer successfully disputes having made the transaction, the merchant payment is reversed by the card issuer.

[0007] These disadvantages provide incentives for a better approach to security for bankcard transactions from the standpoint of both cardholders and merchants, provided it is fast, simple and inexpensive. Many solutions have been proposed to address this need, most notably the Credit Card Association's standard specification, Secure Electronic Transaction (SET) protocol. A problem with solutions such as SET is that they impose a significant cost and performance penalty, requiring both cardholders and merchants to install special software and/or hardware that add significantly to transaction costs, in terms of both money and time.

Summary of the Invention

[0008] It is a feature and advantage of the present invention to provide method and system for securely performing a bankcard transaction which affords all of the account number of security of the SET protocol as well as the ability to authenticate the customer, while maintaining the simplicity of sending a transaction card number over an encrypted link, such as SSL.

[0009] It is another feature and advantage of the present invention to provide a method and system for securely performing a bankcard transaction which eliminates transmitting the customer's actual card number over the Internet to the merchant and likewise eliminates the need for a secure link between the customer and the merchant.

[0010] It is a further feature and advantage of the present invention to provide a method and system for securely performing a bankcard transaction, such as a credit card or debit card transaction, that is fast and easy to implement and that requires little, if any, modification to the existing Internet infrastructure.

[0011] To achieve the stated and other features, advantages and objects, an embodiment of the present invention provides a method and system for securely performing an bankcard transaction in which a transaction card user receives an alternate or anonymous card number tat is not the user's actual card number but tat is designed, for example, to pass any validity checks made by a merchant or the merchant's bank. The alternate or anonymous card number can be used only once

F034 Page 2

DISH-Blue Spike 842
Exhibit 1005, Page 1148

within a limited time period and cannot be copied and replayed. Upon receipt of the anonymous or alternate card number by the transaction card issuer, the anonymous card number can be associated by the card issuer with the proper cardholder and the cardholder's account can be authorized.

[0012] In an embodiment of the present invention, the transaction card user authenticates himself or herself, for example, to an authenticator of the transaction card issuer's server. The transaction card user can authenticate himself or herself, for example, by entering transaction card user information at a computing device, such as a personal computer, a personal digital assistant, or a smart card, coupled to the card issuer's server over a network, such as the Internet.

[0013] In addition, in an embodiment of the present invention, an electronic wallet application of the computing device can be utilized by the transaction card user for sending the transaction card user information to the transaction card issuer's server for user authentication. The transaction card user information includes, for example, one or more of a personal identification number, a password, a biometric sample, a digital signature or the transaction card number for the transaction card user, and the transaction card user information can be encrypted.

[0014] In an alternative aspect for an embodiment of the present invention, the transaction card user authenticates himself or herself with the transaction card user information at a local computing device, such as a personal computer, a personal digital assistant, or a smart card of the transaction card user. In this aspect, the transaction card user authenticates himself or herself on an application of the transaction card user's local computing device, such as an electronic wallet application, by entering the transaction card user information on the application at the local computing device.

[0015] In an embodiment of the present invention, when the transaction card user is authenticated by the transaction card issuer, a number generator of the transaction card issuer's server generates an anonymous card number for the transaction card user. However, in the alternative aspect in which the transaction card user authenticates himself or herself on an application of the transaction card user's local computing device, the anonymous card number is likewise generated at the local computing device, for example, by a number generating application of the local computing device which is synchronized with the number generator of the transaction card issuer's server.

[0016] The anonymous card number for an embodiment of the present invention is generated according to a number generating scheme, such as a random number generating algorithm, a random sequence generator, and/or a secure-hashing algorithm. Further, the anonymous card number is generated according to predefined parameters limiting its use to the particular transaction and/or for a predetermined time period.

[0017] In an embodiment of the present invention, the anonymous card number generated by the transaction card issuer is associated with a transaction card number of the transaction card user, for example, by linking the anonymous card number with the transaction card number by either or both of the number generator or the authorization processor of the transaction card issuer's server.

[0018] However, in the alternative aspect in which the anonymous card number is generated at the transaction card user's local computing device, the anonymous card number is linked with the transaction card number according to a pre-defined sequence synchronization between the number generator of the local computing device and the transaction card issuer's server.

[0019] In an embodiment of the present invention, the anonymous or alternate card number is used in a transaction by the transaction card user in place of the transaction card user's transaction card number. For example, the transaction card user sends the anonymous card number to the merchant, which in turn sends it to the merchant' bank with a request for authorization. The merchant's bank sends the anonymous card number over the card association network to the transaction card issuer. The transaction card issuer's authorization processor receives the anonymous card number linked with the transaction card number and sends an authorization back to the merchant via the card association network and the merchant's bank.

[0020] In another embodiment of the present invention, the anonymous or alternate card number is used in a transaction by the transaction card issuer after authenticating the user. For example, the transaction card user authenticates himself to the issuing bank, and the issuing bank sends the anonymous card number directly to the merchant which, in turn, sends it to the merchant's bank with a request for authorization.

[0021] In another embodiment of the present invention, the transaction card user authenticates himself to the transaction card issuer, and the transaction card issuer sends the anonymous card number, along with an authorization, directly to the merchant which, in turn, sends both the anonymous card number and the authorization to the merchant's bank for verification and processing. The transaction card user uses the actual transaction card number and the alternate card number for billing and communicating to its transaction card user, and the alternate card number and authorization number for settlement with the merchant bank and card processing network.

[0022] Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention.

Brief Description of the Drawings

[0023]

Fig. 1 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous or alternate card number is sent to a cardholder by a card issuer for use in an on-line bankcard transaction;

Fig. 2 is a flow chart which illustrates an example of the process of the cardholder performing a bankcard transaction using the anonymous or alternate card number which was sent to the cardholder by the card issuer for an embodiment of the present invention;

Fig. 3 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous or alternate card number is generated at the cardholder's computing device for use in an on-line bankcard transaction;

Fig. 4 is a flow chart which illustrates an example of the process of the cardholder performing a bankcard transaction using the anonymous or alternate card number which was generated at the cardholder's computing device for an embodiment of the present invention;

Fig. 5 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous or alternate card number is generated a point of sale for the cardholder; and

Fig. 6 is a diagram which illustrates a sample of a Linear Feedback Shift Register used to generate anonymous or alternate card numbers for an embodiment of the present invention.

Detailed Description of the Invention

[0024] Referring now in detail to an embodiment of the invention, an example of which is illustrated in the accompanying drawings, Fig. 1 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous card number is sent to a cardholder by a card issuer for use in an on-line bankcard transaction. An embodiment of the present invention involves a number of entities, such as a cardholder 2, a merchant 4, a merchant (acquiring) bank 6, and a card issuer 8. An embodiment of the present invention also makes use, for example, of computer hardware and software, such as a cardholder's computing device 10, a merchant's website server 12, and a card issuer's server 14, each coupled over a network, such as the Internet 16, as well as a merchant (acquiring) bank server 18 coupled to the merchant server 12 and also coupled to the issuing bank server 14 over a card association network 20. In addition, the card issuer's server comprises, for example, an authenticator 22, an alternate card number generator 24, and an authorization processor 26.

[0025] In an embodiment of the present invention, the cardholder 2 receives an alternate card number (referred to herein as either "anonymous card number" or "alternate card number") from the cardholder's issuing bank 8 that is not the cardholder's actual card number. The anonymous card number is issued after the cardholder 2 authenticates himself or herself directly to the cardholder's card issuer 8. The anonymous card number is utilized only once within a limited period of time. It is designed to pass any validity checks made by the merchant 4 and the merchant's bank 6 and cannot be copied and replayed. Upon receipt of the anonymous card number for authorization, the anonymous card number can be associated by the issuing bank 8 with the proper cardholder 2 and the cardholder's account and can be authorized.

[0026] Fig. 2 is a flow chart which illustrates an example of the process of the user 2 performing a bankcard transaction using the anonymous or alternate card number for an embodiment of the present invention in which the anonymous card number is sent to the cardholder 2 by the card issuer 8. At S1, the merchant's server 12 sends a request over the Internet 16 to the user 2 at the user's computing device 10 for a transaction card number in connection with an on-line transaction for the user 2. At S2, the user 2 receives the request at the user's computing device 10 and sends a request over the Internet 16 to the card issuer's server 14 for an alternate card number. At S3, the card issuer's authenticator 22 receives the request, authenticates the user 2 and obtains an alternate card number linked to the user's actual card number from the card issuer's number generator 24, and sends the alternate card number over the Internet 16 to the user 2 at the user's computing device 10. At S4, the user 2 at the user's computing device 10 sends the alternate card number over the Internet 16 to the merchant' server 12.

[0027] Referring further to Fig. 2, in an embodiment of the present invention, at S5, the merchant's server 12 receives and sends the alternate card number to the merchant (acquiring) bank's server 18 with a request for authorization. At S6, the merchant (acquiring) bank's server 18 receives the request for authorization and sends the request with the alternate card number over the card association network 20 to the card issuer's server 14. At S7, the card issuer's authorization processor 26 receives the request for authorization, links the alternate card number to the user's actual account for authorization, and sends an authorization for the alternate card number to the merchant (acquiring) bank's

server 18 over the card association network 20. At S8, the merchant (acquiring) bank's server 18 receives the authorization and sends it to the merchant's server 12. At S9, the merchant's server 12 receives the authorization and completes the transaction with the user 2.

[0028] Referring again to Fig. 2, in an embodiment of the present invention, the cardholder 2 authenticates himself or herself on-line over a secure (encrypted) line with the cardholder's issuing bank 8 at S2, utilizing, for example, an electronic wallet 28 as shown in Fig. 1. When the cardholder 2 is authenticated, he or she receives the anonymous card number over the same line at S3. Alternatively, at S3, the cardholder 2 can have the anonymous card number sent by the card issuer 8 directly to the merchant 4, in which case, it is not necessary for the cardholder 2 to send the anonymous card number to the merchant 4 at S4.

[0029] Referring once more to Fig. 2, in an embodiment of the present invention, the cardholder 2 authenticates himself or herself to the cardholder's issuing bank 8 by typing in his or her card number and a secret PIN or password or hash of a PIN or password at the user's computing device 10 and sending it over an encrypted link to the issuing bank 8 at S2. The encrypted link ensures that no third party can eavesdrop and steal the card number and PIN. The cardholder 2 can feel secure that the card number, PIN or password or hashed PIN or password are safe with the issuing bank 8, as the issuing bank 8 already knows and safeguards this information. Because the cardholder 2 authenticates himself or herself with a PIN or password, the issuing bank 8 can authenticate the cardholder 2 to the merchant 12. If the transaction or the customer's history warrants, the issuing bank 8 can require more secure authentication, such as additional secrets, matching biometrics, and/or digital signatures.

[0030] In an alternative aspect of an embodiment of the present invention, the issuing bank 8 can install software on the cardholder's PC or information appliance 10, such as a smart card or personal digital assistant (PDA) type computing device, that can generate the anonymous card number after the cardholder 2 identifies himself or herself to the software and/or appliance 10. Fig. 3 is a schematic diagram which illustrates an overview of an example key components and the flow of information between the key components for an alternate aspect of an embodiment of the present invention in which an anonymous card number is generated at the cardholder's computing device 10 in an on-line transaction. In this aspect, the card issuer 8 can install software 30 on the cardholder's computing device 10, which can be a personal computer (PC) or hardware token, such as a smartcard, that generates the anonymous card number locally upon authentication of the cardholder 2.

[0031] Fig. 4 is a flow chart which illustrates an example of the process of the user 2 performing a bankcard transaction for an embodiment of the present invention in which the anonymous card number is generated at the cardholder's computing device 10. Referring to Fig. 4, at S10 , the merchant server 12 sends a request for a transaction card number over the Internet 16 to the cardholder 2 at the cardholder's computing device 10. At S11, the cardholder 2 receives the request at the cardholder's computing device 10, and the number generating software 30 at the cardholder's computing device 10 generates and sends an alternate card number to the merchant's server 12. At S12, the merchant's server 12 receives the alternate card number and sends a request for authorization with the alternate card number to the merchant (acquiring) bank's server 18.

[0032] Referring further to Fig. 4, in an embodiment of the present invention, at S13, the merchant (acquiring) bank's server 18 receives the request and sends the request over the card association network 20 to the card issuer's server 14. At S14, the card issuer's alternate card number generator 24 receives the request, generates the next number in sequence synchronized to the cardholder's software 30, links the alternate card number to the cardholder's actual card number, and sends the cardholder's actual card number to the card issuer's authorization processor 26. At S15, the card issuer's authorization processor 26 receives the cardholder's actual card number and sends an authorization over the card association network 20 to the merchant (acquiring) bank's server 18. At S16, the merchant (acquiring) bank's server 18 receives the authorization and sends it to the merchant's server 12. At S17, the merchant's server 12 receives the authorization and completes the transaction with the user 2.

[0033] In another aspect of an embodiment of the present invention, the card issuer 8, such as a bank, provides an electronic wallet system, including, for example, an electronic wallet server. In this aspect, the issuing bank 8 matches the anonymous card number with the actual user account. If the electronic wallet generates an anonymous card number for the cardholder 2 for which the wallet server is not the issuing bank, then the anonymous card number is sent back to the wallet server for matching the anonymous card number with the actual user card number and for sending it to the issuing bank 8 for authorization. In this situation, the electronic wallet, in effect, performs an acquiring bank function.

[0034] Another aspect of an embodiment of the present invention enables the cardholder 2 to perform a transaction, such as a purchase, at a physical point-of-sale without revealing the cardholder's true card number. Fig. 5 is a schematic diagram which illustrates an example of key components and the flow of information between the key components for an aspect of an embodiment of the present invention in which an alternate card number is generated at a point-of sale for a bankcard transaction. This aspect makes use, for example, of a card 32 with no embossed number but with an input device 34, such as a keypad, a display 36, such as

a liquid crystal display (LCD), and a magnetic stripe 38 whose recording can be altered by an internal microprocessor 40 in the card. This aspect utilizes a point-of sale card device 42 coupled to the merchant (acquiring) bank's server 18, which is coupled over the card association network 20 to the card issuer's server 14.

[0035] Referring to Fig. 5, in the process of the user 2 performing a point-of-sale bankcard transaction for an embodiment of the present invention, the user 2 enters a password onto the input device 34, such as the keypad, or alternatively the user 2 enters a biometric, such as a fingerprint, onto the input device 34, such as a biometric input device. Upon entering the correct password or biometric onto the input device 34, the anonymous card number is displayed on the LCD 36 as the card number, and when the card 32 is dipped in the card device 42, the magnetic strip 38 outputs the anonymous card number. The remainder of the process for the point-of sale bankcard transaction is the similar to steps S11 through S17 of the process of the user performing an on-line bankcard transaction in which the anonymous number is generated at the user's computing device 10 illustrated in Fig. 4.

[0036] Alternatively, in the foregoing aspect of an embodiment of the present invention, when the card 32 is dipped in the card device 42, it can produce the actual number of the cardholder, but the display 36 shows an anonymous number. In this situation, a fraudulent merchant cannot read the cardholder's actual card number. The anonymous number that is displayed can be for a one-time use, in case the number is manually entered at the point of sale, but it cannot be copied and reused. In this case, a fraudulent merchant can conceivably obtain the cardholder's actual card number by skimming the magnetic strip 38, but properties of the magnetic strip 38 can be adjusted to make skimming and copying difficult. The same process can be used, for example, for a telephone order in which, after user activation and authentication, the cardholder's device 10 transmits an alternate card number through the telephone system to the merchant 4.

[0037] In an embodiment of the present invention, the assigned one-time use anonymous card number passes validation by the merchant 4 and the merchant's bank 6, because it has all the required digits in the proper position. The anonymous card number also has the proper routing digits to ensure that the transaction is sent to the correct issuing bank 8 for authentication and authorization approval. When the issuing bank 8 receives the number and requested charge for authorization, it sends the anonymous card number to a special front-end processor 24. The processor 24 can be implemented as a standalone hardware processor, or it can simply be, for example, a software module co-located inside the main authorization processor 26.

[0038] The front-end processor 24 for an embodiment of the present invention maintains a link between the actual card number and the generated anonymous card number and the time frame during which the link is valid. If a match occurs, and the anonymous card number has not already been used or expired, it is replaced with the actual card number and sent on to the normal card processing authorization system 26. Therefore, the requested transaction charge is authorized and linked to the cardholder's account by the cardholder's issuing bank 8 as long as the anonymous number matches the number provided by the issuing bank 8 or its hardware/software token 30 and as long as it has not already been used or passed the expiration period.

[0039] In an embodiment of the present invention, if the transaction is rejected, the cardholder 2 must go, for example, to a website of the cardholder's issuing bank 8 and request a new anonymous card number. The randomly selected anonymous card number is good only for one validation, and a new randomly selected number will not be assigned until the first randomly assigned number is either used or expires, whichever occurs first. Any receipts provided to the customer 2 must show the anonymous account number and the time of the transaction. The issuing bank 8 maintains the anonymous numbers and their links to true account numbers and the date and time of the transaction in order to investigate transactions disputed by the customer 2.

[0040] In the implementation of the method and system for an embodiment of the present invention, the anonymous or alternate card number is a number that is not the cardholder's actual card number. The issuing bank 8 associates the number with the cardholder's actual card number for one-time use over a limited time-duration, such as 15 to 30 minutes. The anonymous card number is generated by substituting new anonymous numbers for the actual numbers in selected positions of the cardholder's number.

[0041] There are a number of ways the anonymous card numbers are generated for an embodiment of the present invention. The generation of anonymous card numbers involves, for example, using a random number generation scheme with the additional requirement that the same number cannot be valid for more than one transaction during the same time period. Associated with the particular random number is the time that it was generated, along with a fixed period of time for which the number can be validly associated with the cardholder 2.

[0042] The assigned anonymous or alternate card number for an embodiment of the present invention can comprise, for example, 9 to 11 digits. For example, the ISO 7812 Identification Cards - Numbering System and Registration Procedure for issuer identifiers specifies that a valid card number consists of a bank identification number, plus an individual account identifier, plus a check digit. The bank identification number (BIN) is the first four or six digits of the number and is used for routing to the proper bank, such as the card issuer 8. The individual account identifier is a personal or individual

F034 Page 6

DISH-Blue Spike 842
Exhibit 1005, Page 1152

number assigned by the card issuing institution 8 for purposes of identifying an individual account. The check digit is the checksum calculated from the rest of the number.

[0043] Most commonly issued credit card numbers comprise 16 digits. For example, a valid credit card number for a financial institution, such as issuing bank 8, can be AAAAAA XXXXXXXXX C, where AAAAAA represents the BIN and is fixed, XXXXXXXXX are nine arbitrarily assigned digits, and C represents the checksum and is calculated from the other digits. Thus, the card issuer 8 can arbitrarily set 9 or 11 of the 16 digits to any number for the one-time use, adjust the checksum to its new correct value, and the card number will check out as valid by the validation systems of the merchant 4 and the merchant's bank 6. A bank desiring to use this scheme must obtain a new BIN to be used exclusively for Internet transactions. This eliminates the need of preventing the issuance of a one-time use number that is duplicative of existing or hot-carded numbers.

[0044] Alternatively, in an embodiment of the present invention, the bank, such as issuing bank 8, can use an existing BIN by reserving one or more special digits in one or more specially designated positions to identify the card number as an anonymous card number, such as AAAAAA S XXXXXXXXX C, where S is the special symbol in designated position number seven. If there are already existing real card numbers with symbol S in position number 7, it is not possible to use these numbers as anonymous card numbers, and they must be rejected as valid anonymous card numbers by the anonymous number generator. In such case, the bank has only 8 or 10 digits available to assign an anonymous card number. Longer numbers can be generated if the card association standards are modified to allow longer bit streams, or if the participating financial institutions agree to accept these longer bit streams.

[0045] In an embodiment of the present invention, the assigned one-time use anonymous card number passes validation by the merchant 4 and merchant's bank 6 because it has all the required digits in the proper position. It is passed to the correct issuing bank 8 because the BIN is correct. The anonymous card number is correctly associated with the cardholder's actual card number by the cardholder's issuing bank 8, as long as it has not passed the expiration period. The cardholder's issuing bank 8 substitutes the cardholder's actual card number for the anonymous card number and passes the number along for normal authorization.

[0046] In an embodiment of the present invention, if the transaction is rejected because the anonymous card number does not pass the match test, the cardholder 2 must go to the web site of the cardholder's issuing bank 8 and request a new number. The assigned anonymous card number is good for only one validation. A new anonymous number will not be assigned until the first number is either used or expires. Any response back to the merchant 4 includes the anonymous card number.

[0047] In one aspect of an embodiment of the present invention, the anonymous or alternate card number is generated at the issuing bank server 14 and transmitted either directly to the merchant 4 or to the cardholder's PC or token 10 for relay to the merchant 4. However, in an alternate aspect of and embodiment of the present invention, the anonymous card number is generated locally at the cardholders PC or hardware device 10, such as a smart card, personal digital assistant (PDA) type device, or Security Dynamics type card. The local/client software 30 can be downloaded from the issuing bank server 8 or installed.

[0048] In an embodiment of the present invention, if the customer 2 or the customer's electronic wallet 28 is asked to re-present the alternate card number in case, for example, its transmission to the merchant 4 was not received or was received garbled, the alternate card number is resent unless it has already expired. If it has expired, a new alternate card number is generated and sent. If the authorization was completed the first time the alternate card number was presented, then it can be recognized as a duplicate charge by the merchant 4 if the alternate card number is the same, since there are two charges for the same amount with the same alternate card number. If the merchant 4 is sent a new alternate card number, then the customer 2 and his or her issuing bank 8 will recognize it, because the customer's credit card statement will reflect a double charge against the customer's actual card number, which was correctly substituted for the alternate card numbers both times.

[0049] In an embodiment of the present invention, if the merchant 4 receives the alternate card number but is asked by the merchant bank 6 to re-present, or if the merchant bank 6 is asked by the credit card network 20 to re-present, then the original alternate card number is re-presented, whether or not the alternate card number has already expired. If the alternate card number has expired, the transaction will not be approved, and the customer 2 or the customer's electronic wallet 28 is requested to send a new alternate card number, which it will do. If the alternate card number has expired or timed-out by the time it reaches the issuing bank 8 for authorization approval, the authorization is denied, and the customer 2 or the customer's electronic wallet 28 must resubmit.

[0050] In an embodiment of the present invention, if the card network 20 stands-in because the authorization by the issuing bank 8 takes too long, then the issuing bank 8 treats the charge as valid, just as it would in any other stand-in situation. The issuing bank 8 knows the actual card number with which the charge is associated, because the issuing bank 8 can match the alternate card number with the actual card number.

[0051] In an embodiment of the present invention, in order to handle any disputes, the issuing bank 8 maintains a log for each transaction of the merchant 4,

with the amount, the alternate card number and the actual card number. The merchant 4 can trace the merchant's sale to the alternate card number, and the customer 2 can trace his or her purchase via the customer's actual card number. The issuing bank 8 can associate or match the two because it has a record of the alternate card number that is associated with the actual card number for the transaction. If the alternate card number is used for two transactions, the issuing bank 8 can spot that situation as well. In fact, if there is an attempt to use the same alternate card number twice for two different charges, the issuing bank 8 will deny the second attempt.

[0052] In an embodiment of the present invention, anonymous card numbers can be generated in several different ways. For example, the anonymous card number sequences can either be continuously generated at fixed time intervals or at each new request event. This can be achieved a number of ways, such as Security Dynamics algorithm, a random sequence generator, and a secure-hashing algorithm. If the issuing bank, such as card issuer 8, that assigns the anonymous card sequence is the same bank that validates it, there is no need to synchronize clocks.

[0053] In an embodiment of the present invention, if a number is generated that has already been assigned and has not yet expired, it will not be assigned, but a new number will be generated. The shorter the expiration period, and the more digits in the assigned number sequence, the less likelihood there is that such a conflict will occur. The anonymous number generator algorithm is designed to only issue new numbers that do not conflict with already issued and non-expired anonymous numbers or already assigned actual card numbers. This means it is designed to prevent the generation of a conflict or is capable of generating a new number within acceptable delays, not exceeding, for example, a couple of seconds, when a conflict does arise.

[0054] Alternatively, in an embodiment of the present invention, the issuing bank can run a number of anonymous number generators in parallel, so tat if one such generator generates a duplicate, a non-duplicate number can be obtained from one of the other number generators, or a batch of alternative numbers can be generated in advance from which the next alternative number can be selected. In an embodiment of the present invention, a single common number generator can be employed to service all cardholder's requests, or a different number generator can be dedicated to each active cardholder or to some subset of the total cardholder population.

[0055] In an embodiment of the present invention, the expiration interval is not so short that it expires before the cardholder 2 has time to send the sequence to the merchant 4 and have it processed and relayed through the merchant bank 6 back to the issuing bank 8. For this purpose, the expiration interval is at least, for example, about 15 minutes, but the expiration interval is adjustable to fit the application and situation. If a new card number sequence is assigned every second, 900 sequences must be generated every 15 minutes, and a typical sequence is 9 to 11 digits long. A 9-digit number generator is designed to produce 1 billion, or 10 to the ninth power, of non-duplicate sequences before it repeats, ensuring that it will not produce a repeat sequence within a 15 minute interval during which 900 sequences are generated.

[0056] An embodiment of the present invention makes use of any of a number of alternate card number generating algorithms. For example, Linear Congruential Generators are pseudo random sequence generators of the form:

$$Xn = (aXn1 + b) \bmod m$$

Where Xn = nth number of the sequence, Xn1= previous number of the sequence, a, b and m are constants where a is called the multiplier, b is called the increment and m is called the modulus. When a, b, and m are properly chosen, they can produce a pseudo-random sequence of maximal length, period m before they repeat themselves. Linear Congruential Generators are fast algorithms, but the output of a Linear Congruential Generator is not cryptographically secure. In other words, a cryptographer can, in a practical period of time, determine the next number of the sequence from examining past numbers in the sequence. Thus this algorithm can be vulnerable to attack.

[0057] However, with this algorithm for an embodiment of the present invention, an eavesdropper cannot obtain past numbers in the sequence when they are sent over encrypted lines. In that case, it would be necessary for the eavesdropper to collect the numbers at a merchant server, and these numbers may not be in sequential order at the particular merchant, since shoppers frequent a number of merchants in relatively random order. The cardholder can be prevented from collecting a sequence of alternate card numbers by selecting the alternate card number from a collection of alternate number generators used to supply numbers to multiple cardholders. This decreases the likelihood that a single eavesdropper can capture a sufficiently long sequence of anonymous numbers from a single anonymous number generator to enable reverse engineering.

[0058] Linear Feedback Shift Registers can also be used to produce pseudo-random sequences of numbers for an embodiment of the present invention, and can be designed to be maximal length. Fig. 6 is a diagram which illustrates a sample Linear Feedback Shift Register for generating anonymous or alternate card numbers for an embodiment of the present invention. The Linear Feedback Shift Register is only one such method for generating a random number. Alternatively, a random number could be used as a seed to a cryptographic hash algorithim or digital signature algorithim for any of the other methods discussed below. Linear

Feedback Shift Registers are also fast and also not cryptographically secure, but they can be combined to produce sequences that, although they cannot be proven to be cryptographically secure, are not known to have been broken. Examples include the "Bilateral Stop and Go Generator" and the "N Threshold Generator".

[0059] Another approach for an embodiment of the present invention employs a symmetric cryptographic algorithm known to be secure, such as RC4 by RSA Data Security, which requires more processing power. If the issuing bank server generates and matches the sequence, it is not necessary for the key to be shared or distributed. There is a certain degree of risk even when using cryptographic algorithms that are known to be secure. Over time, as computers grow in power, previously secure cryptographic algorithms can succumb to practical attacks. For example, 40-bit Data Encryption Standard (DES) is no longer considered secure against attacks, as today's affordable computers have been shown to have sufficient power to break this algorithm within reasonable timeframes in a matter of hours.

[0060] Another approach to generating anonymous or alternate card numbers for an embodiment of the present invention is to pick numbers in a sequence from tables of known truly random numbers, such as RAND tables. The actual selection of numbers from this table can be randomized using one of a number of techniques such as the ones described above. Alternatively, a random sequence can be generated from some actual random physical process, such as measuring keyboard latency, or electrical noise out of an electronic device.

[0061] In an embodiment of the present invention, pseudo-random numbers sequences can be made still further cryptographically secure by combining techniques, such as Linear Feedback Shift Register or symmetric algorithms to select numbers from a random number table, which are then cryptographically hashed with an algorithm such as Secure Hash Algorithm (SHA).

[0062] An aspect of an embodiment of the present invention also provides a general means of an agent authentication. For example, a user can authenticate himself or herself to the user's agent and receive an authenticating number. The authenticating number serves, for example, as a kind of one-time authentication token that is issued to the user and can be used to enable the user to authenticate himself or herself to any other service, without the need for additional passwords or secrets.

[0063] In another aspect of an embodiment of the present invention, since the alternate card number is generated on a per transaction basis, it can be used by the card processor, such as card issuer 8, to keep track of where (over what channel) and to whom (what merchant number was used). For example, if the request for an alternate number was requested at a wallet, such as the user's electronic wallet 28, over the Internet to be supplied to an Internet merchant, such as merchant 4, then the issuing bank 8 can identify and keep track of which purchases were made over the Internet and with which merchants. This information can be used for both fraud management and control purposes and for marketing purposes, such as special merchant promotions or promotions to customers for purchases made over the Internet. Similarly, it can be used to keep track of purchases made over the telephone and the like.

[0064] In another aspect of an embodiment of the present invention, when a server-based wallet, such as the user's electronic wallet 28, is used, it is technically possible for the wallet 28 to receive the merchant payment request form and not only to generate the alternate number, but also to pre-approve the purchase and to provide the merchant 4 with an alternate card number and an authorization code simultaneously. Although technically possible, it would be necessary to have such a process approved by the card association. However, if permitted, such a process has several advantages. From the merchant's perspective, for example, it saves the merchant the time required to make an authorization. Time is critical for transactions made over the Internet.

[0065] In an effort to make the shopping experience fast and convenient for users, many merchants actually take the credit card number and do not even attempt to obtain a credit authorization in real-time. Rather, they batch the transactions up and obtain authorizations after the fact. In that case, a merchant may find after the fact that the authorization was declined, and it becomes necessary for the merchant to get back in touch with a consumer. In the case of digital goods, knowledge of the denial may likely occur after the digital goods and services are already been distributed.

[0066] In the aspect in which the server-based wallet 28 also pre-approves the purchase and provides the merchant 4 with an alternate card number and authorization code simultaneously, in the bank's case, this authorization flow eliminates the risk of stand-in, in which the issuing bank, such as card issuer 8, is unable to get back fast enough, and the card association stands-in for the issuing bank 8 and automatically approves the transaction, with the issuing bank 8 still assuming the risk of collection.

[0067] Various preferred embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the spirit and scope of the present invention. Accordingly, the invention is only limited by the following claims.

Claims

1. A method for performing a transaction by a transaction card user, comprising:

authenticating the transaction card user;

generating an anonymous card number for the transaction card user;

associating the anonymous card number with a transaction card number of the transaction card user; and

authorizing the transaction with the anonymous card number for the transaction card user.

2. The method of claim 1, wherein authenticating the transaction card user further comprises authenticating the transaction card user by a transaction card issuer.

3. The method of claim 2, wherein authenticating the transaction card user further comprises authenticating the transaction card user by a server of the transaction card issuer.

4. The method of claim 2, wherein authenticating the transaction card user further comprises receiving transaction card user information by the transaction card issuer.

5. The method of claim 4, wherein receiving the transaction card user information further comprises receiving the information from the transaction card user.

6. The method of claim 5, wherein receiving the transaction card user information further comprises receiving the information at a computing device coupled to a server of the transaction card issuer.

7. The method of claim 6, wherein receiving the transaction card user information further comprises receiving the information by the transaction card issuer's server in encrypted form.

8. The method of claim 6, wherein receiving the transaction card user information further comprises receiving the information at the computing device coupled over a global network to the transaction card issuer's server.

9. The method of claim 6, wherein the computing device further comprises a personal computer.

10. The method of claim 9, wherein the computing device further comprises an electronic wallet application of the personal computer.

11. The method of claim 6, wherein receiving the transaction card user information further comprises receiving at least one of a personal identification number, a password, a biometric sample, a digital signature, and a transaction card number for the transaction card user.

12. The method of claim 1, wherein authenticating the transaction card user further comprises authenticating the transaction card user at a local computing device.

13. The method of claim 12, wherein the local computing device further comprises one of a personal computer, a personal digital assistant, and a smart card.

14. The method of claim 12, wherein authenticating the transaction card user further comprises authenticating the transaction card user by an application on the local computing device.

15. The method of claim 14, wherein the application of the local computing device further comprises an electronic wallet application.

16. The method of claim 12, wherein authenticating the transaction card user further comprises receiving transaction card user information by an application on the local computing device.

17. The method of claim 16, wherein the transaction card user information further comprises at least one of a personal identification number, a password, a biometric sample, a digital signature, and a transaction card number for the transaction card user.

18. The method of claim 1, wherein generating the anonymous card number further comprises generating the anonymous card number by a transaction card issuer.

19. The method of claim 18, wherein generating the anonymous card number further comprises generating the anonymous card number by a server of the transaction card issuer.

20. The method of claim 19, wherein generating the anonymous card number further comprises generating the anonymous card number by a number generator of the transaction card issuer's server.

21. The method of claim 1, wherein generating the anonymous card number further comprises generating the anonymous card number at a local computing device.

22. The method of claim 21, wherein generating the anonymous card number further comprises generating the anonymous card number by a number generating application on the local computing device.

23. The method of claim 22, wherein generating the anonymous card number further comprises gener-

F034 Page 10

DISH-Blue Spike 842
Exhibit 1005, Page 1156

ating the anonymous card number by the number generating application on the local computing device synchronized with a number generator of a transaction card issuer.

24. The method of claim 1, wherein generating the anonymous card number further comprises generating the anonymous card number according to pre-defined parameters limiting use of the anonymous card number exclusively to the transaction by the transaction card user.

25. The method of claim 1, wherein generating the anonymous card number further comprises generating the anonymous card number according to pre-defined parameters limiting use of the anonymous card number to a predetermined time period.

26. The method of claim 1, wherein generating the anonymous card number further comprises generating the anonymous card number according to a pre-selected number generating scheme selected from a group of schemes consisting of a random number generating algorithm, a random sequence generator, and a secure-hashing algorithm.

27. The method of claim 1, wherein associating the anonymous card number further comprises associating the anonymous card number with the transaction card user's transaction card number by a transaction card issuer.

28. The method of claim 27, wherein associating the anonymous card number further comprises associating the anonymous card number with the transaction card user's transaction card number by a server of the transaction card issuer.

29. The method of claim 28, wherein associating the anonymous card number further comprises linking the anonymous card number with the transaction card user's transaction card number by a number generator of the transaction card issuer's server.

30. The method of claim 29, wherein associating the anonymous card number further comprises linking the anonymous card number with the transaction card user's transaction card number by an authorization processor of the transaction card issuer's server.

31. The method of claim 1, wherein associating the anonymous card number further comprises linking the anonymous card number with the transaction card user's transaction card number according to a pre-defined sequence synchronization with a number generator of a local computing device.

32. The method of claim 31, wherein associating the anonymous card number further comprises linking the anonymous card number with the transaction card user's transaction card number by a server of a transaction card issuer.

33. The method of claim 1, wherein authorizing the transaction further comprises authorizing the transaction by a transaction card issuer.

34. The method of claim 33, wherein authorizing the transaction further comprises authorizing the transaction by an authorization processor of the transaction card issuer.

35. The method of claim 34, wherein authorizing the transaction further comprises receiving the anonymous card number linked to the transaction card user's transaction card number.

36. The method of claim 1, wherein authorizing the transaction further comprises sending the authorization with the anonymous card number to a merchant for the transaction card user.

37. A system for performing a transaction by a transaction card user, comprising:

means for authenticating the transaction card user;
means for generating an anonymous card number for the transaction card user;
means for associating the anonymous card number with a transaction card number of the transaction card user; and
means for authorizing the transaction with the anonymous card number for the transaction card user.

38. The system of claim 37, wherein the means for authenticating the transaction card user further comprises a server of a transaction card issuer.

39. The system of claim 38, wherein the means for authenticating the transaction card user further comprises a computing device coupled to the transaction card issuer's server for receiving transaction card user information.

40. The system of claim 39, wherein the means for authenticating the transaction card user further comprises means of at least one of the computing device and the transaction card issuer's server for encrypting the transaction card user's information.

41. The system of claim 40, further comprising the computing device coupled over a global network to the transaction card issuer's server.

42. The system of claim 41, wherein the computing device further comprises a personal computer.

43. The system of claim 42, wherein the computing device further comprises an electronic wallet application of the personal computer.

44. The system of claim 42, wherein the transaction card user's information further comprises at least one of a personal identification number, a password, a biometric sample, a digital signature, and a transaction card number for the transaction card user.

45. The system of claim 37, wherein the means for authenticating the transaction card user further comprises a local computing device.

46. The system of claim 45, wherein the local computing device further comprises one of a personal computer, a personal digital assistant, and a smart card.

47. The system of claim 46, wherein the means for authenticating the transaction card user further comprises an application on the local computing device.

48. The system of claim 47, wherein the means for authenticating the transaction card user further comprises an electronic wallet application of the local computing device.

49. The system of claim 45, wherein the means for authenticating the transaction card user further comprises an input device of the local computing device for receiving transaction card user information by an application on the local computing device.

50. The system of claim 49, wherein the transaction card user information further comprises at least one of a personal identification number, a password, a biometric sample, a digital signature, and a transaction card number for the transaction card user.

51. The system of claim 37, wherein the means for generating the anonymous card number further comprises a server of the transaction card issuer.

52. The system of claim 51, wherein the means for generating the anonymous card number further comprises a number generator of the transaction card issuer's server.

53. The system of claim 37, wherein the means for generating the anonymous card number further comprises a local computing device.

54. The system of claim 53, wherein the means for generating the anonymous card number further comprises a number generating application on the local computing device.

55. The system of claim 54, wherein the means for generating the anonymous card number further comprises the number generating application on the local computing device synchronized with a number generator of a transaction card issuer.

56. The system of claim 37, wherein the means for generating the anonymous card number further comprises means for generating the anonymous card number with pre-defined parameters limiting user of the anonymous card number exclusively to the transaction for by transaction card user.

57. The system of claim 37, wherein the means for generating the anonymous card number further comprises means for generating the anonymous card number with pre-defined parameters limiting use of the anonymous card number to a predetermined time period.

58. The system of claim 37, wherein the means for generating the anonymous card number further comprises means for generating the anonymous card number according to a pre-selected number generating scheme selected from a group of schemes consisting of a random number generating algorithm, a random sequence generator, and a secure-hashing algorithm.

59. The system of claim 37, wherein the means for associating the anonymous card number further comprises a server of a transaction card issuer.

60. The system of claim 59, wherein the means for associating the anonymous card number further comprise a number generator of the transaction card issuer's server.

61. The system of claim 60, wherein the means for associating the anonymous card number further comprises an authorization processor of the transaction card issuer's server.

62. The system of claim 37, wherein the means for associating the anonymous card number further comprises a number generator of a server of a transaction card issuer in a pre-defined sequence synchronization with a number generator of a local computing device.

63. The system of claim 37, wherein the means for authorizing the transaction further comprises a server of the transaction card issuer.

F034 Page 12

DISH-Blue Spike 842
Exhibit 1005, Page 1158

64. The system of claim 63, wherein the means for authorizing the transaction further comprises an authorization processor of the transaction card issuer's server.

65. The system of claim 37, wherein the means for authorizing the transaction further comprises means for sending an authorization for the transaction with the anonymous card number to a merchant for the transaction card user.

F034 Page 13

DISH-Blue Spike 842
Exhibit 1005, Page 1159

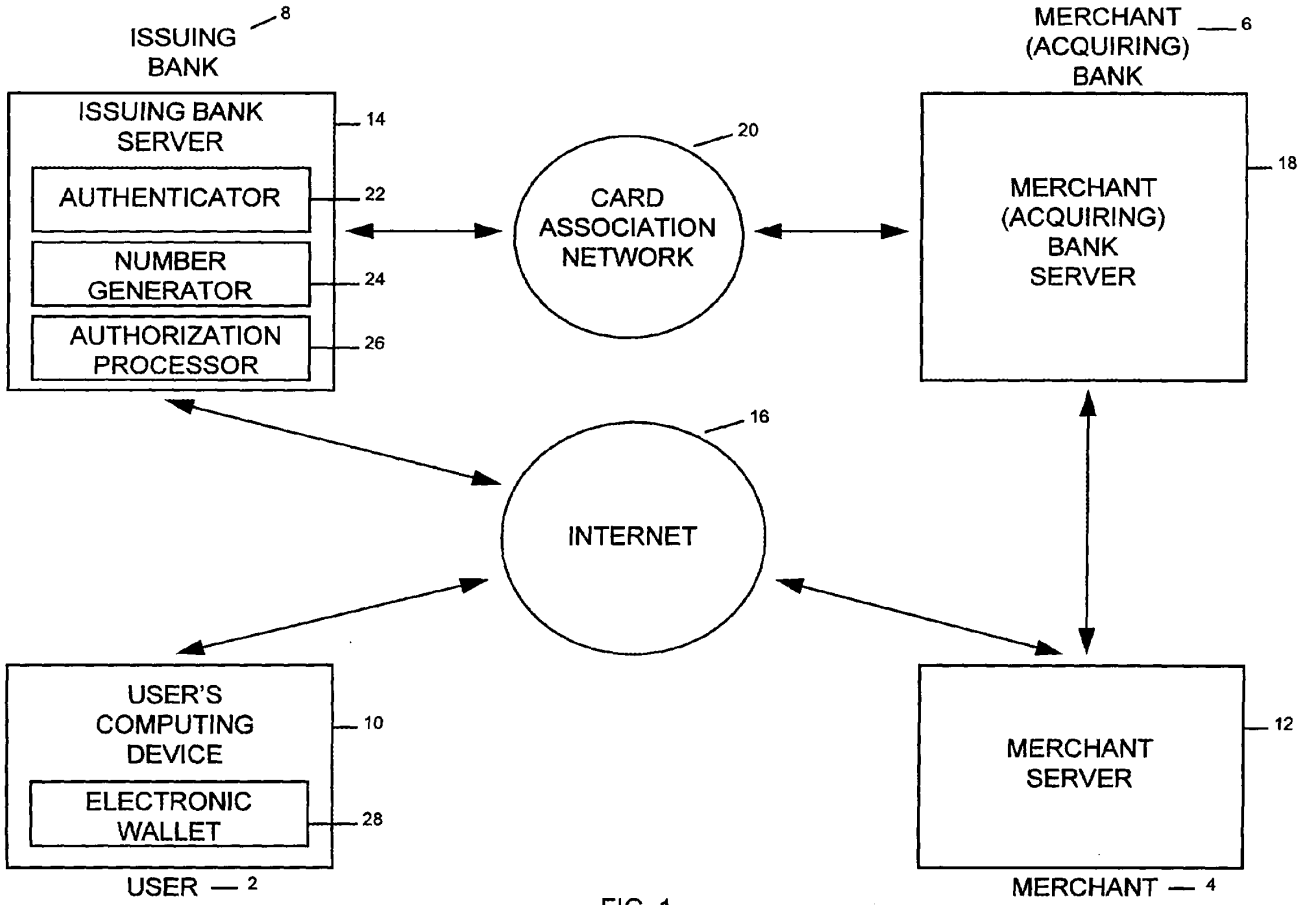


FIG. 1

EP 1 028 401 A2

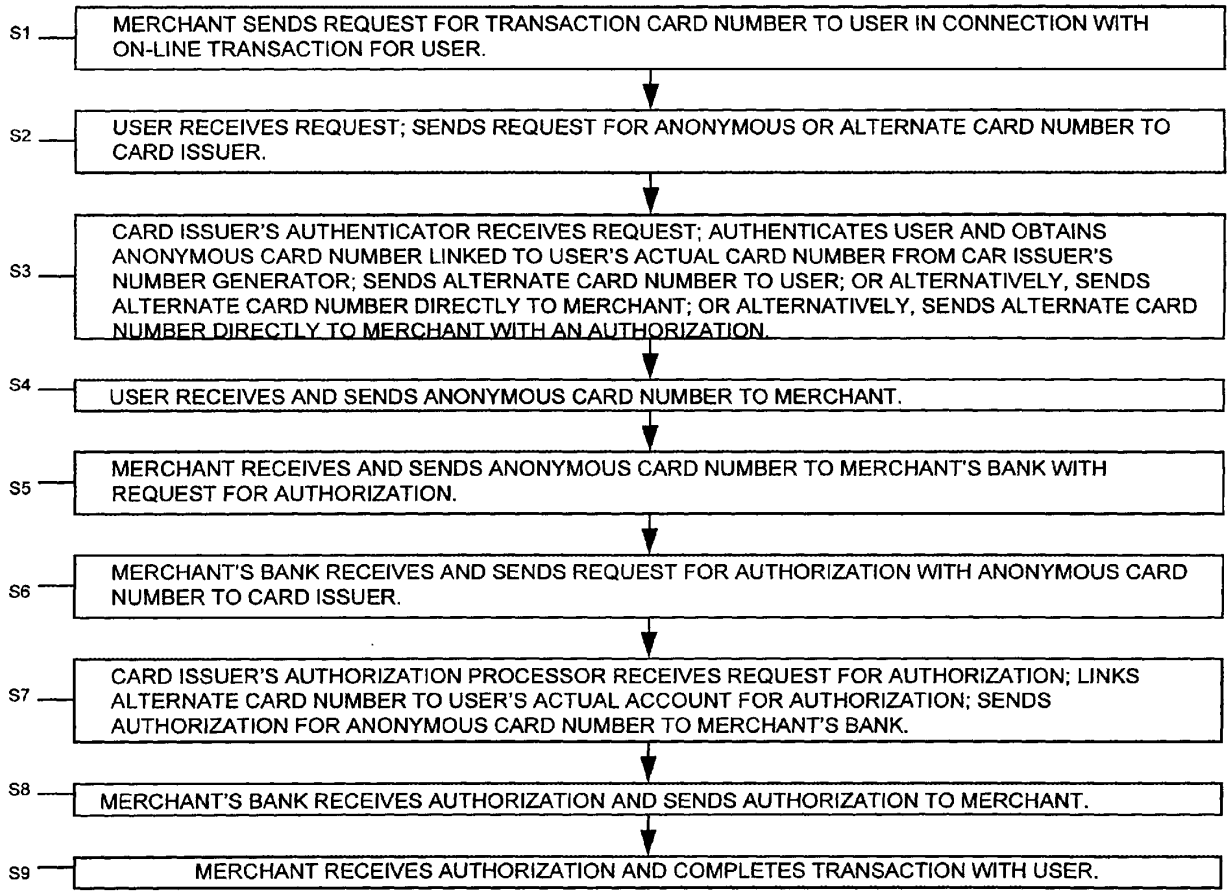

S1
MERCHANT SENDS REQUEST FOR TRANSACTION CARD NUMBER TO USER IN CONNECTION WITH ON-LINE TRANSACTION FOR USER.
S2
USER RECEIVES REQUEST; SENDS REQUEST FOR ANONYMOUS OR ALTERNATE CARD NUMBER TO CARD ISSUER.
S3
CARD ISSUER'S AUTHENTICATOR RECEIVES REQUEST; AUTHENTICATES USER AND OBTAINS ANONYMOUS CARD NUMBER LINKED TO USER'S ACTUAL CARD NUMBER FROM CAR ISSUER'S NUMBER GENERATOR; SENDS ALTERNATE CARD NUMBER TO USER; OR ALTERNATIVELY, SENDS ALTERNATE CARD NUMBER DIRECTLY TO MERCHANT; OR ALTERNATIVELY, SENDS ALTERNATE CARD NUMBER DIRECTLY TO MERCHANT WITH AN AUTHORIZATION.
S4
USER RECEIVES AND SENDS ANONYMOUS CARD NUMBER TO MERCHANT.
S5
MERCHANT RECEIVES AND SENDS ANONYMOUS CARD NUMBER TO MERCHANT'S BANK WITH REQUEST FOR AUTHORIZATION.
S6
MERCHANT'S BANK RECEIVES AND SENDS REQUEST FOR AUTHORIZATION WITH ANONYMOUS CARD NUMBER TO CARD ISSUER.
S7
CARD ISSUER'S AUTHORIZATION PROCESSOR RECEIVES REQUEST FOR AUTHORIZATION; LINKS ALTERNATE CARD NUMBER TO USER'S ACTUAL ACCOUNT FOR AUTHORIZATION; SENDS AUTHORIZATION FOR ANONYMOUS CARD NUMBER TO MERCHANT'S BANK.
S8
MERCHANT'S BANK RECEIVES AUTHORIZATION AND SENDS AUTHORIZATION TO MERCHANT.
S9
MERCHANT RECEIVES AUTHORIZATION AND COMPLETES TRANSACTION WITH USER.

FIG. 2

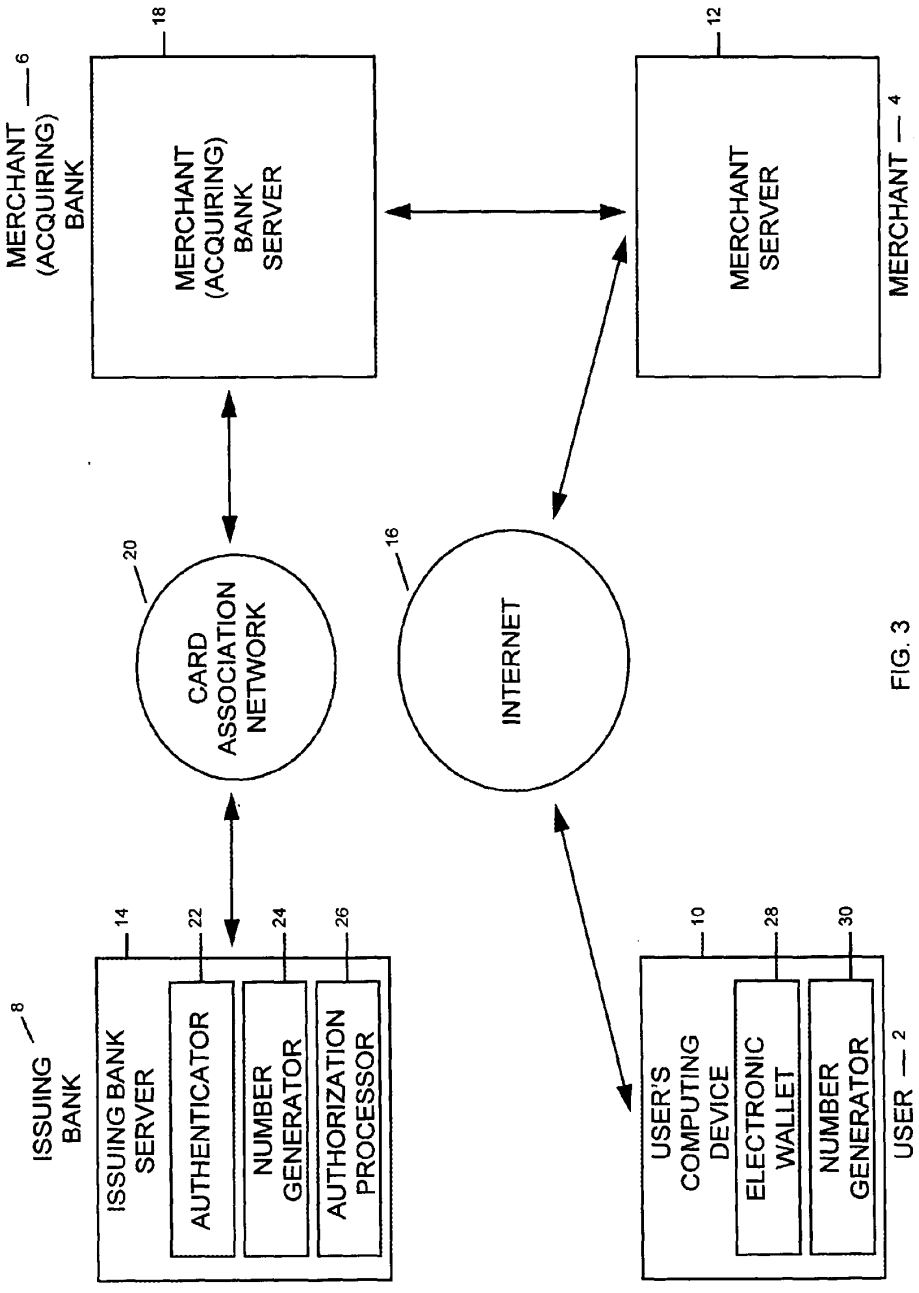


FIG. 3

F034 Page 16

DISH-Blue Spike 842
Exhibit 1005, Page 1162

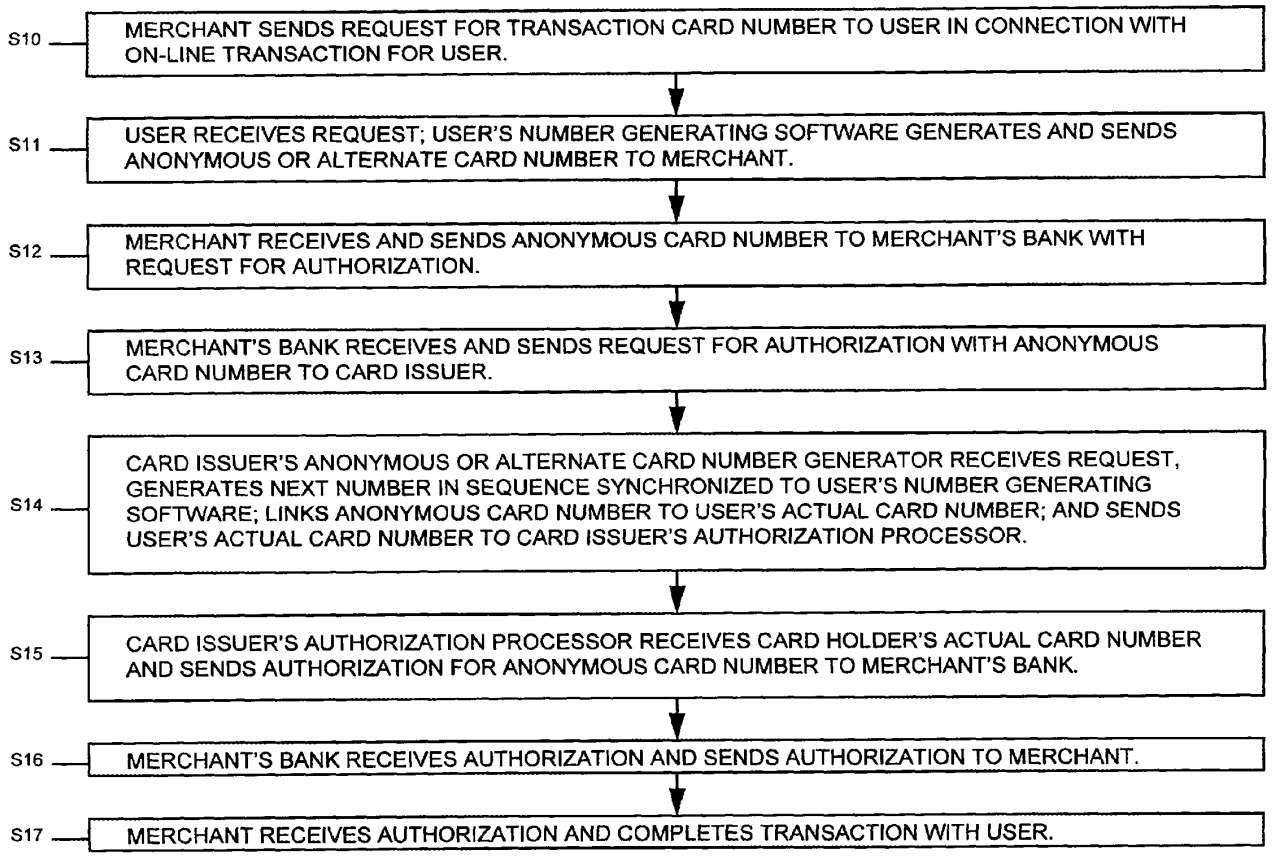

S10
MERCHANT SENDS REQUEST FOR TRANSACTION CARD NUMBER TO USER IN CONNECTION WITH ON-LINE TRANSACTION FOR USER.
S11
USER RECEIVES REQUEST; USER'S NUMBER GENERATING SOFTWARE GENERATES AND SENDS ANONYMOUS OR ALTERNATE CARD NUMBER TO MERCHANT.
S12
MERCHANT RECEIVES AND SENDS ANONYMOUS CARD NUMBER TO MERCHANT'S BANK WITH REQUEST FOR AUTHORIZATION.
S13
MERCHANT'S BANK RECEIVES AND SENDS REQUEST FOR AUTHORIZATION WITH ANONYMOUS CARD NUMBER TO CARD ISSUER.
S14
CARD ISSUER'S ANONYMOUS OR ALTERNATE CARD NUMBER GENERATOR RECEIVES REQUEST, GENERATES NEXT NUMBER IN SEQUENCE SYNCHRONIZED TO USER'S NUMBER GENERATING SOFTWARE; LINKS ANONYMOUS CARD NUMBER TO USER'S ACTUAL CARD NUMBER; AND SENDS USER'S ACTUAL CARD NUMBER TO CARD ISSUER'S AUTHORIZATION PROCESSOR.
S15
CARD ISSUER'S AUTHORIZATION PROCESSOR RECEIVES CARD HOLDER'S ACTUAL CARD NUMBER AND SENDS AUTHORIZATION FOR ANONYMOUS CARD NUMBER TO MERCHANT'S BANK.
S16
MERCHANT'S BANK RECEIVES AUTHORIZATION AND SENDS AUTHORIZATION TO MERCHANT.
S17
MERCHANT RECEIVES AUTHORIZATION AND COMPLETES TRANSACTION WITH USER.

FIG. 4

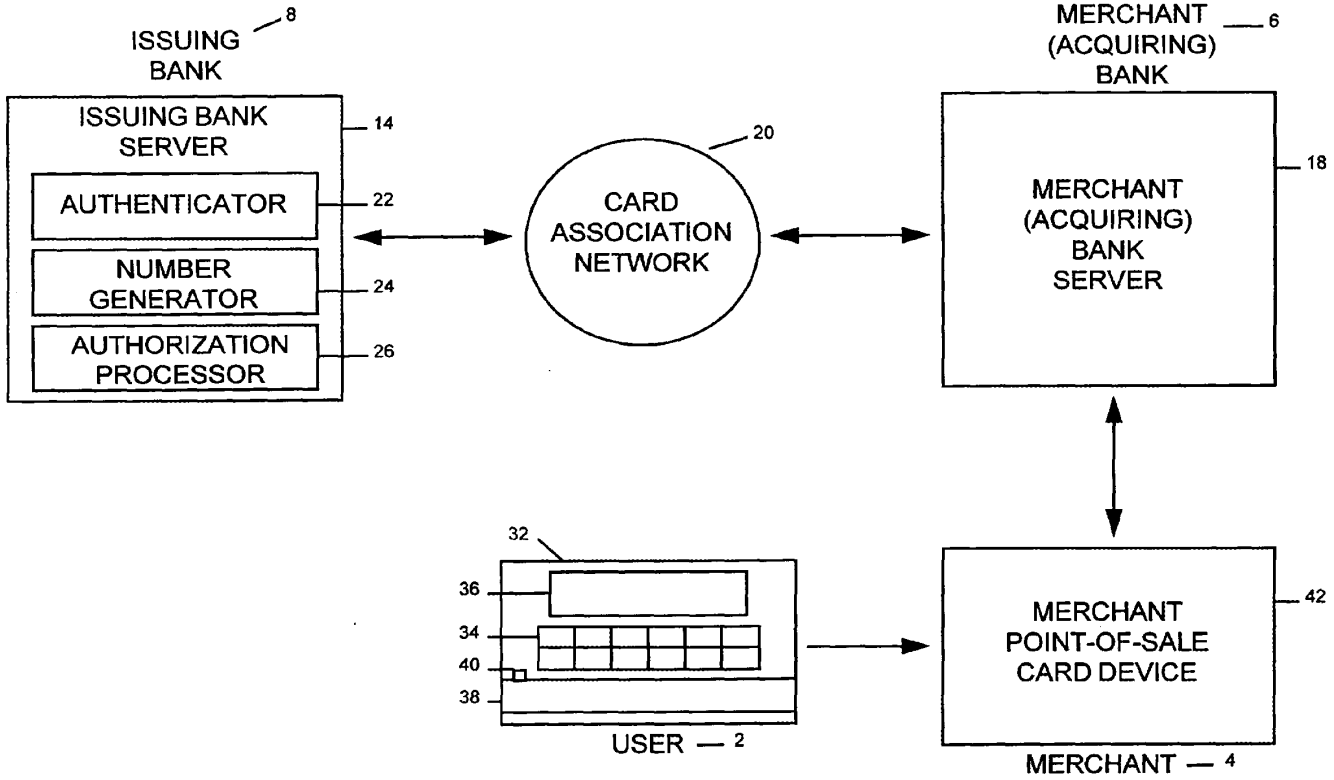


FIG. 5

EP 1 028 401 A2

DISH-Blue Spike 842
Exhibit 1005, Page 1164

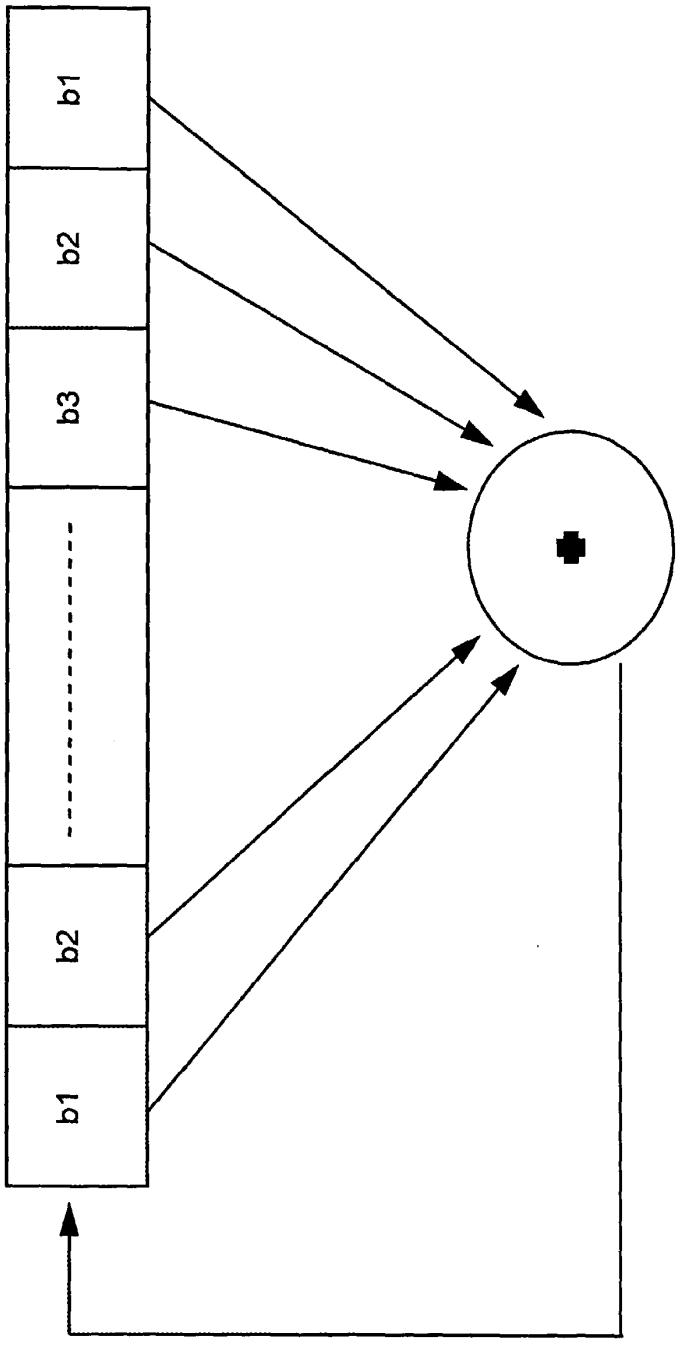


FIG. 6

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/00 — A1

(11) International Publication Number: **WO 00/14648**

(43) International Publication Date: 16 March 2000 (16.03.00)

(21) International Application Number: PCT/US99/20348

(22) International Filing Date: 3 September 1999 (03.09.99)

(30) Priority Data:
60/099,162 4 September 1998 (04.09.98) US

(71) Applicant: IMPOWER, INC. [US/US]; 88 Orchard Road, Princeton, NJ 08540 (US).

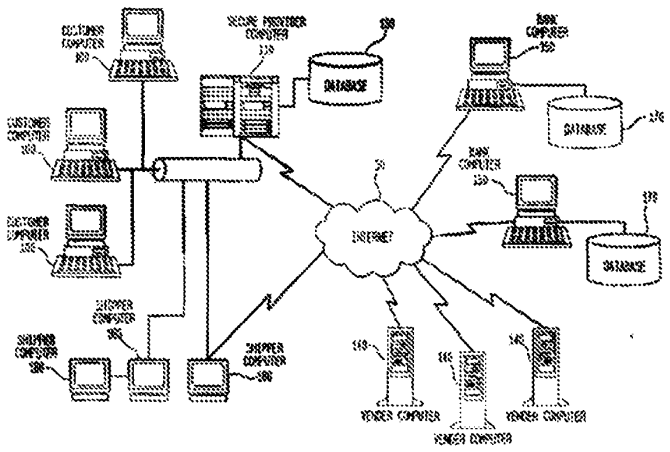
(72) Inventor: BRENER, Harry; 673 Lawrenceville Road, Princeton, NJ 08540 (US).

(74) Agents: WALLACE, Michael, J., Jr. et al.; Lerner, David, Littenberg, Krumholz & Mentlik, LLP, 600 South Avenue West, Westfield, NJ 07090 (US).

(81) Designated States: 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ELECTRONIC COMMERCE WITH ANONYMOUS SHOPPING AND ANONYMOUS VENDOR SHIPPING



(57) Abstract

A computer-implemented method delivers goods purchased from a vendor web site without revealing the customer's identity or physical shipping address to the vendor computer (140). The method includes associating the identity and physical location of each customer with computer (100) linking information which is stored at a secure computer such as a secure provider computer (110) or banking computer (150). The customer computer (100) anonymously connects to the vendor web site (140) and orders goods without revealing his actual identity or physical location. The goods are given by the vendor to a common carrier in a package encoded by the vendor with a transaction identifier or a customer object. The common carrier retrieves the identity and address of the customer from the secure provider computer (110) using the transaction identifier or customer object and delivers the package to the customer's physical address.

VISA - EXHIBIT 1005

DISH-Blue Spike 842
Exhibit 1005, Page 1166

FOR THE PURPOSES OF INFORMATION ONLY

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

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

ELECTRONIC COMMERCE WITH ANONYMOUS SHOPPING AND ANONYMOUS VENDOR SHIPPING

TECHNICAL FIELD

The present invention relates to a method and system of conducting electronic commerce which allows a customer to anonymously visit vendor web sites, anonymously purchase goods and anonymously receive goods without disclosing the customer's identification and home address information to the web site vendor.

BACKGROUND ART

At present day, more and more consumers are using a global communications network such as the Internet to do their shopping. On-line shopping allows users the freedom to quickly browse different vendor web sites, compare prices, locate hard-to-find items, shop across the country and the world, all within an abbreviated period of time. However, for good reasons, many people today are worried about privacy issues when using the Internet and World Wide Web ("the web"). Merely by visiting a web site, detailed information about the customer can be obtained, such as what computer the customer is using, where the computer is connected, which web site the customer last visited, etc. Furthermore, more and more sites are requiring that customers log into the site with personal information in order to use the services of the site. Many customers, however, do not wish to compromise their privacy and reveal their name and address since it will likely be placed in a database and sold as a part of a mailing list to other companies. Further, consumers worry about transmitting personal information such as credit card numbers or bank account numbers on-line, for fear of a third-party monitoring their transmission.

At present, Internet billing systems are known that maintains the confidentiality of the customer information by an Internet access provider vis-à-vis a vendor web site. The Internet access provider creates access to the Internet through the secure provider's web site for the user. The provider then bills the customer's account with the provider or another specified account for transactions with outside vendors,

DISH-Blue Spike 842
Exhibit 1005, Page 1168

without the need for the customer to send his bank account number or credit card information to the vendor. The problem with these billing systems is that they do not provide complete privacy. While customers using such a billing system do not have to reveal their bank account numbers or credit card numbers to outside vendors, they do need to reveal their home addresses to the vendor so that the vendor can mail or ship the customer their order. Many customers, when shopping on-line, wish to remain completely anonymous to vendors in order to avoid future solicitations from the vendor, as well as having their names and addresses potentially added to a mailing list. Although anonymity is important, many shoppers enjoy the benefit of returning to vendor web sites which store information about the shopper (such as via "cookies") so that the same information need not be reentered each time and custom offerings and information can be communicated to the shopper upon revisiting a favorite web site. Accordingly, what is needed is a secure Internet e-commerce system that eliminates the need to provide vendors with both customers' actual identities and shipping addresses, and accordingly provides customers with complete anonymity. It would also be desirable to provide such an e-commerce system whereby the customer can remain anonymous but still visit web sites as a character or persona such that he or she is recognized upon return to the vendor web site.

DISCLOSURE OF THE INVENTION

In accordance with a preferred aspect of the present invention, a computer-implemented method of delivering goods is provided whereby good are purchased from a vendor having a vendor web site accessible over a computer network by a plurality of customers at physical locations. The customers have customer computers connected to the computer network for accessing the vendor web site and electronically purchasing goods therefrom. The method includes: (a) associating the identity and the physical location of each customer with a respective customer object via linking information; (b) storing the linking information at a secure computer at a location remote from the vendor web site; (c) anonymously connecting to the vendor web site by the customer computer using the identity of the customer object without revealing the identity and physical location of the customer; (d) ordering goods at the vendor web site by the customer using the customer computer, and upon initiation of an order by the customer, (i) automatically generating a

DISH-Blue Spike 842
Exhibit 1005, Page 1169

transaction identifier by the vendor computer, (ii) encoding a package of the goods ordered by the customer with the transaction identifier by the vendor and (iii) sending the transaction identifier together with the customer object to the secure computer by the vendor computer; (e) associating the transaction identifier sent by the vendor computer with the identity and physical address of the customer at the secure computer using the linking information and automatically forwarding the transaction identifier and associated identity and physical address of the customer to a computer of a common carrier; (f) delivering the encoded package to the common carrier by the vendor; and (g) reading the transaction identifier by the common carrier, using the identity and the physical location of the customer associated with the transaction identifier and physically delivering the package to the physical location of the customer.

In an alternative preferred embodiment, the computer-implemented method of delivering goods comprises (a) associating the identity and the physical location of each customer with a respective customer object via linking information; (b) storing the linking information at a secure computer at a location remote from the vendor web site; (c) anonymously connecting to the vendor web site by the customer computer using the identity of the customer object without revealing the identity and physical location of the customer; (d) ordering goods at the vendor web site by the customer using the customer computer, and upon initiation of an order by the customer, encoding a package of the goods ordered by the customer with the customer object; (e) delivering the encoded package to the common carrier by the vendor; (f) providing the linking information to the common carrier; and (g) reading the customer object by the common carrier, retrieving the identity and the physical location of the customer associated with the customer object and physically delivering the package to the physical location of the customer.

Desirably, the above methods further comprise sending information representing the cost of the goods ordered by the customer and the customer object from the vendor computer to a financial institution computer via the computer network for credit approval, ascertaining the credit status of the customer object, and automatically sending a message approving or declining credit to the customer to the vendor computer from the financial institution computer. Ascertaining the credit status of the customer object can also

DISH-Blue Spike 842
Exhibit 1005, Page 1170

include ascertaining the identity of the customer based on the linking information obtained by the financial institution from the secure provider.

The step of anonymously connecting to the vendor web site may include revealing one or more customer characteristics to the vendor web site by the customer object so as to allow the vendor web site to use such customer characteristics to customize information and goods presented to the customer upon return to the vendor web site using the customer object. The step of anonymously connecting to the vendor web site is preferably performed automatically without customer interaction on at least some occasions by the customer object programmed to shop for the customer in accordance with directions specified by the customer. The customer object may be personified to the customer via the customer computer through the display of audio and/or visual display.

The secure computer may comprise a secure provider computer allowing the customers to anonymously connect to the vendor web site therethrough, or alternatively, the secure computer can comprise the financial institution computer.

In another preferred embodiment of the present invention, a computer character generating system is provided in the context of a computer system for offering goods, services and/or information from a vendor computer providing access to a vendor web site over a computer network including a plurality of customer computers connected to the network for accessing the vendor web site. The computer character generating system includes (a) a character generation program executable on the vendor computer and containing instructions for causing the vendor computer to generate an interactive vendor character which represents the vendor and interactively guides a customer through the vendor computer site, (b) the character generation program being operative to send character display commands to the customer computer when the customer computer has accessed the vendor web site causing the customer computer to display on a display device associated with the customer computer the interactive vendor character, (c) the interactive vendor character providing a trademark function for the vendor such that the interactive vendor character is identified with the vendor by customers who desire to acquire goods, services and/or information over the computer network from the vendor web site, the interactive vendor character further having a persona such that the vendor character will

DISH-Blue Spike 842
Exhibit 1005, Page 1171

respond to inputs from a customer computer representing communications by a customer in a manner representative of a human having particular personality traits acting in a representative capacity.

Desirably, the vendor computer records the identities of customer computers which interact with the vendor web site and records historical data representing transactions of each customer computer with the vendor computer, and the vendor character responds to inputs from each customer computer based partially on the inputs and partially on the historical data in conjunction with the personality traits. The vendor character preferably has an artificial intelligence function which allows the vendor character to predict responses which would tend to elicit an acquisition by each customer computer based upon the historical data associated with such customer computer, and the interactive vendor character bases responses at least in part upon such predictions. The vendor character can also check for available goods, services and/or information requested by each customer computer and also checks for goods or services which are different from those requested by the customer computer but which are likely to be of interest to such customer computer based upon the historical data. The vendor character can be displayed with facial expressions, movement characteristics and voice accents associated with the personality traits.

In yet another preferred embodiment of the present invention, an interactive computer-implemented method of offering goods, services and/or information is provided with a vendor computer providing access to a vendor web site over a computer network to a plurality of customer computers connected to the network for accessing the vendor web site. The method includes (a) providing a plurality of customer objects representing individuals who desire to acquire goods, services and/or information from the vendor sites, each customer object being provided with a set of user characteristics representing personal preferences and information about the individual; (b) providing a vendor persona object representing the vendor, the vendor persona object being provided with a set of vendor characteristics representing information about the goods, services and/or information offered by the vendor; and (c) visiting the vendor computer site via the network with a customer object such that the customer object and the vendor persona object dynamically

interact with one another to exchange one or more subsets of the set of user characteristics and vendor characteristics for determining whether the goods, services and/or information offered by the vendor computer site are of interest to the user persona object.

The method desirably includes targeting a sales offer by a vendor computer to at least one customer computer via the secure provider computer based upon the purchasing interest and demographic information collected for at least one customer computer by the secure provider computer and provided to the vendor, wherein the customer object is configured by the customer to determine whether the sales offer will be presented to the customer computer.

In yet a further preferred embodiment of the present invention, a method for providing advertising on the web site of a secure provider computer is provided comprising (a) providing a secure provider computer to allow customer computers connected to the secure provider computer to have access to authorized vendor offers on the secure provider web site; and (b) posting one or more vendor offers on the secure provider web site, wherein the offers are only viewable by the customer computers.

In still a further preferred aspect of the present invention, a computer-implemented method for knowingly monitoring network navigation and purchasing history of a plurality of customers by a secure provider is provided,comprising: (a) requiring each customer to first establish an account with the secure provider by requiring each customer to agree to have the customer's demographic information and purchasing history tracked by the secure provider; (b) providing on-line access to a computer network to computers of customers who have established an account via a secure provider computer of the secure provider; and (c) tracking and storing the customers' demographic information and purchasing history by the secure provider computer as the customers update and change their demographic information and make purchases via their customer computers.

Preferably, at least one customer computer is presented with an item to be purchased selected by the secure provider computer based on the customer's demographic information and purchasing history tracked by the secure provider. Further, a sales offer can be targeted by a vendor computer to at least one customer computer via the secure provider computer based on the customer's demographic information and purchasing

DISH-Blue Spike 842
Exhibit 1005, Page 1173

history collected by the secure provide computer and provided to the vendor in a modified form which does not include the customers' identity information, wherein the customer object is configured by the customer to determine whether the sales offer will be presented to the customer computer.

In an even further preferred embodiment of the present invention, a method of providing outside vendor offers on a web site of a secure provider computer is provided, including (a) establishing a secure provider web site allowing member customer computers to have access to an area on the web site that posts outside vendor offers; and (b) configuring the secure provider web site so that the vendor offers are only viewable by the member customer computers. Desirably, only vendors who have signed up with the secure provider in advance are able to view the area on the web site that posts the outside vendor offers.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of a preferred embodiment of a computer system according to the present invention.

FIG. 2 is a flow chart of the steps followed in a preferred method according to the present invention.

FIG. 3 is a depiction of a sample secure provider web site.

FIG. 4 is a depiction of a sample vendor web site.

BEST MODES FOR CARRYING OUT THE INVENTION

Referring to FIG. 1, the computer system of the present invention comprises a network of interconnected computers connected via a global communications network such as the Internet 50. The network of computers comprise plurality of customer computers 100, a secure provider computer 110, a plurality of vendor computers 140, a plurality of bank computers 150 and a plurality of third party carrier or shipping computers 180. Each computer comprises the typical components needed to connect to the Internet and World Wide Web, such as RAM and ROM memory, mass storage, microprocessor(s), display device, user input devices, etc. The secure provider computer 110 and vendor computers 140 also will typically include one or more server computers to allow provision

DISH-Blue Spike 842
Exhibit 1005, Page 1174

of web sites such as a secure provider web site and vendor web sites, which offer goods, services and other information desired.

The present invention desirably allows a customer to shop on-line at vendor web sites in an anonymous fashion. To do so, a customer uses his customer computer 100 (such as a home computer with dial-up connectivity to the Internet) to connect the secure provider computer 110 and login with a certificate based ID and password. Prior to conducting on-line shopping, the customer creates a customer object or on-line personna that represents the preferences of the customer. This is discussed in further detail below. The customer object which can be represented by a name (such as "GOLFO") and the customer's personal information, such as the customer's name and address, are matched up with linking information. This linking information is stored, in one embodiment, in a linking table stored in the database 130 of the secure provider computer 110. This linking table matches up each customer object with the customer's personal information which the customer wants shielded from the vendor web sites. Alternatively, the linking information can be stored in the database 170 of bank computer 150 so that only the bank, and not the secure provider, actually knows the true identity and address of the customer. In either case, the linking information is stored in a secure computer so as to shield the linking information from third parties, including the vendor. Using this linking table, the secure provider computer 110 or the bank computer 150 can determine which customer a given customer object represents.

Once the customer computer 100 is connected to the secure provider computer 110, a secure connection pipeline 120 is provided between the customer computer 100 and the secure provider computer 110 in order to prevent transmissions between the customer computer 100 and the secure provider computer 110 from being monitored. Namely, after the customer joins the web site of the secure provider computer 110, the customer computer 100 is preferably provided with software by the secure provider computer 110. This software enables the customer computer 100 to connect directly to the secure provider computer 110, along a known, fixed node-to-node route, without having to connect to the vendor web site through a different node-to-node network each time as is common over the Internet. Thus, to protect the privacy of the user, the

DISH-Blue Spike 842
Exhibit 1005, Page 1175

customer computers 100 are preferably connected to the secure provider computer 110 through a virtual personal network ("VPN") which provides a private passageway or tunnel through the Internet. As is known in the Internet communications art, in a VPN, computers communicate with each other through firewall computers, so that the only addresses known are those of the firewall computers. This secure pipeline 120 allows the customer to connect directly, node-to-node, with a VPN, when there is communications between the secure provider computer and the vendor computer, so the only address that is revealed to the vendor is the address of the firewall computer. This allows customer computers 100 to communicate from within a network to vendor computers 140 without having their addresses revealed or access to any peripherals or devices on customer computer 100.

With the secure connection, the customer computer 100 can anonymously connect to the web sites of various vendor computers 140 using the Internet via the secure provider's proxy servers. The customer computer 100 can browse for the web sites of vendor computers 140 of interest using various different search methods known in the art. When a customer computer 100 connects to a vendor web site of a vendor computer 140, the vendor computer 140 is provided only with the customer object, which identifies the customer as a fictitious entity without revealing personal information about the customer such as real name or address. When the customer computer 100 notifies the vendor computer 140 that the customer computer 100 would like to make a purchase, the vendor computer 140 contacts a bank computer 150 through the Internet to verify that the customer object on the customer computer 100 has sufficient funds to make the purchase. To facilitate the verification process, the vendor computer 140 forwards the customer object to the bank computer. The bank computer 150 obtains or is already provided with the linking information to link the customer object with personal information about the customer, including customer account information. Once the bank computer 150 determines whether the customer object has sufficient funds to make the purchase, the bank computer 150 notifies the vendor computer 140 whether the customer has sufficient funds to make the purchase. In an alternate embodiment, the vendor computer 140 need

not contact a bank but can simply bill the secure provider computer 110 for the transaction, who will in turn bill the customer.

Once a purchase by the customer has been approved, the vendor arranges for the package to be picked up by a third party carrier. The package, however, must be labeled with information that the shipper can use to ship the package to the correct address, but cannot contain the actual address of the customer, since it is to be shielded from the vendor. To accomplish this, the vendor computer 140, in a preferred embodiment, provides the third party carrier computer 180 with a transaction identifier and the customer object through the Internet to shipper computer 180. The vendor also places the transaction identifier only on the package. Once the shipper comes to the vendor to pick-up the package, the shipper, who is provided with or can ascertain the linking information, knows the address to match up with the transaction identifier. Alternatively, the vendor can simply attach the customer object to the package, such as in the form of a bar code or a label. The third party shipper computer 180 can then contact the secure provider computer 110 directly through a secure pipeline or through the Internet, to retrieve the customer's address from the database 130 or is provided ahead of time with the linking information to match up the customer object with the customer's actual name and address. Alternatively, where the linking information is not known to the secure provider and is known only to the bank, the shipper can retrieve or be provided with the linking information for the transaction identifier and/or the customer object from the bank.

FIG. 2 illustrates a preferred method in accordance with the present invention. As shown in step 200, a customer computer 100 first connects to the web site of the secure provider computer 110, illustrated in FIG. 3, and joins the secure provider's service by filling out a standard form on the web site of the secure provider computer 110. When a customer signs up to use the secure provider web site and services, the customer is prompted to create a "persona" or customer object to be stored on a database 130 on the secure provider computer 110. In one embodiment, this object may have both a public and private segment to a digital certificate or key. In another embodiment, a linking table is also stored on the database 130 of the secure provider computer 110 which provides the link between the customer's personal information, such as the customer's name and

DISH-Blue Spike 842
Exhibit 1005, Page 1177

shipping address, and the customer's object such as a public key, but not the synonym, or name of the object. Alternatively, the linking table is stored only by banking computer and is not known by the secure provider. Thus, while the information about the customer object is stored by the secure provider, in the case where the customer wishes to remain anonymous to the secure provider, the linking information to link customer object to the actual customer is given only to the bank by the customer. The linking table is ultimately used to provide the bank computer with the account number or private key authorization of the customer and to provide the third party carriers with the actual name and address of a customer once the package has been labeled by the vendor with the customer object or transaction identifier.

In one preferred embodiment, the customer can create and modify his customer object via a personalized home page stored on the web site of the secure provider computer 110. For example, if the customer is a golfer, the customer might create the persona or customer object named "GOLFO," which object can then be used to navigate anonymously on the Internet. In creating the persona, the customers can, for example, select an available name (such as GOLFO) and enter in detailed personal information about himself. The GOLFO persona thus functions as the customer's anonymous alter-ego and will contain personal information such as age, sex, interests, hobbies, shirt size, shoe size, likes, dislikes, merchandise the customer has an interest in, etc. This persona, GOLFO, along with all other customers' personas, is stored on the database 130 of the secure provider computer 110, which may or may not store the linking information as explained above.

Once the customer joins the web site of the secure provider computer 110, the customer is provided with a customer object identifier number or certificate, also stored on database 130. The customer's object identifier number or certificate, but not their bank account information, credit card numbers or home address, is preferably stored on a "cookie" or database at the customer computer 100, and is also stored on secure provider computer 110. In this manner, when a customer logs into the secure provider web site using customer computer 100, the customer object identifier number or certificate

can be used by the secure provider computer 110 to identify the user as a customer of the web site of the secure provider computer 110.

Once the customer computer 100 has been identified as a member of the web site of the secure provider computer 110, the customer computer 100 can then access the Internet through the web site of the secure provider computer 110 and begin to securely browse, as shown in step 210.

When the customer computer 100 decides on a web site from which the customer would like to make a purchase, such as the vendor web site illustrated in FIG. 4, the customer computer 100 enters the web site of the vendor computer 140 as shown in step 220, as his "GOLFO" object or persona. Namely, when the customer computer 100 enters the web site of the vendor computer 140, the vendor computer 140 is provided only with GOLFO's persona information that is authorized for release. The GOLFO persona or object provides detailed demographic and psychographic information about the customer so that the vendor computer 140, if desired, can develop a relationship with the customer through his persona. For example, if the customer visits a golf merchant's web site on a regular basis to buy golf shirts, the golf merchant's vendor computer 140 could store a profile of the GOLFO persona. When the vendor computer 140 sees that GOLFO has returned to the web site, the vendor computer 140 can present the customer, through his GOLFO persona, with shirts the vendor may think GOLFO might like based upon the previous purchases of GOLFO, as seen by display 400 on the vendor web site.

In other words, when a customer logs into a vendor web site, the customer will log in with a customer object that does not reveal the actual customer who is linked to the object. The information that is revealed to the vendor would simply be GOLFO at the address of the web site of the secure provider computer 110. In this manner, safe and private visitation of web sites can be achieved through the customer object. The customer object can also be programmed to navigate the Internet on its own, gather relevant information and then report back to the actual customer the information gathered based on the task(s) assigned to the customer object.

In a further aspect of the present invention, the customer object is provided with a credit rating or credit history such that the vendor can determine whether to sell the

goods to the customer. Preferably, the customer object is provided with its own credit facility, which could include, for example, a virtual credit card. Such a virtual credit card is preferably given a name and icon representation so that the customer can easily purchase goods on-time by clicking on the credit card name or icon displayed at the participating vendor's web site. Use of such virtual credit card enables the customer object to readily purchase goods or services on credit. Credit card transactions, when authorized by the customer or customer object identifier, are preferably done through secure transaction protocols, such as digital signature and digital certificates. In such a case, the customer object itself can be provided with the digital signature and certificate information for use in purchasing items.

Once a customer decides to make an on-line purchase from the secure web site, the customer preferably clicks on an icon, such as icon 410 shown in FIG. 4, representing the virtual credit card on the secure provider web site, as shown in step 230. A list of items selected can also be displayed in a "shopping cart" such as shown at display 430 on the vendor web site.

As shown in step 240, the vendor then forwards the customer's object, vendor number, transaction identifier, and the amount of the purchase to bank computer 150. In one embodiment, the customer object comprises a public key and a private key authorization code. In one preferred embodiment, bank computer 150 is provided with a database 170 of the linking information of customer object or public key and customer information that allows the bank computer 150 or credit card company computer to determine who the actual customer is. In another embodiment, the bank computer 150 or credit card company can retrieve the customer object or public key from the secure provider computer 110 and therefore need not be in physical possession of the linking information. The bank computer 150 then determines whether or not to authorize the transaction. Preferably, it is desired that the bank not know the transactional information of the customer so that it cannot determine purchasing history and preferences of the actual customer. Thus, the bank can agree not to use or sell the customer's transactional information for solicitations or the like or, if possible, the bank need not know what is being purchased and from where, only that the customer has the money or credit to cover

DISH-Blue Spike 842
Exhibit 1005, Page 1180

the transaction. Thus, in the case where the secure provider is not provided with the linking information, the customer is assured that the bank is not monitoring his or her transactional information and that the secure provider, who is monitoring the transactional information, cannot link the customer's actual identity to the customer object.

In another embodiment, vendor computers 140 can contact the secure provider computer 110 instead of bank computer 150 to authorize payment. The secure provider computer 110 can either bill the customer, or the customer can create a credit/debit account with the secure provider computer 110. The vendor computer 140 can send the secure provider computer 110 a bill for the purchases of the customer computer 100. The secure provider computer 110, in turn, can send a bill to the customer computer 100, or, if the customer computer 100 has a credit or debit account established with the secure provider computer 110, the secure provider computer 110 could adjust the customer's account accordingly. In another embodiment, the secure provider computer 110 can engage in electronic bill presentation to customer computer 100, and transmit information about the request for payment to bank computer 150.

Once the bank computer 150 has authorized the purchase, as shown in step 250, the bank computer 150 returns the vendor number, the transaction identifier and/or the customer object or public key, and the approval of the transaction back to the vendor computer 140 or to the secure provider computer 110, depending upon which computer transmitted information about the request for payment to bank computer 150. Upon approval of the transaction, the vendor readies the goods for anonymous shipment as explained below.

A key aspect of the present invention is the secure and anonymous shipping protocol used. This secure and anonymous method is provided whereby the customer can have the vendor ship the items ordered to the customer without revealing the customer's name, address or other information about the customer to the vendor. In one preferred embodiment, the present invention uses the transaction identifier that is generated once the customer object decides to purchase given items. As shown in step 260, the vendor computer 140, once ready to ship the items, contacts an authorized shipper (*e.g.*, a carrier who has previously contracted with the secure provider) such as carrier computer 180 and

DISH-Blue Spike 842
Exhibit 1005, Page 1181

discloses only the transaction identifier to the carrier computer 180. In another embodiment, the vendor computer 140 provides the carrier computer 180 with the customer object (such as "GOLFO"). As shown in step 270, the carrier computer 180 then contacts the secure provider computer 110 or the bank computer 150 as the case may be, which then matches up the transaction identifier with the customer. The customer information is then relayed by the secure provider computer 110 or bank computer 150 to the carrier computer 180 who can then ship the items directly to the customer now knowing the address of the customer. Thus, while the secure provider and/or the bank and the shipping company know who the customer is, advantageously, the customer's actual identity is shielded from the vendor.

The customer object can also be used for various other purposes. Thus, in another aspect of the invention, the customer object or persona can gather information on behalf of the customer and then can communicate with the customer interactively, through visual and/or aural means, by using interactive computer techniques such as video playback and voice synthesis to allow the persona to verbally and/or textual describe what information was found. Of course, such information can also be provided in traditional formats such as text on the computer screen. In a further aspect of the present invention, vendor/customer object interaction can occur through e-mail and e-mail systems can be used to further vendor/customer relationships at the object or persona level. In addition, through e-mail, the secure provider can make direct offerings to the customer whether or not the secure provider knows the actual identity of the customer. Thus, vendors and the secure provider can send offerings by e-mail to customer objects provided with their own e-mail addresses and the customer object can respond to such e-mails with return e-mail or by visiting the vendor or secure provider web site.

In order to provide for secure transmissions over the Internet, the present invention can use different encryption methods to provide users with anonymity, and to prevent third parties from improperly obtaining a user's credit card number or bank account number. To this end, in one preferred embodiment, the system uses an RSA public key encryption. As is known to those skilled in the computer security art, RSA key technology has two main attributes. First, it can be the basis of a digital signature system.

DISH-Blue Spike 842
Exhibit 1005, Page 1182

Second, it can be used for storing encryption information. In a RSA digital signature system, the public key is used to verify the digital signature. The private key is used to sign one's signature for a block of data. Holder's of public keys can verify a purchase by requesting that the purchaser digitally sign the block of data. If the signature matches up with the public key, the identity of the purchaser has been confirmed, and the seller can go forward and arrange for the shipment of the device with a third party shipper.

The customer computer 100 is preferably provided with a private key, while the public key is stored on the database 130. The public key will contain information such as a customer object and a customer bank account or credit card number. Most importantly, the public key will not include information such as the customer shipping address, as is required in prior art electronic commerce systems. Once the customer computer 100 has a public key and a private key assigned, the customer computer 100 can then dial onto the Internet through the secure provider computer 110 to begin browsing.

When a customer computer 100 enters the web site of the vendor computer 140, the vendor computer 140 is provided with the public key. When a customer computer 100 notifies the vendor computer 140 that the customer would like to make a purchase from the vendor web site 140, the public key, the transaction number and the amount of the purchase is then forwarded by the vendor computer 140 to a bank computer 150. In a preferred embodiment, bank computer 150 will be provided with access to a database 170 of all public keys. The bank computer 150 can then request that the customer computer 100, using the private key, "sign" for the purchase. Based upon the response from the customer computer 100, and upon the customer's credit history, the bank computer 150 decides whether or not the transaction will be approved. Once the transaction is approved, the vendor computer 140 is notified. The vendor computer 140 can then forward the item purchased by the customer with a transaction number or customer object to a third party carrier as explained above. Using this transaction number or customer object, the carrier computer 180 will be able to retrieve the customer's name and home address from the secure provider computer 110, or the bank computer 150, and can then deliver the package to the customer.

In another preferred embodiment of the present invention, customers can opt into having the secure provider track their on-line surfing activities and their preferences. This is in contrast to web sites which track surfing activity unbeknownst to the user. With the present invention, the customer knows ahead of time, by signing up with the secure provider, that the secure provider will be tracking surfing and transactional habits so as to better serve the customer. For example, by monitoring the browsing habits and purchasing habits of customer computers 100, the secure provider computer 110 can determine commonly purchased items or popular vendors. Additionally, the monitoring of browsing habits can aid the secure provider computer 110 in predicting future purchases or services required by the customer object. Using this information, the secure provider can purchase large quantities of items commonly purchased by its members, and act as a wholesaler for its members, making special deals with the vendors.

The customer is encouraged by the secure provider to use and educate the customer object so that the secure provider can have real-time information to provide just-in-time or just-ahead-of-time product offerings to the customer or customer object. The secure provider computer 110, which will have access to all of the customer data, but not necessarily to the customer's identity or address information, can also provide the stored demographic and preference information to vendor computers 140 without compromising the identity of the customer. In this manner, the provider could allow vendors to send information to targeted object groups which would not be bothersome to the customer since his or her object could make the decision whether to accept the offering from the vendor and/or present the offering back to the customer based on the preferences set by the customer. Thus, the customer object identifier can be, in effect, a screener of "unsolicited" offerings from vendor computers 140. Additionally, the secure provider computer 110 can conduct market research with a depth unavailable using traditional methods. Thus, if the customer computers 100 using customer object identifiers stored on the secure provider computers 110 use such object identifiers for many different shopping missions, the secure provider computer 110 would have access to data about the entire buying habits of its customers. For example, the secure provider database 130 would include information indicating that particular consumers like BMW automobiles and golf

sweaters, whereas other consumers like Audi automobiles and cycling jerseys. The secure provider computer 110 could conduct statistical studies to uncover correlations that would identify potential marketing and buying opportunities. For example, without breaching its obligation of confidence with respect to individual consumer information, the secure provider could conduct a market research study for a manufacturer of golf sweaters and advise the manufacturer to focus on BMW owners rather than Audi owners.

In another preferred embodiment of the present invention, vendor computers 140 can provide special offers to be displayed on the web site of the secure provider computer 110. To accomplish this, the secure provider computer 110 can provide a web page which vendor computers 140 can log onto with a standardized form for the vendors to fill out. The secure provider computer 110 can then post each of the standardized forms onto a virtual bulletin board to a web site available only to customer computers 100. The advantage this embodiment provides is that customers need not shop on a non-secure web site to receive the special offers, since the offers will come via the secure provider computer 110. These offers can be posted for all customer computers 100 to see, or can be directed to specific customer computers 100. Further, customers will have the option of deciding whether or not they wish to even see the offer.

In order to prevent price pirating, the vendor advertisements are preferably posted to an area of the web site of the secure provider computer 110 that is only accessible to customer computers 100. Accordingly, vendor computers 140 will not be able to view the offers coming from other vendor computers 140. Alternatively, authorized vendor computers 140 (i.e., vendors signing up with the secured provider to reach the secure provider's customers) may be allowed to see one another's offers but unauthorized vendors cannot see the offers of authorized vendors.

In yet another aspect of the present invention, an interactive, intelligent virtual vendor representative object (such as a virtual salesperson object) is provided as a guide to a given web site. For instance, when accessing a web site of a vendor computer 140, the vendor object can be provided with a persona such that instead of passively navigating through the site, an animated character or vendor persona is encountered by the customer. The vendor persona then takes on the role of a virtual salesperson, asking

questions of the customer and making recommendations based on the responses by the customer. By interaction with the customer object identifier, the vendor object becomes cumulatively knowledgeable, can store customer preferences and history and proactively pursue the vendor/vendee relationship.

Notoriety of the vendor character or persona apart from the web site is desirable and is preferably enhanced through advertising (such as through print media, TV, radio, etc.) such that the persona becomes "branded" or closely associated with the vendor company and serves as a trademark or service mark of the company. The perception by the customer that the vendor character represents the company as a trademark is desirable for a number of reasons, such as to impart a feeling of familiarity with the character when encountered, create a desire on the customer's part to initially visit the web site to interact with the character, and enhance the customer's comfort level in interacting with the character. All of these benefits will then ultimately help the vendor increase traffic to the web site and raise the comfort level of the customer when he or she visits the web site.

In a related aspect of the present inventions, intelligent, virtual customer objects are desirably provided so that the customer need not search the Internet on his own, interact with vendor objects or personae encountered, or deal with the everyday hassles of the Internet (expired URLs, slow connections, information overload, etc.). The customer can be a customer persona which can be visually displayed on the computer screen and be customized or designed to physically resemble the customer's human characteristics or resemble a caricature of the customer, a familiar character, an animal, or any other visible object. Alternatively, the customer object identifier may be nonvisual or simply represented by a file, icon, programming object, etc. Preferably, a customer can set up a customer object with all of the characteristics, personal information, history and demographic information about the customer such that the object identifier, and not the customer, can expend the "effort" of searching the Internet, shopping and gather information useful or desired by the customer. It should be noted that the customer object is likely to be more proficient than the customer in learning to use Internet or Intranet tools that require more effort, knowledge or know how that the average consumer possesses or desires to exercise.

DISH-Blue Spike 842
Exhibit 1005, Page 1186

For instance, a customer object or persona can be provided with individualized characteristics about the customer, such as that the customer is male, 32 years old, a cigar smoker, a wine enthusiast, a tennis player, drives a sedan, owns a house, likes gardening, etc. The more information supplied to the persona, the more the persona takes on the full characteristics of the customer and enables a "smarter" persona when the persona is searching for information. By way of example, if the customer wants the persona to shop for light-weight sweaters in a size large, but customer forgets to tell the persona that he does not like the color red, the persona may collect possible sweaters to buy including unwanted red sweaters. The customer, upon discovering that red sweaters were located by his persona, can add a new characteristic to the persona that he does not like red sweaters for future search purposes. The more information supplied to the persona, the more intelligent it becomes.

The software provided to both the vendors and customer computers can also allow generation of interactive characters. In this regard, the browser of the customer computer could be provided with the necessary "plug-ins" (such as a Java plug-in or ActiveX control) to allow the rendering of an interactive character on the video screen of the customer computer.

Further, by using artificial intelligence (AI) techniques such as neural-network learning, the customer object or persona can be programmed to learn desired and undesired characteristics of the customer based on continued interaction between the persona and the customer and based on existing preferences. Thus, if the customer has the customer persona shop for sweaters, shorts and ties and merchandise is found including red sweaters, red shorts and red ties, and the customer selects such items in colors other than red, the persona can "learn" through AI techniques that the customer likely does not like the color red for clothing items and thus, when sufficiently confident in its assessment, will no longer shop for red clothing. Thus, the more and more the customer interacts with his persona, the "smarter" the persona becomes and interaction between customer and persona is highly encouraged by the present invention.

Another aspect of the present invention is that the vendor objects can interact with the customer objects in a virtual shopping encounter, as if the customer

wandered into the store of the vendor and was approached by a salesperson. The customer object would relate his preferences (or a subset thereof) to the vendor object who may have the items desired by the customer object. If the vendor object, however, does not have such an item in stock, it may use the information of the customer object to intelligently recommend a different item. For instance, if the customer object is looking to buy a BMW or Mercedes but the vendor object only has AUDIs, it may recommend to the customer object that it consider an AUDI since it deduced that this customer may like German-made cars. If the customer object did not specify that it did not like Audi's, it mat accept the recommendation from the vendor object. The more often the vendor object interacts with the customer object, the more each knows or learns of the other's preferences, needs and offerings. Such an ever-growing object interrelationship can greatly enhance the vendor-customer relationship.

As these and other variations and combinations of features discussed above can be utilized without departing from the present invention as defined by the claims, the foregoing description of the preferred embodiments should be taken by way of illustration rather than by way of limitation of the present invention.

INDUSTRIAL APPLICABILITY

The present invention is applicable to the retail industry or elsewhere where vendors may wish to display their goods or services at a web site on the Internet and allow customers to browse and make purchases from a vendor web site anonymously.

CLAIMS:

1. A computer-implemented method of delivering goods purchased from a vendor having a vendor web site accessible over a computer network by a plurality of customers at physical locations, the customers having customer computers connected to the computer network for accessing the vendor web site and electronically purchasing goods from the vendor web site, comprising:

(a) associating the identity and the physical location of each customer with a respective customer object via linking information;

(b) storing said linking information at a secure computer at a location remote from the vendor web site;

(c) anonymously connecting to the vendor web site by the customer computer using the identity of the customer object without revealing the identity and physical location of the customer;

(d) ordering goods at the vendor web site by the customer using the customer computer, and upon initiation of an order by the customer, (i) automatically generating a transaction identifier by the vendor computer, (ii) encoding a package of the goods ordered by the customer with the transaction identifier by the vendor and (iii) sending the transaction identifier together with the customer object to the secure computer by the vendor computer;

(e) associating the transaction identifier sent by the vendor computer with the identity and physical address of the customer at the secure computer using the linking information and automatically forwarding the transaction identifier and associated identity and physical address of the customer to a computer of a common carrier;

(f) delivering the encoded package to the common carrier by the vendor; and

(g) reading the transaction identifier by the common carrier, using the identity and the physical location of the customer associated with the transaction identifier and physically delivering the package to the physical location of the customer.

DISH-Blue Spike 842
Exhibit 1005, Page 1189

2. The method of claim 1, further comprising sending information representing the cost of the goods ordered by the customer and the customer object from the vendor computer to a financial institution computer via the computer network for credit approval, ascertaining the credit status of the customer object, and automatically sending a message approving or declining credit to the customer to the vendor computer from the financial institution computer.

3. The method of claim 2, wherein the secure computer comprises the financial institution computer.

4. The method of claim 2, wherein ascertaining the credit status of the customer object includes ascertaining the identity of the customer based on the linking information obtained by the financial institution from the secure provider.

5. The method of claim 1, wherein the step of anonymously connecting to the vendor web site includes revealing one or more customer characteristics to the vendor web site by the customer object so as to allow the vendor web site to use such customer characteristics to customize information and goods presented to the customer upon return to the vendor web site using the customer object.

6. The method of claim 1, wherein the step of anonymously connecting to the vendor web site is performed automatically without customer interaction on at least some occasions by the customer object programmed to shop for the customer in accordance with directions specified by the customer.

7. The method of claim 1, wherein the customer object is personified to the customer via the customer computer through the display of audio and/or visual display.

8. The method of claim 1, wherein the secure computer comprises a secure provider computer allowing the customers to anonymously connect to the vendor web site therethrough.

9. A computer-implemented method of delivering goods purchased from a vendor having a computer web site accessible over a computer network by a plurality of customers at physical locations, the customers having customer computers connected to the computer network for accessing the vendor computer site and electronically purchasing goods from the vendor web site, comprising:

(a) associating the identity and the physical location of each customer with a respective customer object via linking information;

(b) storing said linking information at a secure computer at a location remote from the vendor web site;

(c) anonymously connecting to the vendor web site by the customer computer using the identity of the customer object without revealing the identity and physical location of the customer;

(d) ordering goods at the vendor web site by the customer using the customer computer, and upon initiation of an order by the customer, encoding a package of the goods ordered by the customer with the customer object;

(e) delivering the encoded package to the common carrier by the vendor;

(f) providing the linking information to the common carrier; and

(g) reading the customer object by the common carrier, retrieving the identity and the physical location of the customer associated with the customer object and physically delivering the package to the physical location of the customer.

10. The method of claim 9, further comprising sending information representing the cost of the goods ordered by the customer and the customer object from the vendor computer to a financial institution computer via the computer network for credit approval, ascertaining the credit status of the customer object, and automatically sending a message approving or declining credit to the customer to the vendor computer from the financial institution computer.

11. The method of claim 10, wherein the secure computer comprises the financial institution computer.

12. The method of claim 10, wherein the secure computer comprises a secure provider computer allowing customers to anonymously connect to the vendor web site therethrough.

13. The method of claim 10, wherein ascertaining the credit status of the customer object includes ascertaining the identity of the customer based on the linking information obtained by the financial institution from the secure provider.

14. The method of claim 9, wherein the linking information is transmitted to a computer of the common carrier via the computer network.

15. The method of claim 9, wherein the step of anonymously connecting to the vendor web site includes revealing one or more customer characteristics to the vendor web site by the customer object so as to allow the vendor web site to use such customer characteristics to customize information and goods presented to the customer upon return to the vendor web site using the customer object.

16. The method of claim 9, wherein the step of anonymously connecting to the vendor web site is performed automatically without customer interaction on at least some occasions by the customer object programmed to shop for the customer in accordance with directions specified by the customer.

17. The method of claim 9, wherein the customer object is personified to the customer via the customer computer through the display of audio and/or visual display.

18. In a computer system for offering goods, services and/or information from a vendor computer providing access to a vendor web site over a computer network including a plurality of customer computers connected to the network for accessing the vendor web site, a computer character generating system comprising:

(a) a character generation program executable on the vendor computer and containing instructions for causing said vendor computer to generate an interactive vendor character which represents the vendor and interactively guides a customer through the vendor computer site,

(b) said character generation program being operative to send character display commands to said customer computer when said customer computer has accessed the vendor web site causing said customer computer to display on a display device associated with the customer computer said interactive vendor character,

(c) said interactive vendor character providing a trademark function for the vendor such that said interactive vendor character is identified with said vendor by customers who desire to acquire goods, services and/or information over the computer network from said vendor web site, said interactive vendor character further having a persona such that said vendor character will respond to inputs from a customer computer

DISH-Blue Spike 842
Exhibit 1005, Page 1192

representing communications by a customer in a manner representative of a human having particular personality traits acting in a representative capacity.

19. A system as claimed in claim 18, wherein said vendor computer records the identities of customer computers which interact with the vendor web site and records historical data representing transactions of each customer computer with the vendor computer, and wherein said vendor character responds to inputs from each customer computer based partially on said inputs and partially on said historical data in conjunction with said personality traits.

20. A system as claimed in claim 19, wherein said vendor character has an artificial intelligence function which allows said vendor character to predict responses which would tend to elicit an acquisition by each customer computer based upon the historical data associated with such customer computer, and said interactive vendor character bases responses at least in part upon such predictions.

21. A system as claimed in claim 20, wherein said vendor character checks for available goods, services and/or information requested by each said customer computer and also checks for goods or services which are different from those requested by said customer computer but which are likely to be of interest to such customer computer based upon the historical data.

22. A system as claimed in claim 18, wherein said vendor character is displayed with facial expressions, movement characteristics and voice accents associated with said personality traits.

23. An interactive computer-implemented method of offering goods, services and/or information from a vendor computer providing access to a vendor web site over a computer network to a plurality of customer computers connected to the network for accessing the vendor web site, comprising:

(a) providing a plurality of customer objects representing individuals who desire to acquire goods, services and/or information from said vendor sites, each said customer object being provided with a set of user characteristics representing personal preferences and information about the individual;

DISH-Blue Spike 842
Exhibit 1005, Page 1193

(b) providing a vendor persona object representing the vendor, said vendor persona object being provided with a set of vendor characteristics representing information about the goods, services and/or information offered by the vendor; and

(c) visiting said vendor computer site via the network with a customer object such that said customer object and said vendor persona object dynamically interact with one another to exchange one or more subsets of said set of user characteristics and vendor characteristics for determining whether the goods, services and/or information offered by the vendor computer site are of interest to said user persona object.

24. The method of claim 23, further comprising targeting a sales offer by a vendor computer to said at least one customer computer via said secure provider computer based upon the purchasing interest and demographic information collected for said at least one customer computer by said secure provider computer and provided to said vendor, wherein said customer object is configured by the customer to determine whether the sales offer will be presented to the customer computer.

25. A method for providing advertising on the web site of a secure provider computer, the method comprising:

(a) providing a secure provider computer to allow customer computers connected to said secure provider computer to have access to authorized vendor offers on the secure provider web site; and

(b) posting one or more vendor offers on the secure provider web site, wherein said offers are only viewable by the customer computers.

26. A computer-implemented method for knowingly monitoring network navigation and purchasing history of a plurality of customers by a secure provider comprising:

(a) requiring each customer to first establish an account with the secure provider by requiring each customer to agree to have the customer's demographic information and purchasing history tracked by the secure provider;

(b) providing on-line access to a computer network to computers of customers who have established an account via a secure provider computer of the secure provider; and

(c) tracking and storing the customers' demographic information and purchasing history by the secure provider computer as the customers update and change their demographic information and make purchases via their customer computers.

27. The method of claim 26, further comprising presenting at least one customer computer with an item to be purchased selected by the secure provider computer based on the customer's demographic information and purchasing history tracked by the secure provider.

28. The method of claim 26, further comprising targeting a sales offer by a vendor computer to at least one customer computer via the secure provider computer based on the customer's demographic information and purchasing history collected by the secure provide computer and provided to the vendor in a modified form which does not include the customers' identity information, wherein said customer object is configured by the customer to determine whether the sales offer will be presented to the customer computer.

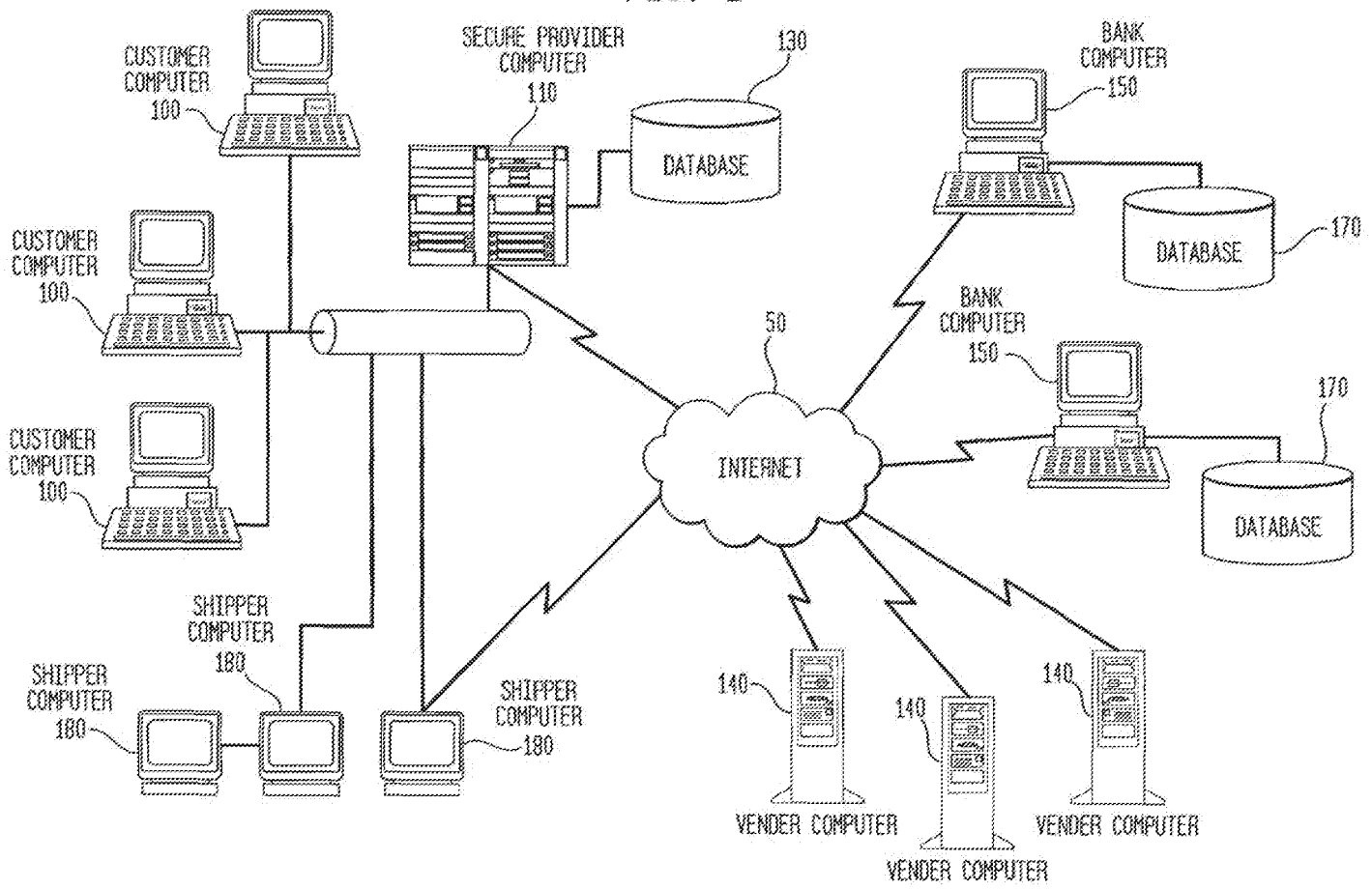
29. A method of providing outside vendor offers on a web site of a secure provider computer comprising:

(a) establishing a secure provider web site allowing member customer computers to have access to an area on the web site that posts outside vendor offers; and

(b) configuring the secure provider web site so that the vendor offers are only viewable by the member customer computers.

30. The method of claim 29, wherein only vendors who have signed up with the secure provider in advance are able to view the area on the web site that posts the outside vendor offers.

FIG. 1



SUBSTITUTE SHEET (RULE 26)

FIG. 2

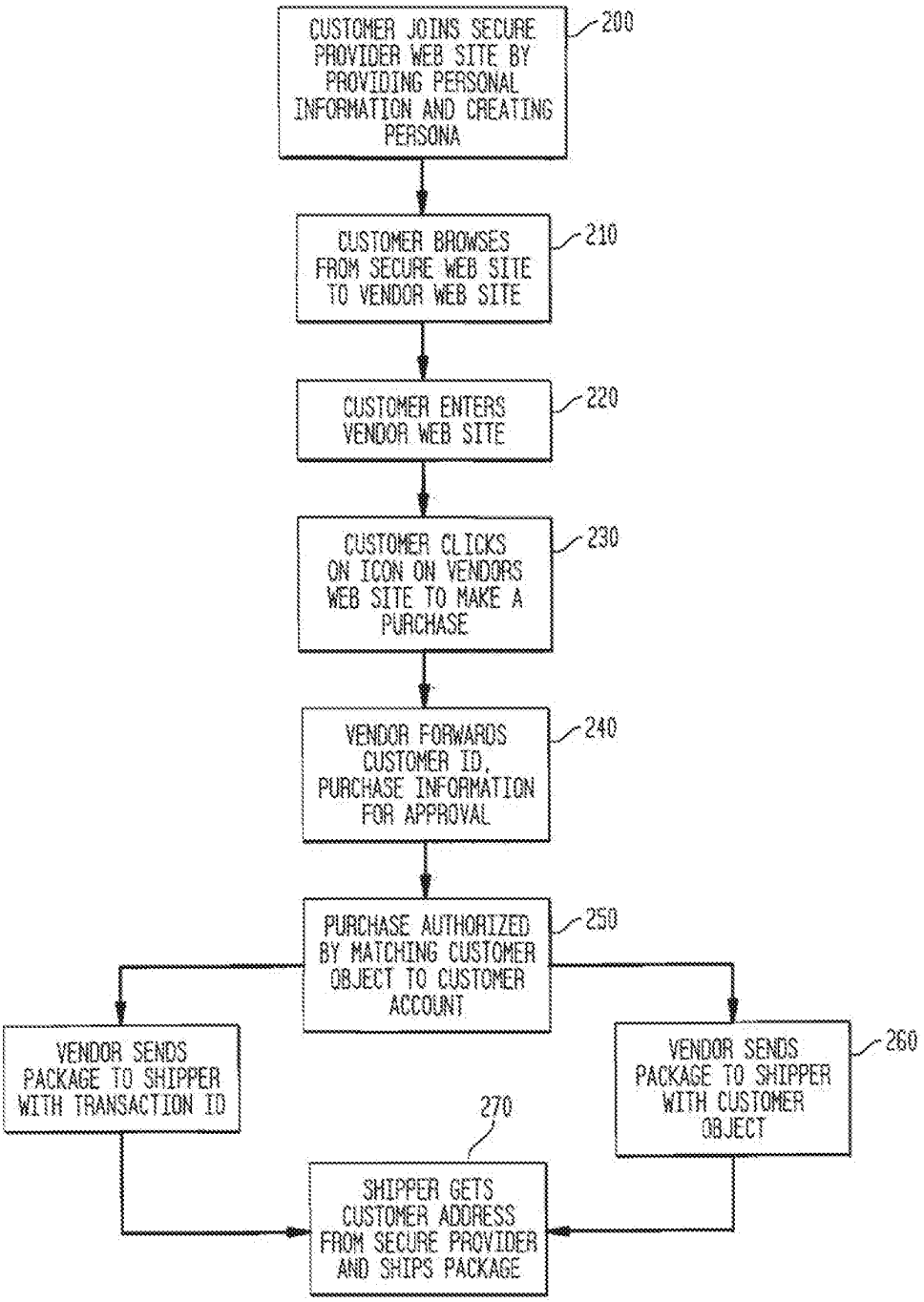

CUSTOMER JOINS SECURE PROVIDER WEB SITE BY PROVIDING PERSONAL INFORMATION AND CREATING PERSONA
200
CUSTOMER BROWSES FROM SECURE WEB SITE TO VENDOR WEB SITE
210
CUSTOMER ENTERS VENDOR WEB SITE
220
CUSTOMER CLICKS ON ICON ON VENDORS WEB SITE TO MAKE A PURCHASE
230
VENDOR FORWARDS CUSTOMER ID, PURCHASE INFORMATION FOR APPROVAL
240
PURCHASE AUTHORIZED BY MATCHING CUSTOMER OBJECT TO CUSTOMER ACCOUNT
250
VENDOR SENDS PACKAGE TO SHIPPER WITH TRANSACTION ID
VENDOR SENDS PACKAGE TO SHIPPER WITH CUSTOMER OBJECT
260
270
SHIPPER GETS CUSTOMER ADDRESS FROM SECURE PROVIDER AND SHIPS PACKAGE

FIG. 3

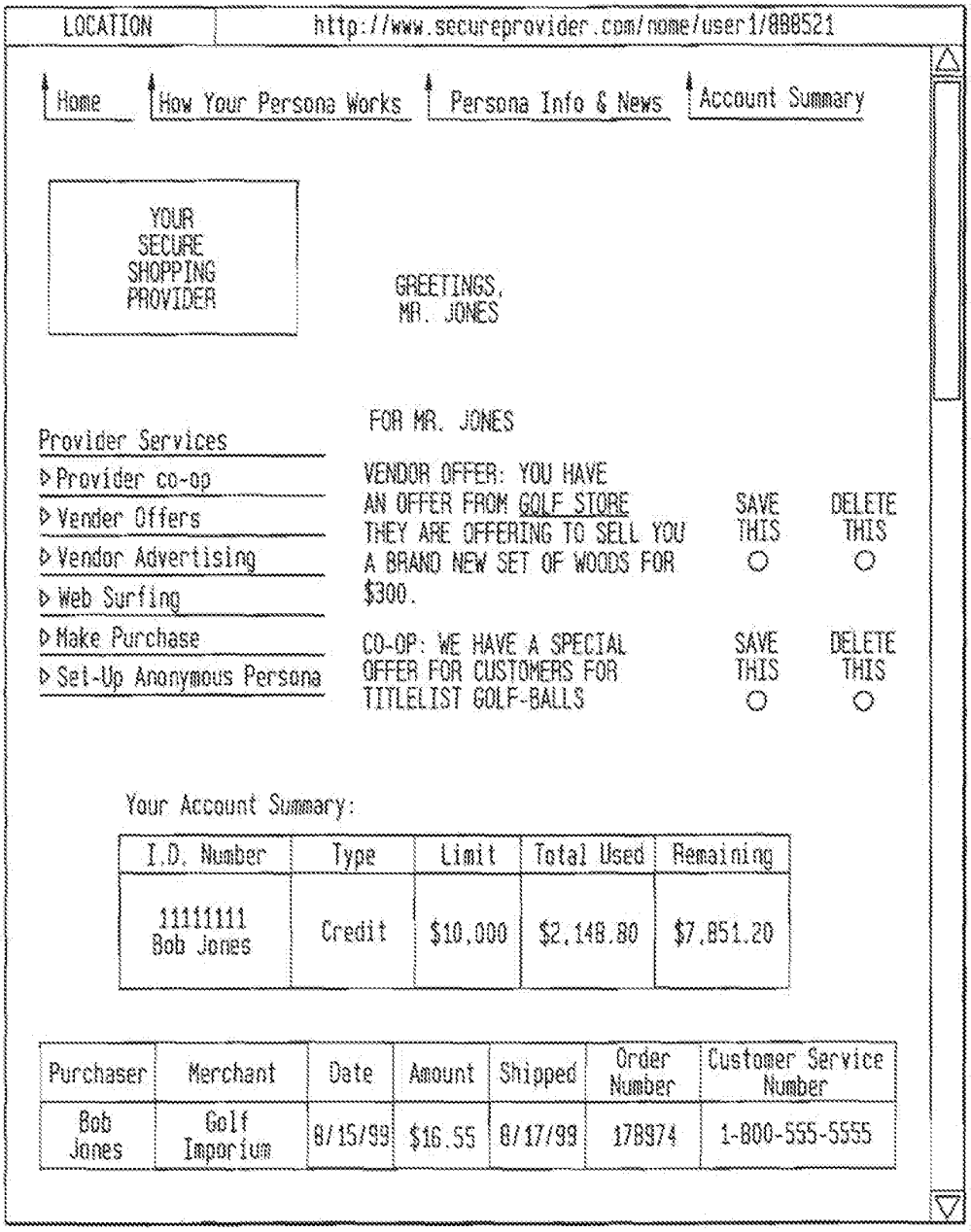
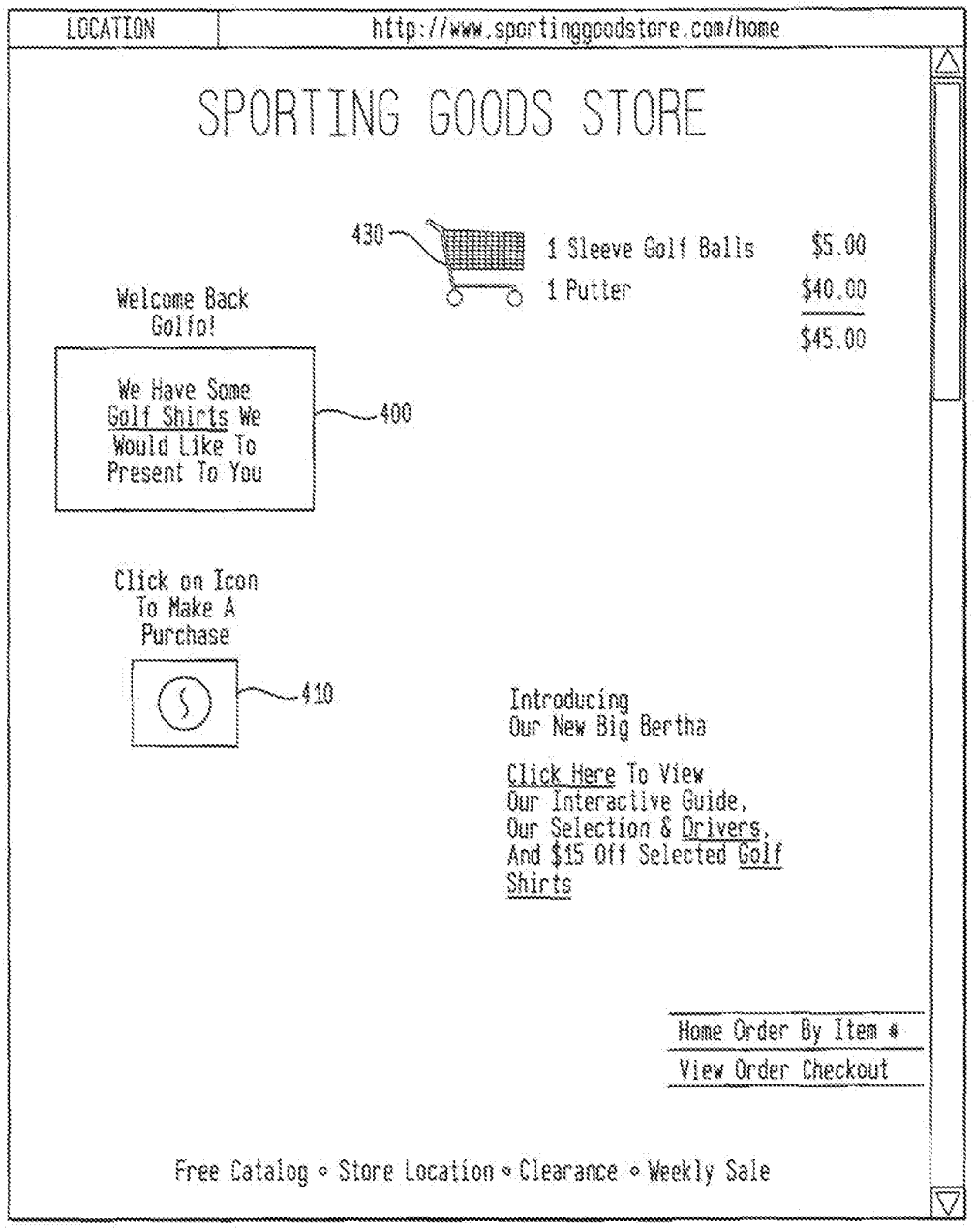

LOCATION
http://www.secureprovider.com/nome/user1/000521
Home
How Your Persona Works
Persona Info & News
Account Summary
YOUR SECURE SHOPPING PROVIDER
GREETINGS, MR. JONES
FOR MR. JONES
Provider Services
Provider co-op
Vender Offers
Vendor Advertising
Web Surfing
Make Purchase
Set-Up Anonymous Persona
VENDOR OFFER: YOU HAVE AN OFFER FROM GOLF STORE THEY ARE OFFERING TO SELL YOU A BRAND NEW SET OF WOODS FOR $300.
SAVE THIS
DELETE THIS
CO-OP: WE HAVE A SPECIAL OFFER FOR CUSTOMERS FOR TITLELIST GOLF-BALLS
SAVE THIS
DELETE THIS
Your Account Summary:
I.D. Number
Type
Limit
Total Used
Remaining
11111111 Bob Jones
Credit
$10,000
$2,148.80
$7,851.20
Purchaser
Merchant
Date
Amount
Shipped
Order Number
Customer Service Number
Bob Jones
Golf Imporium
8/15/99
$16.55
8/17/99
178974
1-800-555-5555

FIG. 4


LOCATION
http://www.sportinggoodstore.com/home
SPORTING GOODS STORE
430
1 Sleeve Golf Balls $5.00
1 Putter $40.00
$45.00
Welcome Back Golfo!
We Have Some Golf Shirts We Would Like To Present To You
400
Click on Icon To Make A Purchase
410
Introducing Our New Big Bertha
Click Here To View Our Interactive Guide, Our Selection & Drivers, And $15 Off Selected Golf Shirts
Home Order By Item #
View Order Checkout
Free Catalog • Store Location • Clearance • Weekly Sale

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/20348

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60
US CL :705/26,27

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/26,27

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

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

DIALOG
search terms: online or electronic shopping, secure

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,E	US 5,970,475 A (BARNES et al) 19 October 1999, see entire document.	1-30
Y,E	US 5,956,699 A (WONG et al) 21 September 1999, see entire document.	1-30
Y,P	US 5,884,272 A (WALKER et al) 16 March 1999, see entire document.	1-30
A	HISEY, P. Internet commerce: Show me the money. Credit Card Management. April 1997. Vol 10. No. 1. pages 68-73.	1-30
A,P	KENWORTHY, K. How safe is the Net? Windows Magazine. December 1998. p. 144.	1-30

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

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"B"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 30 DECEMBER 1999	Date of mailing of the international search report 07 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer E. Todd Voeltz Telephone No. (703) 306-5932

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

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 February 2001 (22.02.2001)

PCT

(10) International Publication Number
WO 01/13275 A1

(51) International Patent Classification⁷: G06F 17/30

(21) International Application Number: PCT/US00/21901

(22) International Filing Date: 10 August 2000 (10.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/374,173 13 August 1999 (13.08.1999) US

(71) Applicant *(for all designated States except US)*: **FLEET-BOSTON FINANCIAL CORPORATION** [US/US]; 100 Federal Street, Boston, MA 02110 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JUNDA, Laurence, E.** [—/US]; 10 McGregor Drive, Sherborn, MA 01770 (US). **GEARHART, Randy, S.** [—/US]; 15 Pine Ridge Circle, Reading, MA 01867 (US).

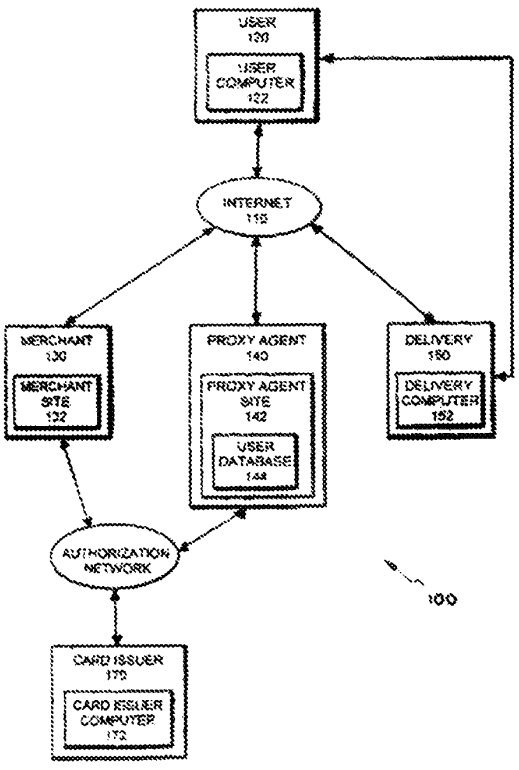
(74) Agents: **BUCKLEY, Linda, M.** et al.; Dike, Bronstein, Roberts & Cushman, Intellectual Property Group, Edwards & Angell, LLP, 130 Water Street, Boston, MA 02109 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, 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 patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: PROXY SYSTEM FOR CUSTOMER CONFIDENTIALITY



(57) Abstract: A system and method for allowing customers to make purchases and take delivery of goods or services with a desired level of security and confidentiality are disclosed. The system and method enable a customer (user) (120) to effect a purchase and a delivery of goods or sevices from a merchant (130) without revealing selected real user data to the merchant. In one embodiment, the system includes proxy user data generator for generating proxy user data (144) corresponding with selected real user data, a database for storing the selected real user data and the corresponding proxy user data, and a purchase authorization request and reply router connectable to a network for routing purchase authorization requests and replies between a system includes a unit for providing real delivery data corresponding with proxy delivery data to a delivery entity (150). The system and method are useful for making purchases and taking delivery from either traditional retail outlets or on-line merchants.

WO 01/13275 A1

DISH-Blue Spike 842
Exhibit 1005, Page 1201

IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

- *With international search report.*
- *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

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.

PROXY SYSTEM FOR CUSTOMER CONFIDENTIALITY

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates generally to information security and confidentiality, and more particularly, to a system and a method for enhancing the security and confidentiality of users who make purchases and take delivery of goods or services. The system and method of the present invention include features that reduce opportunities for unscrupulous individuals or entities to obtain personal user data, and for marketers and others to gather information on the purchasing habits of users, including users who make on-line purchases.

Background

When making purchases of goods or services, customers generally have a variety of payment options available to them with varying levels of confidentiality. For example, customers who pay for their purchases using cash can advantageously maintain their anonymity, because they typically are not required to reveal any personal information to complete the transaction. In contrast, customers who pay for their purchases using credit or debit cards must often present valid identification showing their names and/or residential addresses. At the very least, a customer who uses a credit or debit card must reveal his or her card account number to a merchant, who typically transmits the account number to a third party for validating the account and for obtaining authorization to complete the sale. Further, a customer who takes delivery of his or her purchases at a particular location or via a personal computer must also reveal delivery information such as a shipping address or an e-mail address. As a result, credit or debit card account numbers, information about purchased items, names and addresses of the card holders, etc., can be easily correlated by the merchant and/or the third party and used in their own businesses or sold to others.

This problem is especially acute for customers who make on-line purchases; *i.e.*, customers who purchase goods or services from merchant sites over a public distributed network such as the Internet. Not only can merchants and credit or debit card authorities gain access to a customer's personal information during an on-line transaction, but unscrupulous individuals or entities can also intercept the customer's personal information and/or information about the transaction sent over the network. This can lead to a serious invasion of privacy for the customer and weaken the customer's confidence in the Internet as a viable commercial medium. For example, such unscrupulous individuals or entities may attempt to commit credit card fraud by using intercepted credit card account numbers.

Various systems and methods have been proposed for enhancing customer information security. For example, in US Patent 5,420,926 ("the '926 patent") issued May 30, 1995, to Low et al., a method for making an anonymous non-cash transaction is described. In accordance with that disclosure, a communications exchange is used so that information and/or funds may be transferred without the destination of the transfer knowing the source of the information and/or the funds. Public key encryption is also used so that each party to the transaction and the communications exchange can read only the information the party or the exchange needs for its role in the transaction.

In addition, in US Patent 5,815,665 ("the '665 patent") issued September 29, 1998, to Teper et al., a method of providing an on-line service to a user over a public network is described. According to that disclosure, an on-line brokering service provides user authentication and billing services to allow users to anonymously and securely purchase on-line services from service provider sites over a distributed public network such as the Internet. After performing a user authentication process, the on-line brokering service transmits an anonymous user ID to the service provider site, which can be used by the service provider for subsequently billing the user. A database of user payment information, *e.g.*, credit card numbers and other personal user data, is maintained at the on-line brokering service site and is neither sent over the distributed public network nor exposed to the service provider sites.

However, the methods for enhancing customer information security described in the '926 and '665 patents have some drawbacks. Specifically, if a method for making on-line purchases is to be fully accepted and utilized by customers, then it not only must guard against unauthorized disclosure and use of customer personal information, but it also must be convenient and easy-to-use. Although both the methods of the '926 and '665 patents may be used for enhancing customer information security, they substantially limit the convenience of making on-line purchases by either requiring customers to install and use specialized software on their computers or requiring customers and merchants to communicate indirectly through a third party.

It would therefore be desirable to have a system and a method for making on-line purchases and taking delivery of the purchases that keeps customers' personal information confidential and secure throughout the purchase or purchase and delivery transactions, while still allowing customers and merchants to communicate with each other over the public network without undue interference from any third party. Such a system would be convenient and easy-to-use for all parties involved in purchase and delivery transactions. It would also be desirable to have a system and a method for enhancing customer information security and confidentiality that can be used for both on-line and conventional purchase and delivery transactions.

SUMMARY OF THE INVENTION

The present invention provides a system and a method for enabling a customer (referred to herein as a "user") to make purchases and take delivery of goods or services while keeping some or all of the user's personal information confidential and secure throughout the purchase and delivery transactions. The user's personal information may include, but is not limited to, the user's real name, real residential or shipping address, real e-mail address, and real credit or debit card account number. Before making purchases and/or taking delivery of goods or services, the user obtains proxy personal information for use in place of the user's real personal information during the purchase and/or delivery transactions. Because the user may select the real personal information for which he or she desires

corresponding proxy personal information, a desired level of confidentiality and security in purchase and delivery transactions can be achieved.

An important feature of the present invention is that the user may utilize the proxy personal information in place of the selected real personal information when making purchases and/or taking delivery of goods or services at both traditional retail outlets and on-line merchant sites. By utilizing the proxy personal information when making purchases, the user can obtain virtually the same level of anonymity that cash-paying customers normally enjoy. Further, by utilizing the proxy personal information when making on-line purchases, the user can avoid any potential leakage of his or her real personal information from the on-line network. Moreover, the user can make on-line purchases utilizing the proxy personal information in the same convenient and easy way that he or she would make such purchases using the real personal information.

Another important feature of the present invention is that the proxy personal information may be provided to the user in the form of a proxy credit or debit card. The user utilizes the proxy credit or debit card in the same way that he or she would use a conventional credit or debit card. However, the user may select beforehand the real personal information that he or she desires to be concealed from the merchant when using the proxy credit or debit card. For example, the user may obtain a proxy credit or debit card that incorporates only a proxy credit or debit card account number corresponding with his or her real credit or debit card account number. Accordingly, when the user utilizes the proxy credit or debit card for making purchases, only his or her real credit or debit card account number is concealed from the merchant. In other embodiments of the present invention, the user may obtain a proxy credit or debit card that incorporates proxy personal information corresponding with, *e.g.*, the user's real name, real residential or shipping address, and/or real e-mail address, thereby allowing the user to conceal additional real personal information from the merchant.

Still another important feature of the present invention is that the user may not only select the real personal information for which he or she desires corresponding proxy personal information, but the user may also

select a specific number of purchases that can be made using the proxy personal information, an expiration date for the proxy personal information, and/or a monetary limit for purchases made using the proxy personal information.

The present invention also provides the user with a method for effecting the delivery of the goods or services that conceals the user's real residential or shipping address and/or e-mail address from the merchant. In this embodiment of the present invention, the merchant may deliver goods or services in digital form to the user by utilizing the user's proxy e-mail address. Further, the merchant may deliver goods or services in tangible form to the user by providing the user's proxy residential or shipping address to an accepted delivery service, which obtains the user's corresponding real residential or shipping address and then delivers the goods or services to the user.

In accordance with the present invention, a method of enabling a user to effect a purchase of goods or services from a merchant, without revealing selected real user data to the merchant, includes the steps of generating proxy user data corresponding with the selected real user data; maintaining a database including the selected real user data and the corresponding proxy user data for use in translating the selected real user data into the corresponding proxy user data, and in translating the proxy user data into the corresponding selected real user data; and, routing purchase authorization requests and replies between the merchant and a purchase authorization entity using the selected real user data and the corresponding proxy user data in the database, wherein the requests routed to the purchase authorization entity include the selected real user data, and the replies routed to the merchant include the corresponding proxy user data and do not include the selected real user data.

According to one embodiment of the present invention, the proxy user data can be used for making a selected number of purchases. According to other embodiments, the proxy user data has a selected expiration date and/or a selected monetary limit.

In accordance with another embodiment of the present invention, the method of enabling a user to effect a purchase of goods or services from a merchant, without revealing selected real user data to the merchant, further includes a step of effecting a delivery of the goods or services to the user, wherein the selected real user data does not include either a real name/real shipping address or a real e-mail address.

According to still another feature of the present invention, the goods or services have digital form, and the merchant delivers the digital goods or services directly to the user computer over a network.

According to yet another feature of the present invention, the selected real user data includes a real e-mail address and the corresponding proxy user data includes a proxy e-mail address, and the merchant delivers the digital goods or services to the user utilizing the proxy e-mail address.

In accordance with yet another embodiment of the present invention, the merchant provides the proxy shipping address to a delivery entity, and the method of enabling a user to effect a purchase and delivery of goods or services from the merchant, without revealing selected real user data to the merchant, further includes steps of receiving a request for the real shipping address from the delivery entity, the request including the proxy shipping address; translating the proxy shipping address into the real shipping address using the database; and, providing the real shipping address to the delivery entity for use in subsequently delivering the goods or services to the user.

In accordance with yet another embodiment of the present invention, a method of enabling a user to effect a purchase of goods or services from a merchant using a funding account, includes the steps of generating user account data for the funding account, the user account data having at least one restricted-use attribute; maintaining a database including the user account data; and, routing purchase authorization requests and replies between the merchant and a purchase authorization entity using the user account data in the database, wherein the at least one restricted-use attribute of the user account data is selectable by the user.

DISH-Blue Spike 842
Exhibit 1005, Page 1208

According to another feature of the present invention, the at least one restricted-use attribute corresponds with a selected number of purchases that can be funded using the funding account. According to other features, the at least one restricted-use attribute corresponds with a selected period of time during which purchases can be funded using the funding account, and/or a selected monetary limit for the purchases.

In accordance with another embodiment of the present invention, a method of enabling a user to effect a delivery of goods or services from a merchant, without revealing real delivery data to the merchant, includes the steps of generating proxy delivery data corresponding with the real delivery data; maintaining a database including the real delivery data and the corresponding proxy delivery data for use in translating the proxy delivery data into the corresponding real delivery data; and, providing the real delivery data corresponding with the proxy delivery data to a delivery entity, wherein the user provides the proxy delivery data to the merchant, and wherein the merchant provides the goods or services and the proxy delivery data to the delivery entity for subsequent delivery of the goods or services to the user. The delivery data may include the user's name and/or shipping address.

Still further aspects and advantages will become apparent from a consideration of the ensuing description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood by reference to the following more detailed description and accompanying drawings in which

FIG. 1 is a block diagram of the general architecture of a system that operates in accordance with one embodiment of the present invention;

FIG. 2 is a flow chart showing the steps performed when a user requests proxy user data from a proxy agent according to one embodiment of the present invention;

FIG. 3 is a flow chart showing the steps performed when a user makes an on-line purchase of goods or services according to one embodiment of the present invention; and

FIG. 4 is a flow chart showing the steps performed when the purchased goods or services are delivered to the user according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The systems and methods of the present invention will be illustrated by an embodiment that provides proxy data to a customer, including a proxy name, a proxy shipping address, a proxy e-mail address, and/or proxy credit or debit account data, to provide customer anonymity from the ordering of goods or services to the delivery of the goods or services. However, varying levels of anonymity may be provided in accordance with the present invention, and delivery is optional. In some embodiments, the customer will be provided with only proxy credit or debit account data; and, in other embodiments, the customer will be provided with complete anonymity of identity and location, from the point of purchase to the point of delivery of the goods or services. It should be understood that this detailed description of the present invention is by way of illustration only, and is not intended to limit its scope.

FIG. 1 shows the general architecture of a system 100 that allows a customer to make purchases and take delivery of goods or services while keeping the customer's personal information, *e.g.*, his or her name, shipping address, e-mail address, and/or credit or debit card account number (also known as a "funding account number"), confidential and secure throughout the purchase and the delivery processes.

In this illustrative embodiment, the system 100 includes at least one customer 120 (referred to herein as a "user") having a user computer 122, at least one merchant 130, at least one delivery provider 150 having a delivery computer 152, and at least one proxy agent 140. Each of the computers 122 and 152 are connectable to an untrusted public network 110 such as the Internet. The system 100 further includes a merchant site 132 and a proxy agent site 142, which are directly accessible sites on the Internet 110.

For example, the merchant site 132 and the proxy agent site 142 are accessible on the Internet 110 via a transmission control protocol/Internet protocol (TCP/IP) connection.

In addition, the system 100 includes at least one credit or debit card issuer 170 having a card issuer computer 172 connectable to a network 112 that supports the authorization of credit or debit card transactions. In other preferred embodiments of the present invention, the proxy agent 140 and the card issuer 170 are the same entity. Further, the authorization network 112 may be either a private or a public network, and may also include more than one network.

The card issuer computer 172 communicates with the proxy agent site 142 and the merchant site 132 over the authorization network 112 using a protocol such as any of those conventionally used for processing electronic transactions. Accordingly, software running on the merchant site 132 and the proxy agent site 142 support both the Internet protocol and the banking protocol and can therefore perform the transition in communication from the Internet 110 to the authorization network 112 and vice versa.

The user 120 and the delivery provider 150 utilize the user computer 122 and the delivery computer 152, respectively, to connect to the Internet 110 in any conventional manner. For example, connection between the computers 122 and 152 and the Internet 110 may be made using a modem (not shown) and a telephone line (not shown) via a network service provider (not shown) that is directly connected to the Internet 110. It should be noted that the particular mechanism of how the user computer 122 and the delivery computer 152 form connections with the Internet 110 are not critical to the present invention.

It should also be noted that the user computer 122 and the delivery computer 152 are conventional in design, each typically including a housing that encloses a processor and supporting integrated circuitry, a floppy drive, and a hard disk drive. Each of the computers 122 and 152 also typically includes a keyboard, a mouse, and a monitor for allowing users to enter commands and observe results. For example, the user 120 may enter commands for making purchase selections and observing results such as

DISH-Blue Spike 842
Exhibit 1005, Page 1211

purchase confirmations while making on-line purchases from the merchant site 132 utilizing the user computer 122.

Specifically, the user computer 122 is capable of running a client application, *e.g.*, a browser, which can initiate connections with one or more host machines (not shown) that contain desired sites, *e.g.*, the merchant site 132 and the proxy agent site 142, pass data back and forth between the user computer 122 and the host machines, and then close the connections. Accordingly, the host machines are capable of running server applications that can accept the connections initiated by the client application through the Internet 110. Again, details of how the host machines, the client applications, and the server applications operate are not critical to the present invention, and may take different forms.

The proxy agent 140 may be a bank or other institution that routes purchase authorization requests and replies between merchants (*e.g.*, the merchant 130) and card issuers (*e.g.*, the card issuer 170). Further, the proxy agent site 142 can communicate with the user computer 122, the merchant site 132, the delivery computer 152, and the card issuer computer 172, and pass data back and forth during the purchase and delivery transactions. Although FIG. 1 shows only one proxy agent 140 and only one proxy agent site 142, it should be understood that the system 100 may include a plurality of such proxy agents and sites. For example, different proxy agents and sites might be provided to serve users residing in different geographical areas.

As mentioned above, the system 100 allows a user to make purchases and take delivery of goods or services while keeping some or all of the user's personal information confidential and secure throughout the purchase and delivery transactions. To this end, the proxy agent site 142 includes at least one user database 144 for storing not only the user's personal information such as his or her real name, real shipping address, real e-mail address, and real credit or debit card account number, but also corresponding proxy data such as a proxy name, a proxy shipping address, a proxy e-mail address, and a proxy credit or debit card account number. In accordance with one preferred embodiment of the present invention that provides the highest level of security and confidentiality, the user 120 makes purchases

from the merchant 130 and takes delivery of tangible goods from the delivery provider 150 using only the proxy user data stored in the user database 144, thereby preventing the merchant 130 and others from tracking the user's buying habits and substantially reducing the risk that unscrupulous individuals or entities will intercept, *e.g.*, the user's real credit or debit card account number, and charge unauthorized purchases to his or her account.

For this illustrative embodiment, a procedure will now be described for making purchases and taking delivery of goods or services using the system 100. First, the user 120 registers with the proxy agent 140 for obtaining proxy user data that he or she can use when making purchases and taking delivery of goods or services. The proxy agent 140 then provides the proxy user data to the user 120.

For example, the user 120 registers with the proxy agent 140 according to the procedure shown in FIG. 2. Specifically, the user 120 visits the proxy agent site 142, in block 200, in any conventional manner. For example, the user 120 may utilize an appropriate uniform resource locator (URL) for instructing the web browser running on the user computer 122 to use a particular protocol, *e.g.*, http, to retrieve the home page (not shown) of the proxy agent site 142, *e.g.*, proxy_home.html, located on a particular host machine (not shown), *e.g.*, www.your_bank.com.

Next, the user 120 requests, in block 202, proxy user data from the proxy agent 140. In this illustrative embodiment, the user 120 has a credit or debit card for which he or she requests proxy user data. In a preferred embodiment, the user 120 holds a credit or debit card issued by the proxy agent 140. Accordingly, the user 120 utilizes the home page of the proxy agent 140 to access, *e.g.*, a proxy data request form (not shown). Next, the user 120 fills out the request form including his or her real user data, *e.g.*, real name, real shipping address, and real e-mail address, and then sends the filled-out request form to the proxy agent site 142. It should be understood that the user 120 might alternatively register with the proxy agent 140 without using the user computer 122. For example, the user 120 may utilize the telephone network or regular mail service for providing his or her real user data to the proxy agent 140 during the registration procedure.

In the embodiment wherein the proxy agent 140 has issued the credit or debit card held by the user 120, the user's real credit or debit card account number is already available to the proxy agent 140, and may therefore be easily accessed by the proxy agent 140 for providing a corresponding proxy credit or debit card account number to the user 120. Accordingly, in this preferred embodiment, there is no need for the user 120 to send his or her real credit or debit card account number to the proxy agent 140 over the Internet 110. The software running on the proxy agent site 142 simply utilizes the user's real name, real shipping address, and/or real e-mail address provided on the request form for verifying the existence of the account and determining whether the purchase amount may be charged against the account.

If it is determined, for example, that the user 120 is the holder of a credit or debit card issued by the proxy agent 140, payments have been timely made, and there are funds available on the credit or debit card, then the software on the proxy agent site 142 generates, in block 204, unique proxy user data corresponding with the user's real name, real shipping address, real credit or debit card account number, and real e-mail address, and then provides the generated proxy user data to the user 120 for subsequent use. The user 120 may also be provided with, *e.g.*, an identification number and/or a password for use in making subsequent requests for proxy data. Further, the user 120 may be provided with multiple sets of proxy data, each set corresponding with the user's real data. The proxy user data and the user's identification number/password may be sent to the user computer 122 over the Internet 110 via e-mail or via the client/server applications running on the user computer 122 and the host machine of the proxy agent site 142. It also should be understood that the proxy agent 140 may alternatively utilize the telephone network or regular mail service for providing the proxy user data to the user 120.

In the embodiment of the present invention wherein the credit or debit card held by the user 120 was not issued by the proxy agent 140, the user 120 would also include his or her real credit or debit card account number with the other real user data on the proxy data request form. However, in this embodiment, the server application running on the host

DISH-Blue Spike 842
Exhibit 1005, Page 1214

machine of the proxy agent site 142 preferably encrypts all of the real user data provided on the proxy data request form before the form is sent from the user computer 122 to the proxy agent site 142, thereby minimizing the chance that an unscrupulous individual or entity will intercept and utilize the user's real credit or debit card account number. Alternatively, the user 120 may utilize the telephone network or regular mail service for providing his or her real credit or debit card account number to the proxy agent 140.

Finally, the software on the proxy agent site 142 updates, in block 206, the user database 144 to include the generated proxy user data and ensure that the generated proxy user data accurately corresponds with the real user data, which is also stored in the database 144 for facilitating translations between the generated proxy user data and the real user data. An illustrative portion of the contents of the updated user database 144, including the real user data and the corresponding proxy user data of the user 120, is shown below in TABLE I.

TABLE I

	PROXY USER DATA	REAL USER DATA
USER NAME	AC Member 4325	Jane Doe
USER ADDRESS	AC Proxy Agent Courier – Acct. #4325 Anycity, USA 00000	123 Main Street Apt. #2 Anytown, USA 11111
E-MAIL ADDR.	AC4325@proxyagent.net	jdoe@anyisp.net
FUNDING ACC'T. 1234	XXXX XXXX XXXX 4325	XXXX XXXX XXXX

The illustrative proxy user data and real user data corresponding with the funding account information is shown in TABLE I using the symbol, X, which represents any number from 0 to 9. Complete illustrative funding account numbers are not shown in TABLE I so as not to reproduce any funding account numbers currently in use.

As mentioned above, the software on the proxy agent site 142 generates the proxy user data and then may provide the proxy user data to the user computer 122 for subsequent use by the user 120. Significantly, the proxy user data, which may include the proxy name, the proxy shipping address, the proxy e-mail address, and the proxy credit or debit card

account number of the user 120, is sent to the user computer 122 directly or via e-mail over the Internet 110. As a result, it is foreseeable that an unscrupulous individual or entity may try to intercept the proxy user data at this point in the transaction and then use the proxy user data to make unauthorized purchases.

However, the present invention reduces the risk of such unauthorized use, because it is not only for securely and confidentially allowing customers to make purchases of goods or services, but it is also for allowing customers to take delivery of the goods or services. For this reason, the generated proxy user data preferably includes the proxy shipping address and/or the proxy e-mail address for use in delivering the purchased goods or services. In the preferred embodiment, the purchased goods or services are delivered only to the real address corresponding with the proxy shipping address or the proxy e-mail address. As a result, even if, *e.g.*, an unscrupulous individual intercepted the proxy user data and made an unauthorized purchase, the purchased goods or services would be delivered to the real address corresponding with the proxy shipping address or the proxy e-mail address, and not to the unscrupulous individual. Such individuals would therefore be deterred from intercepting and using the proxy user data because no benefit would be derived therefrom.

Alternatively, some proxy user data may be sent to the user 120 separately from other proxy user data. For example, the proxy name, the proxy shipping address, and the proxy e-mail address may be sent to the user computer 122 over the Internet 110, while the proxy credit or debit card account number is sent to the user 120 via the telephone network or regular mail.

The present invention also minimizes the risk of unauthorized use of proxy user data by optionally making the proxy user data valid for only a limited number of purchases or requiring the user to make a purchase only within a limited period of time. These important features of the present invention will be described in further detail later in this specification.

This illustrative procedure for making purchases and taking delivery of goods or services also includes communications between the user 120

and the merchant 130, and between the merchant 130 and the proxy agent 140. For example, the user 120 communicates with the merchant 130 for making a purchase. The merchant 130 then requests authorization from the proxy agent 140 for charging the user's credit or debit card account for the purchase, and receives either the requested authorization or a refusal to charge the account from the proxy agent 140. Finally, the merchant 130 provides the user 120 with a confirmation of the purchase transaction.

For example, purchases are made and confirmations are provided in accordance with the procedure shown in FIG. 3. Again, the user 120 visits the merchant site 132, in block 300, in any conventional manner. Next, the user 120 utilizes the client application running on the user computer 122 for attempting to make a purchase of goods or services in block 302.

There are many hundreds of merchant sites currently available from which users may make purchases of various types of goods or services. One such merchant site is operated by AMAZON.COM™, Inc., Seattle, Washington, USA. For example, a user may access the AMAZON.COM™ merchant site and select, *e.g.*, books, music, or video products for subsequent purchase. When the user is finished making his or her purchase selections, he or she then typically provides a real name, a real e-mail address, a real shipping address, and a real credit or debit card account number for allowing the AMAZON.COM™ merchant to process and fulfill the purchase order, and then notify the user of the status of the purchase order.

According to the present invention, instead of providing, *e.g.*, the AMAZON.COM™ merchant site with a real name, a real e-mail address, a real shipping address, and a real credit or debit card account number when attempting to make a purchase in block 302, the user 120 provides the merchant site 132 with the proxy user data obtained from the proxy agent 140 in block 204 (see FIG. 2). In this way, the proxy user data acts as a substitute for the user's real data. The system 100 depicted in FIG. 1 may therefore be regarded as a proxy system for maintaining the user's confidentiality during a purchase transaction.

Next, the merchant 130 logs onto the authorization network 112, in block 304, for requesting authorization to charge the user's credit or debit card account for the selected purchase. Accordingly, the proxy user data including the proxy credit or debit card account number is sent over the authorization network 112 from the merchant site 132 to the proxy agent site 142. The software on the proxy agent site 142 then accesses the user database 144 for translating the proxy user data into the real user data, *e.g.*, the proxy credit or debit card account number into the real credit or debit card account number.

If the proxy agent 140 is the bank or other institution that issued the credit or debit card held by the user 120, then the software on the proxy agent site 142 utilizes the real user data obtained from the user database 144 for again verifying the existence of the account and determining whether the purchase amount may be charged against the account. Alternatively, if the proxy agent 140 is not the bank or other institution that issued the credit or debit card to the user 120, then the software on the proxy agent site 142 translates the proxy user data into the corresponding real user data, *e.g.*, the real credit or debit card account number, utilizing the user database 144, substitutes the proxy user data in the authorization request with the corresponding real user data, and then routes the authorization request to the card issuer 170 over the authorization network 112.

Next, the card issuer 170 sends a response to the authorization request to the proxy agent site 142 over the authorization network 112. The software available through the proxy agent site 142 then substitutes any real user data included in the generated authorization information with the corresponding proxy user data, and then routes the authorization information to the merchant site 132 over the authorization network 112 in block 306. A message including a purchase confirmation is then sent, in block 308, from the merchant site 132 to the user computer 122 directly or via the proxy e-mail address over the Internet 110. The message may also include a delivery confirmation, *e.g.*, a shipping or delivery tracking number. Clearly, if the merchant 130 did not receive the necessary authorization information from the proxy agent 140, then the message sent in block 308 would instead include a refusal of the purchase order.

Advantageously, the user 120 is not required to send any real user data to the merchant 130 at any point in the procedure defined by blocks 300 through 308. Further, the proxy agent 140 does not reveal any of the real user data stored in the user database 144 to the merchant 130 at any point during the purchase transaction. Accordingly, complete user confidentiality in purchase transactions is achieved in this illustrative, non-limiting embodiment of the present invention.

This illustrative procedure for making purchases and taking delivery of goods or services further includes communications between the user 120 and the merchant 130, and also communications between the user 120, the merchant 130, the proxy agent 140, and the delivery provider 150. For example, if the purchased goods or services have digital form, then they are sent from the merchant site 132 to the user computer 122 directly or via e-mail over the Internet 110. Alternatively, if the purchased goods or services have tangible form, then the merchant 130 provides them to the delivery provider 150, which then delivers the goods or services to the user 120.

For example, the purchased goods or services are delivered to the user 120 in accordance with the procedure shown in FIG. 4. First, it is determined, in block 400, whether or not the goods or services have digital form. If the goods or services have digital form, then they are sent to the user 120 over the Internet 110, in block 402, by directly downloading them from the merchant site 132 to the user computer 122. For example, digital goods or services can be directly downloaded in a conventional manner via the client and server applications running on the user computer 122 and the host machine of the merchant site 132. Alternatively, the digital goods or services may be sent from the merchant 130 to the user 120 over the Internet 110 as, *e.g.*, an attachment to an e-mail message.

It should be noted that if the digital goods or services are sent from the merchant 130 to the user 120 as an attachment to an e-mail message, then the e-mail message is sent by the merchant 130 to the proxy e-mail address, which was provided to the merchant site 132 along with the other proxy user data in block 302 (see FIG. 3). For example, the e-mail message may be directed to the proxy agent site 142 via the proxy e-mail address.

The software on the proxy agent site 142 may then access the user database 144 for translating the proxy e-mail address into the real e-mail address. Finally, the proxy agent site 142 may redirect the e-mail message to the user computer 122. Alternatively, the merchant 130 may direct the e-mail to the user's real e-mail address, if the user 120 so desires.

Alternatively, if the goods or services have tangible form, then the merchant 130 provides the goods or services to the delivery provider 150 in block 404, who subsequently delivers the goods or services to the user's real shipping address. It should be noted that details of how the merchant 130 provides the goods or services to the delivery provider 150 are not critical to the present invention.

Specifically, when the merchant 130 provides the tangible goods or services to the delivery provider 150, the merchant 130 includes the proxy name and the proxy shipping address of the user 120. For example, a message may be generated and sent, in block 406 from the merchant site 132 to the delivery computer 152 including the proxy name and the proxy shipping address of the user 120. A message confirming receipt of the user's proxy name and proxy shipping address may then be sent, in block 408, from the delivery computer 152 to the merchant site 132. Alternatively, the merchant 130 may utilize the telephone network or regular mail service for providing the user's proxy name and proxy shipping address to the delivery provider 150.

Next, the delivery provider 150 visits the proxy agent site 144, in block 410, over the Internet 110 or a private network, and requests the real user data that corresponds with the proxy user data sent in block 406. The software on the proxy agent site 142 then accesses the user database 144 for obtaining the user's real name and real shipping address, and then generates and sends a message back to the delivery computer 152, in block 412, including this real user data. Alternatively, the delivery provider 150 may utilize the telephone network or regular mail service for obtaining the user's real name and real shipping address from the proxy agent 140.

In this illustrative embodiment, the merchant 130 might also send the user's proxy e-mail address to the delivery provider 150 in block 406; or,

the proxy agent 140 might also send the user's proxy e-mail address to the delivery provider 150 in block 412. This would allow the delivery provider 150 to send an e-mail message to the user 120 for confirming the upcoming delivery of the tangible goods or services. The delivery provider 150 then delivers the tangible goods or services to the user's real shipping address, in block 414.

As described above, all of the user's proxy data, which includes all of the data the user 120 requires to make a purchase and take delivery of the purchase, may be sent through the Internet 110 during the execution of at least two steps in the procedure of the present invention. For example, all of the user's proxy data may be sent from the proxy agent site 142 to the user computer 122 over the Internet 110 in block 204 (FIG. 2). Similarly, all of the proxy data may be sent from the user computer 122 to the merchant site 132 over the Internet 110 in block 302 (FIG. 3) when the user attempts to make an on-line purchase. Even though this proxy data does not include any real user data, an unscrupulous individual or entity may try to intercept the proxy user data at these steps in the procedure and attempt to make an unauthorized purchase using the proxy user data. It is important to note that the merchant 130, especially an on-line merchant, has no way of knowing whether or not the proxy user data was provided to him or her by a bona fide customer, *i.e.*, the user 120.

For this reason, in another preferred embodiment of the present invention, the proxy user data provided by the proxy agent 140 to the user 120 is preferably valid for making only a limited number of purchases, *e.g.*, one and only one purchase. If the user 120 attempts to make an on-line purchase within a relatively short period of time after receiving the proxy user data from the proxy agent 140, then the probability that an unscrupulous individual or entity would intercept the proxy user data and then attempt to make a purchase with the proxy user data within this short period of time is reduced.

However, it is possible that the user 120 may wait a significant period of time before attempting to make a purchase after he or she receives the proxy user data from the proxy agent 140. The proxy user data is therefore more preferably valid not only for a limited number of purchases, but also

DISH-Blue Spike 842
Exhibit 1005, Page 1221

for a limited period of time, *e.g.*, one to twenty-four hours. Therefore, even though the user 120 may decide not to make any purchases after receiving the proxy user data, an unscrupulous individual or entity would not be able to make unauthorized use of the proxy user data after the expiration of the one to twenty-four hour period.

The number of purchases that can be made using the proxy user data, and the expiration period of the proxy user data, may be set at the time the proxy agent 140 provides the proxy user data to the user 120. Alternatively, the user 120 may specify both the number of purchases he or she wishes to make and the expiration period in the proxy data request form in block 202 (FIG. 2). The software on the proxy agent site 142 would then store the specified number of purchases and the specified expiration period in the user database 144 along with the rest of the proxy user data. Further, while routing purchase authorization requests and replies between merchants and card issuers, the proxy agent may also check the user database 144 for determining whether the specified number of purchases has been exceeded or whether the specified time period has expired.

Numerous advantages can be derived from using the proxy system 100 and the procedures of the present invention. For example, the present invention allows users to make purchases and take delivery of the purchases securely and confidentially, especially when making on-line purchases over an untrusted distributed public network such as the Internet. Security is enhanced during the purchase and delivery transactions by only allowing delivery of the purchased goods or services directly to the user computer 122, to the user's e-mail address, or to the user's shipping address. Security is further enhanced by providing proxy user data that can be used only for a limited number of purchases and/or only for a limited period of time. Providing confirmations of transactions at various steps in the procedures still further enhances security. For example, the merchant site 132 provides a confirmation of an on-line purchase at block 308 (FIG. 3); and, the delivery provider 150 provides confirmation of the receipt of proxy user data and an upcoming delivery to the user's real shipping address in blocks 408 and 414, respectively.

In addition, user confidentiality is enhanced during the purchase and delivery transactions by providing proxy user data in place of the user's real name, real shipping address, real e-mail address, and/or real credit or debit card account number. Because the merchant 130 has access to only the proxy user data during the purchase and delivery transactions, it is impossible for him or her to identify the user 120 and track the user's buying habits. This gives users who make credit and/or on-line purchases virtually the same anonymity that cash-paying customers normally enjoy.

In addition, in many embodiments, none of the user 120, the merchant 130, the delivery provider 170, or the card issuer 170 require specialized software on his or her computing system when using the proxy system 100 of the present invention. This is typically the case when the proxy system 100 is used with conventional distributed public networks and conventional authorization networks.

In addition, the proxy system 100 is both convenient and easy-to-use. For example, after obtaining proxy user data from the proxy agent 140, the user 120 visits merchant sites, *e.g.*, the merchant site 132, and makes on-line purchases in the conventional manner with the exception that the user 120 utilizes the proxy user data to make the purchases instead of his or her real user data. The merchant 130 also communicates with the user 120 in the same conventional manner with the exception that he or she receives the proxy user data instead of the real user data. Further, the merchant 130 communicates with the proxy agent 140 as he or she would with a conventional credit or debit card authorization service.

Having described one embodiment, numerous alternative embodiments or variations might be made. Specifically, it was described that the user requests and receives proxy user data from the proxy agent over an untrusted public network such as the Internet. However, this is merely one illustrative example. Further, it should be understood that the manner in which the user requests and obtains the proxy user data from the proxy agent is not critical to the invention. For example, the user might alternatively request and obtain the proxy user data from the proxy agent over a trusted private network or a telephone network. In these alternative embodiments, the probability of an unscrupulous individual or entity

intercepting either the real user data or the proxy user data would be further reduced.

In addition, it was described that a message is generated and sent from the merchant site directly to the user computer for confirming a purchase transaction. However, this is also merely one illustrative example. The purchase confirmation generated at the merchant site might alternatively pass through the proxy agent site before being sent to the user computer. As a result, the proxy agent would be able to maintain a record of the purchase transaction and store the record in the user database along with the user's real data and proxy data. The user may then access these records for keeping track of his or her purchases made using the proxy user data.

In addition, it was described above that the merchant provides tangible goods or services to a particular delivery provider for subsequent delivery to the user's real shipping address. However, this is merely another illustrative example. The user may alternatively specify the delivery provider from a list of delivery providers that are approved for receiving proxy user data and obtaining corresponding real user data from the proxy agent. This would further enhance the security of the user's personal information.

In addition, it was described above that the delivery provider visits the proxy agent site over the Internet or a private network, and requests the real user data that corresponds with the proxy user data. However, when the delivery provider requests a translation of the proxy shipping address into the real shipping address over a private network, specialized software may be required on a computing system available to the delivery provider. To avoid the need for specialized software, the merchant may alternatively provide the tangible goods and the proxy shipping address to any delivery provider, who then delivers the tangible goods with the proxy shipping address to the proxy agent. Next, the proxy agent may provide the tangible goods and the corresponding real shipping address to the delivery provider specified by the user, who then delivers the tangible goods to the user's real shipping address. As a result, the delivery provider is not required to request a translation of the proxy shipping address, and, therefore, does not require specialized software.

In addition, it was described above that the user visits the merchant site directly over the untrusted public network. However, this is also merely another illustrative example. The user may alternatively visit the merchant site through an "anonymizer" web site such as that provided by ANONYMIZER™ Inc., La Mesa, California, USA. This would further enhance confidentiality in on-line purchase transactions by allowing the user not only to prevent his or her personal information from being received by merchant sites, but also, *e.g.*, the IP address of his or her computer on the Internet.

In addition, it was described that the user may specify both the number of purchases he or she wishes to make using the proxy user data and the expiration period of the proxy user data. The user may also specify a monetary limit for purchases that can be made using the proxy user data.

In addition, it was described above in the illustrative procedure that the proxy user data provided by the proxy agent is used in making on-line purchases. However, this is merely one illustrative example. Users may alternatively request and obtain proxy user data from the proxy agent, and then use the proxy user data for making conventional purchases from merchants, *e.g.*, direct purchases from traditional retail outlets. For example, the proxy agent may provide the proxy user data for use with a proxy credit or debit card. In this way, users may make direct credit or debit purchases with virtually the same anonymity that cash-paying customers normally enjoy. The features of restricting the number and the monetary limit of purchases that can be made with the card, and the feature of setting the expiration date of the card, may also be available for making conventional purchases. A proxy credit or debit card may also be provided that includes the user's real personal information, *e.g.*, his or her real credit or debit card account number, but also has the features for restricting use of the card.

In addition, it was described above that the user registers with the proxy agent for obtaining proxy user data that he or she can use when making purchases and taking delivery of goods or services. However, this is also merely one illustrative example. The user may, *e.g.*, register with the

proxy agent once, thereby providing the proxy agent with his or her real user data. The user may then request and obtain new proxy user data corresponding with the real user data from the proxy agent as many times as he or she wishes for subsequently making purchases, without having to re-register with the proxy agent each time. As described above, the user may be provided with, *e.g.*, an identification number and/or a password for use in making subsequent requests for proxy data.

In addition, it was described above that the user makes purchases from the merchant and takes delivery of the purchases using only the proxy user data stored in the user database. It was also described that the user database stores not only the user's personal information such as his or her real name, real shipping address, real e-mail address, and real credit or debit card account number, but also corresponding proxy data such as a proxy name, a proxy shipping address, a proxy e-mail address, and a proxy credit or debit card account number. However, this is merely another illustrative example. In a preferred embodiment, the real user data and the corresponding proxy user data stored in the user database includes all of the user data required to effect the purchase and delivery of goods or services. Some purchase and delivery transactions may therefore require different amounts of user data or different types of user data to effect the transaction.

Further, the user may alternatively request and obtain proxy user data corresponding with only a selected amount of real user data, even if this proxy user data alone would be insufficient for effecting the purchase and delivery of goods or services. For example, the user may decide to request and obtain proxy user data corresponding with only his or her real credit or debit card account number. Accordingly, the proxy agent would generate a proxy credit or debit card account number and store both the proxy card account number and the corresponding real card account number in the user database. The proxy agent would then route purchase authorization requests and replies between the merchant and the card issuer while revealing the real card account number only to the card issuer and concealing the real card account number from the merchant. In this way, the user may select different levels of security and confidentiality for different purchase and delivery transactions.

The present invention has been described in detail including the preferred embodiments thereof. However, it should be appreciated that those skilled in the art, upon consideration of the present disclosure, may make modifications and/or improvements on this invention and still be within the scope and spirit of this invention as set forth in the following claims.

What is claimed is:

1. A method of enabling a user to effect a purchase of goods or services from a merchant without revealing selected real user data to the merchant, comprising the steps of:

(a) generating proxy user data corresponding with the selected real user data;

(b) maintaining a database including the selected real user data and the corresponding proxy user data for use in translating the selected real user data into the corresponding proxy user data, and in translating the proxy user data into the corresponding selected real user data; and

(c) routing purchase authorization requests and replies between the merchant and a purchase authorization entity using the selected real user data and the corresponding proxy user data in the database;

wherein the requests routed to the purchase authorization entity include the selected real user data, and the replies routed to the merchant include the corresponding proxy user data and do not include the selected real user data.

2. The method as recited in claim 1, further including a step of effecting a delivery of the goods or services to the user, wherein the selected real user data includes at least one of a real name, a real shipping address, and a real e-mail address, and the corresponding proxy user data includes at least one of a proxy name, a proxy shipping address, and a proxy e-mail address.

3. The method as recited in claim 2,

wherein the goods or services have digital form,

wherein the merchant delivers the digital goods or services to the user as an e-mail transmission using the proxy e-mail address, and

further including the step of routing the e-mail transmission from the merchant to the user using the proxy e-mail address and the corresponding real e-mail address, wherein the step of routing includes the substeps of receiving the e-mail transmission including the digital goods or services, the e-mail transmission being received at the proxy e-mail address,

DISH-Blue Spike 842
Exhibit 1005, Page 1228

accessing the database for translating the proxy e-mail address into the corresponding real e-mail address, and

sending the e-mail transmission to the corresponding real e-mail address.

4. The method as recited in claim 2, wherein the merchant provides the goods or services, the proxy name, and proxy shipping address to a delivery entity, and the method further includes the steps of

receiving a request for the real name and real shipping address corresponding with the proxy name and proxy shipping address from the delivery entity,

translating the proxy name and proxy shipping address into the real name and real shipping address using the database, and

providing the real name and real shipping address to the delivery entity,

whereby the delivery entity delivers the goods or services to the user.

5. The method as recited in claim 2, wherein the merchant provides the goods or services and the proxy name/proxy shipping address to a first delivery entity,

and the method further includes the steps of

receiving the goods or services and the proxy name/proxy shipping address from the first delivery entity,

translating the proxy name/proxy shipping address into the real name/real shipping address using the database, and

providing the goods or services and the real name/real shipping address to a second delivery entity,

whereby the second delivery entity delivers the goods or services to the user.

6. The method as recited in claim 5, wherein the first delivery entity and the second delivery entity are the same delivery entity.

7. The method as recited in claim 1, wherein the proxy user data generated in step (a) includes at least one restricted-use attribute.

8. The method as recited in claim 7, wherein the restricted-use attribute is selectable by the user.

DISH-Blue Spike 842
Exhibit 1005, Page 1229

9. The method as recited in claim 7, wherein the restricted-use attribute corresponds with at least one of a selected number of purchases that can be authorized by the purchase authorization entity, a selected period of time during which purchases can be authorized by the purchase authorization entity, or a selected monetary limit for purchases that can be authorized by the purchase authorization entity.

10. The method as recited in claim 1, further including the steps of

receiving a request for the proxy user data from the user, the request including the selected real user data, and

providing the proxy user data corresponding with the selected real user data to the user.

11. The method as recited in claim 10, wherein the user is further provided with at least a user ID and/or a password for use in making subsequent requests for proxy user data.

12. The method as recited in claim 10, wherein the request for the proxy user data is received via a network, and the proxy user data is provided to the user via a network.

13. The method as recited in claim 10, wherein the user is provided with more than one set of proxy user data corresponding with the selected real user data.

14. The method as recited in claim 13, wherein the maintaining in step (b) includes updating the database to include each set of proxy user data corresponding with the selected real user data.

15. The method as recited in claim 1, wherein the selected real user data includes real funding account data, and wherein the corresponding proxy user data includes proxy funding account data.

16. The method as recited in claim 1, wherein the routing in step (c) includes the substeps of

(c1) receiving a purchase authorization request from the merchant, the purchase authorization request including the proxy user data,

(c2) translating the proxy user data into the corresponding selected real user data using the database,

(c3) substituting the proxy user data in the purchase authorization request with the corresponding selected real user data, and routing the purchase authorization request to the purchase authorization entity,

(c4) receiving a purchase authorization reply from the purchase authorization entity, the purchase authorization reply including the selected real user data, and

(c5) substituting the selected real user data in the purchase authorization reply with the corresponding proxy user data, and routing the purchase authorization reply to the merchant.

17. The method as recited in claim 1, wherein the user purchases the goods or services from the merchant by visiting a merchant site using a computer, the merchant site and the computer being connectable to a network.

18. The method as recited in claim 1, wherein the database including the selected real user data and the corresponding proxy user data is stored in a storage device on a computer connectable to a network.

19. The method as recited in claim 1, wherein the routing in step (c) is performed over at least one network.

20. A method of enabling a user to effect a purchase of goods or services from a merchant using a funding account, comprising the steps of:

(a) generating user account data for the funding account, the user account data having at least one restricted-use attribute;

(b) maintaining a database including the user account data; and

(c) routing purchase authorization requests and replies between the merchant and a purchase authorization entity using the user account data in the database,

DISH-Blue Spike 842
Exhibit 1005, Page 1231

wherein the restricted-use attribute corresponds with at least one of a number of purchases that can be funded using the funding account, a period of time during which purchases can be funded using the funding account, and/or a monetary limit for purchases that can be funded using the funding account.

21. The method as recited in claim 20, wherein the at least one restricted-use attribute of the user account data is selectable by the user.

22. The method as recited in claim 20, wherein the routing in step (c) includes a substep of determining whether any use restrictions of the user account data have been violated.

23. The method as recited in claim 1, further including steps of tracking purchases made using the user data stored in the database and storing information related to the tracked purchases in the database.

24. The method as recited in claim 20, further including steps of tracking purchases made using the user data stored in the database and storing information related to the tracked purchases in the database.

25. A method of enabling a user to effect a delivery of goods or services from a merchant without revealing real delivery data to the merchant, comprising the steps of:

(a) generating proxy delivery data corresponding with the real delivery data;

(b) maintaining a database including the real delivery data and the corresponding proxy delivery data for use in translating the proxy delivery data into the corresponding real delivery data; and

(c) providing the real delivery data corresponding with the proxy delivery data to a delivery entity,

wherein the user provides the proxy delivery data to the merchant, and

wherein the merchant provides the goods or services and the proxy delivery data to the delivery entity for subsequent delivery of the goods or services to the user.

DISH-Blue Spike 842
Exhibit 1005, Page 1232

26. A system for enabling a user to effect a purchase of goods or services over a distributed network without sending selected real user data over the distributed network, for use with at least one merchant site accessible on the distributed network, each merchant site being connectable to an authorization network for making purchase authorization requests and receiving replies thereto, at least one user computer connected to the distributed network, each user computer running at least one client application for accessing the at least one merchant site on the distributed network, and at least one purchase authorization entity, each purchase authorization entity being accessible on the authorization network and capable of sending replies over the authorization network in response to the purchase authorization requests, the system comprising:

a proxy user data generator for generating proxy user data corresponding with the selected real user data;

a database for storing the selected real user data and the corresponding proxy user data, for use in translating the selected real user data into the corresponding proxy user data and in translating the proxy user data into the corresponding selected real user data; and

a purchase authorization request/reply router connectable to the authorization network for routing purchase authorization requests/replies between each merchant site and each purchase authorization entity using the selected real user data and the corresponding proxy user data stored in the database.

27. A system for enabling a user to effect a purchase of goods or services over a distributed network using a funding account, for use with at least one merchant site accessible on the distributed network, each merchant site being connectable to an authorization network for making purchase authorization requests and receiving replies thereto, at least one user computer connected to the distributed network, each user computer running at least one client application for accessing the at least one merchant site on the distributed network, and at least one purchase authorization entity, each purchase authorization entity being accessible on the authorization network and capable of sending replies over the authorization network in response to the purchase authorization requests, the system comprising:

a user account data generator for generating user account data for the funding account, the user account data having at least one restricted-use attribute;

a database for storing the user account data; and

a purchase authorization request/reply router connectable to the authorization network for routing purchase authorization requests/replies between each merchant site and each purchase authorization entity using the user account data stored in the database,

wherein the restricted-use attribute corresponds with at least one of a number of purchases that can be funded using the funding account, a period of time during which purchases can be funded using the funding account, or a monetary limit for purchases that can be funded using the funding account.

28. A system for enabling a user to effect a delivery of goods or services from an on-line merchant without revealing real delivery data to the on-line merchant, for use with at least one merchant site accessible on a distributed network, at least one user computer connected to the distributed network, each user computer running at least one client application for accessing the at least one merchant site on the distributed network, and at least one delivery entity, the system comprising:

a proxy delivery data generator for generating proxy delivery data corresponding with the real delivery data, for use by the user;

a database for storing the real delivery data and the corresponding proxy delivery data, for use in translating the proxy delivery data into the corresponding real delivery data; and

a unit for receiving a request for the real delivery data corresponding with the proxy delivery data, and for providing the real delivery data in response to the request, for use by the delivery entity in delivering the goods or services to the user.

29. A system for enabling a user to effect a delivery of goods or services over a distributed network via e-mail without sending a real e-mail address over the distributed network, for use with at least one merchant site accessible on a distributed network, and at least one user computer connected to the distributed network, each user computer running at least

one client application for accessing the at least one merchant site on the distributed network, the system comprising:

a proxy e-mail address generator for generating a proxy e-mail address corresponding with the real e-mail address, for use by the user;

a database for storing the real e-mail address and the corresponding proxy e-mail address, for use in translating the proxy e-mail address into the corresponding real e-mail address; and

an e-mail router connectable to the distributed network for routing e-mail between each merchant site and the user computer, wherein the merchant site sends the goods or services over the distributed network using the proxy e-mail address and the e-mail router routes the goods or services sent by the merchant site to the user using the corresponding real e-mail address.

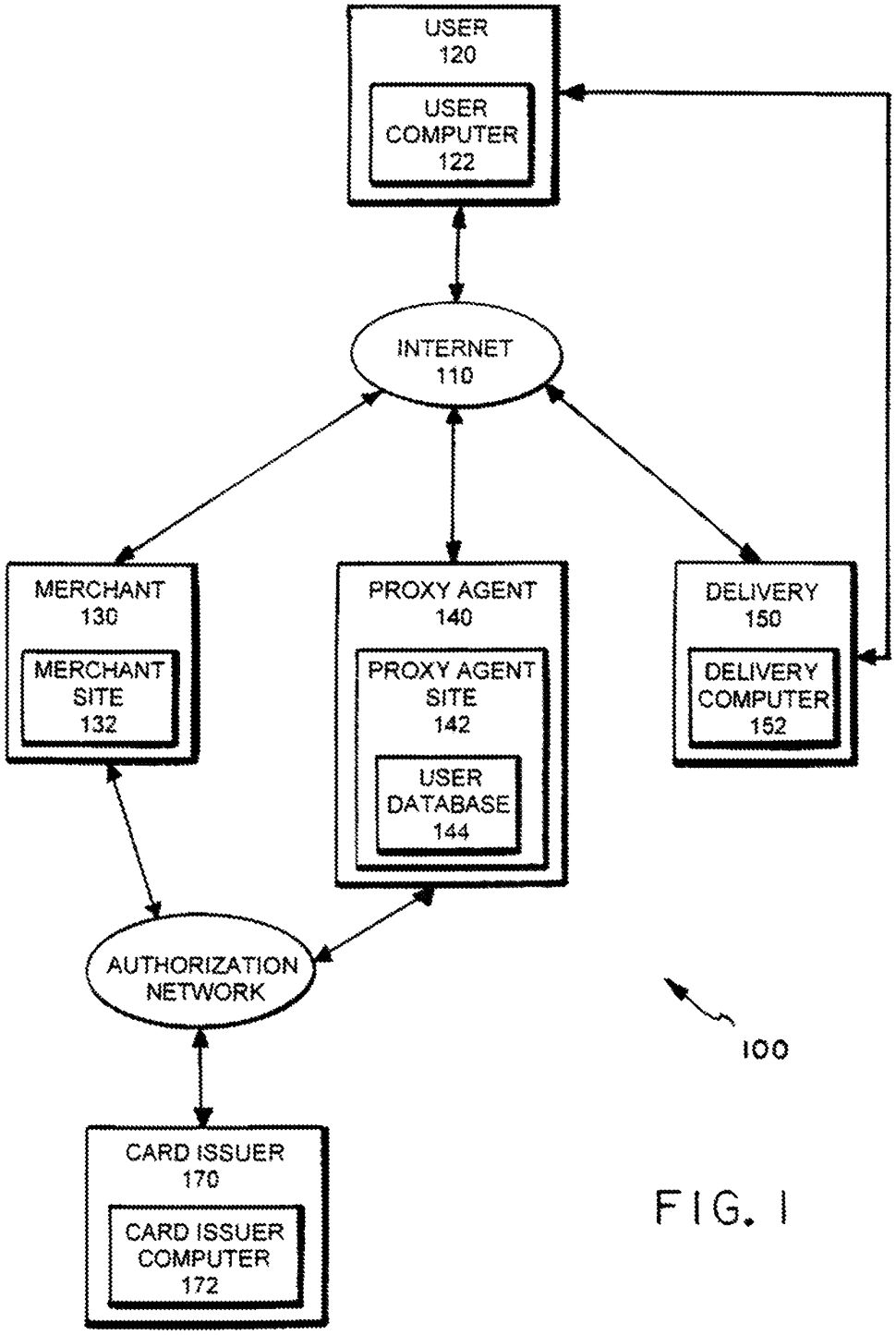


FIG. 1

DISH-Blue Spike 842
Exhibit 1005, Page 1236

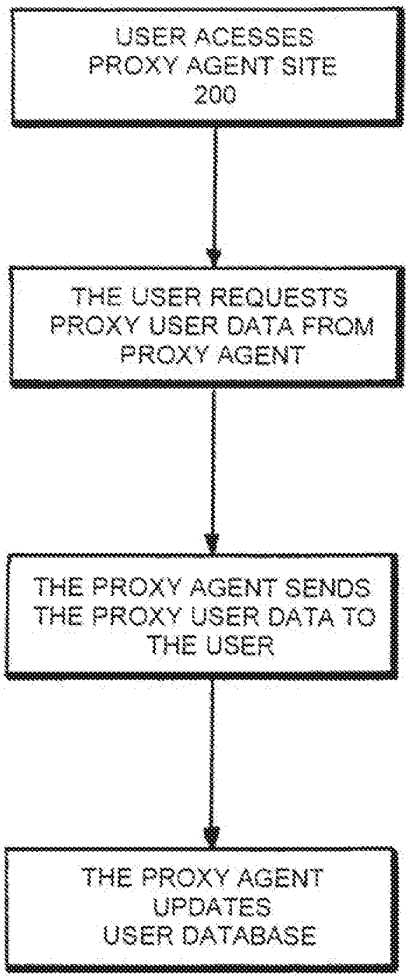

USER ACESSES PROXY AGENT SITE 200
THE USER REQUESTS PROXY USER DATA FROM PROXY AGENT
THE PROXY AGENT SENDS THE PROXY USER DATA TO THE USER
THE PROXY AGENT UPDATES USER DATABASE

FIG. 2

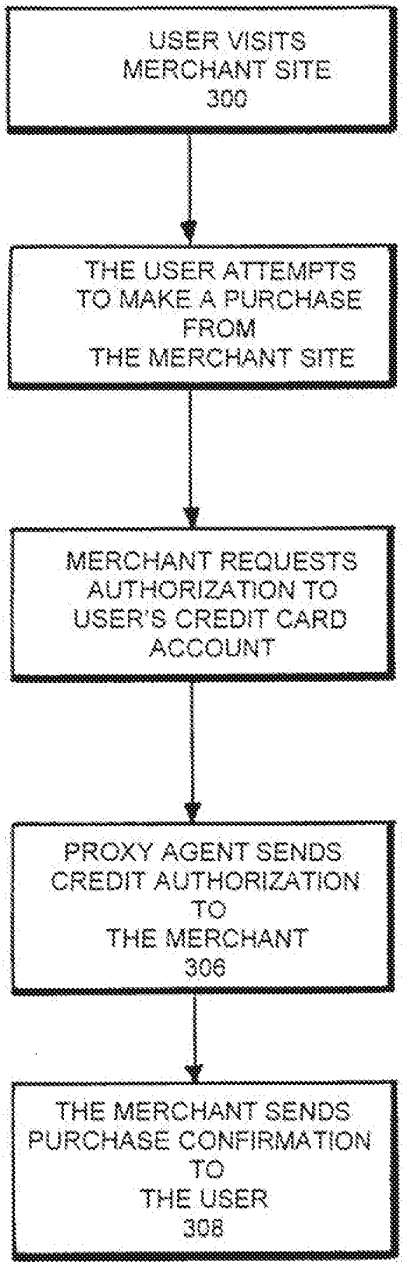

USER VISITS MERCHANT SITE 300
THE USER ATTEMPTS TO MAKE A PURCHASE FROM THE MERCHANT SITE
MERCHANT REQUESTS AUTHORIZATION TO USER'S CREDIT CARD ACCOUNT
PROXY AGENT SENDS CREDIT AUTHORIZATION TO THE MERCHANT 306
THE MERCHANT SENDS PURCHASE CONFIRMATION TO THE USER 308

FIG. 3

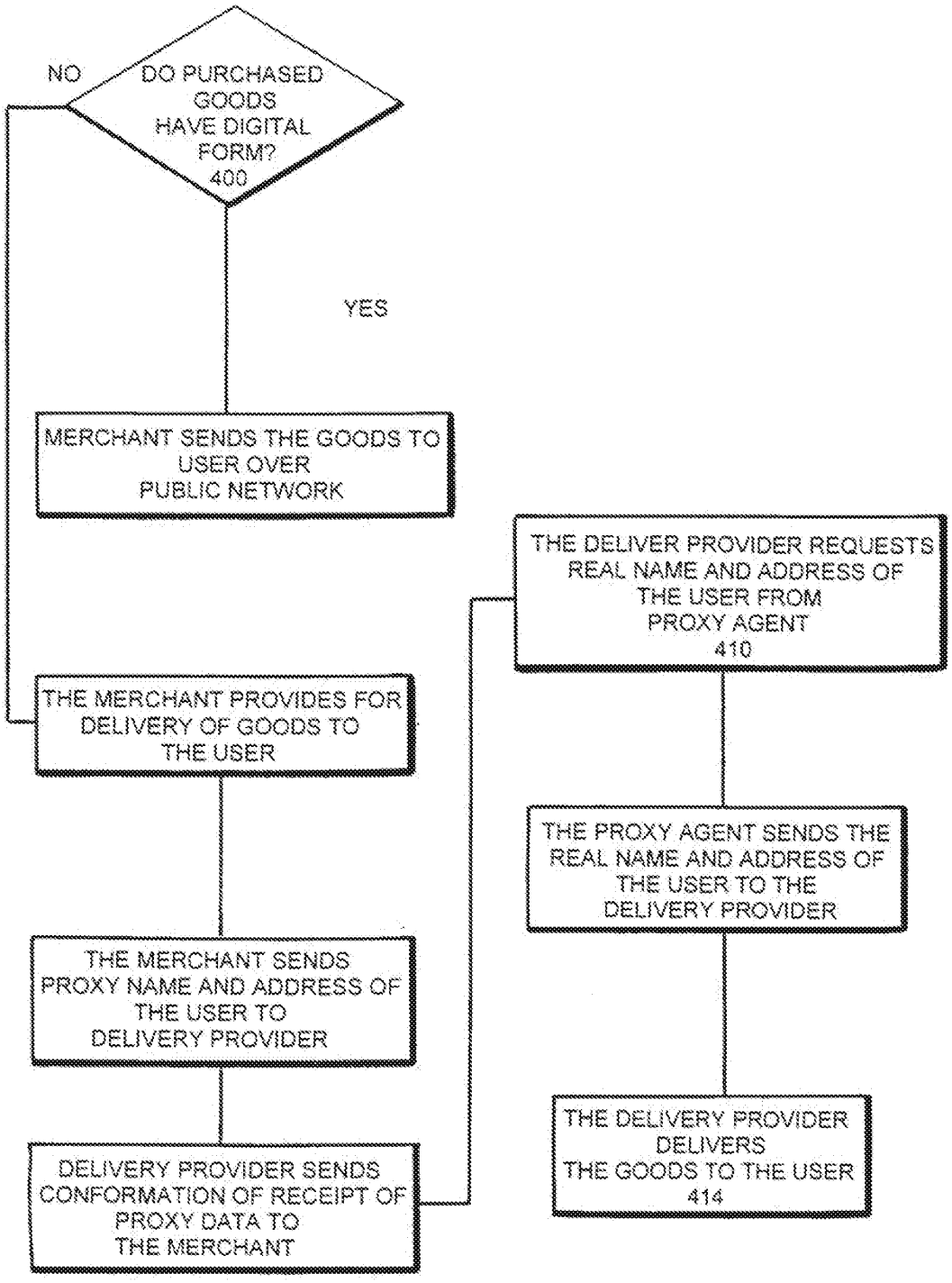

DO PURCHASED GOODS HAVE DIGITAL FORM? 400
NO
YES
MERCHANT SENDS THE GOODS TO USER OVER PUBLIC NETWORK
THE MERCHANT PROVIDES FOR DELIVERY OF GOODS TO THE USER
THE MERCHANT SENDS PROXY NAME AND ADDRESS OF THE USER TO DELIVERY PROVIDER
DELIVERY PROVIDER SENDS CONFORMATION OF RECEIPT OF PROXY DATA TO THE MERCHANT
THE DELIVER PROVIDER REQUESTS REAL NAME AND ADDRESS OF THE USER FROM PROXY AGENT 410
THE PROXY AGENT SENDS THE REAL NAME AND ADDRESS OF THE USER TO THE DELIVERY PROVIDER
THE DELIVERY PROVIDER DELIVERS THE GOODS TO THE USER 414

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/21901

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 17/30
US CL :705/53, 64, 67
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/53, 64, 67

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant p... ges	Relevant to claim No.
A	US 4,529,870 A (CHAUM) 16 JULY 1985 (16.07.85), ALL	1-29
A	US 5,671,280 A (ROSEN) 23 SEPTEMBER 1997 (23.09.97), ALL	1-29
A, P	US 5,987,440 A (O'NEIL et al.) 16 NOVEMBER 1999 (16.11.99), ALL	1-29
A, P	US 6,061,789 A (HAUSER et al.) 09 MAY 2000 (09.05.00), ALL	1-29
A, P	US 6,076,078 A (CAMP et al.) 13 JUNE 2000 (13.06), ALL	1-29

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

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search	Date of mailing of the international search report
06 NOVEMBER 2000	04 JAN 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES P. TRAMMELL Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)*

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G11B 20/00 — A2

(11) International Publication Number: WO 97/43761

(43) International Publication Date: 20 November 1997 (20.11.97)

(21) International Application Number: PCT/US97/08192

(22) International Filing Date: 15 May 1997 (15.05.97)

(30) Priority Data:

60/017,722	15 May 1996 (15.05.96)	US
60/018,132	22 May 1996 (22.05.96)	US
08/689,606	12 August 1996 (12.08.96)	US
08/689,754	12 August 1996 (12.08.96)	US
08/699,712	12 August 1996 (12.08.96)	US
PCT/US96/14262	4 September 1996 (04.09.96)	WO
(34) Countries for which the regional or international application was filed:		US et al.
60/037,931	14 February 1997 (14.02.97)	US

(71) Applicant *(for all designated States except US)*: INTERTRUST TECHNOLOGIES CORP. [US/US]; 460 Oakmead Parkway, Sunnyvale, CA 94086 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SHEAR, Victor, H. [US/US]; 5203 Battery Lane, Bethesda, MD 20814 (US). SIBERT, Olin, W. [US/US]; 30 Ingleside Road, Lexington, MA 02173-2522 (US). VANWIE, David, M. [US/US]; Apartment 216, 965 E. El Camino Real, Sunnyvale, CA 94087 (US). WEBER, Robert, P. [US/US]; 215 Waverley Street #4, Menlo Park, CA 94025 (US).

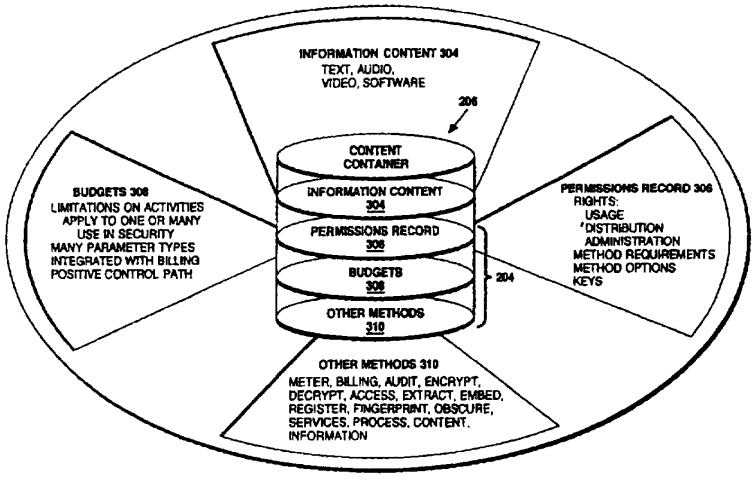
(74) Agent: FARIS, Robert, W.; Nixon & Vanderhye P.C., 8th floor, 1100 North Glebe Road, Arlington, VA 22201-4714 (US).

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

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

(54) Title: CRYPTOGRAPHIC METHODS, APPARATUS AND SYSTEMS FOR STORAGE MEDIAELECTRONIC RIGHTS MANAGEMENT IN CLOSED AND CONNECTED APPLIANCES

(57) Abstract



A rights management arrangement for storage media such as optical digital video disks (DVDs, also called digital versatile disks) provides adequate copy protection in a limited, inexpensive mass-produceable, low-capability platform such as a dedicated home consumer disk player and also provides enhanced, more flexible security techniques and methods when the same media are used with platforms having higher security capabilities. A control object (or set) defines plural rights management rules for instance, price for performance or rules governing redistribution. Low capability platforms may enable only a subset of the control rules such as controls on copying or marking of played material. Higher capability platforms may enable all (or different subsets) of the rules. Cryptographically strong security is provided by encrypting at least some of the information carried by the media and enabling decryption based on the control set and/or other limitations. A secure "software container" can be used to protectively encapsulate (e.g., by cryptographic techniques) various digital property content (e.g., audio, video, game, etc.) and control object (i.e., set of rules) information. A standardized container format is provided for general use on/with various mediums and platforms. In addition, a special purpose container may be provided for DVD medium and appliances (e.g., recorders, players, etc.) that contains DVD program content (digital property) and DVD medium specific rules. The techniques, systems and methods disclosed herein are capable of achieving compatibility with other protection standards, such as for example, CGMA and Matsushita data protection standards adopted for DVDs. Cooperative rights management may also be provided, where plural networked rights management arrangements collectively control a rights management event on one or more of such arrangements.

FOR THE PURPOSES OF INFORMATION ONLY

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

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

CRYPTOGRAPHIC METHODS, APPARATUS AND SYSTEMS FOR STORAGE MEDIA ELECTRONIC RIGHTS MANAGEMENT IN CLOSED AND CONNECTED APPLIANCES

Cross-Reference to Related Applications and Patents

The specifications and drawings of the following prior, commonly assigned published patent specifications are incorporated by reference into this patent specification:

PCT Publication No. WO 96/27155 dated 6 September 1996 entitled "Systems And Methods For Secure Transaction Management And Electronic Rights Protection", which is based on PCT application no. PCT/US96/02303 filed 13 February 1996 and U.S. patent application serial no. 08/388,107 of Ginter et al. entitled filed on February 13, 1995 (hereinafter "Ginter et al");

U.S. Patent No 4,827,508 entitled "Database Usage Metering and Protection System and Method" dated May 2, 1989;

U.S. Patent No. 4,977,594 entitled "Database Usage Metering and Protection System and Method" dated December 11, 1990;

U.S. Patent No. 5,050,213 entitled "Database Usage Metering and Protection System and Method" dated September 17, 1991; and

U.S. Patent No. 5,410,598 entitled "Database Usage Metering and Protection System and Method" dated April 25, 1995; and

European Patent No.EP 329681 entitled "Database Usage Metering and Protection System and Method" dated January 17, 1996.

In addition, the specifications and drawings of the following commonly-assigned prior-filed patent specifications are incorporated by reference into this patent application:

PCT Application No. PCT/US96/14262 filed 4 September 1996 entitled "Trusted Infrastructure Support Systems, Methods And Techniques For Secure Electronic Commerce, Electronic Transactions, Commerce Process Control And Automation, Distributed Computing, And Rights Management," which corresponds to U.S. patent application serial no. 08/699,712 filed on August 12, 1996 (hereinafter "Shear et al.");

DISH-Blue Spike 842
Exhibit 1005, Page 1244

PCT Application No. _____ filed _____, 1997 entitled "Steganographic Techniques For Securely Delivering Electronic Digital Rights Management Control Information Over Insecure Communications Channels," which corresponds to U.S. patent application serial no. 08/689,606 of Van Wie and Weber filed on August 12, 1996 (hereinafter "Van Wie and Weber"); and

PCT Application No. _____ filed _____, 1997 based on U.S. Patent Application serial no.08/689,754 entitled "Systems and Methods Using Cryptography To Protect Secure Computing Environments," of Sibert and Van Wie filed on August 12, 1996 (hereinafter "Sibert and Van Wie").

FIELD OF THE INVENTION

This invention relates to information protection techniques using cryptography, and more particularly to techniques using cryptography for managing rights to information stored on portable media -- one example being optical media such as Digital Video Disks (also known as "Digital Versatile Disks" and/or "DVDs"). This invention also relates to information protection and rights management techniques having selectable applicability depending upon, for example, the resources of the device being

DISH-Blue Spike 842
Exhibit 1005, Page 1245

used by the consumer (e.g., personal computer or standalone player), other attributes of the device (such as whether the device can be and/or typically is connected to an information network ("connected" versus "unconnected")), and available rights. This invention further relates, in part, to cooperative rights management -- where plural networked rights management arrangements collectively control a rights management event on one or more of such arrangements. Further, important aspects of this invention can be employed in rights management for electronic information made available through broadcast and/or network downloads and/or use of non-portable storage media, either independent of, or in combination with portable media.

BACKGROUND OF THE INVENTION

The entertainment industry has been transformed by the pervasiveness of home consumer electronic devices that can play video and/or audio from pre-recorded media. This transformation began in the early 1900s with the invention of the phonograph—which for the first time allowed a consumer to listen to his or her favorite band, orchestra or singer in his or her home whenever he or she wishes. The availability of inexpensive video

DISH-Blue Spike 842
Exhibit 1005, Page 1246

cassette recorders/players beginning in the early 1980s brought about a profound revolution in the movie and broadcast industries, creating an entirely new home consumer market for films, documentaries, music videos, exercise videos, etc.

The entertainment industry has long searched for optimal media for distributing content to home consumers. The original phonograph cylinders distributed by Thomas Edison and other phonograph pioneers had the advantage that they were difficult to copy, but suffered from various disadvantages such as high manufacturing costs, low resistance to breakage, very limited playback time, relatively low playback quality, and susceptibility to damage from wear, scratching or melting. Later-developed wax and vinyl disks could hold more music material but suffered from many of the same disadvantages. Magnetic tapes, on the other hand, could be manufactured very inexpensively and could hold a large amount of program material (e.g., 2, 4 or even 6 hours of video and/or audio). Such magnetic tapes could reproduce program material at relatively high quality, and were not as susceptible to damage or wearing out. However, despite the many clear advantages that magnetic tape provides over other media, the

entertainment industry has never regarded it as an ideal or optimum medium because of its great susceptibility to copying.

Magnetic tape has the very flexible characteristic that it can be relatively easily recorded on. Indeed, the process for recording a magnetic tape is nearly as straightforward as that required for playing back pre-recorded content. Because of the relative ease by which magnetic tape can be recorded, home consumer magnetic tape equipment manufacturers have historically provided dual mode equipment that can both record and play back magnetic tapes. Thus, home audio and video tape players have traditionally had a "record" button that allows a consumer to record his or her own program material on a blank (un-recorded) magnetic tape. While this recording ability has given consumers additional flexibility (e.g., the ability to record a child's first words for posterity, and the ability to capture afternoon soap operas for evening viewing), it has unfortunately also been the foundation of an illegal multi-billion dollar content pirating industry that produces millions of illegal, counterfeit copies every year. This illegal pirating operation—which is international in scope—leeches huge amounts of revenue every year from the world's major

entertainment content producers. The entertainment industry must pass along these losses to honest consumers—resulting in higher box office prices, and higher video and audio tape sales and rental prices.

In the mid 1980s, the audio entertainment industry developed the optical compact disk as an answer to some of these problems. The optical compact disk—a thin, silvery plastic platter a few inches in diameter—can hold an hour or more of music or other audio programming in digital form. Such disks were later also used for computer data. The disk can be manufactured very inexpensively, and provides extremely high quality playback that is resistant to noise because of the digital techniques used to record and recover the information. Because the optical disk can be made from plastic, it is light weight, virtually unbreakable, and highly resistant to damage from normal consumer handling (unlike the prior vinyl records that were easily scratched or worn down even by properly functioning phonographs). And, because recording on an optical disk is, so far, significantly more difficult than playing back an optical disk, home consumer equipment providing both recording and playback capabilities is unlikely, in

the near future, to be as cost-effective as play-only equipment—greatly reducing the potential for illicit copying. Because of these overwhelming advantages, the music industry has rapidly embraced the new digital compact disk technology—virtually replacing older audio vinyl disk media within the space of a few short years.

Indeed, the threat of widespread and easy unauthorized copying in the absence of rights management technologies apparently has been an important contributing factor to the demise of digital audio tape (DAT) as a media for music distribution and, more importantly, home audio recording. Rightsholders in recorded music vigorously opposed the widespread commercialization of inexpensive DAT technology that lacked rights management capabilities since the quality of the digital recording was completely faithful to the digital source on, for example, music CDs. Of course, the lack of rights management was not the only factor at work, since compared with optical media, tape format made random access difficult, for example, playing songs out of sequence.

The video entertainment industry is on the verge of a revolution similar to that wrought by music CDs based on movies in digital format distributed on high capacity read-only optical media. For example, digital optical disk technology has advanced to the point where it is now possible to digitally record, among other things, a full length motion picture (plus sound) on one side of a 5" plastic optical disk. This same optical disk can accommodate multiple high-quality digital audio channels (e.g., to record multi-channel "sensurround" sound for home theaters and/or to record film dialog in multiple different languages on the same disk). This same technology makes it possible to access each individual frame or image of a movie for still image reproduction or—even more exciting—to provide an unprecedented "random access" playback capability that has never before existed in home consumer equipment. This "random access" playback could be used, for example, to delete violence, foul language or nudity at time of playback so that parents could select a "PG" playback version of an "R" rated film at the press of a button. The "random access" capability also has exciting possibilities in terms of allowing viewers to interact with the pre-recorded content (e.g.,

DISH-Blue Spike 842
Exhibit 1005, Page 1251

allowing a health enthusiast to select only those portions of an exercise video helpful to a particular day's workout). See, for example, "Applications Requirements for Innovative Video Programming," DVD Conference Proceedings (Interactive Multimedia Association, 19-20 October 1995, Sheraton Universal Hotel, Universal City, California).

Non-limiting examples of the DVD family of optical media include:

- DVD (Digital Video Disk, Digital Versatile Disk), a non-limiting example of which includes consumer appliances that play movies recorded on DVD disks;

- DVD-ROM (DVD-Read Only Memory), a non-limiting example of which includes a DVD read-only drive and disk connected to a computer or other appliance;

- DVD-RAM (DVD Random Access Memory), a non-limiting example of which includes a read/write drive and optical media in, for example, consumer appliances for home recording and in a computer or other appliance

DISH-Blue Spike 842
Exhibit 1005, Page 1252

for the broadest range of specific applications; and

- Any other high capacity optical media presently known or unknown.

"DVDs" are, of course, not limited to use with movies. Like CDs, they may also be used for other kinds of information, for example:

- sound recordings
- software
- databases
- games
- karaoke
- multimedia
- distance learning
- documentation
- policies and manuals

DISH-Blue Spike 842
Exhibit 1005, Page 1253

- any kind of digital data or other information
- any combination of kinds of digital data or other information
- any other uses presently known or unknown.

The broad range of DVD uses presents a technical challenge: how can the information content distributed on such disks, which might be any kind or combination of video, sound, or other data or information broadly speaking, be adequately protected while preserving or even maximizing consumer flexibility? One widely proposed requirement for the new technology(mainly within the context of video), is, to the extent copying is permitted at all, to either: (a) allow a consumer to make a first generation copy of the program content for their own use, but prevent the consumer from making "copies of copies", or multi-generational copies of a given property (thus keeping honest people honest); or (b) to allow unlimited copying for those properties that rightsholders do not wish to protect against copying, or which consumers have made themselves.

DISH-Blue Spike 842
Exhibit 1005, Page 1254

However, providing only such simplistic and limited copy protection in a non-extensible manner may turn out to be extremely shortsighted—since more sophisticated protection and/or rights management objectives (e.g., more robust and selective application of copy protection and other protection techniques, enablement of pay-per-view models, the ability of the consumer to make use of enhanced functionality such as extracting material or interactivity upon paying extra charges, and receiving credit for redistribution, to name a few) could be very useful now or in the future. Moreover, in optimally approaching protection and rights management objectives, it is extremely useful to take differing business opportunities and threats into account that may relate to information delivered via DVD media, for example, depending upon available resources of the device and/or whether the device is connected or unconnected.

More sophisticated rights management capabilities will also allow studios and others who have rights in movies and/or sound recordings to better manage these important assets, in one example, to allow authorized parties to repurpose pieces of digital film, video and/or audio, whether specific and/or arbitrary pieces,

to create derivative works, multimedia games, in one non-limiting example. Solutions proposed to date for protecting DVD content have generally focused solely on limited copy protection objectives and have failed to adequately address or even recognize more sophisticated rights management objectives and requirements. More specifically, one copy protection scheme for the initial generation of DVD appliances and media is based on an encryption method developed initially by Matsushita and the simple CGMA control codes that indicate permitted copying: a one-generation copy, no copies, or unlimited copying.

SUMMARY OF THE INVENTIONS

Comprehensive solutions for protecting and managing information in systems that incorporate high capacity optical media such as DVD require, among other things, methods and systems that address two broad sets of problems: (a) digital to analog conversion (and vice versa); and (b) the use of such optical media in both connected and unconnected environments. The inventions disclosed herein address these and other problems. For example, in the context of analog to digital conversion (and vice versa), it is contemplated that, in accordance with the present

inventions, at least some of the information used to protect properties and/or describe rights management and/or control information in digital form could also be carried along with the analog signal. Devices that convert from one format and/or medium to another can, for example, incorporate some or all of the control and identifying information in the new context(s), or at least not actively delete such information during the conversion process. In addition, the present inventions provide control, rights management and/or identification solutions for the digital realm generally, and also critically important technologies that can be implemented in consumer appliances, computers, and other devices. One objective of the inventions is to provide powerful rights management techniques that are useful in both the consumer electronics and computer technology markets, and that also enable future evolution of technical capabilities and business models. Another non-limiting objective is to provide a comprehensive control, rights management and/or identification solution that remains compatible, where possible, with existing industry standards for limited function copy protection and for encryption.

DISH-Blue Spike 842
Exhibit 1005, Page 1257

The present inventions provide rights management and protection techniques that fully satisfy the limited copy protection objectives currently being voiced by the entertainment industry for movies while also flexibly and extensibly accommodating a wide range of more sophisticated rights management options and capabilities.

Some important aspects of the present inventions (that are more fully discussed elsewhere in this application) include:

- Selection of control information associated with information recorded on DVD media (for example, rules and usage consequence control information, that comprise non-limiting example elements of a Virtual Distribution Environment (VDE)) that is based at least in part on class of appliance, for example, type of appliance, available resources and/or rights;

- Enabling such selected control information to be, at least in part, a subset of control information used on other appliances and/or classes of appliance, or completely different control information;

DISH-Blue Spike 842
Exhibit 1005, Page 1258

- Protecting information output from a DVD device, such as applying rights management techniques disclosed in Ginter et al. and the present application to the signals transmitted using an IEEE 1394 port (or other serial interface) on a DVD player;

- Creation of protected digital content based on an analog source;

- Reflecting differing usage rights and/or content availability in different countries and/or regions of the world;

- Securely managing information on DVD media such that certain portions may be used on one or more classes of appliance (e.g., a standalone DVD player), while other portions may be used on the same or different classes of appliance (e.g., a standalone DVD player or a PC);

- Securely storing and/or transmitting information associated with payment, auditing, controlling and/or otherwise managing content recorded on DVD media, including techniques related to those disclosed in Ginter et al. and in Shear et al.;

- Updating and/or replacing encryption keys used in the course of appliance operation to modify the scope of information that may be used by appliances and/or classes of appliances;

- Protecting information throughout the creation, distribution, and usage process, for example, by initially protecting information collected by a digital camera, and continuing protection and rights management through the editing process, production, distribution, usage, and usage reporting.

- Allowing "virtual rights machines," consisting of multiple devices and/or other systems that participate and work together in a permanently or in a temporarily connected network to share some or all of the rights management for a single and/or multiple nodes including, for example, allowing resources available in plural such devices and/or other systems, and/or rights associated with plural parties and/or groups using and/or controlling such devices and/or other systems, to be employed in concert (according to rights related rules and controls) so as to govern one or more electronic

DISH-Blue Spike 842
Exhibit 1005, Page 1260

events on any one or more of such devices and/or other systems, such event governance including, for example: viewing, editing, subsetting, anthologizing, printing, copying, titling, extracting, saving, and/or redistributing rights protected digital content.

- Allowing for the exchange of rights among peer-to-peer relating devices and/or other systems, wherein such devices and/or other systems participate in a temporary or permanently connected network, and wherein such rights are bartered, sold for currency, and/or otherwise exchanged for value and/or consideration where such value and/or consideration is exchanged between such peer-to-peer participating commercial and/or consumer devices and/or other systems.

General Purpose DVD/Cost-effective Large Capacity Digital Media Rights Protection and Management

The inventions described herein can be used with any large capacity storage arrangement where cost-effective distribution media is used for commercial and/or consumer digital information delivery and DVD, as used herein, should be read to include any such system.

DISH-Blue Spike 842
Exhibit 1005, Page 1261

Copy protection and rights management are important in practical DVD systems and will continue to be important in other large capacity storage, playback, and recording systems, presently known or unknown, in the future. Protection is needed for some or all of the information delivered (or written) on most DVD media. Such protection against copying is only one aspect of rights management. Other aspects involve allowing rightsholders and others to manage their commercial interests (and to have them enforced, potentially at a distance in time and/or space) regardless of distribution media and/or channels, and the particular nature of the receiving appliance and/or device. Such rights management solutions that incorporate DVD will become even more significant as future generations of recordable DVD media and appliances come to market. Rightsholders will want to maintain and assert their rights as, for example, video, sound recordings, and other digital properties are transmitted from one device to another and as options for recording become available in the market.

The apparent convergence between consumer appliances and computers, increasing network and modem speeds, the declining cost of computer power and bandwidth, and the

DISH-Blue Spike 842
Exhibit 1005, Page 1262

increasing capacity of optical media will combine to create a world of hybrid business models in which digital content of all kinds may be distributed on optical media played on at least occasionally connected appliances and/or computers, in which the one-time purchase models common in music CDs and initial DVD movie offerings are augmented by other models, for example, lease, pay per view, and rent to own, to name just few. Consumers may be offered a choice among these and other models from the same or different distributors and/or other providers. Payment for use may happen over a network and/or other communications channel to some payment settlement service. Consumer usage and audit information may flow back to creators, distributors, and/or other participants. The elementary copy protection technologies for DVD now being introduced cannot support these and other sophisticated models.

As writable DVD appliances and media become available, additional hybrid models are possible, including, for example, the distribution of digital movies over satellite and cable systems. Having recorded a movie, a consumer may elect a lease, rental, pay-per-view, or other model if available. As digital television

DISH-Blue Spike 842
Exhibit 1005, Page 1263

comes to market, the ability of writable DVDs to make faithful copies of on-air programming creates additional model possibilities and/or rights management requirements. Here too, simplistic copy protection mechanisms currently being deployed for the initial read-only DVD technologies will not suffice.

Encryption Is A Means, Not An End

Encryption is useful in protecting intellectual properties in digital format, whether on optical media such as DVD, on magnetic media such as disk drives, in the active memory of a digital device and/or while being transmitted across computer, cable, satellite, and other kinds of networks or transmission means. Historically, encryption was used to send secret messages. With respect to DVD, a key purpose of encryption is to require the use of a copy control and rights management system in order to ensure that only those authorized to do so by rightsholders can indeed use the content.

But encryption is more of a means, rather than an end. A central issue is how to devise methods for ensuring, to the maximal extent possible, that only authorized devices and parties can decrypt the protected content and/or otherwise use information

DISH-Blue Spike 842
Exhibit 1005, Page 1264

only to the extent permitted by the rightsholder(s) and/or other relevant parties in the protected content.

The Present Inventions

The present inventions provide powerful right management capabilities. In accordance with one aspect provided by the present invention, encrypted digital properties can be put on a DVD in a tamper-resistant software "container" such as, for example, a "DigiBox" secure container, together with rules about "no copy" and/or "copy" and/or "numbers of permitted copies" that may apply and be enforced by consumer appliances. These same rules, and/or more flexible and/or different rules, can be enforced by computer devices or other systems that may provide more and/or different capabilities (e.g., editing, excerpting, one or more payment methods, increased storage capability for more detailed audit information, etc.). In addition, the "software container" such as for example, a "DigiBox" secure container, can store certain content in the "clear" (that is, in unencrypted form). For example, movie or music titles, copyright statements, audio samples, trailers, and/or advertising can be stored in the clear and/or could be displayed by any appropriate application or

DISH-Blue Spike 842
Exhibit 1005, Page 1265

device. Such information could be protected for authenticity (integrity) when available for viewing, copying, and/or other activities. At the same time, valuable digital properties of all kinds-film, video, image, text, software, and multimedia— may be stored at least partially encrypted to be used only by authorized devices and/or applications and only under permitted, for example rightsholder-approved, circumstances.

Another aspect provided in accordance with the present invention (in combination with certain capabilities disclosed in Ginter et al.) is that multiple sets of rules could be stored in the same "container" on a DVD disk. The software then applies rules depending on whether the movie, for example, was to be played by a consumer appliance or computer, whether the particular apparatus has a backchannel (e.g., an on-line connection), the national and/or other legal or geographic region in which the player is located and/or the movie is being displayed, and/or whether the apparatus has components capable of identifying and applying such rules. For example, some usage rules may apply when information is played by a consumer device, while other rules may apply when played by a computer. The choice of rules

DISH-Blue Spike 842
Exhibit 1005, Page 1266

may be left up to the rightsholder(s) and/or other participants-- or some rules may be predetermined (e.g., based on the particular environment or application). For example, film rightsholders may wish to limit copying and ensure that excerpts are not made regardless of the context in which the property is played. This limitation might be applied only in certain legal or geographic areas. Alternatively, rightsholders of sound recordings may wish to enable excerpts of predetermined duration (e.g., no more than 20 seconds) and that these excerpts are not used to construct a new commercial work. In some cases, governments may require that only "PG" versions of movies and/or the equivalent rating for TV programs may be played on equipment deployed in their jurisdiction, and/or that the applicable taxes, fees and the like are automatically calculated and/or collected if payments related to content recorded on DVD is requested and/or performed (e.g., pay-per-use of a movie, game, database, software product, etc.; and/or orders from a catalog stored at least in part on DVD media, etc.).

In a microprocessor controlled (or augmented) digital consumer appliance, such rules contemplated by the present

DISH-Blue Spike 842
Exhibit 1005, Page 1267

inventions can be enforced, for example, without requiring more than a relatively few additions to a central, controlling microprocessor (or other CPU, a IEEE 1394 port controller, or other content handling control circuitry), and/or making available some ROM or flash memory to hold the necessary software. In addition, each ROM (or flash or other memory, which such memory may be securely connected to, or incorporated into, such control circuitry in a single, manufactured component) can, in one example, contain one or more digital documents or "certificate(s)" that uniquely identifies a particular appliance, individual identity, jurisdiction, appliance class(es), and/or other chosen parameters. An appliance can, for example, be programmed to send a copy of a digital property to another digital device only in encrypted form and only inside a new, tamper-resistant "software container." The container may also, for example, carry with it a code indicating that it is a copy rather than an original that is being sent. The device may also put a unique identifier of a receiving device and/or class of devices in the same secure container. Consequently, for example, in one particular arrangement, the copy may be playable only on the intended receiving device,

DISH-Blue Spike 842
Exhibit 1005, Page 1268

class(es) of devices, and/or devices in a particular region in one non-limiting example and rights related to use of such copy may differ according to these and/or other variables.

The receiving device, upon detecting that the digital property is indeed a copy, can, for example, be programmed not to make any additional copies that can be played on a consumer device and/or other class(es) of devices. If a device detects that a digital property is about to be played on a device and/or other class(es) of devices other than the one it was intended for, it can be programmed to refuse to play that copy (if desired).

The same restrictions applied in a consumer appliance can, for example, be enforced on a computer equipped to provide rights management protection in accordance with the present inventions. In this example, rules may specify not to play a certain film and/or other content on any device other than a consumer appliance and/or classes of appliances, for example. Alternatively, these same powerful capabilities could be used to specify different usage rules and payment schemes that would apply when played on a computer (and/or in other appliances and/or classes of appliances), as the rightsholder(s) may desire, for example,

DISH-Blue Spike 842
Exhibit 1005, Page 1269

different pricing based upon different geographic or legal locales where content is played.

In addition, if "backchannels" are present—for example, set-top boxes with bi-directional communications or computers attached to networks—the present inventions contemplate electronic, independent delivery of new rules if desired or required for a given property. These new rules may, for example, specify discounts, time-limited sales, advertising subsidies, and/or other information if desired. As noted earlier, determination of these independently delivered rules is entirely up to the rightsholder(s) and/or others in a given model.

The following are two specific examples of a few aspects of the present invention discussed above:

1. An Analog To Digital Copying Example

a) Bob has a VHS tape he bought (or rented) and wants to make a copy for his own use. The analog film has copy control codes embedded so that they do not interfere with the quality of the signal. Bob has a writable DVD appliance

that is equipped to provide rights management protection in accordance with the present invention. Bob's DVD recorder detects the control codes embedded in the analog signal (for example, such recorder may detect watermarks and/or fingerprints carrying rights related control and/or usage information), creates a new secure container to hold the content rules and describe the encoded film, and creates new control rules (and/or delivers to a secure VDE system for storage and reporting certain usage history related information such as user name, time, etc.) based on the analog control codes and/or other information it detected and that are then placed in the DigiBox and/or into a secure VDE installation data store such as a secure data base. Bob can play that copy back on his DVD appliance whenever he chooses.

b) Bob gives the DVD disk he recorded to Jennifer who wishes to play it on computer that has a DVD drive. Her computer is equipped to provide rights management protection in accordance with the present invention. Her computer opens the "DigiBox," detects that this copy is being used on a device different from the one that recorded it (an unauthorized device) and refuses to play the copy.

c) Bob gives the DVD disk to Jennifer as before, but now Jennifer contacts electronically a source of new rules and usage consequences, which might be the studio, a distributor, and/or a rights and permissions clearinghouse, (or she may have sufficient rights already on her player to play the copy). The source sends a DigiBox container to Jennifer with rules and consequences that permit playing the movie on her

DISH-Blue Spike 842
Exhibit 1005, Page 1272

computer while at the same time charging her for use, even though the movie was recorded on DVD by Bob rather than by the studio or other value chain participant.

2. A Digital To Analog Copying Example

a) Jennifer comes home from work, inserts a rented or owned DVD into a player connected to, or an integral part of her TV, and plays the disk. In a completely transparent way, the film is decrypted, the format is converted from digital to analog, and displayed on her analog TV.

b) Jennifer wishes to make a copy for her own use. She plays the film on an DVD device incorporating rights management protection in accordance with the present invention, that opens the DigiBox secure container, accesses the control information, and decrypts the film.

DISH-Blue Spike 842
Exhibit 1005, Page 1273

She records the analog version on her VCR which records a high-quality copy.

c) Jennifer gives the VCR copy to Doug who wishes to make a copy of the analog tape for his own use, but the analog control information forces the recording VCR to make a lower-quality copy, or may prevent copying. In another non-limiting example, more comprehensive rights management information may be encoded in the analog output using the methods and/or systems described in more detail in the above referenced Van Wie and Weber patent application.

In accordance with one aspect provided by this invention, the same portable storage medium, such as a DVD, can be used with a range of different, scaled protection environments providing different protection capabilities. Each of the different environments may be enabled to use the information carried by the portable storage medium based on rights management techniques and/or capabilities supported by the particular environment. For

DISH-Blue Spike 842
Exhibit 1005, Page 1274

example, a simple, inexpensive home consumer disk player may support copy protection and ignore more sophisticated and complex content rights the player is not equipped to enable. A more technically capable and/or secure platform (e.g., a personal computer incorporating a secure processing component possibly supported by a network connection, or a "smarter" appliance or device) may, for example, use the same portable storage medium and provide enhanced usage rights related to use of the content carried by the medium based on more complicated rights management techniques (e.g., requiring payment of additional compensation, providing secure extraction of selected content portions for excerpting or anthologizing, etc.). For example, a control set associated with the portable storage medium may accommodate a wide variety of different usage capabilities—with the more advanced or sophisticated uses requiring correspondingly more advanced protection and rights management enablement found on some platforms and not others. Lower-capability environments can, as another example, ignore (or not enable or attempt to use) rights in the control set that they don't understand, while higher-capability environments (having awareness of the

DISH-Blue Spike 842
Exhibit 1005, Page 1275

overall capabilities they provide), may, for example, enable the rights and corresponding protection techniques ignored by the lower-capability environments.

In accordance with another aspect provided by the invention, a media- and platform-independent security component can be scaled in terms of functionality and performance such that the elementary rights management requirements of consumer electronics devices are subsets of a richer collection of functionality that may be employed by more advanced platforms. The security component can be either a physical, hardware component, or a "software emulation" of the component. In accordance with this feature, an instance of medium (or more correctly, one version of the content irrespective of media) can be delivered to customers independently of their appliance or platform type with the assurance that the content will be protected. Platforms less advanced in terms of security and/or technical capabilities may provide only limited rights to use the content, whereas more advanced platforms may provide more expansive rights based on correspondingly appropriate security conditions and safeguards.

DISH-Blue Spike 842
Exhibit 1005, Page 1276

In accordance with a further aspect provided by the present invention, mass-produced, inexpensive home consumer DVD players (such as those constructed, for example, with minimum complexity and parts count) can be made to be compatible with the same DVDs or other portable storage media used by more powerful and/or secure platforms (such as, for example, personal computers) without degrading advanced rights management functions the storage media may provide in combination with the more powerful and/or secure platforms. The rights management and protection arrangement provided and supported in accordance with this aspect of the invention thus supports inexpensive basic copy protection and can further serve as a commercial convergence technology supporting a bridging that allows usage in accordance with rights of the same content by a limited resource consumer device while adequately protecting the content and further supporting more sophisticated security levels and capabilities by (a) devices having greater resources for secure rights management, and/or (b) devices having connectivity with other devices or systems that can supply further secure rights management resources. This aspect of the invention allows

DISH-Blue Spike 842
Exhibit 1005, Page 1277

multiple devices and/or other systems that participate and work together in a permanently or temporarily connected network to share the rights management for at least one or more electronic events (e.g., managed through the use of protected processing environments such as described in Ginter et al.) occuring at a single, or across multiple nodes and further allows the rights associated with parties and/or groups using and/or controlling such multiple devices and/or other systems to be employed according to underlying rights related rules and controls, this allowing, for example, rights available through a corporate executive's device to be combined with or substitute for, in some manner, the rights of one or more subordinate corporate employees when their computing or other devices of these parties are coupled in a temporary networking relationship and operating in the appropriate context. In general, this aspect of the invention allows distributed rights management for DVD or otherwise packaged and delivered content that is protected by a distributed, peer-to-peer rights management.Such distributed rights management can operate whether the DVD appliance or oth- electronic information usage device is participatin,

DISH-Blue Spike 842
Exhibit 1005, Page 1278

permanently or temporarily connected network and whether or not the relationships among the devices and/or other systems participating in the distributed rights management arrangement are relating temporarily or have a more permanent operating relationship. In this way, the same device may have different rights available depending on the context in which that device is operating (e.g., in a corporate environment such as in collaboration with other individuals and/or with groups, in a home environment internally and/or in collaboration with external one or more specified individuals and/or other parties, in a retail environment, in a classroom setting as a student where a student's notebook might cooperate in rights management with a classroom server and/or instructor PC, in a library environment where multiple parties are collaboratively employing differing rights to use research materials, on a factory floor where a hand held device works in collaboration with control equipment to securely and appropriately perform proprietary functions, and so on).

For example, coupling a limited resource device arrangement, such as a DVD appliance, with an inexpensive network computer (NC), or a personal computer (PC), may allow

DISH-Blue Spike 842
Exhibit 1005, Page 1279

an augmenting (or replacing) of rights management capabilities and/or specific rights of parties and/or devices by permitting rights management to be a result of a combination of some or all of the rights and/or rights management capabilities of the DVD appliance and those of an Network or Personal Computer (NC or PC). Such rights may be further augmented, or otherwise modified or replaced by the availability of rights management capabilities provided by a trusted (secure) remote network rights authority.

These aspects of the present invention can allow the same device, in this example a DVD appliance, to support different arrays, e.g., degrees, of rights management capabilities, in disconnected and connected arrangements and may further allow available rights to result from the availability of rights and/or rights management capabilities resulting from the combination of rights management devices and/or other systems. This may include one or more combinations of some or all of the rights available through the use of a "less" secure and/or resource poor device or system which are augmented, replaced, or otherwise modified through connection with a device or system that is

DISH-Blue Spike 842
Exhibit 1005, Page 1280

"more" or "differently" secure and/or resource rich and/or possesses differing or different rights, wherein such connection employs rights and/or management capabilities of either and/or both devices as defined by rights related rules and controls that describe a shared rights management arrangement.

In the latter case, connectivity to a logically and/or physically remote rights management capability can expand (by, for example, increasing the available secure rights management resources) and/or change the character of the rights available to the user of the DVD appliance or a DVD appliance when such device is coupled with an NC, personal computer, local server, and/or remote rights authority. In this rights augmentation scenario, additional content portions may be available, pricing may change, redistribution rights may change (e.g., be expanded), content extraction rights may be increased, etc.

Such "networking rights management" can allow for a combination of rights management resources of plural devices and/or other systems in diverse logical and/or physical relationships, resulting in either greater or differing rights through the enhanced resources provided by connectivity with one or more

DISH-Blue Spike 842
Exhibit 1005, Page 1281

"remote" rights authorities. Further, while providing for increased and/or differing rights management capability and/or rights, such a connectivity based rights management arrangement can support multi-locational content availability, by providing for seamless integration of remotely available content, for example, content stored in remote, Internet world wide web-based, database supported content repositories, with locally available content on one or more DVD discs.

In this instance, a user may experience not only increased or differing rights but may use both local DVD content and supplementing content (i.e., content that is more current from a time standpoint, more costly, more diverse, or complementary in some other fashion, etc.). In such an instance, a DVD appliance and/or a user of a DVD appliance (or other device or system connected to such appliance) may have the same rights, differing, and/or different rights applied to locally and remotely available content, and portions of local and remotely available content may themselves be subject to differing or different rights when used by a user and/or appliance. This arrangement can support an overall, profound increase in user content opportunities that are seamlessly

DISH-Blue Spike 842
Exhibit 1005, Page 1282

integrated and efficiently available to users in a single content searching and/or usage activity by exploiting the rights management and content resources of plural, connected arrangements.

Such a rights augmenting remote authority may be directly coupled to a DVD appliance and/or other device by modem, or directly or indirectly coupled through the use of an I/O interface, such as a serial 1394 compatible controller (e.g., by communicating between a 1394 enabled DVD appliance and a local personal computer that functions as a smart synchronous or asynchronous information communications interface to such one or more remote authorities, including a local PC or NC or server that serves as a local rights management authority augmenting and/or supplying the rights management in a DVD appliance).

In accordance with yet another aspect provided by this invention, rights provided to, purchased, or otherwise acquired by a participant and/or participant DVD appliance or other system can be exchanged among such peer-to-peer relating devices and/or other systems through the use of one or more permenantly or temporarily networked arrangments. In such a case, rights may be

DISH-Blue Spike 842
Exhibit 1005, Page 1283

bartered, sold, for currency, otherwise exchanged for value, and/or loaned so long as such devices and/or other systems participate in a rights management system, for example, such as the Virtual Distribution Environment described in Ginter, et al., and employ rights transfer and other rights management capabilities described therein. For example, this aspect of the present invention allows parties to exchange games or movies in which they have purchased rights. Continuing the example, an individual might buy some of a neighbor's usage rights to watch a movie, or transfer to another party credit received from a game publisher for the successful superdistribution of the game to several acquaintances, where such credit is transferred (exchanged) to a friend to buy some of the friend's rights to play a different game a certain number of times, etc.In accordance with yet another aspect provided by this invention, content carried by a portable storage medium such as a DVD is associated with one or more encryption keys and a secure content identifier. The content itself (or information required to use the content) is at least partially cryptographically encrypted—with associated decryption keys being required to decrypt the content before the content can be

DISH-Blue Spike 842
Exhibit 1005, Page 1284

used. The decryption keys may themselves be encrypted in the form of an encrypted key block. Different key management and access techniques may be used, depending on the platform.

In accordance with still yet another aspect provided by this invention, electronic appliances that "create" digital content (or even analog content) —e.g., a digital camera/video recorder or audio recorder—can be readily equipped with appropriate hardware and/or software so as to produce content that is provided within a secure container at the outset. For example, content recorded by a digital camera could be immediately packaged in a secure container by the camera as it is recording. The camera could then output content already packaged in a secure container(s). This could preclude the need to encapsulate the content at a later point in time or at a later production stage, thus, saving at least one production-process step in the overall implementation of electronic rights management in accordance with the present invention. Moreover, it is contemplated that the very process of "reading" content for use in the rights management environment might occur at many steps along a conventional production and distribution process (such as during editing and/or

DISH-Blue Spike 842
Exhibit 1005, Page 1285

the so called "pressing" of a master DVD or audio disk, for example). Accordingly, another significant advantage of the present invention is that rights management of content essentially can be extended throughout and across each appropriate content creation, editing, distribution, and usage stages to provide a seamless content protection architecture that protects rights throughout an entire content life cycle.

In one example embodiment, the storage medium itself carries key block decryption key(s) in a hidden portion of the storage medium not normally accessible through typical access and/or copying techniques. This hidden key may be used by a drive to decrypt the encrypted key block—such decrypted key block then being used to selectively decrypt content and related information carried by the medium. The drive may be designed in a secure and tamper-resistant manner so that the hidden keys are never exposed outside of the drive to provide an additional security layer.

In accordance with another example embodiment, a video disk drive may store and maintain keys used to decrypt an encrypted key block. The key block decryption keys may be

DISH-Blue Spike 842
Exhibit 1005, Page 1286

stored in a drive key store, and may be updatable if the video disk drive may at least occasionally use a communications path provided, for example, by a set top box, network port or other communications route.

In accordance with a further example embodiment, a virtual distribution environment secure node including a protected processing environment such as a hardware-based secure processing unit may control the use of content carried by a portable storage medium such as a digital video disk in accordance with control rules and methods specified by one or more secure containers delivered to the secure node on the medium itself and/or over an independent communications path such as a network.

Certain conventional copy protection for DVD currently envisions CGMA copy protection control codes combined with certain encryption techniques first proposed apparently by Matsushita Corporation. Notwithstanding the limited benefits of this approach to digital property protection, the present invention is capable of providing a supplementary, compatible, and far more comprehensive rights management system while also providing

DISH-Blue Spike 842
Exhibit 1005, Page 1287

additional and/or different options and solutions. The following are some additional examples of advantageous features provided in accordance with the inventions:

- Strong security to fully answer content supplier needs.

- Value chain management automation and efficiencies including distributed rights protection, "piece of the tick" payment disaggregation to value chain participants, cost-effective micro-transaction management, and superdistribution, including offline micropayment and microtransaction support for at least occasionally connected devices.

- Simplified, more efficient channel management including support for the use of the same content deliverable on limited resource, greater resource, standalone, and/or connected devices.

- Can be used with any medium and application type and/or all forms of content and content models -- not just compressed video and sound as in some prior techniques and supports the use of copies of the same or materially the

DISH-Blue Spike 842
Exhibit 1005, Page 1288

same content containers across a wide variety of media delivery systems (e.g., broadcast, Internet repository, optical disc, etc) for operation on a wide variety of different electronic appliances (e.g., digital cameras, digital editing equipment, sound recorders, sound editing equipment, movie theater projectors, DVD appliances, broadcast tape players, personal computers, smart televisions, etc).

- Asset management and revenue and/or other consideration maximizing through important new content revenue and/or other consideration opportunities and the enhancement of value chain operating efficiencies.

- Is capable of providing 100% compatibility with the other protection techniques such as, for example, CGMA protection codes and/or Matsushita data scrambling approaches to DVD copy protection.

- Can be employed with a variety of existing data scrambling or protection systems to provide very high degrees of compatibility and/or level of functionality.

DISH-Blue Spike 842
Exhibit 1005, Page 1289

- Allows DVD technology to become a reusable, programmable, resource for an unlimited variety of entertainment, information commerce, and cyberspace business models.

- Enables DVD drive and/or semiconductor component manufacturers and/or distributors and/or other value adding participants to become providers of, and rights holders in, the physical infrastructure of the emerging, connected world of the Internet and Intranets where they may charge for the use of a portion (e.g., a portion they provided) of the distributed, physical infrastructure as that portion participates in commercial networks. Such manufacturers and/or distributors and/or other value adding participants can enjoy the revenue benefits resulting from participation in a "piece of the tick" by receiving a small portion of the revenue received as a result of a participating transaction.

- Provides automated internationalization, regionalization, and rights management in that:

-- DVD content can be supplied with arrays of different rule sets for

DISH-Blue Spike 842
Exhibit 1005, Page 1290

automatic use depending on rights and identity of the user; and

-- Societal rights, including taxes, can be handled transparently.

In addition, the DVD rights management method and apparatus of the present invention provides added benefits to media recorders/publishers in that it:

- Works with a current "keep honest people honest" philosophy.
- Can provide 100% compatibility with other protection schemes such as for example, Matsushita data scrambling and/or CGMA encoded discs.
- Can work with and/or supplement other protection schemes to provide desired degree and/or functionality, or can be used in addition to or instead of other approaches to provide additional and/or different functionality and features.

DISH-Blue Spike 842
Exhibit 1005, Page 1291

- Provides powerful, extensible rights management that reaches beyond limited copy protection models to rights management for the digitally convergent world.

- Empowers recording/publishing studios to create sophisticated asset management tools.

- Creates important business opportunities through controlled use of studio properties in additional multimedia contexts.

- Uniquely ties internationalization, regionalization, superdistribution, repurposing, to content creation processes and/or usage control.

Other aspects of the present invention provide benefits to other types of rightsholders, such as for example:

- Persistent, transparent protection of digital content—globally, through value chain and process layers.

- Significant reduction in revenue loss from copying and pass-along.

DISH-Blue Spike 842
Exhibit 1005, Page 1292

- Converts "pass-along," copying, and many forms of copyright infringement from a strategic business threat to a fundamental business opportunity.

- A single standard for all digital content regardless of media and/or usage locality and other rights variables.

- Major economies of scale and/or scope across industries, distribution channels, media, and content type.

- Can support local usage governance and auditing within DVD players allowing for highly efficient micro-transaction support, including multiparty microtransactions and transparent multiparty microtransactions.

- Empowers rightsholders to employ the broadest range of pricing, business models, and market strategies—as they see fit.

Further aspects of the present invention which may prove beneficial to DVD and other digital medium appliance manufacturers are:

DISH-Blue Spike 842
Exhibit 1005, Page 1293

- Capable of providing bit for bit compatibility with existing discs.

- Content type independent.

- Media independent and programmable/reusable.

- Highly portable transition to next generation of appliances having higher density devices and/or a writable DVD and/or other optical media format(s).

- Participation in revenue flow generated using the appliance.

- Single extensible standard for all digital content appliances.

- Ready for the future "convergent" world in which many appliances are connected in the home using, as one example, IEEE 1394 interfaces or other means (e.g., some appliances will be very much like computers and some computers will be very much like appliances).

DISH-Blue Spike 842
Exhibit 1005, Page 1294

Aspects of the present inventions provide many benefits to computer and OS manufacturers such as for example:

- Implementation in computers as an extension to the operating system, via for example, at least one transparent plug-in, and does not require modifications to computer hardware and/or operating systems.

- Easy, seamless integration into operating systems and into applications.

- Extremely strong security, especially when augmented with "secure silicon" (i.e., hardware/firmware protection apparatus fabricated on chip).

- Transforms user devices into true electronic commerce appliances.

- Provides a platform for trusted, secure rights management and event processing.

- Programmable for customization to specialized requirements.

DISH-Blue Spike 842
Exhibit 1005, Page 1295

Additional features and advantages provided in accordance with the inventions include, for example:

- Information on the medium (for example, both properties and metadata) may be encrypted or not.

- Different information (for example, properties, metadata) may be encrypted using different keys. This provides greater protection against compromise, as well as supporting selective usage rights in the context of a sophisticated rights management system.

- There may be encrypted keys stored on the medium, although this is not required. These keys may be used to decrypt the protected properties and metadata. Encrypted keys are likely to be used because that allows more keying material for the information itself, while still keeping access under control of a single key.

- Multiple sets of encrypted keys may be stored on the medium, either to have different sets of keys associated with different information, or to allow multiple control regimes to use the

DISH-Blue Spike 842
Exhibit 1005, Page 1296

same information, where each control regime may use one or more different keys to decrypt the set of encrypted keys that it uses.

- To support the ability of the player to access rights managed containers and/or content, a decryption key for the encrypted keys may be hidden on the medium in one or more locations that are not normally accessible. The "not normally accessible" location(s) may be physically enabled for drives installed in players, and disabled for drives installed in computers. The enablement may be different firmware, a jumper on the drive, etc.

- The ability of the player to access rights managed containers and/or content may also be supported by one or more stored keys inside the player that decrypts certain encrypted keys on the medium.

- Keys in a player may allow some players to play different properties than others. Keys could be added to, and/or deleted from the player by a network connection (e.g., to a PC, a cable system, and/or a modem connection to a source of new and/or additional keys and/or

DISH-Blue Spike 842
Exhibit 1005, Page 1297

key revocation information) or automatically loaded by "playing" a key distribution DVD.

- Controlling computer use may be supported by some or all of the same techniques that control player use of content and/or rights managemnt information.

- Controlling computer use of content and/or rights management information may be supported by having a computer receive, through means of a trusted rights management system, one or more appropriate keys.

- A computer may receive additional keys that permit decryption of certain encrypted keys on the medium.

- A computer may receive additional keys that permit decryption of one or more portions of encrypted data directly. This may permit selective use of information on the medium without disclosing keys (e.g., a player key that decrypts any encrypted keys).

In accordance with further aspects provided by the present invention, a secure "software container" is provided that allows:

DISH-Blue Spike 842
Exhibit 1005, Page 1298

- Cryptographically protected encapsulation of content, rights rules, and usage controls.

- Persistent protection for transport, storage, and value chain management.

- Sophisticated rules interface architecture.

Elements can be delivered independently, such as new controls, for example, regarding discount pricing (e.g. sale pricing, specific customer or group discounts, pricing based on usage patterns, etc.) and/or other business model changes, can be delivered after the property has been distributed (this is especially beneficial for large properties or physical distribution media (e.g., DVD, CD-ROM) since redistribution costs may be avoided and consumers may continue to use their libraries of discs). In addition, encrypted data can be located "outside" the container. This can allow, for example, use of data stored independently from the controls and supports "streaming" content as well as "legacy" systems (e.g., CGMS).

DISH-Blue Spike 842
Exhibit 1005, Page 1299

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages provided in accordance with these inventions may be better and more completely understood by referring to the following detailed description of presently preferred examples in conjunction with the drawings, of which:

Figure 1A shows example home consumer electronics equipment for using portable storage media such as digital video disks;

Figure 1B shows example secure node equipment for using the same portable storage media but providing more advanced rights management capabilities;

Figure 1C shows an example process for manufacturing protected optical disks;

Figure 2A shows an example architecture of the Figure 1A consumer electronics equipment;

Figure 2B shows an example architecture for the Figure 1B secure node equipment;

DISH-Blue Spike 842
Exhibit 1005, Page 1300

Figure 3 shows example data structures used by the Figure 1A equipment;

Figure 3A and 3B show example control set definitions;

Figures 4A and 4B show example usage techniques provided by the Figure 1A appliance;

Figure 5 shows example data structures used by the Figure 1B secure node for accessing information on the storage medium;

Figure 6 shows an example usage technique performed by the Figure 1B secure node;

Figure 7 is a block diagram illustrating an example of a special secure software container contained on a DVD;

Figure 8 is a block diagram illustrating an example of a secure container along with the video property content stored on a DVD medium;

Figure 9 is a block diagram illustrating another example of a standard container stored on a DVD medium including an additional container having a more complex rule arrangement for use, for example, with a secure node;

DISH-Blue Spike 842
Exhibit 1005, Page 1301

Figure 10 shows an example use of a DVD having a container (i.e., stored on the medium) with a DVD player provided with a secure rights management node, and also shows use of the same DVD with a DVD player that does not have a secure rights management node;

Figure 11 is a block diagram illustrating use of a DVD that does not have a container on a DVD player that is provided with rights management secure node in accordance with the present invention as compared with use of the same DVD with a DVD player that does not have a secure node;

Figures 12-14 show example network configurations; and

Figures 15A-15C show an example virtual rights process.

DETAILED DESCRIPTION OF PRESENTLY PREFERRED EXAMPLE EMBODIMENTS

Overall Example Digital Video Disk Usage System

Figure 1A shows example inexpensive mass-produced home consumer electronics equipment 50 for using information stored on a storage medium 100 such as a portable digitally-encoded optical disk (e.g., a digital video disk or "DVD").

DISH-Blue Spike 842
Exhibit 1005, Page 1302

Consumer equipment 50 includes a dedicated disk player 52, that in some embodiments, may also have the capability to write optical media (writeable DVD disks, or "DVD-RAM") for example) as well, connected to a home color television set 54. A remote control unit 56 may be used to control the disk player 52 and/or television set 54.

In one example, disk 100 may store a feature length motion picture or other video content. Someone wishing to watch the content stored on disk 100 may purchase or rent the disk, insert the disk into player 52 and use remote control 56 (and/or controls 58 that may be provided on player 52) to control the player to play back the content via home television set 54.

In some embodiments, remote control 56 (and/or controls 58 that may be provided on device 52) may be used to control the recording of a movie, for example. Player 52 reads the digitized video and audio information carried by disk 100, converts it into signals compatible with home color television set 54, and provides those signals to the home color television set.

DISH-Blue Spike 842
Exhibit 1005, Page 1303

In some embodiments, television set 54 (and/or a set top box) provide the video signals to be recorded by device 52 on writable optical media, DVD-RAM in one non-limiting example. Television set 54 produces images on screen 54a and produces sounds through loudspeakers 54b based on the signals player 52 provides to the television set.

The same disk 100 may be used by a more advanced platform 60 shown in Figure 1B. Platform 60 may include, for example, a personal computer 62 connected to a display monitor 64, a keyboard 66, a mouse pointing device 68, and a loudspeaker 70. In this example, platform 60 may be able to play back the content stored on disk 100 in the same way as dedicated disk player 52, but may also be capable of more sophisticated and/or advanced uses of the content as enabled by the presence of secure node 72 within the platform. (In some embodiments, platform 60 may also be able to record content on writable optical media, DVD-RAM, in one non-limiting example.) For example, it may be possible, using platform 60 and its secure node 72, to interactively present the motion picture or other content such that the user may input choices via keyboard 66 and/or mouse pointing device 68

DISH-Blue Spike 842
Exhibit 1005, Page 1304

that, in real time, change the presentation provided via display 64 and loudspeaker 60.

As one example, the platform 60 user selects from options displayed on display 64 that cause the content presentation sequence to change (e.g., to provide one of a number of different endings, to allow the user to interactively control the flow of the images presented, etc.). Computer 62 may also be capable of using and manipulating digital data including for example computer programs and/or other information stored on disk 100 that player 52 cannot handle.

Secure node 72 provides a secure rights management facility that may, for example, permit more invasive or extensive use of the content stored on disk. For example, dedicated player 52 may prevent any copying of content stored by disk 100, or it may allow the content to be copied only once and never again. Platform 60 including secure node 72, on the other hand, may allow multiple copies of some or all of the same content—but only if certain conditions are met (e.g., the user of equipment 60 falls within a certain class of people, compensation at an agreed on rate is securely provided for each copy made, only certain excerpts of

DISH-Blue Spike 842
Exhibit 1005, Page 1305

the content are copied, a secure audit trail is maintained and reported for each copy so made, etc.). (In some embodiments, dedicated player 52 may send protected content only to devices authenticated as able to enforce securely rights management rules and usage consequences. In some embodiments, devices may authenticate using digital certificates, one non-limiting example being certificates conforming to the X.509 standard.) Hence, platform 60 including secure node 72 can, in this example, use the content provided by disk 100 in a variety of flexible, secure ways that are not possible using dedicated player 52—or any other appliance that does not include a secure node.

Example Secure Disk Creation and Distribution Process

Figure 1C shows an example secure process for creating a master multimedia DVD disk 100 for use with players 50, 60. In this example, a digital camera 350 converts light images (i.e., pictures) into digital information 351 representing one or a sequence of images. Digital camera 350 in this example includes a secure node 72A that protects the digital information 351 before it leaves camera 350. Such protection can be accomplished, for

DISH-Blue Spike 842
Exhibit 1005, Page 1306

example, by packaging the digital information within one or more containers and/or associating controls with the digital information.

In this example, digital camera 350 provides the protected digital image information 351 to a storage device such as, for example, a digital tape recorder 352. Tape recorder 352 stores the digital image information 351 (along with any associated controls) onto a storage medium such as magnetic tape cartridge 354 for example. Tape recorder 352 may also include a secure node 72B. Secure node 72B in this example can understand and enforce the controls that the digital camera secure node 72A applies to and/or associated with the digital information 351, and/or it may apply its own controls to the stored information.

The same or different tape recorder 352 may play back protected digital information 351 to a digital mixing board 356. Digital mixing board 356 may mix, edit, enhance or otherwise process the digital information 351 to generate processed digital information 358 representing one or a sequence of images. Digital mixing board 356 may receive additional inputs from other devices such as for example other tape recorders, other digital cameras, character generators, graphics generators, animators, or

DISH-Blue Spike 842
Exhibit 1005, Page 1307

any other image-based devices. Any or all of such devices may also include secure nodes 72 to protect the information they generate. In some embodiments, some of the digital information can be derived from equipment including a secure node, and other digital information can be derived from equipment that has no secure node. In still other embodiments, some of the digital information provided to digital mixer 356 is protected and some is not protected.

Digital mixing board 356 may also include a secure node 72C in this example. The digital mixing board secure node 72C may enforce controls applied by digital camera secure node 72A and/or tape recorder secure node 72B, and/or it may add its own protections to the digital information 358 it generates.

In this example, an audio microphone 361 receives sound and converts the sound into analog audio signals. The audio signals in this example are inputted to a digital audio tape recorder 362. In the example shown, tape recorder 362 and audio mixer 364 are digital devices. However, in other embodiments, one, the other or both of these devices may operate in the analog domain. In the example shown, digital audio tape recorder 362 converts the

analog audio signals into digital information representing the sounds, and stores the digital information (and any associated controls) onto a tape 362.

In this example, audio tape recorder 362 includes a secure node 72E that may associate controls with the information stored on tape 363. Such controls may be stored with the information on the tape 363. In another embodiment, microphone 361 may include its own internal secure node 72 that associates control information with the audio information (e.g., by steganographically encoding the audio information with control information). The tape recorder 362 may enforce such controls applied by microphone 361.

Alternatively, microphone 361 may operate in the digital domain and provide digital representations of audio, perhaps including control information supplied by secure node 72 optionally incorporated in microphone 361, directly to connected devices such as audio tape recorder 362. Digital representations may optionally be substituted for analog representations of any signals between the devices in the example Figure 1C.

DISH-Blue Spike 842
Exhibit 1005, Page 1309

The same or different tape recorder 362 may play back the information recorded on tape 363, and provide the information 366 to an audio mixer 364. Audio mixer 364 may edit, mix, or otherwise process the information 366 to produce information 368 representing one or a sequence of sounds. Audio mixer 364 may also receive inputs from other devices such as for example other tape recorders, other microphones, sound generators, musical synthesizers, or any other audio-based devices. Any or all of such devices may also include secure nodes 72 to protect the information they generate. In some embodiments, some of the digital information is derived from equipment including a secure node, and other digital information is derived from equipment that has no secure node. In still other embodiments, some of the digital information provided to audio mixer 364 is protected and some is not protected.

Audio mixer 364 in this example includes a secure node 72F that enforces the controls, if any, applied by audio tape recorder secure node 72E; and/or applies its own controls.

Digital image mixer 356 may provide digital information 358 to "DVD-RAM" equipment 360 that is capable of writing to

DISH-Blue Spike 842
Exhibit 1005, Page 1310

master disks 100 and/or to disks from which master dicks may be created Similarly, audio mixer 364 may provide digital information 368 to equipment 360. Equipment 360 records the image information 358 and audio information 368 onto master disk 100. In this example, equipment 360 may include a secure node 72D that enforces controls applied by digital camera secure node 72A, tape recorder secure node 72B, digital mixer secure node 72C audio tape recorder secure node 72E and/or audio mixer secure node 72F; and/or it may add its own protections to the digital information 358 it writes onto master disks 100. A disk manufacturer can then mass-produce disks 100(1)-100(N) based on the master disk 100 using conventional disk mass-production equipment for distribution through any channels (e.g., video and music stores, websites, movie theaters, etc.). Consumer appliances 50 shown in Figures 1A and 1B may play back the disks 100 – enforcing the controls applied to the information stored on the disks 100. Secure nodes 72 thus maintain end-to-end, persistent secure control over the images generated by digital camera 350 and the sounds generated by microphone 361 during the entire process of making, distributing and using disks 100.

DISH-Blue Spike 842
Exhibit 1005, Page 1311

In the Figure 1C example shown, the various devices may communicate with one another over so-called "IEEE 1394" high-speed digital serial busses. In this context, "IEEE 1394" refers to hardware and software standards set forth in the following standards specification incorporated by reference herein: 1394-1995 IEEE Standard for a High Performance Serial Bus, No. 1-55937-583-3 (Institute of Electrical and Electronics Engineers 1995). This specification describes a high-speed memory mapped digital serial bus that is self-configuring, hot pluggable, low cost and scalable. The bus supports isochronous and asynchronous transport at 100, 200 or 400 Mbps, and flexibly supports a number of different topologies. The specification describes a physical level including two power conductors and two twisted pairs for signalling. The specification further describes physical, link and transaction layer protocols including serial bus management. Alternatively, any other suitable electronic communication means may be substituted for the "IEEE 1394" medium shown in Figure 1C, including other wired media (e.g., Ethernet, universal serial bus), and/or wireless media based on radio-frequency (RF)

DISH-Blue Spike 842
Exhibit 1005, Page 1312

transmission, infra-red signals, and/or any other means and/or types of electronic communication.

Example Dedicated Player Architecture

Figure 2A shows an example architecture for dedicated player 52. In this example, player 52 includes a video disk drive 80, a controller 82 (e.g., including a microprocessor 84, a memory device such as a read only memory 86, and a user interface 88), and a video/audio processing block 90. Video disk drive 80 optically and physically cooperates with disk 100, and reads digital information from the disk. Controller 82 controls disk drive 80 based on program instructions executed by microprocessor 84 and stored in memory 86 (and further based on user inputs provided by user interface 88 which may be coupled to controls 58 and/or remote control unit 56). Video/audio processing block 90 converts digital video and audio information read by disk drive 80 into signals compatible with home color television set 54 using standard techniques such as video and audio decompression and the like. Video/audio processing block 90 may also insert a visual marking indicating the ownership and/or protection of the video program. Block 90 may also

DISH-Blue Spike 842
Exhibit 1005, Page 1313

introduce a digital marking indicating to a standard recording device that the content should not be recorded.

Example Secure Node Architecture

Figure 2B shows an example architecture for platform 60 shown in Figure 1B—which in this example is built around a personal computer 62 but could comprise any number of different types of appliances. In this example, personal computer 62 may be connected to an electronic network 150 such as the Internet via a communications block 152. Computer equipment 62 may include a video disk drive 80' (which may be similar or identical to the disk drive 80 included within example player 52). Computer equipment 62 may further include a microprocessor 154, a memory 156 (including for example random access memory and read only memory), a magnetic disk drive 158, and a video/audio processing block 160. Additionally, computer equipment 62 may include a tamper-resistant secure processing unit 164 or other protected processing environment. Secure node 72 shown in Figure 1B may thus be provided by a secure processing unit 164, software executing on microprocessor 154, or a combination of

the two. Different embodiments may provide secure node 72 using software-only, hardware-only, or hybrid arrangements.

Secure node 72 in this example may provide and support a a general purpose Rights Operating System employing reusable kernel and rights language components. Such a commerce-enabling Rights Operating System provides capabilities and integration for advanced commerce operating systems of the future. In the evolving electronic domain, general purpose, reusable electronic commerce capabilities that all participants can rely on will become as important as any other capability of operating systems. Moreover, a rights operating system that provides, among other things, rights and auditing operating system functions can securely handle a broad range of tasks that relate to a virtual distribution environment. A secure processing unit can, for example, provide or support many of the security functions of the rights and auditing operating system functions. The other operating system functions can, for example, handle general appliance functions. The overall operating system may, for example, be designed from the beginning to include the rights and auditing operating system functions plus the other operating

system functions, or the rights and auditing operating system functions may, in another example, be an add-on to a preexisting operating system providing the other operating system functions. Any or all of these features may be used in combination with the invention disclosed herein.

Example Disk Data Structures and Associated Protections

Figure 3 shows some example data structures stored on disk 100. In this example, disk 100 may store one or more properties or other content 200 in protected or unprotected form. Generally, in this example, a property 200 is protected if it is at least in part encrypted and/or associated information needed to use the property is at least in part encrypted and/or otherwise unusable without certain conditions having being met. For example, property 200(1) may be completely or partially encrypted using conventional secure cryptographic techniques. Another property 200(2) may be completely unprotected so that it can be used freely without any restriction. Thus, in accordance with this example, disk 100 could store both a movie as a protected property 200(1) and an unprotected interview with the actors and producers or a

DISH-Blue Spike 842
Exhibit 1005, Page 1316

"trailer" as unprotected property 200(2). As shown in this example, disk 100 may store any number of different properties 200 in protected or unprotected form as limited only by the storage capacity of the disk.

In one example, the protection mechanisms provided by disk 100 may use any or all of the protection (and/or other) structures and/or techniques described in the above-referenced Shear patents. The Shear patents describe, by way of non-exhaustive example, means for solving the problem of how to protect digital content from unauthorized use. For example, the Shear patent specifications describe, among other things, means for electronically "overseeing" -- through distributed control nodes present in client computers -- the use of digital content. This includes means and methods for fulfilling the consequences of any such use.

Non-limiting examples of certain elements described in the Shear patent specifications include:

(a) decryption of encrypted information,

(b) metering,

(c) usage control in response to a combination of derived metering information and rules set by content providers,

(d) securely reporting content usage information,

(e) use of database technology for protected information storage and delivery,

(f) local secure maintenance of budgets, including, for example, credit budgets,

(g) local, secure storage of encryption key and content usage information,

(h) local secure execution of control processes, and

(i) in many non-limiting instances, the use of optical media.

Any or all of these features may be used in combination in or with the inventions disclosed herein.

Certain of the issued Shear patents' specifications also involve database content being local and remote to users.

DISH-Blue Spike 842
Exhibit 1005, Page 1318

Database information that is stored locally at the end-user's system and complemented by remote, "on-line" database information, can, for example, be used to augment the local information, which in one example, may be stored on optical media (for example, DVD and/or CD-ROM). Special purpose semiconductor hardware can, for example, be used to provide a secure execution environment to ensure a safe and reliable setting for digital commerce activities.

The Shear patents also describe, among other things, database usage control enabled through the use of security, metering, and usage administration capabilities. The specifications describe, *inter alia*, a metering and control system in which a database, at least partially encrypted, is delivered to a user (e.g., on optical media). Non-limiting examples of such optical media may, for example, include DVD and CD-ROM. Subsequent usage can, for example, be metered and controlled in any of a variety of ways, and resulting usage information can be transmitted to a responsible party (as one example).

The Shear patent specifications also describe the generation of a bill in response to the transmitted information. Other

embodiments of the Shear patents provide, for example, unique information security inventions which involve, for example, digital content usage being limited based on patterns of usage such as the quantity of particular kinds of usage. These capabilities include monitoring the "contiguousness," and/or "logical relatedness" of used information to ensure that the electronic "conduct" of an individual does not exceed his or her licensed rights. Still other aspects of the Shear patents describe, among other things, capabilities for enabling organizations to securely and locally manage electronic information usage rights. When a database or a portion of a database is delivered to a client site, some embodiments of the Shear patents provide, for example, optical storage means (non-exhaustive examples of which include DVD and CD-ROM) as the mechanism of delivery. Such storage means can store, for example, a collection of video, audio, images, software programs, games, etc., in one example, on optical media, such as DVD and/or CD-ROM, in addition to other content such as a collection of textual documents, bibliographic records, parts catalogs, and copyrighted or uncopyrighted materials of all kinds.

DISH-Blue Spike 842
Exhibit 1005, Page 1320

Any or all of these features may be used in the embodiments herein.

One specific non-limiting embodiment could, for example, involve a provider who prepares a collection of games. The provider prepares a database "index" that stores information pertaining to the games, such as for example, the name, a description, a creator identifier, the billing rates, and the maximum number of times or total elapsed time each game may be used prior to a registration or re-registration requirement. Some or all of this information could be stored in encrypted form, in one example, on optical media, non-limiting examples of which include DVD and CD-ROM. The provider may then encrypt some or all portions of the games such that a game could not be used unless one or more encrypted portions were decrypted. Typically, decryption would not occur unless provider specified conditions were satisfied, in one example, unless credit was available to compensate for use and audit information reflecting game usage was being stored. The provider could determine, for example: which user activities he or she would allow, whether to meter such activities for audit and/or control purposes, and what, if any, limits

would be set for allowed activities. This might include, for example, the number of times that a game is played, and the duration of each play. Billing rates might be discounted, for example, based on total time of game usage, total number of games currently registered for use, or whether the customer was also registered for other services available from the same provider, etc.

In the non-limiting example discussed above, a provider might, for example, assemble all of the prepared games along with other, related information, and publish the collection on optical media, non-limiting examples of which include CD-ROM and/or DVD. The provider might then distribute this DVD disk to prospective customers. The customers could then select the games they wish to play, and contact the provider. The provider, based on its business model, could then send enabling information to each authorized customer, such as for example, including, or enabling for use, decryption keys for the encrypted portion of the selected games (alternatively, authorization to use the games may have arrived with the DVD and/or CD-ROM disk, or might be automatically determined, based on provider set criteria, by the

DISH-Blue Spike 842
Exhibit 1005, Page 1322

user's secure client system, for example, based on a user's participation in a certified user class). Using the user's client decryption and metering mechanism the customer could then make use of the games. The mechanism might then record usage information, such as for example, the number of times the game was used, and, for example, the duration of each play. It could periodically transmit this information the game provider, thus substantially reducing the administration overhead requirements of the provider's central servers. The game provider could receive compensation for use of the games based upon the received audit information. This information could be used to either bill their customers or, alternatively, receive compensation from a provider of credit.

Although games provide one convenient, non-limiting example, many of these same ideas can be easily applied to all kinds of content, all kinds of properties, including, by way of non-limiting examples:

- video,
- digitized movies,

DISH-Blue Spike 842
Exhibit 1005, Page 1323

- audio,
- images,
- multimedia,
- software,
- games,
- any other kind of property
- any combination of properties.

Other non-limiting embodiments of the Shear patent specifications support, for example, securely controlling different kinds of user activities, such as displaying, printing, saving electronically, communicating, etc. Certain aspects further apply different control criteria to these different usage activities. For example, information that is being browsed may be distinguished from information that is read into a host computer for the purpose of copying, modifying, or telecommunicating, with different cost rates being applied to the different activities (so that, for example,

the cost of browsing can be much less than the cost of copying or printing).

The Shear patent specifications also, for example, describe management of information inside of organizations by both publishers and the customer. For example, an optional security system can be used to allow an organization to prevent usage of all or a portion of an information base unless the user enters his security code. Multiple levels of security codes can be supported to allow restriction of an individual's use according to his security authorization level. One embodiment can, for example, use hardware in combination with software to improve tamper resistance, and another embodiment could employ an entirely software based system. Although a dedicated hardware/software system may under certain circumstances provide assurance against tampering, techniques which may be implemented in software executing on a non-dedicated system may provide sufficient tamper resistance for some applications. Any or all of these features may be used in combination with the technology disclosed in this patent specification.

Figures 3 Disks May Also Store Metadata, Controls and Other Information

In this example, disk 100 may also store "metadata" in protected and/or unprotected form. Player 52 uses metadata 202 to assist in using one or more of the properties 200 stored by disk 100. For example, disk 100 may store one metadata block 202(1) in unprotected form and another metadata block 202(2) in protected form. Any number of metadata blocks 202 in protected and/or unprotected form may be stored by disk 100 as limited only by the disk's storage capacity. In this example, metadata 202 comprises information used to access properties 200. Such metadata 202 may comprise, for example, frame sequence or other "navigational" information that controls the playback sequence of one or more of the properties 200 stored on disk 100. As one example, an unprotected metadata block 202 may access only selected portions of a protected property 200 to generate an abbreviated "trailer" presentation, while protected metadata block 202 may contain the frame playback sequence for the entire video presentation of the property 200. As another example, different metadata blocks 202 may be provided for different "cuts" of the

DISH-Blue Spike 842
Exhibit 1005, Page 1326

same motion picture property 200 (e.g., an R-rated version, a PG-rated version, a director's cut version, etc.).

In this example, disk 100 may store additional information for security purposes. For example, disk 100 may store control rules in the form of a control set 204—which may be packaged in the form of one or more secure containers 206. Commerce model participants can securely contribute electronic rules and controls that represent their respective "electronic" interests. These rules and controls extend a "Virtual Presence™" through which the commerce participants may govern remote value chain activities according to their respective, mutually agreed to rights. This Virtual Presence may take the form of participant specified electronic conditions (e.g., rules and controls) that must be satisfied before an electronic event may occur. These rules and controls can be used to enforce the party's rights during "downstream" electronic commerce activities. Control information delivered by, and/or otherwise available for use with, VDE content containers may, for example, constitute one or more "proposed" electronic agreements which manage the use and/or consequences of the use of such content and which can enact the

DISH-Blue Spike 842
Exhibit 1005, Page 1327

terms and conditions of agreements involving multiple parties and their various rights and obligations.

The rules and controls from multiple parties can be used, in one example, to form aggregate control sets ("Cooperative Virtual Presence™") that ensure that electronic commerce activities will be consistent with the agreements amongst value chain participants. These control sets may, for example, define the conditions which govern interaction with protected digital content (disseminated digital content, appliance control information, etc.). These conditions can, for example, be used to control not only digital information use itself, but also the consequences of such use. Consequently, the individual interests of commerce participants are protected and cooperative, efficient, and flexible electronic commerce business models can be formed. These models can be used in combination with the present invention.

Disks May Store Encrypted Information

Disk 100 may also store an encrypted key block 208. In this example, disk 100 may further store one or more hidden keys 210. In this example, encrypted key block 208 provides one or more cryptographic keys for use in decrypting one or more properties

DISH-Blue Spike 842
Exhibit 1005, Page 1328

200 and/or one or more metadata blocks 202. Key block 208 may provide different cryptographic keys for decrypting different properties 200 and/or metadata blocks 202, or different portions of the same property and/or metadata block. Thus, key block 208 may comprise a large number of cryptographic keys, all of which are or may be required if all of the content stored by disk 100 is to be used. Although key block 208 is shown in Figure 3 as being separate from container 206, it may be included within or as part of the container if desired.

Cryptographic key block 208 is itself encrypted using one or more additional cryptographic keys. In order for player 52 to use any of the protected information stored on disk 100, it must first decrypt corresponding keys within the encrypted key block 208—and then use the decrypted keys from the key block to decrypt the corresponding content.

In this example, the keys required to decrypt encrypted key block 208 may come from several different (possibly alternative) sources. In the example shown in Figure 3, disk 100 stores one or more decryption keys for decrypting key block 208 on the medium itself in the form of a hidden key(s) 210. Hidden key(s) 210 may

DISH-Blue Spike 842
Exhibit 1005, Page 1329

be stored, for example, in a location on disk 100 not normally accessible. This "not normally accessible" location could, for example, be physically enabled for drives 80 installed in players 52 and disabled for drives 80' installed in personal computers 62. Enablement could be provided by different firmware, a jumper on drive 80, etc. Hidden key(s) 210 could be arranged on disk 100 so that any attempt to physically copy the disk would result in a failure to copy the hidden key(s). In one example a hidden key(s) could be hidden in the bit stream coding sequences for one or more blocks as described by J. Hogan (Josh Hogan, "DVD Copy Protection," presentation to DVD copy protect technical meeting #4, 5/30/96, Burbank, CA.)

Alternatively, and/or in addition, keys required to decrypt encrypted key block 208 could be provided by disk drive 80. In this example, disk drive 80 might include a small decryption component such as, for example, an integrated circuit decryption engine including a small secure internal key store memory 212 having keys stored therein. Disk drive 80 could use this key store 212 in order to decrypt encrypted key block 208 without exposing either keys 212 or decrypted key block 208—and then use the

decrypted key from key block 208 to decrypt protected content 200, 202.

Disks May Store and/or Use Secure Containers

In yet another example, the key(s) required to decrypt protected content 200, 202 is provided within secure container 206. Figure 3A shows a possible example of a secure container 206 including information content 304 (properties 200 and metadata 202 may be external to the container—or alternatively, most or all of the data structures stored by video disk 100 may be included as part of a logical and/or actual protected container). The control set 204 shown in Figure 3 may comprise one or more permissions record 306, one or more budgets 308 and/or one or more methods 310 as shown in Figure 3A. Figure 3B shows an example control set 204 providing one or more encryption keys 208, one or more content identifiers 220, and one or more controls 222. In this example, different controls 222 may apply to different equipment and/or classes of equipment such as player 52 and/or computer equipment 62 depending upon the capabilities of the particular platform and/or class of platform. Additionally, controls 220 may apply to different ones of properties 200 and/or

DISH-Blue Spike 842
Exhibit 1005, Page 1331

different ones of metadata blocks 202. For example, a control 222(1) may allow property 200(1) to be copied only once for archival purposes by either player 52 or computer equipment 62. A control 222(2) (which may be completely ignored by player 52 because it has insufficient technical and/or security capabilities but which may be useable by computer equipment 62 with its secure node 72) may allow the user to request and permit a public performance of the same property 200(1) (e.g., for showing in a bar or other public place) and cause the user's credit or other account to be automatically debited by a certain amount of compensation for each showing. A third control 222(3) may, for example, allow secure node 72 (but not player 52) to permit certain classes of users (e.g., certified television advertisers and journalists) to extract or excerpt certain parts of protected property 200(1) for promotional uses. A further control 222(4) may, as another example, allow both video player 52 and secure node 72 to view certain still frames within property 200(1)—but might allow only secure node 72 to make copies of the still frames based on a certain compensation level.

DISH-Blue Spike 842
Exhibit 1005, Page 1332

Example Disks and/or System May Make Use of Trusted Infrastructure

Controls 222 may contain pointers to sources of additional control sets for one or more properties, controls, metadata, and/or other content on the optical disk. In one example, these additional controls may be obtained from a trusted third party, such as a rights and permissions clearinghouse and/or from any other value chain participant authorized by at least one rightsholder to provide at least one additional control set. This kind of rights and permissions clearinghouse is one of several distributed electronic administrative and support services that may be referred to as the "Distributed Commerce Utility," which, among other things, is an integrated, modular array of administrative and support services for electronic commerce and electronic rights and transaction management. These administrative and support services can be used to supply a secure foundation for conducting financial management, rights management, certificate authority, rules clearing, usage clearing, secure directory services, and other transaction related capabilities functioning over a vast electronic network such as the Internet and/or over organization internal Intranets, or even in-home networks of electronic appliances. Non-

limiting examples of these electronic appliances include at least occasionally connected optical media appliances, examples of which include read-only and/or writable DVD players and DVD drives in computers and convergent devices, including, for example, digital televisions and settop boxes incorporating DVD drives.

These administrative and support services can, for example, be adapted to the specific needs of electronic commerce value chains in any number of vertical markets, including a wide variety of entertainment applications. Electronic commerce participants can, for example, use these administrative and support services to support their interests, and/or they can shape and reuse these services in response to competitive business realities. Non-exhaustive examples of electronic commerce participants include individual creators, film and music studios, distributors, program aggregators, broadcasters, and cable and satellite operators.

The Distributed Commerce Utility can, for example, make optimally efficient use of commerce administration resources, and can, in at least some embodiments, scale in a practical fashion to

DISH-Blue Spike 842
Exhibit 1005, Page 1334

optimally accommodate the demands of electronic commerce growth.

The Distributed Commerce Utility may, for example, comprise a number of Commerce Utility Systems. These Commerce Utility Systems can provide a web of infrastructure support available to, and reusable by, the entire electronic community and/or many or all of its participants. Different support functions can, for example, be collected together in hierarchical and/or in networked relationships to suit various business models and/or other objectives. Modular support functions can, for example, be combined in different arrays to form different Commerce Utility Systems for different design implementations and purposes. These Commerce Utility Systems can, for example, be distributed across a large number of electronic appliances with varying degrees of distribution.

The "Distributed Commerce Utility" provides numerous additional capabilities and benefits that can be used in conjunction with the particular embodiments shown in the drawings of this application, non-exhaustive examples of which include:

DISH-Blue Spike 842
Exhibit 1005, Page 1335

- Enables practical and efficient electronic commerce and rights management.

- Provides services that securely administer and support electronic interactions and consequences.

- Provides infrastructure for electronic commerce and other forms of human electronic interaction and relationships.

- Optimally applies the efficiencies of modern distributed computing and networking.

- Provides electronic automation and distributed processing.

- Supports electronic commerce and communications infrastructure that is modular, programmable, distributed and optimally computerized.

- Provides a comprehensive array of capabilities that can be combined to support services that perform various administrative and support roles.

DISH-Blue Spike 842
Exhibit 1005, Page 1336

- Maximizes benefits from electronic automation and distributed processing to produce optimal allocation and use of resources across a system or network.

- Is efficient, flexible, cost effective, configurable, reusable, modifiable, and generalizable.

- Can economically reflect users' business and privacy requirements.

- Can optimally distribute processes -- allowing commerce models to be flexible, scaled to demand and to match user requirements.

- Can efficiently handle a full range of activities and service volumes.

- Can be fashioned and operated for each business model, as a mixture of distributed and centralized processes.

- Provides a blend of local, centralized and networked capabilities that can be uniquely shaped and reshaped to meet changing conditions.

DISH-Blue Spike 842
Exhibit 1005, Page 1337

- Supports general purpose resources and is reusable for many different models; in place infrastructure can be reused by different value chains having different requirements.

- Can support any number of commerce and communications models.

- Efficiently applies local, centralized and networked resources to match each value chain's requirements.

- Sharing of common resources spreads out costs and maximizes efficiency.

- Supports mixed, distributed, peer-to-peer and centralized networked capabilities.

- Can operate locally, remotely and/or centrally.

- Can operate synchronously, asynchronously, or support both modes of operation.

- Adapts easily and flexibly to the rapidly changing sea of commercial opportunities, relationships and constraints of "Cyberspace."

DISH-Blue Spike 842
Exhibit 1005, Page 1338

Any or all of these features may be used in combination with the inventions disclosed herein.

The Distributed Commerce Utility provides, among other advantages, comprehensive, integrated administrative and support services for secure electronic commerce and other forms of electronic interaction. These electronic interactions supported by the Distributed Commerce Utility may, in at least some embodiments, entail the broadest range of appliances and distribution media, non-limiting examples of which include networks and other communications channels, consumer appliances, computers, convergent devices such as WebTV, and optical media such as CD-ROM and DVD in all their current and future forms.

Example Access Techniques

Figures 3, 4A and 4B show example access techniques provided by player 52. In this example, upon disk 100 being loaded into player disk drive 80 (Figure 4A, block 400), the player controller 82 may direct drive 80 to fetch hidden keys 210 from disk 100 and use them to decrypt some or all of the encrypted key block 208 (Figure 4A, block 402). In this example, drive 80 may

DISH-Blue Spike 842
Exhibit 1005, Page 1339

store the keys so decrypted without exposing them to player controller 82 (e.g., by storing them within key store 212 within a secure decryption component such as an integrated circuit based decryption engine) (Figure 4A, block 404). The player 52 may control drive 80 to read the control set 204 (which may or may not be encrypted) from disk 100 (Figure 4A, block 406). The player microprocessor 82 may parse control set 204, ignore or discard those controls 222 that are beyond its capability, and maintain permissions and/or rights management information corresponding to the subset of controls that it can enforce (e.g., the "copy once" control 222(1)).

Player 52 may then wait for the user to provide a request via control inputs 58 and/or remote control unit 56. If the control input is a copy request ("yes" exit to Figure 4A, decision block 408), then player microprocessor 84 may query control 222(1) to determine whether copying is allowed, and if so, under what conditions (Figure 4A, decision block 410). Player 52 may refuse to copy the disk 100 if the corresponding control 222(1) forbids copying ("no" exit to Figure 4A, decision block 410), and may allow copying (e.g., by controlling drive 80 to sequentially access

all of the information on disk 100 and provide it to an output port not shown) if corresponding control 222(1) permits copying ("yes" exit to Figure 4A, decision block 410; block 412). In this example, player 52 may, upon making a copy, store an identifier associated with disk 100 within an internal, non-volatile memory (e.g., controller memory 86) or elsewhere if control 222(1) so requires. This stored disk identifier can be used by player 52 to enforce a "copy once" restriction (i.e., if the user tries to use the same player to copy the same disk more than once or otherwise as forbidden by control 222(1), the player can deny the request).

If the user requests one of properties 200 to be played or read ("yes" exit to Figure 4A, decision block 414), player controller 82 may control drive 80 to read the corresponding information from the selected property 200 (e.g., in a sequence as specified by metadata 202) and decrypt the read information as needed using the keys initially obtained from key block 208 and now stored within drive key storage 212 (Figure 4A, block 416).

Figure 4B is a variation on the Figure 4A process to accommodate a situation in which player 52 itself provides decryption keys for decrypting encrypted key block 208. In this

DISH-Blue Spike 842
Exhibit 1005, Page 1341

example, controller 82 may supply one or more decryption keys to drive 80 using a secure protocol such a Diffie-Hellman key agreement, or through use of a shared key known to both the drive and some other system or component to which the player 52 is or once was coupled (Figure 4B, block 403). The drive 80 may use these supplied keys to decrypt encrypted key block 208 as shown in Figure 4A, block 404, or it may use the supplied keys to directly decrypt content such as protected property 200 and/or protected metadata 202(2).

As a further example, the player 52 can be programmed to place a copy it makes of a digital property such as a film in encrypted form inside a tamper-resistant software container. The software container may carry with it a code indicating that the digital property is a copy rather than an original. The sending player 52 may also put its own unique identifier (or the unique identifier of an intended receiving device such as another player 52, a video cassette player or equipment 50) in the same secure container to enforce a requirement that the copy can be played only on the intended receiving device. Player 52 (or other receiving device) can be programmed to make no copies (or no

DISH-Blue Spike 842
Exhibit 1005, Page 1342

additional copies) upon detecting that the digital property is a copy rather than an original. If desired, a player 52 can be programmed to refuse to play a digital property that is not packaged with the player's unique ID.

Example Use of Analog Encoding Techniques

In another example, more comprehensive rights management information may be encoded by player 52 in the analog output using methods for watermarking and/or fingerprinting.Today, a substantial portion of the "real world" is analog rather than digital. Despite the pervasiveness of analog signals, existing methods for managing rights and protecting copyright in the analog realm are primitive or non-existent. For example:

- Quality degradation inherent in multigenerational analog copying has not prevented a multi-billion dollar pirating industry from flourishing.

- Some methods for video tape copy and pay per view protection attempt to prevent any copying at all of commercially released content, or allow only one

generation of copying. These methods can generally be easily circumvented.

- Not all existing devices respond appropriately to copy protection signals.

- Existing schemes are limited for example to "copy/no copy" controls.

- Copy protection for sound recordings has not been commercially implemented.

A related problem relates to the conversion of information between the analog and digital domains. Even if information is effectively protected and controlled initially using strong digital rights management techniques, an analog copy of the same information may no longer be securely protected.

For example, it is generally possible for someone to make an analog recording of program material initially delivered in digital form. Some analog recordings based on digital originals are of quite good quality. For example, a Digital Versatile Disk

("DVD") player may convert a movie from digital to analog format and provide the analog signal to a high quality analog home VCR. The home VCR records the analog signal. A consumer now has a high quality analog copy of the original digital property. A person could re-record the analog signal on a DVD-RAM. This recording will in many circumstances have substantial quality – and would no longer be subject to "pay per view" or other digital rights management controls associated with the digital form of the same content.

Since analog formats will be with us for a long time to come, rightsholders such as film studios, video rental and distribution companies, music studios and distributors, and other value chain participants would very much like to have significantly better rights management capabilities for analog film, video, sound recordings and other content. Solving this problem generally requires a way to securely associate rights management information with the content being protected.

In combination with other rights management capabilities, watermarking and/or fingerprinting, may provide "end to end"

DISH-Blue Spike 842
Exhibit 1005, Page 1345

secure rights management protection that allows content providers and rights holders to be sure their content will be adequately protected -- irrespective of the types of devices, signaling formats and nature of signal processing within the content distribution chain. This "end to end" protection also allows authorized analog appliances to be easily, seamlessly and cost-effectively integrated into a modern digital rights management architecture.

Watermarking and/or fingerprinting may carry, for example, control information that can be a basis for a Virtual Distribution Environment ("VDE") in which electronic rights management control information may be delivered over insecure (e.g., analog) communications channels. This Virtual Distribution Environment is highly flexible and convenient, accommodating existing and new business models while also providing an unprecedented degree of flexibility in facilitating ad hoc creation of new arrangements and relationships between electronic commerce and value chain participants -- regardless of whether content is distributed in digital and/or analog formats.

DISH-Blue Spike 842
Exhibit 1005, Page 1346

Watermarking together with distributed, peer-to-peer rights management technologies providers numerous advantages, including, but not limited to:

- An indelible and invisible, secure technique for providing rights management information.

- An indelible method of associating electronic commerce and/or rights management controls with analog content such as film, video, and sound recordings.

- Persistent association of the commerce and/or rights management controls with content from one end of a distribution system to the other -- regardless of the number and types of transformations between signaling formats (for example, analog to digital, and digital to analog).

- The ability to specify "no copy/ one copy/ many copies" rights management rules, and also more

DISH-Blue Spike 842
Exhibit 1005, Page 1347

complex rights and transaction pricing models (such as, for example, "pay per view" and others).

- The ability to fully and seamlessly integrate with comprehensive, general electronic rights management solutions.

- Secure control information delivery in conjunction with authorized analog and other non-digital and/or non-secure information signal delivery mechanisms.

- The ability to provide more complex and/or more flexible commerce and/or rights management rules as content moves from the analog to the digital realm and back.

- The flexible ability to communicate commerce and/or rights management rules implementing new, updated, or additional business models to authorized analog and/or digital devices.

DISH-Blue Spike 842
Exhibit 1005, Page 1348

Any or all of these features may be used in combination in and/or with the inventions disclosed in the present specification.

Briefly, watermarking and/or fingerprinting methods may, using "steganographical" techniques, substantially indelibly and substantially invisibly encode rights management and/or electronic commerce rules and controls within an information signal such as, for example, an analog signal or a digitized (for example, sampled) version of an analog signal, non-limiting examples of which may include video and/or audio data, that is then decoded and utilized by the local appliance. The analog information and stenographically encoded rights management information may be transmitted via many means, non-limiting examples of which may include broadcast, cable TV, and/or physical media, VCR tapes, to mention one non-limiting example. Any or all of these techniques may be used in combination in accordance with the inventions disclosed herein.

Watermarking and/or fingerprinting methods enable at least some rights management information to survive transformation of the video and/or other information from analog to digital and from

DISH-Blue Spike 842
Exhibit 1005, Page 1349

digital to analog format. Thus in one example, two or more analog and/or digital appliances may participate in an end-to-end fabric of trusted, secure rights management processes and/or events.

Example, More Capable Embodiments

As discussed above, the example control set shown in Figure 3B provides a comprehensive, flexible and extensible set of controls for use by both player 52 and computer equipment 62 (or other platform) depending upon the particular technical, security and other capabilities of the platform. In this example, player 52 has only limited technical and security capabilities in order to keep cost and complexity down in a mass-produced consumer item, and therefore may essentially ignore or fail to enable some or all of the controls 222 provided within control set 204. In another example, the cost of memory and/or processors may continue to decline and manufacturers may choose to expand the technical and security capabilities of player 52. A more capable player 52 will provide more powerful, robust, and flexible rights management capabilities.

DISH-Blue Spike 842
Exhibit 1005, Page 1350

Figure 5 shows an example arrangement permitting platform 60 including secure node 72 to have enhanced and/or different capabilities to use information and/or rights management information on disk 100, and Figure 6 shows an example access technique provided by the secure node. Referring to Figure 5, secure node 72 may be coupled to a network 150 whereas player 52 may not be—giving the secure node great additional flexibility in terms of communicating security related information such as audit trails, compensation related information such as payment requests or orders, etc. This connection of secure node 72 to network 150 (which may be replaced in any given application by some other communications technique such as insertion of a replaceable memory cartridge) allows secure node 72 to receive and securely maintain rights management control information such as an additional container 206' containing an additional control set 204'. Secure node 72 may use control set 204' in addition or in lieu of a control set 204 stored on disk 100. Secure node 72 may also maintain a secure cryptographic key store 212 that may provide cryptographic keys to be used in lieu of or in addition to any keys 208, 210 that may be stored on disk 100.

DISH-Blue Spike 842
Exhibit 1005, Page 1351

Because of its increased security and/or technical capabilities, secure node 72 may be able to use controls 222 within control set 204 that player 52 ignores or cannot use—and may be provided with further and/or enhanced rights and/or rights management capabilities based on control set 204' (which the user may, for example, order specially and which may apply to particular properties 200 stored on disk 100 and/or particular sets of disks).

Example Secure Node Access Techniques

The Figure 6 example access technique (which may be performed by platform 60 employing secure node 72, for example) involves, in this particular example, the secure node 72 fetching property identification information 220 from disk 100 (Figure 6, block 502), and then locating applicable control sets and/or rules 204 (which may be stored on disk 100, within secure node 72, within one or more repositories the secure node 72 accesses via network 150, and/or a combination of any or all of these techniques) (Figure 6, block 504). Secure node 72 then loads the necessary decryption keys and uses them to decrypt information as required (Figure 6, block 506). In one example, secure node 72 obtains the necessary keys from secure containers 206 and/or 206'

DISH-Blue Spike 842
Exhibit 1005, Page 1352

and maintains them within a protected processing environment such as SPU 164 or a software-emulated protected processing environment without exposing them externally of that environment. In another example, the secure node 72 may load the necessary keys (or a subset of them) into disk drive 82' using a secure key exchange protocol for use by the disk drive in decrypting information much in the same manner as would occur within player 52 in order to maintain complete compatibility in drive hardware.

Secure node 72 may monitor user inputs and perform requested actions based on the particular control set 204, 204'. For example, upon receiving a user request, secure node 72 may query the control set 204, 204' to determine whether it (they) permits the action the user has requested (Figure 6, block 508) and, if permitted, whether conditions for performing the requested operation have been satisfied (Figure 6, block 510). In this example, secure node 72 may effect the operations necessary to satisfy any such required conditions such as by, for example, debiting a user's locally-stored electronic cash wallet, securely requesting an account debit via network 150, obtaining and/or

DISH-Blue Spike 842
Exhibit 1005, Page 1353

checking user certificates to ensure that the user is within an appropriate class or is who he or she says he is, etc.—using network 150 as required (Figure 6, block 510). Upon all necessary conditions being satisfied, secure node 72 may perform the requested operation (and/or enable microprocessor 154 to perform the operation) (e.g., to release content) and may then generate secure audit records which can be maintained by the secure node and/or reported at the time or later via network 150 (Figure 6, block 512).

If the requested operation is to release content (e.g., make a copy of the content), platform 60 (or player 52 in the example above) may perform the requested operation based at least in part on the particular controls that enforce rights over the content. For example, the controls may prevent platform 60 from releasing content except to certain types of output devices that cannot be used to copy the content, or they may release the content in a way that discourages copying (e.g., by "fingerprinting" the copy with an embedded designation of who created the copy, by intentionally degrading the released content so that any copies made from it will be inferior, etc.). As one specific example, a

video cassette recorder (not shown) connected to platform 60 may be the output device used to make the copy. Because present generations of analog devices such as video cassette recorders are incapable of making multigenerational copies without significant loss in quality, the content provider may provide controls that permit content to be copied by such analog devices but not by digital devices (which can make an unlimited number of copies without quality loss). For example, platform 60 may, under control of digital controls maintained by secure node 72, release content to the video cassette recorder only after the video cassette recorder supplies the platform a digital ID that designates the output device as a video cassette recorder -- and may refuse to provide any output at all unless such a digital ID identifying the output device as a lower quality analog device is provided. Additionally or in the alternative, platform 60 may intentionally degrade the content it supplies to the video cassette recorder to ensure that no acceptable second -generation copies will be made. In another example, more comprehensive rights management information may be encoded by platform 60 in the analog output using watermarking and/or fingerprinting.

DISH-Blue Spike 842
Exhibit 1005, Page 1355

Additional Examples of Secure Container Usage

Figure 7 shows a basic example of a DVD medium 700 containing a kind of secure container 701 for use in DVDs in accordance with the present invention. As shown in this example, container 701 ("DigiBox for DVDs") could be a specialized version of a "standard" container tailored especially for use with DVD and/or other media, or it could, alternatively (in an arrangement shown later in Figure 8), be a fully "standard" container. As shown in this example, the specialized container 701 incorporates features that permit it to be used in conjunction with content information, metadata, and cryptographic and/or protection information that is stored on the DVD medium 700 in the same manner as would have been used had container 701 not been present. Thus, specialized container 701 provides compatibility with existing data formats and organizations used on DVDs and/or other media. In addition, a specialized container 701 can be tailored to support only those features necessary for use in support of DVD and/or other media, so that it can be processed and/or manipulated using less powerful or less expensive computing resources than would be required for complete support of a "standard" container object.

DISH-Blue Spike 842
Exhibit 1005, Page 1356

In this example, specialized "DVD only" container 701 includes a content object (a property) 703 which includes an "external reference" 705 to video title content 707, which may be stored on the DVD and/or other medium in the same manner as would have been used for a medium not including container 701. The video title content 707 may include MPEG-2 and/or AC-3 content 708, as well as scrambling (protection) information 710 and header, structure and/or meta data 711. External reference 705 contains information that "designates" (points to, identifies, and/or describes) specific external processes to be applied/executed in order to usecontent and other information not stored in container 701. In this example, external reference 705 designates video title content 707 and its components 708, 710, and 711. Alternatively, container 701 could store some or all of the video title content in the container itself, using a format and organization that is specific to container 701, rather than the standard format for the DVD and/or other medium 700.

In this example, container 701 also includes a control object (control set) 705 that specifies the rules that apply to use of video title content 707. As indicates by solid arrow 702, control object

DISH-Blue Spike 842
Exhibit 1005, Page 1357

705 "applies to" content object (property) 703. As shown in this example, rule 704 can specify that protection processes, for example CGMA or the Matsushita data scrambling process, be applied, and can designate, by external reference 709 contained in rule 704, data scrambling information 710 to be used in carrying out the protection scheme. The shorthand "do CGMA" description in rule 704 indicates that the rule requires that the standard CGMA protection scheme used for content on DVD media is to be used in conjunction with video title content 707, but a different example could specify arbitrary other rules in control object 705 in addition to or instead of the "do CGMA" rule, including other standard DVD protection mechanisms such as the Matsushita data scrambling scheme and/or other rights management mechanisms. External reference 709 permits rule 704 to be based on protection information 710 that is stored and manipulated in the same format and manner as for a DVD medium that does not incorporate container 701 and/or protection information that is meaningful only in the context of processing container 701.

Figure 8 shows a example of a DVD medium 800 containing a "standard" secure container 801. In this example, the

DISH-Blue Spike 842
Exhibit 1005, Page 1358

"standard" container provides all of the functionality (if desired) of the Figure 7 container, but may offer additional and/or more extensive rights management and/or content use capabilities than available on the "DVD only" container (e.g., the capacity to operate with various different platforms that use secure nodes).

Figure 9 shows a more complex example of DVD medium 800 having a standard container 901 that provides all of the functionality (if desired) of the Figure 7 container, and that can function in concert with other standard containers 902 located either on the same DVD medium or imported from another remote secure node or network. In this example, standard container 902 may include a supplementary control object 904 which applies to content object 903 of standard container 901. Also in this example, container 902 may provide an additional rule(s) such as, for example, a rule permitting/extending rights to allow up to a certain number (e.g., five) copies of the content available on DVD 900. This arrangement, for example, provides added flexibility in controlling rights management of DVD content between multiple platforms via access through "backchannels" such as via a set-top

DISH-Blue Spike 842
Exhibit 1005, Page 1359

box or other hardware having bi-directional communications capabilities with other networks or computers.

Additional Use of A DVD Disk With A Secure Container

Figure 10 illustrates the use of a "new" DVD disk—i.e., one that includes a special DVD secure container in the medium. This container may, in one example, be used or two possible use scenarios: a first situation in which the disk is used on an "old" player (DVD appliance, i.e., a DVD appliance that is not equipped with a secure node to provide rights management in accordance with the present invention; and a second situation in which the disk is used on a "new" player—i.e., a DVD appliance which is equipped with a secure node to provide rights management in accordance with the present invention. In this example, a secure node within the "new" player is configured with the necessary capabilities to process other copy protection information such as, for example, CGMA control codes and data scrambling formats developed and proposed principally by Matsushita.

For example, in the situation shown in Figure 10, the "new" player (which incorporates a secure node in accordance with the

DISH-Blue Spike 842
Exhibit 1005, Page 1360

present invention) can recognize the presence of a secure container on the disk. The player may then load the special DVD secure container from the disk into the resident secure node. The secure node opens the container, and implements and/or enforces appropriate rules and usage consequences associated with the content by applying rules from the control object. These rules are extremely flexible. In one example, the rules may, for example, call for use of other protection mechanisms (such as, for example, CGMA protection codes and Matsushita data scrambling) which can be found in the content (or property) portion of the container.

In another example shown in Figure 10, the special DVD container on the disk still allows the "old" player to use to a predetermined limited amount content material which may be used in accordance with conventional practices.

Example Use of A DVD Disk With No Secure Container

Referring now to Figure 11, a further scenario is discussed. Figure 11 illustrates use of an "old" DVD disk with two possible use examples: a first example in which the disk is used on an "old" player—i.e., a DVD appliance that is not equipped with a secure

DISH-Blue Spike 842
Exhibit 1005, Page 1361

node for providing rights management in accordance with the present invention—and a second example in which the disk is used on a "new" player (i.e., equipped with a secure node).

In the first case, the "old" player will play the DVD content in a conventional manner. In the second scenario, the "new" player will recognize that the disk does not have a container stored in the medium. It therefore constructs a "virtual" container in resident memory of the appliance. To do this, it constructs a container content object, and also constructs a control object containing the appropriate rules. In one particular example, the only applicable rule it need apply is to "do CGMA" -- but in other examples, additional and/or different rules could be employed. The virtual container is then provided to the secure node within the "new" player for implementing management of use rights in accordance with the present invention. Although not shown in Figures 10 and 11, use of "external references" may also be provided in both virtual and non-virtual containers used in the DVD context.

DISH-Blue Spike 842
Exhibit 1005, Page 1362

Example Illustrative Arrangements for Sharing, Brokering and Combining Rights When Operating in At Least Occasionally Connected Scenarios

As described above, the rights management resources of several different devices and/or other systems can be flexibly combined in diverse logical and/or physical relationships, resulting for example in greater and/or differing rights. Such rights management resource combinations can be effected through connection to one or more remote rights authorities. Figures 12-14 show some non-limiting examples of how rights authorities can be used in various contexts.

For example, Figure 12 shows a rights authority broker 1000 connected to a local area network (LAN) 1002. LAN 1002 may connect to wide area network if desired. LAN 1002 provides connectivity between rights authority broker 1000 and any number of appliances such as for example a player 50, a personal computer 60, a CD "tower" type server 1004. In the example shown, LAN 1002 includes a modem pool (and/or network

DISH-Blue Spike 842
Exhibit 1005, Page 1363

protocol server, not shown)1006 that allows a laptop computer 1008 to connect to the rights authority broker 1000 via dial-up lines 1010. Alternatively, laptop 1008 could communicate with rights authority broker 1000 using other network and/or communication means, such as the Internet and/or other Wide Area Networks (WANs). A disk player 50A may be coupled to laptop 1008 at the laptop location. In accordance with the teachings above, any or all of devices shown in Figure 12 may include one or more secure nodes 72.

Rights authority broker 1000 may act as an arbiter and/or negotiator of rights. For example, laptop 1008 and associated player 50A may have only limited usage rights when operating in a stand-alone configuration. However, when laptop 1008 connects to rights authority broker 1000 via modem pool 1006 and LAN 1002 and/or by other communication means, the laptop may acquire different and/or expanded rights to use disks 100 (e.g., availability of different content portions, different pricing, different extraction and/or redistribution rights, etc.) Similarly, player 50, equipment 60 and equipment 1004 may be provided with an enhanced and/or different set of disk usage rights through

DISH-Blue Spike 842
Exhibit 1005, Page 1364

communication with rights authority broker 1000 over LAN 1002. Communication to and from rights authority broker 1000 is preferably secured through use of containers of the type disclosed in the above-referenced Ginter et al. patent specification.

Figure 13 shows another example use of a rights authority broker 1000 within a home environment. In this example, the laptop computer 1008 may be connected to a home-based rights authority broker 1000 via a high speed serial IEEE 1394 bus and/or by other electronic communication means. In addition, rights authority broker 1000 can connect with any or all of:

- a high definition television 1100,
- one or more loudspeakers 1102 or other audio transducers,
- one or more personal computers 60,
- one or more set-top boxes 1030,
- one or more disk players 50,
- one or more other rights authority brokers 1000A-1000N and

DISH-Blue Spike 842
Exhibit 1005, Page 1365

- any other home or consumer equipment or appliances.

Any or all of the equipment listed above may include a secure node 72.

Figure 14 shows another example use of a rights authority broker 1000. In this example, rights authority broker 1000 is connected to a network 1020 such as a LAN, a WAN, the Internet, etc. Network 1020 may provide connectivity between rights authority broker 1000 and any or all of the following equipment:

- one or more connected or occasionally connected disk players 50A, 50B;
- one more networked computers 1022;
- one or more disk reader towers/servers 1004;
- one or more laptop computers 1008;
- one or more Commerce Utility Systems such as a rights and permissions clearinghouse 1024 (see Shear et al., "Trusted Infrastructure..." specification referenced above);

DISH-Blue Spike 842
Exhibit 1005, Page 1366

- one or more satellite or other communications uplinks 1026;
- one or more cable television head-ends 1028;
- one or more set-top boxes 1030 (which may be connected to satellite downlinks 1032 and/or disk players 50C);
- one or more personal computer equipment 60;
- one or more portable disk players 1034 (which may be connected through other equipment, directly, and/or occasionally unconnected);
- one or more other rights authority brokers 1000A-1000N; and
- any other desired equipment.

Any or all of the above-mentioned equipment may include one or more secure nodes 72. Rights authority broker 1000 can distribute and/or combine rights for use by any or all of the other components shown in Figure 14. For example, rights authority broker 100 can supply further

DISH-Blue Spike 842
Exhibit 1005, Page 1367

secure rights management resources to equipment connected to the broker via network 1020. Multiple equipment shown in Figure 14 can participate and work together in a permanently or temporarily connected network 1020 to share the rights management for a single node. Rights associated with parties and/or groups using and/or controlling such multiple devices and/or other systems can be employed according to underlying rights related rules and controls. As one example, rights available through a corporate executive's laptop computer 1008 might be combined with or substituted for, in some manner, the rights of one or more subordinate corporate employees when their computing or other devices 60 are coupled to network 1020 in a temporary networking relationship. In general, this aspect of the invention allows distributed rights management for DVD or otherwise packaged and delivered content that is protected by a distributed, peer-to-peer rights management. Such a distributed rights management can operate whether the DVD appliance or other content usage device is participating in a permanently or temporarily

DISH-Blue Spike 842
Exhibit 1005, Page 1368

connected network 1020, and whether or not the relationships among the devices and/or other systems participating in the distributed rights management arrangement are relating temporarily or have a more permanent operating relationship.

For example, laptop computer 1008 may have different rights available depending on the context in which that device is operating. For example, in a general corporate environment such as shown in Figure 12, the laptop 1008 may have one set of rights. However, the same laptop 1008 may be given a different set of rights when connected to a more general network 1020 in collaboration with specified individuals and/or groups in a corporation. The same laptop 1008 may be given a still different set of rights when connected in a general home environment such as shown by example in Figure 13. The same laptop 1008 could be given still different rights when connected in still other environments such as, by way of non-limiting example:

- a home environment in collaboration with specified individuals and/or groups,

DISH-Blue Spike 842
Exhibit 1005, Page 1369

- a retail environment,
- a classroom setting as a student,
- a classroom setting in collaboration with an instructor, in a library environment,
- on a factory floor,
- on a factory floor in collaboration with equipment enabled to perform proprietary functions, and so on.

As one more particular example, coupling a limited resource device arrangement such as a DVD appliance 50 shown in Figure 14 with an inexpensive network computer (NC) 1022 may allow an augmenting (or replacing) of rights management capabilities and/or specific rights of parties and/or devices by permitting rights management to be a result of a combination of some or all of the rights and/or rights management capabilities of the DVD appliance and those of an Network or Personal Computer (NC or PC). Such rights may be further augmented, or otherwise modified or replaced by the availability of rights management capabilities provided by a trusted (secure) remote network rights authority 1000.

DISH-Blue Spike 842
Exhibit 1005, Page 1370

The same device, in this example a DVD appliance 50, can thus support different arrays, e.g., degrees, of rights management capabilities, in disconnected and connected arrangements and may further allow available rights to result from the availability of rights and/or rights management capabilities resulting from the combination of rights management devices and/or other systems. This may include one or more combinations of some or all of the rights available through the use of a "less" secure and/or resource poor device or system which are augmented, replaced, or otherwise modified through connection with a device or system that is "more" or "differently" secure and/or resource rich and/or possesses differing or different rights, wherein such connection employs rights and/or management capabilities of either and/or both devices as defined by rights related rules and controls that describe a shared rights management arrangement.

In the latter case, connectivity to a logically and/or physically remote rights management capability can expand (by, for example, increasing the available secure rights management resources) and/or change the character of the rights available to the user of the DVD appliance 50 or a DVD appliance when such

DISH-Blue Spike 842
Exhibit 1005, Page 1371

device is coupled with an NC 1022, personal computer 60, and/or remote rights authority 1000. In this rights augmentation scenario, additional content portions may be available, pricing may change, redistribution rights may change (e.g., be expanded), content extraction rights may be increased, etc.

Such "networking rights management" can allow for a combination of rights management resources of plural devices and/or other systems in diverse logical and/or physical relationships, resulting in either greater or differing rights through the enhanced resources provided by connectivity with one or more "remote" rights authorities. Further, while providing for increased and/or differing rights management capability and/or rights, such a connectivity based rights management arrangement can support multi-locational content availability, by providing for seamless integration of remotely available content, for example, content stored in remote, Internet world wide web-based, database supported content repositories, with locally available content on one or more DVD discs 100.

In this instance, a user may experience not only increased or differing rights but may be able to use to both local DVD content

DISH-Blue Spike 842
Exhibit 1005, Page 1372

and supplementing content (i.e., content that is more current from a time standpoint, more costly, more diverse, or complementary in some other fashion, etc.). In such an instance, a DVD appliance 50 and/or a user of a DVD appliance (or other device or system connected to such appliance) may have the same rights, differing, and/or different rights applied to locally and remotely available content, and portions of local and remotely available content may themselves be subject to differing or different rights when used by a user and/or appliance. This arrangement can support an overall, profound increase in user content opportunities that are seamlessly integrated and efficiently available to users in a single content searching and/or usage activity.

Such a rights augmenting remote authority 1000 may be directly coupled to a DVD appliance 50 and/or other device by modem (see item 1006 in Figure 12) and/or directly or indirectly coupled through the use of an I/O interface, such as a serial 1394 compatible controller (e.g., by communicating between a 1394 enabled DVD appliance and a local personal computer that functions as a smart synchronous or asynchronous information communications interface to such one or more remote authorities,

including a local PC 60 or NC 1022 that serves as a local rights management authority augmenting and/or supplying the rights management in a DVD appliance) and/or by other digital communication means such as wired and/or wireless network connections.

Rights provided to, purchased, or otherwise acquired by a participant and/or participant DVD appliance 50 or other system can be exchanged among such peer-to-peer relating devices and/or other systems so long as they participate in a permanently or temporarily connected network. 1020. In such a case, rights may be bartered, sold, for currency, otherwise exchanged for value, and/or loaned so long as such devices and/or other systems participate in a rights management system, for example, such as the Virtual Distribution Environment described in Ginter, et al., and employ rights transfer and other rights management capabilities described therein. For example, this aspect of the present invention allows parties to exchange games or movies in which they have purchased rights. Continuing the example, an individual might buy some of a neighbor's usage rights to watch a movie, or transfer to another party credit received from a game

DISH-Blue Spike 842
Exhibit 1005, Page 1374

publisher for the successful superdistribution of the game to several acquaintances, where such credit is transferred (exchanged) to a friend to buy some of the friend's rights to play a different game a certain number of times, etc.

Example Virtual Rights Process

Figures 15A-15C shows an example of a process in which rights management components of two or more appliances or other devices establish a virtual rights machine environment associated with an event, operation and/or other action. The process may be initiated in a number of ways. In one example, an appliance user (and/or computer software acting on behalf of a user, group of users, and/or automated system for performing actions) performs an action with a first appliance (e.g., requesting the appliance to display the contents of a secure container, extract a portion of a content element, run a protected computer program, authorize a work flow process step, initiate an operation on a machine tool, play a song, etc.) that results in the activation of a rights management component associated with such first appliance (Figure 15A, block 1500). In other examples, the process may get started in response to an automatically generated event (e.g., based

DISH-Blue Spike 842
Exhibit 1005, Page 1375

on a time of day or the like), a random or pseudo-random event, and/or a combination of such events with a user-initiated event.

Once the process begins, a rights management component such as a secure node 72 (for example, an SPE and/or HPE as disclosed in Ginter et al.) determines which rights associated with such first appliance, if any, the user has available with respect to such an action (Figure 15A, block 1502). The rights management component also determines the coordinating and/or cooperating rights associated with such an action available to the user located in whole or in part on other appliances (Figure 15A, block 1502).

In one example, these steps may be performed by securely delivering a request to a rights authority server 1000 that identifies the first appliance, the nature of the proposed action, and other information required or desired by such a rights authority server. Such other information may include, for example:

- the date and time of the request,
- the identity of the user,
- the nature of the network connection,

DISH-Blue Spike 842
Exhibit 1005, Page 1376

- the acceptable latency of a response, etc.), and/or
- any other information.

In response to such a request, the rights authority server 1000 may return a list (or other appropriate structure) to the first appliance. This list may, for example, contain the identities of other appliances that do, or may, have rights and/or rights related information relevant to such a proposed action.

In another embodiment, the first appliance may communicate (e.g., poll) a network with requests to other appliances that do, or may, have rights and/or rights related information relevant to such proposed action. Polling may be desirable in cases where the number of appliances is relatively small and/or changes infrequently. Polling may also be useful, for example, in cases where functions of a rights authority server 1000 are distributed across several appliances.

The rights management component associated with the first appliance may then, in this example, check the security level(s) (and/or types) of devices and/or users of other appliances that do, or may, have rights and/or rights related information relevant to

DISH-Blue Spike 842
Exhibit 1005, Page 1377

such an action (Figure 15A, block 1506). This step may, for example, be performed in accordance with the security level(s) and/or device type management techniques disclosed in Sibert and Van Wie, and the user rights, secure name services and secure communications techniques disclosed in Ginter et al. Device and/or user security level determination may be based, for example, in whole or in part on device and/or user class.

The rights management component may then make a decision as to whether each of the other appliance devices and/or users have a sufficient security level to cooperate in forming the set of rights and/or rights related information associated with such an action (Figure 15A, block 1508). As each appliance is evaluated, some devices and/or users may have sufficient security levels, and others may not. In this example, if a sufficient security level is not available ("No" exit to decision block 1508), the rights management component may create an audit record (for example, an audit record of the form disclosed in Ginter et al.) (Figure 15A, block 1510), and may end the process (Figure 15A, block 1512). Such audit record may be for either immediate transmission to a responsible authority and/or for local storage and later

DISH-Blue Spike 842
Exhibit 1005, Page 1378

transmission, for example. The audit recording step may include, as one example, incrementing a counter that records security level failures (such as the counters associated with summary services in Ginter et al.)

If the devices and/or users provide the requisite security level ("Yes" exit to block 1508), the rights management component in this example may make a further determination based on the device and/or user class(es) and/or other configuration and/or characteristics (Figure 15B, block 1514). Such determination may be based on any number of factors such as for example:

- the device is accessible only through a network interface that has insufficient throughput;
- devices in such a class typically have insufficient resources to perform the action, or relevant portion of the action, at all or with acceptable performance, quality, or other characteristics;

DISH-Blue Spike 842
Exhibit 1005, Page 1379

- the user class is inappropriate due to various conditions (e.g., age, security clearance, citizenship, jurisdiction, or any other class-based or other user characteristic); and/or
- other factors.

In one example, decision block 1514 may be performed in part by presenting a choice to the user that the user declines.

If processes within the rights management component determines that such device and/or user class(es) are inappropriate("No" exit to block 1514), the rights management component may write an audit record if required or desired (Figure 15B, block 1516) and the process may end (Figure 15B, block 1518).

If, on the other hand, the rights management component determines that the device and/or user classes are appropriate to proceed ("Yes" exit to block 1514), the rights management component may determine the rights and resources available for performing the action on the first appliance and the other appliances acting together (Figure 15B, block 1520). This step may be performed, for example, using any or all of the method

DISH-Blue Spike 842
Exhibit 1005, Page 1380

processing techniques disclosed in Ginter et al. For example, method functions may include event processing capabilities that formulate a request to each relevant appliance that describes, in whole or in part, information related to the action, or portion of the action, potentially suitable for processing, in whole or in part, by such appliance. In this example, such requests, and associated responses, may be managed using the reciprocal method techniques disclosed in Ginter et al. If such interaction requires additional information, or results in ambiguity, the rights management component may, for example, communicate with the user and allow them to make a choice, such as making a choice among various available, functionally different options, and/or the rights management component may engage in a negotiation (for example, using the negotiation techniques disclosed in Ginter et al.) concerning resources, rights and/or rights related information.

The rights management component next determines whether there are sufficient rights and/or resources available to perform the requested action (Figure 15B, decision block 1522). If there are insufficient rights and/or resources available to perform the action ("No" exit to block 1522), the rights management component may

DISH-Blue Spike 842
Exhibit 1005, Page 1381

write an audit record (Figure 15B, block 1524), and end the process (Figure 15B, block 1526).

In this example, if sufficient rights and/or resources are available ("Yes" exit to block 1522), the rights management component may make a decision regarding whether additional events should be processed in order to complete the overall action (Figure 15B, block 1528). For example, it may not be desirable to perform only part of the overall action if the necessary rights and/or resources are not available to complete the action. If more events are necessary and/or desired ("Yes" exit to block 1528), the rights management component may repeat blocks 1520, 1522 (and potentially perform blocks 1524, 1526) for each such event.

If sufficient rights and/or resources are available for each of the events ("No" exit to block 1528), the rights management component may, if desired or required, present a user with a choice concerning the available alternatives for rights and/or resources for performing the action (Figure 15B, block 1530). Alternatively and/or in addition, the rights management component may rely on user preference information (and/or defaults) to "automatically" make such a determination on behalf

DISH-Blue Spike 842
Exhibit 1005, Page 1382

of the user (for example, based on the overall cost, performance, quality, etc.). In another embodiment, the user's class, or classes, may be used to filter or otherwise aid in selecting among available options. In still another embodiment, artificial intelligence (including, for example, expert systems techniques) may be used to aid in the selection among alternatives. In another embodiment, a mixture of any or all of the foregoing (and/or other) techniques may be used in the selection process.

If there are no acceptable alternatives for rights and/or resources, or because of other negative aspects of the selection process (e.g., a user presses a "Cancel" button in a graphical user interface, a user interaction process exceeds the available time to make such a selection, etc.), ("No" exit to block 1530) the rights management component may write an audit record (Figure 15B, block 1532), and end the process (Figure 15B, block 1534).

On the other hand, if a selection process identifies one or more acceptable sets of rights and/or resources for performing the action and the decision to proceed is affirmative ("Yes" exit to block 1530), the rights management component may perform the proposed action using the first appliance alone or in combination

DISH-Blue Spike 842
Exhibit 1005, Page 1383

with any additional appliances (e.g., a rights authority 1000, or any other connected appliance) based on the selected rights and/or resources (Figure 15C, block 1536). Such cooperative implementation of the proposed actions may include for example:

- performing some or all of the action with the first appliance;
- performing some or all of the action with one or more appliances other than the first appliance (e.g., a rights authority 1000 and/or some other appliance);
- performing part of the action with the first appliance and part of the action with one or more other appliances; or
- any combination of these.

For example, this step may be performed using the event processing techniques disclosed in Ginter et al.

As one illustrative example, the first appliance may have all of the resources necessary to perform a particular task (e.g., read certain information from an optical disk), but may lack the rights necessary to do so. In such an instance, the first appliance may

DISH-Blue Spike 842
Exhibit 1005, Page 1384

obtain the additional rights it requires to perform the task through the steps described above. In another illustrative example, the first appliance may have all of the rights required to perform a particular task, but it may not have the resources to do so. For example, the first appliance may not have sufficient hardware and/or software resources available to it for accessing, processing or otherwise using information in certain ways. In this example, step 1536 may be performed in whole or in part by some other appliance or appliances based in whole or in part on rights supplied by the first appliance. In still another example, the first appliance may lack both rights and resources necessary to perform a certain action, and may rely on one or more additional appliances to supply such resources and rights.

In this example, the rights management component may, upon completion of the action, write one or more audit records (Figure 15C, block 1538), and the process may end (Figure 15C, block 1540).

* * * * * *

DISH-Blue Spike 842
Exhibit 1005, Page 1385

An arrangement has been described which adequately satisfies current entertainment industry requirements for a low cost, mass-produceable digital video disk or other high capacity disc copy protection scheme but which also provides enhanced, extensible rights management capabilities for more advanced and/or secure platforms and for cooperative rights management between devices of lessor, greater, and/or differing rights resources. While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the invention.

DISH-Blue Spike 842
Exhibit 1005, Page 1386

We Claim:

1. An electronic appliance including:

a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

a secure node coupled to the disk use arrangement, the secure node providing at least one rights management process.

2. An electronic appliance including:

a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

at least one processing arrangement coupled to the disk use arrangement, the processing arrangement selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.

DISH-Blue Spike 842
Exhibit 1005, Page 1387

3. A system as in claim 2 wherein the processing arrangement selects a subset of control information used on another appliance and/or class of appliance.

4. A system as in claim 2 wherein the processing arrangement selects different control information from the information selected by another appliance and/or class of appliance.

5. A system as in claim 2 wherein at least some of the control information comprises an analog signal.

6. A system as in claim 2 wherein at least some of the control information comprises digitally encoded information.

7. In an appliance capable of using digital versatile disks, a method including the following steps:

DISH-Blue Spike 842
Exhibit 1005, Page 1388

at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.

8. A method as in claim 7 wherein the selecting step includes the step of selecting a subset of control information used on another appliance and/or class of appliance.

9. A method as in claim 7 wherein the selecting step includes the step of selecting, from control information stored on the storage medium, a different set of control information than the control information selected by another appliance and/or class of appliance.

DISH-Blue Spike 842
Exhibit 1005, Page 1389

10. An electronic appliance including:

a disk use arrangement for reading information from a digital versatile disk optical storage medium; and

at least one processing arrangement coupled to the disk use arrangement, the processing arrangement protecting information read from the storage medium.

11. An appliance as in claim 10 wherein the processing arrangement includes a rights management arrangement that applies at least one rights management technique to the read information.

12. An appliance as in claim 10 wherein the appliance further includes at least one port compliant at least in part with the IEEE 1394-1995 high speed serial bus standard, and the processing arrangement couples the protected information to the port.

DISH-Blue Spike 842
Exhibit 1005, Page 1390

13. In an electronic appliance, a method including the following steps:

reading information from a digital versatile disk optical storage medium; and

protecting the information read from the optical storage medium.

14. A method as in claim 13 wherein the protecting step includes the step of applying at least one rights management technique to the read information.

15. A method as in claim 13 further including the step of sending the protected information to an IEEE 1394 port.

16. An electronic appliance including:

DISH-Blue Spike 842
Exhibit 1005, Page 1391

a disk use arrangement for using information stored, or to be stored, on a digital versatile disk optical storage medium; and

at least one protecting arrangement coupled to the disk use arrangement and also coupled to receive at least one analog signal, the protecting arrangement creating protected digital information based at least in part on the analog signal.

17. In an electronic appliance, a method including the following steps:

receiving at least one analog signal; and

creating protected digital content based at least in part on the analog signal for storage on a digital versatile disk.

18. In an electronic appliance, a method including the following steps:

reading at least one analog signal from a digital versatile disk;

DISH-Blue Spike 842
Exhibit 1005, Page 1392

creating protected digital content based at least in part on the analog signal; and

outputting the protected digital content.

19. An electronic appliance including:

a disk use arrangement for using information stored, or to be stored, on a digital versatile disk optical storage medium; and

at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement treating the storage medium and/or information obtained from the storage medium differently depending on the geographical and/or jurisdictional context of the appliance.

20. In an electronic appliance, a method including the steps of:

reading information from at least one digital versatile disk; and

performing at least one rights management operation based at least in part on the geographical and/or jurisdictional context of the appliance.

21. An electronic appliance including:

a disk use arrangement for using at least one secure container stored on a digital versatile disk optical storage medium; and

at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement processing the secure container.

22. In an electronic appliance, a method including the following steps:

reading at least one secure container from at least one digital versatile disk; and

performing at least one rights management operation on the secure container.

DISH-Blue Spike 842
Exhibit 1005, Page 1394

23. An electronic appliance including:

at least one rights management arrangement for generating and/or modifying at least one secure container for storage onto a digital versatile disk optical storage medium.

24. In an electronic appliance, a method including the step of performing at least one rights management operation on at least one secure container for storage onto a digital versatile disk optical storage medium.

25. A digital versatile disk use system and/or method characterized in that the system and/or method uses at least one secure container.

26. A digital versatile disk use system and/or method characterized in that the system and/or method uses at least one

DISH-Blue Spike 842
Exhibit 1005, Page 1395

secure container of the type disclosed in PCT Publication No. WO 96/27155.

27. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and

a secure arrangement that securely manages information on the storage medium such that at least a first portion of the information may be used on at least a first class of appliance while at least a second portion of the information may be used on at least a second class of appliance

28. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium;

DISH-Blue Spike 842
Exhibit 1005, Page 1396

using at least a first portion of the information on at least a first class of appliance; and

using at least a second portion of the information on at least a second class of appliance.

29. A system including first and second classes of electronic appliances each including a secure processing arrangement, the first appliance class secure arrangement securely managing and/or using at least a first portion of the information, the second appliance class secure arrangement securely managing and/or using at least a second portion of the information.

30. A system as in claim 29 wherein the first and second information portions are different, and the second appliance class secure arrangement does not use the first information portion.

31. A system as in claim 29 wherein the first appliance class does not use the second information portion.

DISH-Blue Spike 842
Exhibit 1005, Page 1397

32. In a system including first and second classes of electronic appliances each including a secure arrangement, a method comprising:

(a) securely managing and/or using at least a first portion of the information with the first appliance class secure arrangement, and

(b) securely managing and/or using at least a second portion of the information with the second appliance class secure arrangement.

33. A method as in claim 32 wherein the first and second information portions are different, and step (b) does not use the first information portion.

34. A method as in claim 32 wherein step (a) does not use the second information portion.

DISH-Blue Spike 842
Exhibit 1005, Page 1398

35. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and

a secure arrangement that securely stores and/or transmits information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.

36. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium; and

securely storing and/or transmitting information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.

DISH-Blue Spike 842
Exhibit 1005, Page 1399

37. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium;

a cryptographic engine coupled to the disk use arrangement, the engine using at least one cryptographic key; and

a secure arrangement that securely updates and/or replaces at least one cryptographic key used by the cryptographic engine to at least in part modify the scope of information usable by the appliance.

38. A method of operating an electronic appliance including:

writing information onto and/or reading information from a digital versatile disk optical storage medium;

using at least one cryptographic key in conjunction with said information; and

DISH-Blue Spike 842
Exhibit 1005, Page 1400

securely updating and/or replacing at least one cryptographic key used by the cryptographic engine to at least in part modify the scope of information useable by the appliance.

39. A digital versatile disk appliance characterized in that at least one cryptographic key used by the appliance is securely updated and/or replaced to at least in part modify the scope of information that can be used by the appliance.

40. An appliance as in claim 39 further characterized in that the key updating and/or replacing is based on class of appliance.

41. An electronic appliance having a class associated therewith, characterized in that at least one cryptographic key set used by the appliance class is selected to help ensure security of information released from at least one digital versatile disk.

DISH-Blue Spike 842
Exhibit 1005, Page 1401

42. A digital camera for generating at least one image to be written onto a digital versatile disk optical storage medium, characterized in that the camera includes at least one information protecting arrangement that at least in part protects the image so that the information is persistently protected through subsequent processes such as editing, production, writing onto a digital versatile disk, and/or reading from a digital versatile disk.

43. A digital camera for generating image information that can be written onto a digital versatile disk optical storage medium, a method comprising:

capturing at least one image with a digital camera; and

protecting information provided by the digital camera so that the information is selectively persistently protected through subsequent processes such as distribution, editing and/or production, writing onto the digital versatile disk optical storage medium, and/or reading from the digital versatile disk optical storage medium.

DISH-Blue Spike 842
Exhibit 1005, Page 1402

44. In an electronic appliance including a disk use arrangement, a method comprising:

reading information from at least one digital versatile disk optical storage medium; and

persistently protecting at least some of the read information through at least one subsequent editing and/or production process.

45. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium; and

securely managing information on the storage medium, including the step of using at least a first portion of the information on at least a first class of appliance, and using at least a second portion of the information on at least a second class of appliance.

DISH-Blue Spike 842
Exhibit 1005, Page 1403

46. A method of providing copy protection and/or use rights management of at least one digital property content and/or secure container to be stored and/or distributed on a digital versatile disk medium, comprising the step(s) of:

providing a set of use control(s) within a cryptographically encapsulated data structure having a predetermined format, the data structure format defining at least one secure software container for providing use rights information for digital property content to be stored on the digital versatile disk medium.

47. A method as in claim 46 further including the step of using at least one digital property content stored on an optical disk in accordance with the use controls, including the step of using a prescribed secure cryptographic key or set of cryptographic keys for using rights information.

48. A method as in claim 46 further including the step of decrypting control rules and/or other selected encrypted

DISH-Blue Spike 842
Exhibit 1005, Page 1404

information content encapsulated in the software container using at least one set of cryptographic keys.

49. A method as in claim 46 further including the step of applying decrypted control rules to regulate use in accordance with control information contained within said control rules, so as to facilitate management of a diverse set of use and distribution rights which may be specific to different users and/or optical disk appliances.

50. A method of providing rights management of digital property stored on digital versatile disk according to claim 46 wherein said secure container data structure comprises:

one or more content objects comprising digital property content; and

one or more control objects comprising a set of control rules defining copy protection, use and distribution rights to digital property content stored on the optical disk.

DISH-Blue Spike 842
Exhibit 1005, Page 1405

51. A method of providing rights management of digital property stored on a digital versatile disk according to claim 46, wherein a content object further comprises one or more reference pointers to digital property content stored elsewhere on the digital versatile disk.

52. A method of providing rights management of digital property stored on a digital versatile disk according to claim 46, wherein a control object further comprises one or more reference pointers to control information stored elsewhere on the digital versatile disk.

53. A method of providing rights management of digital property stored on digital versatile disk according to claim 46, wherein digital information stored on said optical disk includes one or more metadata blocks comprising further information used in conjunction with the control rules to use digital property content stored elsewhere on the optical disk.

DISH-Blue Spike 842
Exhibit 1005, Page 1406

54. A method of providing rights management of digital property stored on digital versatile disk according to claim 46, wherein a metablock may be either of a protected type or of an unprotected type.

55. An arrangement for implementing a rights management system for controlling copy protection, use and/or distribution rights to multi-media digital property content stored or otherwise contained on a digital versatile disk, comprising:

an encrypted data structure defining a secure information container stored on an optical disk medium, the encrypted data structure including and/or referencing at least one content object and at least one control object associated with the content object, said content object comprising digital property content and said control object comprising rules defining use rights to the digital property content.

DISH-Blue Spike 842
Exhibit 1005, Page 1407

56. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a content object further comprises one or more reference pointers to digital property content stored elsewhere on the digital versatile disk.

57. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises one or more reference pointers to control information stored elsewhere on the digital versatile disk.

58. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein an control object further comprises information for controlling various operations of an optical disk appliance or computer.

DISH-Blue Spike 842
Exhibit 1005, Page 1408

59. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises information for controlling various operations of an optical disk appliance or computer.

60. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises a rule specifying decoding and/or enforcement of CGMA encoded copy protection rules associated with the digital content property.

61. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a control object further comprises a rule specifying at least one content scrambling system compatible encoding/decoding of digital property content.

DISH-Blue Spike 842
Exhibit 1005, Page 1409

62. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein said optical disk contains a block of stored information comprising encrypted keys used for decryption of said encrypted data structure.

63. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein said optical disk contains a block of stored information comprising hidden keys used for decryption of said encrypted keys.

64. An arrangement for implementing a rights management system for digital versatile disks according to claim 55, wherein a content object further comprises one or more reference pointers to digital property content stored on a separate storage medium.

DISH-Blue Spike 842
Exhibit 1005, Page 1410

65. A rights management system for providing copy protection, use and/or distribution rights management for multi-media digital property content stored or otherwise contained on a digital versatile disk for access by an optical disk player device that uses digital property content stored on said optical disk medium, wherein said appliance includes a microprocessor controller for decrypting and using control rules and other selected encrypted information content encapsulated in the secure container by using a prescribed cryptographic key and applying said decrypted control rules to regulate use in accordance with control information contained within said control rules, so as to facilitate management of a diverse set of use and/or distribution rights which may be specific to different users and/or optical disk appliances, the system including:

an optical disk medium having stored thereon an encrypted data structure defining a secure information container, the encrypted data structure comprising and/or referencing at least one content object and at least one control object, said content object comprising digital property content, said control object

comprising rules defining use rights associated with the digital property.

66. A method for providing copy protection, use and distribution rights management of multi-media digital property stored on and/or distributed via digital versatile disk, said optical disk medium having stored thereon an encrypted data structure defining a secure container for housing rights and/or copy protection information pertaining to digital property content stored on the optical disk, wherein an optical disk player appliance for using digital property content stored on an optical disk must utilize a prescribed secure cryptographic key or set of keys to use the secure container, said data structure comprising one or more content objects comprising digital property content and one or more control objects comprising a set of rules defining use rights to digital property, comprising the steps of:

(a) decrypting control rules and other selected encrypted information content encapsulated in the secure container using one or more cryptographic keys; and

DISH-Blue Spike 842
Exhibit 1005, Page 1412

(b) applying decrypted control rules to regulate use and/or distribution of digital property content stored on the optical disk in accordance with control information contained within the control rules, so as to provide customized use and/or distribution rights that are specific to different optical disk user platforms and/or optical disk appliances.

67. A rights management system for providing copy protection, use and/or distribution rights management of digital property stored or otherwise contained on a digital versatile disk, comprising:

a secure container means provided on an optical disk medium for cryptographically encapsulating digital property content stored on the optical disk, said container means comprising a content object means for containing digital property content and a control object means for containing control rules for regulating use and/or distribution of said digital property content stored on the optical disk.

DISH-Blue Spike 842
Exhibit 1005, Page 1413

68. The rights management system of claim 67 wherein an optical disk player appliance for using information stored on an optical disk comprises a secure node means for using said secure container means provided on an optical disk and implementing said control rules to control operation of said player appliance to regulate use of said digital property content.

69. In a system including plural electronic appliances at least temporarily connected to one another, a rights authority broker that determines what appliances are connected and specifies at least one rights management context depending on said determination.

70. An electronic appliance at least temporarily connected to a rights authority broker, the electronic appliance receiving at least one rights context from the rights authority broker when the device is connected to the rights authority broker.

71. A first electronic appliance at least temporarily connected to a second electronic appliance, the first

electronic appliance selecting between at least first and second rights management contexts depending at least in part on whether the first appliance is connected to the second electronic appliance.

72. In a system including first and second electronic appliances that may be selectively coupled to communicate with one another, an arrangement for defining at least one different rights management control based at least in part on whether the first and second electronic appliances are connected.

73. A method of defining at least one rights management context comprising:

(a) determining whether a first electronic appliance is present; and

(b) defining at least one rights management control set based at least in part on the determining step (a).

DISH-Blue Spike 842
Exhibit 1005, Page 1415

74. A method of defining at least one rights management context including:

(a) coupling an optical disk storing information to an electronic appliance that can be selectively connected to a rights management broker;

(b) determining whether the electronic appliance is currently coupled to a rights management broker; and

(c) conditioning at least one aspect of use of at least some of the information stored on the optical disk based on whether the electronic appliance is coupled to the rights management broker.

75. A method as in claim 74 wherein step (c) includes the step of obtaining at least one rights management context from the rights management broker.

76. A method as in claim 74 wherein step (c) includes the step of obtaining at least one combined control set from the rights management broker.

DISH-Blue Spike 842
Exhibit 1005, Page 1416

77. A method of defining at least one rights management context including:

(a) coupling an optical disk storing information to an electronic appliance;

(b) using at least some of the information stored on the optical disk based on a first rights management context;

(c) coupling the electronic appliance to a rights management broker; and

(d) concurrently with step (c), using at least some of the information stored on the optical disk based on a second rights management context different from the first rights management context

78. An electronic appliance include a secure node and an optical disk reader, the electronic appliance applying different rights management contexts to protected information stored on an optical disk coupled to the optical disk reader depending at least in part on whether the electronic appliance is coupled to at least one additional secure node.

DISH-Blue Spike 842
Exhibit 1005, Page 1417

79. An electronic appliance including:

an optical disk reading and/or writing arrangement;

a secure node coupled to the optical disk reading and/or writing arrangement, the secure node performing at least one rights management related function with respect to at least some information read by the optical disk reading and/or writing arrangement; and

at least one serial bus port coupled to the secure node, the serial bus port for providing any or all of the functions, structures, protocols and/or methods of IEEE 1394-1995.

80. A digital versatile disk appliance including:

means for watermarking content; and

serial bus means for communicating the watermarked content,

wherein the serial bus means complies with IEEE 1394-1995.

DISH-Blue Spike 842
Exhibit 1005, Page 1418

81. An optical disk reading and/or writing device including:

at least one secure node capable of watermarking content and/or processing watermarked content; and

an IEEE 1394-1995 serial bus port.

82. An optical disk using device comprising:

a secure processing unit; and

an IEEE 1394-1995 serial bus port.

83. A device as in claim 82 wherein the secure processing unit includes a channel manager.

84. A device as in claim 82 wherein the secure processing unit executes a rights operating system in whole or in part.

85. A device as in claim 82 wherein the secure processing unit includes a tamper-resistant barrier.

86. A device as in claim 82 wherein the secure processing unit includes an encryption/decryption engine.

DISH-Blue Spike 842
Exhibit 1005, Page 1419

87. A rights cooperation method comprising:

(a) connecting an appliance to at least one further appliance;

(b) determining whether the first and/or further appliance and/or user(s) of said first and/or further appliance have appropriate rights and/or resources for performing an action; and

(c) selectively performing the action based at least in part on the determination.

88. A rights cooperation method comprising:

(a) connecting an appliance to at least one further appliance;

(b) determining whether the first and/or further appliance and/or user(s) of said first and/or further appliance have appropriate security for performing an action; and

(c) cooperating between the first and further appliance to selectively perform the action.

89. A cooperative rights management arrangement comprising:

DISH-Blue Spike 842
Exhibit 1005, Page 1420

a communications arrangement that allows at least first and second appliances to communicate; and

an arrangement that processes at least one event based at least in part on assessing and/or pooling rights and/or resources between the first and second appliances.

90. An optical disk using system and/or method including at least some of the elements shown in Figure 1A.

91. An optical disk using system and/or method including at least some of the elements shown in Figure 1B.

92. An optical disk using system and/or method including at least some of the elements shown in Figure 1C.

93. An optical disk using system and/or method including at least some of the elements shown in Figure 2A.

94. An optical disk using system and/or method including at least some of the elements shown in Figure 2B.

DISH-Blue Spike 842
Exhibit 1005, Page 1421

95. An optical disk using system and/or method including at least some of the elements shown in Figure 3.

96. An optical disk using system and/or method using at least some of the elements shown in Figure 3A.

97. An optical disk using system and/or method using at least some of the control set elements shown in Figure 3B.

98. An optical disk using system and/or method using at least some of the elements shown in Figure 4A.

99. An optical disk using system and/or method using at least some of the elements shown in Figure 4B.

DISH-Blue Spike 842
Exhibit 1005, Page 1422

100. An optical disk using system and/or method using at least some of the elements shown in Figure 5.

101. An optical disk using system and/or method using at least some of the elements shown in Figure 6.

102. An optical disk using system and/or method using at least some of the elements shown in Figure 7.

103. An optical disk using system and/or method using at least some of the elements shown in Figure 8.

104. An optical disk using system and/or method using at least some of the elements shown in Figure 9.

105. An optical disk using system and/or method using at least some of the elements shown in Figure 10.

DISH-Blue Spike 842
Exhibit 1005, Page 1423

106. An optical disk using system and/or method using at least some of the elements shown in Figure 11.

107. An optical disk using system and/or method including at least some of the elements shown in Figure 12.

108. An optical disk using system and/or method including at least some of the elements shown in Figure 13.

109. An optical disk using system and/or method including at least some of the elements shown in Figure 14.

110. A system and/or method including some or all of the elements shown in Figures 15A-15C.

111. A system and/or method as in any one of the preceding claims, further including, in combination, any element described in any one of the following prior patent specifications:

PCT Publication No. WO 96/27155;

DISH-Blue Spike 842
Exhibit 1005, Page 1424

European Patent No. EP 329681;

PCT Application No. PCT/US96/14262;

U.S. Patent Application Serial No. 08/689,606; and/or

U.S. Patent Application Serial No. 08/689,754.

112. A system or process as in any of the preceding claims wherein the phrase "high capacity optical disk" is substituted for "digital versatile disk."

113. A method of clearing or otherwise processing information resulting at least in part from one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

114. A system and/or method for defining rules for use in one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

DISH-Blue Spike 842
Exhibit 1005, Page 1425

115. A system and/or method for defining rules and associated content for use in one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

116. A system and/or method for producing an optical disk for use with one or more digital versatile disk appliances and/or methods as defined in any of the preceding claims.

117. A system and/or method for clearing audit information from one or more appliances and/or methods as defined in any of the preceding claims.

118. In an network including at least one electronic appliance that reads information from and/or writes information to at least one digital versatile disk optical storage medium, and securely communicates information associated with at least one of

DISH-Blue Spike 842
Exhibit 1005, Page 1426

payment, auditing, usage, access, controlling and/or otherwise managing content recorded on the storage medium, a method of processing said communicated information including the step of generating at least one payment request and/or order based at least in part on the information.

119. A method of defining at least one control set for storage on a high capacity optical disk that can storage images, audio, text and/or other information, the high capacity optical disk for use by any of plural different electronic appliance types, the method including the step of specifying at least one control that provides different conditions and/or consequences depending upon at least one of the following:

electronic appliance class;

electronic appliance security;

electronic appliance user class;

electronic appliance connectivity;

DISH-Blue Spike 842
Exhibit 1005, Page 1427

electronic appliance resources;

electronic appliance access to resources; and

rights management cooperation between plural electronic appliances.

DISH-Blue Spike 842
Exhibit 1005, Page 1428

Fig.1B

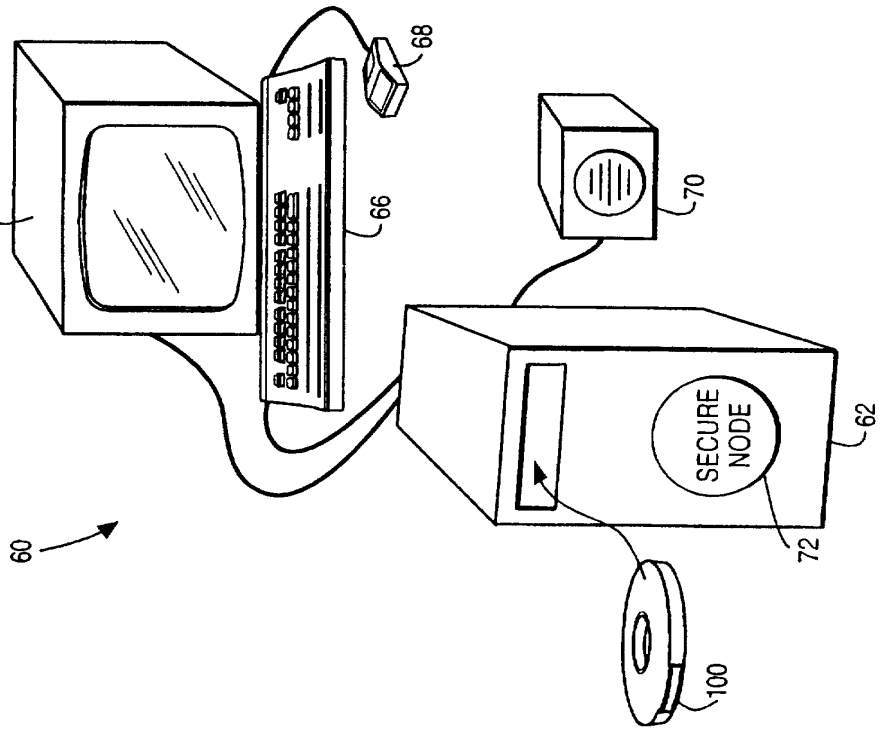
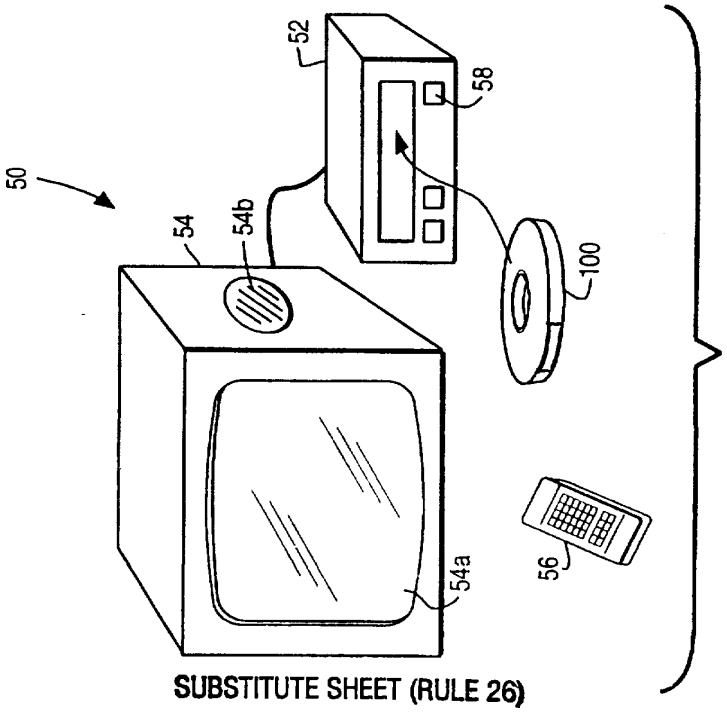


Fig.1A



DISH-Blue Spike 842
Exhibit 1005, Page 1430

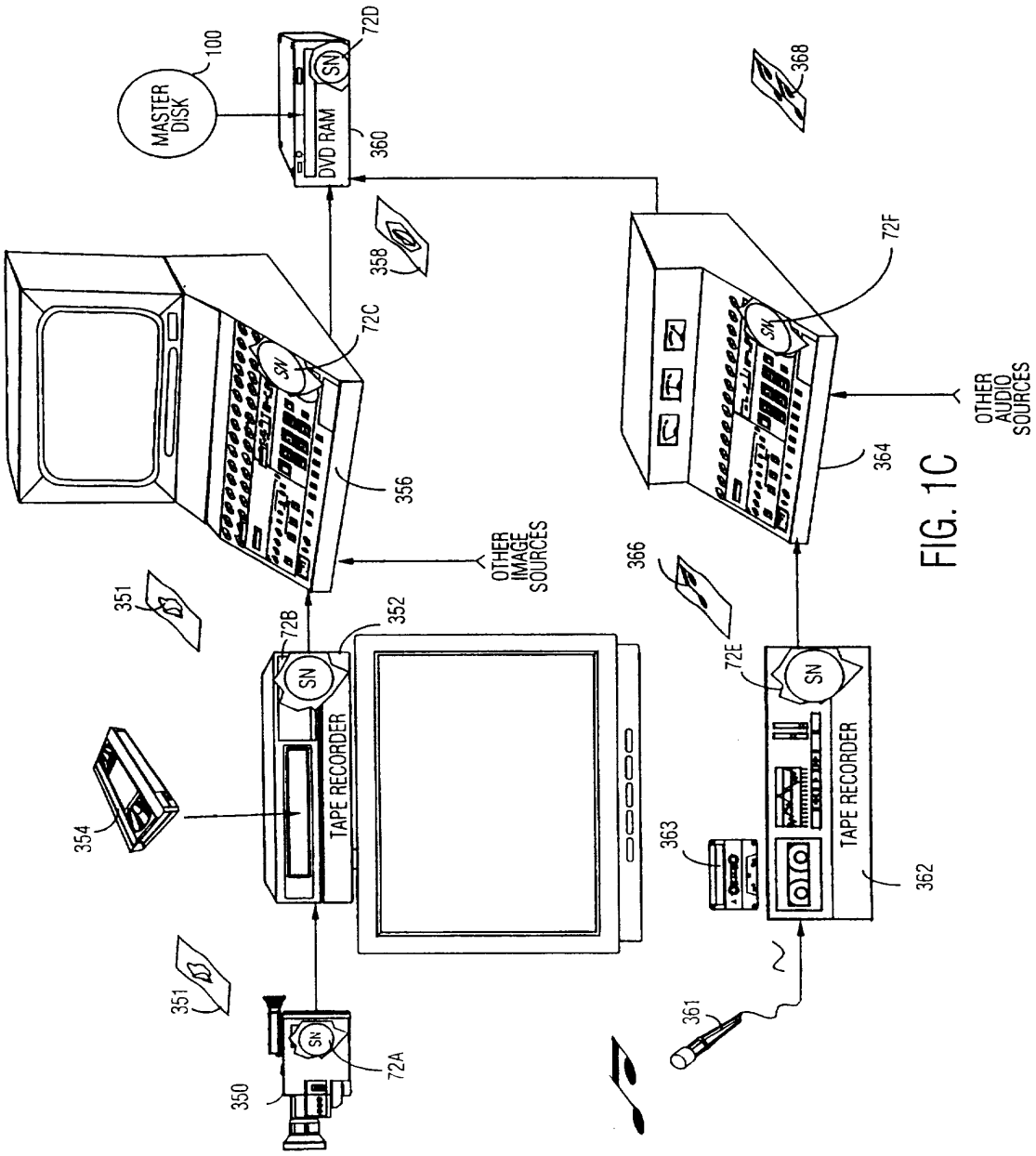


FIG. 1C

SUBSTITUTE SHEET (RULE 26)

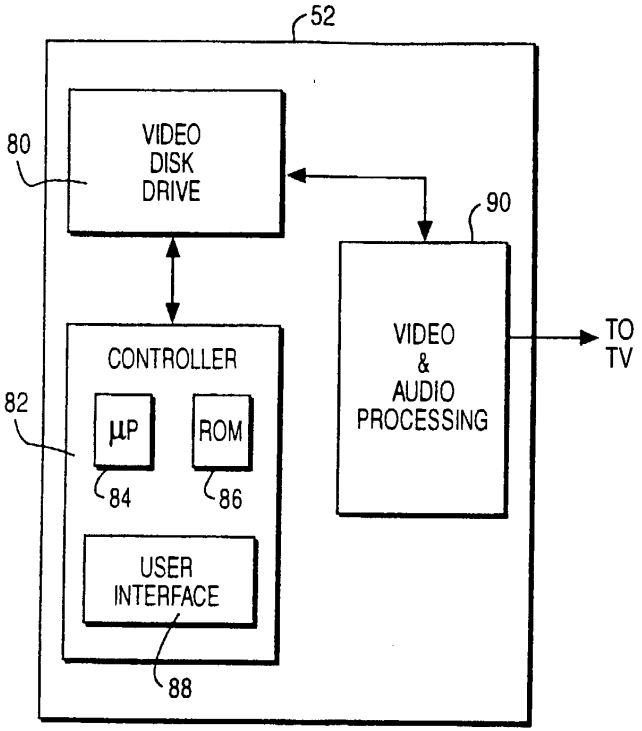


Fig.2A

EXAMPLE PLAYER ARCHITECTURE

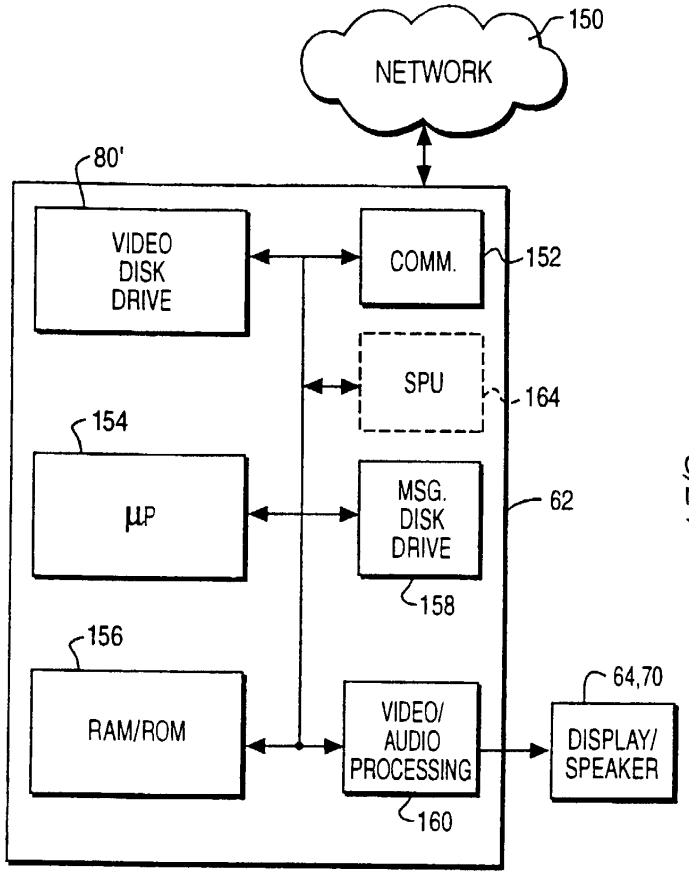
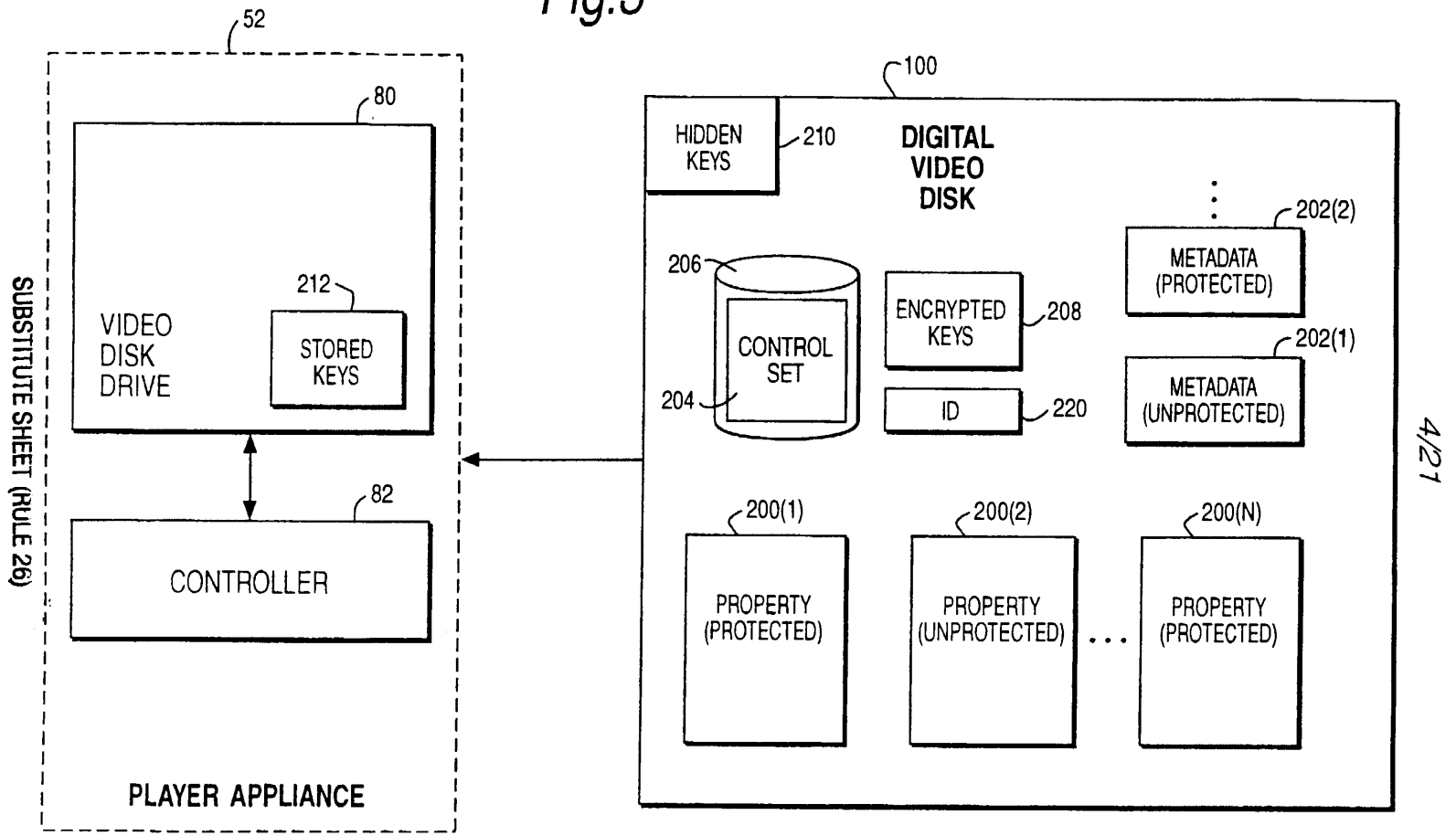


Fig.2B

EXAMPLE SECURE NODE ARCHITECTURE

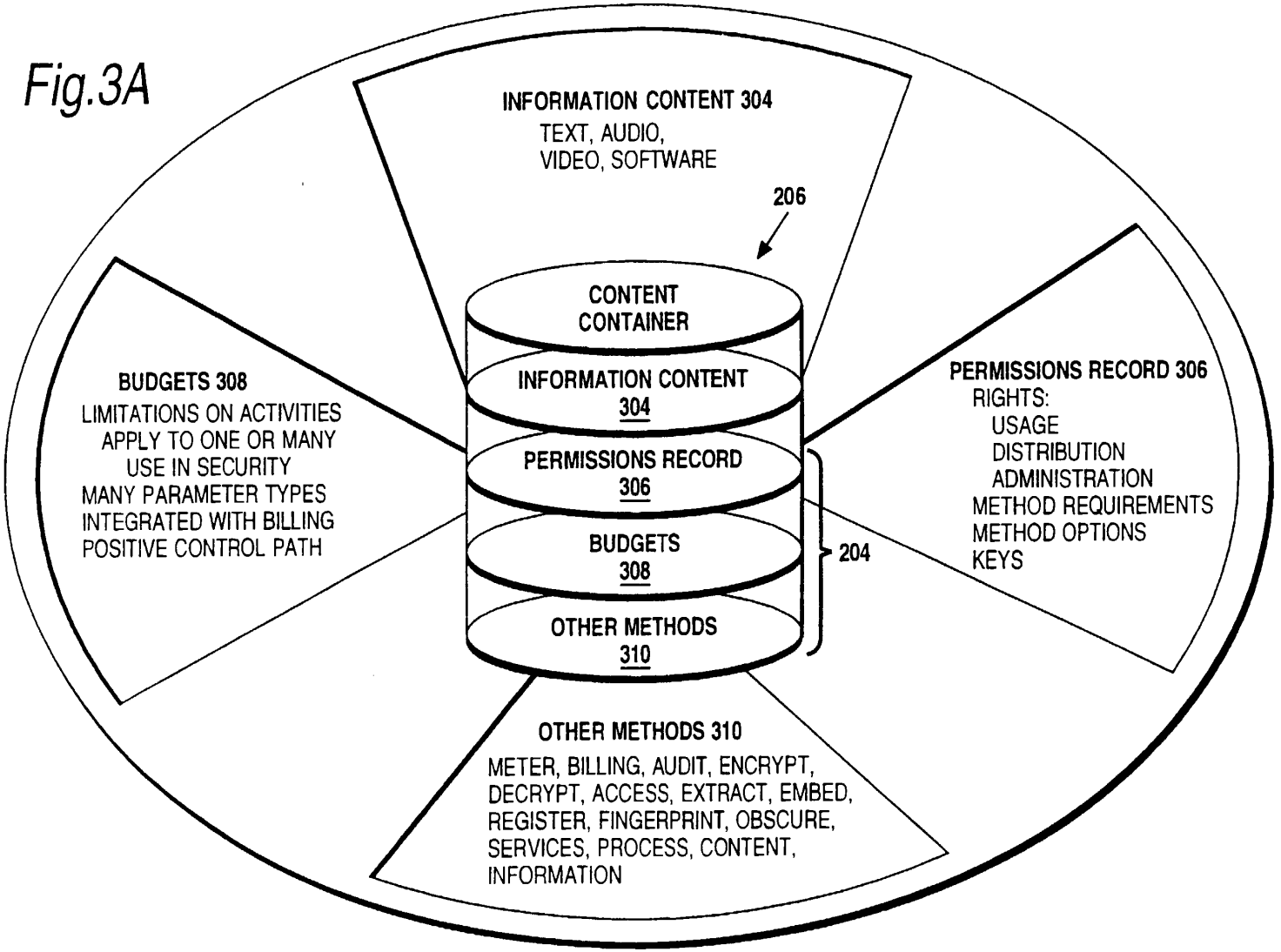
Fig.3



SUBSTITUTE SHEET (RULE 26)

DISH-Blue Spike 842
Exhibit 1005, Page 1432

Fig.3A


INFORMATION CONTENT 304
TEXT, AUDIO,
VIDEO, SOFTWARE
206
CONTENT
CONTAINER
INFORMATION CONTENT
304
PERMISSIONS RECORD
306
BUDGETS
308
OTHER METHODS
310
204
BUDGETS 308
LIMITATIONS ON ACTIVITIES
APPLY TO ONE OR MANY
USE IN SECURITY
MANY PARAMETER TYPES
INTEGRATED WITH BILLING
POSITIVE CONTROL PATH
PERMISSIONS RECORD 306
RIGHTS:
USAGE
DISTRIBUTION
ADMINISTRATION
METHOD REQUIREMENTS
METHOD OPTIONS
KEYS
OTHER METHODS 310
METER, BILLING, AUDIT, ENCRYPT,
DECRYPT, ACCESS, EXTRACT, EMBED,
REGISTER, FINGERPRINT, OBSCURE,
SERVICES, PROCESS, CONTENT,
INFORMATION

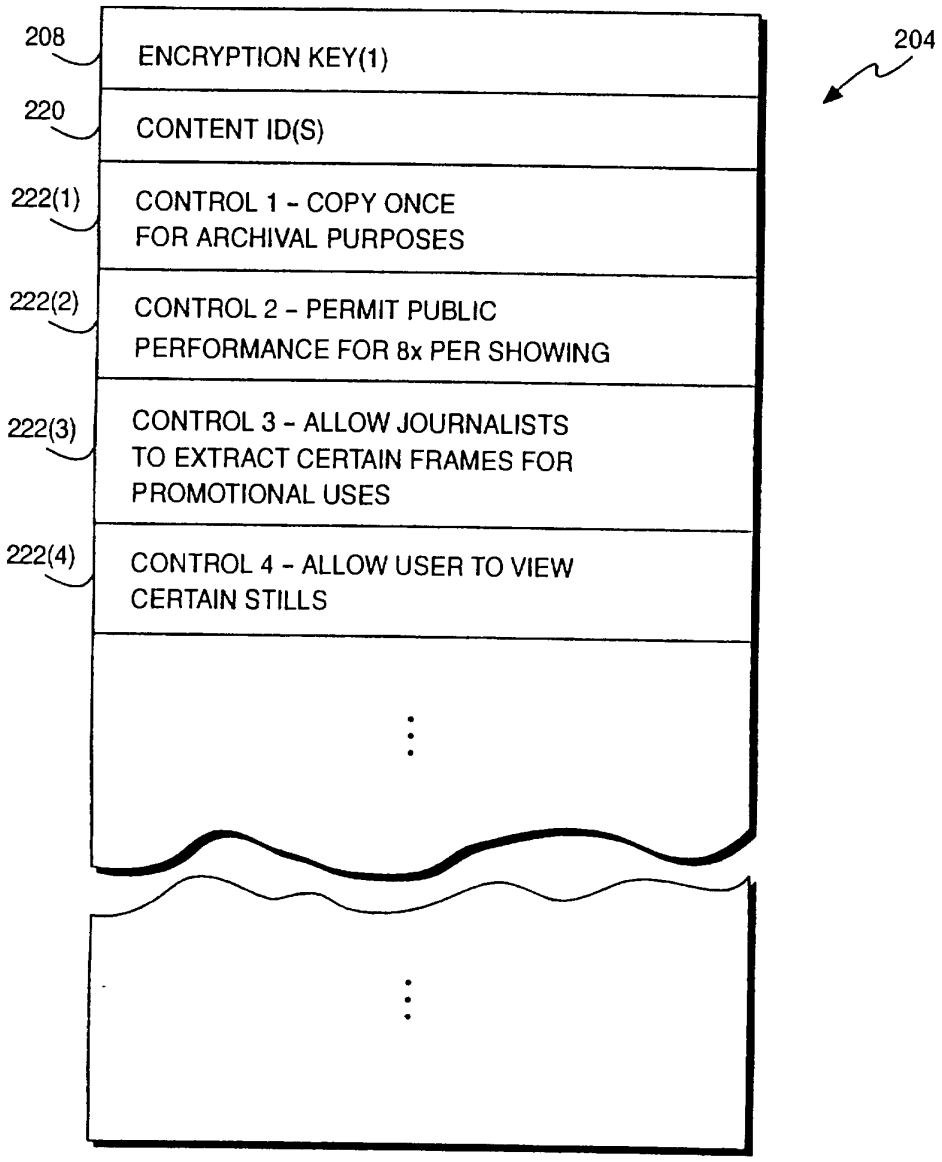


Fig.3B

EXAMPLE CONTROL SET

Fig.4A
EXAMPLE PLAYER STEPS

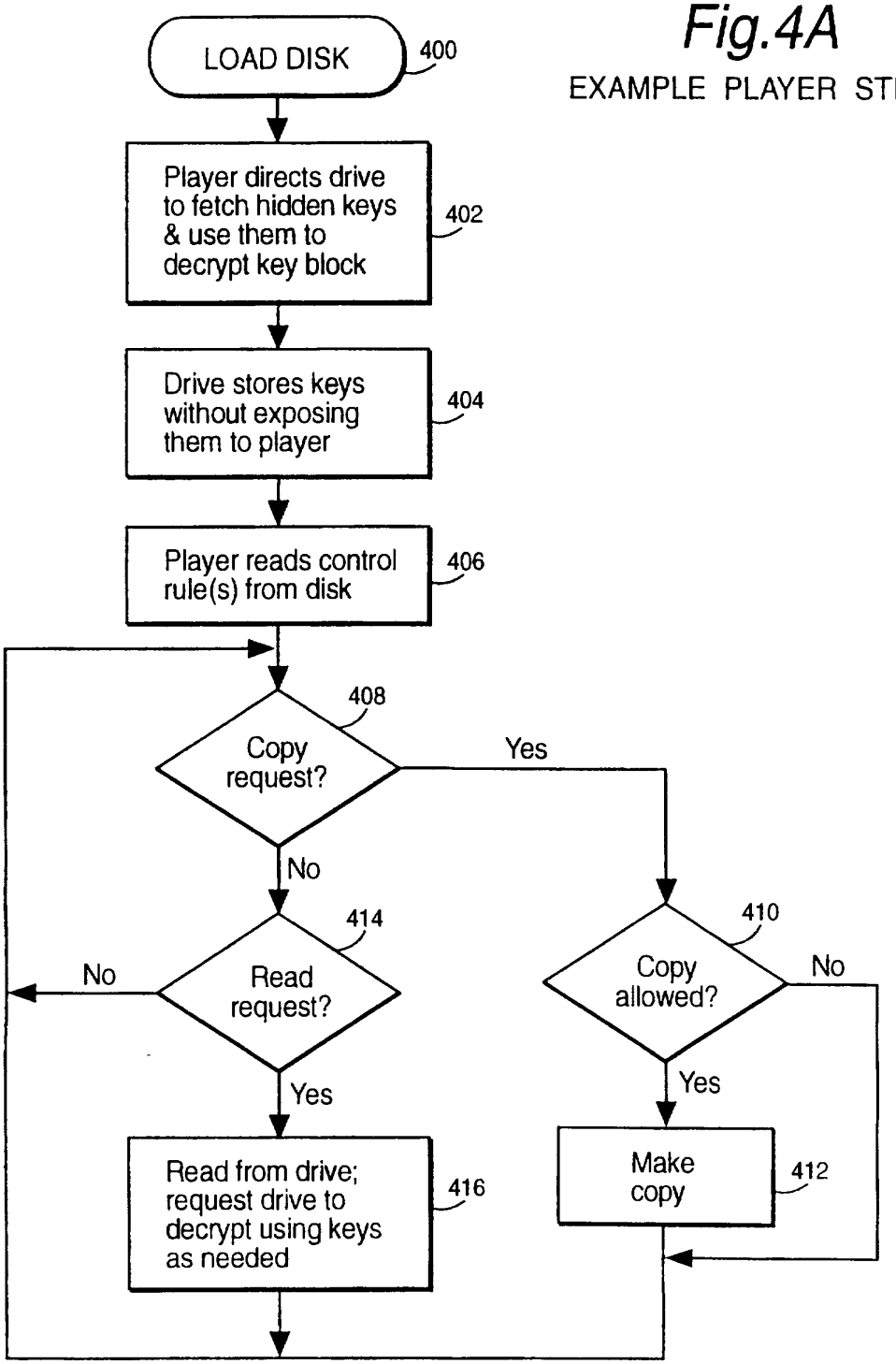
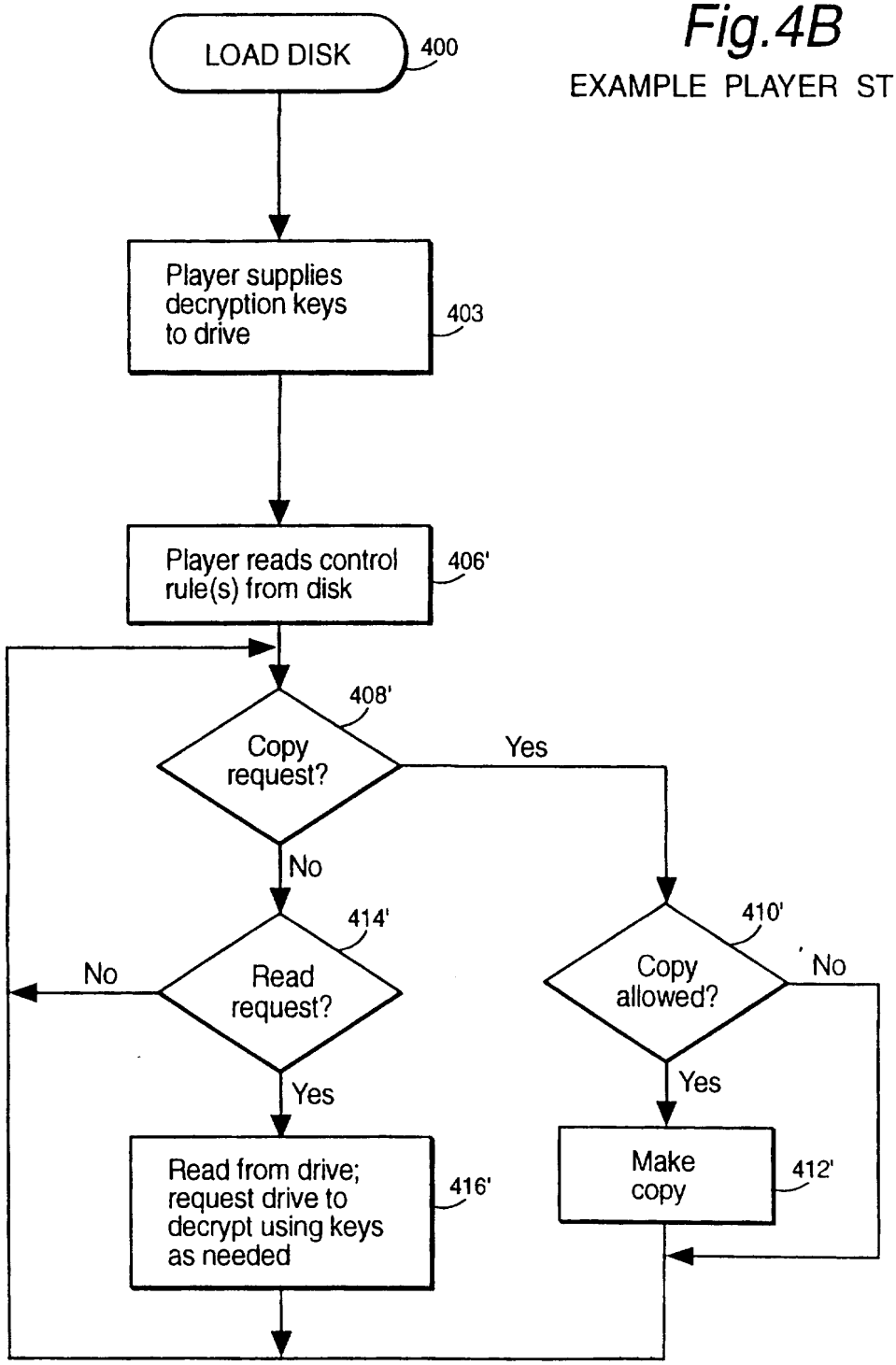


Fig.4B
EXAMPLE PLAYER STEPS



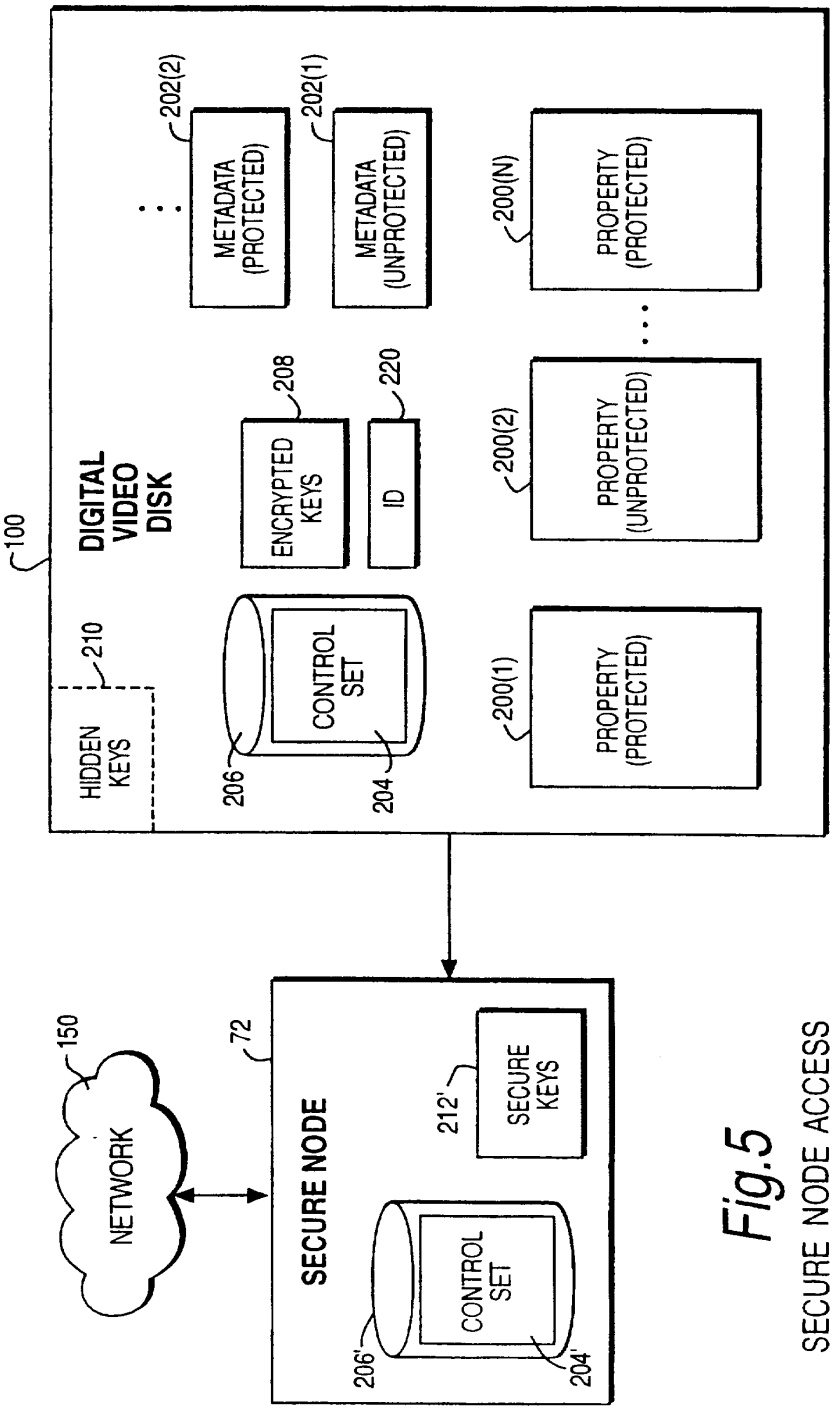


Fig.5
SECURE NODE ACCESS

DISH-Blue Spike 842
Exhibit 1005, Page 1437

Fig.6

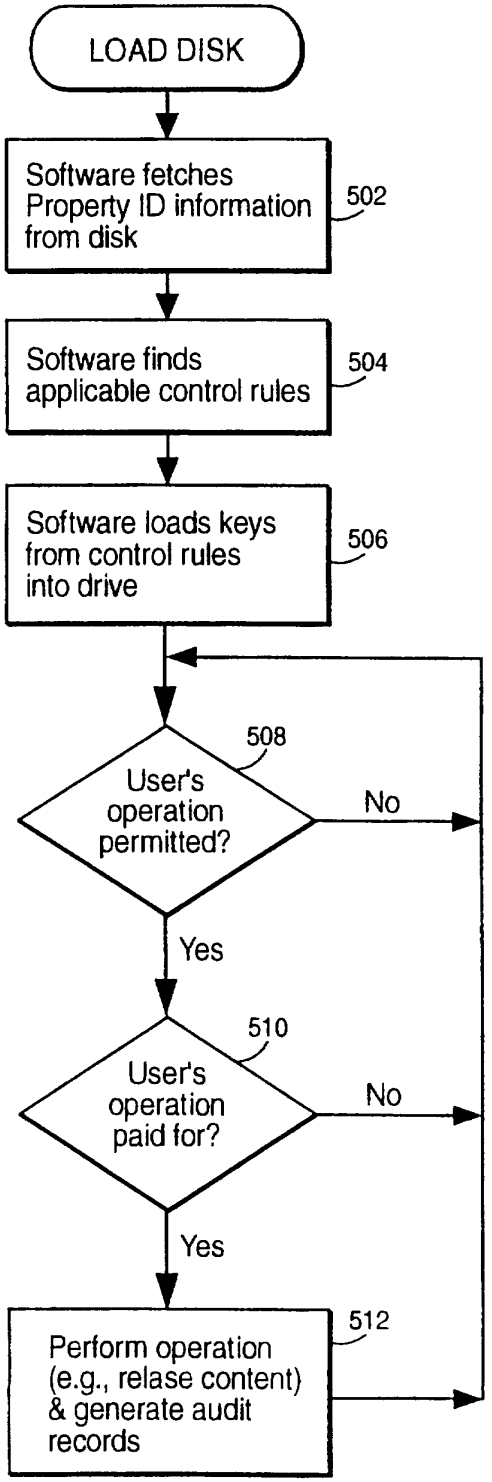
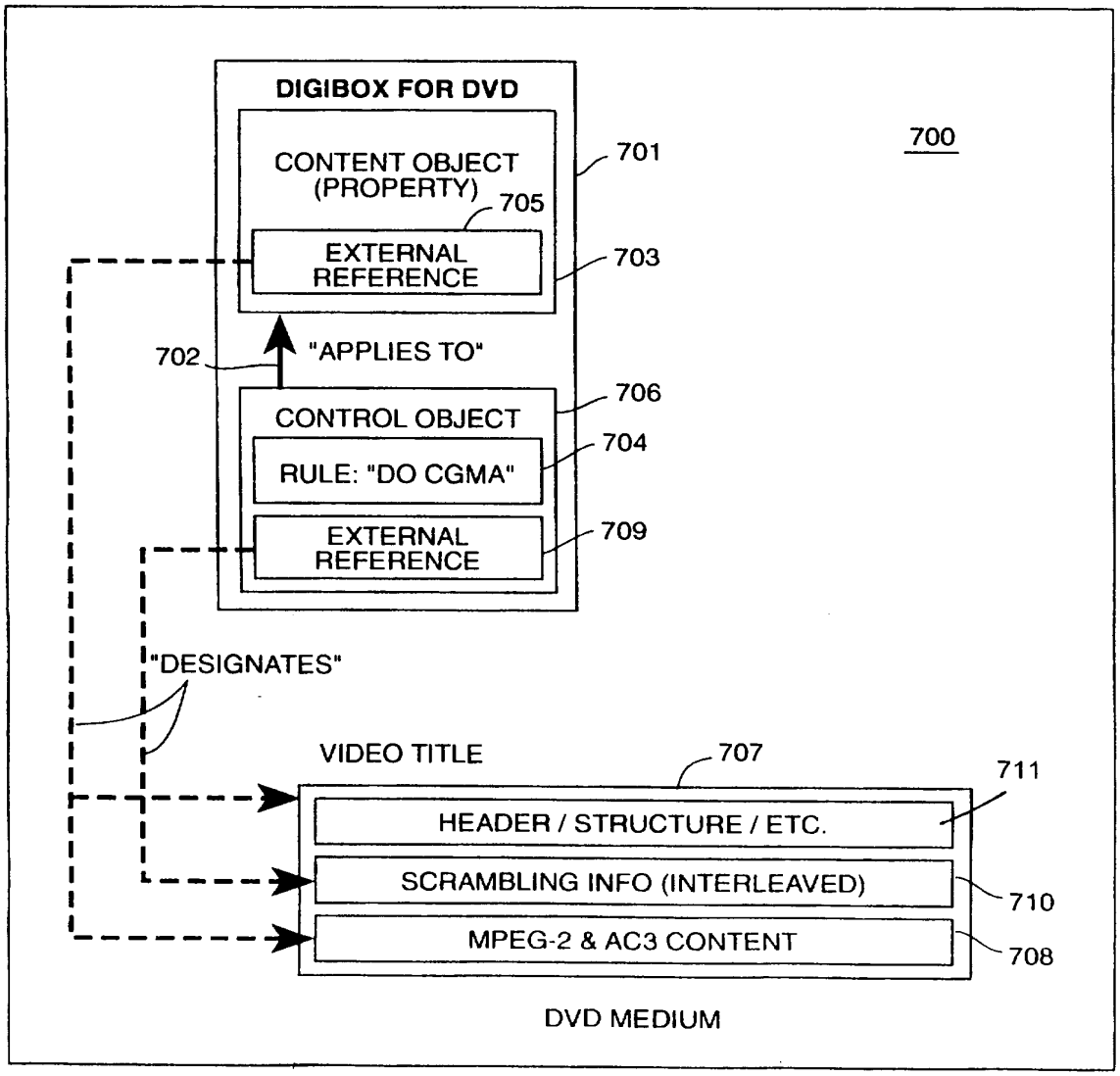
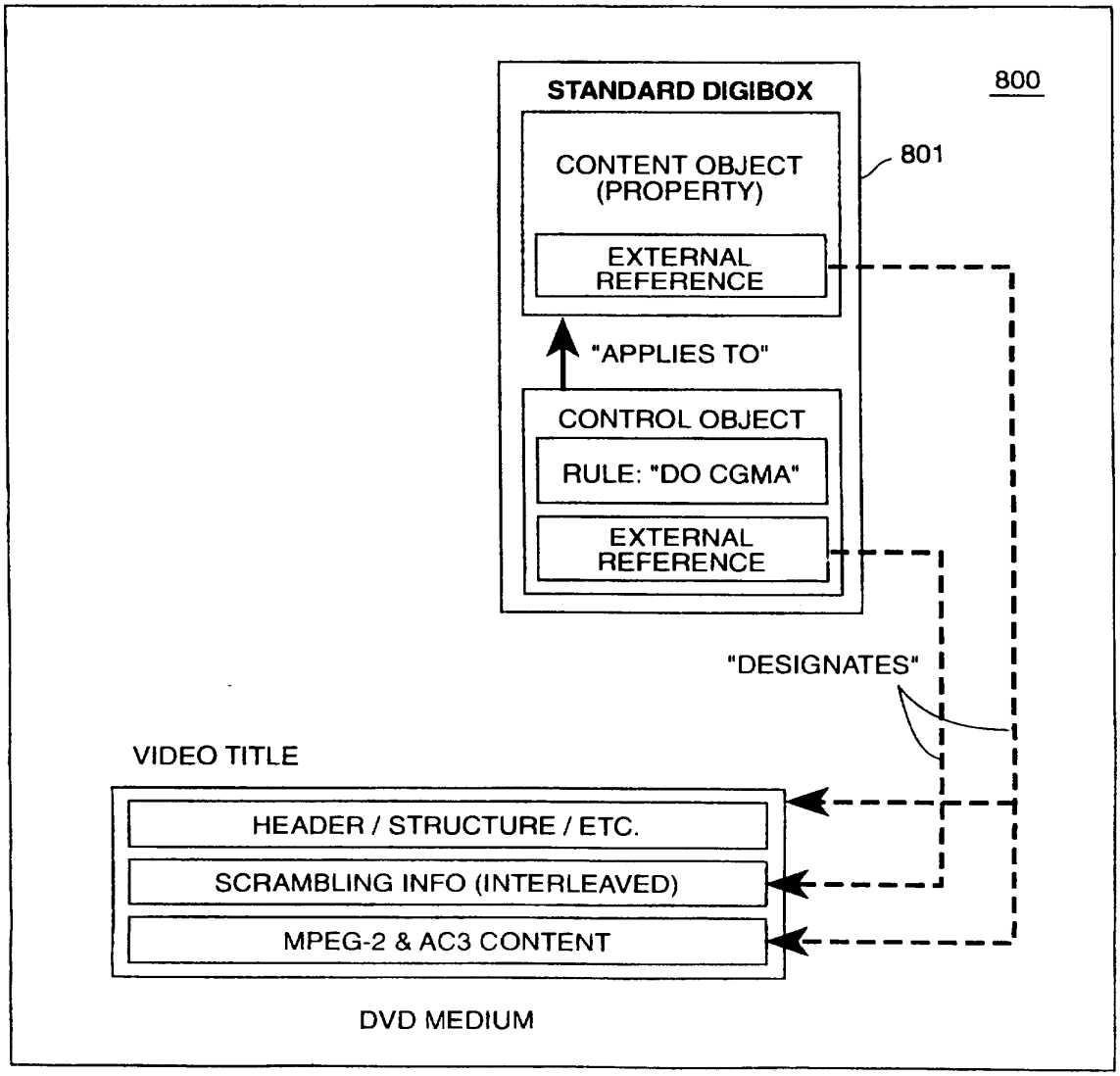

LOAD DISK
Software fetches Property ID information from disk
502
Software finds applicable control rules
504
Software loads keys from control rules into drive
506
508
User's operation permitted?
No
Yes
510
User's operation paid for?
No
Yes
512
Perform operation (e.g., relase content) & generate audit records

FIG. 7



DISH-Blue Spike 842
Exhibit 1005, Page 1439

FIG. 8



DISH-Blue Spike 842
Exhibit 1005, Page 1440

FIG. 9

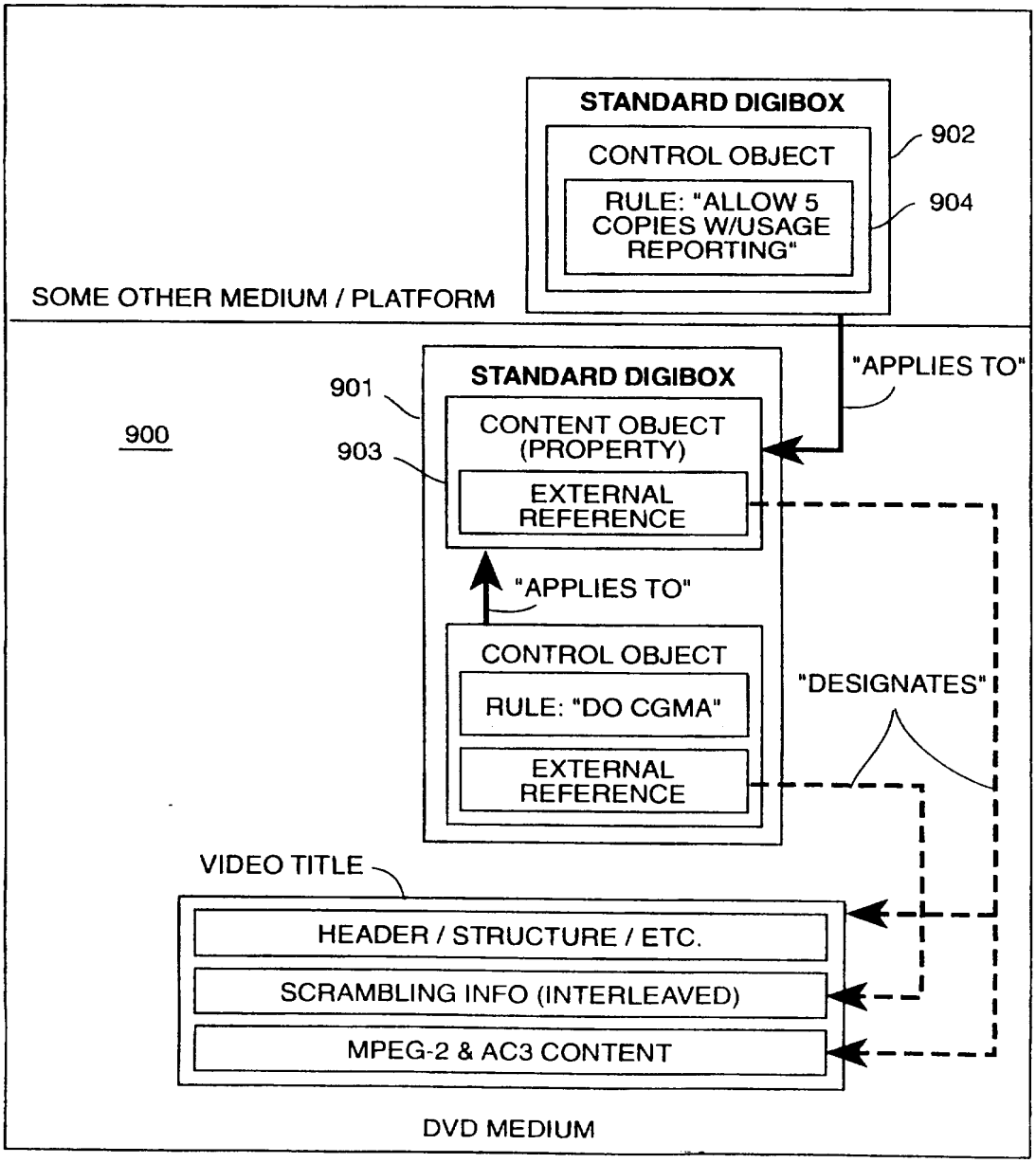

STANDARD DIGIBOX
CONTROL OBJECT
RULE: "ALLOW 5 COPIES W/USAGE REPORTING"
902
904
SOME OTHER MEDIUM / PLATFORM
"APPLIES TO"
STANDARD DIGIBOX
901
900
CONTENT OBJECT (PROPERTY)
903
EXTERNAL REFERENCE
"APPLIES TO"
CONTROL OBJECT
RULE: "DO CGMA"
EXTERNAL REFERENCE
"DESIGNATES"
VIDEO TITLE
HEADER / STRUCTURE / ETC.
SCRAMBLING INFO (INTERLEAVED)
MPEG-2 & AC3 CONTENT
DVD MEDIUM

FIG. 10

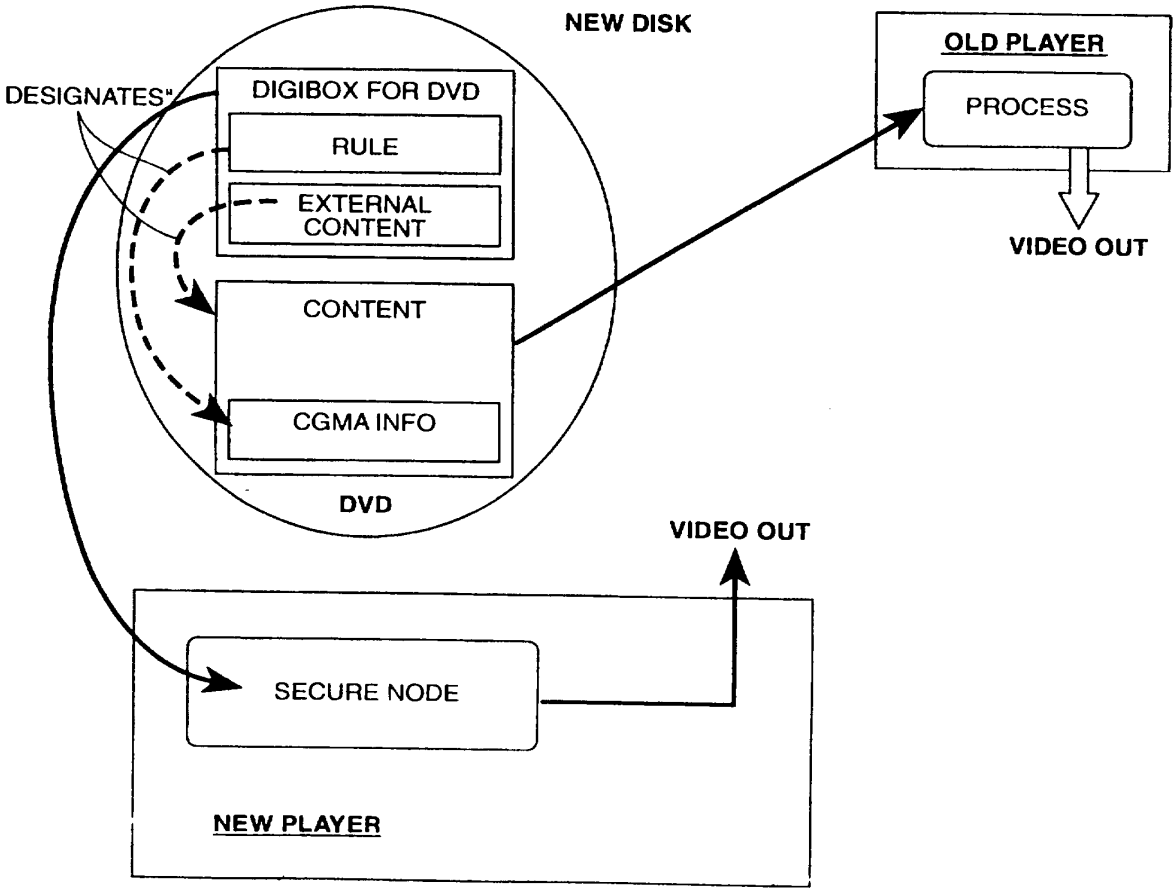
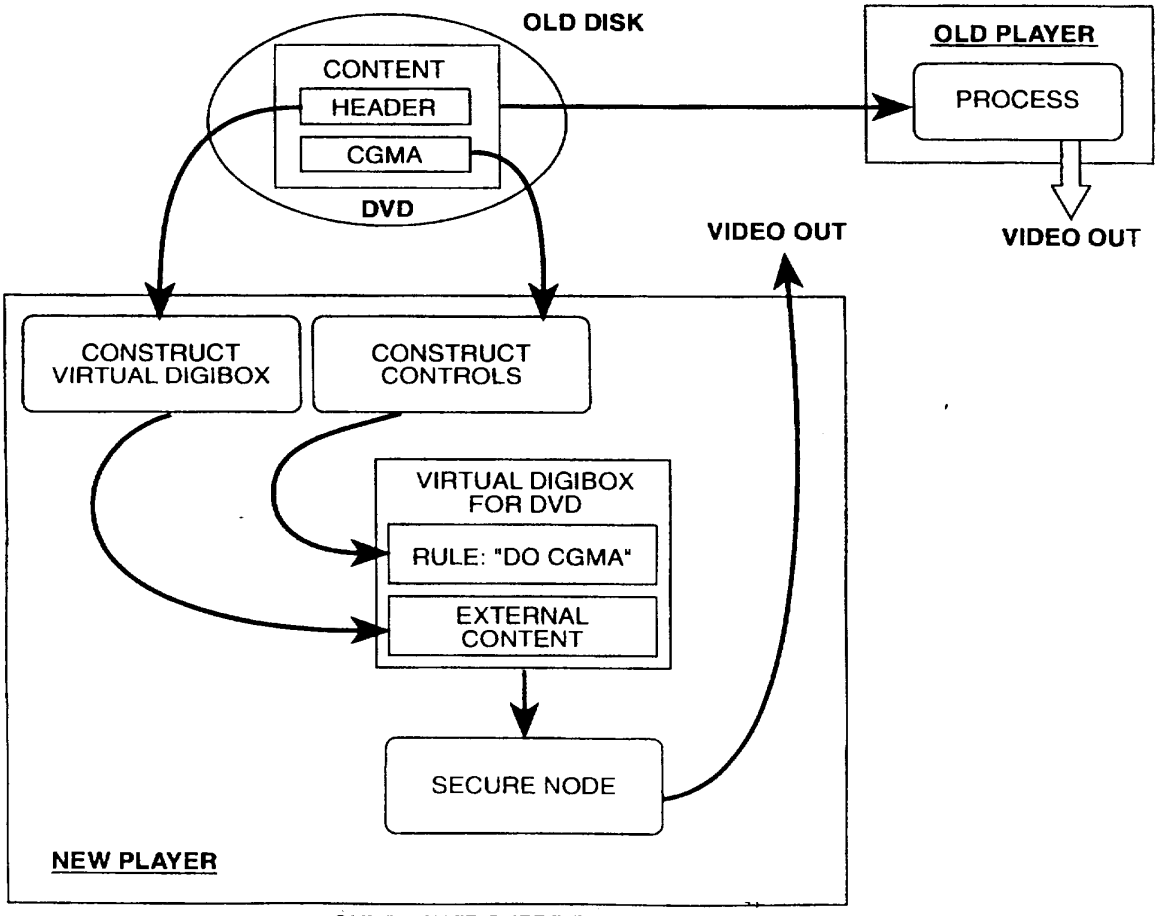

NEW DISK
DESIGNATES"
DIGIBOX FOR DVD
RULE
EXTERNAL CONTENT
CONTENT
CGMA INFO
DVD
OLD PLAYER
PROCESS
VIDEO OUT
VIDEO OUT
SECURE NODE
NEW PLAYER

FIG. 11


OLD DISK
CONTENT
HEADER
CGMA
DVD
OLD PLAYER
PROCESS
VIDEO OUT
VIDEO OUT
CONSTRUCT VIRTUAL DIGIBOX
CONSTRUCT CONTROLS
VIRTUAL DIGIBOX FOR DVD
RULE: "DO CGMA"
EXTERNAL CONTENT
SECURE NODE
NEW PLAYER

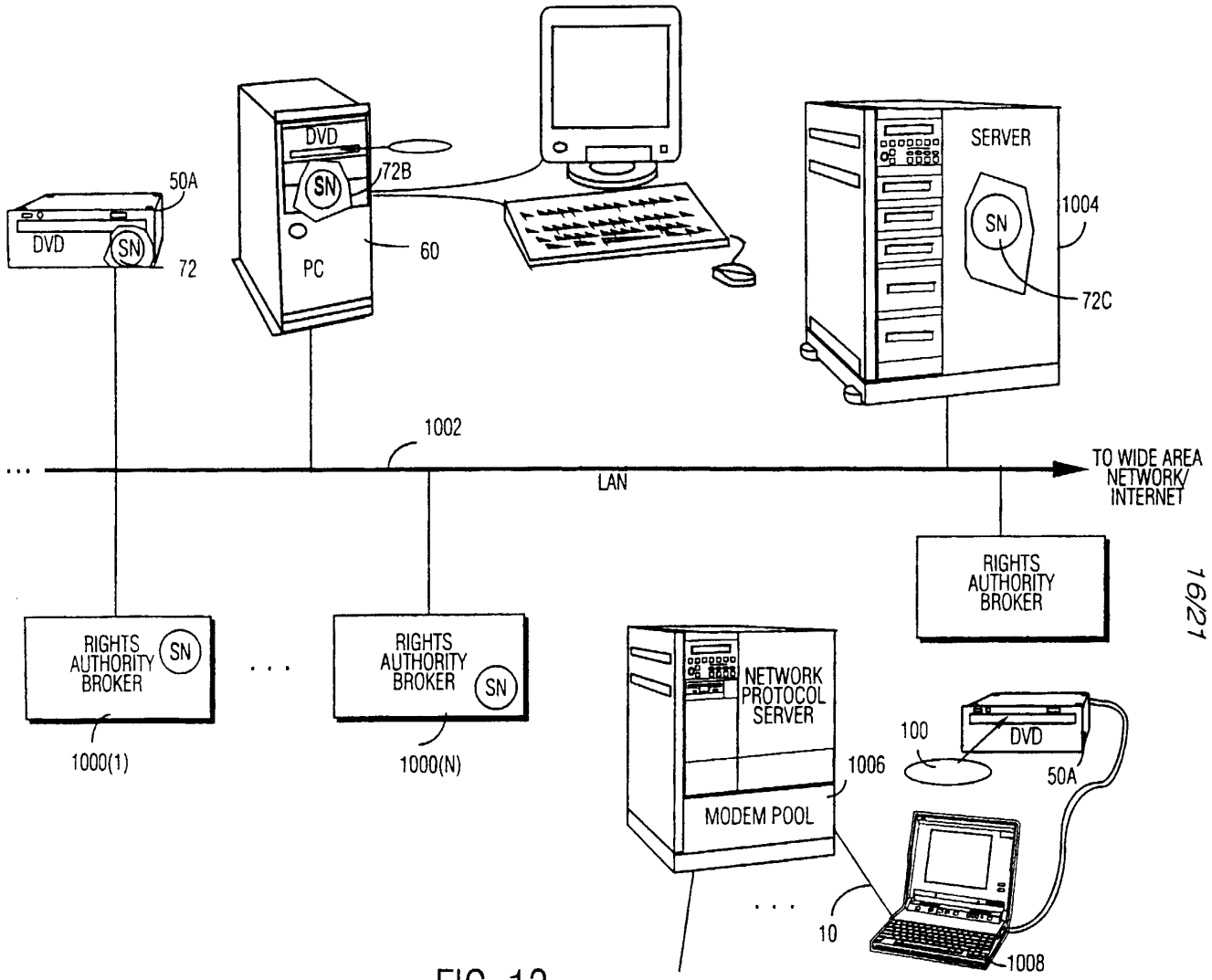

DVD
SN
50A
72
DVD
SN
72B
PC
60
SERVER
SN
1004
72C
1002
LAN
TO WIDE AREA NETWORK/ INTERNET
RIGHTS AUTHORITY BROKER
SN
1000(1)
RIGHTS AUTHORITY BROKER
SN
1000(N)
RIGHTS AUTHORITY BROKER
NETWORK PROTOCOL SERVER
1006
MODEM POOL
100
DVD
50A
10
1008

FIG. 12

DISH-Blue Spike 842
Exhibit 1005, Page 1445

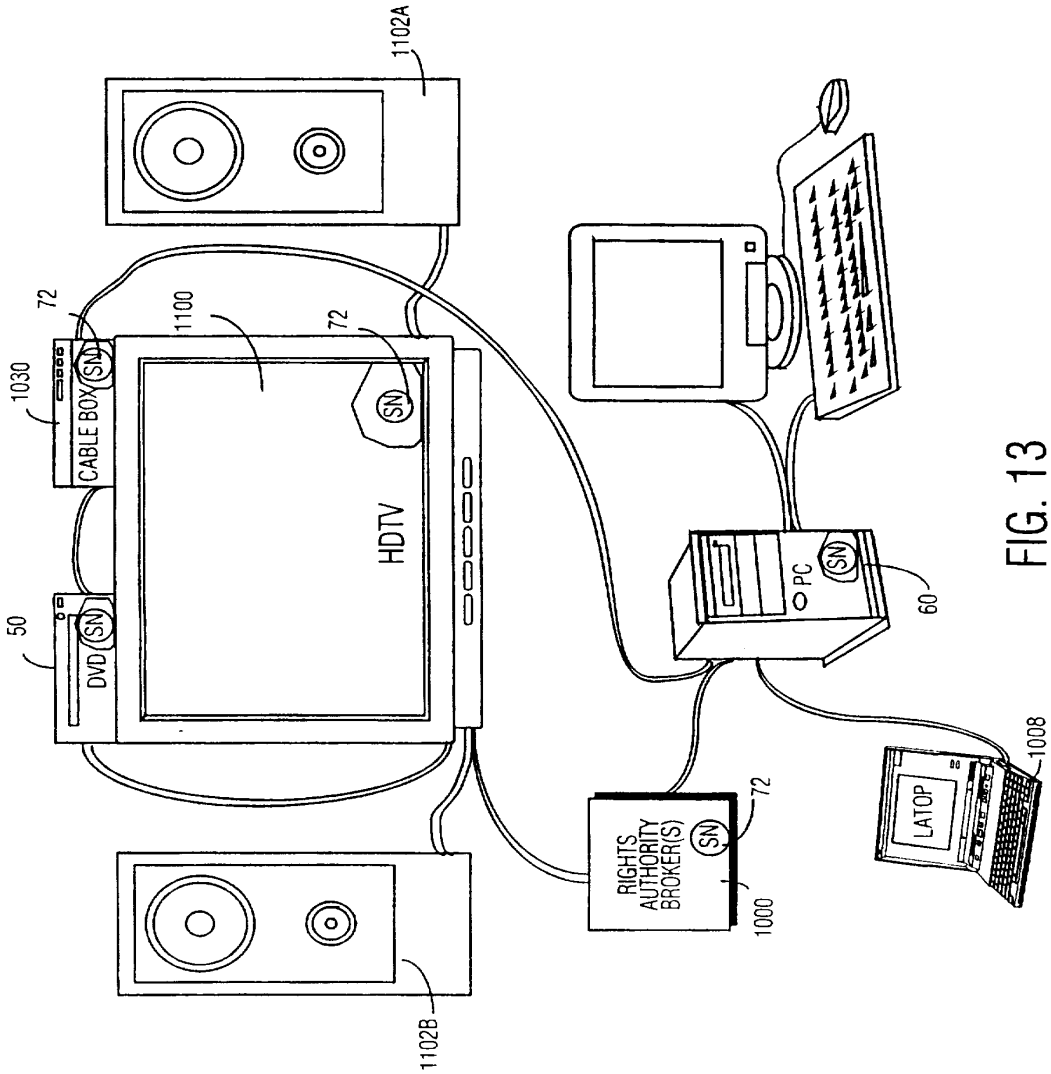


FIG. 13

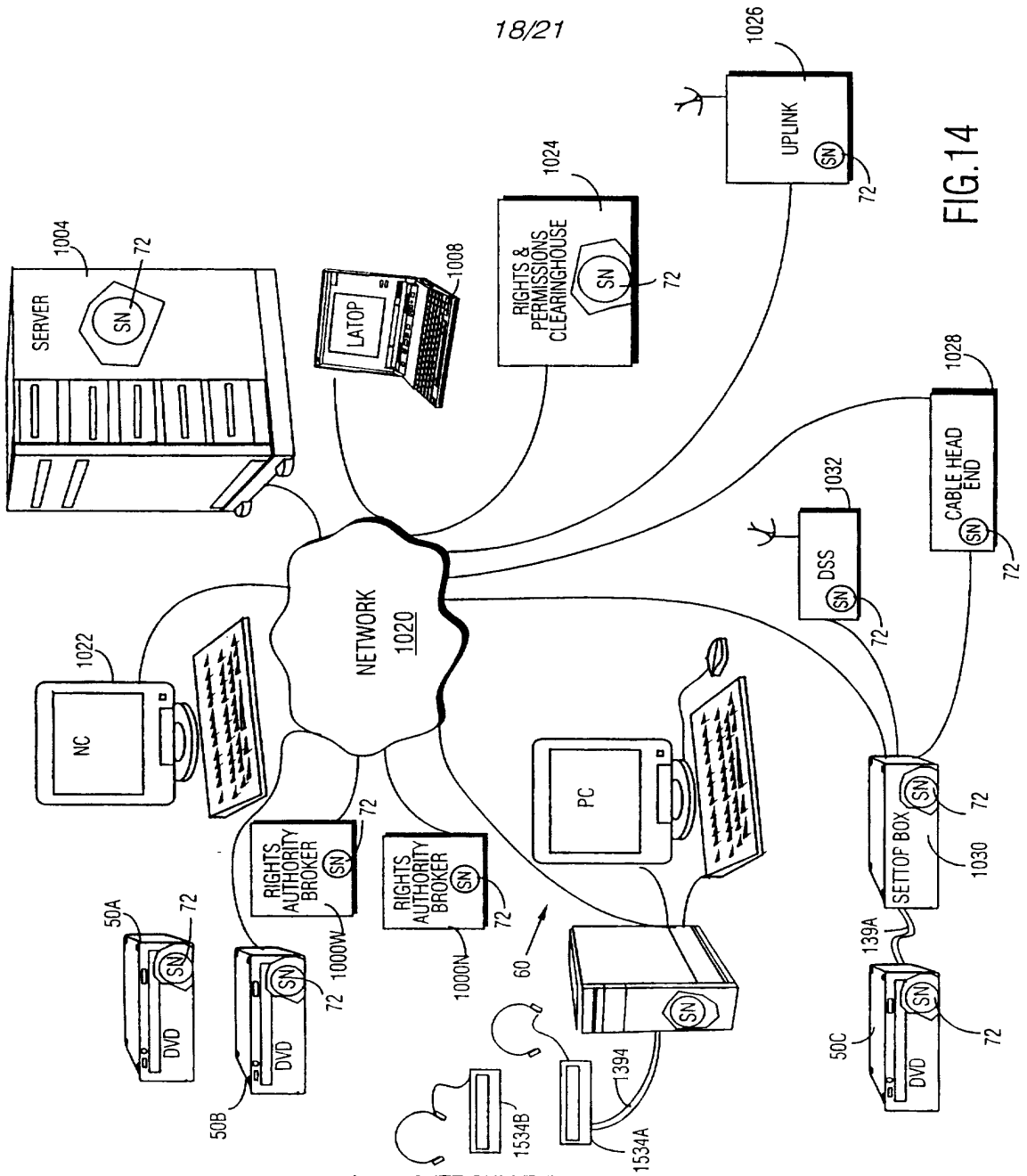


FIG.14

DISH-Blue Spike 842
Exhibit 1005, Page 1446

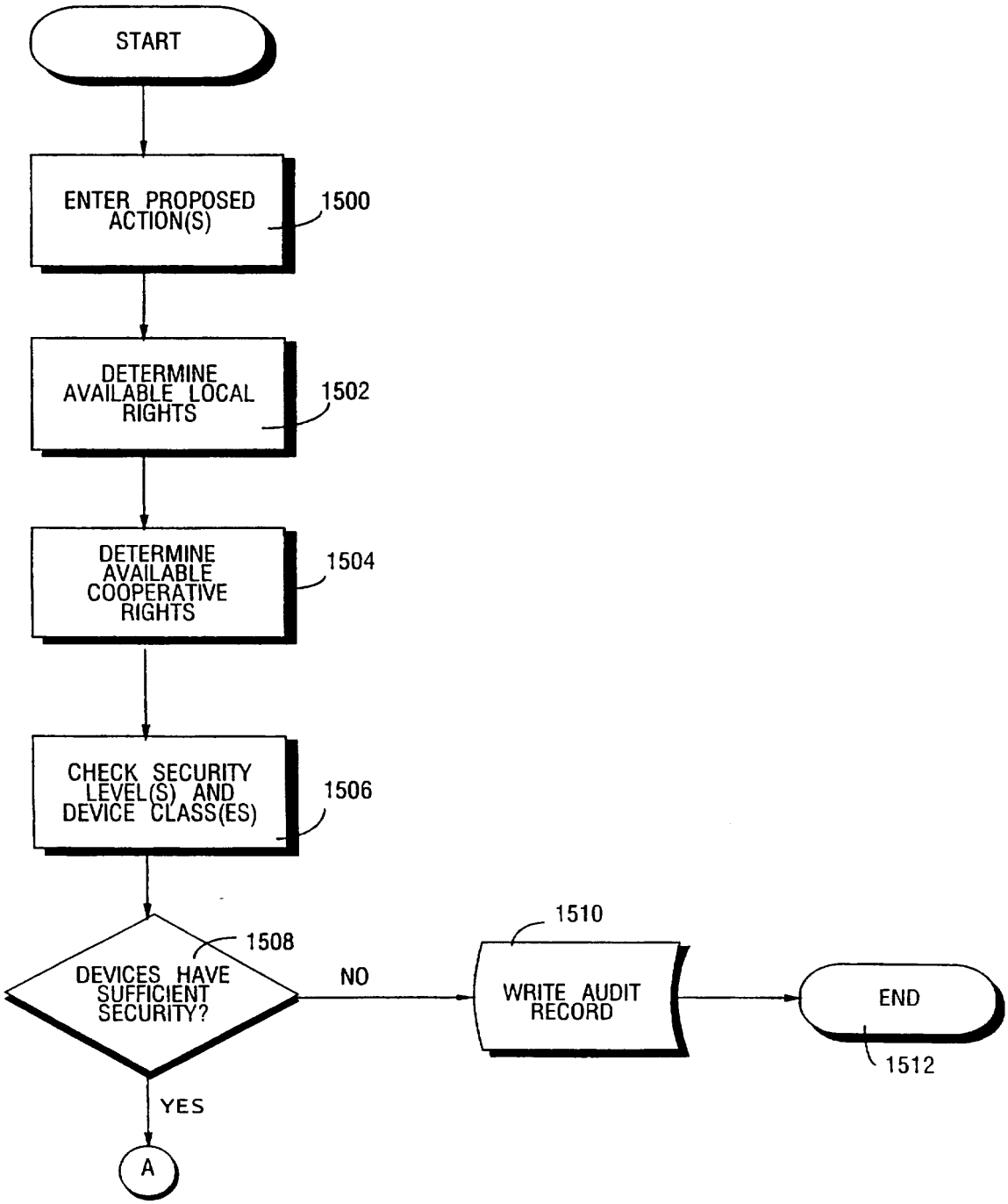

START
ENTER PROPOSED ACTION(S)
1500
DETERMINE AVAILABLE LOCAL RIGHTS
1502
DETERMINE AVAILABLE COOPERATIVE RIGHTS
1504
CHECK SECURITY LEVEL(S) AND DEVICE CLASS(ES)
1506
DEVICES HAVE SUFFICIENT SECURITY?
1508
NO
1510
WRITE AUDIT RECORD
END
1512
YES
A

FIG.15A

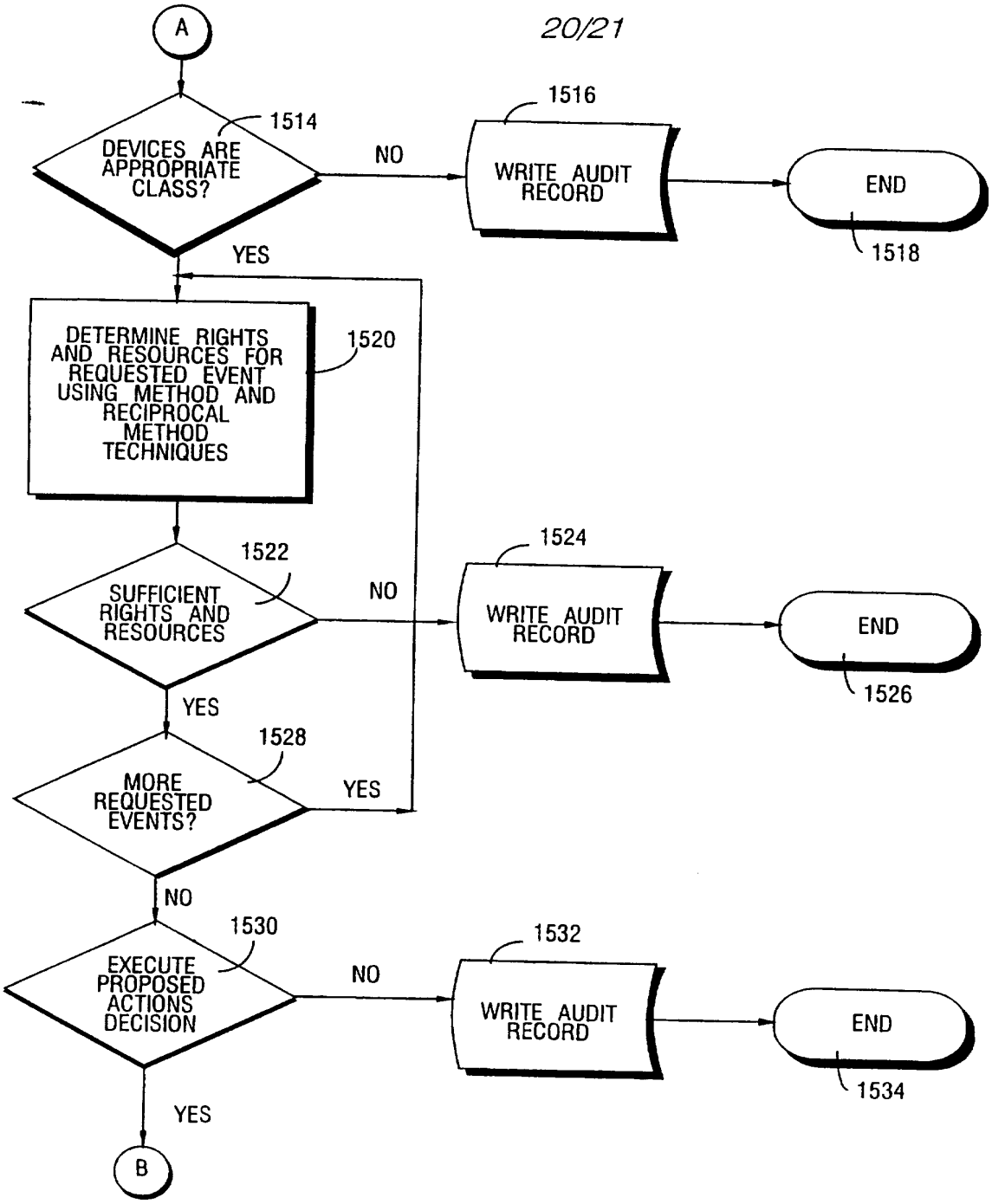
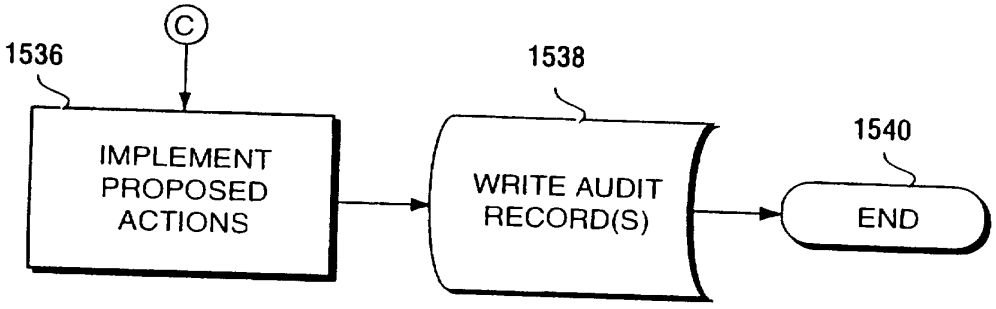

A
DEVICES ARE APPROPRIATE CLASS?
1514
NO
1516
WRITE AUDIT RECORD
END
1518
YES
DETERMINE RIGHTS AND RESOURCES FOR REQUESTED EVENT USING METHOD AND RECIPROCAL METHOD TECHNIQUES
1520
SUFFICIENT RIGHTS AND RESOURCES
1522
NO
1524
WRITE AUDIT RECORD
END
1526
YES
MORE REQUESTED EVENTS?
1528
YES
NO
EXECUTE PROPOSED ACTIONS DECISION
1530
NO
1532
WRITE AUDIT RECORD
END
1534
YES
B

FIG.15B

FIG. 15C


C
1536
IMPLEMENT PROPOSED ACTIONS
1538
WRITE AUDIT RECORD(S)
1540
END

Electronic Acknowledgement Receipt

EFS ID:	35194940
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-FEB-2019
Filing Date:	16-MAY-2018
Time Stamp:	19:23:32
Application Type:	Reexam (Third Party)

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	Foreign Reference	F030_Exhibit3_WO9955089_Lam_90014152Image.pdf	4187869 993e9519e9aba965c63675a03af6808e38939526	no	42

Warnings:

Information:					
2	Foreign Reference	F031_WO9942996_1999-08-25_FukudaA.pdf	6299721 c277b4676920b7938a5fc0d55f96bb9d08cf651d	no	67
Warnings:					
Information:					
3	Foreign Reference	F032_JPH05334072Beetcher072A.pdf	2134423 db2f9a181f8b355edbdfbda4efbf919ab2d82a01	no	20
Warnings:					
Information:					
4	Foreign Reference	F033_WO1997043761_Intertrust.pdf	2682690 d7aae1d31b8e3617d0123fc6a9aa162887fe6ce4	no	209
Warnings:					
Information:					
5	Foreign Reference	F034_EP1028401_SchutzerA.pdf	2849115 88ff47b7572fac5c89e03c77e19d9d72d6e9b60a	no	19
Warnings:					
Information:					
6	Foreign Reference	F035_WO0014648_BrenerE.pdf	5923593 074472f9622a63bd48713c660194422fee76cded	no	35
Warnings:					
Information:					
7	Foreign Reference	F036_WO0113275_JundaE.pdf	6705954 ac00e2eebdabc2ad88451fce91e98ea5dd5743b2	no	40
Warnings:					
Information:					
8	Foreign Reference	F037_WO9743761X.pdf	1845949 628827fbe7fc959003d0685f3a3dedd64a8b19a3	no	209
Warnings:					
Information:					

9	Non Patent Literature	L257_Lacy_SCOT0016-5_7-21-2015.pdf	1991401 90bceadf0d7c3a59112f9a7268b8e1117218daef	no	7
Warnings:					
Information:					
10	Non Patent Literature	L258_Kohl_SCOT0016-5_7-21-2015.pdf	1109640 bbbbced4d6b6293555a5826ff3149dc326acf9db	no	6
Warnings:					
Information:					
11	Non Patent Literature	L259_Faber_SCOT0016-5_7-21-2015.pdf	1506800 00fd1cb84913bcd2196e84e103978dd4c6bda3d3	no	7
Warnings:					
Information:					
12	Non Patent Literature	L260_ORDERGrantingGoogles MJP.pdf	156810 2b118ee45494bfd0f463701a1364b4b494a48cc4	no	18
Warnings:					
Information:					
13	Non Patent Literature	L261_OrderDenyingRehearing.pdf	174377 8130b3a680f0ccff043532d60b65cc8fa607c8ea	no	2
Warnings:					
Information:					
14	Non Patent Literature	L262_SecureDelivery_IEEEXploreDocument.pdf	1953190 5745085f6cc59af29afbf7abe1d3a377747795ec	no	3
Warnings:					
Information:					
15	Non Patent Literature	L263_BlueSpike_v_Google_Judgment.pdf	919426 e0e9f8dae5205c102cc8d0d973e17c9b1a03e627	no	2
Warnings:					
Information:					

16	Non Patent Literature	L264_16_2223_DenialOfCert.pdf	2402953 b408ba998d20ed3c690fca3f08fee0231c88a153	no	17
Warnings:					
Information:					
17	Non Patent Literature	L265A_Augut_Image.pdf	3182963 4d0ee4a14bc58640b6174957b926ac433f047a13	no	16
Warnings:					
Information:					
18	Non Patent Literature	L265DeclarationofAnnaLysyanskayaReexam90014152I.pdf	6438314 d2a0ffd0a78e02a9df5f809571f29332e08e3a50	no	84
Warnings:					
Information:					
19	Non Patent Literature	L0266ProposedTermsforConstruction_reexam90014152I.pdf	2332953 332a0cce0f40ac1f27084080d8e86d03ac05039a	no	61
Warnings:					
Information:					
20	Non Patent Literature	L0267EnglishTranslationofJPH05334072_Beetcher072I.pdf	1918975 f6886b334a8395426698cf261555d30b75486b8d	no	19
Warnings:					
Information:					
21	Non Patent Literature	L0268DeclarationofClaudioSilva_reexam90014138Image.pdf	10101961 6549a5f06894d44dca5a6e72569a8a7f5aaa5343	no	166
Warnings:					
Information:					
22	Non Patent Literature	L0269DeclarationofClaudioSilva_reexam90014137Image.pdf	9880426 f776fdfc40995158a65be5cd8da7c93715e88867	no	120
Warnings:					
Information:					

23	Non Patent Literature	L0270IPR201701061_5745569_EX1003Image.pdf	2600166 f557ff8cf88cb86a2fd3d5f5eb6d746137aff16c	no	21
Warnings:					
Information:					
24	Non Patent Literature	L0271IPR201701061_5745569EX1004OstrovskyImage.pdf	5036986 e8d2cbf02dda2de0a84db087b214630882bd17ea	no	53
Warnings:					
Information:					
25	Non Patent Literature	L0272IPR201701061_5745569EX1006OstrovskyImage.pdf	1377794 a9ab30d27439ce3600826bc772f7dc53b888c11b	no	10
Warnings:					
Information:					
26	Non Patent Literature	L0273IPR201701061EX1007_OstrovskyDecImage.pdf	14876631 e338771cc9f5e3c50570b853123a46b21e60e32b	no	50
Warnings:					
Information:					
27	Non Patent Literature	L0274IPR201701061EX1008_MarkmanImage.pdf	3675753 9b1fad13d9aa76652daee846eb6126b6be6d856e	no	13
Warnings:					
Information:					
28	Non Patent Literature	L0275IPR201701109_EX1005Image.pdf	2211243 6f37ef3d34aa4bba631a16fdd859d2f84ea92fa1	no	11
Warnings:					
Information:					
29	Non Patent Literature	L0276IPR201701109_8930719_EX1008Image.pdf	12189328 b7a53dc7affcdc28cc32b2435fe9d44a0db72e74	no	71
Warnings:					
Information:					

30	Non Patent Literature	L0277RokuInitialInvalidityContentions.pdf	175656 6fa5363f647790972a9f826417cb2ca46936f778	no	50
Warnings:					
Information:					
31	Non Patent Literature	L0278_BS_v_Roku_RokuBatesNumbers00005564_5598l.pdf	2453549 62e9d86f5c7132e87949c241523fcfec43e2fd73	no	35
Warnings:					
Information:					
32	Non Patent Literature	L0279_BS_v_ROKU_RokuBatesNumbers00005948-5949.pdf	1127490 369369f467f623361d0292384d9ba90ccf111a82	no	2
Warnings:					
Information:					
33	Non Patent Literature	L0280_BS_Roku_RokuBatesNumbers00005952-5953.pdf	1094750 ec97aa568e58e9704e4ce6e47723d0ccc22c1b03	no	2
Warnings:					
Information:					
34	Non Patent Literature	L-0281_BS_v_Roku_RokuBatesNumber00005954.pdf	770981 d5e8804225b25e69a027f1e61a3243252ea94c6e	no	1
Warnings:					
Information:					
35	Non Patent Literature	L-0282_BS_v_Roku_RokuBatesNumber0005955-5956.pdf	895030 5a797f1ea5ae9b43e11578dee73ab137436fa81e	no	2
Warnings:					
Information:					
36	Non Patent Literature	L-0283_BS_v_Roku_RokuBatesNumber00005963.pdf	629304 f14dbe3f65964638c58366878ea0d008144fd80a	no	1
Warnings:					
Information:					

37	Non Patent Literature	L-0284_BS_v_Roku_RokuBates Number00005964-5965.pdf	860412 4d8ca2ed7d64b780c5c75528cfc43d8eccc5d507	no	2
Warnings:					
Information:					
38	Non Patent Literature	L-0285_BS_v_Roku_RokuBates Number00005966.pdf	635711 1d75094a3e06b509e6c76ad230589f4aee345bee	no	1
Warnings:					
Information:					
39	Non Patent Literature	L-0286_BS_v_Roku_RokuBates Number00005967.pdf	1764984 d32f1db6c38af9f391e7db5bcba731223da5155c	no	8
Warnings:					
Information:					
40	Non Patent Literature	L-0287_BS_v_Roku_RokuBates Number00005520-5521.pdf	752619 665199aab1b567dce3f6dab46e1865180ce0bd2c	no	2
Warnings:					
Information:					
41	Non Patent Literature	L-0288_BS_v_Roku_RokuBates Number00005957-5958.pdf	799952 3d5d2320a354ffac41ef4c9e30ab50fce99918b5	no	2
Warnings:					
Information:					
42	Non Patent Literature	L-0289_BS_v_Roku_RokuBates Number00005961-5962.pdf	794365 e2e5fa7e3364626454 7e2c62f56497d2f734a74c	no	2
Warnings:					
Information:					
43	Non Patent Literature	L-0290_BS_v_Roku_RokuBates Number00005959-5960.pdf	767153 f85197e176422192bf9eb50f29d2853e7bf43e59	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	132189360		

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.

Electronic Acknowledgement Receipt

EFS ID:	35195398
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-FEB-2019
Filing Date:	16-MAY-2018
Time Stamp:	20:10:29
Application Type:	Reexam (Third Party)

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	Non Patent Literature	L-0291_BS_v_Roku_RokuBates Number00005950-5951.pdf	1026764 2f4adfb91178fc981cc03227dbf9f6215390d844	no	2

Warnings:

Information:					
2	Non Patent Literature	L-0292_BS_v_Roku_RokuBatesNumber00005954.pdf	771346 c06114c8258462720278ccceddea798fcbf7b26b	no	1
Warnings:					
Information:					
3	Non Patent Literature	L-0293_BS_v_Roku_RokuBatesNumber00005773-5774.pdf	1245051 72954a80241149f6b0785626e862c7f961ea583a	no	2
Warnings:					
Information:					
4	Non Patent Literature	L-0294_RokuPriorArtIndexLetter_Marked_Image.pdf	909029 34a84be069fed4a99733b7d740e0f3acd16714f5	no	6
Warnings:					
Information:					
5	Non Patent Literature	L-0295_ROKU5516-7_Guglielmo.pdf	635342 8892dbbca1fc19c2a1f14f94a25b6f75ece22704	no	2
Warnings:					
Information:					
6	Non Patent Literature	L-0296_ROKU5518-19_Boscardin.pdf	611001 1bc5cd4da1ef096d43080ba58e0791ea8ae09144	no	2
Warnings:					
Information:					
7	Non Patent Literature	L-0297_ROKU_5520-5521_ContentGuard.pdf	581578 65a7d67094829419c70978366df9f6011f6d4d6d	no	2
Warnings:					
Information:					
8	Non Patent Literature	L-0298_ROKU5538-40_PictureMark.pdf	700177 2d693dc7a304edde10245a8e504d70eaa4904190	no	3
Warnings:					
Information:					

9	Non Patent Literature	L-0299_ROKU5660-62.pdf	654224 be4db16e418535d2692ba7d29b0652c78179a568	no	3
Warnings:					
Information:					
10	Non Patent Literature	L-0300_ROKU5967-74_Giles.pdf	824103 d6cb5b4d1d48e68ec5b11deefd025a8df7d2b019	no	8
Warnings:					
Information:					
		Total Files Size (in bytes):	7958615		

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.

Electronic Acknowledgement Receipt

EFS ID:	35195761
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-FEB-2019
Filing Date:	16-MAY-2018
Time Stamp:	20:59:03
Application Type:	Reexam (Third Party)

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	Non Patent Literature	L-301A.pdf	5830023 b4a4a72b8ebe8d43dd17da9e447f3bd87fe21a6e	no	661

Warnings:

Information:					
2	Non Patent Literature	L-301B.pdf	6699265 bfb1d2497c91478c073e92c56191b863139afa8f	no	707
Warnings:					
Information:					
3	Non Patent Literature	L-301C.pdf	3668678 2e950b3280a0bee47d661d8d5f64963c15fdd7fd	no	345
Warnings:					
Information:					
4	Non Patent Literature	L-301D.pdf	4791569 ca2b8ba5cb29ba68e9351f88b926244addf60588	no	416
Warnings:					
Information:					
5	Non Patent Literature	L-301E.pdf	1974041 04f57762df30cfaf143dc163e596a415337a3d17	no	164
Warnings:					
Information:					
6	Non Patent Literature	L-302_aucsmith.PDF	251223 67f81cfe65654e3b03263e5e48494dbb9efe927b	no	17
Warnings:					
Information:					
7	Non Patent Literature	L-303_CreatingMulti-DRME.pdf	109240 ff37098e1636f0044bd1e0262c49620bb3f92a93	no	5
Warnings:					
Information:					
8	Non Patent Literature	L-304_DiffieHellmanE.pdf	10647007 bdc54f16a97c725302b2d971810d474a1ca8b97b	no	11
Warnings:					
Information:					

9	Non Patent Literature	L-305_DIVXE.pdf	56609 46b9bc303f40b1c4693f1fbd4860292baf673e2d	no	4
Warnings:					
Information:					
10	Non Patent Literature	L-306_ElectronicWaterMarkE.pdf	1617408 da7052a8b822fb96d5e9ecd3d3754227c47bd6bd	no	9
Warnings:					
Information:					
11	Non Patent Literature	L-307_FirstOpenEE.pdf	149923 63bf413a9d0fa0166c651d111a639f5b2ccd6f1e	no	8
Warnings:					
Information:					
12	Non Patent Literature	L-308_WasAppleE.pdf	319022 95229a24e0c57c69229c21d33acc409a3dd83ebb	no	10
Warnings:					
Information:					
13	Non Patent Literature	L-309_SurvivingE.pdf	66623 8892d70ca61db5e145cd5d435331a21253d97d2b	no	21
Warnings:					
Information:					
14	Non Patent Literature	L-310_TestingI.pdf	1119307 b334a65c82b1563418e29910f0a5386833b66bc9	no	19
Warnings:					
Information:					
15	Non Patent Literature	L-311_InformationHidingE.pdf	404833 9085ccdb3c699368de055b0093aa9704e75b62ad	no	17
Warnings:					
Information:					

16	Non Patent Literature	L-312_OnSoftwareProtection.pdf	891856 876bd957ae0e76bf8290b046c9b7300f66b02999	no	12
Warnings:					
Information:					
17	Non Patent Literature	L-313_ContinuousSteganographicE.pdf	288131 8f0eb4c8e31083e642622b4ae2c620e7e3ec4bfe	no	10
Warnings:					
Information:					
18	Non Patent Literature	L-314_Music.pdf	508565 c8756a76401e4bc495006c1fa9bbe5ffb19f9b87	no	3
Warnings:					
Information:					
19	Non Patent Literature	L-315_MicrosoftUnveilsE.pdf	41220 73a2a2760075913d5b896d03e6038fa06dbaf5eb	no	4
Warnings:					
Information:					
20	Non Patent Literature	L-316_Marlin.pdf	393715 17382e6386b6a010ec5eeddc3bd1427a7d911461	no	3
Warnings:					
Information:					
21	Non Patent Literature	L-317_MarlinDRM.pdf	122134 90e9aa08db64f6543c35ea5600a44081b001b7f3	no	2
Warnings:					
Information:					
22	Non Patent Literature	L-318_LinaroClear.pdf	1483422 32cdf03836dbb14bd485b3c70fd2e9faf863725b	no	13
Warnings:					
Information:					

23	Non Patent Literature	L-319_LegacyWindowsE.pdf	32534 c732528b5498ae8d5f7ec291a36c64694a5b0fdd	no	3
Warnings:					
Information:					
24	Non Patent Literature	L-320_Unlocking.pdf	260540 2d48eb2ae24e76e2c7f65dd33b258fbfeb58aa99	no	3
Warnings:					
Information:					
25	Non Patent Literature	L-321_Exploring.pdf	249559 6ab2f00dcbe7ecac475771b95c81bbda640d2eaa	no	4
Warnings:					
Information:					
26	Non Patent Literature	L-322_IntellectualProperty.pdf	867120 056678825f46c4689a025d9a67871aeacad275d8	no	14
Warnings:					
Information:					
27	Non Patent Literature	L-323_TheIncredibly.pdf	1161294 d1136e922d454427f1cee9e4aa79607c0f44308d	no	19
Warnings:					
Information:					
28	Non Patent Literature	L-324_RobustI.pdf	2261290 f39a35f1d680a3df1c55aa7b7513c6e6b1ded0de	no	15
Warnings:					
Information:					
		Total Files Size (in bytes):	46266151		

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.

Reexamination Control Number: 90014138
Confirmation No: 7638
RE: Reexamination of USP 9104842

Patent Owner Information Disclosure Statement

Submitted herewith:
This IDS
Reference citation list, listing references U1 to U480; P1 to P102; F1 to F37; and L1 to L324.
References: F30 to F37; and L257 to L324.
Certificate of Service attesting to service of the foregoing on the requestor.

Gov. fees: 806/2806/3806 1.17(p) Submission of IDS $240.00

/RichardNeifeld/
Richard Neifeld, Reg. No. 35,299
Attorney for patent owner

REMARKS

This is an Information Disclosure Statement (IDS).

The applicant has maintained a list of all references cited in all of the applications owned by or owned by entities controlled by Scott Moskowitz.

The IDS filed 3-20-2015 in the application (11895388) that issued into the USP9104842 shows that references U1 to U406; P01 to P98; F01 to F29; and L1 to L256 were cited during original prosecution.

The applicant's current list cites: U-1 to U480; P1 to P102; F1 to F37; and L1 to L324.

Accordingly, the applicant is presenting the updated reference citation list. The references cited in this list that were not made of record in original prosecution of the patent are: U407 to U480; P99 to P102; F30 to F37; and L257 to L324.

Accordingly, the applicant is providing copies of the references that are not US patent application publications or US patents. These references are F30 to F37; and L257 to L324.

Please note the following.

New reference L301 is an expert report in support of Vizio in an ongoing litigation.

The patentee is paying the IDS fee of $240 when filing this IDS.

The patentee is serving the reexamination requestor prior to filing this IDS.

/RichardNeifeld/
Richard Neifeld, Reg. No. 35,299
Attorney for patent owner

Reexamination Control Number: 90014138
Confirmation No: 7638
RE: Reexamination of USP 9104842

37 CFR 1.248 Certificate of Service

I served by first class mail (priority mail):

In paper:
(1) Patent Owner Information Disclosure Statement
(2) The current reference citation list;
(3) This Certificate of Service

Stored on a portable USB drive:
(4) Pdf copies of the aforementioned paper documents and pdf copies of referencesF30 to F37; and L257 to L324;

on the third parte reexamination requestor at his correspondence address:

Attn: Joseph P. Edell
FISCH SIGLER LLP
5301 WISCONSIN AVENUE, NW
FOURTH FLOOR
WASHINGTON, DC 20015

Date of Service: 2-18-2019

/RichardNeifeld/
Richard Neifeld, Reg. No. 35,299
Attorney for patent owner

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF UNITED STATES PATENTS - U series

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 01	3947825	March 1976	Cassada	X
	U 02	3984624	October 1976	Waggener	X
	U 03	3986624	October 1976	Cates, Jr. et al.	X
	U 04	4038596	July 1977	Lee	X
	U 05	4200770	April 1980	Hellman et al.	X
	U 06	4218582	August 1980	Hellman et al.	X
	U 07	4339134	July 1982	Macheel	X
	U 08	4390898	June 1983	Bond et al.	X
	U 09	4405829	September 1983	Rivest et al.	X
	U 010	4424414	January 1984	Hellman et al.	X
	U 011	4528588	July 1985	Lofberg	X
	U 012	4672605	June 1987	Hustig et al.	X
	U 013	4748668	May 1988	Shamir et al.	X
	U 014	4789928	December 1988	Fujisaki	X
	U 015	4827508	May 1989	Shear	X
	U 016	4876617	October 1989	Best et al.	X
	U 017	4896275	January 1990	Jackson	X
	U 018	4908873	March 1990	Philibert et al.	X
	U 019	4939515	July 1990	Adelson	X
	U 020	4969204	November 1990	Melnychuk et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 021	4972471	November 1990	Gross et al.	X
	U 022	4977594	December 1990	Shear	X
	U 023	4979210	December 1990	Nagata et al.	X
	U 024	4980782	December 1990	Ginkel	X
	U 025	5050213	September 1991	Shear	X
	U 026	5073925	December 1991	Nagata et al.	X
	U 027	5077665	December 1991	Silverman et al.	X
	U 028	5113437	May 1992	Best et al.	X
	U 029	5136581	August 1992	Muehrcke	X
	U 030	5136646	August 1992	Haber et al.	X
	U 031	5136647	August 1992	Haber et al.	X
	U 032	5142576	August 1992	Nadan	X
	U 033	5161210	November 1992	Druyvesteyn et al.	X
	U 034	5210820	May 1993	Kenyon	X
	U 035	5243423	September 1993	DeJean et al.	X
	U 036	5243515	September 1993	Lee	X
	U 037	5287407	February 1994	Holmes	X
	U 038	5319735	June 1994	Preuss et al.	X
	U 039	5341429	August 1994	Stringer et al.	X
	U 040	5341477	August 1994	Pitkin et al.	X
	U 041	5363448	November 1994	Koopman et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 042	5365586	November 1994	Indeck et al.	X
	U 043	5369707	November 1994	Follendore, III	X
	U 044	5379345	January 1995	Greenberg	X
	U 045	5394324	February 1995	Clearwater	X
	U 046	5398285	March 1995	Borgelt et al.	X
	U 047	5406627	April 1995	Thompson et al.	X
	U 048	5408505	April 1995	Indeck et al.	X
	U 049	5410598	April 1995	Shear	X
	U 050	5412718	May 1995	Narasimhalv et al.	X
	U 051	5418713	May 1995	Allen	X
	U 052	5428606	June 1995	Moskowitz	X
	U 053	5450490	September 1995	Jensen et al.	X
	U 054	5469536	November 1995	Blank	X
	U 055	5471533	November 1995	Wang et al.	X
	U 056	5478990	December 1995	Montanari et al.	X
	U 057	5479210	December 1995	Cawley et al.	X
	U 058	5487168	January 1996	Geiner et al.	X
	U 059	5493677	February 1996	Balogh et al.	X
	U 060	5497419	March 1996	Hill	X
	U 061	5506795	April 1996	Yamakawa	X
	U 062	5513126	April 1996	Harkins et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 063	5513261	April 1996	Maher	X
	U 064	5530739	June 1996	Okada	X
	U 065	5530751	June 1996	Morris	X
	U 066	5530759	June 1996	Braudaway et al.	X
	U 067	5539735	July 1996	Moskowitz	X
	U 068	5548579	August 1996	Lebrun et al.	X
	U 069	5568570	October 1996	Rabbani	X
	U 070	5579124	November 1996	Aijala et al.	X
	U 071	5581703	December 1996	Baugher et al.	X
	U 072	5583488	December 1996	Sala et al.	X
	U 073	5598470	January 1997	Cooper et al.	X
	U 074	5606609	February 1997	Houser et al.	X
	U 075	5613004	March 1997	Cooperman et al.	X
	U 076	5617119	April 1997	Briggs et al.	X
	U 077	5625690	April 1997	Michel et al.	X
	U 078	5629980	May 1997	Stefik et al.	X
	U 079	5633932	May 1997	Davis et al.	XX
	U 080	5634040	May 1997	Her et al.	X
	U 081	5636276	June 1997	Brugger	X
	U 082	5636292	June 1997	Rhoads	X
	U 083	5640569	June 1997	Miller et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 084	5646997	July 1997	Barton	X
	U 085	5657461	August 1997	Harkins et al.	X
	U 086	5659726	August 1997	Sandford, II et al.	X
	U 087	5664018	September 1997	Leighton	X
	U 088	5673316	September 1997	Auerbach et al.	X
	U 089	5677952	October 1997	Blakely et al.	X
	U 090	5680462	October 1997	Miller et al.	X
	U 091	5687236	November 1997	Moskowitz et al.	X
	U 092	5689587	November 1997	Bender et al.	X
	U 093	5696828	December 1997	Koopman, Jr.	X
	U 094	5719937	February 1998	Warren et al.	X
	U 095	5721788	February 1998	Powell et al.	X
	U 096	5734752	March 1998	Knox	X
	U 097	5737416	April 1998	Cooper et al.	X
	U 098	5737733	April 1998	Eller	X
	U 099	5740244	April 1998	Indeck et al.	X
	U 0100	5745569	April 1998	Moskowitz et al.	X
	U 0101	5748783	May 1998	Rhoads	X
	U 0102	5751811	May 1998	Magnotti et al.	X
	U 0103	5754697	May 1998	Fu et al.	X
	U 0104	5757923	May 1998	Koopman, Jr.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0105	5765152	June 1998	Erickson	X
	U 0106	5768396	June 1998	Sone	X
	U 0107	5774452	June 1998	Wolosewicz	X
	U 0108	5790677	August 1998	Fox et al.	X
	U 0109	5799083	August 1998	Brothers et al.	X
	U 0110	5809139	September 1998	Grirod et al.	X
	U 0111	5809160	September 1998	Powell et al.	X
	U 0112	5822432	October 1998	Moskowitz et al.	X
	U 0113	5828325	October 1998	Wolosewicz et al.	X
	U 0114	5832119	November 1998	Rhoads	X
	U 0115	5848155	December 1998	Cox	X
	U 0116	5850481	December 1998	Rhoads	X
	U 0117	5859920	January 1999	Daly et al.	X
	U 0118	5860099	January 1999	Milios et al.	X
	U 0119	5862260	January 1999	Rhoads	X
	U 0120	5870474	February 1999	Wasilewski et al.	X
	U 0121	5884033	March 1999	Duvall et al.	X
	U 0122	5889868	March 1999	Moskowitz et al.	X
	U 0123	5893067	April 1999	Bender et al.	X
	U 0124	5894521	April 1999	Conley	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0125	5903721	May 1999	Sixtus	X
	U 0126	5905800	May 1999	Moskowitz et al.	X
	U 0127	5905975	May 1999	Ausubel	X
	U 0128	5912972	June 1999	Barton	X
	U 0129	5915027	June 1999	Cox et al.	X
	U 0130	5917915	June 1999	Hirose	X
	U 0131	5918223	June 1999	Blum	X
	U 0132	5920900	July 1999	Poole et al.	X
	U 0133	5923763	July 1999	Walker et al.	X
	U 0134	5930369	July 1999	Cox et al.	X
	U 0135	5930377	July 1999	Powell et al	. X
	U 0136	5940134	August 1999	Wirtz	X
	U 0137	5943422	August 1999	Van Wie et al.	X
	U 0138	5963909	October 1999	Warren et al.	X
	U 0139	5973731	October 1999	Schwab	X
	U 0140	5974141	October 1999	Saito	X
	U 0141	5991426	November 1999	Cox et al.	X
	U 0142	5999217	December 1999	Berners-Lee	X
	U 0143	6009176	December 1999	Gennaro et al.	X
	U 0144	6029126	February 2000	Malvar	X
	U 0145	6041316	March 2000	Allen	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0146	6044471	March 2000	Colvin	X
	U 0147	6049838	April 2000	Miller et al.	X
	U 0148	6051029	April 2000	Paterson et al.	X
	U 0149	6061793	May 2000	Tewfik et al.	X
	U 0150	6069914	May 2000	Cox	X
	U 0151	6078664	June 2000	Moskowitz et al.	X
	U 0152	6081251	June 2000	Sakai et al.	X
	U 0153	6081587	June 2000	Reyes et al.	X
	U 0154	6088455	July 2000	Logan et al.	X
	U 0155	6131162	October 2000	Yoshiura et al.	X
	U 0156	6141753	October 2000	Zhao et al.	X
	U 0157	6141754	October 2000	Choy	X
	U 0158	6154571	November 2000	Cox et al.	X
	U 0159	6192138	February 2001	Yamadaji	X
	U 0160	6199058	March 2001	Wong et al.	X
	U 0161	6205249	March 2001	Moskowitz	X
	U 0162	6208745	March 2001	Florenio et al.	X
	U 0163	6230268	May 2001	Miwa et al.	X
	U 0164	6233347	May 2001	Chen et al.	X
	U 0165	6233684	May 2001	Stefik et al.	X
	U 0166	6240121	May 2001	Senoh	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0167	6263313	July 2001	Milstead et al.	X
	U 0168	6272634	August 2001	Tewfik et al.	X
	U 0169	6275988	August 2001	Nagashima et al.	X
	U 0170	6278780	August 2001	Shimada	X
	U 0171	6278791	August 2001	Honsinger et al.	X
	U 0172	6282300	August 2001	Bloom et al.	X
	U 0173	6282650	August 2001	Davis	X
	U 0174	6285775	September 2001	Wu et al.	X
	U 0175	6301663	October 2001	Kato et al.	X
	U 0176	6310962	October 2001	Chung et al.	X
	U 0177	6330335	December 2001	Rhoads	X
	U 0178	6330672	December 2001	Shur	X
	U 0179	6345100	February 2002	Levine	X
	U 0180	6351765	February 2002	Pietropaolo et al.	X
	U 0181	6363483	March 2002	Keshav	X
	U 0182	6373892	April 2002	Ichien et al.	X
	U 0183	6373960	April 2002	Conover et al.	X
	U 0184	6374036	April 2002	Ryan et al.	X
	U 0185	6377625	April 2002	Kim	X
	U 0186	6381618	April 2002	Jones et al.	X
	U 0187	6381747	April 2002	Wonfor et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0188	6385329	May 2002	Sharma et al.	X
	U 0189	6389538	May 2002	Gruse et al.	X
	U 0190	6405203	June 2002	Collart	X
	U 0191	6415041	July 2002	Oami et al.	X
	U 0192	6425081	July 2002	Iwamura	X
	U 0193	6430301	August 2002	Petrovic	X
	U 0194	6430302	August 2002	Rhoads	X
	U 0195	6442283	August 2002	Tewfik et al.	X
	U 0196	6446211	September 2002	Colvin	X
	U 0197	6453252	September 2002	Laroche	X
	U 0198	6457058	September 2002	Ullum et al.	X
	U 0199	6463468	October 2002	Buch et al.	X
	U 0200	6484264	November 2002	Colvin	X
	U 0201	6493457	December 2002	Quackenbush	X
	U 0202	6502195	December 2002	Colvin	X
	U 0203	6522767	February 2003	Moskowitz et al.	X
	U 0204	6522769	February 2003	Rhoads et al.	X
	U 0205	6523113	February 2003	Wehrenberg	X
	U 0206	6530021	March 2003	Epstein et al.	X
	U 0207	6532284	March 2003	Walker et al.	X
	U 0208	6539475	March 2003	Cox et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0209	6557103	April 2003	Boncelet, Jr. et al.	X
	U 0210	6584125	June 2003	Katto	X
	U 0211	6587837	July 2003	Spagna et al.	X
	U 0212	6598162	July 2003	Moskowitz	X
	U 0213	6606393	August 2003	Xie et al.	X
	U 0214	6647424	November 2003	Pearson et al.	X
	U 0215	6658010	December 2003	Enns et al.	X
	U 0216	6665489	December 2003	Collart	X
	U 0217	6668246	December 2003	Yeung et al.	X
	U 0218	6668325	December 2003	Collberg et al	. X
	U 0219	6687683	February 2004	Harada et al.	X
	U 0220	6725372	April 2004	Lewis et al	. X
	U 0221	6754822	June 2004	Zhao	X
	U 0222	6775772	August 2004	Binding et al.	X
	U 0223	6784354	August 2004	Lu et al.	X
	U 0224	6785815	August 2004	Serret-Avila et al.	X
	U 0225	6785825	August 2004	Colvin	X
	U 0226	6792548	September 2004	Colvin	X
	U 0227	6792549	September 2004	Colvin	X
	U 0228	6795925	September 2004	Colvin	X
	U 0229	6799277	September 2004	Colvin	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0230	6813717	November 2004	Colvin	X
	U 0231	6813718	November 2004	Colvin	X
	U 0232	6823455	November 2004	Macy et al.	X
	U 0233	6834308	December 2004	Ikezoye et al.	X
	U 0234	6842862	January 2005	Chow et al.	X
	U 0235	6853726	February 2005	Moskowitz et al.	X
	U 0236	6857078	February 2005	Colvin	X
	U 0237	6931534	August 2005	Jandel et al.	X
	U 0238	6966002	November 2005	Torrubia-Saez	X
	U 0239	6983337	November 2005	Wold	X
	U 0240	6977894	December 2005	Achilles et al.	X
	U 0241	6978370	December 2005	Kocher	X
	U 0242	6986063	January 2006	Colvin	X
	U 0243	7007166	February 2006	Moskowitz et al.	X
	U 0244	7020285	March 2006	Kirovski et al.	X
	U 0245	7035409	April 2006	Moskowitz	X
	U 0246	7043050	May 2006	Yuval	X
	U 0247	7046808	May 2006	Metois et al.	X
	U 0248	7050396	May 2006	Cohen et al.	X
	U 0249	7051208	May 2006	Venkatesan et al.	X
	U 0250	7058570	June 2006	Yu et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0251	7093295	August 2006	Saito	X
	U 0252	7095874	August 2006	Moskowitz et al	. X
	U 0253	7103184	September 2006	Jian	X
	U 0254	7107451	September 2006	Moskowitz	X
	U 0255	7123718	October 2006	Moskowitz et al.	X
	U 0256	7127615	October 2006	Moskowitz	X
	U 0257	7150003	December 2006	Naumovich et al.	X
	U 0258	7152162	December 2006	Moskowitz et al.	X
	U 0259	7159116	January 2007	Moskowitz	X
	U 0260	7162642	January 2007	Schumann et al.	X
	U 0261	7177429	February 2007	Moskowitz et al.	X
	U 0262	7177430	February 2007	Kim	X
	U 0263	7206649	April 2007	Kirovski et al.	X
	U 0264	7231524	June 2007	Bums	X
	U 0265	7233669.	June 2007	Candelore	X
	U 0266	7240210	July 2007	Michak et al.	X
	U 0267	7266697	September 2007	Kirovski et al	. X
	U 0268	7287275	October 2007	Moskowitz	X
	U 0269	7289643	October 2007	Brunk et al.	X
	U 0270	7343492	March 2008	Moskowitz et al.	X
	U 0271	7346472	March 2008	Moskowitz et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0272	7362775	April 2008	Moskowitz	X
	U 0273	7363278	April 2008	Schmelzer et al.	X
	U 0274	7409073	August 2008	Moskowitz et al.	X
	U 0275	7457962	November 2008	Moskowitz	X
	U 0276	7460994	December 2008	Herre et al.	X
	U 0277	7475246	January 2009	Moskowitz	X
	U 0278	7530102	May 2009	Moskowitz	X
	U 0279	7532725	May 2009	Moskowitz et al.	X
	U 0280	7568100	July 2009	Moskowitz et al.	X
	U 0281	7647502	January 2010	Moskowitz	X
	U 0282	7647503	January 2010	Moskowitz	X
	U 0283	7779261	August 2010	Moskowitz	X
	U 0284	6990453	January 2006	Wang	X
	U 0285	6081597	June 2000	Hoffstein	X
	U 0286	7035049	Apr 2006	Yamamoto	X
	U 0287	7664263	Feb 2010	Moskowitz	X
	U 0288	7286451	Oct 2007	Wirtz	X
	U 0289	6385324	May 2002	Koppen	X
	U 0290	6674858	Jan 2004	Kimura	X
	U 0291	6148333	Nov 2000	Guedalia	X
	U 0292	6418421	Jun 2002	Hurtado	X

DATE:	EXAMINER'S SIGNATURE:

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0293	6385596	May 2002	Wiser	X
	U 0294	6226618	May 2001	Downs	X
	U 0295	6957330	Oct 2005	Hughes	X
	U 0296	5842213	Nov 1998	Odom	X
	U 0297	5818818	Oct 1998	Soumiya	X
	U 0298	6590996	Jun 2003	Reed	X
	U 0299	5949055	Sept 1999	Fleet	X
	U 0300	6067622	May 2000	Moore	X
	U 0301	7761712	Jun 2010	Moskowitz	X
	U 0302	7743001	Jun 2010	Vermeulen	X
	U 0303	6865747	Mar 2005	Mercier	X
	U 0304	6611599	Aug 2003	Natarajan	X
	U 0305	6480937	Nov 2002	Vorbach	X
	U 0306	6398245	Jun 2002	Gruse	X
	U 0307	6950941	Sept 2005	Lee	X
	U 0308	6983058	Jan 2006	Fukuoka	X
	U 0309	5675653	Oct 1997	Nelson	X
	U 0310	6804453	Oct 2004	Sasamoto	X
	U 0311	6178405	Jan 2001	Ouyang	X
	U 0312	5839100	Nov 1998	Wegener	X
	U 0313	5781184	Jul 1998	Wasserman	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0314	5617506	Apr 1997	Burk	X
	U 0315	5327520	Jul 1994	Chen	X
	U 0316	5111530	May 1992	Kutaragi	X
	U 0317	7095715	Aug 2006	Buckman	X
	U 0318	6173322	Jan 2001	Hu	X
	U 0319	5754938	May 1998	Herz	X
	U 0320	6035398	Mar 2000	Bjorn	X
	U 0321	5901178	May 1999	Lee	X
	U 0322	8214175	July 2012	Moskowitz	X
	U 0323	8265278	Sept 2012	Moskowitz	X
	U 0324	8161286	Nov 2010	Moskowitz	X
	U 0325	8307213	Jan 2011	Moskowitz	X
	U 0326	8121343	May 2012	Moskowitz	X
	U 0327	5437050	Jul 1995	Lamb	X
	U 0328	5123045	Jun 1992	Ostrovsky	X
	U 0329	7310815	Dec 2007	Yanovsky	X
	U 0330	8179846	May 2012	Dolganow	X
	U 0331	7719966	May 2010	Luft	X
	U 0332	7630379	Dec 2009	Morishita	X
	U 0333	5949973	Sept 1999	Yarom	X
	U 0334	8400566	Mar. 2013	Terry	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0335	5649284	July 1997	Yoshinobu	X
	U 0336	7444506	Oct 2008	Datta	X
	U 0337	6480963	Oct 2002	Tachibana	X
	U 0338	6510513	Jan 2003	Darrow	X
	U 0339	5189411	Feb 1993	Collar	X
	U 0340	5293633	Mar 1994	Robbins	X
	U 0341	4633462	Dec 1986	Stifle	X
	U 0342	5103461	Mar 1992	Cain	X
	U 0343	6272535	Aug 2001	Iwamura	X
	U 0344	6029195	Feb 2000	Herz	X
	U 0345	8095949	Jan 2012	Hendricks	X
	U 0346	5297032	Mar 1994	Trojan	X
	U 0347	5644727	Jul 1997	Atkins	X
	U 0348	5721781	Feb 1998	Deo	X
	U 0349	5822436	Oct 1998	Rhoads	X
	U 0350	5845266	Dec 1998	Lupien	X
	U 0351	5864827	Jan 1999	Wilson	X
	U 0352	5875437	Feb 1999	Atkins	X
	U 0353	5892900	Apr 1999	Ginter	X
	U 0354	6108722	Aug 2000	Troeller	X
	U 0355	6029146	Feb 2000	Hawkins	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0356	6032957	Mar 2000	Kiyosaki	X
	U 0357	6134535	Oct 2000	Belzberg	X
	U 0358	6185683	Feb 2001	Ginter	X
	U 0359	6233566	May 2001	Levine	X
	U 0360	6253193	Jun 2001	Ginter	X
	U 0361	6272474	Aug 2001	Garcia	X
	U 0362	6317728	Nov 2001	Kane	X
	U 0363	6363488	Mar 2002	Ginter	X
	U 0364	6389402	May 2002	Ginter	X
	U 0365	6427140	Jul 2002	Ginter	X
	U 0366	6484153	Nov 2002	Walker	X
	U 0367	6556976	Aug 1987	Callen	X
	U 0368	6574608	Jun 2003	Dahod	X
	U 0369	6601044	Jul 2003	Wallman	X
	U 0370	6594643	Jul 2003	Freeny	X
	U 0371	6618188	Sep 2003	Haga	X
	U 0372	6778968	Aug 2004	Gulati	X
	U 0373	6839686	Jan 2005	Galant	X
	U 0374	6856867	Feb 2005	Woolston	X
	U 0375	6876982	Apr 2005	Lancaster	X
	U 0376	7003480	Feb 2006	Fox	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0377	5822436	Oct 1998	Rhoads	X
	U 0378	6324649	Nov 2001	Eyres	X
	U 0379	5375055	Dec 1994	Togher	X
	U 0380	6018722	Jan 2000	Ray	X
	U 0381	6138239	Oct 2000	Veil	X
	U 0382	6484153	Nov 2002	Walker	X
	U 0383	6615188	Aug 2004	Breen	X
	U 0384	6856967	Jan 2005	Woolston	X
	U 0385	5790783	Aug 1998	Lee	X
	U 0386	6650761	Nov 2003	Rodriguez	X
	U 0387	6735702	May 2004	Yavatkar	X
	U 0388	6792424	Sept 2004	Burns	X
	U 0389	4790564	Dec 1988	Larcher	X
	U 0390	6111517	Aug 2000	Atick	X
	U 0391	5164992	Nov 1992	Turk	X
	U 0392	6674877	Jan 2004	Jojie	X
	U 0393	5291560	Mar 1994	Daugman	X
	U 0394	8492633	Jul 2013	Ellis	X
	U 0395	7672838	Mar 2010	Ellis	X
	U 0396	7254538	Aug 2007	Ellis	X
	U 0397	7812241	Oct 2010	Ellis	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0398	7672916	Mar 2010	Poliner	X
	U 0399	5991431	Nov 1999	Borza	X
	U 0400	4529870	Jul 1985	Chaum	X
	U 0401	6704451	Mar 2004	Hekstra	X
	U 0402	6532298	Mar 2003	Cambier	X
	U 0403	8949619	Feb 2015	Parry	X
	U 0404	4855584	Aug 1989	Tomiyama	X
	U 0405	4749354	Jun 1988	Kerman	X
	U 0406	5570339	Oct 1996	Nagano	X
	U 0407	6128735	Oct 2000	Goldstein	
	U 0408	7672317	Mar 2010	Gateva	
	U 0409	6389403	May 2002	Dorak	
	U 0410	7233948	Jun 2007	Shamoon	
	U 0411	8428185	Apr 2013	Driessen	
	U 0412	8095794	Jan 2012	Johnston	
	U 0413	8041038	Oct 2011	Lacy	
	U 0414	7802101	Sept 2010	Johnston	
	U 0415	7725808	May 2010	Johnston	
	U 0416	7529941	May 2009	Johnston	
	U 0417	7492902	Feb 2009	Lacy	
	U 0418	7451319	Nov 2008	Johnston	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0419	7353447	Nov 2008	Johnston	
	U 0420	7146503	Dec 2006	Johnston	
	U 0421	7131007	Oct 2006	Johnston	
	U 0422	7076426	Jul 2006	Buetnagel	
	U 0423	7042933	May 2006	Driessen	
	U 0424	6885749	Apr 2005	Chang	
	U 0425	6850559	Feb 2005	Driessen	
	U 0426	6760443	Jul 2004	Lacy	
	U 0427	6718507	Apr 2004	Johnston	
	U 0428	6704576	May 2004	Brachman	
	U 0429	6493457	Dec 2002	Quackenbush	
	U 0430	6341165	Jan 2002	Gbur	
	U 0431	6266419	Jul 2001	Lacy	
	U 0432	5825976	Oct 1998	Dorward	
	U 0433	5463641	Oct 1995	Dorward	
	U 434	6345389	Feb 2002	Dureau	
	U 435	7028327	Apr 2006	Dougherty	
	U 436	7725720	May 2010	Moreillon	
	U 437	6154172	Nov 2000	Piccionelli	
	U 438	6233736	May 2001	Wolzien	
	U 439	7020888	Mar 2006	Reynolds	

DATE:	EXAMINER'S SIGNATURE:

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 440	7028327	Apr 2006	Dougherty	
	U 441	7055169	May 2006	Delpuch	
	U 442	7421729	Sept 2008	Zenoni	
	U 443	7950033	May 2011	Pierre	
	U 444	7996861	Aug 2011	Delpuch	
	U 445	7251825	Jul 2007	Collet	
	U 446	7725740	May 2010	Kudelski	
	U 447	8356188	Jan 2013	Kudelski	
	U 448	RE40334	May 2008	Maillard	
	U449	7945781	May 2011	Rhoads	
	U450	8095796	Jan 2012	Conwell	
	U451	9934408	Apr 2018	Moskowitz	
	U452	6687375	Feb 2004	Matyas	
	U453	6469239	Oct 2002	Fukuda	
	U454	5933497	Aug 1999	Beetcher	
	U455	5935243	Aug 1999	Hasebe	
	U456	5982892	Nov 1999	Hicks	
	U457	5745604	Apr 1998	Rhoads	
	U458	6236971	May 2002	Stefik	
	U459	7263497	Aug 2007	Wiser	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U460	6552127	Apr 2003	Kurowski	
	U461	6952774	Oct 2005	Kirovski	
	U462	6122403	Sep 2000	Rhoads	
	U463	6513118	Jan 2003	Iwamura	
	U464	7103574	Sep 2006	Peinado	
	U465	6678465	Jan 2004	Swan	
	U466	6898706	May 2005	Venkatesan	
	U467	6959288	Oct 2005	Medina	
	U468	5109437	Apr 1992	Honda	
	U469	6128626	Oct 2000	Beauchesne	
	U470	5995630	Nov 1999	Borza	
	U471	6,434,238	Aug 2002	Chaum	
	U472	9070151	Jun 2015	Moskowitz	
	U473	5870723	Feb 1999	Pare	
	U474	5280527	Jan 1994	Gullman	
	U475	6453301	Sep 2002	Niwa	
	U476	5930767	Jul 1999	Reber	
	U477	6000832	Dec 1999	Franklin	
	U478	4885778	Dec 1989	Weiss	
	U479	6820204	Nov 2004	Desai	
	U480	6553127	Apr 2003	Kurowski	

DATE:	EXAMINER'S SIGNATURE:

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

DATE:	EXAMINER'S SIGNATURE:

LISTING OF UNITED STATES PUBLISHED APPLICATIONS - P Series

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 01	20010010078	July 2001	Moskowitz	X
	P 02	20010043594	November 2001	Ogawa et al.	X
	P 03	20020010684	January 2002	Moskowitz	X
	P 04	20020026343	February 2002	Duenke	X
	P 05	20020056041	May 2002	Moskowitz	X
	P 06	20020071556	June 2002	Moskowitz et al.	X
	P 07	20020073043	June 2002	Herman et al.	X
	P 08	20020097873	July 2002	Petrovic	X
	P 09	20020103883	August 2002	Haverstock et al.	X
	P 010	20020161741	October 2002	Wang et al.	X
	P 011	20030126445	July 2003	Wehrenberg	X
	P 012	20030133702	July 2003	Collart	X
	P 013	20030200439	October 2003	Moskowitz	X
	P 014	20030219143	November 2003	Moskowitz et al.	X
	P 015	20040028222	February 2004	Sewell et al.	X
	P 016	20040037449	February 2004	Davis et al.	X
	P 017	20040049695	March 2004	Choi et al.	X
	P 018	20040059918	March 2004	Xu	X
	P 019	20040083369	April 2004	Erlingsson et al.	X
	P 020	20040086119	May 2004	Moskowitz	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 021	20040093521	May 2004	Hamadeh et al.	X
	P 022	20040117628	June 2004	Colvin	X
	P 023	20040117664	June 2004	Colvin	X
	P 024	20040125983	July 2004	Reed et al.	X
	P 025	20040128514.	July 2004	Rhoads	X
	P 026	20040225894	November 2004	Colvin	X
	P 027	20040243540	December 2004	Moskowitz et al.	X
	P 028	20050135615	June 2005	Moskowitz et al.	X
	P 029	20050160271	July 2005	Brundage et al.	X
	P 030	20050177727	August 2005	Moskowitz et al.	X
	P 031	20050246554	November 2005	Batson	X
	P 032	20060005029	January 2006	Petrovic et al.	X
	P 033	20060013395	January 2006	Brundage et al.	X
	P 034	20060013451	January 2006	Haitsma	X
	P 035	20060041753	February 2006	Haitsma	X
	P 036	20060101269	May 2006	Moskowitz et al.	X
	P 037	20060140403	June 2006	Moskowitz	X
	P 038	20060285722	December 2006	Moskowitz et al.	X
	P 039	20070011458	January 2007	Moskowitz	X
	P 040	20070028113	February 2007	Moskowitz	X
	P 041	20070064940	March 2007	Moskowitz et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 042	20070079131.	April 2007	Moskowitz et al.	X
	P 043	20070083467	April 2007	Lindahl et al.	X
	P 044	20070110240	May 2007	Moskowitz et al.	X
	P 045	20070113094	May 2007	Moskowitz et al.	X
	P 046	20070127717	June 2007	Herre et al.	X
	P 047	20070226506	September 2007	Moskowitz	X
	P 048	20070253594	November 2007	Lu et al.	X
	P 049	20070294536.	December 2007	Moskowitz et al.	X
	P 050	20070300072	December 2007	Moskowitz	X
	P 051	20070300073	December 2007	Moskowitz	X
	P 052	20080005571	January 2008	Moskowitz	X
	P 053	20080005572	January 2008	Moskowitz	X
	P 054	20080016365	January 2008	Moskowitz	X
	P 055	20080022113	January 2008	Moskowitz	X
	P 056	20080022114	January 2008	Moskowitz	X
	P 057	20080028222	January 2008	Moskowitz	X
	P 058	20080046742	February 2008	Moskowitz	X
	P 059	20080075277	March 2008	Moskowitz et al.	X
	P 060	20080109417	May 2008	Moskowitz	X
	P 061	20080133927	June 2008	Moskowitz et al.	X
	P 062	20080151934	June 2008	Moskowitz et al.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 063	20090037740	February 2009	Moskowitz	X
	P 064	20090089427	April 2009	Moskowitz et al.	X
	P 065	20090190754	July 2009	Moskowitz et al.	X
	P 066	20090210711	August 2009	Moskowitz	X
	P 067	20090220074	September 2009	Moskowitz et al.	X
	P 068	20100002904	January 2010	Moskowitz	X
	P 069	20100005308	January 2010	Moskowitz	X
	P 070	20100098251	Apr 2010	Moskowitz	X
	P 071	20100220861	Sept 2010	Moskowitz	X
	P 072	20100202607	Aug 2010	Moskowitz	X
	P 073	20020047873	June 2002	Petrovic	X
	P 074	20020009208	Jan 2002	Alattar	X
	P 075	20010029580	October 2001	Moskowitz	X
	P 076	20100182570	July 2010	Chota	X
	P 077	20100077220	March 2010	Moskowitz	X
	P 078	20100077219	March 2010	Moskowitz	X
	P 079	20100064140	March 2010	Moskowitz	X
	P 080	20100153734	June 2010	Moskowitz	X
	P 081	20100106736	April 2010	Moskowitz	X
	P 082	20060251291	November 2006	Rhoads	X
	P 083	20030002862	January 2003	Rodriguez	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 084	20030005780	May 2003	Hansen	X
	P 085	20020152179	Oct 2002	Racov	X
	P 086	20030027549	Feb 2003	Kiel	X
	P 087	20020057651	May 2002	Roberts	X
	P 088	20110069864	March 2011	Moskowitz	X
	P 089	20100313033	Dec 2010	Moskowitz	X
	P 090	20110019691	Jan 2011	Moskowitz	X
	P 091	20030023852	Jan. 2003	Wold	X
	P 092	20030033321	Feb 2003	Schrempp	X
	P 093	20130145058	June 2013	Shuholm	X
	P 094	20120057012	Mar. 2012	Sitrick	X
	P 095	20110128445	Jun 2011	Carrieres	X
	P 096	20020188570	Dec 2002	Holliman	X
	P 097	20020069174	Jun 2002	Fox	X
	P 098	20130226957	Feb 27 2013	Ellis	
	P 099	20090319639	Dec 2009	Gao	
	P100	20030005780	May 2003	Pahl	
	P101	20020097873	June 2002	Petrovic	
	P102	20030021419	Jan 2003	Hansen	

DATE:	EXAMINER'S SIGNATURE:

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

DATE:	EXAMINER'S SIGNATURE:

LISTING OF FOREIGN AND INTERNATIONAL PATENT DOCUMENTS - F Series

EXAMINER INITIALS	REFERENCE NUMBER (F SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	COUNTRY OR REGION	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	F 01-	EP0372601	Jun., 1990	EP		X
	F 02-	EP0565947	Oct., 1993	EP		X
	F 03-	EP0581317	Feb., 1994	EP		X
	F 04-	EP0649261	Apr., 1995	EP		X
	F 05-	EP0651554	May., 1995	EP		X
	F 06-	EP1354276	Dec., 2007	EP		X
	F 07-	NL 1005523	Sep., 1998	NL		X
	F 08-	WO9514289	May., 1995	WO		X
	F 09-	WO9629795	Sep., 1996	WO		X
	F 010-	WO9724833	Jul., 1997	WO		X
	F 011-	WO9744736	Nov., 1997	WO		X
	F 012-	WO9837513	Aug., 1998	WO		X
	F 013-	WO9952271	Oct., 1999	WO		X
	F 014-	WO9962044	Dec., 1999	WO		X
	F 015-	WO9963443	Dec., 1999	WO		X
	F 016-	WO9726733	Jan. 1997	WO		X
	F 017-	WO98002864	Jul. 1997	WO		X
	F 018-	WO0057643	Sept 2000	WO		X
	F 019-	WO9642151	Dec 1996	WO		X
	F 020-	EP0872073	July 1996	EP		X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REFERENCE NUMBER (F SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	COUNTRY OR REGION	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	F 021-	WO0118628	March 2001	WO		X
	F 022-	WO0143026	June 2001	WO		X
	F 023-	WO0203385	Jan 2002	WO		X
	F 024-	WO9701892	June 1995	WO		X
	F 025-	WO9726732	July 1997	WO		X
	F 026-	WO9802864	Jan 1998	WO		X
	F 027-	EP1547337	Mar 2006	EP		X
	F 028-	EP0581317A2	Feb 1994	EP		X
	F 029-	WO023385A1	Oct 2002	WO		X
	F030	WO9955089	Mar 2009	WO		
	F031	WO9942996	Aug 1999	WO		
	F032	H05334072	Dec 1993	JP		
	F033	WO97043761	Nov 1997	WO		
	F034	EP 1028401	Aug 2000	EP		
	F035	WO 0014648	Mar 2000	WO		
	F036	WO 01/13275	Feb 2001	WO		
	F037	WO97/43761	Nov 1997	WO		

DATE:	EXAMINER'S SIGNATURE:

LISTING OF NON PATENT LITERATURE - L Series

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	1	L- 01	N/A	US. Appl. No. 08/999,766, filed Jul. 23, 1997, entitled "Steganographic Method and Device", published as 7568100 07-28-2009, cited as U280.	X
	2	L- 02	N/A	EPO Application No. 96919405.9, entitled "Steganographic Method and Device"; published as EP0872073 (A2), 10-21-1998, cited herein as F20.	X
	3	L- 03	N/A	U.S. Appl. No. 11/050,779, filed Feb. 7, 2005, entitled "Steganographic Method and Device", published as 20050177727 A1 08-11-2005, cited herein as P30.	X
	4	L- 04	N/A	U.S. Appl. No. 08/674,726, filed Jul. 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management", published as 7362775 04-22-2008, cited herein as U272 .	X
	5	L- 05	N/A	U.S. Appl. No. 09/545,589, filed Apr. 7, 2000, entitled "Method and System for Digital Watermarking", published as 7007166 02-28-2006, cited herein as U243	X
	6	L- 06	N/A	U.S. Appl. No. 11/244,213, filed Oct. 5, 2005, entitled "Method and System for Digital Watermarking", published as 2006-0101269 A1 05-11-2006, cited herein as P36	X
	7	L- 07	N/A	U.S. Appl. No. 11/649,026, filed Jan. 3, 2007, entitled "Method and System for Digital Watermarking", published as 2007-0113094 A1 05-17-2007, cited herein as P45.	X
	8	L- 08	N/A	U.S. Appl. No. 09/046,627, filed Mar. 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 6,598,162 07-22-2003, cited herein as U212.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	9	L- 09	N/A	U.S. Appl. No. 10/602,777, filed Jun. 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 2004-0086119 A1 05-06-2004, cited herein P20.	X
	10	L- 010	N/A	U.S. Appl. No. 09/053,628, filed Apr. 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", 6,205,249 03-20-2001, cited herein as U161.	X
	11	L- 011	N/A	U.S. Appl. No. 09/644,098, filed Aug. 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 7,035,409 04-25-2006, cited herein as U245.	X
	12	L- 012	N/A	Jap. App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; which is a JP national stage of PCT/US1999/007262, published as WO/1999/052271, 10/14/1999, F13 here in above..	X
	13	L- 013	N/A	U.S. Appl. No. 09/767,733, filed Jan. 24, 2001 entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 2001-0010078 A1 07-26-2001, cited herein as P1.	X
	14	L- 014	N/A	U.S. Appl. No. 11/358,874, filed Feb. 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 2006-0140403 A1 06-29-2006, cited herein as P37.	X
	15	L- 015	N/A	U.S. Appl. No. 10/417,231, filed Apr. 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth", published as 2003-0200439 A1 10-23-2003, cited herein as P13,	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	16	L- 016	N/A	U.S. Appl. No. 09/789,711, filed Feb. 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2001-0029580 A1 10-11-2001, cited herein as P75.	X
	17	L- 017	N/A	U.S. Appl. No. 11/497,822, filed Aug. 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2007-0011458 A1 01-11-2007, cited herein as P39.	X
	18	L- 018	N/A	U.S. Appl. No. 11/599,964, filed Nov. 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2008-0046742 A1 02-21-2008, cited herein as P58.	X
	19	L- 019	N/A	U.S. Appl. No. 11/599,838, filed Nov. 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2007-0226506 A1 09-27-2007, cited herein as P47.	X
	20	L- 020	N/A	U.S. Appl. No. 10/369,344, filed Feb. 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", published as 2003-0219143 A1 11-27-2003, cited herein as P14.	X
	21	L- 021	N/A	U.S. Appl. No. 11/482,654, filed Jul. 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", published as 2006-0285722 A1 12-21-2006, cited herein as P38.	X
	22	L- 022	N/A	U.S. Appl. No. 09/594,719, filed Jun. 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 7,123,718 10-17-2006, cited herein as U255.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	23	L- 023	N/A	U.S. Appl. No. 11/519,467, filed Sep. 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 2007-0064940 A1 03-22-2007, cited herein as P41.	X
	24	L- 024	N/A	U.S. Appl. No. 09/731,040, filed Dec. 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions", 2002-0010684 A1 01-24-2002, cited herein as P3.	X
	25	L- 025	N/A	U.S. Appl. No. 11/512,701, filed Aug. 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions", published as 2007-0028113 A1 02-01-2007, cited herein as P40.	X
	26	L- 026	N/A	U.S. Appl. No. 10/049,101, filed Feb. 8, 2002, entitled "A Secure Personal Content Server", published as 7,475,246 01-06-2009, cited herein as U277.	X
	27	L- 027	N/A	PCT Application No. PCT/US00/21189, filed Aug. 4, 2000, entitled, "A Secure Personal Content Server", Pub. No.: WO/2001/018628 ; Publication Date: 15.03.2001, cited herein as F21.	X
	28	L- 028	N/A	U.S. Appl. No. 09/657,181, filed Sep. 7, 2000, entitled "Method and Device For Monitoring And Analyzing Signals", published as 7,346,472 03-18-2008, cited herein as U271.	X
	29	L- 029	N/A	U.S. Appl. No. 10/805,484, filed Mar. 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals", published as 2004-0243540 A1 12-02-2004, cited herein as P27.	X
	30	L- 030	N/A	U.S. Appl. No. 09/956,262, filed Sep. 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects", published as 2002-0056041 A1 05-09-2002, cited herein as P05	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	31	L- 031	N/A	U.S. Appl. No. 11/518,806, filed Sep. 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects", 2008-0028222 A1 01-31-2008, cited herein as P57.	X
	32	L- 032	N/A	U.S. Appl. No. 11/026,234, filed Dec. 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" , published as 2005-0135615 A1 06-23-2005, cited herein as P28.	X
	33	L- 033	N/A	U.S. Appl. No. 11/592,079, filed Nov. 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks", published as 2007-0079131 A1 04-05-2007, cited herein as P42.	X
	34	L- 034	N/A	U.S. Appl. No. 09/731,039, filed Dec. 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects", published as 2002-0071556 A1 06-13-2002, cited herein as P06.	X
	35	L- 035	N/A	U.S. Appl. No. 11/647,861, filed Dec. 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects", published as 2007-0110240 A1 05-17-2007, cited herein as P44.	X
	36	L- 036	1996	Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996.	X
	37	L- 037	1997	Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 46, 1997.	X
	38	L- 038	1997	Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p. 207.	X
	39	L- 039	1984	Brealy, et al., Principles of Corporate Finance, "Appendix A--Using Option Valuation Models", 1984, pp. 448-449.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	40	L- 040	2001	Copeland, et al., Real Options: A Practitioner's Guide, 2001 pp. 106-107, 201-202, 204-208.	X
	41	L- 041	1995	Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/SarkAsses.html on.	X
	42	L- 042	1995	Crawford, D.W. "Pricing Network Usage: A Market for Bandwidth of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March.	X
	43	L- 043	1988	Low, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.nj.nec.com/366503.html.	X
	44	L- 044	1995	Caronni, Germano, "Assuring Ownership Rights for Digital Images", published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed) Viewing Publishing Company Germany 1995.	X
	45	L- 045	1996	Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the European conf. on Multimedia Applications, Services & Techniques Louvain-La-Nevve Belgium May 1996.	X
	46	L- 046	1996	Gruhl, Daniel et al., Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science, Cambridge, England (May/Jun. 1996).	X
	47	L- 047	1995	Oomen, A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J.AudioEng. Sc., vol. 43, No. 1/2, pp. 23-28 (1995).	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	48	L- 048	1992	Ten Kate, W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng.Soc., vol. 40,No. 5,pp. 376-383 (1992).	X
	49	L- 049	1993	Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993).	X
	50	L- 050	1988	Sklar, Bernard, Digital Communications, pp. 601-603 (1988).	X
	51	L- 051	1984	Jayant, N.S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs, NJ, pp. 486-509 (1984)	X
	52	L- 052	1995	Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., vol. 2420, pp. 164-173, 1995.	X
	53	L- 053	1995	Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995.	X
	54	L- 054	1997	Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997.	X
	55	L- 055	1994	Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994.	X
	56	L- 056	1990	Ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990).	X
	57	L- 057	1994	Van Schyndel, et al., "A digital Watermark," IEEE Int'l Computer Processing Conference, Austin,TX, Nov. 13-16, 1994, pp. 86-90.	X
	58	L- 058	1996	Smith, et al. "Modulation and Information Hiding in Images", Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-Jun. 1, 1996, pp. 207-227.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	59	L- 059	1997	Kutter, Martin et al., "Digital Signature of Color Images Using Amplitude Modulation", SPIE-E197, vol. 3022, pp. 518-527.	X
	60	L- 060	1997	Puate, Joan et al., "Using Fractal Compression Scheme to Embed a Digital Signature into an Image", SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118.	X
	61	L- 061	1996	Swanson, Mitchell D.,et al., "Transparent Robust Image Watermarking", Proc. of the 1996 IEEE Int'l Conf. on Image Processing, vol. 111, 1996 , pp. 211-214.	X
	62	L- 062	1996	Swanson, Mitchell D., et al. "Robust Data Hiding for Images", 7th IEEE Digital Signal Processing Workshop, Leon, Norway. Sep. 1-4, 1996, pp. 37-40.	X
	63	L- 063	Unknown	Zhao, Jian et al., "Embedding Robust Labels into Images for Copyright Protection", Proceeding of the Know Right '95 Conference, pp. 242-251.	X
	64	L- 064	1995	Koch, E., et al., "Towards Robust and Hidden Image Copyright Labeling", 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun. 1995 Neos Marmaras pp. 4.	X
	65	L- 065	1995	Van Schyandel, et al., "Towards a Robust Digital Watermark", Second Asain Image Processing Conference, Dec. 6-8, 1995, Singapore, vol. 2, pp. 504-508.	X
	66	L- 066	1995	Tirkel,A.Z., "A Two-Dimensional Digital Watermark", DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8, 1995, pp. 7.	X
	67	L- 067	1996	Tirkel,A.Z., "Image Watermarking--A Spread Spectrum Application", ISSSTA '96, Sep. 1996, Mainz, German, pp. 6.	X
	68	L- 068	1996	O'Ruanaidh, et al. "Watermarking Digital Images for Copyright Protection", IEEE Proceedings, vol. 143, No. 4, Aug. 1996, pp. 250-256.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	69	L- 069	Unknown	Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institude, Techinal Report 95-10, pp. 33.	X
	70	L- 070	1969	Kahn, D., "The Code Breakers", The MacMillan Company, 1969, pp. xIII, 81-83, 513, 515, 522-526, 863.	X
	71	L- 071	1997	Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480 (3/14/1997).	X
	72	L- 072	1996	Dept. of Electrical Engineering, Del Ft University of Technology, Del ft The Netherlands, Cr.C. Langelaar et al.,"Copy Protection for Multimedia Data based on Labeling Techniques", Jul. 1996 9 pp.	X
	73	L- 073	Unknown	F. Hartung, et al., "Digital Watermarking of Raw and Compressed Video", SPIE vol. 2952, pp. 205-213.	X
	74	L- 074	1996	Craver, et al., "Can Invisible Watermarks Resolve Rightful Ownerships?", IBM Research Report, RC 20509 (Jul. 25, 1996) 21 pp.	X
	75	L- 075	1988	Press, et al., "Numerical Recipes in C", Cambridge Univ. Press, 1988, pp. 398-417.	X
	76	L- 076	1995	Pohlmann, Ken C., "Principles of Digital Audio", 3rd Ed., 1995, pp. 32-37, 40-48:138, 147-149, 332, 333, 364, 499-501, 508-509, 564-571.	X
	77	L- 077	1991	Pohlmann, Ken C., "Principles of Digital Audio", 2nd Ed., 1991, pp. 1-9, 19-25, 30-33, 41-48, 54-57, 86-107, 375-387.	X
	78	L- 078	1994	Schneier, Bruce, Applied Cryptography, John Wiley & Sons, Inc., New York, 1994, pp. 68, 69, 387-392, 1-57, 273-275, 321-324.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	79	L- 079	1996	Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, Jun. 17-23, 1996 Hiroshima, Japan, 0-8186-7436-9196, pp. 473-480.	X
	80	L- 080	1998	Johnson, et al., "Transform Permuted Watermarking for Copyright Protection of Digital Video", IEEE Globecom 1998, Nov. 8-12, 1998, New York New York vol. 2 1998 pp. 684-689 (ISBN 0-7803-4985-7).	X
	81	L- 081	1996	Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, May 7, 1996 pp. 1-18.	X
	82	L- 082	1996	Bender, et al., "Techniques for Data Hiding", IBM Systems Journal, (1996) vol. 35, Nos. 3 & 4,1996, pp. 313-336.	X
	83	L- 083	2003	Moskowitz, "Bandwith as Currency", IEEE Multimedia, Jan.-Mar. 2003, pp. 14-21.	X
	84	L- 084	2006	Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction--Digital Rights Management" pp. 3-22.	X
	85	L- 085	2001	Rivest, et al., "PayWord and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, Apr. 27, 2001, pp. 1-18.	X
	86	L- 086	2000	Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB)(2000).	X
	87	L- 087	2002	Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security; Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 Apr. 10, 2002 pp. 80-84.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	88	L- 088	2006	Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking" ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006 (to appear) 13.	X
	89	L- 089	2002	Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Cryptography Research, Inc. 2002-2003 14 pages.	X
	90	L- 090	1995	Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring) Mar. 5, 1995 pp. 20-25 vol. CONF40.	X
	91	L- 091	1998	Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, Sep. 30, 1998, pp. 1501-1510 vol. 30 No. 16-18 NL North Holland.	X
	92	L- 092	1999	Konrad, K. et al., "Trust and Electronic Commerce--more than a technical problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems Oct. 19-22, 1999, pp. 360-365 Lausanne.	X
	93	L- 093	1998	Kini, et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216). Jan. 6-9, 1998. pp. 51-61. Los.	X
	94	L- 094	1997	Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sep. 1997, pp. 118-124, vol. 5 No. 3, ACM, USA.	X
	95	L- 095	1999	Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp. 1079-1107 Jul. 1999 vol. 87 No. 7 IEEE.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	96	L- 096	N/A	European Search Report & European Search Opinion in EP07112420	X
	97	L- 097	2006	STAIND (The Singles 1996-2006), Warner Music--Atlantic, Pre-Release CD image, 2006, 1 page.	X
	98	L- 098		DUPLICATE OF L-97, DELETED BY 11/16/2010 by RAN.	X
	99	L- 099	2003	Radiohead ("Hail To The Thief"), EMI Music Group--Capitol, Pre-Release CD image, 2003, 1 page.	X
	100	L- 0100	N/A	DUPLICATE OF L-4, DELETED BY RN UPON REVIEW ON 11/18/2010. RAN	X
	101	L- 0101	N/A	U.S. Appl. No. 60/169,274, filed Dec. 7, 1999, entitled "Systems, Methods And Devices For Trusted Transactions".	X
	102	L- 0102		DUPLICATE OF L-22, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	103	L- 0103		DUPLICATE OF L-27, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	104	L- 0104	N/A	U.S. Appl. No. 60/234,199, filed Sep. 20, 2000, "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects".	X
	105	L- 0105	N/A	U.S. Appl. No. 09/671,739, filed Sep. 29, 2000, entitled "Method And Device For Monitoring And Analyzing Signals".	X
	106	L- 0106		DUPLICATE OF L-34, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	107	L- 0107		DUPLICATE OF L-24, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	108	L- 0108		DUPLICATE OF L-57, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	109	L- 0109		DUPLICATE OF L-58, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	110	L- 0110		DUPLICATE OF L-59, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	111	L- 0111		DUPLICATE OF L-61, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	112	L- 0112		DUPLICATE OF L-62, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	113	L- 0113		DUPLICATE OF L-63, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	114	L- 0114		DUPLICATE OF L-65, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	115	L- 0115	Unknown.	Tirkel, A.Z., "A Two-Dimensional Digital Watermark", Scientific Technology, 686, 14, date unknown. (citation revised upon review on 11/16/10 by RAN.)	X
	116	L- 0116		DUPLICATE OF L-65, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	117	L- 0117		DUPLICATE OF L-68, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	118	L- 0118		DUPLICATE OF L-69, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	119	L- 0119		DUPLICATE OF L-70, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	120	L- 0120		DUPLICATE OF L-71, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	121	L- 0121		DUPLICATE OF L-72, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	122	L- 0122		DUPLICATE OF L-73, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	123	L- 0123		DUPLICATE OF L-74, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	124	L- 0124		DUPLICATE OF L-75, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	125	L- 0125		DUPLICATE OF L-076, REMOVED. RN. 11/16/2010	X
	126	L- 0126		DUPLICATE OF L-77, REMOVED. RN. 11/16/2010	X
	127	L- 0127		DUPLICATE OF L-78, REMOVED. RN. 11/16/2010	X
	128	L- 0128		DUPLICATE OF L-79, REMOVED. RN. 11/16/2010	X
	129	L- 0129		EP0581317A2, MOVED TO FOREIGN PATENT PUBS as F-028	X
	130	L- 0130		DUPLICATE OF L-52, REMOVED. RN. 11/16/2010	X
	131	L- 0131		DUPLICATE OF L-36, REMOVED. RN. 11/16/2010	X
	132	L- 0132		DUPLICATE OF L-38, REMOVED. RN. 11/16/2010.	X
	133	L- 0133		DUPLICATE OF L-37, REMOVED. RN. 11/16/2010	X
	134	L- 0134		DUPLICATE OF L-36, REMOVED. RN. 11/16/2010	X
	135	L- 0135		DUPLICATE OF L-37, REMOVED. RN. 11/16/2010	X
	136	L- 0136		DUPLICATE OF L-38, REMOVED. RN. 11/16/2010	X
	137	L- 0137		DUPLICATE OF L-39, REMOVED. RN. 11/16/2010	X
	138	L- 0138		DUPLICATE OF L-40, REMOVED. RN. 11/16/2010	X
	139	L- 0139		DUPLICATE OF L-41, REMOVED. RN. 11/16/2010	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	140	L- 0140		DUPLICATE OF L-42, REMOVED. RN. 11/16/2010	X
	141	L- 0141		DUPLICATE OF L-43, REMOVED. RN. 11/16/2010	X
	142	L- 0142		DUPLICATE OF L-44, REMOVED. RN. 11/16/2010	X
	143	L- 0143		DUPLICATE OF L-45, REMOVED. RN. 11/16/2010.	X
	144	L- 0144		DUPLICATE OF L-46, REMOVED. RN. 11/16/2010.	X
	145	L- 0145		DUPLICATE OF L-47, REMOVED. RN. 11/16/2010	X
	146	L- 0146		DUPLICATE OF L-48, REMOVED. RN. 11/16/2010	X
	147	L- 0147		DUPLICATE OF L-49, REMOVED. RN. 11/16/2010	X
	148	L- 0148		DUPLICATE OF L-50, REMOVED. RN. 11/16/2010	X
	149	L- 0149		DUPLICATE OF L-51, REMOVED. RN. 11/16/2010	X
	150	L- 0150		DUPLICATE OF L-52, REMOVED. RN. 11/16/2010	X
	151	L- 0151		DUPLICATE OF L-63, REMOVED. RN. 11/16/2010	X
	152	L- 0152		DUPLICATE OF L-54, REMOVED. RN. 11/16/2010	X
	153	L- 0153		DUPLICATE OF L-55, REMOVED. RN. 11/16/2010.	X
	154	L- 0154		DUPLICATE OF L-80, REMOVED. RN. 11/16/2010.	X
	155	L- 0155	N/A	PCT International Search Report in PCT/US95/08159.	X
	156	L- 0156	N/A	PCT International Search Report in PCT/US96/10257.	X
	157	L- 0157	N/A	Supplementary European Search Report in EP 96919405.	X
	158	L- 0158	N/A	PCT International Search Report in PCT/US97/00651.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	159	L- 0159	N/A	PCT International Search Report in PCT/US97/00652	X
	160	L- 0160	N/A	PCT International Search Report in PCT/US97/11455.	X
	161	L- 0161		PCT International Search Report in PCT/US99/07262.	X
	162	L- 0162		PCT International Search Report in PCT/US00/06522	X
	163	L- 0163		Supplementary European Search Report in EP00919398	X
	164	L- 0164		PCT International Search Report in PCT/US00/18411.	X
	165	L- 0165		PCT International Search Report in PCT/US00/18411.	X
	166	L- 0166		PCT International Search Report in PCT/US00/33126	X
	167	L- 0167		PCT International Search Report in PCT/US00/21189	X
	168	L- 0168		Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110.	X
	169	L- 0169	1996	Schneider, M., et al. "A Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC. Lausanne) Sep. 16-19, 1996, pp. 227-230, IEEE ISBN.	X
	170	L- 0170	1997	Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	X
	171	L- 0171	1998	Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, vol. 1 Oct. 4-7, 1998, pp. 455-459.	X
	172	L- 0172	1998	Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, vol. 1525, Apr. 14-17, 1998, pp. 218-238 ISBN: 3-540-65386-4.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	173	L- 0173	1996	Ross Anderson, "Stretching the Limits of Steganography," LNCS, vol. 1174, May/Jun. 1996, 10 pages, ISBN: 3-540-61996-8.	X
	174	L- 0174	1997	Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997 4 pages.	X
	175	L- 0175	1997	Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing Aug. 21, 1997, 19 pages.	X
	176	L- 0176	2008	OASIS (Dig Out Your Soul), Big Brother Recordings Ltd, Promotional CD image, 2008, 1 page.	X
	177	L- 0177	1998	Rivest, R. "Chaffing and Winnowing: Confidentiality without Encryption", MIT Lab for Computer Science, http://people.csail.mit.edu/rivest/Chaffing.txt Apr. 24, 1998, 9 pp.	X
	178	L- 0178	2003	PortalPlayer, PP5002 digital media management system-on-chip, May 1, 2003, 4 pp.	X
	179	L- 0179	2001	VeriDisc, "The Search for a Rational Solution to Digital Rights Management (DRM)", http://64.244.235.240/news/whitepaper, /docs/veridisc.sub.--white.sub.--paper.pdf, 2001, 15 pp.	X
	180	L- 0180	2008	Cayre, et al., "Kerckhoff's-Based Embedding Security Classes for WOA Data Hiding", IEEE Transactions on Information Forensics and Security, vol. 3 No. 1, Mar. 2008, 15 pp.	X
	181	L- 0181	1999	Wayback Machine, dated Jan. 17, 1999, http://web.archive.org/web/19990117020420/http://www.netzero.com/, accessed on Feb. 19, 2008.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	182	L- 0182	1997	Namgoong, H., "An Integrated Approach to Legacy Data for Multimedia Applications", Proceedings of the 23rd EUROMICRO Conference, vol., Issue 1-4, Sep. 1997, pp. 387-391.	X
	183	L- 0183	2007	Wayback Machine, dated Aug. 26, 2007, http://web.archive,org/web/20070826151732/http://www.screenplaysmag.com/t-abid/96/articleType/ArticleView/articleId/495/Default.aspx/.	X
	184	L- 0184	2009	"YouTube Copyright Policy: Video Identification tool--YouTube Help", accessed Jun. 4, 2009, http://www.google.com/support/youtube/bin/answer.py?h1=en&answer=83766, 3 pp.	X
	185	L- 0185	N/A	U.S. Appl. No. 12/665,002, filed Dec. 22, 2009, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 20100182570 A1 07-22-2010, P76.	X
	186	L- 0186	N/A	U.S. Appl. No. 12/592,331, filed Nov. 23, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 20100077220 A1 03-25-2010, P77.	X
	187	L- 0187	N/A	U.S. Appl. No. 12/590,553, filed Nov. 10, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 20100077219 A1 03-25-2010, P78.	X
	188	L- 0188	N/A	U.S. Appl. No. 12/590,681, filed Nov. 12, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 20100064140 A1 03-11-2010, P79.	X
	189	L- 0189	N/A	U.S. Appl. No. 12/655,036, filed Dec. 22, 2009, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 20100153734 A1 06-17-2010, P80 .	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	190	L- 0190	N/A	U.S. Appl. No. 12/655,357, filed Dec. 22, 2009, entitled "Method And Device For Monitoring And Analyzing Signals", published as 20100106736 A1 04-29-2010, P81.	X
	191	L- 0191	N/A	PCT Application No. PCT/US95/08159, filed Jun. 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing", published as WO/1997/001892; Publication Date: 16.01.1997, F24.	X
	192	L- 0192	N/A	PCT Application No. PCT/US96/10257, filed Jun. 7, 1996, entitled "Steganographic Method and Device"--corresponding to--EPO Application No. 96919405.9, entitled "Steganographic Method and Device", published as WO/1996/042151; Publication Date: 27.12.1996; F19.	X
	193	L- 0193	N/A	PCT Application No. PCT/US97/00651, filed Jan. 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code", published as WO/1997/026732; Publication Date: 24.07.1997.	X
	194	L- 0194	N/A	PCT Application No. PCT/US97/00652, filed Jan. 17, 1997, entitled, "Method for an Encrypted Digital Watermark", published as WO/1997/026733; Publication Date: 24.07.1997	X
	195	L- 0195	N/A	PCT Application No. PCT/US97/11455, filed Jul. 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data", published as WO/1998/002864; Publication Date: 22.01.1998	X
	196	L- 0196	N/A	PCT Application No. PCT/US99/07262, filed Apr. 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking", published as WO/1999/052271; Publication Date: 14.10.1999.	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	197	L- 0197	N/A	PCT Application No. PCT/US00/06522, filed Mar. 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as WO/2000/057643; Publication Date: 28.09.2000.	X
	198	L- 0198	N/A	PCT Application No. PCT/US00/18411, filed Jul. 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques"	X
	199	L- 0199	N/A	PCT Application No. PCT/US00/33126, filed Dec. 7, 2000, entitled "Systems, Methods and Devices for Trusted Transactions", published as WO/2001/043026; Publication Date: 14.06.2001.	X
	200	L- 0200	N/A	EPO Divisional Patent Application No. 07112420.0, entitled "Steganographic Method and Device" corresponding to PCT Application No. PCT/US96/10257, published as WO/1996/042151, 12/27/1996, cited herein above as F019.	X X
	201	L- 0201	N/A	US Provisional Application 60/222,023 filed July 31, 2007 entitled "Method and apparatus for recognizing sound and signals in high noise and distortion"	X
	202	L- 0202	N/A	US Application 11/458,639 filed July 19, 2006 entitled "Methods and Systems for Inserting Watermarks in Digital Signals", published as 20060251291 A1 11-09-2006, P82.	X
	203	L- 0203	1995	"Techniques for Data Hiding in Audio Files," by Morimoto, 1995	X
	204	L- 0204	1998	Howe, Dennis July 13, 1998 http://foldoc..org//steganography	X
	205	L- 0205	N/A	CSG, Computer Support Group and CSGNetwork.com 1973 http://www.csgnetwork.com/glossarys.html	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	206	L- 0206	2010	QuinStreet Inc. 2010 What is steganography?-A word definition from the Webopedia Computer Dictionary http://www.webopedia.com/terms/steganography.html	X
	207	L- 0207	2000	Graham, Robert August 21, 2000 "Hacking Lexicon" http://robertgraham.com/pubs/hacking-dict.html	X
	208	L- 0208	2010	Farkex, Inc 2010 "Steganography definition of steganography in the Free Online Encyclopedia" http://encyclopedia2.Thefreedictionary.com/steganography	X
	209	L- 0209	1989	Horowitz, et al., The Art of Eletronics. 2nd Ed., 1989, pp7	X
	210	L- 0210	2004	Jimmy eat world ("futures"), Interscope Records, Pre-Release CD image, 2004, 1 page.	X
	211	L- 0211	2001	Aerosmith ("Just Push Play"), Pre-Release CD image, 2001, 1 page.	X
	212	L- 0212	2002	Phil Collins(Testify) Atlantic, Pre-Release CD image, 2002, 1 page.	X
	213	L- 0213	1998	U. are U. Reviewer's Guide (U are U Software, 1998)	X
	214	L- 0214	1998	U. are U. wins top honors! - Marketing Flyer (U. are U. Software, 1998).	X
	215	L- 0215	1998	Digital Persona, Inc., U. are U. Fingerprint Recognition System: User Guide (Version 1.0, 1998).	X
	216	L- 0216	1998	Digital Persona White Paper pp 8-9 published April 15, 1998.	X
	217	L- 0217	2000	Digital Persona, Inc., "Digital Persona Releases U. are. U Pro Fingerprint Security Systems for Windows NT, 2000, '98, '95", (2000, February)	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	218	L- 0218	2011	SonicWall, Inc. 2011 "The Network Security SonicOS Platform-Deep Packet Inspection" http://www.sonicwall.com/us/en/products/Deep_Packet_Inspection.html	X
	219	L- 0219	2011	Rick Merritt, PARC hosts summit on content-centric nets, EETimes, Aug. 12, 2011, http://www.eetimes.com/electronics-news/4218741/PARC-hosts-summit-on-content-centric-nets	X
	220	L- 0220	2011	Afanasyev, et. al., Communications of the ACM: Privacy Preserving Network Forensics 2011	X
	221	L- 0221	2008	SonicWall, Inc., 2008 "The Advantages of a Multi-core Architecture In Network Security Appliances" http://www.sonicwall.com/downloads/WP-ENG-010_Multicore...	X
	222	L- 0222	2013	Voip-Pal.Com Inc's Lawful Intercept Patent Application Receives the Allowance for Issuance as a Patent, http://finance.yahoo.com/news/voip-pal-com-inc-lawful-133000133.html	X
	223	L- 0223	2013	Deep Content Inspection - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Deep_content_inspection (last visited Apr. 4, 2013)	X
	224	L- 0224	2009	Dexter, et. al, "Multi-view Synchronization of Human Actions and Dynamic Scenes" pp 1-11, 2009	X
	225	L- 0225	2011	Kudrle, et al., "Fingerprinting for Solving A/V Synchronization Issues within Broadcast Environments", 2011	X
	226	L- 0226	2010	Junego, et. al., "View-Independent Action Recognition from Temporal Self-Similarities", 2011	X
	227	L- 0227	2009	Dexter, et al., "Multi-view Synchronization Of Image Sequences", 2009	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	228	L- 0228	2013	Blue Spike, LLC. v. Texas Instruments, Inc et. al, (No: 6:12-CV-499-MHS), Audible Magic Corporations's amended Answer (E.D. TX filed 7/15/2013) (Document 885 page ID 9581), (PACER)	X
	229	L- 0229	2006	Moskowitz, "Introduction-Digital Rights Management," Multimedia Security Technologies for Digital Rights Management (2006), Elsevier	X
	230	L- 0230	1999	George, Mercy; Chouinard, Jean-Yves; Georgana, Nicolas. Digital Watermarking of Images and video using Direct Sequence Spread Spectrum Techniques. 1999 IEEE Canadian Conference on Electrical and Computer Engineering Vol. 1. Pub. Date: 1999 Relevant pages 116-121. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=807181	X
	231	L- 0231	4/4/2014	Shazam Entertainment Limited's Amended Answer to Blue Spike, LLC's complaint and counterclaims against Blue Spike LLC, Blue Spike, Inc and Scott A. Moskowitz , Shazam Entertainment Ltd v. Blue Spike, LLC, Blue Spike, Inc, and Scott Moskowitz (E.D.T.X Dist Ct.) Case No. 6:12-CV-00499-MHS	X X
	232	L- 0232	4/4/2014	Audible Magic Corporation's Second Amended Answer to Blue Spike LLC's Original Complaint for patent infringement and counterclaims against Blue Spike LLC, Blue Spike, Inc and Scott Moskowitz. Blue Spike LLC v. Texas Instruments, Audible Magic Corporation (E.D.T.X Dist Ct.) Case No. 6:12-CV-499-MHS	X
	233	L- 0233	12/19/2011	Shrivastava, et.al. ,"Data-Driven Visual Similarity for Cross-Domain Image Matching", 2011 ACM Transaction of Graphics (TOG), ACM SIGGRAPH Asia vol. 30 number 6, http://graphics.cs.cmu.edu/projects/crossDomainMatching/	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	234	L- 0234	12/6/2011	Spice, Byron, "Carnegie Mellon Researchers Develop Computerized Method for Finding Similar Images in Photos, Paintings, Sketches", Carnegie Mellon News, Dec 6, 2011, Carnegie Mellon University. http://www.cmu.edu/news/stories/archives/2011/december/dec6_matchingimages.html	X
	235	L- 0235	10/16/2014	Memorandum Opinion and Order, Blue Spike LLC v. Texas Instruments, Inc. et al., (E.D.T.X Dist Ct), Case No. 6:12-CV-0499-MHS-CMC (Doc#1831 PageID#27507)	X
	236	L- 0236	10/16/2014	Memorandum Opinion and Order, Blue Spike LLC v. Texas Instruments, Inc. et al., (E.D.T.X Dist Ct), Case No. 6:12-CV-0499-MHS-CMC (Doc#1834 PageID#27597)	X
	237	L- 0237	1989	Yu, Che-Fn,"Access Control and Authorization Plan for Customer Control of Network Services", IEEE GLOBECOM 1989 Pub 1989. pgs 862-869. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=64085	X
	238	L- 0238	1996	Jaeger, Trent; Prakash, Atul; Rubin, Aviel D, "A System Architecture for Flexible Control of Downloaded Executable Content." Proceedings of the Fifth International Workshop on Object-Oreintation in Operating Systems. Pub 1996, pgs 14-18. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=557855	X
	239	L- 0239	5/2011	"Activate Your Product Through The Online License Management System (LMS)", May 2011 Juniper Networks, Inc., USA	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	240	L- 0240	5/2011	"Activate Your Software Capacity and/or Features", May 2011, Juniper Networks, USA	X
	241	L- 0241	5/2011	"Download and Activate Your Software", May 2011, Juniper Networks, Inc., USA	X
	242	L- 0242	9/2009	"Electronic Fulfillment of Feature, Capacity and Subscription License Activation Keys via the License Management System (LMS)", September 2009, Juniper Networks, Inc., USA	X
	243	L- 0243	7/2009	"Juniper Networks License Management System (LMS) FAQ", July 2009, Juniper Networks, Inc., USA	X
	244	L- 0244	12/2014	"License Activation Keys", Dec14, 2014, http://www.juniper.net/generate_license/	X
	245	L- 0245	3/2014	"License code and configuration key reference [AX 2012]", Mar 25, 2014, Microsoft http://technet.microsoft.com/en-us/library/hh378074.aspx	X
	246	L- 0246	12/2014	"License Codes", Dec 14, 2014, Oracle http://www.oracle.com/us/support/licensecodes/index.html	X
	247	L- 0247	12/2014	"PeopleSoft Enterprise: License Codes", Dec 14, 2014, http://www.oracle.com/us/support/licensecodes/peoplesoft-enterprise/index.html	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	248	L- 0248	12/2014	"Primavera License Key Files", Dec 14, 2014, http://www.oracle.com/us/support/licensecodes/primavera/index.html	X
	249	L- 0249	12/2014	"Siebel License Keys", Dec 14, 2014, http://www.oracle.com/us/support/licensecodes/siebel/index.html	X
	250	L- 0250	03/2009	"How to transfer a license activation key to an RMA replacement device", March 2009, Juniper Networks, Inc. USA	X
	251	L- 0251	12/2014	"How to register a license key in My VMware (2011177)", Dec 14, 2014, http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=ex&bbid=TSEBB_1334428459608&url=&stateId=1%200%20462914399&dialogID=462898852&docTypeID=DT_KB_1_1&externalId=2011177&sliceId=1&rfId=	X
	252	L- 0252	7/2001	CHAUSSEE, "Inside Windows Product Activation", July 2001, http://www.licenturion.com/xp	X
	253	L- 0253	12/2014	"How to generate and validate a software key license", Dec 14, 2014, Stack Overflow, http://stackoverflow.com/questions/599837/how-to-generate-and-validate-a-software-license-key	X

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	254	L- 0254	7/2005	DONSW, "License Key Generation", Jul 2005, Code Project, http://www.codeproject.com/articles/11012/License-Key-Generation	X
	255	L- 0255	12/2004	"How are Software License Keys generated?", Dec 14, 2014, Stack Overflow, http://stackoverflow.com/questions/3002067/how-are-software-license-keys-generated	X
	256	L- 0256	3/2015	Decision on Appeal, USPTO PTAB Appeal No. 2012-011854 for application 11/895,388 issued March 12, 2015.	X
	257	L- 0257	1997	Lacy, Jack; Snyder, James H.: Maher, David P. "Music on the Internet and the Intellectual Property Protection Problem". Proceedings of the IEEE International Symposium on Industrial Electronics, 1997m ISIE '97 Vol. 1. Pages SS77-SS833. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=707419	
	258	L- 0258	1998	Kohl, Ulrich; Lotspiech, Jeffrey; Nusser, Stefan, "Security for the Digital Library - Protecting Documents Rather Than Channesl Proceedings". Ninth International Workshop on Database and Expert Systems Applications, 1998, Pgs. 316-321. http://ieeexplore.ieee.org/stamp/stamp/jsp?tp=&arnumber=707419	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	259	L- 0259	1997	von Faber, Eberhard; Hammelrath, Robert; Franz-Peter. The Secure Distribution of Digital Contents. Proceedings, 13th Annual Computer Security Applications Conference, 1997. pgs 16-22. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=651739	
	260	L- 0260	2015	Order Granting Motion For Judgment on the Pleadings, Blue Spike, LLC v. Google Inc. (N.D.Cal. Dist Ct.) Case No. 14-cv-01650-YGR	
	261	L-0261	2017	Order Denying Petition for Panel Rehearing and Rehearing en Banc, Blue Spike, LLC v. Google Inc. (N.D.C.A. Dist Ct.) Case No. 4:14-cv-01650-YGR	
	262	L-0262	1999	AUGOT, DANIEL, "Secure Delivery Of Images over Open Networks", Proceedings of the IEEE, Vol. 87, Issue 7, July 1999, Abstract. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=771076	
	263	L-0263	2016	Blue Spike, LLC v. Google, Inc, 2016-1054 (Fed. Cir. 10/14/2016), judgement adverse to Blue Spike, LLC.	
	264	L-0264	2017	Blue Spike LLC v. Google, Inc., 16-1223 (6/12/2017) denial of writ of certiorari.	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	265	L-0265	2018	Declaration of Dr. Anna Lysyanskaya ("Lysyanskaya Declaration") in Reexam 90014152	
	265 A	L-0265A	2018	AUGOT, DANIEL, "Secure Delivery Of Images over Open Networks", Proceedings of the IEEE, Vol. 87, Issue 7, July 1999, pp. 1251-1266	
	266	L-0266	2018	Plaintiff Blue Spike, LLC's Proposed Terms for Construction, Pursuant to Patent Rule (P.R.) 4-2 in Blue Spike, LLC v. Juniper Networks, Inc., Case No. 6:17-cv-16-KNM (E.D. Tex.)	
	267	L-0267	2018	English Translation of JP H05334072 (Beetcher '072)	
	268	L-0268	2018	Declaration of Dr. Claudio Silva ("Silva Declaration") filed in reexam 90014138	
	269	L-0269	2018	Declaration of Dr. Claudio Silva ("Silva Declaration") filed in reexam 90014137	
	270	L-0270	1987	Ex 1003 in IPR2017-01061, Oded Goldreich, Towards a Theory of Software Protection and Simulation by Oblivious RAMs, 1987 Symposium on Theory of Computing 182-194 (May 1987) ("Goldreich")	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	271	L-0271	1992	Ex 1004 in IPR2017-01061, Rafail Ostrovsky, Software Protection and Simulation on Oblivious RAMs (May 17, 1992) (MIT Ph.D. Thesis) ("Ostrovsky 1992")	
	272	L-0272	1990	Ex 1006 Rafail Ostrovsky, Efficient Computation on Oblivious RAMs, 1990 Symposium on Theory of Computing 514-523 (May 1990) ("Ostrovsky 1990")	
	273	L-0273	1990	Ex 1007 in IPR2017-01061, Expert Declaration of Rafail Ostrovsky, Ph.D.	
	274	L-0274	2016	Ex 1008 in IPR2017-01061, Claim Construction Order entered May 16, 2016 in an unrelated litigation, Blue Spike, LLC v. Huawei Techs. Co. et al., Case No. 6:13-cv-00679, Dkt. 194.	
	275	L-0275	1997	Ex 1005 in IPR2017-01109, Stephanie Forrest et al., Building Diverse Computer Systems, The Sixth Workshop on Hot Topics in Operating Systems, 67-71 (IEEE, May 1997) ("Forrest")	
	276	L-0276	2017	Ex 1008 in IPR2017-01109, Expert Declaration of Rafail Ostrovsky, Ph.D.	
	277	L-0277	2018	C.A. No. 17-928 (LPS), "Defendant's Initial Invalidity Contentions"	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	278	L-0278	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'SDMI' and 'Portable Device Spec." (Bates numbered pages: ROKU_00005564 to 5598 containing document titled "SDMI Portable Device Specification, Part 1, Version 1.0, dated "8th July, 1999"	
	279	L-0279	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005948 to 5949 containing document titled "Liquid Audio Delivers Web Server and Production Tools For Online Music Commerce" dated "March 12, 1997")	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	280	L-0280	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005952 to 5953 containing document titled "Liquid Audio to Develop Internet Technology with Dolby" dated "Aug 26 1996")	
	281	L-0281	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered page: ROKU00005954 containing document titled "Liquid Audio Supports Solana's Digital Watermark System for Online Music Delivery" dated "Jan. 23, 1997")	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	282	L-0282	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005955 to ROKU00005956 containing document titled "IUMA Bets on Liquid Audio", dated "6.Dec.98.PST")	
	283	L-0283	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005963 containing document beginning "Here is an online directory...." dated "4/24/97")	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	284	L-0284	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Num bered pages: ROKU00005964 to ROKU000065 containing document beginning "Utilizing an exclusive, enhanced version...." undated)	
	285	L-0285	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered page: ROKU00005966 containing document beginning "Liquid Audio is developing...." undated)	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	286	L-0286	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered page: ROKU00005967 containing document titled "Liquid Audio fine tunes Music on Demand", undated)	
	287	L-0287	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Xerox Corp.' (Bates numbered pages: ROKU00005520 to ROKU00005521, containing document titled "ContentGuard Marketplace", undated)	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	288	L-0288		Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Xerox Corp.' (Bates numbered pages: ROKU00005957 to ROKU00005958, document titled "CONTENTGUARD", undated)	
	289	L-0289	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Rights Server.' (Bates numbered page: ROKU00005961 to ROKU00005962, containing document titled "ContentGuard Rights Server", undated)	
		L-0290	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Publisher.' (Bates numbered page: ROKU00005959 to ROKU00005960, containing document titled "ContentGuard Publisher", undated.)	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-0291	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Solana,' 'Electronic DNA,' 'E-DNA,' and 'Solana Technology.' (Bates numbered pages: ROKU00005950 to ROKU00005951, containing document titled "Solana's E-DNA Digital Watermark Technology to Protect Audio Distributed via the Net", dated "Jan, 1997")	
		L-0292	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Solana,' 'Electronic DNA,' 'E-DNA,' and 'Solana Technology.' (Bates numbered page: ROKU00005954, containing documen titled "Liquid Audio Supports Solana's Digital Watermark System for Online Music Delivery", dated "Jan. 23, 1997")	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-0293	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Digital River,' 'Digital,' and 'Secure Sales System.' (Bates numbered pages: ROKU00005773 to ROKU00005774, containing document titled "Digital River", undated)	
		L-0294		Index identifying Bates numbers pages containing alleged prior art, provided by defendant Roku in Blue Spike v Roku ligation, Blue Spike v. Roku C.A. No. 17-928 (LPS).	
		L-0295		ROKU5516-7, C. Guglielmo, Net Music with A Watermark, 1/17/1999	
		L-0296		L-0296 ROKU5518-19 Boscardin, 4/30/1997	
		L-0297		L-0297 ROKU 5520-5521 ContentGuard, 4/7/2000	
		L-0298		L-0298 ROKU 0000553, 11/2/1998	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-0299		L-0299 ROKU5600-02,1/17/1999	
		L-0300		L-0300 ROKU5967-74 Giles, 6/19/1997	
		L-301	2018	Expert Report of Dr. Markus Jakobsson, PH.D. December 3, 2018	
		L-301A	2018	Exhibits A-1 to A-5 of L-301	
		L-301B	2018	Exhibits B-1 to B-5 of L-301	
		L-301C	2018	Exhibits C-1 to C-5 of L-301	
		L-301D	2018	Exhibits D-1 to D-5 of L-301	
		L-301E	2018	Exhibits E-1 to E-5 of L-301	
		L-302		L-302 Tamper Resistant Software: An Implementation. Date unknown.	
		L-303	2018	L-303 Creating multi-DRM protected videos with free tools - Axinom	
		L-304	1976	L-304 Hellmanm, New Directions in Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-305	2018	L-305 DIVX (Digital Video Express) (1998 – 1999)	
		L-306		L-306 Electronic Watermark	
		L-307	2018	L-307 First open source W3C EME solution provided on the 96Boards HiKey platform Posted on Tuesday, June 14, 2016 in Blog (/categories/#blog) By Linaro (/author/linaro/) Authors: Mark Gregotski and Zoltan Kuscsik	
		L-308		L-308 WasApple	
		L-309		L-309 Surviving a Standards War: Lessons Learned from The Life and Death of DIVX David Dranove and Neil Gandal1 January 2004	
		L-310		L-310 Testing Digital Watermark Resistance to Destruction Sabrina Sowers and Abdou Youssef† The George Washington University Department of Electrical Engineering and Computer Science Washington, DC USA 20052 {sowers, youssef}@seas.gwu.edu	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-311	Jul 1999	L-311 Information Hiding|A Survey Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.	
		L-312		L-312 On Software Protection Via Function Hiding Tomas Sander and Christian F. Tschudin International Computer Science Institute, Date unknown.	
		L-313	1998	L-313 Continuous Steganographic Data Transmission Using Uncompressed Audio Chr. Neubauer, J. Herre, and K. Brandenburg Fraunhofer Institut f¨ur Integrierte Schaltungen, 91058 Erlangen, Germany	
		L-314		L-314 Music and Media, January 27, 2001, Vol. 18, Issue 5	
		L-315	2018	L-315 Microsoft Unveils Windows Media Player for Palm-Size and Pocket PCs, January 6, 2000	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-316	2018	L-316 Marlin founders release technology specifications and announce developer conferences Open specifications for protected content sharing technology and community development initiatives to drive interoperability Sunnyvale, CA, May 8, 2006	
		L-317	2018	L-317 Marlin DRM Announces Solution for Enhanced Content Protection (ECP) for UHD Content January 15, 2018 03:01 AM Eastern Standard Time	
		L-318	2015	L-318 Linaro Clear Key, Jan 2015	
		L-319	2018	Legacy Windows Media License Agreements Applies to: Windows Media Player	
		L-320	2018	L-320 Unlocking the iPod Jon Johansen became a geek hero by breaking the DVD code. Now he's liberating iTunes - whether Apple likes it or not. By Robert Levine, Fortune October 23 2006: 2:54 PM EDT	
		L-321		L-321 Exploring Steganography: Seeing the Unseen by Neil Johnson and Sushil Jajoda, Hua Li, October 6, 1999, date Unknown	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-322		L-322 Intellectual Property Protection Systems and Digital Watermarking Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, James H. Snyder, date unknown.	
		L-323	2018	L-323 The Incredibly Technical History of Digital Rights Management, Ernie Smith 10, 19, 2017,	
		L-324		L-324 Robust Digital Watermarking Based on Key-Dependent Basis Functions Jiri Fridrich, date unknown	

DATE:	EXAMINER'S SIGNATURE:

Electronic Acknowledgement Receipt

EFS ID:	35195831
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-FEB-2019
Filing Date:	16-MAY-2018
Time Stamp:	21:11:02
Application Type:	Reexam (Third Party)

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		2019-02-15_IDS_90014138.pdf	35668 560670133ac329ef1455413b3736726737c78ebc	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Form (SB08)	1	2
	Affidavit-not covered under specific rule	3	3

Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	2019-02-18ReferenceCitationList_90014138.pdf	429253 47a6b4f7c519ed297b3003e8fe2560ec75600c20	no	75
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
		Total Files Size (in bytes):	464921		

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.

Electronic Acknowledgement Receipt

EFS ID:	35196004
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-FEB-2019
Filing Date:	16-MAY-2018
Time Stamp:	21:47:11
Application Type:	Reexam (Third Party)

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	Non Patent Literature	L-301_Jakobsson_embedFonts E1.pdf	10202024 0583ad2847cf0a7c6040087c08b507f2eb7727bd	no	162

Warnings:

Information:	
Total Files Size (in bytes):	10202024

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.

Reexamination Control Number: 90014138
Confirmation No: 7638
RE: Reexamination of USP 9104842

Patent Owner Information Disclosure Statement

The patentee previously submitted and IDS listing references U1 to U480; P1 to P102; F1 to F37; and L1 to L301 and provided copies where necessary.

This IDS cites and provides copies of additional references L302-L328

The undersigned was advised by USPTO officials that no fee is due when filing an IDS in a reexamination.

				Reexamination Control Number: **90014138**	
		L-302		L-302_Tamper Resistant Software: An Implementation. Date unknown.	
		L-303	2018	L-303_Creating multi-DRM protected videos with free tools - Axinom	
		L-304	1976	L-304_Hellmanm, New Directions in Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976	
		L-305	2018	L-305_DIVX (Digital Video Express) (1998 – 1999)	
		L-306		L-306_Electronic Watermark	
		L-307	2018	L-307_First open source W3C EME solution provided on the 96Boards HiKey platform Posted on Tuesday, June 14, 2016 in Blog (/categories/#blog) By Linaro (/author/linaro/) Authors: Mark Gregotski and Zoltan Kuscsik	
		L-308		L-308_WasApple	
		L-309		L-309_Surviving a Standards War: Lessons Learned from The Life and Death of DIVX David Dranove and Neil Gandal1 January 2004	
		L-310		L-310_Testing Digital Watermark Resistance to Destruction Sabrina Sowers and Abdou Youssef† The George Washington University Department of Electrical Engineering and Computer Science Washington, DC USA 20052 {sowers, youssef}@seas.gwu.edu	
		L-311	Jul 1999	L-311_Information Hiding|A Survey Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.	

				Reexamination Control Number: **90014138**	
		L-312		L-312_On Software Protection Via Function Hiding Tomas Sander and Christian F. Tschudin International Computer Science Institute, Date unknown.	
		L-313	1998	L-313_Continuous Steganographic Data Transmission Using Uncompressed Audio Chr. Neubauer, J. Herre, and K. Brandenburg Fraunhofer Institut f¨ur Integrierte Schaltungen, 91058 Erlangen, Germany	
		L-314		L-314_Music and Media, January 27, 2001, Vol. 18, Issue 5	
		L-315	2018	L-315_Microsoft Unveils Windows Media Player for Palm-Size and Pocket PCs, January 6, 2000	
		L-316	2018	L-316_Marlin founders release technology specifications and announce developer conferences Open specifications for protected content sharing technology and community development initiatives to drive interoperability Sunnyvale, CA, May 8, 2006	
		L-317	2018	L-317_Marlin DRM Announces Solution for Enhanced Content Protection (ECP) for UHD Content January 15, 2018 03:01 AM Eastern Standard Time	
		L-318	2015	L-318_Linaro Clear Key, Jan 2015	
		L-319	2018	Legacy Windows Media License Agreements Applies to: Windows Media Player	
		L-320	2018	L-320 Unlocking the iPod Jon Johansen became a geek hero by breaking the DVD code. Now he's liberating iTunes - whether Apple likes it or not. By Robert Levine, Fortune October 23 2006: 2:54 PM EDT	

				Reexamination Control Number: **90014138**	
		L-321		L-321_Exploring Steganography: Seeing the Unseen by Neil Johnson and Sushil Jajoda, Hua Li, October 6, 1999, date Unknown	
		L-322		L-322_Intellectual Property Protection Systems and Digital Watermarking Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, James H. Snyder, date unknown.	
		L-323	2018	L-323_The Incredibly Technical History of Digital Rights Management, Ernie Smith 10, 19, 2017,	
		L-324		L-324_Robust Digital Watermarking Based on Key-Dependent Basis Functions Jiri Fridrich, date unknown	
		L-325	2019	L-325 DI 36 2019-02-26 STATEMENT Joint Claim Construction and Prehearing Statement, Case 2:19-cv-00748-JAK-JPR Document 36	
		L-326	2019	L-326 DI 39 2019-03-05 BRIEF filed by def Opening Claim Construction Brief, Case 2:19-cv-00748-JAK-JPR Document 39	
		L-327	2019	L-327 DI 40 2019-03-05 OPENING CLAIM CONSTRUCTION BRIEF, Case 2:19-cv-00748-JAK-JPR Document 40	
		L-328	2019	L-328 3/10/2019 Email identifying copyright registration titled "Giovanni Master (audio digital watermark source code)", Claimant Scott Moskowitz, Registration Number/Date "TXu000892516/1999-02-08"; and Date of Creation: "1999."	

Truly,

/RichardNeifeld/
RICHARD NEIFELD, ATTORNEY FOR PATENTE
REG. NO. 35,299

Reexamination Control Number: 90014138
Confirmation No: 7638
RE: Reexamination of USP 9104842

37 CFR 1.234 Certificate of Service

I served by first class mail (priority mail):
In paper format:
This IDS and Certificate of Service
On a portable USB drive:
Copies of references L302-L328

on the third parte reexamination requestor at his correspondence address:

Attn: Joseph P. Edell
FISCH SIGLER LLP
5301 WISCONSIN AVENUE, NW
FOURTH FLOOR
WASHINGTON, DC 20015

Date of Service: 3-25-2019

/RichardNeifeld/
Richard Neifeld, Reg. No. 35,299
Attorney for patent owner

Electronic Acknowledgement Receipt

EFS ID:	35505648
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	25-MAR-2019
Filing Date:	16-MAY-2018
Time Stamp:	14:16:42
Application Type:	Reexam (Third Party)

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)	2019-03-22_IDS_90014138.pdf	123882 30d50951122d85f778679d6f3382612f4722d687	no	5
Warnings:					

Information:					
This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	L-302_aucsmith.PDF	251223 67f81cfe65654e3b03263e5e48494dbb9efe927b	no	17
Warnings:					
Information:					
3	Non Patent Literature	L-303_CreatingMulti-DRME.pdf	109240 ff37098e1636f0044bd1e0262c49620bb3f92a93	no	5
Warnings:					
Information:					
4	Non Patent Literature	L-304_DiffieHellmanE.pdf	10647007 bdc54f16a97c725302b2d971810d474a1ca8b97b	no	11
Warnings:					
Information:					
5	Non Patent Literature	L-305_DIVXE.pdf	56609 46b9bc303f40b1c4693f1fbd4860292baf673e2d	no	4
Warnings:					
Information:					
6	Non Patent Literature	L-306_ElectronicWaterMarkE.pdf	1617408 da7052a8b822fb96d5e9ecd3d3754227c47bd6bd	no	9
Warnings:					
Information:					
7	Non Patent Literature	L-307_FirstOpenEE.pdf	149923 63bf413a9d0fa0166c651d111a639f5b2ccd6f1e	no	8
Warnings:					
Information:					
8	Non Patent Literature	L-308_WasAppleE.pdf	319022 95229a24e0c57c69229c21d33acc409a3dd83ebb	no	10
Warnings:					
Information:					

9	Non Patent Literature	L-309_SurvivingE.pdf	66623 8892d70ca61db5e145cd5d435331a21253d97d2b	no	21
Warnings:					
Information:					
10	Non Patent Literature	L-310_TestingI.pdf	1119307 b334a65c82b1563418e29910f0a5386833b66bc9	no	19
Warnings:					
Information:					
11	Non Patent Literature	L-311_InformationHidingE.pdf	404833 9085ccdb3c699368de055b0093aa9704e75b62ad	no	17
Warnings:					
Information:					
12	Non Patent Literature	L-312_OnSoftwareProtection.pdf	891856 876bd957ae0e76bf8290b046c9b7300f66b02999	no	12
Warnings:					
Information:					
13	Non Patent Literature	L-313_ContinuousSteganographicE.pdf	288131 8f0eb4c8e31083e642622b4ae2c620e7e3ec4bfe	no	10
Warnings:					
Information:					
14	Non Patent Literature	L-314_Music.pdf	508565 c8756a76401e4bc495006c1fa9bbe5ffb19f9b87	no	3
Warnings:					
Information:					
15	Non Patent Literature	L-315_MicrosoftUnveilsE.pdf	41220 73a2a2760075913d5b896d03e6038fa06dbaf5eb	no	4
Warnings:					
Information:					

16	Non Patent Literature	L-316_Marlin.pdf	393715 17382e6386b6a010ec5eeddc3bd1427a7d911461	no	3
Warnings:					
Information:					
17	Non Patent Literature	L-317_MarlinDRM.pdf	122134 90e9aa08db64f6543c35ea5600a44081b001b7f3	no	2
Warnings:					
Information:					
18	Non Patent Literature	L-318_LinaroClear.pdf	1483422 32cdf03836dbb14bd485b3c70fd2e9faf863725b	no	13
Warnings:					
Information:					
19	Non Patent Literature	L-319_LegacyWindowsE.pdf	32534 c732528b5498ae8d5f7ec291a36c64694a5b0fdd	no	3
Warnings:					
Information:					
20	Non Patent Literature	L-320_Unlocking.pdf	260540 2d48eb2ae24e76e2c7f65dd33b258fbfeb58aa99	no	3
Warnings:					
Information:					
21	Non Patent Literature	L-321_Exploring.pdf	249559 6ab2f00dcbe7ecac475771b95c81bbda640d2eaa	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	19136753		

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.

Electronic Acknowledgement Receipt

EFS ID:	35505696
Application Number:	90014138
International Application Number:	
Confirmation Number:	7638
Title of Invention:	DATA PROTECTION METHOD AND DEVICE
First Named Inventor/Applicant Name:	9104842
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	25-MAR-2019
Filing Date:	16-MAY-2018
Time Stamp:	14:17:18
Application Type:	Reexam (Third Party)

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	Non Patent Literature	L-322_IntellectualProperty.pdf	867120 056678825f46c4689a025d9a67871aeacad275d8	no	14

Warnings:

Information:					
2	Non Patent Literature	L-323_TheIncredibly.pdf	1161294 d1136e922d454427f1cee9e4aa79607c0f44308d	no	19
Warnings:					
Information:					
3	Non Patent Literature	L-324_RobustI.pdf	2261290 f39a35f1d680a3df1c55aa7b7513c6e6b1ded0de	no	15
Warnings:					
Information:					
4	Non Patent Literature	L-325_JointClaimConstruction.pdf	735014 0229eb71b42235c68ad73e45bd81048bf92f3ac5	no	8
Warnings:					
Information:					
5	Non Patent Literature	L-326_BRIEF_def.pdf	766413 af402a760fcef16c217c7f2ed987f113a8bfe2bd	no	30
Warnings:					
Information:					
6	Non Patent Literature	L-327_Brief_Plaintiff.pdf	914518 c97dedd8b502855ea1d7d3beb2c46cdc4b761f97	no	32
Warnings:					
Information:					
7	Non Patent Literature	L-328_GiovanniCopyrightReg.pdf	577161 e3e2d038e975aa51aaae89bd50ea1775ef307d0c	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	7282810	

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,138	05/16/2018	9104842		7638

31518 7590 04/01/2019

NEIFELD IP LAW, PC
5400 Shawnee Road
Suite 310
ALEXANDRIA, VA 22312-2300

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
04/01/2019	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Joseph F. Edell
Fisch Sigler LLP
5301 Wisconsin Ave, NW
Fourth Floor
Washington, DC 20015

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,138* .

PATENT UNDER REEXAMINATION *9104842* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

FINAL OFFICE ACTION

***ex parte* Reexamination**

This is an *ex parte* reexamination of U.S. Patent Number: 9,104,842 issued to Moskowitz, hereinafter the '842 Patent. This action addresses patent claims 11-14 for which it has been determined in the Order mailed 6/19/2018 that a substantial new question of patentability was raised in the Request for ex parte reexamination filed 5/16/2018. This action addresses the Patent Owner Response filed 2/11/2019.

The present application is being examined under the pre-AIA first to invent provisions.

Availability of References as Prior Art:

Claims 11-14 are reexamined on the basis of the following references:

U.S. Patent No. 5,933,497 issued to Beetcher (hereinafter Beetcher / Ex.3)

Japanese Patent Application Publication No. H05334072 issued to Beetcher (hereinafter Beetcher '072 / Ex.4)

PCT Application Publication No. WO 97/26732 issued to Cooperman (hereinafter Cooperman / Ex. 6)

U.S. Patent No. 5,935,243 issued to Hasebe (hereinafter Hasebe / Ex. 7)

Prosecution History

U.S. Patent Application Serial No. 11/895,388, which resulted in issued Patent 9,104,842 (hereinafter the '842 patent), was filed on August 24, 2007.

During prosecution of the '842 Patent, claims 1-64 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Holmes et al. (US Patent Number: 5,287,407) in further view of Houser et al. (US Patent Number: 5,606,609).

Claims 32-45 and 52-64 were remaining in the case and rejected over Holmes and Houser (supra), when the claims went to appeal.

The Examiners Answer, dated 8/8/2012, subsequently withdrew the rejections of claims 34, 45, 54, and 58, with claims 34, 45, and 54 left as objected to as being dependent upon a rejected base claim, and claim 58 (now patent claim 11) noted as 'recites allowable subject matter', with no further elaboration.

In the Decision on Appeal, dated 3/12/2015, the board considered the rejections under 35 U.S.C. § 103(a) (supra) and rendered the judgment that:

> DECISION
>
> The rejection of claims 32, 33, 35, 37, 39, 52, 53, 55–57, 59, and 63–64 under 35 U.S.C. § 103(a) is affirmed.
>
> The rejection of claims 36, 38, 40–44, and 60–62 under 35 U.S.C. § 103(a) is reversed.

The Board in the Decision specifically noted, with respect to the reversed claims, that:

Claims 36 and 60 (patent claim 12)

Claims 36 and 60 include limitations that **require the underlying software functionality be enabled upon the presence or detection of a key, or other software code**. See, e.g., Claim 60 ("software code will provide said specified underlying functionality only after receipt of said first license key"). Appellant argues neither Holmes nor Houser teaches or suggests enabling software functionality based on a license key. App. Br. 80, 98. We agree. Holmes states the data block containing the identification information "does not play any part in the function of the software of the master file itself." Holmes, col. 3, ll. 41-42. Accordingly, we cannot sustain the rejection of claims 36 and 60.

Claim 61 (patent claim 13)

Appellant contends the Examiner's rejection of claim 61 does not address various limitations of the claim, such as "**encoding said first code resource to form an encoded first code resource**," or an "**encoded first code resource, and a decode resource for decoding said encoded first code resource**" in the software. App. Br. 99-100. The Examiner relies on reasoning found in the rejections of claims 32 and 43. Final Act. 7. The Examiner's findings do not support the combination of Houser and Holmes teaches or suggests a modified software code comprising an encoded first code resource and a decode resource for decoding the encoded first code resource, wherein the decode resource is configured to decode the encoded first code resource upon receipt of a first license key. Accordingly, we do not sustain the rejection of claim 61.

Claim 62 (patent claim 14)

Appellant argues "neither Holmes nor Houser disclose or suggest encoding code interrelationships between code resources of the software." App. Br. 103-04. The Examiner bases the rejection of claim 62 on the reasons set forth in rejecting claims 32 and 61. Final Act. 8. We disagree the same reasons apply. For example, claims 32 and 61 do not recite limitations regarding "**software code interrelationships between code resources that result in a specified underlying functionality**." Because the Examiner has not shown how the references teach or suggest all the limitations of claim 62, we do not sustain its rejection.

On 6/4/2015, the Examiner issued a Notice of Allowance based on the Board's March 12, 2015 decision. After the notice of allowance. Patent Owner requested claim amendments, adding, in pertinent part, the term "product" to claim 58. The patent issued on August 11, 2015.

IDS

Where the IDS citations are submitted but not described, the examiner is only responsible for cursorily reviewing the references. The initials of the examiner on the PTO-1449 indicate only that degree of review unless the reference is either applied against the claims, or discussed by the examiner as pertinent art of interest, in a subsequent office action. See Guidelines for Reexamination of Cases in View of In re Portola Packaging, Inc., 110 F.3d 786, 42 USPQ2d 1295 (Fed. Cir. 1997), 64 FR at 15347, 1223 Off. Gaz. Pat. Office at 125 (response to comment 6).

Consideration by the examiner of the information submitted in an IDS means that the examiner will consider the documents in the same manner as other documents in Office search files are considered by the examiner while conducting a search of the prior art in a proper field of search. The initials of the examiner placed adjacent to the citations on the PTO-1449 or PTO/SB/08A and 08B or its equivalent mean that the information has been considered by the examiner to the extent noted above.

Regarding IDS submissions MPEP 2256 recites the following: "Where patents, publications, and other such items of information are submitted by a party (patent owner or requester) in compliance with the requirements of the rules, the requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information."

Accordingly, the IDS submissions of 2/19/2019 and 3/25/2019 have been considered by the Examiner only with the scope required by MPEP 2256, unless otherwise noted.

REJECTIONS

The rejections below are confined to what has been deemed to be the best available art from the Request. However, prior to conclusion of this reexamination proceeding, claims must be patentable over all prior art cited in the order granting reexamination in order to be considered patentable or confirmed on the reexamination

certificate. The references cited in the request but not utilized in the current office action appear to be largely cumulative to the teachings in the reference applied below.

Claim Rejections – 35 USC § 102 and § 103

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Beetcher Reference

Claims 12 and 14 are anticipated by Beetcher under 35 U.S.C. § 102(a).

(The Beetcher '072 reference is equally applicable, however is not relied upon here for the sake of brevity, please see third party requestors mapping for correspondence on pages 50-81 of the Request)

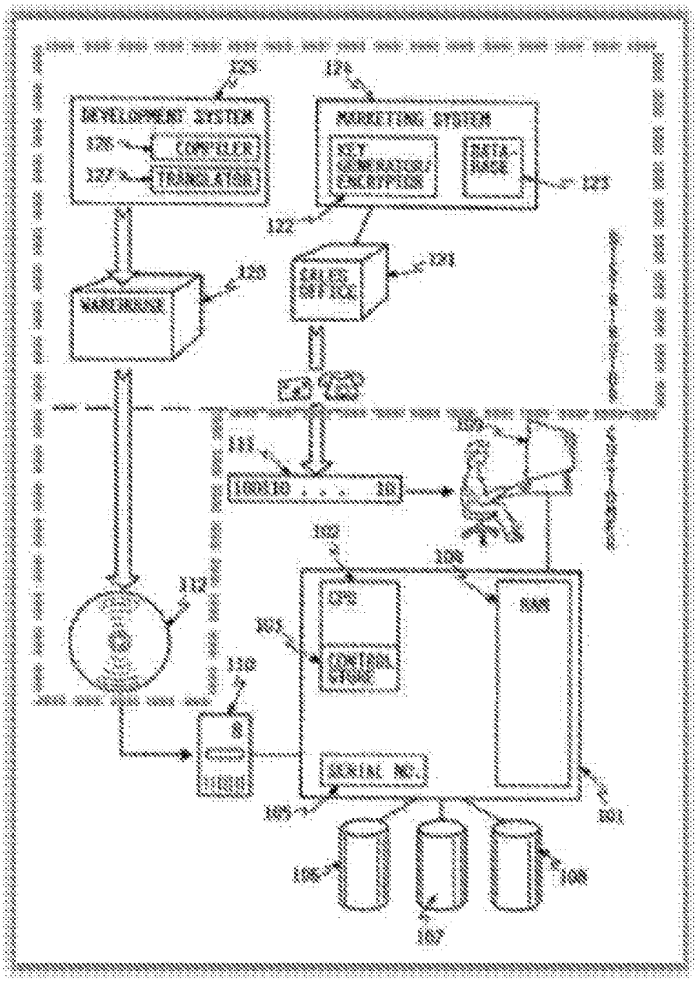
In summary:

Beetcher teaches utilizing components of the product key (version # / product #) when encoding software code via a templating algorithm (see column 9, lines 1-20 and column 6, lines 22-40). The resultant executable code including referencable triggers inserted therein executable via checks to interrelated entries in the product lock table (see column 4, lines 14-23). Where the software module is said to be distributed as compiled object code with embedded entitlement verification triggering instructions that contain version # and product # fields (see column 6, lines 41-58). Thereinafter trigger enabled software codes segments are only executable if an entitlement key is provided that enables the corresponding trigger / flag (see column 4, lines 14-23 and column 9, line 49 through column 10, line 47).

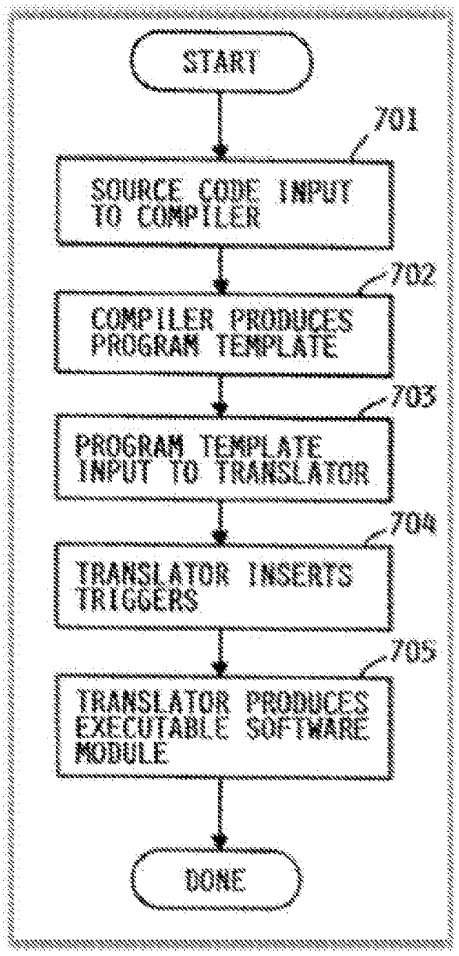
Claim 12

a) Preamble: "A method for encoding software code using a computer having a processor and memory, the method comprising"

Beetcher discloses claim 12's preamble. Specifically, Beetcher describes a method for encoding software code using a computer with a processor and memory. Beetcher details that the software distributor has "development computer system 125, which contains compiler 126 and translator 127" where "[t]he software modules are recorded on software recording media 112" and "entitlement key generator/encrypter 122 and a database 123 containing customer information." (see Beetcher at 5:38-48; see also id. at 9:1-20). Beetcher specifies these compiling and key generating functions may be performed by a single computer (Id. at 5:51-58). Below annotated Figure 1 illustrates the distributor's computer system distributing memory media 112 and compiling encoded software code:



Beetcher's Figure 7 illustrates the software code being encoded to include watermarking triggers decoded by the customer's licensing information (Id. at 9:1-20, Fig. 7).



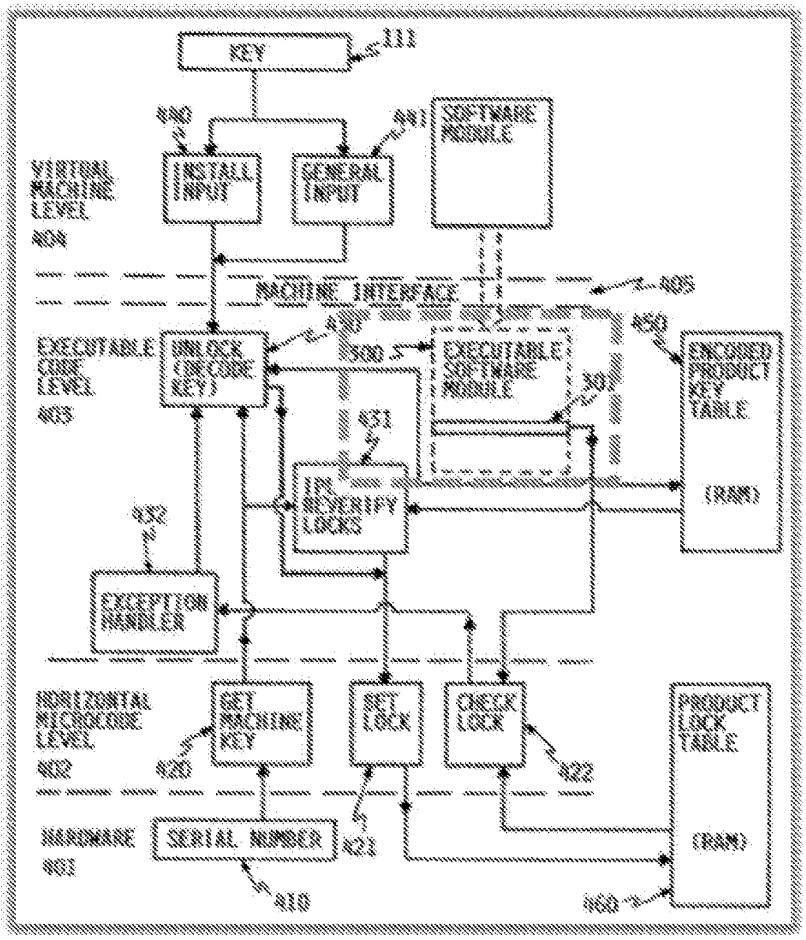
As such, a POSITA would have understood that Beetcher's distributor compiles and stores the encoded software code using a processor and memory akin to the console's CPU 102 and memory devices 106-108. As expert Dr. Silva explains in his declaration (Ex. 9), Beetcher's computer would necessarily include a processor and memory in order to function. (Silva Declaration at ¶¶156-59)

b) Element 12.1: "storing a software code in said memory"

Beetcher discloses element 12.1. Specifically, Beetcher discloses a development system 125 for compiling and translating for the software code (Beetcher at 5:38-48, 9:1-20). Beetcher details that the software code is stored as disks 112 in warehouse 120. A POSITA would have understood that developer system 125 stores the compiled and translated code in memory and records that code onto disks 112 for distribution to customers. As expert Dr. Silva explains in his declaration (Ex. 9), Beetcher's computer would necessarily include store software code in memory in order to function. (Silva Declaration at ¶ 62)

c) Element 12.2: "wherein said software code comprises a first code resource and provides a specified underlying functionality when installed on a computer system"

Beetcher discloses element 12.2. Specifically, Beetcher explains that its software code includes multiple code resources that include a first code resource. (Beetcher at 5:40-43, 6:1-15) Beetcher's code resources include software modules 300 (dashed box) including sub-objects within the code, as shown below in annotated Figure 4 and Figure 3 (Id. at 6:41-45, 8:14-17, Fig. 4; see also id. at 7:45-48, Fig. 3). These sub-objects control multiple functions of the software installed on the customer's computer system 101 (Id. at 6:58-65, 11:4-39; see also id. at Abstract, 4:28-33, 6:65-7:5, claim 3). And Beetcher's software prevents unwanted "patching" of these sub-objects by including entitlement verification triggering instructions 301 (Id. at 4:25-33, 11:11-39; see also id. at Abstract, 3:14-18).


KEY
111
440
441
SOFTWARE MODULE
VIRTUAL MACHINE LEVEL
404
INSTALL INPUT
GENERAL INPUT
MACHINE INTERFACE
405
EXECUTABLE CODE LEVEL
403
UNLOCK (DECODE KEY)
430
500
EXECUTABLE SOFTWARE MODULE
301
450
ENCODED PRODUCT KEY TABLE
(RAM)
431
IPL REVERIFY LOCKS
432
EXCEPTION HANDLER
HORIZONTAL MICROCODE LEVEL
402
GET MACHINE KEY
420
GET LOCK
CHECK LOCK
422
PRODUCT LOCK TABLE
(RAM)
HARDWARE
401
SERIAL NUMBER
421
410
460

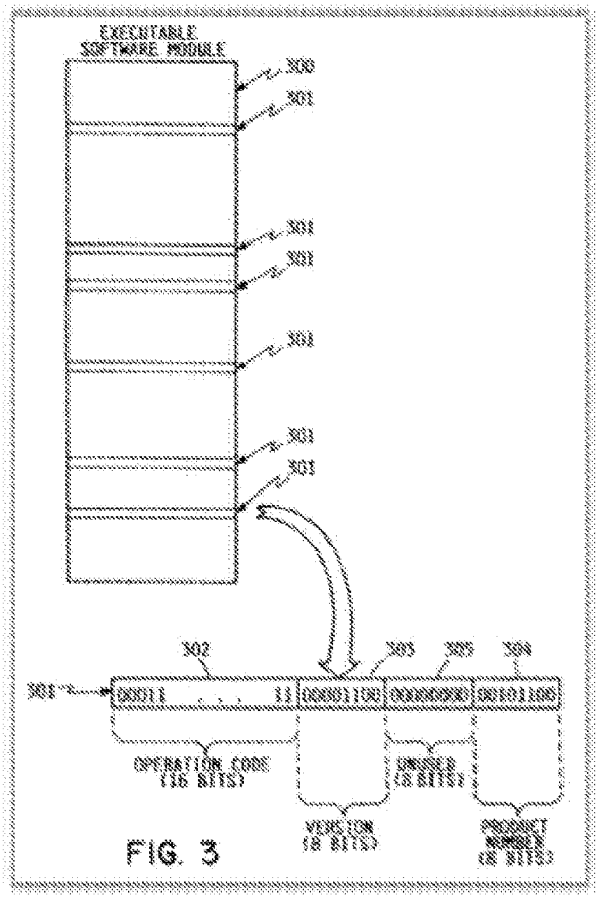


FIG. 3

The '842 Patent refers to sub-objects and a memory scheduler as examples of code resources ('842 Patent at 11:55-65, 15:36-42). APOSITA would have understood that Beetcher's module sub-objects are sub –objects (Silva Declaration at 65-66).

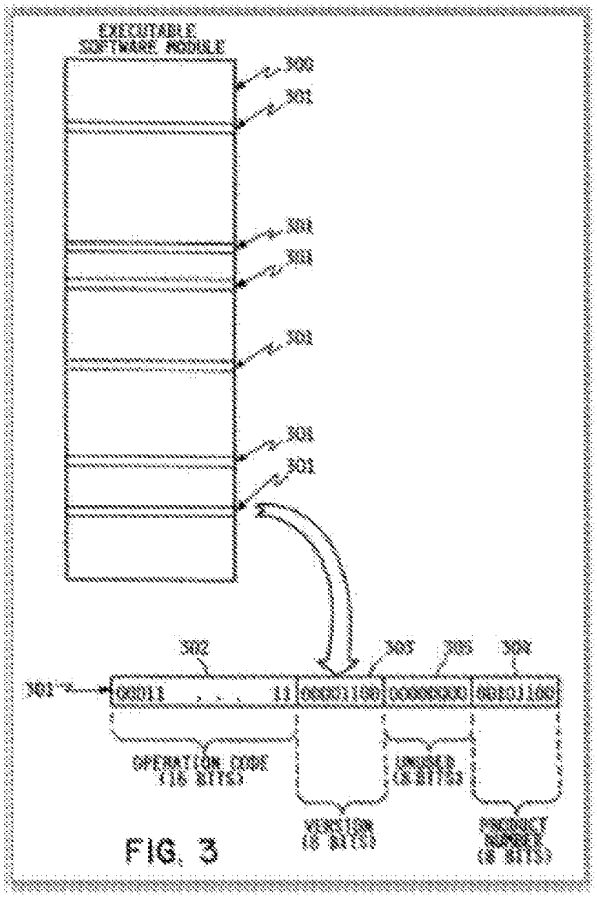
Based on Beetcher's description, a POSITA would have understood that one sub-object in module 300 is a first code resource providing a specified underlying functionality when installed on the customer's computer system 101 and unlocked using the license information (key) (Id. at If 67).

d) Element 12.3: "encoding, by said computer using at least a first license key and an encoding algorithm, said software code, to form a first license key encoded software code"

Beetcher discloses element 12.3. Beetcher describes encoding its software code by the distributor system that includes development system 125 and marketing system 124, which may be "a single computer system performing both functions."(Beetcher at 5:37-58, 6:41-65, 11:4-39) Specifically, Beetcher describes encoding a first license key data into the software code where that key is used to authorize access to the software product:

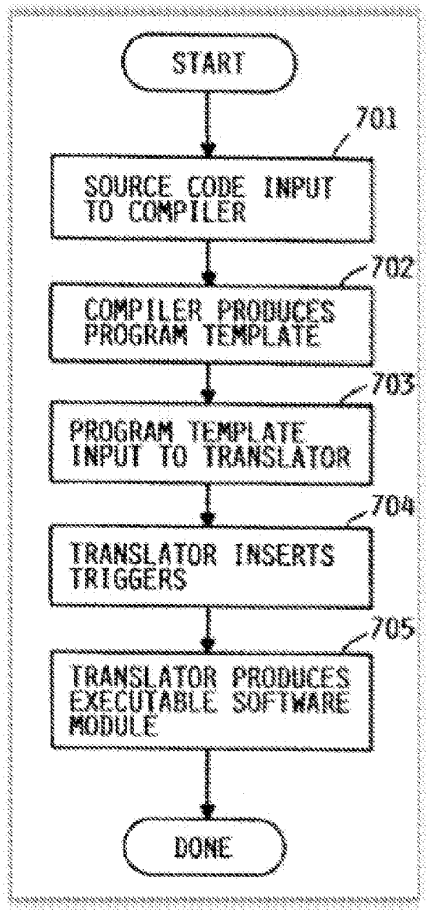
> Software module 300 is part of a program product in compiled object code form which executes on system 101.... [T]he actual executable code operates at executable code level 403, as shown by the box in broken lines. The executable code contains entitlement verification triggering instructions 301 (only one shown), which are executed by horizontal microcode check lock function 422. (Id. at 8:13-23; see also id. at 4:3-21, 6:20-55, 7:39-44, 8:58-67, 9:51-56, 10:22-38)

This encoding is illustrated in Figure 3:



The computer in Beetcher's development system 125 performs the encoding, as shown in Figure 7 at step 704, detailed as: "The program template serves as input to translator 127 at step 704, along with its product number and version number identification. Translator 127 automatically generates a substantial number of entitlement verification triggers, inserts them in random locations in the object code....." (Id. at 9:10-16; see also id< at 5:3'8-47, 9:1-10, 9:16-20, Fig. 7; Silva Declaration at 70-72)

Moreover, the computer in Beetcher's development system 125 uses an encoding algorithm to encode the first license key. Beetcher's system uses a set of instructions, as shown in Figure 7, to encode triggers into the software code to form the first license key : (Beetcher at 9:10-16: see also id. at 5 :38-47, 9:1-1Q, 9:16-20, Fig. 7; Silva Declaration at ¶ 73)



The compiler begins the process by producing a template (step 702), next the template is input into the translator (step 703), then the translator encodes the triggers/license keys into the code (step 704), and finally the translator resolves

references after key insertion to produce the executable module (Beetcher at 9:6-20, Fig. 7). As such, a POSITA would have understood Beetcher's Figure 7 illustrates an encoding algorithm. (Silva Declaration at ¶74) Beetcher's encoding process is further described with respect to element 11.3.

As shown above, Beetcher teaches inserting entitlement verification triggers, using key data such as product / version numbers, into the software and including within these triggers functions of the software itself necessary for the software to properly execute (see 4:25-33, 9:1-48, and 11:4-39). Where these entitlement verification triggers are positioned in the object code with an addressability alignment that has a simple relationship to the product number. The resultant software module is in a specialized format that requires a key to execute (unlock) the software module (see 8:54-67).

Moreover, during the original prosecution, Patent Owner specified that "[e]ncoding using a key and an algorithm is known." (Ex. 2, Prosecution History at 519) As such, a POSITA would have understood that Beetcher's encoding technique necessarily includes a first license key and an encoding algorithm to form a first license key encoded software code (Silva Declaration at 70-75).

e) Element 12.4: "wherein, when installed on a computer system, said first license key encoded software code will provide said specified underlying functionality only after receipt of said first license key"

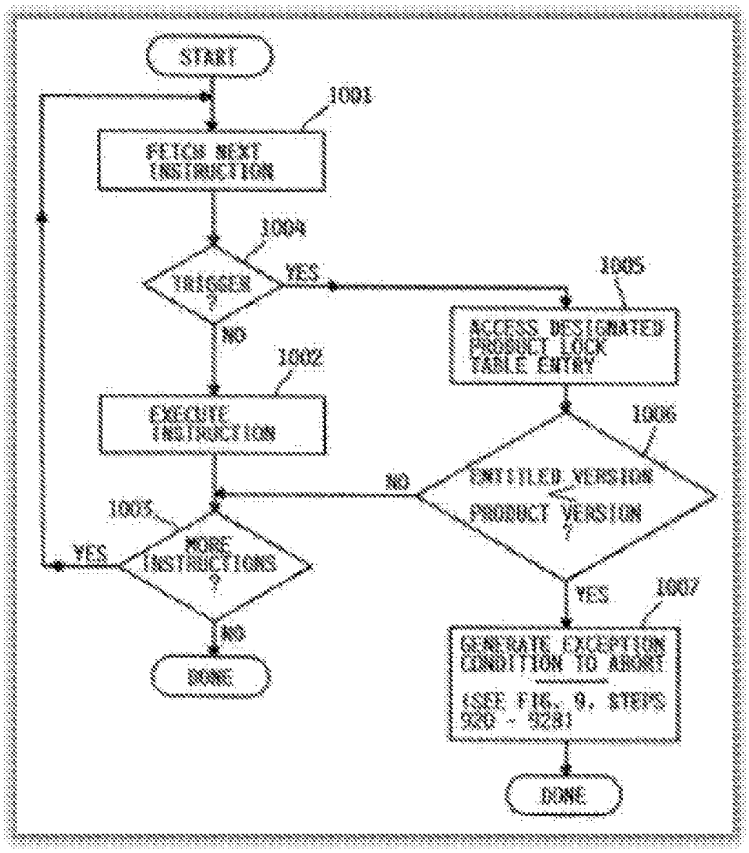
Beetcher discloses element 12.4. Specifically, Beetcher explains that its first license key encoded software code provides the specified underlying functionality only after receipt of the first license key. (Beetcher at 6:58-65, 11:4-39; see also id. at Abstract, 3:14-18, 4:25-33, 6:65-7:5, claim 3) For instance, Beetcher states:

> For support of such a traditional compilation path where the object code format is known by customers, additional barriers to patching of the object code to nullify or alter the entitlement triggering instructions maybe appropriate. One such additional barrier would be to define the entitlement triggering instruction to simultaneously perform some other function. In this case, it is critical that the alternative function performed by the triggering instruction cannot be performed by any other simple instruction. The alternative function must be so selected that any compiled software module will be reasonably certain of containing a number of instructions performing the function. If these criteria are met, the compiler can automatically generate the object code to perform the alternative function (and simultaneously, the entitlement verification trigger) as part of its normal compilation procedure. This definition would provide a significant hairier to patching of the object code to nullify the entitlement triggering instructions. (Id. at 11:10-28)

And as described with respect to element 12.3, Beetcher teaches encoding the triggering instructions into the software code that is unlocked via the first license key.

Beetcher's Figure 10, as provided below, illustrates providing the software's underlying functionality based on the first license key (trigger information). For instance, Beetcher explains:

System 101 executes the module by fetching (step 1001) and executing (step 1002) object code instructions until done (step 1003). If any instruction is an entitlement verification triggering instruction 301 (step 1004) check lock function 422 is invoked. Check lock function 422 accesses the product lock table entry 601 corresponding to the product number contained in the triggering instruction at step 1005. If the version number in product lock table 460 is equal to or greater than the version number 303 contained in triggering instruction 301, the software is entitled to execute (step 1006). (Id. at 10:49-60; see also id. at 10:48-49, 10:60-11:3; Silva Declaration at ¶ 78-82)



Claim 14

a) Preamble: "A method for encoding software code using a computer having a processor and memory, comprising"

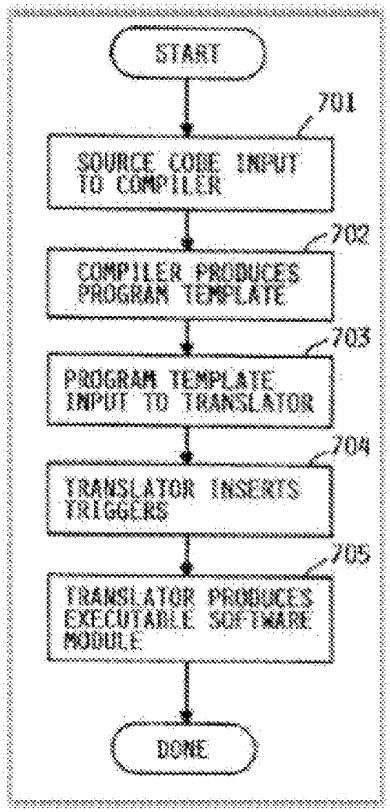
Under the broadest reasonable construction, the preamble is non-limiting. Nevertheless, Beetcher discloses claim 14's preamble. Claim 14's preamble is the same as each of claim 12 and 13's preamble. As explained above, Beetcher discloses a method for encoding software using a computer with a processor and memory. As such, Beetcher teaches this preamble (Id. at ¶ 103).

b) Element 14.1: "storing a software code in said memory"

Beetcher discloses element 12.1. Specifically, Beetcher discloses a development system 125 for compiling and translating for the software code (Beetcher at 5:38-48, 9:1-20). Beetcher details that the software code is stored as disks 112 in warehouse 120. A POSITA would have understood that developer system 125 stores the compiled and translated code in memory and records that code onto disks 112 for distribution to customers. As expert Dr. Silva explains in his declaration (Ex. 9), Beetcher's computer would necessarily include store software code in memory in order to function. (Silva Declaration at ¶ 62) (Id. at ¶ 105).

c) Element 14.2: "wherein said software code defines software code interrelationships between code resources that result in a specified underlying functionality when installed on a computer system"

Beetcher discloses element 14.2. Beetcher details that its software code is compiled into executable code by compiler 126. This compiler works with translator 127 to compile the software sub-objects and insert triggering information (Beetcher at 8:14-17). And Beetcher specifies that translator 127 "resolves references" in the software code, which corresponds to defining code interrelationships between code resources (Id. at 9:11-18; Silva Declaration at ¶ 107). As shown in steps 701 and 702 of Figure 7, Beetcher teaches its software code is input into compiler 126 that produces a template of the software code: (Beetcher at 8:14-17, 9:1-20, Fig. 7; see also id. at 5:37-39, 6:41-45, 7:63-66)



A POSITA would have understood-that this software code template also defines the code interrelationships- between the code resources.164 As the Patent Owner specified during the original prosecution, software code interrelationships are defined during the compiling process of conventional software applications:

> What the examiner has implied by alleging that the "specification ... fails to teach or mention 'software code interrelations hips'" is that software-code interrelationships were somehow unknown in the art, which clearly is not the ease. As admitted, in the specification at the beginning of paragraph [0051], an "application" comprises "sub-objects" whose "order in the computer memory is of vital importance" in order to perform an intended function. And as admitted further in paragraph [0051J. "When a program is compiled, then, it consists of a collection of these sub-objects, whose exact order or arrangement in memory is not important, so long as any sub-object which uses another sub-object knows where in memory it can be found." Paragraph [0051] of course refers to conventional applications. Accordingly, that is admittedly a discussion of what is already know by one skilled in the art. Accordingly, the examiner's statement that the specification lacks written description support for "software code interrelationships" is inconsistent with the fact that such interrelationships were explained in paragraphs [0051] and [0052] as a fundamental basis of preexisting modem computer programs. (Ex. 2, Prosecution History at 519)

Moreover, during the original prosecution, Patent Owner specified that "interrelationships between code resources are not that which is novel." (Id.) Based on Patent Owner's concessions, it is deemed that a POSITA would have understood that Beetcher's code necessarily defines code interrelationships between code resources (Silva Declaration at ¶ 109).

Beetcher further teaches that the code resource interrelationships specify the underlying application functionalities when installed on the customer's computer 101. For instance, Beetcher's software code includes multiple entitlement verification triggers

(Beetcher at 4:15-33, 9:1-3, 10:22-34, Fig. 3; see also id. At 6:45-65, 8:19-22, 10:52-11:39). And Beetcher details that certain code resources include triggering instruction that controls the underlying functionalities of the software code:

> [An] additional barrier would be to define the entitlement triggering instruction to simultaneously perform some other function.... The alternative function must be so selected that any compiled software module will be reasonably certain of containing a number of instructions performing the function. If these criteria are met, the compiler can automatically generate the object code to perform the alternative function (and simultaneously, the entitlement verification trigger) as part of its normal compilation procedure. This definition would provide a significant barrier to patching of the object code to nullify the entitlement triggering instructions. (Id. at 11:14-28; see also id. at 4:25-33, 6:58-65)

Beetcher further explains that "the triggering instruction is also a direct instruction to perform some other useful work .... [E]xecution of the triggering instruction causes system 101 to perform some other operation simultaneous with the entitlement verification." (Id. at 6:58-65 (Beetcher specifies that these functions are those "which do not require that an operand for the action be specified in the instruction.")) As such, a POSITA would have understood that the code interrelationships between Beetcher's code resources result in a specified underlying functionality once installed. (Silvia Declaration at ¶¶ 110-11)

d) Element 14.3: "encoding, by said computer using at least a first license key and an encoding algorithm, said software code, to form a first license key encoded software code"

Beetcher discloses element 12.3. Beetcher describes encoding its software code by the distributor system that includes development system 125 and marketing system 124, which may be "a single computer system performing both functions."(Beetcher at 5:37-58, 6:41-65, 11:4-39) Specifically, Beetcher describes encoding a first license key into the software code where that key is used to authorize access to the software product:

> Software module 300 is part of a program product in compiled object code form which executes on system 101.... [T]he actual executable code operates at executable code level 403, as shown by the box in broken lines. The executable code contains entitlement verification triggering instructions 301 (only one shown), which are executed by horizontal microcode check lock function 422. (Id. at 8:13-23; see also id. at 4:3-21, 6:20-55, 7:39-44, 8:58-67, 9:51-56, 10:22-38)

This encoding is illustrated in Figure 3:

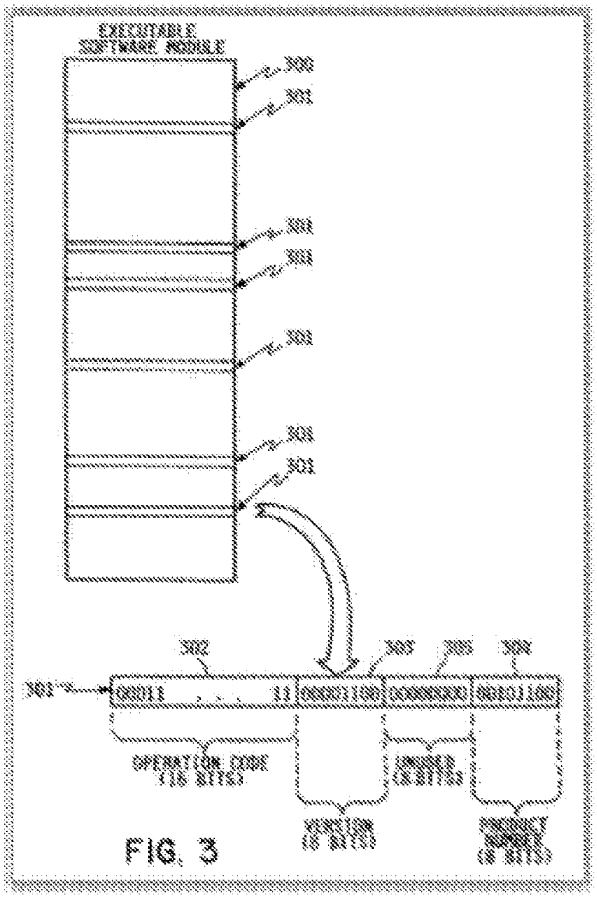
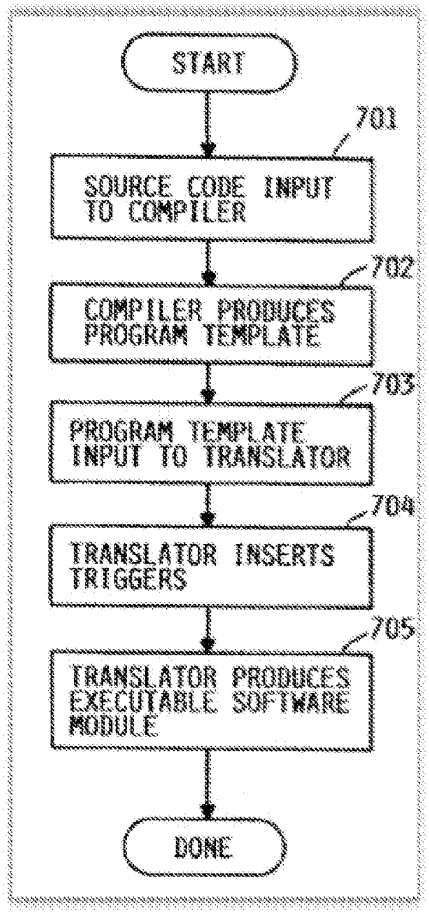


FIG. 3

The computer in Beetcher's development system 125 performs the encoding, as shown in Figure 7 at step 704, detailed as: "The program template selves as input to translator 127 at step 704, along with its product number and version number identification. Translator 127 automatically generates a substantial number of entitlement verification triggers, inserts them in random locations in the object code....." (Id. at 9:10-16; see also id< at 5:3'8-47, 9:1-10, .9:16-20, Fig. 7; Silva Declaration at 70-72)

Moreover, the computer in Beetcher's development system 125 uses an encoding algorithm to encode the first license key. Beetcher's system uses a set of instructions, as shown in Figure 7, to encode triggers into the software code to form the first license key : (Beetcher at 9:10-16: see also id. at 5 :38-47, 9:1-1Q, 9:16-20, Fig. 7; Silva Declaration at ¶ 73)



The compiler begins the process by producing a template (step 702), next the template is input into the translator (step 703), then the translator encodes the triggers/license keys into the code (step 704). And finally the translator resolves

references after key insertion to produce the executable module (Beetcher at 9:6-20, Fig. 7). As such, a POSITA would have understood Beetcher's Figure 7 illustrates an encoding algorithm. (Silva Declaration at ¶74) Beetcher's encoding process is further described with respect to element 11.3.

As shown above, Beetcher teaches inserting entitlement verification triggers, using key data such as product / version numbers, into the software and including within these triggers functions of the software itself necessary for the software to properly execute (see 4:25-33, 9:1-48, and 11:4-39). Where these entitlement verification triggers are positioned in the object code with an addressability alignment what has a simple relationship to the product number. The resultant software module is in a specialized format that requires a key to execute (unlock) the software module (see 8:54-67).

Moreover, during the original prosecution, Patent Owner specified that "[e]ncoding using a key and an algorithm is known." (Ex. 2, Prosecution History at 519) As such, a POSITA would have understood that Beetcher's encoding technique necessarily includes a first license key and an encoding algorithm to form a first license key encoded software code (Silva Declaration at 70-75 and 114-115).

e) Element 14.4: "in which at least one of said software code interrelationships are encoded"

Beetcher discloses element 14.4. As described with respect to element 14.2, Beetcher teaches that its software code defines code interrelationships between code resources and triggering information 301 in the code control certain underlying software functionality. And Beetcher details that triggering information 301 is encoded into the software code. (Beetcher at 4:25-33, 6:58-65, 11:4-39) For instance, Beetcher explains that the triggering instructions will be encoded into the code resources controlling software functionality:

> [An] additional barrier would be to define the entitlement triggering instruction to simultaneously perform some other function.... The alternative function must be so selected that any compiled software module will be reasonably certain of containing a number of instructions performing the function. If these criteria are met, the compiler can automatically generate the object code to perform the alternative function (and simultaneously, the entitlement verification trigger) as part of its normal compilation procedure. This definition would provide a significant barrier to patching of the object code to nullify the entitlement triggering instructions. (Id. at 11:14-28; see also id. at 4:25-33, 6:58-65)

And Beetcher details that "the triggering instruction is also a direct instruction to perform some other useful work .... [E]xecution of the triggering instruction causes system 101 to perform some other operation simultaneous with the entitlement verification." (Id. at 6:58-65 (Beetcher specifies that these functions are those "which do not require that an operand for the action be specified in the instruction.")) Accordingly, a POSITA would have understood that this encoded triggering information includes encoded code interrelationship of the coder resources. (Silva Declaration at ¶ 117-19)

Accordingly, Beetcher discloses claim 14.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Beetcher clearly encodes its software module prior to distribution using key data to lock portions of the software from being executed without the user providing an appropriate key for unlocking said portions. Where the software module code is modified in format to include entitlement verification triggers which themselves are made to encompass functions of the software themselves and so positioned within the object code with an addressability alignment that has a simple relationship to the product number found in the key. This encoding meeting both definitions provided by the Patent Owner:

> "In digital processing, **encode** and **decode** mean **changes in digital representation of information**."
>
> In **computers**, **encoding is** the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding **is** the opposite process -- the conversion of an **encoded** format back into the original sequence of characters. Nov 14, 2005

Beetcher, however, is not as clear with its description of how this encoded software is again accessed. Though Beetcher makes clear that a key is required to access this reformatted content, it doesn't specify whether this key just unlocks the content for use or truly removes the encryption applied (decryption). It is for this reason that Beetcher is deemed ineffective in covering the limitations of claim 11 and claim 13. Given the above cited reason, the lack of further clarification in the other Beetcher

document (Exhibit 3), and the removal of Cooperman (Exhibit 6) and Hasebe (Exhibit 7) as prior art per declarations filed the Patent owner claims 11 and 13 are herein CONFIRMED.

Any comments considered necessary by PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

Response to Arguments

Applicant's arguments filed 2/11/2019 have been fully considered but they are not persuasive. Declarations filed by Scott Moskowitz under 37 CFR 1.131 and 37 CFR 1.132 prove effective in removing the rejections under Cooperman (Exhibit 6) and Hasebe (Exhibit 7), but arguments directed at Beetcher were not effective in removing all the applied rejections.

Arguments directed at Cooperman and Hasebe:

37 CFR 1.131 Declaration

The Declaration filed on 2/11/2019 under 37 CFR 1.131(a) is sufficient to overcome the Cooperman and Hasebe references.

A Declaration under 37 CFR 1.131 was filed by the sole inventor Scott Moskowitz on 2/11/2019, in which Mr. Moskowitz provided evidence to establish both actual and constructive reduction to practice prior to the effective date of the references.

- Mr. Moskowitz states that, on 1/3/1996 he completed a draft disclosure of a patent application with the goal of providing security to executable code (see Attachment 27). The attached document shows on page 4 full support for the claims of the subject patent US 9,104,842 and is dated 1/3/1996 (see page 8).

- Mr. Moskowitz further notes that, on 1/17/1996 an application containing a substantially identical disclosure to that in Attachment 27 was filed with the USPTO (see application number 08/587,943 or Attachment 1). Note: this application is listed for priority within the Cooperman reference. However, Attachment 27 proves that the work was that of Mr. Moskowitz.

MPEP 715.01(a) states in part:

> When subject matter disclosed in a patent or patent application publication (reference) naming an inventive entity including inventor S and another joint inventor is claimed in a later application naming inventor S without the joint inventor, the reference may be properly applied under pre-AIA 35 U.S.C. 102(a), (e), or (f) until overcome by an affidavit or declaration under 37 CFR 1.131(a) showing prior invention (see MPEP § 715) or by an affidavit or declaration under 37 CFR 1.132. An unequivocal declaration under 37 CFR 1.132 by S that he/she conceived or invented the subject matter that was disclosed but not claimed in the patent or application publication and relied on in the rejection has been sufficient to overcome the rejection. *In re DeBaun,* 687 F.2d 459, 214 USPQ 933 (CCPA 1982). However, if the affidavit or declaration under 37 CFR 1.132 is only a naked assertion of inventorship, which occurred long ago, by an inventor who has an interest at stake and it fails to provide any context, explanation or evidence to support that assertion, documentary evidence contemporaneous with the invention may be needed to provide some degree of corroboration. See *EmeraChem Holdings, LLC v. Volkswagen Grp. of Am., Inc.*, 859 F.3d 1341, 123 USPQ2d 1146 (Fed. Cir. 2017) (The court found the declaration submitted by inventor Campbell more than twenty years after the invention insufficient to establish that he and Mr. Guth (deceased) were the inventors of the subject matter disclosed in a patent naming Campbell, Guth, Danziger, and Padron as inventors.). Where the reference is a U.S. patent or patent application publication which includes a claim reciting the subject matter relied upon in a rejection and that subject matter anticipates or would render obvious the subject matter of a claim in the application under examination, a declaration under 37 CFR 1.132 must also explain the presence of the additional inventor in the reference (e.g., the disclosure in claim 1 of the reference is relied upon to reject the claims; the affidavit or declaration explains that S is the sole inventor of claim 1, and the additional

inventor and S are joint inventors of claim 2 of the reference). Testimony or disclaimer from the other inventor(s) named in the reference is usually not required but, if submitted, should be considered by the examiner.

In this situation where the Patent Owner is attempting to remove a reference by an inventive entity including the Patent Owner, Mr. Moskowitz has shown both that he (Mr. Moskowitz) alone previously disclosed the invention, and further provided Attachment 27 as documentary evidence contemporaneous with the invention.

The Patent Owner has shown the above in the 1.131 Declaration. It is noted that "*affidavits or declarations submitted for the purpose of establishing that the reference discloses inventor's or at least one joint inventor's invention are properly filed under 37 CFR 1.132, rather than 37 CFR 1.131(a), such affidavits submitted improperly under 37 CFR 1.131(a) will be considered as though they were filed under 37 CFR 1.132 to traverse a ground of rejection. In re Facius, 408 F.2d 1396, 161 USPQ 294 (CCPA 1969).*" (see MPEP 715.01(a))

The above facts and supporting documentation are effective in establishing invention of the subject matter of the rejected claims prior to the effective date of the references (Cooperman 7/24/1997 and Hasebe 7/1/1996) and by Mr. Moskowitz.

Note: Mr. Cooperman has further been shown to have surrendered any rights to US Patent 9,104,842 to the Patent Owner as per settlement agreement set forth in

Attachment 7 directed at the PCT relied upon in the rejection (specifically, page 17, 2.2, 2.5).

37 CFR 1.132 Declaration of Scott Moskowitz

The 37 CFR 1.132 Declaration of Scott Moskowitz is substantially a copy of the arguments presented within the Response document with all contentions against the rejection listed and answered below.

Arguments directed at Beetcher:

Overarching principle of Beetcher:

The Problem, identified in Beetcher, was distributed software could be executed by anyone in possession of the software or a copy of the software.

The Solution was to insert entitlement verification triggers (including key data such as product / version numbers) into the software and including within these triggers functions of the software itself necessary for the software to properly execute (see 4:25-33 and 11:4-39). Where these entitlement verification triggers are positioned in the object code with an addressability alignment that has a simple relationship to the product number (later distributed within the key).

This software being in a specialized format that requires a key to execute (unlock) a software module (see 8:54-67).

How Beetcher utilized encoded content:

The way a key enables execution of the modified object code is by setting entitlements for software modules in an encoded product key table. When software is executing object code is executed until an entitlement verification triggering instruction 301 is encountered, then a check lock function is invoked. The check lock function accesses the product lock table entry corresponding to the product number contained in the triggering instruction and if the version number in the product lock table is equal to or greater than the version number contained in the triggering instruction the software is entitled to execute, otherwise program execution is terminated. (see 10:48-65)

-in other words a comparison is done between content of the software module and key to determine permission to execute, and if enabled program execution continues as normal, by removing the barrier to normal execution applied in the above described encoding.

In column 11, lines 4-59, Beetcher shows an alternate method of incorporating entitlement triggering instructions in the object code providing additional sophistication. Where they are placed either by their relationship to a product number (encoding scheme) and/or inserted with additional code to perform some other function (alternate encoded feature); where these schemes are used to further protect the code from patching. Here the product number used for encoding is separately provided via the entitlement key used to unlock the hidden code element.

Here Beetcher recognizes that if the object code is in a 'format… known to customers' there is a need to add 'additional sophistication' to the object code to create an additional barrier to patching the object code that would nullify the entitlements (specifically see 11:4-15). To protect against this Beetcher's entitlement triggering instructions are injected into the object code through a non-traditional compilation path, thereby creating a 'significant barrier to patching', with the trigging instructions further including functionality important for the software module to properly execute (specifically see 11:15-28 and 4:14-33). Here Beetcher places the object code into a specialized format where entitlement triggering instructions are positioned in the object code with an addressability alignment that has a simple relationship to the product number it identifies (see specifically 11:18-39).

This placing object code / triggering instructions into a specialized format for transmission to customers aligns with the definition of 'encoding' as provided by the Patent Owner:

> In **computers**, **encoding is** the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding **is** the opposite process -- the conversion of an **encoded** format back into the original sequence of characters. Nov 14, 2005

Claim 11

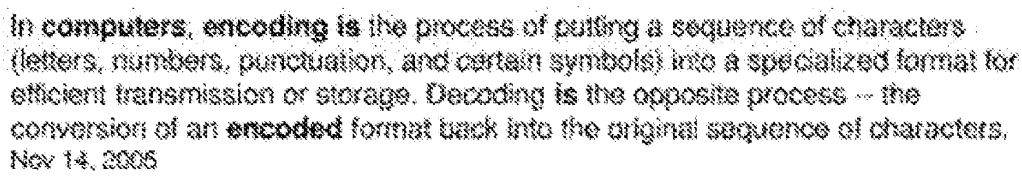
Beetcher clearly encodes its software module prior to distribution using key data to lock portions of the software from being executed without the user providing an

appropriate key for unlocking said portions. Where the software module code is modified in format to include entitlement verification triggers which themselves are made to encompass functions of the software themselves and so positioned within the object code with an addressability alignment that has a simple relationship to the product number found in the key. This encoding meeting both definitions provided by the Patent Owner:

(1)

"In digital processing, **encode** and **decode** mean **changes in digital representation of information**."

(2)


In **computers**, **encoding is** the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding **is** the opposite process -- the conversion of an **encoded** format back into the original sequence of characters. Nov 14, 2006

Beetcher, however, is not as clear with its description of how this encoded software is again accessed. Though Beetcher makes clear that a key is required to access this reformatted content, it doesn't specify whether this key just unlocks the content for use or truly removes the encryption applied (decryption). **It is for this reason that Beetcher is deemed ineffective in covering the limitations of claim 11 (and claim 13) and is herein confirmed.**

The Examiner nevertheless still address below relevant arguments directed at claim 11:

VII.2.3.

Patent Owner argues that "Beetcher contains no disclosure indicating that Beetcher's entitlement key is part of Beetcher's installed software module."

In response, the Examiner respectfully agrees, but notes that components of the key are stored in the software in the code of the software module. Specifically, the product number and version number both make up parts of the key and parts of the entitlement verification triggers in the object code / software module (see column 9, lines 1-48).

VII.3.2. - VII.3.3.

Patent Owner presents that *"Claim 11 requires "license information" be "input in response to said prompt" by the software product loaded on the computer. That follows from claim 11's limitation "loading a software product on a computer." It follows necessarily because the sequence of claimed steps, loading, prompting, and then using, are predicated on the occurrence of the earlier steps. The software product cannot prompt, unless it has been loaded. The software product cannot use information input in response to a prompt, unless the prompt has already occurred which means the software has already been loaded. Therefore, claim 11 defines a process in which the licensing information input in response to the prompt is not part of the loaded software product."*

…

"Thus, Beetcher's installed software module does not include encrypted entitlement key 111. Therefore, Beetcher's encrypted entitlement key 111 (input in response to

Beetcher's prompt) and its unencrypted version of the key and information therefrom that is stored in memory do not correspond to claim 11's loaded software product."

In response, the Examiner again agrees that the software module does not include the encrypted entitlement key, but rather the software module's object code is placed into a specialized format with defined addressability alignment of its embedded entitlement verification triggering instructions 301 that the entitlement key unlocks to make usable. Here the encoding / specialized formatting / positioning according to addressability alignment is based upon the product number resident in both the entitlement verification triggering instructions 301 and the entitlement key 111 (used to identify and unlock the software). (see 11:28-39)

VII.4

Here the Patent Owner argues a different definition for 'encoding' and 'decoding', presenting that:

"In digital processing, **encode** and **decode** mean **changes in digital representation of information**."

The Examiner believes this is important as what nearly all arguments are focused around is whether Beetcher teaches encoding of the software module (that asks for key input) and subsequent unlocking of the software module using the key.

-encode

The Examiner can't see how the Patent Owner is arguing that the software module is not encoded, given the software / object code is modified from a "format (is) known by customers" to include "barriers to patching of the object code". Such as (1) to have inserted entitlement triggering instructions themselves include critical functions of the software or (2) to have the entitlement triggers inserted in the software in positions with an "addressability alignment that has a simple relationship to the product number they identify" during compilation. (see 11:28-39)

-decode

On the other end surely it is clear that this encoded software would need some function performed on it from its protected state to be usable for its intended purpose, where the Beetcher invention purpose is the providing of this key separate from the software that enables execution of previously blocked / encoded code segments. Where, as previously noted, these keys include the product number that the object code was reformatted according to ("instructions must be positioned in the object code with an addressability alignment that has a simple relationship to the product number that it identifies"). Having the key (which includes the product number) makes addressability alignment known thereby enabling unlocking of the code, albeit by leaving the code in the encoded state while selectively enabling execution of enabled portions.

Additionally, the Patent Owner presents a definition for 'routine', presenting that:

"a "routine" defines a section of a computer program that performs a particular task"

Here, though some of the Check Lock Function may be resident code it uses content about set locks from the Software Module and Keys in the comparison that determines if a particular object code instruction is locked (see column 10, lines 40-65).

Claim 12

VII.9

Patent Owner argues that "Beetcher does not disclose key based encoding to form its software module."

In response, the Examiner respectfully submits that Beetcher teaches insert entitlement verification triggers (including key data such as product / version numbers) into the software and including within these triggers functions of the software itself necessary for the software to properly execute (see 4:25-33, 9:1-48, and 11:4-39). Where these entitlement verification triggers are positioned in the object code with an addressability alignment what has a simple relationship to the product number. The resultant software module is in a specialized format that requires a key to execute (unlock) the software module (see 8:54-67).

Furthermore, during the original prosecution, Patent Owner specified that "[e]ncoding using a key and an algorithm is known." (Ex. 2, Prosecution History at 519)

As such, a POSITA would have understood that Beetcher's encoding technique necessarily includes a first license key and an encoding algorithm to form a first license key encoded software code (Silva Declaration at 70-75).

Patent Owner argues that "Beetcher teaches conventional compiling of its high level code, followed by inserting instructions 301 at various locations therein, and then followed by resolving the references (addresses) in the compiled code caused by the insertion of instances of instructions 301. Beetcher does not teach key based encoding to form its software module. Accordingly, Beetcher does not anticipate claim 12."

In response, the Examiner respectfully submits that, as previously noted, Beetcher is not limited to simple insertion of instructions, but rather these instructions are made to encompass functionality important for the software module to properly execute (specifically see 11:15-28 and 4:14-33). Here Beetcher places the object code into a specialized format where entitlement triggering instructions are positioned in the object code with an addressability alignment that has a simple relationship to the product number it identifies (see specifically 11:18-39).

This placing object code / triggering instructions into a specialized format for transmission to customers aligns with the definition of 'encoding' as provided by the Patent Owner:

In **computers**, **encoding is** the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding **is** the opposite process -- the conversion of an **encoded** format back into the original sequence of characters. Nov 14, 2005

VII.11

Patent Owner argues that "Beetcher's software module 300 does not receive Beetcher's instruction 301 after being installed on Beetcher's customer computer 101. Therefore, Beetcher's instruction 301 does not correspond to claim 12's receipt of a first license key."

In response, the Examiner respectfully submits that this argument appears to be confusing Beetcher's entitlement verification triggers 301 for Beetcher's keys 111. Beetcher inserts entitlement verification triggers within the software code (see 301 from figure 4), where these are created from content of the key, but are not the key itself. Rather they are unlockable via a separately transmitted key 111 (shown separately in figure 4). Though generation of the software code utilizes information in the entitlement key, the entitlement key information is separately transmitted to the destination system (similar to claim 1), where only after receipt of the key can protected software modules be executed (see column 10, line 47 through column 11, line 3). "Products are unlocked on demand". Furthermore when re-initialization occurs the keys are check again against a rebuilt product lock table (see column 10, lines 20-46).

Patent Owner argues that "Beetcher Does Not Disclose Instruction 301 is a "first license key," as Defined by Claim 12

…

Beetcher discloses that instruction 301 stores software version information, not a license key. And Beetcher discloses that the same software module 300 is distributed to

all of its customers containing this generic instruction 301. Accordingly, corresponding instruction 301 to a license key that must be received by the installed software program is incorrect for this additional reason."

In response, the Examiner respectfully submits that Beetcher's entitlement verification triggering instructions 301 are not argued by the 3PR nor the Examiner to correspond directly to the "first license key", but rather the entitlement verification triggering instructions 301 are shown to contain similar information (namely product # / version #) to the key. Here the software module is "translated" to a different format where entitlement triggers are inserted into the object code including key information (product # / version #) that is later used to unlock or enable regular execution (how it would operate without inserted triggers). (see column 9, lines 1-48)

Claim 13

Claim 13 is confirmed for reasons similar to those described with respect to claim 11.

Claim 14

VIII.16

Claim 14 is only argued for "the same reasons stated for claim 12". Accordingly, the responses provided above to the Patent Owner's contentions hold equally applicable here.

Summary

Claims 12 and 14 are **REJECTED**.

Claims 11 and 13 are **CONFIRMED**.

Litigation Reminder

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent Number: 9,104,842 throughout the course of this reexamination proceeding. The third part requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

Conclusion

THIS ACTION IS MADE FINAL.

A shortened statutory period for response to this action is set to expire 2 from the mailing date of this action.

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

Extensions of time in reexamination proceedings are provided for in 37 CFR 1.550(c). A request for extension of time must be filed on or before the day on which a response to this action is due, and it must be accompanied by the petition fee set forth in 37 CFR 1.17(g). The mere filing of a request will not affect any extension of time. An extension of time will be granted only for sufficient cause, and for a reasonable time specified.

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

By Mail to: Mail Stop Ex Parte Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via

the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/DENNIS G BONSHOCK/
Primary Examiner, Art Unit 3992

Conferee:

/ADAM L BASEHOAR/
Primary Examiner, Art Unit 3992

/ALEXANDER J KOSOWSKI/
Supervisory Patent Examiner, Art Unit 3992

Office Action in Ex Parte Reexamination	**Control No.** 90/014,138	**Patent Under Reexamination** 9104842	
	Examiner DENNIS G BONSHOCK	**Art Unit** 3992	**AIA Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

a. ☑ Responsive to the communication(s) filed on 11 February 2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☑ This action is made FINAL.

c. ☐ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892.
2. ☑ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 11-14 are subject to reexamination.
1b. ☑ Claims 1-10 are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☑ Claims 11 and 13 are patentable and/or confirmed.
4. ☑ Claims 12 and 14 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____.
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ **Patent Owner** ☑ **Third Party**

Joseph F. Edell
Fisch Sigler LLP
5301 Wisconsin Ave, NW
Fourth Floor
Washington, DC 20015

LITIGATION REVIEW ☑	/DGB/ (examiner initials)	2018-06-13T00:00:00 (date)
Case Name		Director Initials
6:17cv16		
6:18cv174		
6:18cv181		
6:18cv195		
6:18cv223		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Previous Prosecution Searched	12/6/2018	DGB
litigation Searched	12/6/2018	DGB

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

DISH-Blue Spike 842
Exhibit 1005, Page 1612

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF UNITED STATES PATENTS - U series

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 01	3947825	March 1976	Cassada	X
	U 02	3984624	October 1976	Waggener	X
	U 03	3986624	October 1976	Cates, Jr. et al.	X
	U 04	4038596	July 1977	Lee	X
	U 05	4200770	April 1980	Hellman et al.	X
	U 06	4218582	August 1980	Hellman et al.	X
	U 07	4339134	July 1982	Macheel	X
	U 08	4390898	June 1983	Bond et al.	X
	U 09	4405829	September 1983	Rivest et al.	X
	U 010	4424414	January 1984	Hellman et al.	X
	U 011	4528588	July 1985	Lofberg	X
	U 012	4672605	June 1987	Hustig et al.	X
	U 013	4748668	May 1988	Shamir et al.	X
	U 014	4789928	December 1988	Fujisaki	X
	U 015	4827508	May 1989	Shear	X
	U 016	4876617	October 1989	Best et al.	X
	U 017	4896275	January 1990	Jackson	X
	U 018	4908873	March 1990	Philibert et al.	X
	U 019	4939515	July 1990	Adelson	X
	U 020	4969204	November 1990	Melnychuk et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 021	4972471	November 1990	Gross et al.	X
	U 022	4977594	December 1990	Shear	X
	U 023	4979210	December 1990	Nagata et al.	X
	U 024	4980782	December 1990	Ginkel	X
	U 025	5050213	September 1991	Shear	X
	U 026	5073925	December 1991	Nagata et al.	X
	U 027	5077665	December 1991	Silverman et al.	X
	U 028	5113437	May 1992	Best et al.	X
	U 029	5136581	August 1992	Muehrcke	X
	U 030	5136646	August 1992	Haber et al.	X
	U 031	5136647	August 1992	Haber et al.	X
	U 032	5142576	August 1992	Nadan	X
	U 033	5161210	November 1992	Druyvesteyn et al.	X
	U 034	5210820	May 1993	Kenyon	X
	U 035	5243423	September 1993	DeJean et al.	X
	U 036	5243515	September 1993	Lee	X
	U 037	5287407	February 1994	Holmes	X
	U 038	5319735	June 1994	Preuss et al.	X
	U 039	5341429	August 1994	Stringer et al.	X
	U 040	5341477	August 1994	Pitkin et al.	X
	U 041	5363448	November 1994	Koopman et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 042	5365586	November 1994	Indeck et al.	X
	U 043	5369707	November 1994	Follendore, III	X
	U 044	5379345	January 1995	Greenberg	X
	U 045	5394324	February 1995	Clearwater	X
	U 046	5398285	March 1995	Borgelt et al.	X
	U 047	5406627	April 1995	Thompson et al.	X
	U 048	5408505	April 1995	Indeck et al.	X
	U 049	5410598	April 1995	Shear	X
	U 050	5412718	May 1995	Narasimhalv et al.	X
	U 051	5418713	May 1995	Allen	X
	U 052	5428606	June 1995	Moskowitz	X
	U 053	5450490	September 1995	Jensen et al.	X
	U 054	5469536	November 1995	Blank	X
	U 055	5471533	November 1995	Wang et al.	X
	U 056	5478990	December 1995	Montanari et al.	X
	U 057	5479210	December 1995	Cawley et al.	X
	U 058	5487168	January 1996	Geiner et al.	X
	U 059	5493677	February 1996	Balogh et al.	X
	U 060	5497419	March 1996	Hill	X
	U 061	5506795	April 1996	Yamakawa	X
	U 062	5513126	April 1996	Harkins et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 063	5513261	April 1996	Maher	X
	U 064	5530739	June 1996	Okada	X
	U 065	5530751	June 1996	Morris	X
	U 066	5530759	June 1996	Braudaway et al.	X
	U 067	5539735	July 1996	Moskowitz	X
	U 068	5548579	August 1996	Lebrun et al.	X
	U 069	5568570	October 1996	Rabbani	X
	U 070	5579124	November 1996	Aijala et al.	X
	U 071	5581703	December 1996	Baugher et al.	X
	U 072	5583488	December 1996	Sala et al.	X
	U 073	5598470	January 1997	Cooper et al.	X
	U 074	5606609	February 1997	Houser et al.	X
	U 075	5613004	March 1997	Cooperman et al.	X
	U 076	5617119	April 1997	Briggs et al.	X
	U 077	5625690	April 1997	Michel et al.	X
	U 078	5629980	May 1997	Stefik et al.	X
	U 079	5633932	May 1997	Davis et al.	XX
	U 080	5634040	May 1997	Her et al.	X
	U 081	5636276	June 1997	Brugger	X
	U 082	5636292	June 1997	Rhoads	X
	U 083	5640569	June 1997	Miller et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 084	5646997	July 1997	Barton	X
	U 085	5657461	August 1997	Harkins et al.	X
	U 086	5659726	August 1997	Sandford, II et al.	X
	U 087	5664018	September 1997	Leighton	X
	U 088	5673316	September 1997	Auerbach et al.	X
	U 089	5677952	October 1997	Blakely et al.	X
	U 090	5680462	October 1997	Miller et al.	X
	U 091	5687236	November 1997	Moskowitz et al.	X
	U 092	5689587	November 1997	Bender et al.	X
	U 093	5696828	December 1997	Koopman, Jr.	X
	U 094	5719937	February 1998	Warren et al.	X
	U 095	5721788	February 1998	Powell et al.	X
	U 096	5734752	March 1998	Knox	X
	U 097	5737416	April 1998	Cooper et al.	X
	U 098	5737733	April 1998	Eller	X
	U 099	5740244	April 1998	Indeck et al.	X
	U 0100	5745569	April 1998	Moskowitz et al.	X
	U 0101	5748783	May 1998	Rhoads	X
	U 0102	5751811	May 1998	Magnotti et al.	X
	U 0103	5754697	May 1998	Fu et al.	X
	U 0104	5757923	May 1998	Koopman, Jr.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0105	5765152	June 1998	Erickson	X
	U 0106	5768396	June 1998	Sone	X
	U 0107	5774452	June 1998	Wolosewicz	X
	U 0108	5790677	August 1998	Fox et al.	X
	U 0109	5799083	August 1998	Brothers et al.	X
	U 0110	5809139	September 1998	Grirod et al.	X
	U 0111	5809160	September 1998	Powell et al.	X
	U 0112	5822432	October 1998	Moskowitz et al.	X
	U 0113	5828325	October 1998	Wolosewicz et al.	X
	U 0114	5832119	November 1998	Rhoads	X
	U 0115	5848155	December 1998	Cox	X
	U 0116	5850481	December 1998	Rhoads	X
	U 0117	5859920	January 1999	Daly et al.	X
	U 0118	5860099	January 1999	Milios et al.	X
	U 0119	5862260	January 1999	Rhoads	X
	U 0120	5870474	February 1999	Wasilewski et al.	X
	U 0121	5884033	March 1999	Duvall et al.	X
	U 0122	5889868	March 1999	Moskowitz et al.	X
	U 0123	5893067	April 1999	Bender et al.	X
	U 0124	5894521	April 1999	Conley	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0125	5903721	May 1999	Sixtus	X
	U 0126	5905800	May 1999	Moskowitz et al.	X
	U 0127	5905975	May 1999	Ausubel	X
	U 0128	5912972	June 1999	Barton	X
	U 0129	5915027	June 1999	Cox et al.	X
	U 0130	5917915	June 1999	Hirose	X
	U 0131	5918223	June 1999	Blum	X
	U 0132	5920900	July 1999	Poole et al.	X
	U 0133	5923763	July 1999	Walker et al.	X
	U 0134	5930369	July 1999	Cox et al.	X
	U 0135	5930377	July 1999	Powell et al	. X
	U 0136	5940134	August 1999	Wirtz	X
	U 0137	5943422	August 1999	Van Wie et al.	X
	U 0138	5963909	October 1999	Warren et al.	X
	U 0139	5973731	October 1999	Schwab	X
	U 0140	5974141	October 1999	Saito	X
	U 0141	5991426	November 1999	Cox et al.	X
	U 0142	5999217	December 1999	Berners-Lee	X
	U 0143	6009176	December 1999	Gennaro et al.	X
	U 0144	6029126	February 2000	Malvar	X
	U 0145	6041316	March 2000	Allen	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0146	6044471	March 2000	Colvin	X
	U 0147	6049838	April 2000	Miller et al.	X
	U 0148	6051029	April 2000	Paterson et al.	X
	U 0149	6061793	May 2000	Tewfik et al.	X
	U 0150	6069914	May 2000	Cox	X
	U 0151	6078664	June 2000	Moskowitz et al.	X
	U 0152	6081251	June 2000	Sakai et al.	X
	U 0153	6081587	June 2000	Reyes et al.	X
	U 0154	6088455	July 2000	Logan et al.	X
	U 0155	6131162	October 2000	Yoshiura et al.	X
	U 0156	6141753	October 2000	Zhao et al.	X
	U 0157	6141754	October 2000	Choy	X
	U 0158	6154571	November 2000	Cox et al.	X
	U 0159	6192138	February 2001	Yamadaji	X
	U 0160	6199058	March 2001	Wong et al.	X
	U 0161	6205249	March 2001	Moskowitz	X
	U 0162	6208745	March 2001	Florenio et al.	X
	U 0163	6230268	May 2001	Miwa et al.	X
	U 0164	6233347	May 2001	Chen et al.	X
	U 0165	6233684	May 2001	Stefik et al.	X
	U 0166	6240121	May 2001	Senoh	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0167	6263313	July 2001	Milstead et al.	X
	U 0168	6272634	August 2001	Tewfik et al.	X
	U 0169	6275988	August 2001	Nagashima et al.	X
	U 0170	6278780	August 2001	Shimada	X
	U 0171	6278791	August 2001	Honsinger et al.	X
	U 0172	6282300	August 2001	Bloom et al.	X
	U 0173	6282650	August 2001	Davis	X
	U 0174	6285775	September 2001	Wu et al.	X
	U 0175	6301663	October 2001	Kato et al.	X
	U 0176	6310962	October 2001	Chung et al.	X
	U 0177	6330335	December 2001	Rhoads	X
	U 0178	6330672	December 2001	Shur	X
	U 0179	6345100	February 2002	Levine	X
	U 0180	6351765	February 2002	Pietropaolo et al.	X
	U 0181	6363483	March 2002	Keshav	X
	U 0182	6373892	April 2002	Ichien et al.	X
	U 0183	6373960	April 2002	Conover et al.	X
	U 0184	6374036	April 2002	Ryan et al.	X
	U 0185	6377625	April 2002	Kim	X
	U 0186	6381618	April 2002	Jones et al.	X
	U 0187	6381747	April 2002	Wonfor et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0188	6385329	May 2002	Sharma et al.	X
	U 0189	6389538	May 2002	Gruse et al.	X
	U 0190	6405203	June 2002	Collart	X
	U 0191	6415041	July 2002	Oami et al.	X
	U 0192	6425081	July 2002	Iwamura	X
	U 0193	6430301	August 2002	Petrovic	X
	U 0194	6430302	August 2002	Rhoads	X
	U 0195	6442283	August 2002	Tewfik et al.	X
	U 0196	6446211	September 2002	Colvin	X
	U 0197	6453252	September 2002	Laroche	X
	U 0198	6457058	September 2002	Ullum et al.	X
	U 0199	6463468	October 2002	Buch et al.	X
	U 0200	6484264	November 2002	Colvin	X
	U 0201	6493457	December 2002	Quackenbush	X
	U 0202	6502195	December 2002	Colvin	X
	U 0203	6522767	February 2003	Moskowitz et al.	X
	U 0204	6522769	February 2003	Rhoads et al.	X
	U 0205	6523113	February 2003	Wehrenberg	X
	U 0206	6530021	March 2003	Epstein et al.	X
	U 0207	6532284	March 2003	Walker et al.	X
	U 0208	6539475	March 2003	Cox et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0209	6557103	April 2003	Boncelet, Jr. et al.	X
	U 0210	6584125	June 2003	Katto	X
	U 0211	6587837	July 2003	Spagna et al.	X
	U 0212	6598162	July 2003	Moskowitz	X
	U 0213	6606393	August 2003	Xie et al.	X
	U 0214	6647424	November 2003	Pearson et al.	X
	U 0215	6658010	December 2003	Enns et al.	X
	U 0216	6665489	December 2003	Collart	X
	U 0217	6668246	December 2003	Yeung et al.	X
	U 0218	6668325	December 2003	Collberg et al	. X
	U 0219	6687683	February 2004	Harada et al.	X
	U 0220	6725372	April 2004	Lewis et al	. X
	U 0221	6754822	June 2004	Zhao	X
	U 0222	6775772	August 2004	Binding et al.	X
	U 0223	6784354	August 2004	Lu et al.	X
	U 0224	6785815	August 2004	Serret-Avila et al.	X
	U 0225	6785825	August 2004	Colvin	X
	U 0226	6792548	September 2004	Colvin	X
	U 0227	6792549	September 2004	Colvin	X
	U 0228	6795925	September 2004	Colvin	X
	U 0229	6799277	September 2004	Colvin	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0230	6813717	November 2004	Colvin	X
	U 0231	6813718	November 2004	Colvin	X
	U 0232	6823455	November 2004	Macy et al.	X
	U 0233	6834308	December 2004	Ikezoye et al.	X
	U 0234	6842862	January 2005	Chow et al.	X
	U 0235	6853726	February 2005	Moskowitz et al.	X
	U 0236	6857078	February 2005	Colvin	X
	U 0237	6931534	August 2005	Jandel et al.	X
	U 0238	6966002	November 2005	Torrubia-Saez	X
	U 0239	6983337	November 2005	Wold	X
	U 0240	6977894	December 2005	Achilles et al.	X
	U 0241	6978370	December 2005	Kocher	X
	U 0242	6986063	January 2006	Colvin	X
	U 0243	7007166	February 2006	Moskowitz et al.	X
	U 0244	7020285	March 2006	Kirovski et al.	X
	U 0245	7035409	April 2006	Moskowitz	X
	U 0246	7043050	May 2006	Yuval	X
	U 0247	7046808	May 2006	Metois et al.	X
	U 0248	7050396	May 2006	Cohen et al.	X
	U 0249	7051208	May 2006	Venkatesan et al.	X
	U 0250	7058570	June 2006	Yu et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0251	7093295	August 2006	Saito	X
	U 0252	7095874	August 2006	Moskowitz et al	. X
	U 0253	7103184	September 2006	Jian	X
	U 0254	7107451	September 2006	Moskowitz	X
	U 0255	7123718	October 2006	Moskowitz et al.	X
	U 0256	7127615	October 2006	Moskowitz	X
	U 0257	7150003	December 2006	Naumovich et al.	X
	U 0258	7152162	December 2006	Moskowitz et al.	X
	U 0259	7159116	January 2007	Moskowitz	X
	U 0260	7162642	January 2007	Schumann et al.	X
	U 0261	7177429	February 2007	Moskowitz et al.	X
	U 0262	7177430	February 2007	Kim	X
	U 0263	7206649	April 2007	Kirovski et al.	X
	U 0264	7231524	June 2007	Bums	X
	U 0265	7233669.	June 2007	Candelore	X
	U 0266	7240210	July 2007	Michak et al.	X
	U 0267	7266697	September 2007	Kirovski et al	. X
	U 0268	7287275	October 2007	Moskowitz	X
	U 0269	7289643	October 2007	Brunk et al.	X
	U 0270	7343492	March 2008	Moskowitz et al.	X
	U 0271	7346472	March 2008	Moskowitz et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0272	7362775	April 2008	Moskowitz	X
	U 0273	7363278	April 2008	Schmelzer et al.	X
	U 0274	7409073	August 2008	Moskowitz et al.	X
	U 0275	7457962	November 2008	Moskowitz	X
	U 0276	7460994	December 2008	Herre et al.	X
	U 0277	7475246	January 2009	Moskowitz	X
	U 0278	7530102	May 2009	Moskowitz	X
	U 0279	7532725	May 2009	Moskowitz et al.	X
	U 0280	7568100	July 2009	Moskowitz et al.	X
	U 0281	7647502	January 2010	Moskowitz	X
	U 0282	7647503	January 2010	Moskowitz	X
	U 0283	7779261	August 2010	Moskowitz	X
	U 0284	6990453	January 2006	Wang	X
	U 0285	6081597	June 2000	Hoffstein	X
	U 0286	7035049	Apr 2006	Yamamoto	X
	U 0287	7664263	Feb 2010	Moskowitz	X
	U 0288	7286451	Oct 2007	Wirtz	X
	U 0289	6385324	May 2002	Koppen	X
	U 0290	6674858	Jan 2004	Kimura	X
	U 0291	6148333	Nov 2000	Guedalia	X
	U 0292	6418421	Jun 2002	Hurtado	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0293	6385596	May 2002	Wiser	X
	U 0294	6226618	May 2001	Downs	X
	U 0295	6957330	Oct 2005	Hughes	X
	U 0296	5842213	Nov 1998	Odom	X
	U 0297	5818818	Oct 1998	Soumiya	X
	U 0298	6590996	Jun 2003	Reed	X
	U 0299	5949055	Sept 1999	Fleet	X
	U 0300	6067622	May 2000	Moore	X
	U 0301	7761712	Jun 2010	Moskowitz	X
	U 0302	7743001	Jun 2010	Vermeulen	X
	U 0303	6865747	Mar 2005	Mercier	X
	U 0304	6611599	Aug 2003	Natarajan	X
	U 0305	6480937	Nov 2002	Vorbach	X
	U 0306	6398245	Jun 2002	Gruse	X
	U 0307	6950941	Sept 2005	Lee	X
	U 0308	6983058	Jan 2006	Fukuoka	X
	U 0309	5675653	Oct 1997	Nelson	X
	U 0310	6804453	Oct 2004	Sasamoto	X
	U 0311	6178405	Jan 2001	Ouyang	X
	U 0312	5839100	Nov 1998	Wegener	X
	U 0313	5781184	Jul 1998	Wasserman	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0314	5617506	Apr 1997	Burk	X
	U 0315	5327520	Jul 1994	Chen	X
	U 0316	5111530	May 1992	Kutaragi	X
	U 0317	7095715	Aug 2006	Buckman	X
	U 0318	6173322	Jan 2001	Hu	X
	U 0319	5754938	May 1998	Herz	X
	U 0320	6035398	Mar 2000	Bjorn	X
	U 0321	5901178	May 1999	Lee	X
	U 0322	8214175	July 2012	Moskowitz	X
	U 0323	8265278	Sept 2012	Moskowitz	X
	U 0324	8161286	Nov 2010	Moskowitz	X
	U 0325	8307213	Jan 2011	Moskowitz	X
	U 0326	8121343	May 2012	Moskowitz	X
	U 0327	5437050	Jul 1995	Lamb	X
	U 0328	5123045	Jun 1992	Ostrovsky	X
	U 0329	7310815	Dec 2007	Yanovsky	X
	U 0330	8179846	May 2012	Dolganow	X
	U 0331	7719966	May 2010	Luft	X
	U 0332	7630379	Dec 2009	Morishita	X
	U 0333	5949973	Sept 1999	Yarom	X
	U 0334	8400566	Mar. 2013	Terry	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0335	5649284	July 1997	Yoshinobu	X
	U 0336	7444506	Oct 2008	Datta	X
	U 0337	6480963	Oct 2002	Tachibana	X
	U 0338	6510513	Jan 2003	Darrow	X
	U 0339	5189411	Feb 1993	Collar	X
	U 0340	5293633	Mar 1994	Robbins	X
	U 0341	4633462	Dec 1986	Stifle	X
	U 0342	5103461	Mar 1992	Cain	X
	U 0343	6272535	Aug 2001	Iwamura	X
	U 0344	6029195	Feb 2000	Herz	X
	U 0345	8095949	Jan 2012	Hendricks	X
	U 0346	5297032	Mar 1994	Trojan	X
	U 0347	5644727	Jul 1997	Atkins	X
	U 0348	5721781	Feb 1998	Deo	X
	U 0349	5822436	Oct 1998	Rhoads	X
	U 0350	5845266	Dec 1998	Lupien	X
	U 0351	5864827	Jan 1999	Wilson	X
	U 0352	5875437	Feb 1999	Atkins	X
	U 0353	5892900	Apr 1999	Ginter	X
	U 0354	6108722	Aug 2000	Troeller	X
	U 0355	6029146	Feb 2000	Hawkins	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0356	6032957	Mar 2000	Kiyosaki	X
	U 0357	6134535	Oct 2000	Belzberg	X
	U 0358	6185683	Feb 2001	Ginter	X
	U 0359	6233566	May 2001	Levine	X
	U 0360	6253193	Jun 2001	Ginter	X
	U 0361	6272474	Aug 2001	Garcia	X
	U 0362	6317728	Nov 2001	Kane	X
	U 0363	6363488	Mar 2002	Ginter	X
	U 0364	6389402	May 2002	Ginter	X
	U 0365	6427140	Jul 2002	Ginter	X
	U 0366	6484153	Nov 2002	Walker	X
	U 0367	6556976	Aug 1987	Callen	X
	U 0368	6574608	Jun 2003	Dahod	X
	U 0369	6601044	Jul 2003	Wallman	X
	U 0370	6594643	Jul 2003	Freeny	X
	U 0371	6618188	Sep 2003	Haga	X
	U 0372	6778968	Aug 2004	Gulati	X
	U 0373	6839686	Jan 2005	Galant	X
	U 0374	6856867	Feb 2005	Woolston	X
	U 0375	6876982	Apr 2005	Lancaster	X
	U 0376	7003480	Feb 2006	Fox	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0377	5822436	Oct 1998	Rhoads	X
	U 0378	6324649	Nov 2001	Eyres	X
	U 0379	5375055	Dec 1994	Togher	X
	U 0380	6018722	Jan 2000	Ray	X
	U 0381	6138239	Oct 2000	Veil	X
	U 0382	6484153	Nov 2002	Walker	X
	U 0383	6615188	Aug 2004	Breen	X
	U 0384	6856967	Jan 2005	Woolston	X
	U 0385	5790783	Aug 1998	Lee	X
	U 0386	6650761	Nov 2003	Rodriguez	X
	U 0387	6735702	May 2004	Yavatkar	X
	U 0388	6792424	Sept 2004	Burns	X
	U 0389	4790564	Dec 1988	Larcher	X
	U 0390	6111517	Aug 2000	Atick	X
	U 0391	5164992	Nov 1992	Turk	X
	U 0392	6674877	Jan 2004	Jojie	X
	U 0393	5291560	Mar 1994	Daugman	X
	U 0394	8492633	Jul 2013	Ellis	X
	U 0395	7672838	Mar 2010	Ellis	X
	U 0396	7254538	Aug 2007	Ellis	X
	U 0397	7812241	Oct 2010	Ellis	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0398	7672916	Mar 2010	Poliner	X
	U 0399	5991431	Nov 1999	Borza	X
	U 0400	4529870	Jul 1985	Chaum	X
	U 0401	6704451	Mar 2004	Hekstra	X
	U 0402	6532298	Mar 2003	Cambier	X
	U 0403	8949619	Feb 2015	Parry	X
	U 0404	4855584	Aug 1989	Tomiyama	X
	U 0405	4749354	Jun 1988	Kerman	X
	U 0406	5570339	Oct 1996	Nagano	X
	U 0407	6128735	Oct 2000	Goldstein	
	U 0408	7672317	Mar 2010	Gateva	
	U 0409	6389403	May 2002	Dorak	
	U 0410	7233948	Jun 2007	Shamoon	
	U 0411	8428185	Apr 2013	Driessen	
	U 0412	8095794	Jan 2012	Johnston	
	U 0413	8041038	Oct 2011	Lacy	
	U 0414	7802101	Sept 2010	Johnston	
	U 0415	7725808	May 2010	Johnston	
	U 0416	7529941	May 2009	Johnston	
	U 0417	7492902	Feb 2009	Lacy	
	U 0418	7451319	Nov 2008	Johnston	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 0419	7353447	Nov 2008	Johnston	
	U 0420	7146503	Dec 2006	Johnston	
	U 0421	7131007	Oct 2006	Johnston	
	U 0422	7076426	Jul 2006	Buetnagel	
	U 0423	7042933	May 2006	Driessen	
	U 0424	6885749	Apr 2005	Chang	
	U 0425	6850559	Feb 2005	Driessen	
	U 0426	6760443	Jul 2004	Lacy	
	U 0427	6718507	Apr 2004	Johnston	
	U 0428	6704576	May 2004	Brachman	
	U 0429	6493457	Dec 2002	Quackenbush	
	U 0430	6341165	Jan 2002	Gbur	
	U 0431	6266419	Jul 2001	Lacy	
	U 0432	5825976	Oct 1998	Dorward	
	U 0433	5463641	Oct 1995	Dorward	
	U 434	6345389	Feb 2002	Dureau	
	U 435	7028327	Apr 2006	Dougherty	
	U 436	7725720	May 2010	Moreillon	
	U 437	6154172	Nov 2000	Piccionelli	
	U 438	6233736	May 2001	Wolzien	
	U 439	7020888	Mar 2006	Reynolds	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U 440	7028327	Apr 2006	Dougherty	
	U 441	7055169	May 2006	Delpuch	
	U 442	7421729	Sept 2008	Zenoni	
	U 443	7950033	May 2011	Pierre	
	U 444	7996861	Aug 2011	Delpuch	
	U 445	7251825	Jul 2007	Collet	
	U 446	7725740	May 2010	Kudelski	
	U 447	8356188	Jan 2013	Kudelski	
	U 448	RE40334	May 2008	Maillard	
	U449	7945781	May 2011	Rhoads	
	U450	8095796	Jan 2012	Conwell	
	U451	9934408	Apr 2018	Moskowitz	
	U452	6687375	Feb 2004	Matyas	
	U453	6469239	Oct 2002	Fukuda	
	U454	5933497	Aug 1999	Beetcher	
	U455	5935243	Aug 1999	Hasebe	
	U456	5982892	Nov 1999	Hicks	
	U457	5745604	Apr 1998	Rhoads	
	U458	6236971	May 2002	Stefik	
	U459	7263497	Aug 2007	Wiser	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (U SERIES)	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	U460	6552127	Apr 2003	Kurowski	
	U461	6952774	Oct 2005	Kirovski	
	U462	6122403	Sep 2000	Rhoads	
	U463	6513118	Jan 2003	Iwamura	
	U464	7103574	Sep 2006	Peinado	
	U465	6678465	Jan 2004	Swan	
	U466	6898706	May 2005	Venkatesan	
	U467	6959288	Oct 2005	Medina	
	U468	5109437	Apr 1992	Honda	
	U469	6128626	Oct 2000	Beauchesne	
	U470	5995630	Nov 1999	Borza	
	U471	6,434,238	Aug 2002	Chaum	
	U472	9070151	Jun 2015	Moskowitz	
	U473	5870723	Feb 1999	Pare	
	U474	5280527	Jan 1994	Gullman	
	U475	6453301	Sep 2002	Niwa	
	U476	5930767	Jul 1999	Reber	
	U477	6000832	Dec 1999	Franklin	
	U478	4885778	Dec 1989	Weiss	
	U479	6820204	Nov 2004	Desai	
	U480	6553127	Apr 2003	Kurowski	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

LISTING OF UNITED STATES PUBLISHED APPLICATIONS - P Series

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 01	20010010078	July 2001	Moskowitz	X
	P 02	20010043594	November 2001	Ogawa et al.	X
	P 03	20020010684	January 2002	Moskowitz	X
	P 04	20020026343	February 2002	Duenke	X
	P 05	20020056041	May 2002	Moskowitz	X
	P 06	20020071556	June 2002	Moskowitz et al.	X
	P 07	20020073043	June 2002	Herman et al.	X
	P 08	20020097873	July 2002	Petrovic	X
	P 09	20020103883	August 2002	Haverstock et al.	X
	P 010	20020161741	October 2002	Wang et al.	X
	P 011	20030126445	July 2003	Wehrenberg	X
	P 012	20030133702	July 2003	Collart	X
	P 013	20030200439	October 2003	Moskowitz	X
	P 014	20030219143	November 2003	Moskowitz et al.	X
	P 015	20040028222	February 2004	Sewell et al.	X
	P 016	20040037449	February 2004	Davis et al.	X
	P 017	20040049695	March 2004	Choi et al.	X
	P 018	20040059918	March 2004	Xu	X
	P 019	20040083369	April 2004	Erlingsson et al.	X
	P 020	20040086119	May 2004	Moskowitz	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 021	20040093521	May 2004	Hamadeh et al.	X
	P 022	20040117628	June 2004	Colvin	X
	P 023	20040117664	June 2004	Colvin	X
	P 024	20040125983	July 2004	Reed et al.	X
	P 025	20040128514.	July 2004	Rhoads	X
	P 026	20040225894	November 2004	Colvin	X
	P 027	20040243540	December 2004	Moskowitz et al.	X
	P 028	20050135615	June 2005	Moskowitz et al.	X
	P 029	20050160271	July 2005	Brundage et al.	X
	P 030	20050177727	August 2005	Moskowitz et al.	X
	P 031	20050246554	November 2005	Batson	X
	P 032	20060005029	January 2006	Petrovic et al.	X
	P 033	20060013395	January 2006	Brundage et al.	X
	P 034	20060013451	January 2006	Haitsma	X
	P 035	20060041753	February 2006	Haitsma	X
	P 036	20060101269	May 2006	Moskowitz et al.	X
	P 037	20060140403	June 2006	Moskowitz	X
	P 038	20060285722	December 2006	Moskowitz et al.	X
	P 039	20070011458	January 2007	Moskowitz	X
	P 040	20070028113	February 2007	Moskowitz	X
	P 041	20070064940	March 2007	Moskowitz et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 042	20070079131.	April 2007	Moskowitz et al.	X
	P 043	20070083467	April 2007	Lindahl et al.	X
	P 044	20070110240	May 2007	Moskowitz et al.	X
	P 045	20070113094	May 2007	Moskowitz et al.	X
	P 046	20070127717	June 2007	Herre et al.	X
	P 047	20070226506	September 2007	Moskowitz	X
	P 048	20070253594	November 2007	Lu et al.	X
	P 049	20070294536.	December 2007	Moskowitz et al.	X
	P 050	20070300072	December 2007	Moskowitz	X
	P 051	20070300073	December 2007	Moskowitz	X
	P 052	20080005571	January 2008	Moskowitz	X
	P 053	20080005572	January 2008	Moskowitz	X
	P 054	20080016365	January 2008	Moskowitz	X
	P 055	20080022113	January 2008	Moskowitz	X
	P 056	20080022114	January 2008	Moskowitz	X
	P 057	20080028222	January 2008	Moskowitz	X
	P 058	20080046742	February 2008	Moskowitz	X
	P 059	20080075277	March 2008	Moskowitz et al.	X
	P 060	20080109417	May 2008	Moskowitz	X
	P 061	20080133927	June 2008	Moskowitz et al.	X
	P 062	20080151934	June 2008	Moskowitz et al.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 063	20090037740	February 2009	Moskowitz	X
	P 064	20090089427	April 2009	Moskowitz et al.	X
	P 065	20090190754	July 2009	Moskowitz et al.	X
	P 066	20090210711	August 2009	Moskowitz	X
	P 067	20090220074	September 2009	Moskowitz et al.	X
	P 068	20100002904	January 2010	Moskowitz	X
	P 069	20100005308	January 2010	Moskowitz	X
	P 070	20100098251	Apr 2010	Moskowitz	X
	P 071	20100220861	Sept 2010	Moskowitz	X
	P 072	20100202607	Aug 2010	Moskowitz	X
	P 073	20020047873	June 2002	Petrovic	X
	P 074	20020009208	Jan 2002	Alattar	X
	P 075	20010029580	October 2001	Moskowitz	X
	P 076	20100182570	July 2010	Chota	X
	P 077	20100077220	March 2010	Moskowitz	X
	P 078	20100077219	March 2010	Moskowitz	X
	P 079	20100064140	March 2010	Moskowitz	X
	P 080	20100153734	June 2010	Moskowitz	X
	P 081	20100106736	April 2010	Moskowitz	X
	P 082	20060251291	November 2006	Rhoads	X
	P 083	20030002862	January 2003	Rodriguez	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (P SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	P 084	20030005780	May 2003	Hansen	X
	P 085	20020152179	Oct 2002	Racov	X
	P 086	20030027549	Feb 2003	Kiel	X
	P 087	20020057651	May 2002	Roberts	X
	P 088	20110069864	March 2011	Moskowitz	X
	P 089	20100313033	Dec 2010	Moskowitz	X
	P 090	20110019691	Jan 2011	Moskowitz	X
	P 091	20030023852	Jan. 2003	Wold	X
	P 092	20030033321	Feb 2003	Schrempp	X
	P 093	20130145058	June 2013	Shuholm	X
	P 094	20120057012	Mar. 2012	Sitrick	X
	P 095	20110128445	Jun 2011	Carrieres	X
	P 096	20020188570	Dec 2002	Holliman	X
	P 097	20020069174	Jun 2002	Fox	X
	P 098	20130226957	Feb 27 2013	Ellis	
	P 099	20090319639	Dec 2009	Gao	
	P100	20030005780	May 2003	Pahl	
	P101	20020097873	June 2002	Petrovic	
	P102	20030021419	Jan 2003	Hansen	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF FOREIGN AND INTERNATIONAL PATENT DOCUMENTS - F Series

EXAMINER INITIALS	REFERENCE NUMBER (F SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	COUNTRY OR REGION	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	F 01-	EP0372601	Jun., 1990	EP		X
	F 02-	EP0565947	Oct., 1993	EP		X
	F 03-	EP0581317	Feb., 1994	EP		X
	F 04-	EP0649261	Apr., 1995	EP		X
	F 05-	EP0651554	May., 1995	EP		X
	F 06-	EP1354276	Dec., 2007	EP		X
	F 07-	NL 1005523	Sep., 1998	NL		X
	F 08-	WO9514289	May., 1995	WO		X
	F 09-	WO9629795	Sep., 1996	WO		X
	F 010-	WO9724833	Jul., 1997	WO		X
	F 011-	WO9744736	Nov., 1997	WO		X
	F 012-	WO9837513	Aug., 1998	WO		X
	F 013-	WO9952271	Oct., 1999	WO		X
	F 014-	WO9962044	Dec., 1999	WO		X
	F 015-	WO9963443	Dec., 1999	WO		X
	F 016-	WO9726733	Jan. 1997	WO		X
	F 017-	WO98002864	Jul. 1997	WO		X
	F 018-	WO0057643	Sept 2000	WO		X
	F 019-	WO9642151	Dec 1996	WO		X
	F 020-	EP0872073	July 1996	EP		X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIALS	REFERENCE NUMBER (F SERIES)	PUBLICATION NUMBER	PUBLICATION DATE	COUNTRY OR REGION	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	F 021-	WO0118628	March 2001	WO		X
	F 022-	WO0143026	June 2001	WO		X
	F 023-	WO0203385	Jan 2002	WO		X
	F 024-	WO9701892	June 1995	WO		X
	F 025-	WO9726732	July 1997	WO		X
	F 026-	WO9802864	Jan 1998	WO		X
	F 027-	EP1547337	Mar 2006	EP		X
	F 028-	EP0581317A2	Feb 1994	EP		X
	F 029-	WO023385A1	Oct 2002	WO		X
	F030	WO9955089	Mar 2009	WO		
	F031	WO9942996	Aug 1999	WO		
	F032	H05334072	Dec 1993	JP		
	F033	WO97043761	Nov 1997	WO		
	F034	EP 1028401	Aug 2000	EP		
	F035	WO 0014648	Mar 2000	WO		
	F036	WO 01/13275	Feb 2001	WO		
	F037	WO97/43761	Nov 1997	WO		

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Printed: February 18, 2019 (2:03pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\90014138, USP9104842, SCOT0014-4\Drafts\2019-02-18ReferenceCitationList_90014138.wpd
37 CFR 1.98(a)(1)(i) REEXAMINATION CONTROL NUMBER AND ATTORNEY DOCKET: **90014138**
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF NON PATENT LITERATURE - L Series

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	1	L- 01	N/A	US. Appl. No. 08/999,766, filed Jul. 23, 1997, entitled "Steganographic Method and Device", published as 7568100 07-28-2009, cited as U280.	X
	2	L- 02	N/A	EPO Application No. 96919405.9, entitled "Steganographic Method and Device"; published as EP0872073 (A2), 10-21-1998, cited herein as F20.	X
	3	L- 03	N/A	U.S. Appl. No. 11/050,779, filed Feb. 7, 2005, entitled "Steganographic Method and Device", published as 20050177727 A1 08-11-2005, cited herein as P30.	X
	4	L- 04	N/A	U.S. Appl. No. 08/674,726, filed Jul. 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management", published as 7362775 04-22-2008, cited herein as U272 .	X
	5	L- 05	N/A	U.S. Appl. No. 09/545,589, filed Apr. 7, 2000, entitled "Method and System for Digital Watermarking", published as 7007166 02-28-2006, cited herein as U243	X
	6	L- 06	N/A	U.S. Appl. No. 11/244,213, filed Oct. 5, 2005, entitled "Method and System for Digital Watermarking", published as 2006-0101269 A1 05-11-2006, cited herein as P36	X
	7	L- 07	N/A	U.S. Appl. No. 11/649,026, filed Jan. 3, 2007, entitled "Method and System for Digital Watermarking", published as 2007-0113094 A1 05-17-2007, cited herein as P45.	X
	8	L- 08	N/A	U.S. Appl. No. 09/046,627, filed Mar. 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 6,598,162 07-22-2003, cited herein as U212.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	9	L- 09	N/A	U.S. Appl. No. 10/602,777, filed Jun. 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 2004-0086119 A1 05-06-2004, cited herein P20.	X
	10	L- 010	N/A	U.S. Appl. No. 09/053,628, filed Apr. 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", 6,205,249 03-20-2001, cited herein as U161.	X
	11	L- 011	N/A	U.S. Appl. No. 09/644,098, filed Aug. 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 7,035,409 04-25-2006, cited herein as U245.	X
	12	L- 012	N/A	Jap. App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; which is a JP national stage of PCT/US1999/007262, published as WO/1999/052271, 10/14/1999, F13 here in above..	X
	13	L- 013	N/A	U.S. Appl. No. 09/767,733, filed Jan. 24, 2001 entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 2001-0010078 A1 07-26-2001, cited herein as P1.	X
	14	L- 014	N/A	U.S. Appl. No. 11/358,874, filed Feb. 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 2006-0140403 A1 06-29-2006, cited herein as P37.	X
	15	L- 015	N/A	U.S. Appl. No. 10/417,231, filed Apr. 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth", published as 2003-0200439 A1 10-23-2003, cited herein as P13,	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	16	L- 016	N/A	U.S. Appl. No. 09/789,711, filed Feb. 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2001-0029580 A1 10-11-2001, cited herein as P75.	X
	17	L- 017	N/A	U.S. Appl. No. 11/497,822, filed Aug. 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2007-0011458 A1 01-11-2007, cited herein as P39.	X
	18	L- 018	N/A	U.S. Appl. No. 11/599,964, filed Nov. 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2008-0046742 A1 02-21-2008, cited herein as P58.	X
	19	L- 019	N/A	U.S. Appl. No. 11/599,838, filed Nov. 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2007-0226506 A1 09-27-2007, cited herein as P47.	X
	20	L- 020	N/A	U.S. Appl. No. 10/369,344, filed Feb. 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", published as 2003-0219143 A1 11-27-2003, cited herein as P14.	X
	21	L- 021	N/A	U.S. Appl. No. 11/482,654, filed Jul. 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", published as 2006-0285722 A1 12-21-2006, cited herein as P38.	X
	22	L- 022	N/A	U.S. Appl. No. 09/594,719, filed Jun. 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 7,123,718 10-17-2006, cited herein as U255.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	23	L- 023	N/A	U.S. Appl. No. 11/519,467, filed Sep. 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 2007-0064940 A1 03-22-2007, cited herein as P41.	X
	24	L- 024	N/A	U.S. Appl. No. 09/731,040, filed Dec. 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions", 2002-0010684 A1 01-24-2002, cited herein as P3.	X
	25	L- 025	N/A	U.S. Appl. No. 11/512,701, filed Aug. 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions", published as 2007-0028113 A1 02-01-2007, cited herein as P40.	X
	26	L- 026	N/A	U.S. Appl. No. 10/049,101, filed Feb. 8, 2002, entitled "A Secure Personal Content Server", published as 7,475,246 01-06-2009, cited herein as U277.	X
	27	L- 027	N/A	PCT Application No. PCT/US00/21189, filed Aug. 4, 2000, entitled, "A Secure Personal Content Server", Pub. No.: WO/2001/018628 ; Publication Date: 15.03.2001, cited herein as F21.	X
	28	L- 028	N/A	U.S. Appl. No. 09/657,181, filed Sep. 7, 2000, entitled "Method and Device For Monitoring And Analyzing Signals", published as 7,346,472 03-18-2008, cited herein as U271.	X
	29	L- 029	N/A	U.S. Appl. No. 10/805,484, filed Mar. 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals", published as 2004-0243540 A1 12-02-2004, cited herein as P27.	X
	30	L- 030	N/A	U.S. Appl. No. 09/956,262, filed Sep. 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects", published as 2002-0056041 A1 05-09-2002, cited herein as P05	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	31	L- 031	N/A	U.S. Appl. No. 11/518,806, filed Sep. 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects", 2008-0028222 A1 01-31-2008, cited herein as P57.	X
	32	L- 032	N/A	U.S. Appl. No. 11/026,234, filed Dec. 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" , published as 2005-0135615 A1 06-23-2005, cited herein as P28.	X
	33	L- 033	N/A	U.S. Appl. No. 11/592,079, filed Nov. 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks", published as 2007-0079131 A1 04-05-2007, cited herein as P42.	X
	34	L- 034	N/A	U.S. Appl. No. 09/731,039, filed Dec. 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects", published as 2002-0071556 A1 06-13-2002, cited herein as P06.	X
	35	L- 035	N/A	U.S. Appl. No. 11/647,861, filed Dec. 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects", published as 2007-0110240 A1 05-17-2007, cited herein as P44.	X
	36	L- 036	1996	Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996.	X
	37	L- 037	1997	Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 46, 1997.	X
	38	L- 038	1997	Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p. 207.	X
	39	L- 039	1984	Brealy, et al., Principles of Corporate Finance, "Appendix A--Using Option Valuation Models", 1984, pp. 448-449.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	40	L- 040	2001	Copeland, et al., Real Options: A Practitioner's Guide, 2001 pp. 106-107, 201-202, 204-208.	X
	41	L- 041	1995	Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/SarkAsses.html on.	X
	42	L- 042	1995	Crawford, D.W. "Pricing Network Usage: A Market for Bandwidth of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March.	X
	43	L- 043	1988	Low, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.nj.nec.com/366503.html.	X
	44	L- 044	1995	Caronni, Germano, "Assuring Ownership Rights for Digital Images", published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed) Viewing Publishing Company Germany 1995.	X
	45	L- 045	1996	Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the European conf. on Multimedia Applications, Services & Techniques Louvain-La-Nevve Belgium May 1996.	X
	46	L- 046	1996	Gruhl, Daniel et al., Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science, Cambridge, England (May/Jun. 1996).	X
	47	L- 047	1995	Oomen, A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J.AudioEng. Sc., vol. 43, No. 1/2, pp. 23-28 (1995).	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	48	L- 048	1992	Ten Kate, W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng.Soc., vol. 40,No. 5,pp. 376-383 (1992).	X
	49	L- 049	1993	Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993).	X
	50	L- 050	1988	Sklar, Bernard, Digital Communications, pp. 601-603 (1988).	X
	51	L- 051	1984	Jayant, N.S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs, NJ, pp. 486-509 (1984)	X
	52	L- 052	1995	Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., vol. 2420, pp. 164-173, 1995.	X
	53	L- 053	1995	Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995.	X
	54	L- 054	1997	Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997.	X
	55	L- 055	1994	Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994.	X
	56	L- 056	1990	Ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990).	X
	57	L- 057	1994	Van Schyndel, et al., "A digital Watermark," IEEE Int'l Computer Processing Conference, Austin,TX, Nov. 13-16, 1994, pp. 86-90.	X
	58	L- 058	1996	Smith, et al. "Modulation and Information Hiding in Images", Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-Jun. 1, 1996, pp. 207-227.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	59	L- 059	1997	Kutter, Martin et al., "Digital Signature of Color Images Using Amplitude Modulation", SPIE-E197, vol. 3022, pp. 518-527.	X
	60	L- 060	1997	Puate, Joan et al., "Using Fractal Compression Scheme to Embed a Digital Signature into an Image", SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118.	X
	61	L- 061	1996	Swanson, Mitchell D.,et al., "Transparent Robust Image Watermarking", Proc. of the 1996 IEEE Int'l Conf. on Image Processing, vol. 111, 1996 , pp. 211-214.	X
	62	L- 062	1996	Swanson, Mitchell D., et al. "Robust Data Hiding for Images", 7th IEEE Digital Signal Processing Workshop, Leon, Norway. Sep. 1-4, 1996, pp. 37-40.	X
	63	L- 063	Unknown	Zhao, Jian et al., "Embedding Robust Labels into Images for Copyright Protection", Proceeding of the Know Right '95 Conference, pp. 242-251.	X
	64	L- 064	1995	Koch, E., et al., "Towards Robust and Hidden Image Copyright Labeling", 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun. 1995 Neos Marmaras pp. 4.	X
	65	L- 065	1995	Van Schyandel, et al., "Towards a Robust Digital Watermark", Second Asain Image Processing Conference, Dec. 6-8, 1995, Singapore, vol. 2, pp. 504-508.	X
	66	L- 066	1995	Tirkel,A.Z., "A Two-Dimensional Digital Watermark", DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8, 1995, pp. 7.	X
	67	L- 067	1996	Tirkel,A.Z., "Image Watermarking--A Spread Spectrum Application", ISSSTA '96, Sep. 1996, Mainz, German, pp. 6.	X
	68	L- 068	1996	O'Ruanaidh, et al. "Watermarking Digital Images for Copyright Protection", IEEE Proceedings, vol. 143, No. 4, Aug. 1996, pp. 250-256.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	69	L- 069	Unknown	Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institude, Techinal Report 95-10, pp. 33.	X
	70	L- 070	1969	Kahn, D., "The Code Breakers", The MacMillan Company, 1969, pp. xIII, 81-83, 513, 515, 522-526, 863.	X
	71	L- 071	1997	Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480 (3/14/1997).	X
	72	L- 072	1996	Dept. of Electrical Engineering, Del Ft University of Technology, Del ft The Netherlands, Cr.C. Langelaar et al.,"Copy Protection for Multimedia Data based on Labeling Techniques", Jul. 1996 9 pp.	X
	73	L- 073	Unknown	F. Hartung, et al., "Digital Watermarking of Raw and Compressed Video", SPIE vol. 2952, pp. 205-213.	X
	74	L- 074	1996	Craver, et al., "Can Invisible Watermarks Resolve Rightful Ownerships?", IBM Research Report, RC 20509 (Jul. 25, 1996) 21 pp.	X
	75	L- 075	1988	Press, et al., "Numerical Recipes in C", Cambridge Univ. Press, 1988, pp. 398-417.	X
	76	L- 076	1995	Pohlmann, Ken C., "Principles of Digital Audio", 3rd Ed., 1995, pp. 32-37, 40-48:138, 147-149, 332, 333, 364, 499-501, 508-509, 564-571.	X
	77	L- 077	1991	Pohlmann, Ken C., "Principles of Digital Audio", 2nd Ed., 1991, pp. 1-9, 19-25, 30-33, 41-48, 54-57, 86-107, 375-387.	X
	78	L- 078	1994	Schneier, Bruce, Applied Cryptography, John Wiley & Sons, Inc., New York, 1994, pp. 68, 69, 387-392, 1-57, 273-275, 321-324.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	79	L- 079	1996	Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, Jun. 17-23, 1996 Hiroshima, Japan, 0-8186-7436-9196, pp. 473-480.	X
	80	L- 080	1998	Johnson, et al., "Transform Permuted Watermarking for Copyright Protection of Digital Video", IEEE Globecom 1998, Nov. 8-12, 1998, New York New York vol. 2 1998 pp. 684-689 (ISBN 0-7803-4985-7).	X
	81	L- 081	1996	Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, May 7, 1996 pp. 1-18.	X
	82	L- 082	1996	Bender, et al., "Techniques for Data Hiding", IBM Systems Journal, (1996) vol. 35, Nos. 3 & 4,1996, pp. 313-336.	X
	83	L- 083	2003	Moskowitz, "Bandwith as Currency", IEEE Multimedia, Jan.-Mar. 2003, pp. 14-21.	X
	84	L- 084	2006	Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction--Digital Rights Management" pp. 3-22.	X
	85	L- 085	2001	Rivest, et al., "PayWord and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, Apr. 27, 2001, pp. 1-18.	X
	86	L- 086	2000	Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB)(2000).	X
	87	L- 087	2002	Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security; Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 Apr. 10, 2002 pp. 80-84.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	88	L- 088	2006	Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking" ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006 (to appear) 13.	X
	89	L- 089	2002	Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Cryptography Research, Inc. 2002-2003 14 pages.	X
	90	L- 090	1995	Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring) Mar. 5, 1995 pp. 20-25 vol. CONF40.	X
	91	L- 091	1998	Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, Sep. 30, 1998, pp. 1501-1510 vol. 30 No. 16-18 NL North Holland.	X
	92	L- 092	1999	Konrad, K. et al., "Trust and Electronic Commerce--more than a technical problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems Oct. 19-22, 1999, pp. 360-365 Lausanne.	X
	93	L- 093	1998	Kini, et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216). Jan. 6-9, 1998. pp. 51-61. Los.	X
	94	L- 094	1997	Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sep. 1997, pp. 118-124, vol. 5 No. 3, ACM, USA.	X
	95	L- 095	1999	Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp. 1079-1107 Jul. 1999 vol. 87 No. 7 IEEE.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	96	L- 096	N/A	European Search Report & European Search Opinion in EP07112420	X
	97	L- 097	2006	STAIND (The Singles 1996-2006), Warner Music--Atlantic, Pre-Release CD image, 2006, 1 page.	X
	98	L- 098		DUPLICATE OF L-97, DELETED BY 11/16/2010 by RAN.	X
	99	L- 099	2003	Radiohead ("Hail To The Thief"), EMI Music Group--Capitol, Pre-Release CD image, 2003, 1 page.	X
	100	L- 0100	N/A	DUPLICATE OF L-4, DELETED BY RN UPON REVIEW ON 11/18/2010. RAN	X
	101	L- 0101	N/A	U.S. Appl. No. 60/169,274, filed Dec. 7, 1999, entitled "Systems, Methods And Devices For Trusted Transactions".	X
	102	L- 0102		DUPLICATE OF L-22, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	103	L- 0103		DUPLICATE OF L-27, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	104	L- 0104	N/A	U.S. Appl. No. 60/234,199, filed Sep. 20, 2000, "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects".	X
	105	L- 0105	N/A	U.S. Appl. No. 09/671,739, filed Sep. 29, 2000, entitled "Method And Device For Monitoring And Analyzing Signals".	X
	106	L- 0106		DUPLICATE OF L-34, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	107	L- 0107		DUPLICATE OF L-24, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	108	L- 0108		DUPLICATE OF L-57, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	109	L- 0109		DUPLICATE OF L-58, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	110	L- 0110		DUPLICATE OF L-59, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	111	L- 0111		DUPLICATE OF L-61, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	112	L- 0112		DUPLICATE OF L-62, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	113	L- 0113		DUPLICATE OF L-63, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	114	L- 0114		DUPLICATE OF L-65, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	115	L- 0115	Unknown.	Tirkel, A.Z., "A Two-Dimensional Digital Watermark", Scientific Technology, 686, 14, date unknown. (citation revised upon review on 11/16/10 by RAN.)	X
	116	L- 0116		DUPLICATE OF L-65, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	117	L- 0117		DUPLICATE OF L-68, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	118	L- 0118		DUPLICATE OF L-69, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	119	L- 0119		DUPLICATE OF L-70, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	120	L- 0120		DUPLICATE OF L-71, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	121	L- 0121		DUPLICATE OF L-72, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	122	L- 0122		DUPLICATE OF L-73, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	123	L- 0123		DUPLICATE OF L-74, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	124	L- 0124		DUPLICATE OF L-75, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	X
	125	L- 0125		DUPLICATE OF L-076, REMOVED. RN. 11/16/2010	X
	126	L- 0126		DUPLICATE OF L-77, REMOVED. RN. 11/16/2010	X
	127	L- 0127		DUPLICATE OF L-78, REMOVED. RN. 11/16/2010	X
	128	L- 0128		DUPLICATE OF L-79, REMOVED. RN. 11/16/2010	X
	129	L- 0129		EP0581317A2, MOVED TO FOREIGN PATENT PUBS as F-028	X
	130	L- 0130		DUPLICATE OF L-52, REMOVED. RN. 11/16/2010	X
	131	L- 0131		DUPLICATE OF L-36, REMOVED. RN. 11/16/2010	X
	132	L- 0132		DUPLICATE OF L-38, REMOVED. RN. 11/16/2010.	X
	133	L- 0133		DUPLICATE OF L-37, REMOVED. RN. 11/16/2010	X
	134	L- 0134		DUPLICATE OF L-36, REMOVED. RN. 11/16/2010	X
	135	L- 0135		DUPLICATE OF L-37, REMOVED. RN. 11/16/2010	X
	136	L- 0136		DUPLICATE OF L-38, REMOVED. RN. 11/16/2010	X
	137	L- 0137		DUPLICATE OF L-39, REMOVED. RN. 11/16/2010	X
	138	L- 0138		DUPLICATE OF L-40, REMOVED. RN. 11/16/2010	X
	139	L- 0139		DUPLICATE OF L-41, REMOVED. RN. 11/16/2010	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	140	L- 0140		DUPLICATE OF L-42, REMOVED. RN. 11/16/2010	X
	141	L- 0141		DUPLICATE OF L-43, REMOVED. RN. 11/16/2010	X
	142	L- 0142		DUPLICATE OF L-44, REMOVED. RN. 11/16/2010	X
	143	L- 0143		DUPLICATE OF L-45, REMOVED. RN. 11/16/2010.	X
	144	L- 0144		DUPLICATE OF L-46, REMOVED. RN. 11/16/2010.	X
	145	L- 0145		DUPLICATE OF L-47, REMOVED. RN. 11/16/2010	X
	146	L- 0146		DUPLICATE OF L-48, REMOVED. RN. 11/16/2010	X
	147	L- 0147		DUPLICATE OF L-49, REMOVED. RN. 11/16/2010	X
	148	L- 0148		DUPLICATE OF L-50, REMOVED. RN. 11/16/2010	X
	149	L- 0149		DUPLICATE OF L-51, REMOVED. RN. 11/16/2010	X
	150	L- 0150		DUPLICATE OF L-52, REMOVED. RN. 11/16/2010	X
	151	L- 0151		DUPLICATE OF L-63, REMOVED. RN. 11/16/2010	X
	152	L- 0152		DUPLICATE OF L-54, REMOVED. RN. 11/16/2010	X
	153	L- 0153		DUPLICATE OF L-55, REMOVED. RN. 11/16/2010.	X
	154	L- 0154		DUPLICATE OF L-80, REMOVED. RN. 11/16/2010.	X
	155	L- 0155	N/A	PCT International Search Report in PCT/US95/08159.	X
	156	L- 0156	N/A	PCT International Search Report in PCT/US96/10257.	X
	157	L- 0157	N/A	Supplementary European Search Report in EP 96919405.	X
	158	L- 0158	N/A	PCT International Search Report in PCT/US97/00651.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	159	L- 0159	N/A	PCT International Search Report in PCT/US97/00652	X
	160	L- 0160	N/A	PCT International Search Report in PCT/US97/11455.	X
	161	L- 0161		PCT International Search Report in PCT/US99/07262.	X
	162	L- 0162		PCT International Search Report in PCT/US00/06522	X
	163	L- 0163		Supplementary European Search Report in EP00919398	X
	164	L- 0164		PCT International Search Report in PCT/US00/18411.	X
	165	L- 0165		PCT International Search Report in PCT/US00/18411.	X
	166	L- 0166		PCT International Search Report in PCT/US00/33126	X
	167	L- 0167		PCT International Search Report in PCT/US00/21189	X
	168	L- 0168		Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110.	X
	169	L- 0169	1996	Schneider, M., et al. "A Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC. Lausanne) Sep. 16-19, 1996, pp. 227-230, IEEE ISBN.	X
	170	L- 0170	1997	Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	X
	171	L- 0171	1998	Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, vol. 1 Oct. 4-7, 1998, pp. 455-459.	X
	172	L- 0172	1998	Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, vol. 1525, Apr. 14-17, 1998, pp. 218-238 ISBN: 3-540-65386-4.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	173	L- 0173	1996	Ross Anderson, "Stretching the Limits of Steganography," LNCS, vol. 1174, May/Jun. 1996, 10 pages, ISBN: 3-540-61996-8.	X
	174	L- 0174	1997	Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997 4 pages.	X
	175	L- 0175	1997	Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing Aug. 21, 1997, 19 pages.	X
	176	L- 0176	2008	OASIS (Dig Out Your Soul), Big Brother Recordings Ltd, Promotional CD image, 2008, 1 page.	X
	177	L- 0177	1998	Rivest, R. "Chaffing and Winnowing: Confidentiality without Encryption", MIT Lab for Computer Science, http://people.csail.mit.edu/rivest/Chaffing.txt Apr. 24, 1998, 9 pp.	X
	178	L- 0178	2003	PortalPlayer, PP5002 digital media management system-on-chip, May 1, 2003, 4 pp.	X
	179	L- 0179	2001	VeriDisc, "The Search for a Rational Solution to Digital Rights Management (DRM)", http://64.244.235.240/news/whitepaper, /docs/veridisc.sub.--white.sub.--paper.pdf, 2001, 15 pp.	X
	180	L- 0180	2008	Cayre, et al., "Kerckhoff's-Based Embedding Security Classes for WOA Data Hiding", IEEE Transactions on Information Forensics and Security, vol. 3 No. 1, Mar. 2008, 15 pp.	X
	181	L- 0181	1999	Wayback Machine, dated Jan. 17, 1999, http://web.archive.org/web/19990117020420/http://www.netzero.com/, accessed on Feb. 19, 2008.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	182	L- 0182	1997	Namgoong, H., "An Integrated Approach to Legacy Data for Multimedia Applications", Proceedings of the 23rd EUROMICRO Conference, vol., Issue 1-4, Sep. 1997, pp. 387-391.	X
	183	L- 0183	2007	Wayback Machine, dated Aug. 26, 2007, http://web.archive,org/web/20070826151732/http://www.screenplaysmag.com/t-abid/96/articleType/ArticleView/articleId/495/Default.aspx/.	X
	184	L- 0184	2009	"YouTube Copyright Policy: Video Identification tool--YouTube Help", accessed Jun. 4, 2009, http://www.google.com/support/youtube/bin/answer.py?h1=en&answer=83766, 3 pp.	X
	185	L- 0185	N/A	U.S. Appl. No. 12/665,002, filed Dec. 22, 2009, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 20100182570 A1 07-22-2010, P76.	X
	186	L- 0186	N/A	U.S. Appl. No. 12/592,331, filed Nov. 23, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 20100077220 A1 03-25-2010, P77.	X
	187	L- 0187	N/A	U.S. Appl. No. 12/590,553, filed Nov. 10, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 20100077219 A1 03-25-2010, P78.	X
	188	L- 0188	N/A	U.S. Appl. No. 12/590,681, filed Nov. 12, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 20100064140 A1 03-11-2010, P79.	X
	189	L- 0189	N/A	U.S. Appl. No. 12/655,036, filed Dec. 22, 2009, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 20100153734 A1 06-17-2010, P80 .	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	190	L- 0190	N/A	U.S. Appl. No. 12/655,357, filed Dec. 22, 2009, entitled "Method And Device For Monitoring And Analyzing Signals", published as 20100106736 A1 04-29-2010, P81.	X
	191	L- 0191	N/A	PCT Application No. PCT/US95/08159, filed Jun. 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing", published as WO/1997/001892; Publication Date: 16.01.1997, F24.	X
	192	L- 0192	N/A	PCT Application No. PCT/US96/10257, filed Jun. 7, 1996, entitled "Steganographic Method and Device"--corresponding to--EPO Application No. 96919405.9, entitled "Steganographic Method and Device", published as WO/1996/042151; Publication Date: 27.12.1996; F19.	X
	193	L- 0193	N/A	PCT Application No. PCT/US97/00651, filed Jan. 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code", published as WO/1997/026732; Publication Date: 24.07.1997.	X
	194	L- 0194	N/A	PCT Application No. PCT/US97/00652, filed Jan. 17, 1997, entitled, "Method for an Encrypted Digital Watermark", published as WO/1997/026733; Publication Date: 24.07.1997	X
	195	L- 0195	N/A	PCT Application No. PCT/US97/11455, filed Jul. 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data", published as WO/1998/002864; Publication Date: 22.01.1998	X
	196	L- 0196	N/A	PCT Application No. PCT/US99/07262, filed Apr. 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking", published as WO/1999/052271; Publication Date: 14.10.1999.	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	197	L- 0197	N/A	PCT Application No. PCT/US00/06522, filed Mar. 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as WO/2000/057643; Publication Date: 28.09.2000.	X
	198	L- 0198	N/A	PCT Application No. PCT/US00/18411, filed Jul. 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques"	X
	199	L- 0199	N/A	PCT Application No. PCT/US00/33126, filed Dec. 7, 2000, entitled "Systems, Methods and Devices for Trusted Transactions", published as WO/2001/043026; Publication Date: 14.06.2001.	X
	200	L- 0200	N/A	EPO Divisional Patent Application No. 07112420.0, entitled "Steganographic Method and Device" corresponding to PCT Application No. PCT/US96/10257, published as WO/1996/042151, 12/27/1996, cited herein above as F019.	X X
	201	L- 0201	N/A	US Provisional Application 60/222,023 filed July 31, 2007 entitled "Method and apparatus for recognizing sound and signals in high noise and distortion"	X
	202	L- 0202	N/A	US Application 11/458,639 filed July 19, 2006 entitled "Methods and Systems for Inserting Watermarks in Digital Signals", published as 20060251291 A1 11-09-2006, P82.	X
	203	L- 0203	1995	"Techniques for Data Hiding in Audio Files," by Morimoto, 1995	X
	204	L- 0204	1998	Howe, Dennis July 13, 1998 http://foldoc..org//steganography	X
	205	L- 0205	N/A	CSG, Computer Support Group and CSGNetwork.com 1973 http://www.csgnetwork.com/glossarys.html	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	206	L- 0206	2010	QuinStreet Inc. 2010 What is steganography?-A word definition from the Webopedia Computer Dictionary http://www.webopedia.com/terms/steganography.html	X
	207	L- 0207	2000	Graham, Robert August 21, 2000 "Hacking Lexicon" http://robertgraham.com/pubs/hacking-dict.html	X
	208	L- 0208	2010	Farkex, Inc 2010 "Steganography definition of steganography in the Free Online Encyclopedia" http://encyclopedia2.Thefreedictionary.com/steganography	X
	209	L- 0209	1989	Horowitz, et al., The Art of Eletronics. 2nd Ed., 1989, pp7	X
	210	L- 0210	2004	Jimmy eat world ("futures"), Interscope Records, Pre-Release CD image, 2004, 1 page.	X
	211	L- 0211	2001	Aerosmith ("Just Push Play"), Pre-Release CD image, 2001, 1 page.	X
	212	L- 0212	2002	Phil Collins(Testify) Atlantic, Pre-Release CD image, 2002, 1 page.	X
	213	L- 0213	1998	U. are U. Reviewer's Guide (U are U Software, 1998)	X
	214	L- 0214	1998	U. are U. wins top honors! - Marketing Flyer (U. are U. Software, 1998).	X
	215	L- 0215	1998	Digital Persona, Inc., U. are U. Fingerprint Recognition System: User Guide (Version 1.0, 1998).	X
	216	L- 0216	1998	Digital Persona White Paper pp 8-9 published April 15, 1998.	X
	217	L- 0217	2000	Digital Persona, Inc., "Digital Persona Releases U. are. U Pro Fingerprint Security Systems for Windows NT, 2000, '98, '95", (2000, February)	X

DATE:	EXAMINER'S SIGNATURE:
03/15/2019	/DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	218	L- 0218	2011	SonicWall, Inc. 2011 "The Network Security SonicOS Platform-Deep Packet Inspection" http://www.sonicwall.com/us/en/products/Deep_Packet_Inspection.html	X
	219	L- 0219	2011	Rick Merritt, PARC hosts summit on content-centric nets, EETimes, Aug. 12, 2011, http://www.eetimes.com/electronics-news/4218741/PARC-hosts-summit-on-content-centric-nets	X
	220	L- 0220	2011	Afanasyev, et. al., Communications of the ACM: Privacy Preserving Network Forensics 2011	X
	221	L- 0221	2008	SonicWall, Inc., 2008 "The Advantages of a Multi-core Architecture In Network Security Appliances" http://www.sonicwall.com/downloads/WP-ENG-010_Multicore...	X
	222	L- 0222	2013	Voip-Pal.Com Inc's Lawful Intercept Patent Application Receives the Allowance for Issuance as a Patent, http://finance.yahoo.com/news/voip-pal-com-inc-lawful-133000133.html	X
	223	L- 0223	2013	Deep Content Inspection - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Deep_content_inspection (last visited Apr. 4, 2013)	X
	224	L- 0224	2009	Dexter, et. al, "Multi-view Synchronization of Human Actions and Dynamic Scenes" pp 1-11, 2009	X
	225	L- 0225	2011	Kudrle, et al., "Fingerprinting for Solving A/V Synchronization Issues within Broadcast Environments", 2011	X
	226	L- 0226	2010	Junego, et. al., "View-Independent Action Recognition from Temporal Self-Similarities", 2011	X
	227	L- 0227	2009	Dexter, et al., "Multi-view Synchronization Of Image Sequences", 2009	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	228	L- 0228	2013	Blue Spike, LLC. v. Texas Instruments, Inc et. al, (No: 6:12-CV-499-MHS), Audible Magic Corporations's amended Answer (E.D. TX filed 7/15/2013) (Document 885 page ID 9581), (PACER)	X
	229	L- 0229	2006	Moskowitz, "Introduction-Digital Rights Management," Multimedia Security Technologies for Digital Rights Management (2006), Elsevier	X
	230	L- 0230	1999	George, Mercy; Chouinard, Jean-Yves; Georgana, Nicolas. Digital Watermarking of Images and video using Direct Sequence Spread Spectrum Techniques. 1999 IEEE Canadian Conference on Electrical and Computer Engineering Vol. 1. Pub. Date: 1999 Relevant pages 116-121. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=807181	X
	231	L- 0231	4/4/2014	Shazam Entertainment Limited's Amended Answer to Blue Spike, LLC's complaint and counterclaims against Blue Spike LLC, Blue Spike, Inc and Scott A. Moskowitz , Shazam Entertainment Ltd v. Blue Spike, LLC, Blue Spike, Inc, and Scott Moskowitz (E.D.T.X Dist Ct.) Case No. 6:12-CV-00499-MHS	X X
	232	L- 0232	4/4/2014	Audible Magic Corporation's Second Amended Answer to Blue Spike LLC's Original Complaint for patent infringement and counterclaims against Blue Spike LLC, Blue Spike, Inc and Scott Moskowitz. Blue Spike LLC v. Texas Instruments, Audible Magic Corporation (E.D.T.X Dist Ct.) Case No. 6:12-CV-499-MHS	X
	233	L- 0233	12/19/2011	Shrivastava, et.al. ,"Data-Driven Visual Similarity for Cross-Domain Image Matching", 2011 ACM Transaction of Graphics (TOG), ACM SIGGRAPH Asia vol. 30 number 6, http://graphics.cs.cmu.edu/projects/crossDomainMatching/	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	234	L- 0234	12/6/2011	Spice, Byron, "Carnegie Mellon Researchers Develop Computerized Method for Finding Similar Images in Photos, Paintings, Sketches", Carnegie Mellon News, Dec 6, 2011, Carnegie Mellon University. http://www.cmu.edu/news/stories/archives/2011/december/dec6_matchingimages.html	X
	235	L- 0235	10/16/2014	Memorandum Opinion and Order, Blue Spike LLC v. Texas Instruments, Inc. et al., (E.D.T.X Dist Ct), Case No. 6:12-CV-0499-MHS-CMC (Doc#1831 PageID#27507)	X
	236	L- 0236	10/16/2014	Memorandum Opinion and Order, Blue Spike LLC v. Texas Instruments, Inc. et al., (E.D.T.X Dist Ct), Case No. 6:12-CV-0499-MHS-CMC (Doc#1834 PageID#27597)	X
	237	L- 0237	1989	Yu, Che-Fn,"Access Control and Authorization Plan for Customer Control of Network Services", IEEE GLOBECOM 1989 Pub 1989. pgs 862-869. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=64085	X
	238	L- 0238	1996	Jaeger, Trent; Prakash, Atul; Rubin, Aviel D, "A System Architecture for Flexible Control of Downloaded Executable Content." Proceedings of the Fifth International Workshop on Object-Oreintation in Operating Systems. Pub 1996, pgs 14-18. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=557855	X
	239	L- 0239	5/2011	"Activate Your Product Through The Online License Management System (LMS)", May 2011 Juniper Networks, Inc., USA	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	240	L- 0240	5/2011	"Activate Your Software Capacity and/or Features", May 2011, Juniper Networks, USA	X
	241	L- 0241	5/2011	"Download and Activate Your Software", May 2011, Juniper Networks, Inc., USA	X
	242	L- 0242	9/2009	"Electronic Fulfillment of Feature, Capacity and Subscription License Activation Keys via the License Management System (LMS)", September 2009, Juniper Networks, Inc., USA	X
	243	L- 0243	7/2009	"Juniper Networks License Management System (LMS) FAQ", July 2009, Juniper Networks, Inc., USA	X
	244	L- 0244	12/2014	"License Activation Keys", Dec14, 2014, http://www.juniper.net/generate_license/	X
	245	L- 0245	3/2014	"License code and configuration key reference [AX 2012]", Mar 25, 2014, Microsoft http://technet.microsoft.com/en-us/library/hh378074.aspx	X
	246	L- 0246	12/2014	"License Codes", Dec 14, 2014, Oracle http://www.oracle.com/us/support/licensecodes/index.html	X
	247	L- 0247	12/2014	"PeopleSoft Enterprise: License Codes", Dec 14, 2014, http://www.oracle.com/us/support/licensecodes/peoplesoft-enterprise/index.html	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	248	L- 0248	12/2014	"Primavera License Key Files", Dec 14, 2014, http://www.oracle.com/us/support/licensecodes/primavera/index.html	X
	249	L- 0249	12/2014	"Siebel License Keys", Dec 14, 2014, http://www.oracle.com/us/support/licensecodes/siebel/index.html	X
	250	L- 0250	03/2009	"How to transfer a license activation key to an RMA replacement device", March 2009, Juniper Networks, Inc. USA	X
	251	L- 0251	12/2014	"How to register a license key in My VMware (2011177)", Dec 14, 2014, http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=ex&bbid=TSEBB_1334428459608&url=&stateId=1%200%20462914399&dialogID=462898852&docTypeID=DT_KB_1_1&externalId=2011177&sliceId=1&rfId=	X
	252	L- 0252	7/2001	CHAUSSEE, "Inside Windows Product Activation", July 2001, http://www.licenturion.com/xp	X
	253	L- 0253	12/2014	"How to generate and validate a software key license", Dec 14, 2014, Stack Overflow, http://stackoverflow.com/questions/599837/how-to-generate-and-validate-a-software-license-key	X

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	254	L- 0254	7/2005	DONSW, "License Key Generation", Jul 2005, Code Project, http://www.codeproject.com/articles/11012/License-Key-Generation	X
	255	L- 0255	12/2004	"How are Software License Keys generated?", Dec 14, 2014, Stack Overflow, http://stackoverflow.com/questions/3002067/how-are-software-license-keys-generated	X
	256	L- 0256	3/2015	Decision on Appeal, USPTO PTAB Appeal No. 2012-011854 for application 11/895,388 issued March 12, 2015.	X
	257	L- 0257	1997	Lacy, Jack; Snyder, James H.: Maher, David P. "Music on the Internet and the Intellectual Property Protection Problem". Proceedings of the IEEE International Symposium on Industrial Electronics, 1997m ISIE '97 Vol. 1. Pages SS77-SS833. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=707419	
	258	L- 0258	1998	Kohl, Ulrich; Lotspiech, Jeffrey; Nusser, Stefan, "Security for the Digital Library - Protecting Documents Rather Than Channesl Proceedings". Ninth International Workshop on Database and Expert Systems Applications, 1998, Pgs. 316-321. http://ieeexplore.ieee.org/stamp/stamp/jsp?tp=&arnumber=707419	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	259	L- 0259	1997	von Faber, Eberhard; Hammelrath, Robert; Franz-Peter. The Secure Distribution of Digital Contents. Proceedings, 13th Annual Computer Security Applications Conference, 1997. pgs 16-22. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=651739	
	260	L- 0260	2015	Order Granting Motion For Judgment on the Pleadings, Blue Spike, LLC v. Google Inc. (N.D.Cal. Dist Ct.) Case No. 14-cv-01650-YGR	
	261	L-0261	2017	Order Denying Petition for Panel Rehearing and Rehearing en Banc, Blue Spike, LLC v. Google Inc. (N.D.C.A. Dist Ct.) Case No. 4:14-cv-01650-YGR	
	262	L-0262	1999	AUGOT, DANIEL, "Secure Delivery Of Images over Open Networks", Proceedings of the IEEE, Vol. 87, Issue 7, July 1999, Abstract. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=771076	
	263	L-0263	2016	Blue Spike, LLC v. Google, Inc, 2016-1054 (Fed. Cir. 10/14/2016), judgement adverse to Blue Spike, LLC.	
	264	L-0264	2017	Blue Spike LLC v. Google, Inc., 16-1223 (6/12/2017) denial of writ of certiorari.	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	265	L-0265	2018	Declaration of Dr. Anna Lysyanskaya ("Lysyanskaya Declaration") in Reexam 90014152	
	265 A	L-0265A	2018	AUGOT, DANIEL, "Secure Delivery Of Images over Open Networks", Proceedings of the IEEE, Vol. 87, Issue 7, July 1999, pp. 1251-1266	
	266	L-0266	2018	Plaintiff Blue Spike, LLC's Proposed Terms for Construction, Pursuant to Patent Rule (P.R.) 4-2 in Blue Spike, LLC v. Juniper Networks, Inc., Case No. 6:17-cv-16-KNM (E.D. Tex.)	
	267	L-0267	2018	English Translation of JP H05334072 (Beetcher '072)	
	268	L-0268	2018	Declaration of Dr. Claudio Silva ("Silva Declaration") filed in reexam 90014138	
	269	L-0269	2018	Declaration of Dr. Claudio Silva ("Silva Declaration") filed in reexam 90014137	
	270	L-0270	1987	Ex 1003 in IPR2017-01061, Oded Goldreich, Towards a Theory of Software Protection and Simulation by Oblivious RAMs, 1987 Symposium on Theory of Computing 182-194 (May 1987) ("Goldreich")	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	271	L-0271	1992	Ex 1004 in IPR2017-01061, Rafail Ostrovsky, Software Protection and Simulation on Oblivious RAMs (May 17, 1992) (MIT Ph.D. Thesis) ("Ostrovsky 1992")	
	272	L-0272	1990	Ex 1006 Rafail Ostrovsky, Efficient Computation on Oblivious RAMs, 1990 Symposium on Theory of Computing 514-523 (May 1990) ("Ostrovsky 1990")	
	273	L-0273	1990	Ex 1007 in IPR2017-01061, Expert Declaration of Rafail Ostrovsky, Ph.D.	
	274	L-0274	2016	Ex 1008 in IPR2017-01061, Claim Construction Order entered May 16, 2016 in an unrelated litigation, Blue Spike, LLC v. Huawei Techs. Co. et al., Case No. 6:13-cv-00679, Dkt. 194.	
	275	L-0275	1997	Ex 1005 in IPR2017-01109, Stephanie Forrest et al., Building Diverse Computer Systems, The Sixth Workshop on Hot Topics in Operating Systems, 67-71 (IEEE, May 1997) ("Forrest")	
	276	L-0276	2017	Ex 1008 in IPR2017-01109, Expert Declaration of Rafail Ostrovsky, Ph.D.	
	277	L-0277	2018	C.A. No. 17-928 (LPS), "Defendant's Initial Invalidity Contentions"	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	278	L-0278	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'SDMI' and 'Portable Device Spec." (Bates numbered pages: ROKU_00005564 to 5598 containing document titled "SDMI Portable Device Specification, Part 1, Version 1.0, dated "8th July, 1999"	
	279	L-0279	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005948 to 5949 containing document titled "Liquid Audio Delivers Web Server and Production Tools For Online Music Commerce" dated "March 12, 1997")	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	280	L-0280	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005952 to 5953 containing document titled "Liquid Audio to Develop Internet Technology with Dolby" dated "Aug 26 1996")	
	281	L-0281	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered page: ROKU00005954 containing document titled "Liquid Audio Supports Solana's Digital Watermark System for Online Music Delivery" dated "Jan. 23, 1997")	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	282	L-0282	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005955 to ROKU00005956 containing document titled "IUMA Bets on Liquid Audio", dated "6.Dec.98.PST")	
	283	L-0283	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered pages: ROKU00005963 containing document beginning "Here is an online directory...." dated "4/24/97")	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	284	L-0284	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Num bered pages: ROKU00005964 to ROKU000065 containing document beginning "Utilizing an exclusive, enhanced version...." undated)	
	285	L-0285	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered page: ROKU00005966 containing document beginning "Liquid Audio is developing...." undated)	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	286	L-0286	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Liquid Audio,' 'Liquid Music,' and 'Liquid Server.' (Bates Numbered page: ROKU00005967 containing document titled "Liquid Audio fine tunes Music on Demand", undated)	
	287	L-0287	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Xerox Corp.' (Bates numbered pages: ROKU00005520 to ROKU00005521, containing document titled "ContentGuard Marketplace", undated)	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
	288	L-0288		Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Xerox Corp.' (Bates numbered pages: ROKU00005957 to ROKU00005958, document titled "CONTENTGUARD", undated)	
	289	L-0289	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Rights Server.' (Bates numbered page: ROKU00005961 to ROKU00005962, containing document titled "ContentGuard Rights Server", undated)	
		L-0290	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'ContentGuard' and 'Publisher.' (Bates numbered page: ROKU00005959 to ROKU00005960, containing document titled "ContentGuard Publisher", undated.)	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-0291	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Solana,' 'Electronic DNA,' 'E-DNA,' and 'Solana Technology.' (Bates numbered pages: ROKU00005950 to ROKU00005951, containing document titled "Solana's E-DNA Digital Watermark Technology to Protect Audio Distributed via the Net", dated "Jan, 1997")	
		L-0292	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Solana,' 'Electronic DNA,' 'E-DNA,' and 'Solana Technology.' (Bates numbered page: ROKU00005954, containing documen titled "Liquid Audio Supports Solana's Digital Watermark System for Online Music Delivery", dated "Jan. 23, 1997")	

DATE:	EXAMINER'S SIGNATURE:
03/15/2019	/DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-0293	2018	Blue Spike v. Roku C.A. No. 17-928 (LPS), Bates numbered pages resulting from search of Roku Bates number range ROKU00004985-ROKU00005974 for terms 'Digital River,' 'Digital,' and 'Secure Sales System.' (Bates numbered pages: ROKU00005773 to ROKU00005774, containing document titled "Digital River", undated)	
		L-0294		Index identifying Bates numbers pages containing alleged prior art, provided by defendant Roku in Blue Spike v Roku ligation, Blue Spike v. Roku C.A. No. 17-928 (LPS).	
		L-0295		ROKU5516-7, C. Guglielmo, Net Music with A Watermark, 1/17/1999	
		L-0296		L-0296 ROKU5518-19 Boscardin, 4/30/1997	
		L-0297		L-0297 ROKU 5520-5521 ContentGuard, 4/7/2000	
		L-0298		L-0298 ROKU 0000553, 11/2/1998	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-0299		L-0299 ROKU5600-02,1/17/1999	
		L-0300		L-0300 ROKU5967-74 Giles, 6/19/1997	
		L-301	2018	Expert Report of Dr. Markus Jakobsson, PH.D. December 3, 2018	
		L-301A	2018	Exhibits A-1 to A-5 of L-301	
		L-301B	2018	Exhibits B-1 to B-5 of L-301	
		L-301C	2018	Exhibits C-1 to C-5 of L-301	
		L-301D	2018	Exhibits D-1 to D-5 of L-301	
		L-301E	2018	Exhibits E-1 to E-5 of L-301	
		L-302		L-302 Tamper Resistant Software: An Implementation. Date unknown.	
		L-303	2018	L-303 Creating multi-DRM protected videos with free tools - Axinom	
		L-304	1976	L-304 Hellmanm, New Directions in Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-305	2018	L-305 DIVX (Digital Video Express) (1998 – 1999)	
		L-306		L-306 Electronic Watermark	
		L-307	2018	L-307 First open source W3C EME solution provided on the 96Boards HiKey platform Posted on Tuesday, June 14, 2016 in Blog (/categories/#blog) By Linaro (/author/linaro/) Authors: Mark Gregotski and Zoltan Kuscsik	
		L-308		L-308 WasApple	
		L-309		L-309 Surviving a Standards War: Lessons Learned from The Life and Death of DIVX David Dranove and Neil Gandal1 January 2004	
		L-310		L-310 Testing Digital Watermark Resistance to Destruction Sabrina Sowers and Abdou Youssef† The George Washington University Department of Electrical Engineering and Computer Science Washington, DC USA 20052 {sowers, youssef}@seas.gwu.edu	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-311	Jul 1999	L-311 Information Hiding|A Survey Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.	
		L-312		L-312 On Software Protection Via Function Hiding Tomas Sander and Christian F. Tschudin International Computer Science Institute, Date unknown.	
		L-313	1998	L-313 Continuous Steganographic Data Transmission Using Uncompressed Audio Chr. Neubauer, J. Herre, and K. Brandenburg Fraunhofer Institut f¨ur Integrierte Schaltungen, 91058 Erlangen, Germany	
		L-314		L-314 Music and Media, January 27, 2001, Vol. 18, Issue 5	
		L-315	2018	L-315 Microsoft Unveils Windows Media Player for Palm-Size and Pocket PCs, January 6, 2000	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-316	2018	L-316 Marlin founders release technology specifications and announce developer conferences Open specifications for protected content sharing technology and community development initiatives to drive interoperability Sunnyvale, CA, May 8, 2006	
		L-317	2018	L-317 Marlin DRM Announces Solution for Enhanced Content Protection (ECP) for UHD Content January 15, 2018 03:01 AM Eastern Standard Time	
		L-318	2015	L-318 Linaro Clear Key, Jan 2015	
		L-319	2018	Legacy Windows Media License Agreements Applies to: Windows Media Player	
		L-320	2018	L-320 Unlocking the iPod Jon Johansen became a geek hero by breaking the DVD code. Now he's liberating iTunes - whether Apple likes it or not. By Robert Levine, Fortune October 23 2006: 2:54 PM EDT	
		L-321		L-321 Exploring Steganography: Seeing the Unseen by Neil Johnson and Sushil Jajoda, Hua Li, October 6, 1999, date Unknown	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

EXAMINER INITIAL	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a	REFERENCES CITED AND CONSIDERED BY EXAMINER IN PARENT CASE IDENTIFIED BY PLACEMENT OF "X"
		L-322		L-322 Intellectual Property Protection Systems and Digital Watermarking Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, James H. Snyder, date unknown.	
		L-323	2018	L-323 The Incredibly Technical History of Digital Rights Management, Ernie Smith 10, 19, 2017,	
		L-324		L-324 Robust Digital Watermarking Based on Key-Dependent Basis Functions Jiri Fridrich, date unknown	

DATE: 03/15/2019	EXAMINER'S SIGNATURE: /DENNIS G BONSHOCK/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Reexamination Control Number: 90014138
Confirmation No: 7638
RE: Reexamination of USP 9104842

Patent Owner Information Disclosure Statement

The patentee previously submitted and IDS listing references U1 to U480; P1 to P102; F1 to F37; and L1 to L301 and provided copies where necessary.

This IDS cites and provides copies of additional references L302-L328

The undersigned was advised by USPTO officials that no fee is due when filing an IDS in a reexamination.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

				Reexamination Control Number: **90014138**	
		L-302		L-302_Tamper Resistant Software: An Implementation. Date unknown.	
		L-303	2018	L-303_Creating multi-DRM protected videos with free tools - Axinom	
		L-304	1976	L-304_Hellmanm, New Directions in Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976	
		L-305	2018	L-305_DIVX (Digital Video Express) (1998 – 1999)	
		L-306		L-306_Electronic Watermark	
		L-307	2018	L-307_First open source W3C EME solution provided on the 96Boards HiKey platform Posted on Tuesday, June 14, 2016 in Blog (/categories/#blog) By Linaro (/author/linaro/) Authors: Mark Gregotski and Zoltan Kuscsik	
		L-308		L-308_WasApple	
		L-309		L-309_Surviving a Standards War: Lessons Learned from The Life and Death of DIVX David Dranove and Neil Gandal1 January 2004	
		L-310		L-310_Testing Digital Watermark Resistance to Destruction Sabrina Sowers and Abdou Youssef† The George Washington University Department of Electrical Engineering and Computer Science Washington, DC USA 20052 {sowers, youssef}@seas.gwu.edu	
		L-311	Jul 1999	L-311_Information Hiding|A Survey Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.	

/DENNIS G BONSHOCK/ 03/26/2019

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

				Reexamination Control Number: **90014138**	
		L-312		L-312_On Software Protection Via Function Hiding Tomas Sander and Christian F. Tschudin International Computer Science Institute, Date unknown.	
		L-313	1998	L-313_Continuous Steganographic Data Transmission Using Uncompressed Audio Chr. Neubauer, J. Herre, and K. Brandenburg Fraunhofer Institut f˙ur Integrierte Schaltungen, 91058 Erlangen, Germany	
		L-314		L-314_Music and Media, January 27, 2001, Vol. 18, Issue 5	
		L-315	2018	L-315_Microsoft Unveils Windows Media Player for Palm-Size and Pocket PCs, January 6, 2000	
		L-316	2018	L-316_Marlin founders release technology specifications and announce developer conferences Open specifications for protected content sharing technology and community development initiatives to drive interoperability Sunnyvale, CA, May 8, 2006	
		L-317	2018	L-317_Marlin DRM Announces Solution for Enhanced Content Protection (ECP) for UHD Content January 15, 2018 03:01 AM Eastern Standard Time	
		L-318	2015	L-318_Linaro Clear Key, Jan 2015	
		L-319	2018	Legacy Windows Media License Agreements Applies to: Windows Media Player	
		L-320	2018	L-320 Unlocking the iPod Jon Johansen became a geek hero by breaking the DVD code. Now he's liberating iTunes - whether Apple likes it or not. By Robert Levine, Fortune October 23 2006: 2:54 PM EDT	

/DENNIS G BONSHOCK/ 03/26/2019

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

				Reexamination Control Number: **90014138**	
		L-321		L-321_Exploring Steganography: Seeing the Unseen by Neil Johnson and Sushil Jajoda, Hua Li, October 6, 1999, date Unknown	
		L-322		L-322_Intellectual Property Protection Systems and Digital Watermarking Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, James H. Snyder, date unknown.	
		L-323	2018	L-323_The Incredibly Technical History of Digital Rights Management, Ernie Smith 10, 19, 2017,	
		L-324		L-324_Robust Digital Watermarking Based on Key-Dependent Basis Functions Jiri Fridrich, date unknown	
		L-325	2019	L-325 DI 36 2019-02-26 STATEMENT Joint Claim Construction and Prehearing Statement, Case 2:19-cv-00748-JAK-JPR Document 36	
		L-326	2019	L-326 DI 39 2019-03-05 BRIEF filed by def Opening Claim Construction Brief, Case 2:19-cv-00748-JAK-JPR Document 39	
		L-327	2019	L-327 DI 40 2019-03-05 OPENING CLAIM CONSTRUCTION BRIEF, Case 2:19-cv-00748-JAK-JPR Document 40	
		L-328	2019	L-328 3/10/2019 Email identifying copyright registration titled "Giovanni Master (audio digital watermark source code)", Claimant Scott Moskowitz, Registration Number/Date "TXu000892516/1999-02-08"; and Date of Creation: "1999."	

Truly,

/RichardNeifeld/
RICHARD NEIFELD, ATTORNEY FOR PATENTE
REG. NO. 35,299

/DENNIS G BONSHOCK/ 03/26/2019

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

Reexamination Control Number: 90014138
Confirmation No: 7638
RE: Reexamination of USP 9104842

37 CFR 1.234 Certificate of Service

I served by first class mail (priority mail):
In paper format:
This IDS and Certificate of Service
On a portable USB drive:
Copies of references L302-L328

on the third parte reexamination requestor at his correspondence address:

Attn: Joseph P. Edell
FISCH SIGLER LLP
5301 WISCONSIN AVENUE, NW
FOURTH FLOOR
WASHINGTON, DC 20015

Date of Service: 3-25-2019

/RichardNeifeld/
Richard Neifeld, Reg. No. 35,299
Attorney for patent owner

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,138	05/16/2018	9104842		7638

31518 7590 06/28/2019

NEIFELD IP LAW, PC
5400 Shawnee Road
Suite 310
ALEXANDRIA, VA 22312-2300

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/28/2019	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Joseph F. Edell
Fisch Sigler LLP
5301 Wisconsin Ave, NW
Fourth Floor
Washington, DC 20015

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,138* .

PATENT UNDER REEXAMINATION *9104842* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

Notice of Intent to Issue Ex Parte Reexamination Certificate	**Control No.** 90/014,138	**Patent Under Reexamination** 9104842	
	Examiner DENNIS G BONSHOCK	**Art Unit** 3992	**AIA Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☑ Prosecution on the merits is (or remains) closed in this *ex parte* reexamination proceeding. This proceeding is subject to reopening at the initiative of the Office or upon petition. *Cf.* 37 CFR 1.313(a). A Certificate will be issued in view of
   (a) ☐ Patent owner's communication(s) filed: _____.
   (b) ☑ Patent owner's failure to file an appropriate timely response to the Office action mailed: 01 April 2019.
   (c) ☐ Patent owner's failure to timely file an Appeal Brief (37 CFR 41.31).
   (d) ☐ The decision on appeal by the ☐ Board of Patent Appeals and Interferences ☐ Court dated _____
   (e) ☐ Other: _____.
2. The Reexamination Certificate will indicate the following:
   (a) Change in the Specification: ☐ Yes ☑ No
   (b) Change in the Drawing(s): ☐ Yes ☑ No
   (c) Status of the Claim(s):
      (1) Patent claim(s) confirmed: 11 and 13.
      (2) Patent claim(s) amended (including dependent on amended claim(s)): _____
      (3) Patent claim(s) canceled: 12 and 14.
      (4) Newly presented claim(s) patentable: _____.
      (5) Newly presented canceled claims: _____.
      (6) Patent claim(s) ☐ previously ☐ currently disclaimed: _____
      (7) Patent claim(s) not subject to reexamination: 1-10.
3. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
4. ☑ Note the attached statement of reasons for patentability and/or confirmation. Any comments considered necessary by patent owner regarding reasons for patentability and/or confirmation must be submitted promptly to avoid processing delays. Such submission(s) should be labeled: "Comments On Statement of Reasons for Patentability and/or Confirmation."
5. ☐ Note attached NOTICE OF REFERENCES CITED (PTO-892).
6. ☐ Note attached LIST OF REFERENCES CITED (PTO/SB/08 or PTO/SB/08 substitute).
7. ☐ The drawing correction request filed on _____ is: ☐approved ☐disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐None of the certified copies have
   ☐been received.
   ☐not been received.
   ☐been filed in Application No. _____.
   ☐been filed in reexamination Control No. _____.
   ☐been received by the International Bureau in PCT Application No. _____.

   * Certified copies not received: _____.
9. ☑ Note attached Examiner's Amendment.
10. ☐ Note attached Interview Summary (PTO-474).
11. ☐ Other: _____.

All correspondence relating to this reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	

cc: Requester (if third party requester)

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

ex parte Reexamination

This Office action address claims 11-14 of U.S. Patent Number: 9,104,842 issued to Moskowitz, hereinafter the '842 Patent. This action is responsive to the lack of a Patent Owners after-final response to the Final Office Action of 4/1/2019, which rejected patent claims 12 and 14 while noting reasons for confirmation of 11 and 13. It had been determined in the Order Granting *ex parte* Reexamination mailed 5/16/2018 that a substantial new question of patentability was raised in the Request for ex parte reexamination filed 2/11/2019.

EXAMINER'S AMENDMENT

Claims 12 and 14 were subject to rejection in the Final Office Action mailed 4/1/2019. Patent owner failed to timely respond to said Final Office Action on Application/Control Number: 90/014,138.

Accordingly claims 12 and 14 have been cancelled. See CFR 1.550(d) and MPEP § 2266.

Claims 12 and 14 are CANCELLED.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Beetcher encodes its software module prior to distribution using key data to lock portions of the software from being executed without the user providing an appropriate key for unlocking said portions. The software module code is modified in format to include entitlement verification triggers which themselves are made to encompass functions of the software and so positioned within the object code with an addressability alignment that has a simple relationship to the product number found in the key. This encoding meeting both definitions provided by the Patent Owner:

(a)

"In digital processing, **encode** and **decode** mean **changes in digital representation of information**."

(b)

In **computers**, **encoding is** the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding **is** the opposite process -- the conversion of an **encoded** format back into the original sequence of characters. Nov 14, 2005

Beetcher, however, is not as clear with its description of how this encoded software is again accessed. Though Beetcher makes clear that a key is required to access this reformatted content, it doesn't specify whether this key just unlocks the content for use or truly removes the encryption applied (decryption). It is for this reason that Beetcher is deemed ineffective in covering the limitations of claim 11 and claim 13.

Given the above cited reason, the lack of further clarification in the other Beetcher document (Exhibit 3), and the removal of Cooperman (Exhibit 6) and Hasebe (Exhibit 7) as prior art per declarations filed by the Patent owner **claims 11 and 13 are herein CONFIRMED.**

Any comments considered necessary by PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

Conclusion

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

By Mail to: Mail Stop Ex Parte Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900

Central Reexamination Unit

By hand: Customer Service Window

Randolph Building

401 Dulany Street

Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/DENNIS G BONSHOCK/
Primary Examiner, Art Unit 3992

Conferees:

/RSD/

/ALEXANDER J KOSOWSKI/
Supervisory Patent Examiner, Art Unit 3992

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

CPC								
Symbol							Type	Version
G06F	/	21	/	10			F	2013-01-01
G06F	/	21	/	602			I	2013-01-01
G06F	/	21	/	335			I	2013-01-01
G06T	/	1	/	0021			I	2013-01-01
H04L	/	9	/	3247			I	2013-01-01
G06F	/	21	/	6209			I	2013-01-01
H04L	/	9	/	065			I	2013-01-01
G06F	/	21	/	16			I	2013-01-01
G06F	/	21	/	125			I	2013-01-01
H04L	/	9	/	3236			I	2013-01-01
G06F	/	2211	/	007			A	2013-01-01
G06F	/	2221	/	2107			A	2013-01-01
H04L	/	2209	/	605			A	2013-01-01
G06F	/	2221	/	0737			A	2013-01-01
G06T	/	2201	/	0083			A	2013-01-01
G06T	/	2201	/	0064			A	2013-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

(Assistant Examiner)	(Date)	Total Claims Allowed: 2	
/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	13 June 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20190611

DISH-Blue Spike 842
Exhibit 1005, Page 1701

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F21/10	/	21	/	10
G06F21/60	/	21	/	60
G06F21/33	/	21	/	33
G06T1/00	/	1	/	00
H04L9/32	/	9	/	32
G06F21/62	/	21	/	62
H04L9/06	/	9	/	06
G06F21/16	/	21	/	16
G06F21/12	/	21	/	12

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

(Assistant Examiner)	(Date)	Total Claims Allowed: 2	
/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	13 June 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

(Assistant Examiner)	(Date)	Total Claims Allowed: 2	
/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	13 June 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office Part of Paper No.: 20190611

DISH-Blue Spike 842
Exhibit 1005, Page 1703

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Certificate Date	Certificate Number
		C1

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
Joseph F. Edell Fisch Sigler LLP 5301 Wisconsin Ave, NW Fourth Floor Washington, DC 20015

LITIGATION REVIEW ☑	/DGB/ (examiner initials)	2018-06-13T00:00:00 (date)
Case Name		Director Initials
6:17cv16		
6:18cv174		
6:18cv181		
6:18cv195		
6:18cv223		
1-18cv1406		
1-19cv160		
1-19cv158		
1-18cv1512		
1-18cv1427		
6-18cv333		
5-18cv3392		
6-18cv242		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,138	9104842
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Previous Prosecution Searched	06/20/2019	DGB
litigation Searched	06/20/2019	DGB

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

Lexis Advance®
Research

Document: July 2018 Retail Patent Litigation Report

July 2018 Retail Patent Litigation Report

Retail Patent Litigation Blog

November 20, 2018 Tuesday 12:00 PM EST

Copyright 2018 Newstex LLC All Rights Reserved

Length: 1244 words

Byline: R. David Donoghue

Body

Nov 20, 2018(Retail Patent Litigation Blog: http://www.retailpatentlitigation.com/ Delivered by Newstex) The typical summer filing trend continued in July. NPEs appeared to be on a summer break as filings remained low. Frequent filers included Coding Technologies, Internet Media Interactive and Landmark Technology. As usual, I prepared the report in partnership with and using Docket Navigator and its powerful database. Docket Navigator is a valuable resource, and the place to go if you want to keep track of new patent litigation filings or want to know what is happening in particular cases, how your judge has historically handled a particular type of motion, or a particular plaintiff's litigation history.

Finally, please let me know if you have thoughts about the report or changes you would like to see. I am preparing it as a service for retailers and their supply chain who may want an overview of the patent litigation landscape. So, I am very open to your suggestions for improving the report. Internet Media Interactive Corp. v. Build-A-Bear Workshop, Inc. (D. Del.; N.D. Ill.) (multiple cases). Judge: District Judge Charles P. Kocoras Claim: Infringement Defendants: Build-A-Bear Workshop, Inc. The Coca-Cola Company The Boeing Company Plaintiff: Internet Media Interactive Corp. Pls. Cnsl: Haller Law; and O'Keily Ernst ...yce Patent: 6,049,835 (System for providing easy access to the World Wide Web utilizing a published list of preselected Internet locations together with their unique multi-digit jump codes). Coding Technologies, LLC v. Xymogen, Inc. (M.D. Fla.; N.D. Ga.; D. Del.) (multiple cases). Judges: Magistrate Judge Gregory J. Kelly; District Judge Gregory A. Presnell; District Judge Anne C. Conway Claim: Infringement Defendants: Xymogen, Inc. Elmer's Products Inc. Primo Water Corporation SOL Republic, Inc. Delta Faucet Company Plaintiff: Coding Technologies, LLC Pls. Cnsl: Watson LLP; and Stamoulis ...inblatt Patent: 8,540,159 (Method for providing mobile service using code-pattern). Aeritas, LLC v. Best Buy Co., Inc. (E.D. Tex.). Claim: Infringement Defendant: Best Buy Co., Inc. Plaintiff: Aeritas, LLC Pls. Cnsl: DelGiorno

DISH-Blue Spike 842
Exhibit 1005, Page 1706

IP Law Patents: 8,055,285 (Mixed-mode interaction); 9,390,435 (Mixed-mode interaction); and 9,888,107 (Mixed-mode interaction). Sookbox Development LLC v. Walmart Inc. f/k/a Wal-Mart Stores, Inc. (E.D. Tex.) (multiple cases). Claim: Infringement Defendants: Walmart Inc. f/k/a Wal-Mart Stores, Inc. Fry's Electronics, Inc. Best Buy Co., Inc. Plaintiff: Sookbox Development LLC Pls. Cnsl: Chaudhari Law Patent: 9,497,137 (Digital content connectivity and control via a plurality of controllers that are treated discriminatively). Allconnect, Inc. v. Consumer Brands, LLC (C.D. Cal.; W.D. Tex.) (multiple cases). Judge: District Judge Lee Yeakel ⋙ Claim: Infringement Defendants: Consumer Brands, LLC Microbrand Media, LLC Kandela, LLC Plaintiff: Allconnect, Inc. Pls. Cnsl: Morris Manning ...rtin; and Russ August ...bat Patents: 8,346,624 (Systems and methods for recommending third party products and services); and 8,433,617 (Systems and methods for identifying third party products and services available at a geographic location). Landmark Technology, LLC v. Learning Resources, Inc. (N.D. Ill.). Judge: District Judge Robert W. Gettleman ⋙ Claim: Infringement Defendant: Learning Resources, Inc. Plaintiff: Landmark Technology, LLC Pls. Cnsl: Rabicoff Law Patent: 6,289,319 (Automatic business and financial transaction processing system). UnoWeb Virtual, LLC v. Alibaba.com Hong Kong Limited (E.D. Tex.) (multiple cases). Judge: District Judge Rodney Gilstrap ⋙ Claim: Infringement Defendants: com Hong Kong Limited com Limited Sears Holdings Corporation Plaintiff: UnoWeb Virtual, LLC Pls. Cnsl: Capshaw DeRieux; and Carsten Law Patents: 8,307,047 (Method of a first host of first content retrieving second content from a second host and presenting both contents to a user); 9,589,273 (Method of three-level hosting infrastructure); and 8,037,091 (Method of using a code to track user access to content). Wapp Tech Limited Partnership et al v. Hewlett Packard Enterprise Company (E.D. Tex.) (multiple cases). Claim: Infringement Defendants: Hewlett Packard Enterprise Company Micro Focus International plc Wells Fargo ...mpany Bank of America Corp. Plaintiffs: Wapp Tech Corp. Wapp Tech Limited Partnership Pls. Cnsl: Toler Law Group Patents: 8,924,192 (Systems including network simulation for mobile application development and online marketplaces for mobile application distribution, revenue sharing, content distribution, or combinations thereof); 9,298,864 (System including network simulation for mobile application development); and 9,971,678 (Systems including device and network simulation for mobile application development). Hawk Technology Systems, LLC v. Treasure Island, LLC, et al. (D. Nev.). Judges: District Judge Richard F. Boulware, II ⋙; Magistrate Judge George Foley, Jr. ⋙ Claim: Infringement Defendant: Treasure Island, LLC Plaintiff: Hawk Technology Systems, LLC Pls. Cnsl: Law Office of Kurt C. Lambeth Patents: RE 37,342 (Dual format digital video production system); and RE 43,462 (Video monitoring and conferencing system). Chapterhouse, LLC v. Shopify, Inc. (E.D. Tex.). Judge: District Judge Rodney Gilstrap ⋙ Claim: Infringement Defendant: Shopify, Inc. Plaintiff: Chapterhouse, LLC Pls. Cnsl: The Mort Law Firm Patents: 7,552,087 (Electronic transaction receipt system and method); 7,742,989 (Digital receipt generation from information electronically read from product); 8,112,356 (System and method for providing automated secondary purchase opportunities to consumers); and 8,606,698 (Electronic transaction receipt system and method). Riggs Technology Holdings, LLC v. McGraw-Hill Education, Inc. (D. Del.) (multiple cases). Claim: Infringement Defendants: McGraw-Hill Education, Inc. Internet Brands, Inc. Thomson Reuters USA Inc. Plaintiff: Riggs Technology Holdings, LLC Pls. Cnsl: Rabicoff Law; and Stamoulis ...inblatt Patent: 7,299,067 (Methods and systems for managing the provision of training provided remotely through electronic data networks to users of remote electronic devices). Blue Spike LLC v. Dish Network Corporation et al. (E.D. Tex.) (multiple cases). Claim: Infringement Defendants: DISH Network Corporation DISH Network LLC Dish Network Service LLC American Airlines Group Inc. American Airlines, Inc. Plaintiff: Blue Spike LLC Pls. Cnsl: Garteiser Honea Patents: 7,159,116 (Systems, methods and devices for trusted transactions); 7,287,275 (Methods, systems and devices for packet watermarking and efficient provisioning of bandwidth); 7,475,246 (Secure personal content server); 8,224,705 (Methods, systems and devices for packet watermarking and efficient provisioning of bandwidth); 8,473,746 (Methods, systems and devices for packet watermarking and efficient provisioning of bandwidth); 8,538,011 (Systems, methods and devices for trusted transactions); 8,739,295 (Secure personal content server); 9,021,602 (Data protection method and device); **9,104,842** (Data protection method and device); 9,934,408 (Secure personal content server); RE 44,222 (Methods, systems and devices for packet watermarking and efficient provisioning of bandwidth); RE 44,307 (Methods, systems and devices for packet watermarking and efficient provisioning of bandwidth); and 7,664,263 (Method for combining transfer functions with predetermined key creation).

DISH-Blue Spike 842
Exhibit 1005, Page 1707

Classification

Language: English

Publication-Type: Web Blog

Journal Code: CHIC-116304

Subject: LITIGATION (88%); JUDGES (87%); PATENTS (86%); TRENDS (68%); BLOGS & MESSAGE BOARDS (63%); Hawk Technology; Retail Litigation Report; Landmark Technology; Internet Media Interactive; Coding Technologies

Company: BUILD-A-BEAR WORKSHOP INC (91%); COCA-COLA CO (67%); BOEING CO (67%); BEST BUY CO INC (65%); PRIMO WATER CORP (64%); ELMER'S PRODUCTS INC (64%); DELTA FAUCET CO (64%); WAL-MART STORES INC (63%); FRY'S ELECTRONICS INC (60%); O'KELLY ERNST & BIELLI LLC (54%)

Ticker: BBW (NYSE) (91%); KO (NYSE) (67%); BOE (LSE) (67%); BA (NYSE) (67%); BBY (NYSE) (65%); PRMW (NASDAQ) (64%); WMT (NYSE) (63%)

Industry: RETAILERS (68%); BLOGS & MESSAGE BOARDS (63%)

Load-Date: November 20, 2018

Content Type: News

Terms: 9104842 or 9,104,842

Narrow By: -None-

Date and Time: Jun 13, 2019 10:52:42 a.m. EDT

DISH-Blue Spike 842
Exhibit 1005, Page 1708

LexisNexis® About LexisNexis® Privacy Policy Terms & Conditions Sign Out Copyright © 2019 LexisNexis. All rights reserved. RELX Group™

US009104842C1

(12) EX PARTE REEXAMINATION CERTIFICATE (11540th)

United States Patent
Moskowitz

(10) **Number: US 9,104,842 C1**
(45) **Certificate Issued: Jul. 17, 2019**

(54) **DATA PROTECTION METHOD AND DEVICE**

(75) Inventor: **Scott A. Moskowitz**, Sunny Isles Beach, FL (US)

(73) Assignee: **WISTARIA TRADING LTD**

Reexamination Request:
No. 90/014,138, May 16, 2018

Reexamination Certificate for:
Patent No.: **9,104,842**
Issued: **Aug. 11, 2015**
Appl. No.: **11/895,388**
Filed: **Aug. 24, 2007**

Related U.S. Application Data

(60) Division of application No. 10/602,777, filed on Jun. 25, 2003, now Pat. No. 7,664,263, which is a continuation of application No. 09/046,627, filed on Mar. 24, 1998, now Pat. No. 6,598,162.

(51) **Int. Cl.**

G06F 21/10	(2013.01)
G06F 21/60	(2013.01)
G06F 21/33	(2013.01)
G06T 1/00	(2006.01)
H04L 9/32	(2006.01)
G06F 21/62	(2013.01)
H04L 9/06	(2006.01)
G06F 21/16	(2013.01)
G06F 21/12	(2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/10*** (2013.01); ***G06F 21/125*** (2013.01); ***G06F 21/16*** (2013.01); ***G06F 21/335*** (2013.01); ***G06F 21/602*** (2013.01); ***G06F 21/6209*** (2013.01); ***G06T 1/0021*** (2013.01); ***H04L 9/065*** (2013.01); ***H04L 9/3236*** (2013.01); ***H04L 9/3247*** (2013.01); *G06F 2211/007* (2013.01); *G06F 2221/0737* (2013.01); *G06F 2221/2107* (2013.01); *G06T 2201/0064* (2013.01); *G06T 2201/0083* (2013.01); *H04L 2209/605* (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

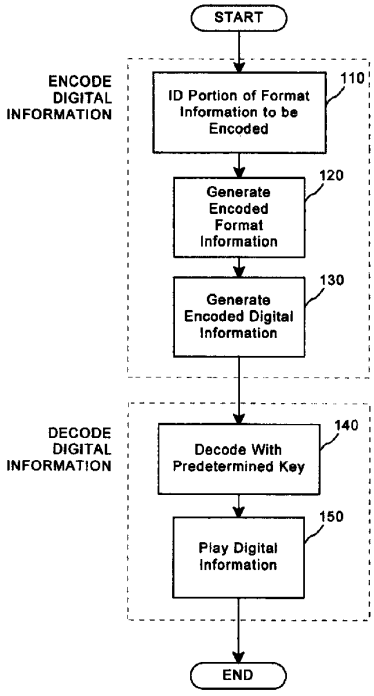
(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/014,138, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner — Dennis G Bonshock

(57) **ABSTRACT**

An apparatus and method for encoding and decoding additional information into a digital information in an integral manner. More particularly, the invention relates to a method and device for data protection.



EX PARTE REEXAMINATION CERTIFICATE

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **11** and **13** is confirmed.

Claims **12** and **14** are cancelled.

Claims **1-10** were not reexamined.

* * * * *