(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2004 (24.06.2004)

PCT

(10) International Publication Number
WO 2004/053720 A1

(51) International Patent Classification[7]: G06F 17/00, 15/16, 11/30, 17/60

(21) International Application Number: PCT/US2003/031630

(22) International Filing Date: 6 October 2003 (06.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/415,991	5 October 2002 (05.10.2002)	US
60/478,985	14 June 2003 (14.06.2003)	US
60/492,774	4 August 2003 (04.08.2003)	US
60/499,761	3 September 2003 (03.09.2003)	US
60/500,897	4 September 2003 (04.09.2003)	US
60/506,115	25 September 2003 (25.09.2003)	US

(71) Applicant *(for all designated States except US)*: **INLET IP HOLDINGS LLC** [US/US]; P.O. Box 1383, Marlton, NJ 08053-6383 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **FRIEND, Jeffrey, Edward** [US/US]; 715 Kettle Run Rd., Marlton, NJ 08053 (US).

(74) Agent: **NEUNER, George, W.**; Edwards & Angell, LLP, P.O. Box 9169, Boston, MA 02209 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

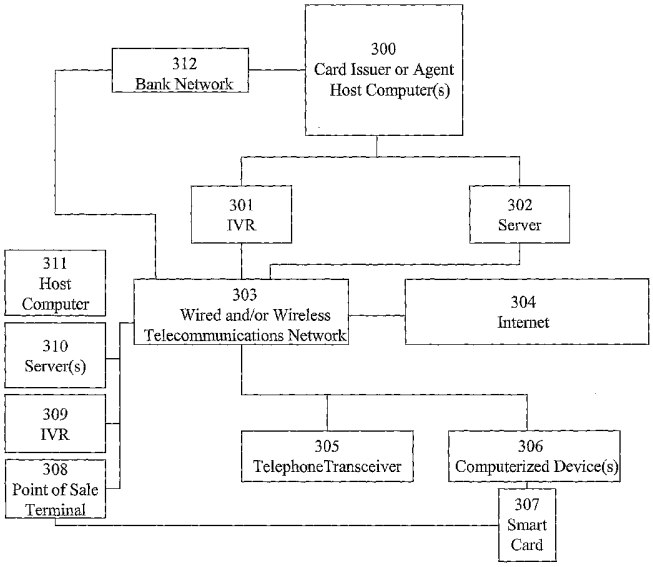
Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: SECURE SYSTEM FOR CREATING AND PROCESSING DIGITAL SIGNATURES AND METHOD FOR USE THEREOF



(57) Abstract: The present invention provides for the enhancement of security for electronic commerce transactions through use of a transaction identification number (TIN) capable of operating as a proxy and also a user digital signature. For transactions involving the transfer of digital content, the invention further provides for the user digital digital signature to be embedded in the digital content in the course of the transaction. Operating in conjunction with Card Issuer or Agent Host Computer(s) (300) are an account manager, a user database, a TIN, a MAC Coding Unit and Comparator, and a traditional Processing System. In addition, other participants may be involved in some phases of the transaction such as settlement institutions collectively represented as Bank Network (312).

WO 2004/053720 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE SYSTEM FOR CREATING AND PROCESSING DIGITAL SIGNATURES AND METHOD FOR USE THEREOF

This application claims as priority U.S. Provisional Patent Applications 60/415991 filed 10/5/02 entitled "System and Method for Creating and Processing Digital Signatures Using Intelligent Authorization," 60/478985 filed 6/14/03 entitled "Secure System for Processing Digital Signatures and Method for Use Thereof," 60/ filed 8/04/03 entitled "Secure System for Processing Digital Signatures Using Clock Signal Activation and Private Key Transfer," 60/ filed 9/02/03 entitled "Secure System for Processing Digital Signatures Using Clock Signal Activation and Secret Key Transfer," and 60/ filed 9/04/03 entitled "Secure System for Processing Digital Signatures Using Clock Signal Activation and Secret Key Transfer," and 60/ filed 9/25/03 entitled "Secure System for Processing Digital Signatures and Method for Use Thereof."

FIELD OF INVENTION

A system and method for creating and processing digital signatures. More specifically, a system and method for enhancing the security of electronic commerce transactions through use of a transaction identification number capable of operating as both a proxy account number and digital signature.

BACKGROUND OF THE INVENTION

Digital signatures are destined to play a critical role in the future of electronic commerce. The integrity of electronic transactions and the Internet marketplace as a whole depends on the ability to reliably authenticate the various parties to a transaction and to correctly identify and account for the information exchanged between them.

One important area of application for digital signatures is Digital Rights Management (DRM), the business involved with mass distribution of proprietary digital content over the Internet (e.g. music, movies, games, digital telephone jingles, video, photographs, software, news & magazine articles, research data, tickets, coupons, etc.).

The primary purpose of DRM is to establish a system for controlling distribution so as to guarantee the maximum return on value of digital content for content distributors, owners and creators. Naturally, a big part of this is the need for security protections to guard against unauthorized use and distribution of licensed digital content.

Complicating this need for security is the commitment major media companies have to the practice commonly referred to in the industry as "super distribution." This is when a consumer who has legally purchased or licensed some form of digital content has the desire to share the content with an associate or friend who they feel might enjoy it as much as them. Digital content owners and creators such as music record label executives and recording artists see super distribution as invaluable to getting the word out about a new song, CD or video. They have made it abundantly clear that for any DRM security solution to be embraced by the industry, it must support super distribution.

One of the more interesting conclusions being reached by experts in the field is that for a security solution to be effective, it does not necessarily have to provide a foolproof means of preventing unauthorized use or distribution of digital content. Rather, an effective approach to security would be to provide a tamperproof means of binding a user's identity to the digital content they purchase and use, for instance through the embedding of a user digital signature. Research shows that simply knowing their identity is permanently bound to a copy of digital content would be enough to deter the vast majority of users from risking its unauthorized use or distribution. And should such a copy end up being illegally copied and distributed, the presence of the digital signature would also provide a means for any suspicious copies to be traced back to the original point of purchase and ultimately the buyer of record.

In light of the above, there is another aspect of security that needs to be addressed for any DRM system to be truly effective. It is critical that both providers (i.e. content distributors, owners, and creators) and users to have a high degree of confidence in the metadata accompanying digital content. Ensuring the integrity of metadata makes it possible for providers and users to know with certainty the creator or source of the content, that the content has not been tampered with or altered, and that the content was legally distributed and obtained, etc. The list of information able to be

conveyed through metadata is long and varied and can include, for example, updated statistics regarding the runtime of applications involving the use of digital content (e.g. movie, song, game, etc). This is an area in which again the application of a user digital signature can be valuable to the overall security of a DRM system.

Serving as a backdrop to the introduction of the invention is also the pressure being applied today by merchants on card issuers (e.g. banks) and their agents (e.g. acquirer processors, merchant banks, etc.) to lower the fees (e.g. interchange fees, discount fees, per transaction fees, etc.) charged in conjunction with credit and debit card transactions. As a result, it would seem there is a clear need in the marketplace from the perspective of banks and other players in the credit card industry for the introduction of value added services capable of providing an incentive for either maintaining or increasing the current fees charged for transactions or increasing the overall total volume of card-based transactions.

In accordance with the above, it is desirable to provide a means for creating and processing user digital signatures for protection against the illegal distribution of digital content by binding user identity to distributed digital content without creating an impediment to the industry supported practice of super distribution.

Further, it is desirable to provide a means of creating and processing user digital signatures that helps to ensure a high degree of confidence in the metadata accompanying licensed digital content to the benefit of both digital content providers and users.

Further, it is desirable to provide a means of creating and processing user digital signatures whereby credit and debit card numbers are incorporated in a way that poses no risk to customer accounts while at the same time makes possible value added services capable of providing incentives for supporting or even increasing the fees charged for card-based transactions.

Note that while the invention may be ideally suited for use in conjunction with a DRM system and the purchase, leasing or rental of licensed digital content as well as other described alternative embodiments, it is to be understood that one or more of the innovations disclosed herein are likely to be generally applicable to other digital data environments and applications not necessarily involving licensed digital content or the other

described alternative embodiments. The invention is also not to be limited by use of the description "user digital signature" and may in fact be implemented on behalf of entities other than individual users (e.g. companies, clubs, groups, governmental bodies, network systems, operating systems, software clients or agents, central processing units, etc.).

SUMMARY OF THE INVENTION

The present invention provides for the enhancement of security for electronic commerce transactions through use of a transaction identification number (TIN) capable of operating as a proxy or "limited use" user account number (e.g. credit or debit card, checking, social security, etc.) and also a user digital signature. For transactions involving the transfer of digital content (e.g. music, movies, games, digital telephone jingles, video, photographs, software, news & magazine articles, research data, tickets, coupons, etc.), the invention further provides for the user digital signature to be embedded in the digital content in the course of the transaction.

According to one embodiment of the invention, the runtime cycle of an application operating in conjunction with a user computerized device is used as a measure for signaling the start of the digital signing process. Another embodiment is provided in which the runtime cycle of a microprocessor is used as a measure for signaling the start of the digital signing process. Yet another embodiment is provided in which actual time is used as a measure for signaling the start of the digital signing process.

The invention further provides a system and method in which a first party is able to transfer digital content to a second party or parties wherein the second party or parties is able to be authenticated, the digital signature of the first party authenticated, any relevant data (e.g. metadata such as licensing rights) updated, a second party or parties user digital signature created and embedded in the transferred digital content in the course of the transaction. In addition, the invention provides for the presence of a first party or parties user digital signature(s) in digital content transferred to a second party or parties to function as a signal for a process in which the subsequent electronic commerce transactions involving the transferred digital content result in a monetary and/or non-monetary credit being applied to the first party or parties account(s) as an incentive or commission.

Another aspect of the invention provides for a user digital signature to function as a digital "hall pass" for facilitating secure user access to web sites featuring "pay per view" or "pay per use" digital content. In addition, the user digital signature is also able to operate as a key useful in facilitating the transfer of push media messages (e.g. target email, instant messaging) from merchants (e.g. digital content providers) to users.

In the case of target email messages, another aspect of the invention provides for a dynamic online email catalog to serve as an intermediary tool for receiving, distributing, and ranking for display target email messages sent by merchants to users and whereby users are able to access, view and respond to stored and managed email messages.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an example of one embodiment of the TIN in the form of a 16-digit proxy account number (e.g. credit or debit card account) with an embedded message authentication code (MAC) and date and/or time stamp.

FIG. 2 illustrates an embodiment of that aspect of the invention involved with the creation of an embedded MAC from various input parameters.

FIG. 3 illustrates components of a system in accord with an embodiment of the present invention for processing digital signatures.

FIG. 4 illustrates an embodiment of that aspect of the invention involved with digitally signing various data types (e.g. DOIs, URLs, metadata), services (e.g. email) and dynamic mechanisms (e.g. java applet, as part of the process of resolving a DOI through use of the "Handle System" either through direct input from the user or through the use of an agent.

FIG. 5 is an illustration useful in describing that aspect of the invention involved with the use of the runtime cycle of an application (e.g. movie, song, video game, etc.) as a measure for signaling the start of a process involving the creation and application of digital signatures.

FIG. 5A illustrates an embodiment of the invention involved with the use of a runtime cycle of a microprocessor as a measure for signaling the start of a process involving the creation and application of digital signatures.

FIG. 5B illustrates an embodiment of the invention involved with the use of time as a measure for signaling the start of a process involving the creation and application of digital signatures.

FIG. 6 illustrates steps involved with one embodiment of a method for using the runtime cycle of an application (e.g. movie, song, video game, etc.) as a measure for signaling the start of a process involving the creation and application of digital signatures.

FIG. 6A illustrates steps involved with one embodiment of a method for using clock signal activation as a means for signaling the start of a process involving the creation and application of digital signatures.

FIG. 6B illustrates steps involved with one embodiment of a method for using time as a means for signaling the start of a process involving the creation and application of digital signatures.

FIG. 7 is an illustration useful in describing that aspect of the invention involved with the transfer of digital content by a first party to a secure intermediary location (e.g. card issuer or agent host computer(s) thereby restricting its distribution to one or more second parties to a process involving the creation and application of a user digital signature(s).

FIG. 7A illustrates steps involved with one embodiment of a method for verifying the identity of the "user of record" for signed digital content suspected of being used, copied or shared in violation of the license agreement.

FIG. 8 illustrates an embodiment of the graphical user interface of a Dynamic Online Email Catalog.

FIG. 9 illustrates an embodiment of a pseudo email address with date and/or time stamp.

FIG. 10 illustrates an embodiment of a method describing generally the steps involved with the generation, issuance and use of pseudo email addresses.

FIG. 11 is a block diagram useful in illustrating a search apparatus useful for searching a database of records (e.g. Internet records) in which results are able to be displayed in rank order based upon different functions of time (e.g. average) with respect to the length of time (i.e. life span) that individual user email addresses or different aggregate groups of user email addresses have been established with a particular second party (e.g. merchant) or a group of second parties (e.g. merchant affiliate network).

DETAILED DESCRIPTION OF THE INVENTION
INCLUDING THE PREFERRED EMBODIMENTS

FIG. 1 illustrates an example of one embodiment of a transaction identification number (TIN) in the form of a 16-digit proxy account number (e.g. credit or debit card account) with an embedded message authentication code (MAC) and a date stamp and time stamp.

The example shown includes a single-digit lead-in identifier useful in identifying the card network (e.g. Visa or Mastercard), a seven-digit bank identification number (BIN) useful in identifying the card issuer, a four-digit user (customer) identification number, and a single-digit checksum compliant with conventional card network operations.

The TIN as illustrated represents an improvement to similar proxy account numbers contained in existing and pending U.S. patents. For the purpose of this application incorporated by reference is U.S. Patent 6,000,832 entitled "Electronic online commerce card with customer generated transaction proxy number for online transactions."

Alternative embodiments of the present invention provide for various combinations comprising one or more of the featured identifiers in varying order and for those identifiers to inhabit varying lengths of fields that could have a total length equal to, less than, or greater than 16 digits.

For example, one alternative embodiment could involve a TIN comprising a user identifier portion, a multiple-digit MAC portion, a date stamp portion and time stamp portion. This would be applicable in the scenario in which the TIN would not be required to conform to the attributes of a proxy credit or debit card number for the purpose of facilitating electronic payment.

Another example is an alternative embodiment in which the date stamp might take the form of a year expressed in terms of "99" instead of the illustrated "1999" and a time stamp expressed in hours and minutes instead of the illustrated "120000" showing hours, minutes and seconds. Another alternative embodiment provides for milliseconds or other fractional time representations to be included. There is also the possibility of either just a date stamp portion or a time stamp portion.

The TIN might also include other information fields for identifiers not featured. For example, one alternative embodiment could involve a

merchant (e.g. digital content provider) and/or agent identifier portion in addition to other identifier portions (e.g. transaction authorization number).

The various ways to limit the form and use of the TIN is subject only to practical considerations and the writing of application software to operate the system with such limitations.

FIG. 2 illustrates an embodiment of that aspect of the invention involved with the creation of a MAC from various input parameters. The MAC is generated as a function of various inputs from a list including a user private or secret key, user-specific information (e.g. name, account number, etc.) and transaction specific data [e.g. transaction amount, merchant ID, goods or services IDs including Digital Object Identifier (DOI), Uniform Resource Locator (URL), identifiers for services such as email and dynamic mechanisms such as java applets and Common Gateway Interface (CGI) Scripts, various types of data including the message digest or hash of a document, various types of metadata including content licensing rights and updated statistics regarding application operation, date and/or time of transaction, digital signature generation or application, authorization, etc.].

In addition to the above examples of user-specific information being used in the formation of a MAC, there is also an embodiment involving the input of biometric information either previously stored to memory or gathered as part of an ongoing electronic commerce transaction. One embodiment involves the use of a computerized device (e.g. smart card) enabled with an integrated biometric sensor with means of creating a real-time digital scan of a thumb or fingerprint and comparing the result to a scan securely stored within the smart card. Another embodiment involves the creation of a real-time digital scan of a thumb or fingerprint and transferring the result for second or third party verification during the course of an electronic commerce transaction. An example of prior art describing a device capable of performing such a function is U.S. Patent Application 20020095587 filed January 17, 2001 and entitled "Smart card with integrated biometric sensor."

Another embodiment for inputting biometric information involves the creation of digital scan from a user's voice. This could be accomplished by storing a voice scan with the merchant or a trusted third party (e.g. bank). This scan could then be compared to one created in real time from a user's voice recorded while talking during the placement of an order for digital

content over the telephone or a scan created prior to a transaction by having a user speak into an enabled computerized device.

Various types of biometric information (e.g. retina scan, facial scan, digital photograph and video, etc.) and various means for incorporating such information for use with the present invention will be obvious to those skilled in the art.

The alternatives involving the input of biometric information makes another embodiment possible in which no private key is used to render the MAC, only one or more of other various inputs.

Each of the above described embodiments represent improvements over those embodiments described in U.S. Patent 6,000,832.

FIG. 3 illustrates components of a system in accord with an embodiment of the present invention for processing digital signatures. Central to this system is Card Issuer or Agent Host Computer(s) 300 in which those processes are housed to meet the various requirements of the invention. The card issuer agents might include other types of card-issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. In addition, other participants may be involved in some phases of the transaction such as intermediary settlement institutions collectively represented as Bank Network 312.

Operating in conjunction with Card Issuer or Agent Host Computer(s) 300 is an account manager and a user database. The account manager is preferably implemented in software that executes on Card Issuer or Agent Host Computer(s) 300, such as a relational database that manages the user database. Also operating in conjunction with Card Issuer or Agent Host Computer(s) 300 is a Transaction Number Identifier, a MAC Coding Unit and Comparator, and a traditional Processing System.

Card Issuer or Agent Host Computer(s) 300 connects via IVR (Interactive Voice Response Unit) 301 and Wired and/or Wireless Telecommunications Network 303 to Telephone Transceiver 305; connects via Server 302 and Telecommunications Network 303 and Internet 304 to Computerized Device(s) 306 and Smart Card 307 in the case of web-based communications; connects via Server 302 and Telecommunications Network 303 to Computerized Device(s) 306 and Smart Card 307 in the case of direct dial-up connections; connects via Bank Network 312 and Wired and/or

Wireless Telecommunications Network 303 to Merchant or Agent Host Computer(s) 311; connects via Bank Network 312 and Wired and/or Wireless Telecommunications Network 303 to IVR 309 and Merchant or Agent Host Computer(s) 311; connects via Bank Network 312 and Wired and/or Wireless Telecommunications Network 303 and Internet 304 to Server 310 and Merchant or Agent Host Computer(s) 311.

Note that the system illustrated in FIG. 3 may be further adapted to take the form of other types of networks such as an interactive cable or satellite television network.

Computerized Device(s) 306 can take various forms (e.g. personal, laptop or notebook computer, personal digital assistant, set-top box, media player and/or recorder, digital telephone, digital photo or video camera, electronic book, etc.) any of which may be enabled with an integrated biosensor or microphone per the additional embodiments outlined above for the creation of a digital signature involving a digital image of a finger or thumbprint or voice scan. Computerized Device(s) 306 runs an operating system capable of supporting multiple applications. Preferably, the operating system is multitasking, allowing simultaneous execution of multiple applications in a graphical user interface (GUI) environment, included among the applications a web browser preferably enabled for use of web services programming languages (e.g. Extensible Markup Language (XML). The operating system includes a key store to securely hold one or more private or secret keys used for encryption, decryption, digital signing, and other cryptographic functions. The key store is a password-protected storage location that grants access upon entry of an appropriate password. The user preferably selects the password as part of the registration process.

Several software components are stored in memory contained within Computerized Device 306 in addition to the browser. They include a registration module and a MAC coding unit as illustrated in FIG. 2. The registration module and MAC coding unit may be supplied to the user during the registration process.

Smart Card 307 preferably incorporates a personal digital signature device in which those processes are housed to meet the various requirements of the invention. U.S. Patent 6,408,388 describes an embodiment of a "Personal date/time device" and is hereby included by reference. Smart Card 307 is able to be carried by a user for the purposes

of accessing and securely downloading digital content "in store" from Point of Sale Terminal 308 and/or Host Computer(s) 311. Alternatively, Smart Card 307 is also able to operate in conjunction with User Computerized Device(s) 306 in carrying out the various functions of the invention.

Telephone Transceiver 305 is useful as a means for a user to connect via Wired and/or Wireless Telecommunications Network 304 to IVR 309 and Merchant or Agent Host Computer(s) 311 and IVR 301 and Card Issuer or Agent Host Computer(s) 300 for the purpose of recording and storing a user voice for the creation of a bio-metric digital scan if needed.

Telephone Transceiver 305 is also useful as a means for a user to connect via Wired and/or Wireless Telecommunications Network 304 to IVR 309 for the purpose placing an order for digital content by telephone. In this instance, the digital content is preferably forwarded to the user out of band in the form of a CD or DVD embedded with a digital signature as provided for by the present invention. Alternatively, the digital content could be forwarded to the user online.

Telephone Transceiver 305 is also useful as a means for a user to connect via Wired and/or Wireless Telecommunications Network 304 to IVR 309 or alternatively to IVR 301 for the purpose of registering as a participant in conjunction with the present invention.

A. Following is described that aspect of the invention involved with web-based, MOTO (mail order – telephone order) and in-store transactions providing for the creation and processing of user digital signatures including the embedding of such signatures as part of the transferred digital content.

In accord with an embodiment of the system illustrated as part of FIG. 3, the present invention is implemented using custom-written applications in the form of software modules operating in conjunction with Card Issuer or Agent Host Computer(s) 300 and Computerized Device(s) 306 and Smart Card 307. The custom-written application is issued to users via download or out of band via disk for use with Computerized Device(s) 306 and Smart Card 307 or alternatively it can be packaged as part of an operating system or other product. If needed an upgrade is capable of being similarly issued to users for the purpose of making the browser operating in conjunction with Computerized Device(s) web-services language enabled.

Operating in conjunction with Merchant or Agent Host Computer(s) 311 and Server 310 are custom-written applications supporting a DRM

system able to interact with Computerized Device 306 using a common web-services language. Preferably, the DRM system also makes use of the "Handle System" for resolving web pages displaying information pertaining to specific digital content identified using DOIs.

U.S. Patent 6,000,832 describes three distinct phases suitable for the present invention; a registration phase, a transaction phase, and a payment-authorization phase. In addition the present invention includes a transfer phase, an application run time signing phase and a super distribution phase.

The registration phase and payment-authorization phase of the present invention follow closely with the methodology and steps outlined in U.S. Patent 6,000, 832. The noticeable exception being the inclusion of a date and/or time stamp as part of the TIN during the pre-authorization process.

According to one embodiment involving a web-based transaction, during the transaction phase the user invokes the browser to surf the Web for a particular product (e.g. movie, song, etc.) or service [e.g. software such as customer relationship management systems (CRM)], or to visit a web site of a particular content provider. Server 310 obtains information about a title of a desired video from Host Computer(s) 311 for display at Computerized Device(s) 306 via the web browser. When a user makes a selection, Host Computer(s) 311 responds with a request for a user digital certificate. Preferably, the user is able to select the digital certificate of the credit or debit card they wish to use. The digital certificate, with the credit or debit card number as one of its attributes, is encrypted with the user's private key. The private key is part of a private/public key pair. The certificate is transferred to the content provider or agent who then redirects the certificate to Bank Network 112 with required merchant information. Preferably, the Bank Network uses the available information to locate the user's public key and decrypt the certificate wherein the card number is submitted for pre-authorization as a matter of securing the various protections offered through the credit card industry.

According to one embodiment, if preauthorization is unsuccessful, then the transaction is terminated and the appropriate messages returned to the content provider or agent and the user. If preauthorization is successful, the card issuer or agent generates a trusted date stamp and

time stamp, updates attribute information as required (e.g. credit limit), signs the certificate with its own private key, and returns the certificate to the content provider who then redirects the certificate back to the user. Preferably, receipt of the signed certificate by Computerized Device(s) 306 results in the retrieval of the bank's public key from storage in order to authenticate the signed date stamp and time stamp.

According to one embodiment, if authentication is unsuccessful, the date stamp and time stamp is considered untrustworthy and is discarded and the possibility of a trusted relationship abandoned by the user. On the other hand, if authentication is successful, the date stamp and time stamp is considered trusted and as a result vouches for the trustworthiness of the content provider. Preferably, this results in the CPU signaling the custom-written application. Alternatively, the user opens the custom-written application by clicking on a special button appearing on the GUI of the browser to invoke a wizard to guide the user through the steps of generating a TIN suitable for the transaction. A dialog box opens up on screen and requests entry of the user's password. The user types in the password. The operating system checks the password prior to allowing access to the key store. If the password is approved, the user is prompted again. The dialog box may also request entry of various transaction-specific data. Preferably, the wizard software automatically collects the transaction-specific data appearing in conjunction with the order form. Additionally, one or more of the above detailed steps could be eliminated by use of a user software agent (e.g. electronic wallet). The step of password entry might also be eliminated or performed at an earlier step prior to the transaction.

Preferably, the custom-written application generates a secret (symmetric) key, calls the MAC coding unit operating in conjunction with Computerized Device(s) 306 and inputs the secret key, the transaction-specific data that preferably includes the trusted date and time, and any user-specific data. The input parameters are entered to the MAC coding unit, which then computes a MAC or code number as a function of the secret key, the transaction-specific data, and the user-specific data. Preferably, the coding unit derives a code number according to a cryptographic hashing function of the symmetric key and various input parameters (e.g. cargo container weight, cargo container density, etc.)

Computerized Device(s) 306 embeds the code number in the available places in the TIN reserved for the code number. Computerized Device(s) 306 computes a checksum from the pre-known prefix, the user identification number, and the code number and appends the check sum and the trusted date stamp and time stamp. The process creates a TIN with an embedded code number or MAC that is specific to the electronic commerce transaction effectively binding the identity of the user to the digital content.

According to a preferred embodiment the TIN is transferred from Computerized Device(s) 306 to a volatile memory associated with Host Computer(s) 311. In addition, the secret key used in forming the TIN is transferred for the purpose of providing the content provider or agent with the means of verifying the user digital signature.

According to one embodiment the process can include the step of retrieving the user private key from key store. The private key is used to encrypt the secret key used in forming the digital signature. The encrypted key along with the input parameters including the DOI(s) and URL(s) and other data relevant to the digital content, the digital signature and the user digital certificate are "pushed" to the content provider or agent. The content provider or agent authenticates the user's public key via the contents of the associated digital certificate and other information available at the time of the transaction. An alternate embodiment provides for no user digital certificate and rather for available information to be used in locating a public key stored in conjunction with a user account. In either of these embodiments, the user public key is used to decrypt the encrypted symmetric key that is then used to verify the digital signature. A third possible embodiment is for the secret key to be pushed to the content provider unencrypted.

According to one embodiment of the present invention, if verification is unsuccessful, the appropriate message is returned to the user and the transaction is terminated. If verification is successful, the TIN, the secret key and any information relevant to the transaction are retained in the volatile memory associated with Host Computer(s) 311 in anticipation of the transfer phase of the present invention.

The CPU operating within Host Computer(s) 311 signals the custom-written application which then begins the process of signing the metadata associated with the digital content prior to its transfer from Host

Computer(s) 311 to Computerized Device(s) 306. The digital signatures formed at this point preferably comprise a user identification portion, a MAC portion, and a date stamp and time stamp portion. Other identifier portions are also possible such as a BIN and a content provider identification number. However, preferably a checksum is not incorporated so as to increase the efficiency and overall speed of the signing process. An alternative embodiment is possible where a checksum may be calculated.

As the metadata is being signed the custom-written application embeds the digital signatures within the digital content. U.S. Patent Application 20020138736 filed January 22, 2001 by Morin describes a tamper-proof means in which the incorporation of the digital signature could be accomplished during the transfer process without negatively impacting the quality of the digital content. An alternative embodiment provides for the signing and embedding process to be completed before the digital content is actually transferred.

An additional embodiment provides for the efficiency and speed with which the CPUs operating within Host Computer(s) 311 are able to perform the signing and embedding process to be enhanced through the incorporation of such methods as that described in Processor Coupling: Integrating Compile Time and Runtime Scheduling for Parallelism, Keckler, S. W., and Dally, W.J., Massachusetts Institute of Technology.

Upon completion of the signing and embedding process, if payment authorization is not required, the TIN and secret key are stored in non-volatile memory in conjunction with the user account. If payment authorization is required, the TIN and the secret key along with any other required information are forwarded to the card issuer or agent as part of an authorization request preferably via Wired and/or Wireless Telecommunications Network 303 and Bank Network 312 or alternatively Internet 304. The custom-written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 uses the secret key to authenticate the TIN as a matter of conducting a payment authorization in conjunction with the user account.

According to one embodiment, if the payment authorization is unsuccessful, the transaction is terminated and the appropriate message along with the TIN and secret key are returned to the content provider or agent and the user notified of the failed transaction. If payment

authorization is successful, the TIN and secret key are returned to the content provider or agent and stored in conjunction with the user account and the user is notified of the successful transaction.

In an alternative embodiment, upon completion of the signing and embedding process, if payment authorization is not required, the TIN and secret key are stored in non-volatile memory in conjunction with the user account controlled by the content provider or agent. If payment authorization is required, a copy of the TIN and secret key along with any other required information are forwarded to the card issuer or agent as part of an authorization request preferably via Wired and/or Wireless Telecommunications Network 303 and Bank Network 312 or alternatively Internet 304. The custom-written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 uses the secret key to authenticate the TIN as a matter of conducting a payment authorization in conjunction with the user account.

According to one embodiment, if the payment authorization is unsuccessful, the transaction is terminated and the appropriate message is returned to the content provider or agent and the user notified of the failed transaction. If payment authorization is successful, copies of the TIN and secret key are stored in conjunction with both the user account controlled by the card issuer or agent and the user account controlled by the content provider or agent and the user notified of the successful transaction.

In another alternative embodiment, the encrypted secret key along with the input parameters including the DOI(s) and URL(s) and other data relevant to the digital content, the digital signature and the user digital certificate are "pushed" to the card issuer or agent. The card issuer or agent authenticates the user's public key via the contents of the associated digital certificate and other information available at the time of the transaction. An alternate embodiment provides for no user digital certificate and rather for available information to be used in locating a public key stored in conjunction with a user account. In either of these embodiments, the user public key is used to decrypt the encrypted symmetric key that is then used to verify the digital signature. A third possible embodiment is for the secret key to be pushed to the card issuer or agent unencrypted.

According to one embodiment, if verification is unsuccessful, the appropriate message is returned to the content provider or agent and the

user and the transaction is terminated. If verification is successful, the TIN, the secret key and any information relevant to the transaction are transferred to the volatile memory associated with Host Computer(s) 311 in anticipation of the transfer phase.

Upon completion of the signing and embedding process, if payment authorization is not required, the TIN and secret key are stored in non-volatile memory in conjunction with the user account controlled by the content provider or agent. If payment authorization is required, the TIN and the secret key along with any other required information are forwarded to the card issuer or agent as part of an authorization request preferably via Wired and/or Wireless Telecommunications Network 303 and Bank Network 312 or alternatively Internet 304. The custom-written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 uses the secret key to authenticate the TIN as a matter of conducting a payment authorization in conjunction with the user account.

According to one embodiment, if the payment authorization is unsuccessful, the transaction is terminated and the appropriate message is returned to the content provider or agent and the user notified of the failed transaction. If payment authorization is successful, the TIN and secret key are stored in conjunction with the user account controlled by the card issuer or agent.

A further enabling of the authorization phase is made possible by an additional embodiment of the invention involving the BIN illustrated in FIG. 1. It is a practice by many card issuers to assign specific BINs to specific types of card products. In doing so, the BINs can also be made to function as a signal for the application of different interchange rates. Here is described an embodiment whereby special BIN(s) can be assigned as part of the transaction phase to signal the application of a special fee (e.g. interchange rate) in response to a transaction initiated for the purpose of using a digital signature process for enhancing the security of a transaction involving the transfer of digital content. Note, that in the case of the user digital signature being applied during a transaction not requiring electronic payment, a specific BIN can be employed to signal that no fee is to be applied to the transaction.

Another alternative embodiment provides that no digital signature be used as for electronic payment. In this case some other means of payment would be incorporated.

There are alternative embodiments of the invention in which use of Smart Card 307 may perform the functions of a personal digital signature device while operating in association with Computerized Device 306 or operating independently and in place of Computerized Device(s) 306. In one embodiment involving the "in store" transfer of digital content, Smart Card 307 connects to Point of Sale Terminal 308 which is enabled with the custom-written application and wherein those processes are housed to meet the various requirements of the invention. The step of entering a PIN and possibly other steps would be carried out in association with a card reader device and keypad operating in conjunction with Point of Sale Terminal 308. An alternative embodiment provides for Point of Sale Terminal 308 to include means for delivering a system clock signal to Smart Card 307 during the course of a transaction for the purpose of carrying out the various functions of the invention.

In one embodiment for in-store transactions, digital content is stored in a non-volatile memory associated with Merchant or Agent Host Computer(s) 311 or transferred to a volatile memory associated with Merchant or Agent Host Computer(s) from a portable memory device (e.g. CD, DVD, etc.). Here, the digital content is ultimately transferred to a portable memory device (e.g. CD, DVD, etc) using a means for transference operating in conjunction with Merchant or Agent Host Computer(s) 311 (e.g. CD Burner, DVD Burner, etc.). Preferably, Smart Card 307 functions as a personal digital signature device operating in conjunction with Merchant or Agent Host Computer(s) 311 and/or possibly Point of Sale Terminal 308 in order to perform the various functions of the invention in which a user digital signature is generated and applied to the digital content in the course of completing the transaction. An alternative embodiment provides for the use of a private or secret key for creating the digital signature that does not involve random key generation but rather makes use of a static private or secret key(s) stored on Smart Card 307 that may be used for repeated transactions. In this case, an embodiment provides for verification of a single digital signature as part of the payment-authorization phase.

FIG. 4 illustrates an embodiment of that aspect of the invention involved with digitally signing various data types such as a DOI 401, other DOI(s) 401, URL(s) 402 and other data (e.g. metadata) and services (e.g. email) and dynamic mechanisms (e.g. java applet) 403, as part of the process of resolving a DOI through use of the "Handle System" either through direct input from the user or through the use of agent software.

Note that the invention is not limited by use of the Handle System as other embodiments for selecting digital content and services are likely to be obvious to those skilled in the art.

FIG. 5 is useful in illustrating an embodiment describing the use of the runtime cycle of an application 500 (e.g. movie, song, video game, etc.) as a measure for signaling the start of a process involving the creation and application of digital signatures. Runtime Cycle 501 reaches a point of completion represented as a single clockwise rotation. Digital Signature 502 is applied to the DOIs and other pertinent metadata including any available statistics regarding application operation.

Alternative embodiments provide for the Digital Signature 502 to also be applied at other points such as the start of an application runtime cycle.

FIG. 5A is useful in illustrating an embodiment of the invention involving the use of a runtime cycle of a microprocessor as a measure for signaling the start of a process involving the creation and application of digital signatures. System Clock 503 is preferably a derived system clock. Runtime Cycle 504 reaches a point of completion represented as a single clockwise rotation. Digital Signature 502 is applied.

Alternative embodiments provide for the Digital Signature 502 to also be applied at other points such as the start of a cycle.

Preferably, System Clock 503 operates at a cycle time less than the main clock system. It is envisioned that alternative embodiments could provide for System Clock 503 to be a Main System Clock.

FIG. 5B is useful in illustrating an embodiment of the invention involving the use of a runtime cycle of a clock 505 as a measure for signaling the start of a process involving the creation and application of digital signatures. Runtime Cycle 506 reaches a point of completion represented as a single clockwise rotation. At the point the cycle is complete (a particular time or elapsed period of time), Digital Signature 500 is applied.

Alternative embodiments provide for the Digital Signature 500 to also be applied at other points such as the start of a cycle.

FIG. 6 illustrates steps involved with one embodiment of a method for using the runtime cycle of an application (e.g. movie, song, video game, etc.) as a measure for signaling the start of a process involving the creation and application of digital signatures. The steps comprise: initialization of the application; runtime activation (e.g. movie playback); data (e.g. metadata) update; runtime deactivation (e.g. stop, pause, game completion, etc.); software module invocation; generation and application of the user digital signature (preferably to the metadata operating in conjunction with the digital content).

FIG. 6A illustrates steps involved with one embodiment of a method for using clock signal activation for signaling the start of a process involving the creation and application of digital signatures. The steps comprise: a derived system clock cycle is completed; a clock signal is used to signal the software module; a clock signal is used to trigger the transfer of data; a digital signature is generated; a digital signature is applied.

FIG. 7 is an illustration useful in describing that aspect of the invention involved with the use of an intermediary location for the transfer of digital content from a user to one or more additional users. This aspect of the invention provides the means by which much of what has been described in conjunction with FIG. 3 above is able to be repeated for secondary transactions (e.g. super distribution) in which a user transfers signed digital content to a secure intermediary location (e.g. Card Issuer or Agent Host Computer(s) 300 or Host Computer(s) 311) in a digital network environment (e.g. Internet or private dial-up network).

One embodiment of the invention provides for a first party user digital signature to be identified and processed during the transfer of digital content from User 1 to a secure intermediary location (e.g. Card Issuer or Agent Host Computer(s) 300). If authentication is not successful, the transfer is terminated and an error message created and issued to User 1. If authentication is successful, the digital content is transferred and stored and the user digital signature is indexed in conjunction with information necessary for facilitating a credit to a User 1 account.

Following successful transfer and storage of digital content to a secure intermediary location, User 1 initiates a process of super distribution

by notifying one or more users illustrated as User 2, User 3, User 4, etc. preferably through electronic means (e.g. email) via Computerized Device(s) 306 and possibly Smart Card 307. Responding to the message possibly by clicking an enclosed URL (and possibly DOI), Users 2, 3, 4 etc. are able to connect with the secure intermediary location whereby they are able to initiate a transaction for the purposes of securely downloading the posted digital content using various means made possible by the present invention. It is possible that in connecting to the intermediary location, Users 2, 3, 4, etc. are first made available to information describing in greater detail the digital content promoted by User 1. This information may originate with User 1 and/or with other parties such as the digital content provider or creator.

Should Users 2, 3, 4, etc., elect to initiate a transaction involving electronic payment, the transaction phase involving such a secondary transaction would involve the initiation of a transaction using the indexed information and resulting in a credit being applied to a User 1 account (e.g. money payment, points, frequent flyer miles, credit to future digital content purchase, etc.).

Note that subsequent to the initial secondary transactions, future transactions may also involve similar steps as those outlined above in which Users 2, 3, 4, etc. are able to fulfill the role of User 1 (i.e. first party) and initiate the process of super distribution with one or more additional users (second parties). In instances where a single copy of downloaded digital content is transferred via the intermediary location two or more times, it may be that during future transactions requiring electronic payment more than one of the previous first parties as evidenced by the presence of multiple user digital signatures are able to initiate transactions in which each of the previous first parties are awarded a credit based upon the established rules and regulations of the super distribution network.

An alternative embodiment provides that transfer of signed digital content via the intermediary location is limited to a single transaction whereby playback of the digital content by Users 2, 3, 4, etc., is restricted to a specific period of time or limited number of playbacks based upon the agreed to licensing rights updated and signed as part of the transfer process.

FIG. 7A illustrates steps involved with one embodiment of a method for verifying the identity of the "user of record" for signed digital content suspected of being used, copied or shared in violation of the license agreement.

The steps comprise: a piece of suspicious digital content is confiscated; the transaction number identifier operating in conjunction with Digital Content Provider or Agent Host Computer(s) 311 identifies an embedded digital signature and transfers the identified digital signature to the account manager operating in conjunction with Host Computer(s) 311; the account manager preferably utilizes the Digital Content Provider/Agent ID and User ID portions to identify a user account; if a record is located, the secret key, the user specific and transaction specific information is retrieved; the account manager submits the key and the information to the MAC coding and comparator unit and computes a MAC which is compared to the MAC extracted from the digital signature. If the two MACs match, the Digital Content Provider and/or Agent has a degree of certainty the suspicious digital content originated with the "user of record."

If no record of a user account is located in the above process, the digital signature is deemed invalid.

B. Following is described that aspect of the invention providing for the creation and processing of user digital signatures to function as a digital "hall pass" for facilitating secure user access to web sites featuring "pay per view" or "pay for use" digital content.

Another aspect of the present invention provides for securing the transfer of digital content or access to services in a time-metered controlled access environment. One example is the transfer of digital content from a web site to a user over the Internet in which pre-authorizations and periodic payment authorizations are preferably utilized. Another example is the access to and use of web services (e.g. CRM) over the Internet. Other examples include the transfer of digital programming over an interactive cable or satellite television network.

In this aspect of the invention, the TIN is preferably able to function as a digital "hall pass" for granting secure access to a web site and also as a means for billing users for such access based on time.

According to one embodiment involving a web-based transaction, during the transaction phase the user invokes a browser to visit a web site or an affiliated network of web sites by using a mouse to click on a hyperlinks associated with the domain name of the web site.

There are also alternative embodiments by which a user is able to access a web site using the invention. One alternative embodiment is for a user to invoke automatic connection to a web site or affiliated network of web sites by engaging a CD-ROM enabled with the custom-written application for facilitating the functions of the invention in association with User Computerized Device(s) 306. Another alternative embodiment is for the user to invoke automatic connection to a web site or affiliated network of web sites by clicking on a response hyperlinks contained in an email. Another alternative embodiment is for the user to initiate a search by inputting the name, URL, or other information associated with the web site or affiliated network of web sites into a search engine.

According to one embodiment, invoking automatic connection to a web site or an affiliated network using the enabled CD-ROM for example preferably begins with the transfer of written instructions to User Computerized Device 306 and a wizard being invoked to guide the user through the steps of using the services provided through the CD-ROM. A dialog box opens up on screen and requests entry of the user's password preferably established during the registration phase. The user types in the password. The operating system checks the password prior to allowing access to the key store. If the password is approved, a process is initiated in which the web browser stored on Computerized Device(s) 306 is invoked. Alternatively, this step is bypassed if the browser is detected to already be in operation. In addition, a browser plug-in residing on the CD-ROM is invoked for operation in association with the web browser. The browser plug-in preferably limits the IP addresses able to be accessed by web browser to those of the preferred web site or affiliated network of web sites similar to a list of "favorites" commonly featured in Internet Explorer and other consumer web browsers.

Continuing with one embodiment, the web browser is preferably connected to the IP address of a selected password-protected site. Upon connection to the site, Host Computer(s) 311 responds with a request for a user digital certificate. Preferably, the user is able to select the digital

certificate of the credit or debit card they wish to use just as with the steps detailed above for the transaction phase involving downloaded digital content. The transaction-specific data used in forming the MAC preferably includes the IP address of the password-protected site. The process creates a TIN that effectively binds the identity of the user to the password-protected site and its associated URL(s).

The transaction phase continues, including the steps detailed above for pushing to the content provider or agent the secret key along with the input parameters including the IP address of the password-protected web site and its associated URL(s). As a result, the transferred TIN functions as a digital "hall pass" by being verified and with successful verification continuing to be used in conjunction with the custom-written application for forming digital signatures throughout the duration of the user's visit to the password-protected site.

According to one embodiment, digital signatures are formed in response to a particular time or elapsed period of time (e.g. one every second beginning with the time marked by successful pre-authorization).

According to another embodiment, the rate charged for access to the web site (e.g. per minute rate) can be constant or fluctuate during a user visit depending on the pricing structure established by the digital content or service provider which can be dependent on such variables as the type of digital content or service accessed, the governmental region having jurisdiction based on the location of either the web site or the computer system(s) in which the digital signature process is performed, the relative financial status of the user in relation to other users (e.g. net worth comparison), the relative "cost of living" factors impacting the user based on their geographical location in comparison to the geographic location of the web site or the computer system(s) in which the digital signature process is performed, etc. The invention is not to be limited by the number of factors that can be considered in establishing a pricing structure for accessing digital content or services.

Additional embodiments will be obvious to those skilled in the art.

C. Following is described that aspect of the invention providing for the creation and processing of user digital signatures to function as a key for facilitating the transfer of push media messages (e.g. target email, instant

messaging, etc.) wherein a dynamic online email catalog is incorporated as an intermediary tool for receiving, distributing, and ranking for display target email messages sent by merchants to users and whereby users are able to access, view and respond to stored and managed email messages.

According to another aspect of the invention, if verification of the TIN is successful during the initiation of a user visit to a web site, a record of the TIN with date stamp and time stamp is stored to a logging server along with other relevant information available at the time of the transaction. The possible information includes personally and non-personally identifiable information.

One embodiment provides the stored TIN to be mapped to the user's email address during a payment authorization transactionthe course of a transaction between the user and the digital content provider or agent or alternatively through a mailing list. Another embodiment provides for the TIN to be mapped to a user pseudo email address preferably created during the course of a transaction between the user and the digital content provider or agent. Another embodiment provides the TIN itself to take the form of an email address identifier. Another embodiment provides for the user email address to be stored in conjunction with a list server for use by merchants or agents or other parties.

In addition, an embodiment provides for these email addresses to comply with the requirements of the email address functions described below as part of an additional aspect of the invention comprising a dynamic online email catalog.

Another embodiment also provides the stored TIN to be mapped to the user's instant messaging client.

FIG. 8 illustrates an embodiment of the invention for a dynamic online email catalog. A key aspect of the invention is the creation of web site 100 to serve as an intermediary tool for accessing, viewing and responding to stored and managed email messages. The technology required for creating and operating the web site is readily available and in use today as a means for providing users web-based email [e.g. Internet Message Access Protocol (IMAP)] as a supplemental service to regular email [e.g. Post Office Protocol (POP)] accessed from their home PC.

Each user of the email catalog preferably has an assigned private user area (i.e. personal catalog) within web site 800 that only they are able

to access. Users are granted access to the private user area by going to the web site and entering their regular e-mail address or another static identifier that they submitted or received in exchange for a submitted identifier when they first signed up for the service. As an added security measure, one embodiment enables users to use a PIN (Personal Identification Number) together with their static identifier. Other available means of secure access include users clicking on a prompt available on their PC home page, e-wallet, digital phone screen, etc.

Preferably, within each private user area is found a plurality of mailboxes 801, 802, 803, 804. The mailboxes are arranged so as to populate the screen much like different product categories and listings in conventional online catalogs. FIG. 8 shows one embodiment including four mailboxes of equal size and proportion. Another embodiment provides for increasing numbers of mailboxes to be added to the display. Another embodiment provides for multiple web pages to accommodate added mailboxes. Another embodiment calls for the mailboxes to be arranged in various ways and among other graphics and hyperlinks so as to increase the style and flexibility of the information choices provided through the display. Each mailbox is preferably labeled with specific product and service categories (e.g. men's casual wear, insurance services, etc.) or alternatively the names of specific product/service providers (e.g. merchants) depending on the intended use of the mailbox.

The infrastructure supporting web site 800 is preferably located within Card Issuer or Agent Host Computer(s) 300 and Server 302. Preferably, a MAPI-enabled server (Message Application Program Interface) comprises the custom-written application necessary for fulfilling the functions of the invention. In addition, there is preferably a mail list server and database wherein is stored user email addresses which have been mapped to various profile designations identified through personally and non-personally identifiable information. The list server is preferably a password-protected server.

FIG. 9 illustrates an embodiment of a pseudo "from" email address with date and/or time stamp. The address shown includes an identifier portion comprising a user TIN and a date stamp and time stamp portion. The "from" email address is used by merchants in sending push media messages to users following electronic commerce transactions.

FIG. 10 illustrates steps included in one embodiment of a method used in conjunction with the system illustrated in FIG. 3 to generate, issue and store pseudo email addresses in combination with user personally identifiable information (e.g. name, primary email address, credit card primary account number, etc.) and/or non-personally identifiable information (e.g. demographic profile, financial net worth, etc.).

A user requests a pseudo email address preferably from the card issuer or agent. In receiving the request for a pseudo email address, a process of authentication is initiated by a custom-written application operating in conjunction with the Card Issuer or Agent Host Computers 300. Upon successful authentication of the user, the custom-written application generates the pseudo email address, stores the address with the user personally identifiable and non-personally identifiable information in a way that maps it to the user's primary email address, and transfers the pseudo address preferably to the user web browser operating in conjunction with User Computerized Device 306.

Once issued, the pseudo email address functions like a regular email address. Preferably, the user retains the ability to discontinue or suspend the active status of the pseudo email address similar to the methods currently employed for limited use credit or debit card numbers. Preferably, the user is able to perform the steps necessary for discontinuing or suspending the active status of an email address by accessing their private user area of the dynamic online email catalog.

The process involved with a merchant sending a TIN-enabled email address to a user preferably follows closely with the steps previously detailed for a payment authorization request using the present invention. The merchant forwards an email with the "from" address containing the TIN and the IP address of the merchant, the secret key used in forming the TIN and any other required information. In receiving the email message, the custom-written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 uses the secret key to authenticate the TIN as a though conducting a payment authorization.

According to one embodiment, if verification of the TIN is unsuccessful, the email is flagged as "not trusted" and forwarded to the user preferably to an area of the dynamic online email catalog designated for "not trusted" messages. If verification is successful, the email is preferably

flagged as trusted and forwarded to the user preferably to an area of the dynamic online email catalog designated for "not trusted" messages. The TIN and secret key are returned to the content provider or agent and placed back into storage in conjunction with the user account.

Preferably, a similar process for authentication is employed when receiving instant messages from merchants.

According to one embodiment, organization of email messages in the dynamic online email catalog can involve ranking received email messages according to bids placed by merchants or their agents. Another embodiment provides that organization of email messages in the dynamic online email catalog can preferably have newly arriving email messages to specific mailboxes take priority position within specific retail categories over previously sent emails from the same originating address. This preferably involves having incoming emails trigger the sub-listing or deletion of previously received email messages so as to avoid a situation in which a deluge of emails from a specific second party would bury competing emails messages from other second parties.

An additional embodiment involves the use of the date and/or time stamp of the TIN used in conjunction with incoming marketing messages to help in enabling a process in which incoming email messages (possibly within certain product and service categories) are displayed in rank order based on the average length of "customer relationship" maintained by individual merchants across all of their participating users or as an alternative embodiment those participating users of a certain profile classification. This is preferably accomplished by a process in which a comparison is conducted of all active and deactivated or suspended date and/or time stamped "from" email addresses established with individual merchants and other second parties. The process operates in conjunction with Card Issuer or Agent Host Computer(s) 300. The ranking of received email messages would be prioritized according to a trust score reflecting different functions of time (e.g. average) with respect to the total relative lengths of time (i.e. life spans) that individual "from" email addresses or different aggregate groups of "from" email addresses have been established with a specific user or a group of users (e.g. an affinity or demographic group) wherein those scores reflecting longer life spans are given higher priority placement and as a result higher visibility within mailboxes 801,

802, 803, 804 displayed on web page 800. Supporting this is preferably a process similar to the means in which conventional HTML email is managed wherein it is common that some or all of the content (e.g. graphics and/or heading) of the first received of unread emails is made visible to the user.

An simplified example of a trust score calculation is able to be illustrated by considering two different merchants each of them with three customers having active pseudo email address accounts and three customer names associated with deactivated pseudo email addresses. In order to determine a trust score, one embodiment involving a custom written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 looks at the date and/or time stamps of the three active addresses for each merchant, looks at the current date and time, calculates a snapshot of the combined total length of time for the three active addresses for each merchant, looks at the date and/or time stamps of the three deactivated addresses for each merchant, looks at the date and time the addresses were deactivated, calculates the combined total length of time for the three deactivated addresses for each merchant, adds together the combined total lengths of time for both the three active and three deactivated addresses for each merchant, divides by six the total resulting from the addition of the combined lengths of time for both the three active and three deactivated addresses for each merchant. The same embodiment then compares the two time averages and determines the highest time average (i.e. trust score).

When a user accesses a private user area, the act of doing so preferably invokes a process whereby the trust scores of the second parties are calculated in real time and compared. This information is taken into account with the result being that the email messages originating from second parties with higher trust scores are given priority placement in each of the mailboxes displayed by the dynamic online email catalog. An alternative embodiment less demanding on the operational demands of the system provides for the trust score to be calculated once every 24 hours for all product and service providers.

Use of the trust score ranking system would be preferable in the situation where second parties are limited to one email per each product/service category mailbox in a user private area.

The exception would be the scenario in which specific mailboxes appearing in a private user area are assigned exclusively to specific product/service providers. Here, second parties or their agents are preferably able to select the amount of email storage capacity they wish to maintain in conjunction with various user accounts with the total charges for storage being determined based upon the amount of storage leased. Second parties or their agents are also preferably able to tailor storage capacity to fit particular user profiles (e.g. customers who access the dynamic online email catalog at a certain frequency, customers known to have made past purchases, or customers exceeding a certain spending amount, etc.).

FIG. 11 is a block diagram illustrating the functional elements of a search apparatus incorporating that aspect of the invention involved with searching a database of records (e.g. Internet records, email records across different aggregate user groups) in response to user requests for the purpose of locating and retrieving information in which the search results are able to be displayed in rank order based on different functions of time (e.g. average) with respect to the length of time (i.e. life span) that individual user email addresses or different aggregate groups of user email addresses have been established with a particular second party (e.g. merchant) or a group of second parties (e.g. merchant affiliate network) identified with the individual ranked search results. A system and method for providing a search apparatus and method capable of meeting the requirements of the current invention with certain modifications is described in U.S. Patent Document 5,924,090 "Method and apparatus for searching a database of records" and is hereby incorporated herein in its entirety by reference.

The search apparatus operates in conjunction with Search Engine Host Computer(s) 1100 which a user is able to access from User Computerized Device 306 via Wired and/or Wireless Telecommunications Network 303 and Internet 304. According to a preferred embodiment, the apparatus 1100 includes a search processor 1101 and a grouping processor 1102. The grouping processor comprises a record processor 1103, a candidate generator 1104, a weighing processor 1105, and a display processor 1106. These elements are software modules and have been so identified merely to illustrate the functionality of the invention. The apparatus 1100 communicates with a User Computerized Device 304 (Note

that alternatively a conventional telephone can be substituted in conjunction with a sophisticated voice activation system) and a database(s) 1108, which preferably includes Internet and push driven content records (e.g. target email messages), via an I/O bus 1109. The apparatus 1100 is capable of communicating with a plurality of remotely located users over a wide area network (e.g. the Internet).

In addition, there is an embodiment providing for the incorporation of an electronic language translator as an added innovation to the present invention. An Electronic Language Translator preferably operates within Card Issuer or Agent Host Computer(s) 300. A system and method for providing an electronic language translator capable of meeting the requirements of the current invention is described in U.S. Patent Document 20010029455 "Method and apparatus for providing multilingual translation over a network" and is hereby incorporated herein in its entirety by reference.

In U.S. Patent Document 20010029455 there is described a means in which a source language text (e.g. English) is received as an input to the electronic language translator, the source language test is translated at the electronic language translator at the time of submission into one or more target language texts (e.g. Japanese), and a user is then provided with an option of viewing one or more of the target language texts with or without the source language text. U.S. Patent Document 20010029455 further describes a data provider as being any device that supplies either static or dynamic data to a client device over the data transmission infrastructure wherein the invention of an electronic language translator is capable of acting as an intermediary in data exchange, translating the data from one language to another as it passes from client device to data provider, from data provider to client device, or from client device to client device.

ALTERNATIVE EMBODIMENTS

The present invention makes possible several significant alternative embodiments.

Secure Shipping & Tracking

The present invention provides a system and method ideally suited for increasing both the security and efficiency of wireless package tracking and freight shipping systems. This is particularly true for international

shipments where security risks are often considered to be higher than with purely domestic shipments and postal rates often change as shipments cross over government lines.

According to one embodiment, the invention makes use of a TIN as illustrated in FIG. 1. The MAC is formed using various inputs including a private or secret key, user-specific information and transaction specific information such as a cargo container identification number, cargo container weight, cargo container density, global positioning coordinates (GPS), interim shipping rates, etc.

In the case of shipments across seas, a company representative chooses to place the shipping order over the Internet using Computerized Device 306. According to one embodiment, the user invokes the browser to connect over the Web to a password-protected site operated by the freight carrier or agent. When the company rep types in the password and hits enter, Host Computer(s) 311 responds with a request for a user digital certificate. Preferably, the shipper is able to select the digital certificate of the company credit card he wishes to use for the transaction. The digital certificate, with the credit or debit card number as one of its attributes, is encrypted with the shipper's private key. The private key is part of a private/public key pair. The certificate is transferred to the freight carrier or carrier agent who then redirects the certificate to Bank Network 112 or alternatively Internet 304 with required merchant information. Preferably, Bank Network 112 uses available information to locate the shipper's public key and decrypt the certificate wherein the card number is submitted for pre-authorization as a matter of securing the various protections offered through the credit card industry.

According to one embodiment, if preauthorization is unsuccessful, then the transaction is terminated and the appropriate messages returned to the freight carrier or agent and the shipper. If preauthorization is successful, the card issuer or agent generates a trusted date stamp and time stamp, updates attribute information as required (e.g. credit limit), signs the certificate with its own private key, and returns the certificate to the freight carrier or agent who then redirects the certificate back to the shipper. Preferably, receipt of the signed certificate by Computerized Device(s) 306 results in the retrieval of the bank's public key from storage in order to authenticate the signed date stamp and time stamp.

According to one embodiment, if authentication is unsuccessful, the date stamp and time stamp is considered untrustworthy and is discarded and the possibility of a trusted relationship abandoned by the shipper. On the other hand, if authentication is successful, the date stamp and time stamp is considered trusted and as a result vouches for the trustworthiness of the freight carrier or agent. Preferably, this results in the CPU signaling the custom-written application. Alternatively, the shipper opens the custom-written application by clicking on a special button appearing on the GUI of the browser to invoke a wizard to guide the shipper through the steps of generating a TIN suitable for the transaction. A dialog box opens up on screen and requests entry of the shipper's password. The shipper types in the password. The operating system checks the password prior to allowing access to the key store. If the password is approved, the shipper is prompted again. The dialog box may also request entry of various transaction-specific data. Preferably, the wizard software automatically collects the transaction-specific data appearing in conjunction with the order form. Additionally, one or more of the above detailed steps could be eliminated by use of a user software agent (e.g. electronic wallet). The step of password entry might also be eliminated or performed at an earlier step prior to the transaction.

Preferably, the custom-written application generates a secret (symmetric) key, calls the MAC coding unit operating in conjunction with Computerized Device(s) 306 and inputs the secret key, the transaction-specific data that preferably includes the trusted date and time, and any user-specific data. The input parameters are entered to the MAC coding unit, which then computes a MAC or code number as a function of the secret key, the transaction-specific data, and the user-specific data. Preferably, the coding unit derives a code number according to a cryptographic hashing function of the symmetric key and input parameters.

Computerized Device(s) 306 embeds the code number in the available places in the TIN reserved for the code number. Computerized Device(s) 306 computes a checksum from the pre-known prefix, the shipper identification number, and the code number and appends the check sum and the trusted date stamp and time stamp. The process creates a TIN with an embedded code number or MAC that is specific to the electronic commerce transaction

effectively binding the identity of the shipper to the shipping order being shipped.

According to a preferred embodiment, the TIN is transferred from Computerized Device(s) 306 to a volatile memory associated with Host Computer(s) 311. In addition, the secret key used in forming the TIN is transferred for the purpose of providing the freight carrier or agent with the means of verifying the user digital signature.

According to one embodiment the process can include the step of retrieving the shipper private key from key store. The private key is used to encrypt the secret key used in forming the digital signature. The encrypted key along with the input parameters and other data relevant to the shipping order, the digital signature and the shipper digital certificate are "pushed" to the freight carrier or agent. The freight carrier or agent authenticates the shipper's public key via the contents of the associated digital certificate and other information available at the time of the transaction. An alternate embodiment provides for no shipper digital certificate and rather for available information to be used in locating a public key stored in conjunction with a shipper account. In either of these embodiments, the shipper public key is used to decrypt the encrypted symmetric key that is then used to verify the digital signature. A third possible embodiment is for the secret key to be pushed to the content provider unencrypted.

If payment authorization is required, the TIN and the secret key along with any other required information are forwarded to the card issuer or agent as part of an authorization request preferably via Wired and/or Wireless Telecommunications Network 303 and Bank Network 312. The custom-written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 uses the secret key to authenticate the TIN as a matter of conducting a payment authorization in conjunction with the user account.

According to one embodiment, if the payment authorization is unsuccessful, the transaction is terminated and the appropriate message along with the TIN and secret key are returned to the freight carrier or agent and the shipper notified of the failed transaction. If payment authorization is successful, the TIN and secret key are retained by the card issuer or agent and stored in conjunction with the user account and the user is notified of the successful transaction.

In an alternative embodiment, if payment authorization is not required, the TIN and secret key are stored in non-volatile memory in conjunction with the user account controlled by the content provider or agent. If payment authorization is required, a copy of the TIN and secret key along with any other required information are forwarded to the card issuer or agent as part of an authorization request preferably via Wired and/or Wireless Telecommunications Network 303 and Bank Network 312 or alternatively Internet 304. The custom-written application operating in conjunction with Card Issuer or Agent Host Computer(s) 300 uses the secret key to authenticate the TIN as a matter of conducting a payment authorization in conjunction with the user account.

According to one embodiment, if the payment authorization is unsuccessful, the transaction is terminated and the appropriate message is returned to the freight carrier or agent and the user notified of the failed transaction. If payment authorization is successful, copies of the TIN and secret key are stored in conjunction with both the user account controlled by the card issuer or agent and the user account controlled by the freight carrier or agent and the user notified of the successful transaction.

According to one embodiment of the present invention, if verification is unsuccessful, the appropriate message is returned to the user and the transaction is terminated. If verification is successful, the TIN, the secret key and any information relevant to the transaction are retained in the volatile memory associated with Host Computer(s) 311 in anticipation of the transfer phase of the present invention.

According to one embodiment, the CPU operating within Host Computer(s) 311 signals the custom-written application which transfers the TIN, the secret key and any information relevant to the transaction to a non-volatile memory for temporary storage.

FIG. 12 is an illustration useful in describing the wireless transmission of data to computerized tracking devices fastened to the cargo containers being shipped. Preferably, the containers move along a conveyer until they enter a security checkpoint which is serviced by a light beam apparatus (e.g. infrared scanner, microwave, etc.) capable of reading data to the tracking devices.

According to one embodiment, once a container arrives at a checkpoint, the individual container comes to a brief stop just long enough

for various proper measures to be taken. Preferably, the first stop after a container is loaded has the TIN, the secret key and any information relevant to the transaction, transferred from temporary storage and beamed to the computerized tracking device where it is incorporated for use by the custom-written application for creating and processing digital signatures. After the various measures have been completed, the container is sent on its way.

Future stops at security checkpoint can involve measures including, weighing, x-raying, GPS coordinates and rate information, etc. According to one embodiment, once the container has been delivered to its intended destination, the container and the computerized tracking device would be subjected to a special light beam capable of reading data and calculating the total distances traveled together with the applicable rates, and preferably charging the shipper's credit card for payment.

From a security standpoint, the signed data also provides a trusted record of information regarding the cargo's travels.

FIG. 13 is an illustration showing a similar security checkpoint process being applied to a cargo ship. To either side of the ship is situated a powerful light beam capable of either blanketing targeted portions of the ship or alternatively directing their beam to a network receptor capable of directing the data to its intended destinations.

Putting the invention to use this way, preferably by stationing the security checkpoint along inlet waterways, would prove invaluable in saving both time and money due to the vast complications presented by the increased security for shipments.

Authenticating Outputs of Computer Software

The invention is ideally suited for widespread application as a means of not only assuring confidence in data records but also a means of exercising electronic payment based on those records.

One embodiment includes home and business electric meters. Those in the industry are well aware of the problems concerning discrepancies in billing. Today, digital signature technology is being put to use with newer computerized systems as a way of increasing accuracy.

The invention is perfectly suited to operate in this environment similar to the shipping embodiment outlined above. The digital signature process would create an ongoing record of power usage by date and time stamping the usage records. In addition, the incorporation of a credit card

for example as part of the TIN would provide a means of exercising periodic payment. This would prove exceptionally time and cost saving for large business properties with numerous meters where the property owner or management company may be extremely sensitive to under-billing due to the fact that many of them make a practice of buying electricity wholesale and reselling it to clients.

Smart Cards

Another embodiment where the invention has widespread application possibilities is with smart cards. An example would be a parking meter outfitted to take a smart card as part of a transaction. The invention provides the means by which a smart card enabled with the digital signature process could initiate a transaction and by reinsertion some time later culminate a transaction with the elapsed time calculated and the appropriate rate applied.

In another additional alternative embodiment of the invention, the TIN can be distributed for application in a web services environment from which the number may be extracted, interpreted and processed as part of an enhanced digital signature process comprising detached, enveloped, or enveloping signatures.

Although the invention has been described in detail, it is to be understood that variations therein and modifications thereto may be made by those skilled in the art without departing from the spirit and scope of the invention. For example, the functions of the host computer can be provided by various microprocessors, servers, and memory storage devices working together in a system. The invention is not limited by the terminology used to describe the invention or various embodiments herein.

CLAIMS

What I Claim Is:

1. A Dynamic Online Email Catalog comprising means to collect, categorize, arrange, store and display direct email marketing messages to a designated recipient.

2. The Dynamic Online Email Catalog of claim 1, further comprising
means for processing the email to place in categories.

3. The Dynamic Online Email Catalog of claim 1, further comprising
means for arranging and storing the a plurality of email messages in categories according to subject matter

4. The Dynamic Online Email Catalog of claim 1, further comprising
means for assigning a trust value to the message and means for ranking the messages in accord with the trust value.

5. The Dynamic Online Email Catalog of claim 1, further comprising
means for providing an electronic language translator wherein a source language text (e.g. English) is received as an input to the electronic language translator, the source language test is translated at the electronic language translator at the time of submission into one or more target language texts (e.g. Japanese).

6. A method for handling and enhancing utilization of email marketing messages to a designated recipient, the method comprising collecting, categorizing, arranging and storing the email marketing messages in a central data base, and displaying the messages in an arranged format for use by the designated recipient.

7. An email address format comprising a plurality of portions including an identifier portion associated with a designated user, a date/time stamp portion and web site identifier portion.

8. The email address format of claim 7, further comprising a vendor identifier portion.

9. The email address format of claim 7, further comprising a category identifier portion.

10. A system for a mailing list manager comprising;

means for processing email messages received from second party affiliates by extracting a portion of the originating "from" address to create a new "from" address combining with a portion of the domain address of a sponsoring second party,

means for forwarding the email pursuant to a request for messages relating to a particular desired subject matter.

11. A system for a search apparatus comprising;

means for ranking the records within a search results list with priority

given to those records associated with an entity having a registered trust score with the Dynamic Online Email Catalog of claim 1.

means for ranking the records associated with an entity having a registered trust score with the Dynamic Online Email Catalog of claim 1 wherein priority is given to a record based upon the higher calculated trust score comprising the steps of looking at the date and/or time of creation, issuance or use of active communication links established between members of a specific user group and a single shared entity; looking at the current date and time; calculating a snapshot of the combined total length of time for all of the active addresses; looking at the date and/or time of creation, issuance or use of deactivated communication links previously established between members of the same specific user group and the same single shared entity; looking at the date and time the addresses were deactivated; calculating the combined total length of time for all of the deactivated addresses; adding together the combined total lengths of time for all of the active and deactivated addresses; dividing by the total number of active and deactivated addresses the total resulting from the addition of the combined lengths of time for both the active and deactivated addresses.

16-Digit TIN w/ MAC & Date/Time Stamp

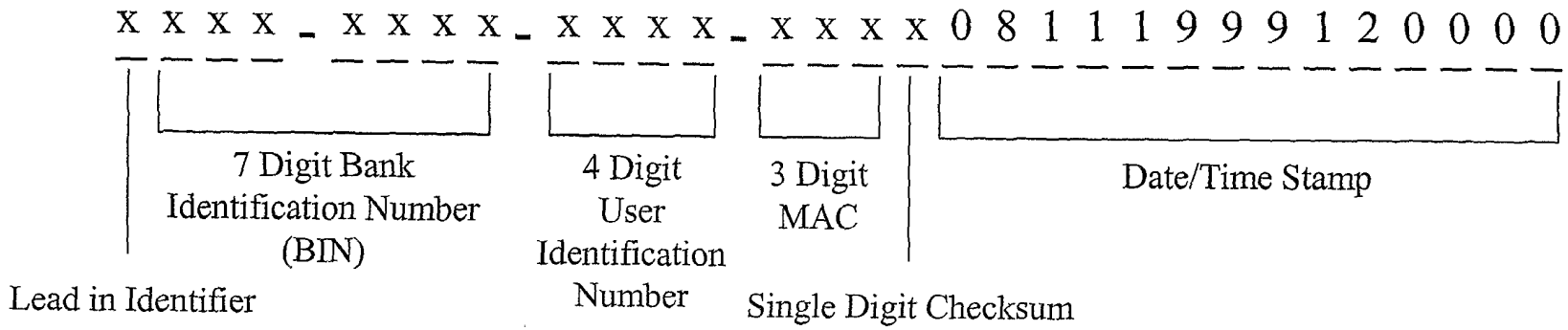


FIG. 1

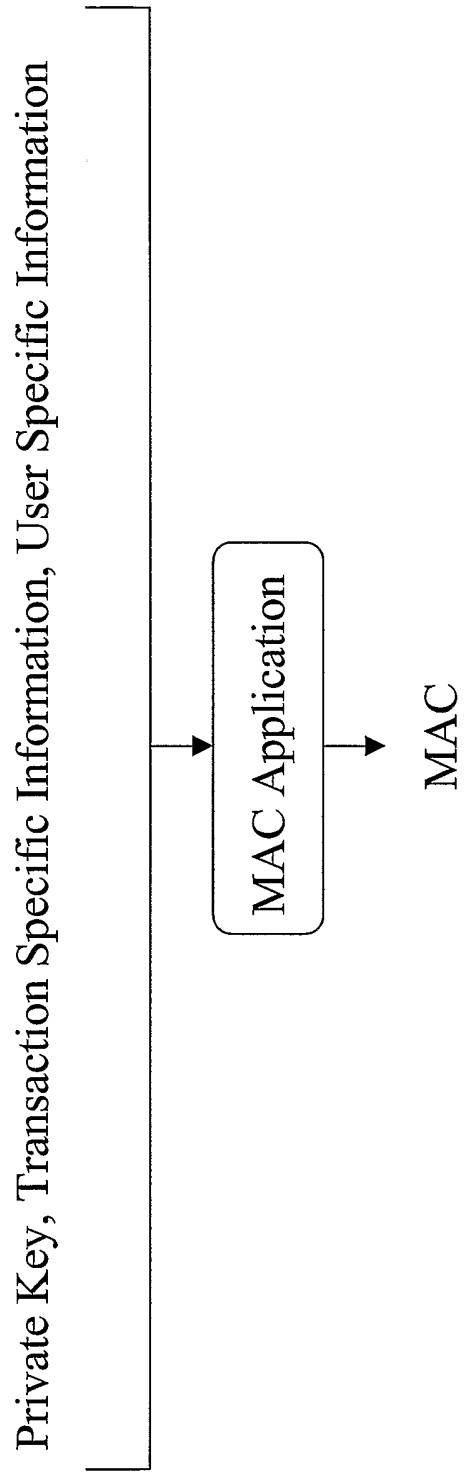
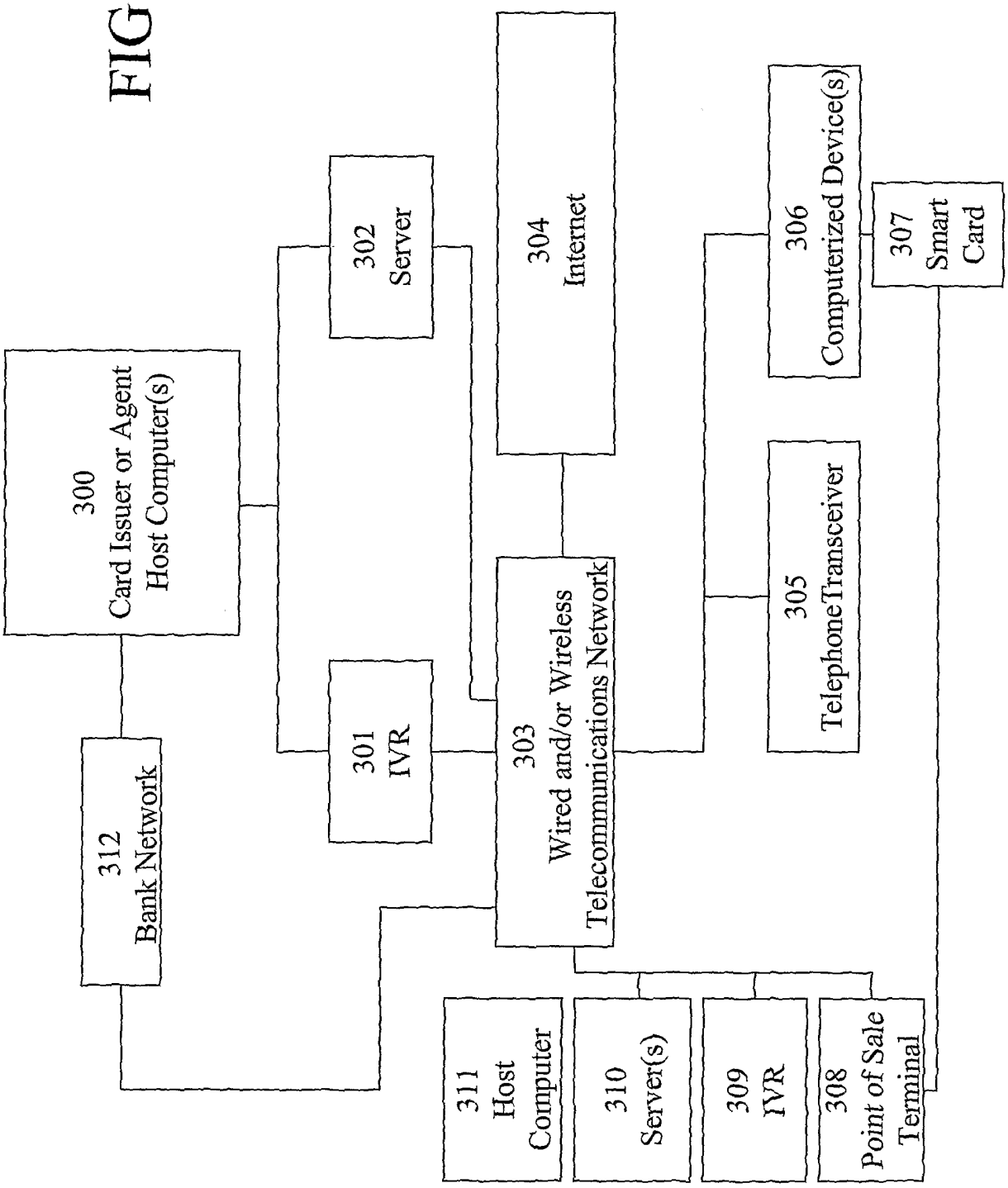

Private Key, Transaction Specific Information, User Specific Information
MAC Application
MAC

FIG. 2

FIG. 3


300
Card Issuer or Agent
Host Computer(s)
302
Server
304
Internet
306
Computerized Device(s)
307
Smart
Card
312
Bank Network
301
IVR
303
Wired and/or Wireless
Telecommunications Network
305
Telephone Transceiver
311
Host
Computer
310
Server(s)
309
IVR
308
Point of Sale
Terminal

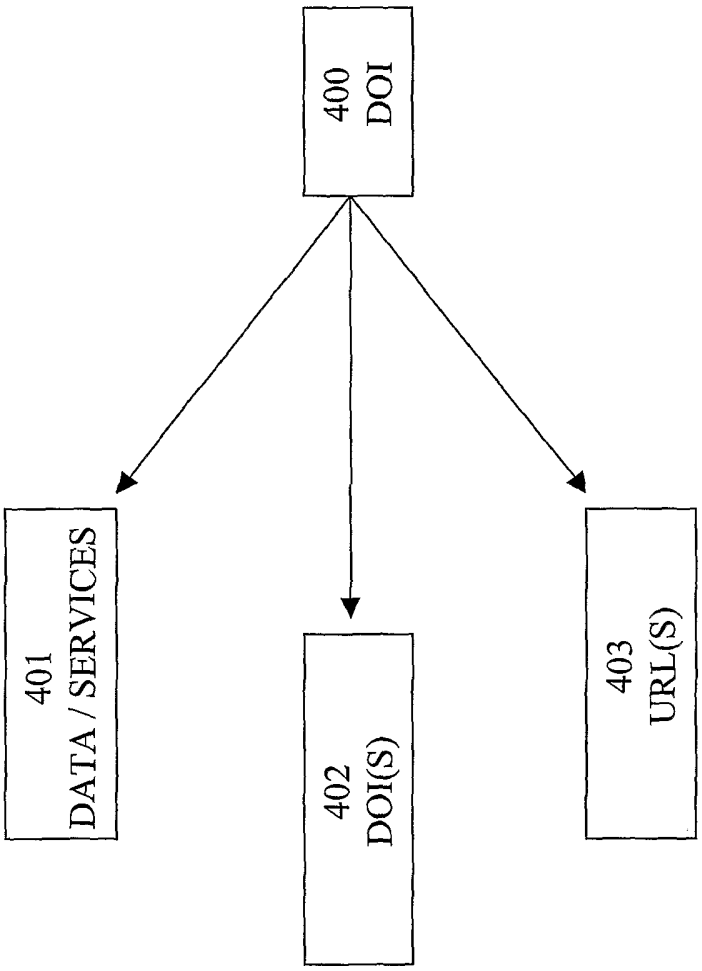


FIG. 4

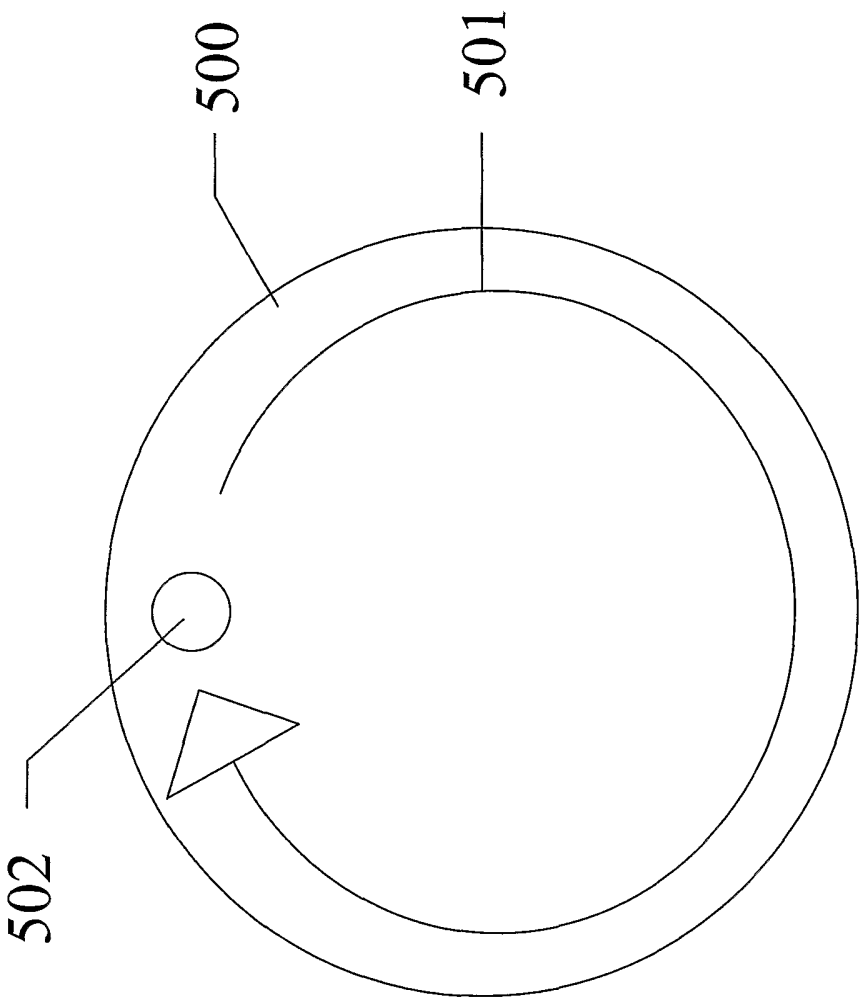


FIG. 5

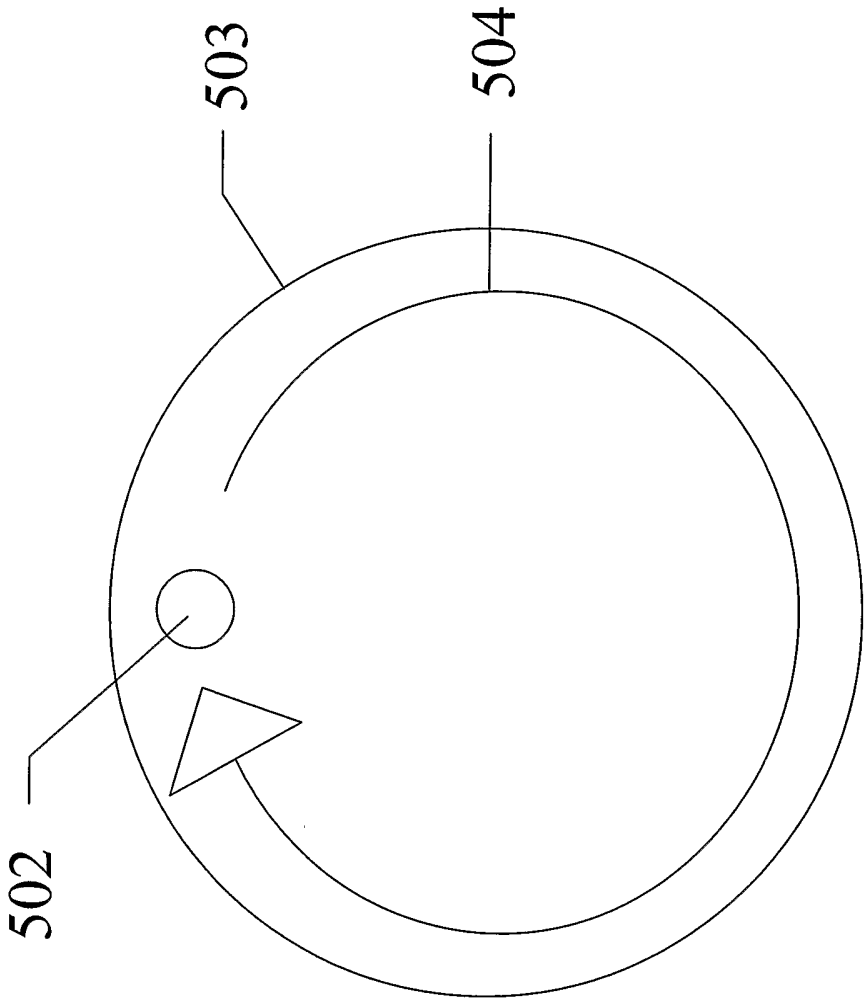


FIG. 5A

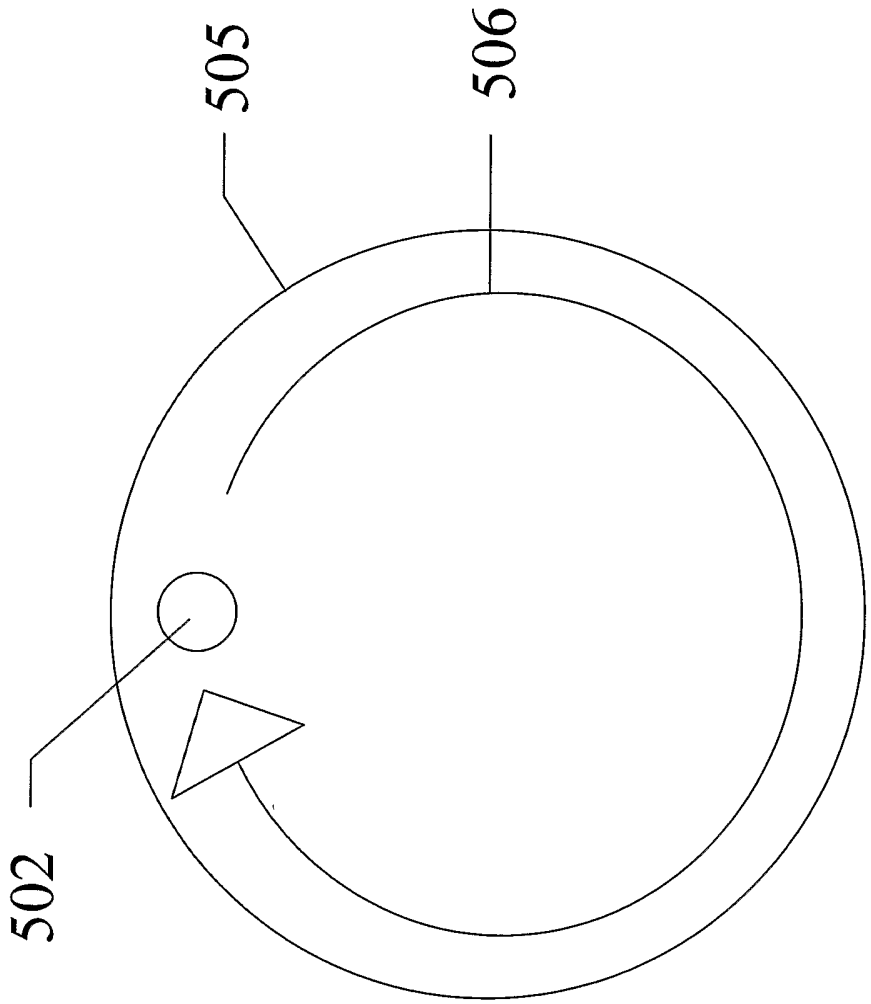


FIG. 5B

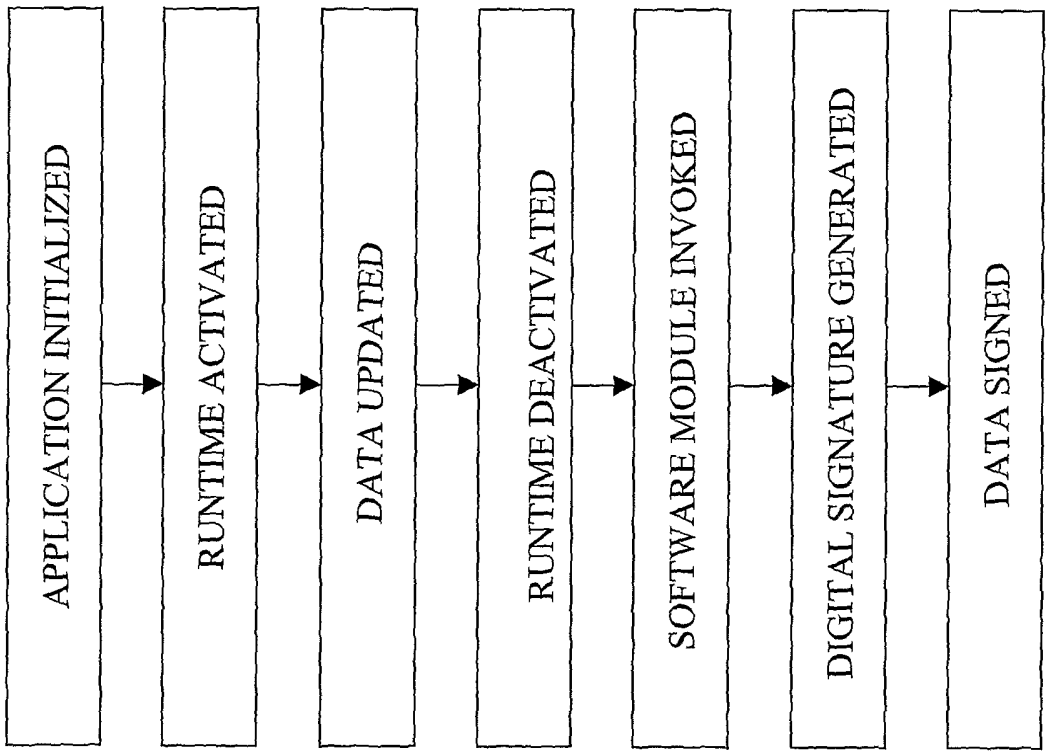

APPLICATION INITIALIZED
RUNTIME ACTIVATED
DATA UPDATED
RUNTIME DEACTIVATED
SOFTWARE MODULE INVOKED
DIGITAL SIGNATURE GENERATED
DATA SIGNED

FIG. 6

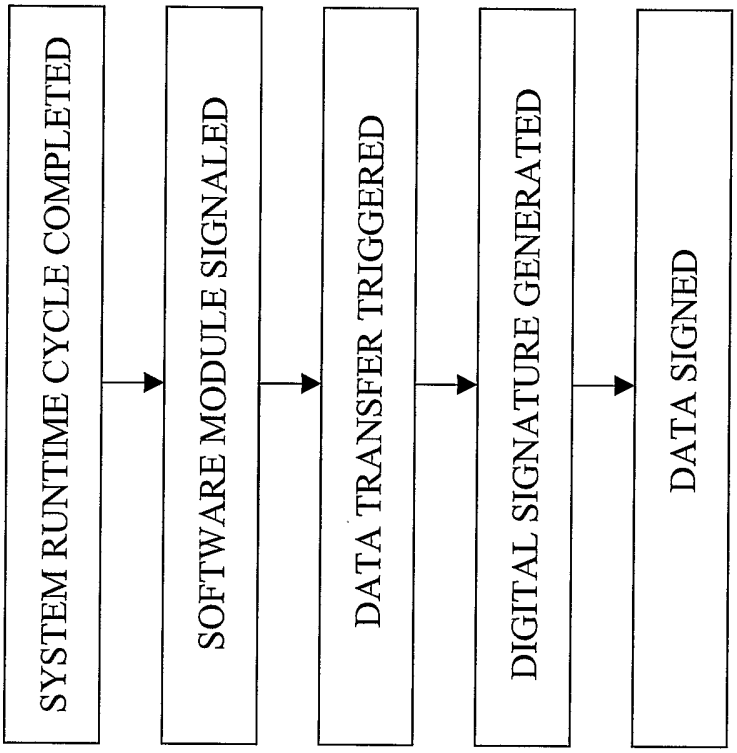

SYSTEM RUNTIME CYCLE COMPLETED
SOFTWARE MODULE SIGNALED
DATA TRANSFER TRIGGERED
DIGITAL SIGNATURE GENERATED
DATA SIGNED

FIG. 6A

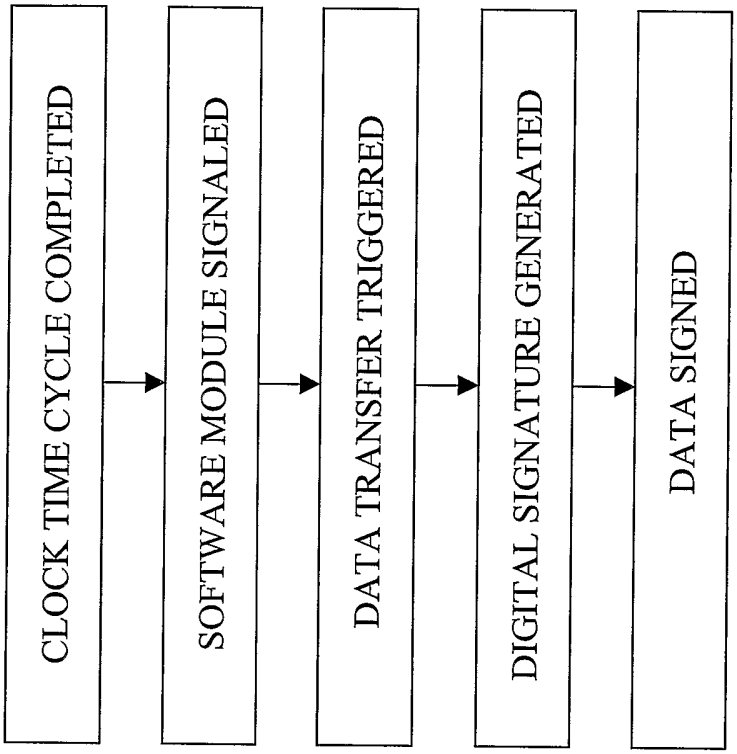

CLOCK TIME CYCLE COMPLETED
SOFTWARE MODULE SIGNALED
DATA TRANSFER TRIGGERED
DIGITAL SIGNATURE GENERATED
DATA SIGNED

FIG. 6B

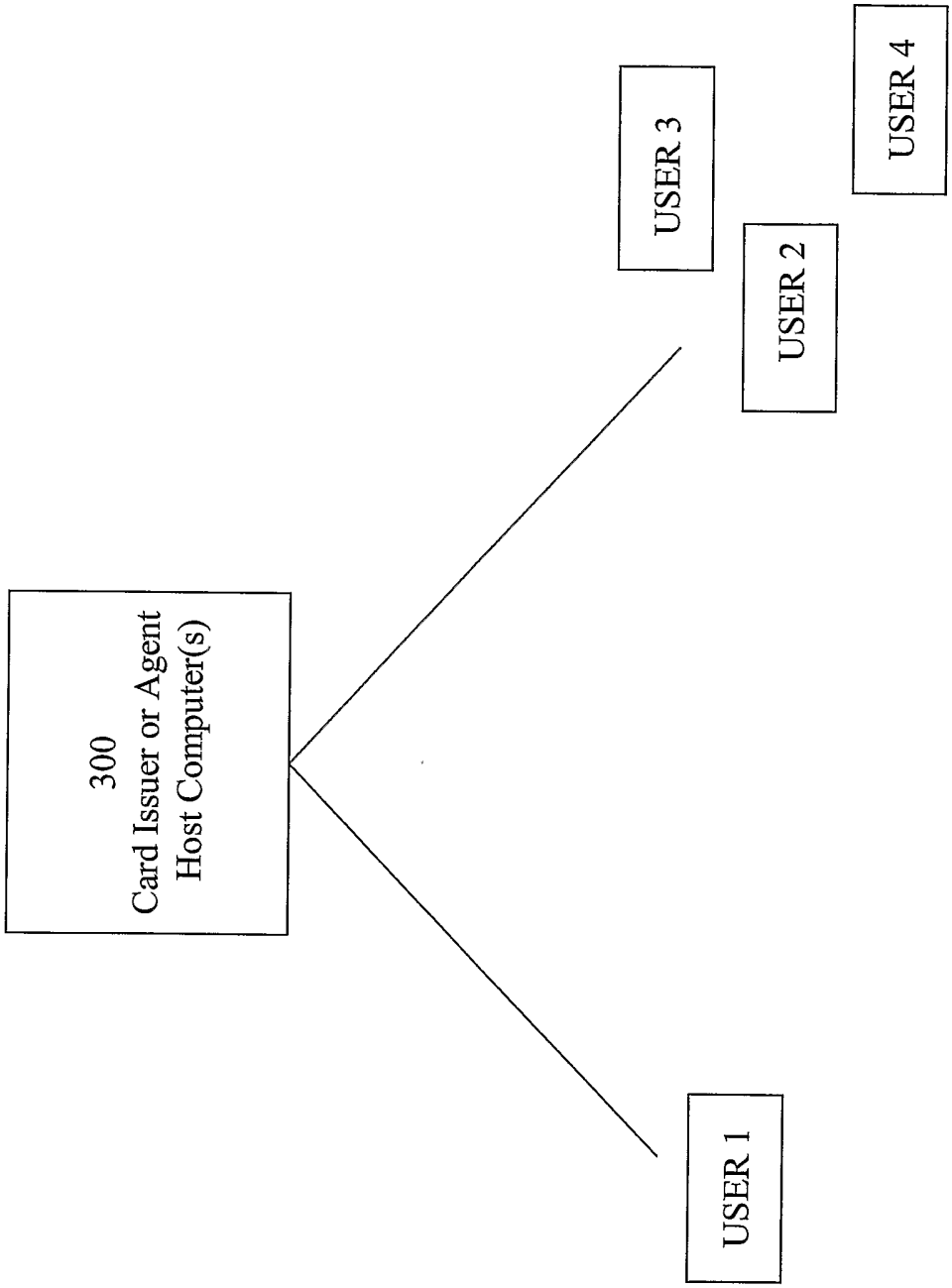

300
Card Issuer or Agent
Host Computer(s)
USER 1
USER 2
USER 3
USER 4

FIG. 7

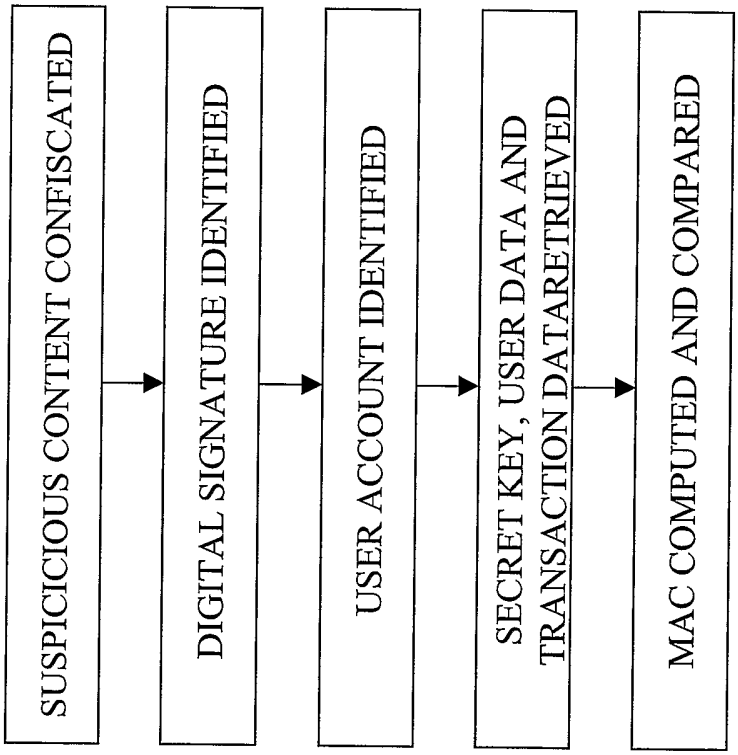

SUSPICIOUS CONTENT CONFISCATED
DIGITAL SIGNATURE IDENTIFIED
USER ACCOUNT IDENTIFIED
SECRET KEY, USER DATA AND TRANSACTION DATARETRIEVED
MAC COMPUTED AND COMPARED

FIG. 7A

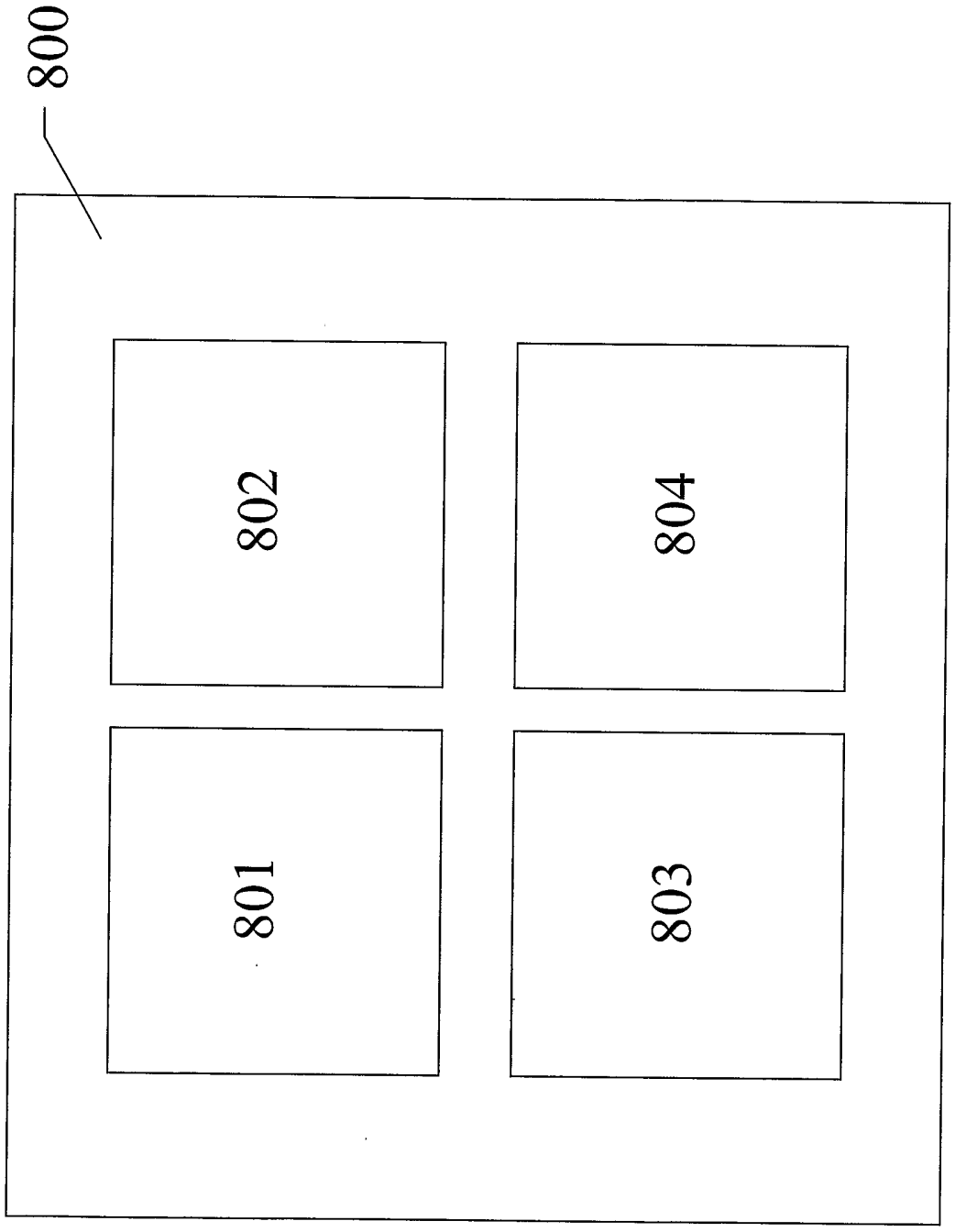


FIG. 8

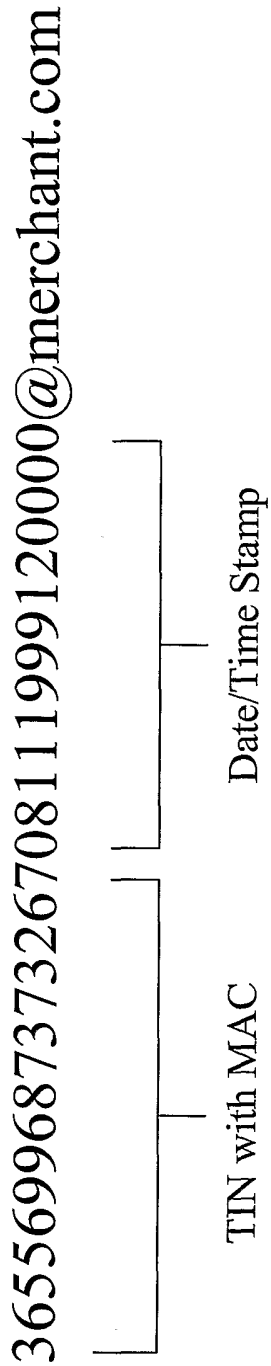

365569968737326708111999120000@merchant.com
TIN with MAC
Date/Time Stamp

FIG. 9

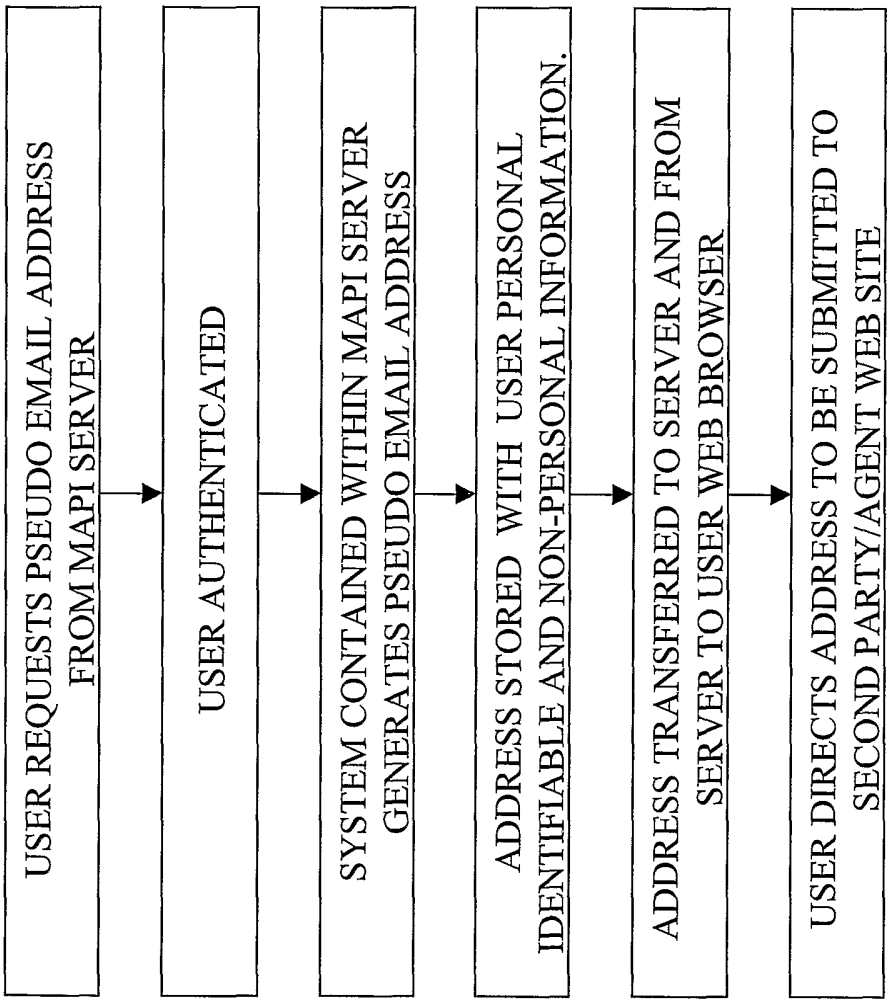

USER REQUESTS PSEUDO EMAIL ADDRESS FROM MAPI SERVER
USER AUTHENTICATED
SYSTEM CONTAINED WITHIN MAPI SERVER GENERATES PSEUDO EMAIL ADDRESS
ADDRESS STORED WITH USER PERSONAL IDENTIFIABLE AND NON-PERSONAL INFORMATION.
ADDRESS TRANSFERRED TO SERVER AND FROM SERVER TO USER WEB BROWSER
USER DIRECTS ADDRESS TO BE SUBMITTED TO SECOND PARTY/AGENT WEB SITE

FIG. 10

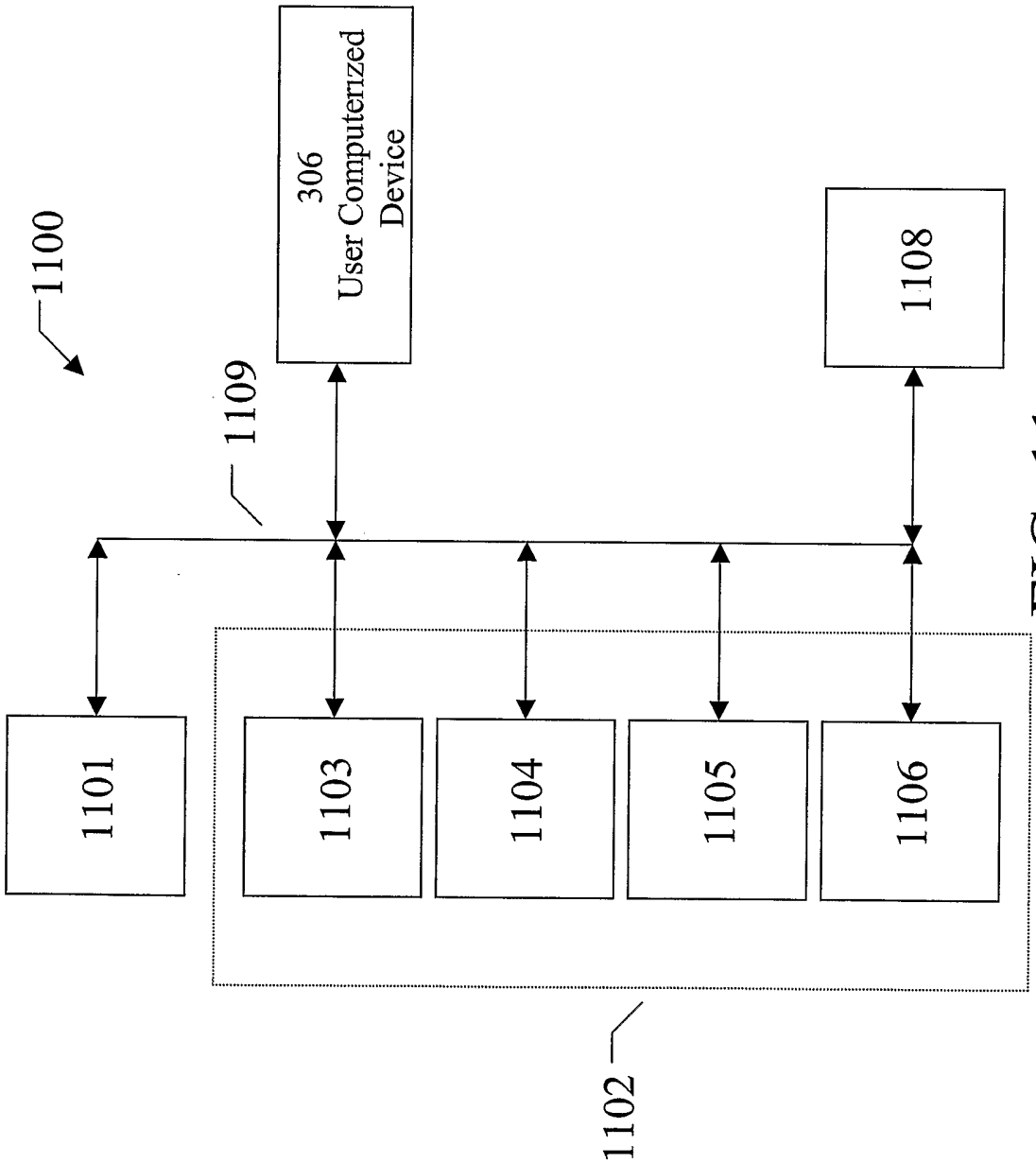

1100
306
User Computerized
Device
1108
1109
1101
1103
1104
1105
1106
1102

FIG. 11

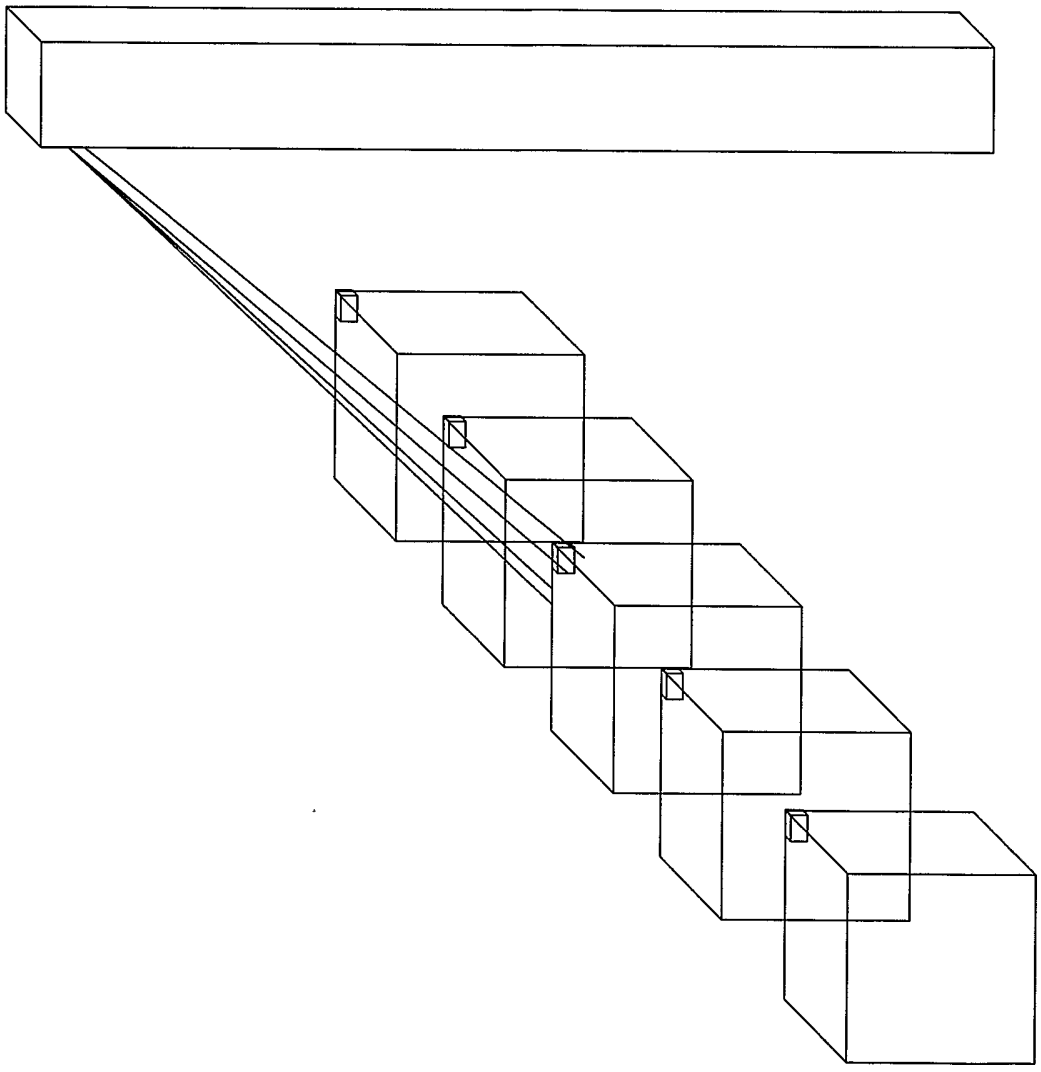


FIG. 12

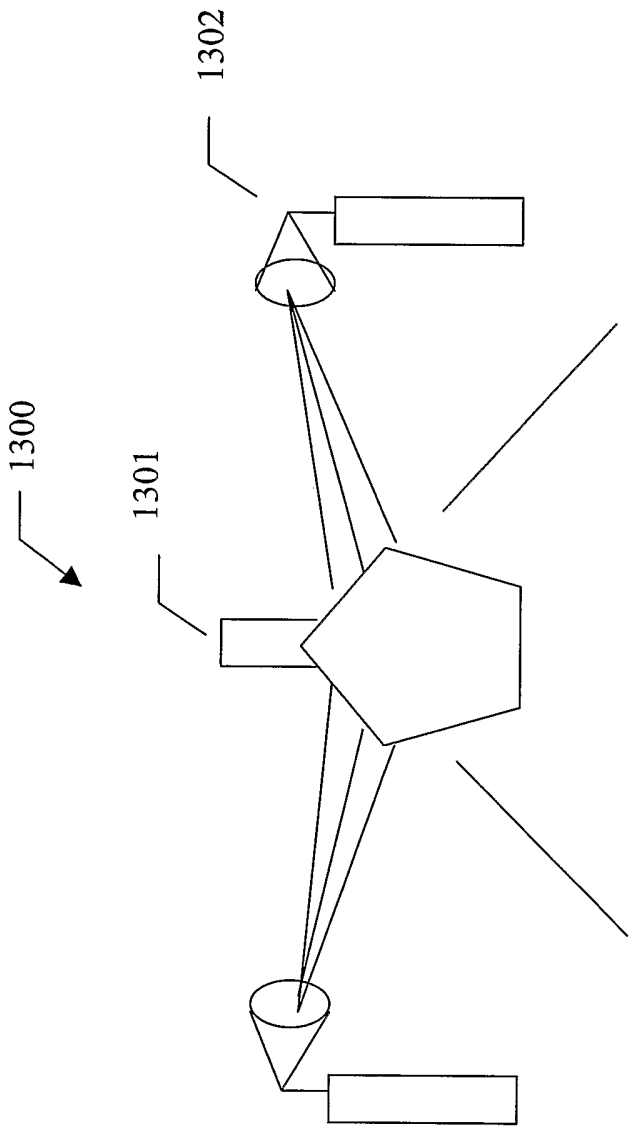


FIG. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/31630

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/00, 15/16, 11/30, 17/60
US CL : 713/200, 156; 700/232; 235/379, 380; 709/203, 206

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. : 713/200, 201, 156, 159, 172, 176, 178, 202; 700/232; 235/379, 380; 709/203, 206, 228, 238

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 passages	Relevant to claim No.
X, E	US 6,643,687 B1(DICKIE et al.) 04 November 2003 (04.11.2003), column 3, lines 44-61.	1-6 and 10-11
X, P	US 6,618,747 B1 (FLYNN et al.) 09 September 2003 (09.09.2003), column 3, lines 6-40).	7-9
A	US 6,000,832 A (FRANKLIN et al.) 14 December 1999 (14.12.1999), column 2, lines 38.	1-11
A	US 6,408,388 B1 (FISCHER) 18 June 2002 (18.06.2002), column 3, lines 6-54.	1-11

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

* Special categories of cited documents:

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

"E" earlier application or patent published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search
04 April 2004 (04.04.2004)

Date of mailing of the international search report
22 APR 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
for Michelle R. Eason
Emmanuel L. Moise

Telephone No. (703)305-3900