Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2386502 A1 2001/04/26

(21) 2 386 502

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2000/10/02
(87) Date publication PCT/PCT Publication Date: 2001/04/26
(85) Entrée phase nationale/National Entry: 2002/04/02
(86) N° demande PCT/PCT Application No.: US 2000/027069
(87) N° publication PCT/PCT Publication No.: 2001/030016
(30) Priorité/Priority: 1999/10/01 (09/411,004) US

(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 29/06

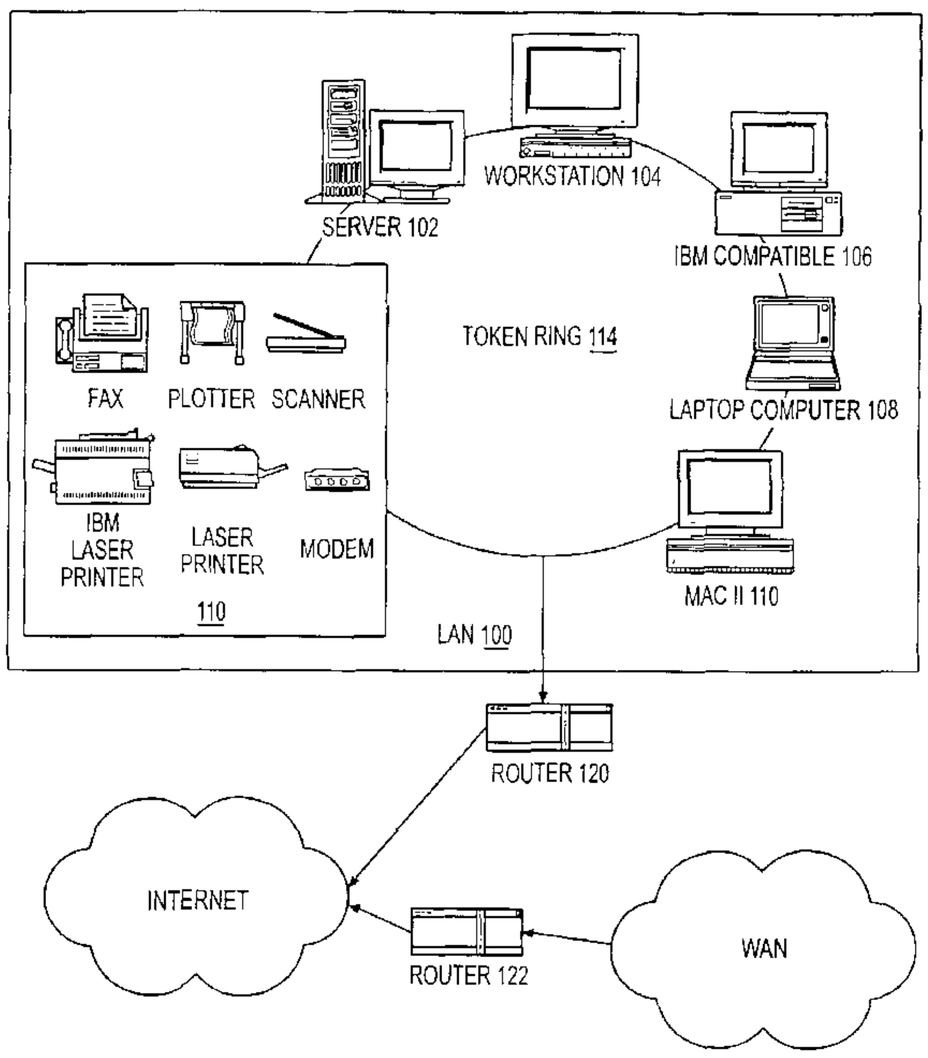
(71) Demandeur/Applicant:
ECOMXML INC., US

(72) Inventeurs/Inventors:
ZHANG, CHUNRU, US;
CAI, MING, US

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : PROCEDE PERMETTANT D'EMPECHER DES PARTIES DE DENONCER APRES COUP UNE TRANSACTION EXECUTEE AVEC UNE TIERCE PARTIE DE CONFIANCE

(54) Title: A METHOD FOR NON-REPUDIATION USING A TRUSTED THIRD PARTY



(57) Abrégé/Abstract:
A protocol for prohibiting non-repudiation by transacting parties involved in an executed electronic transaction, whereby a trusted third party is responsible for ensuring non-repudiation. In this protocol, a sender uses a secret sharing technology to divide the original session key into a first sub-session key and a second sub-session key. The first and second sub-session keys must be combined into the original session key in order for a recipient to decrypt a product that is encrypted with the original session key. The sender includes the first sub-session key that is encrypted with a recipient's public key and an encrypted product in a first message. Then the sender transmits the first message to the recipient. The recipient uses the first message as evidence of non-repudiation of origin, i.e., evidence of non-repudiation that the sender sent the transaction. The recipient transmits, to the sender, a second message requesting the second sub-session key. The sender may use the second message as evidence of non-repudiation of receipt, i.e., evidence of non-repudiation that the recipient received the transaction. Thereafter, the sender includes the second sub-session key which is encrypted with the trusted third party's public key in a third message that is forwarded to the trusted third party.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/30016 A3

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US00/27069

(22) International Filing Date: 2 October 2000 (02.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/411,004 1 October 1999 (01.10.1999) US

(71) Applicant: **ECOMXML INC.** [US/US]; 1080 Taylorsville Road, Suite 101, Washington Crossing, PA 19870 (US).

(72) Inventors: **ZHANG, Chunru**; 7413 Oxford Avenue, Apt. 15, Philadelphia, PA 19111 (US). **CAI, Ming**; 612 Hummingbird Lane, Bensalem, PA 19020 (US).

(74) Agent: **NEAL, Arlene, P.**; Morgan Lewis & Bockius LLP, 1800 M. Street, N.W., Washington, DC 20036-5869 (US).

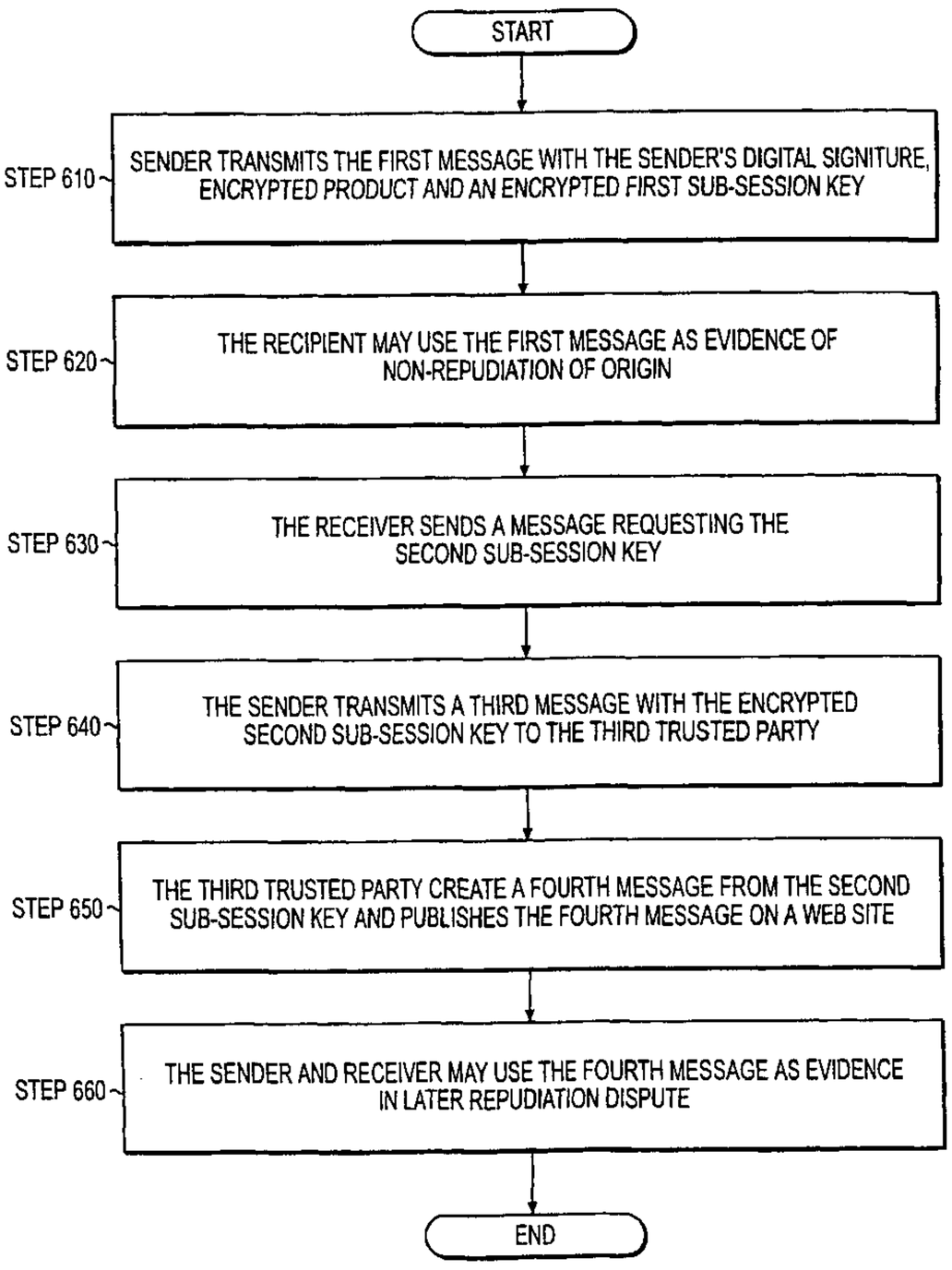
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE,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

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

Published:
— *with international search report*

[Continued on next page]

(54) Title: A METHOD FOR NON-REPUDIATION USING A TRUSTED THIRD PARTY



NON-REPUDIATION PROTOCOL 600

(57) Abstract: A protocol for prohibiting non-repudiation by transacting parties involved in an executed electronic transaction, whereby a trusted third party is responsible for ensuring non-repudiation. In this protocol, a sender uses a secret sharing technology to divide the original session key into a first sub-session key and a second sub-session key. The first and second sub-session keys must be combined into the original session key in order for a recipient to decrypt a product that is encrypted with the original session key. The sender includes the first sub-session key that is encrypted with a recipient's public key and an encrypted product in a first message. Then the sender transmits the first message to the recipient. The recipient uses the first message as evidence of non-repudiation of origin, i.e., evidence of non-repudiation that the sender sent the transaction. The recipient transmits, to the sender, a second message requesting the second sub-session key. The sender may use the second message as evidence of non-repudiation of receipt, i.e., evidence of non-repudiation that the recipient received the transaction. Thereafter, the sender includes the second sub-session key which is encrypted with the trusted third party's public key in a third message that is forwarded to the trusted third party.

WO 01/30016 A3

WO 01/30016 A3

(88) Date of publication of the international search report:
13 December 2001

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

A Method for Prohibiting Transacting Parties from Subsequently Repudiating an Executed Transaction With a Trusted Third Party

FIELD OF THE INVENTION

The present invention relates to protocols for ensuring security during electronic commerce in a computer network, and more particularly, to a protocol for preventing parties involved in an electronic commerce transaction from later repudiating the transaction.

BACKGROUND OF THE INVENTION

Electronic commerce, in the form of electronic data interchange (EDI), was initially utilized in inter-business trading by entities in certain industries. Entities involved in EDI employed a combination of technologies including dedicated communications lines, dial-up links, mainframe terminal emulation and packet-switching data networks and they generally relied on value added network (VAN) service providers. VAN service providers typically provide data communication services and assist industries/clients in such areas as software configuration, security, auditing, transaction tracing, and recovery of lost data. The costs associated with VAN services generally prohibited entities and individuals involved in short-term, low-volume trading from engaging in electronic commerce.

Transacting parties employing VAN services traditionally required weeks of preparation before the actual electronic transaction occurred. This preparation typically

included negotiating technical and administrative protocols and executing legal agreements. Electronic trading relationships between transacting parties generally involved long-term, high-volume trading between familiar, if not primary, business partners. This type of relationship typically justified the high cost of electronic commerce using VAN service providers. The emergence of the Internet, however, reduced the need for VAN service providers and enabled one-term or short-term transacting parties to engage in electronic commerce.

The Internet now provides an efficient means of transacting business between buyers and sellers of goods and services. For example, Internet users may utilize electronic mail as a quick means of negotiating business agreements, and selling vendors may utilize web sites to enable other vendors or individuals, without long term relationships with the selling vendors, to purchase merchandize on-line from the selling vendor. However, due to the public nature of the Internet, a third party may easily intercept and/or manipulate transactions over the World Wide Web (Web), thereby, breaching electronic security. As the volume of Internet electronic commerce between transacting parties with short and long-term relationships grows, so too will electronic commerce security issues.

In order to guarantee an electronic commerce system where each message in an EDI transaction is secured, security requirements, such as confidentiality, integrity, authenticity, authorization and non-repudiation, must be satisfied. Many computer systems use a password mechanism to control access to information. In these systems each user typically has a password that is kept secret and when the user needs access to

protected information, the user enters the secret password into the system. This scheme works well in conventional computer systems where the user's password is not revealed to others. However, in a network, particularly the Internet where an attached computer is capable of capturing a copy of all network traffic at a routing point, a simple password mechanism is susceptible to eavesdropping. If a user at one location sends a password across the network to a computer at another location, a third party who wiretaps the network may obtain a copy of the password. Therefore, to ensure that the content of messages in electronic transactions remain confidential despite wiretapping, the messages must be encrypted.

Encryption, in essence, scrambles bits of a message in such a way that only the intended recipient can unscramble them. Hence, a third party who intercepts a copy of the encrypted message will be unable to extract information from encrypted message. As would be understood, several encryption technologies exist. For example, symmetric key encryption algorithms or secret key cryptography have been developed to satisfy the confidentiality requirement. The encryption algorithms enable a sender to encrypt a message in a non-distinguishable cipher by using a secret key and only a recipient holding the same shared secret key can decrypt the encrypted message.

To satisfy the integrity requirement, hash functions may be used to generate a message integrity check in order for the recipient of the message to determine its integrity In general, together with public key cryptography, cryptographic hashing mechanisms encode the message in a message authentication code that a third party cannot break or forge. Thus, only the receiver can use the same hash function to check whether the

message is compromised or not, and also to verify whether it came from the real sender or not.

A digital signature mechanism that includes a pair of keys, may be used to authenticate the sender of a message. The sender signs the message with one key in the pair of keys known only to the sender, for example, the sender's private key. The recipient uses the other key in the pair of keys, for example the sender's public key, to verify the message. The recipient knows who sent the message because only the sender has the private key. To ensure that the message is not copied and later resent, the original message may also contain a date/time stamp, i.e., the date and time that the message was created. Controlling who has responsibility for each item of information and how such responsibility is delegated to others satisfies the authorization requirement. Despite these technical advances in electronic commerce, a transacting party may subsequently deny sending or receive a message in the transaction or the entire transaction. A protocol that prohibits one or more transacting parties from repudiating the transaction is required to satisfy the non-repudiation requirement.

The non-repudiation requirement is a communication attribute that prohibits one party, in an electronic transaction, from denying that the transaction occurred. There are two kinds of non-repudiation requirements dealing with subsequent denials of the transaction: non-repudiation of origin, which is non-repudiation by the sender that the transaction was sent; and non-repudiation of receipt, which is non-repudiation by the recipient that the transaction was received. While a sender and recipient, in a VAN, with long-standing relationships may trust each other and thus have limited or no concern

about repudiation, this is rarely the case with Internet transactions. Typically in an Internet transaction, one transacting party may not trust the other party or both parties may not trust each other. Moreover, in Internet commerce the trust level between transacting parties is dynamic because it is generally easy for one party to cheat without being discovered. For example, if the sender initially trusts the recipient but later suspects the recipient of cheating, the sender's trust level for the recipient is likely to change.

To solve the repudiation problem, some methodologies implement a traditional protocol whereby, the sender includes a desired product and the sender's digital signature in a first message and the recipient may use the digital signature as evidence of non-repudiation of origin. The recipient retrieves the desired product from the first message and is thereafter expected to send a reply message, with the recipient's digital signature, to the sender. The sender may use the reply message as evidence of non-repudiation of receipt. This protocol works best when the sender trusts the recipient. However, this scheme allows an unscrupulous recipient to deny receiving the first message and to fail to send the reply message. Hence, the sender has no way of determining if the recipient actually received the first message. Additionally, the sender has no way of determining if the first message was successfully delivered to the recipient or destroyed during a system malfunction. Since the tradition protocol cannot properly ensure non-repudiation of receipt, the sender must somehow ensure that the recipient will always acknowledge receipt of the message.

Some methods employ a trusted third party in each transaction, i.e., each message

in the transaction must pass through the trusted third party. The trusted third party verifies that each security requirement is fulfilled and that each party behaves appropriately in order to prevent repudiation by both parties and to prevent other breaches in security. Requiring the trusted third party to process all security requirements in each transaction increases the costs associated with electronic commerce. Additionally, as the number of transacting parties and the number of transactions between transacting parties increase, it may be difficult to find a trusted third party to process every transaction.

Moreover, other problems exist with the current trusted third party scheme. In the current scheme, the sender includes in the first message a product that is encrypted with a session key and transmits the first message to the recipient. The recipient requests the session key in order to decrypt the product in the first message. The sender transmits the session key that is encrypted with the recipient's public key to the trusted third party. The trusted third party thereafter transmits the session key to the recipient. However, a corrupt recipient may wiretap the network during transmission of the session key to the trusted third party. Since the session key is encrypted with the recipient's public key, the recipient may decrypt the session key with the recipient's private key and then decrypt the encrypted product with the intercepted session key. The corrupt recipient may later repudiate the transaction and the sender has no way of proving that the recipient retrieved the session key from the trusted third party. On the other hand, if the sender encrypts the session key with the trusted third party's public key, while trusted third parties are usually reputable organization, a corrupt trusted third party may decrypt the session key with it's private key and then decrypt the encrypted product. The sender may encrypt the session

key with the recipient's and trusted third party's public keys and thereby require the recipient to retrieve the key from the trusted third party, however, this solution is difficult to achieve in asymmetric cryptography.

A co-pending United States application *filed* HEREWITH, *titled*, A Method for Prohibiting Transacting Parties from Subsequently Repudiating an Executed Transaction Without a trusted third party, and incorporated by reference, relates to a protocol that does not have a trusted third party involved in the electronic transaction. In this protocol, the sender sends to the recipient in the encrypted first message, a product that is encrypted with the session key. The first message also includes the sender's digital signature, but it does not include the session key. The encrypted first message is used as evidence of non-repudiation of origin. A second message from the recipient requesting the session key is used as evidence of non-repudiation of receipt. Thereafter, the sender generates a third message containing the session key that is encrypted with the recipient's public key. The sender stores the third message in a public key repository on the sender's web site. The recipient is thereafter required to go to the sender's web site to retrieve the third message. The sender maintains the key repository. By monitoring activity on the sender's site, the sender can prove to the appropriate authorities during subsequent repudiation by the recipient that the recipient retrieved the session key from the key repository. This invention works well in a situation where the sender is trustworthy and the recipient does not have to worry about repudiation by the sender.

However in a situation where repudiation by the sender is an issue, this invention may not sufficiently solve the problem since the sender maintains the key repository and

the recipient must trust the sender to publish the key at the required time. An unscrupulous sender may publish the key after the required time and manipulate the time stamp in the message with the session key to prove that the key was actually published on time. Hence, when repudiation of origin and receipt is an issue, a protocol that does not require one transacting party to rely on the trustworthiness of another transacting party is required.

SUMMARY OF THE INVENTION

The present invention relates to a protocol for prohibiting non-repudiation by transacting parties involved in an executed electronic transaction, whereby a trusted third party is responsible for ensuring non-repudiation. In this protocol, a sender uses a secret sharing technology to divide an original session key into a first sub-session key and a second sub-session key. The first and second sub-session keys must be combined into the original session key in order for a recipient to decrypt a product that is encrypted with the original session key. The sender includes the first sub-session key that is encrypted with a recipient's public key and an encrypted product in a first message. Then the sender transmits the first message to the recipient. The recipient uses the first message as evidence of non-repudiation of origin, i.e., evidence of non-repudiation that the sender sent the transaction. The recipient transmits, to the sender, a second message requesting the second sub-session key. The sender may use the second message as evidence of non-repudiation of receipt, i.e., evidence of non-repudiation that the recipient received the transaction. Thereafter, the sender includes the second sub-session key which is

encrypted with the trusted third party's public key in a third message that is forwarded to the trusted third party. The trusted third party decrypts the third message to retrieve the second sub-session key and then re-encrypts the second sub-session key with the recipient's public key. The trusted third party includes the re-encrypted second sub-session key in a fourth message and publishes the fourth message on the trusted third party's web site where the recipient is responsible for retrieving it. This protocol therefore ensures non-repudiation of origin and non-repudiation of receipt without reliance on the trustworthiness of one or more transacting parties. Furthermore, by involving the trusted third party in minimal transaction processing, i.e., only non-repudiation processing, the responsibility and liability of the trusted third party is reduced, thereby reducing the cost associated with trusted third parties in electronic transactions.

Specifically in the preferred embodiment of the invention, the sender encrypts a requested product with the session key and includes the encrypted product, the sender's digital signature and the first sub-session key in the first message. Only the recipient can decrypt the first sub-session key with the recipient's private key. In order to decrypt the first message and retrieve the requested product, the recipient must also obtain the second sub-session key. The recipient may use the encrypted first message with the first sub-session key and the sender's digital signature as evidence of non-repudiation of origin. When the recipient requests the second sub-session key with a message that includes the recipient's digital signature, the sender may use the request message as evidence of non-repudiation of receipt. The sender thereafter encrypts the second sub-session key with the

trusted third party's public key and includes the encrypted second sub-session key in the third message. Thus, only the trusted third party can obtain the second sub-session key. The trusted third party decrypts the third message in order to obtain the second sub-session key. The trusted third party re-encrypts the second sub-session with the recipient's public key and includes the re-encrypted second sub-session key in a fourth message. The trusted third party publishes the fourth message in a key repository on trusted third party's web site. Thereafter, only the recipient can decrypt the second sub-session key with the recipient's private key.

The recipient is required to go to the trusted third party's web site to retrieve the fourth message. Subsequently, the recipient combines the first and second sub-session keys to form the original session key in order to decrypt the encrypted product in the first message. The trusted third party maintains the key repository. By monitoring activity on the trusted third party's site, the trusted third party can prove to the appropriate authorities during subsequent repudiation by the recipient that the recipient retrieved the second sub-session key from the key repository.

Additional features and advantages of the invention will be set forth in the description that follows, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and advantages of the invention will be realized and attained by the system particularly pointed out in the written description and claims hereof as well as the appended drawings.

To achieve these and other advantages and in accordance with the purpose of the invention, as embodied and broadly described, the present invention provides a method

for ensuring non-repudiation by transacting parties involved in an executed electronic transaction, the transacting parties using a trusted third party to resolve repudiation disputes, the method comprising the steps of: generating, by a sending party, a session key and dividing the session key into a plurality of sub-session keys comprising a first sub-session key and a second sub-session key; sending, by the sending party to a receiving party, a first cryptographic message, the first cryptographic message including a product that is encrypted with the session key, a digital signature of the sending party, and the first sub-session key; requesting upon receipt of the first cryptographic message, by the receiving party from the sending party, the second sub-session key in a second message, the second message including the receiving party digital signature; transmitting upon receipt of the second message, from the sending party to a trusted third party, a third cryptographic message with the second sub-session key, the second sub-session key encrypted with the trusted third party's public key; obtaining, by the trusted third party, the second sub-session key from the third cryptographic message and generating a fourth cryptographic message; publishing, by the trusted third party, the fourth cryptographic message on the trusted third party's web site; retrieving, by the receiving party, the fourth cryptographic message from the trusted third party's web site; and combining, by the receiving party, a predefined number of the plurality of sub-session keys into a required session key in order to retrieve encrypted product from the first cryptographic message.

The invention alternatively provides a system for ensuring non-repudiation by transacting parties involved in an executed electronic transaction, the transacting parties using a trusted third party to resolve repudiation disputes, the system comprises: means

for generating, by a sending party, a session key and dividing the session key into a plurality of sub-session keys comprising a first sub-session key and a second sub-session key; means for sending, by the sending party to a receiving party, a first cryptographic message, the first cryptographic message including a product that is encrypted with the session key, a digital signature of the sending party, and the first sub-session key; means for requesting upon receipt of the first cryptographic message, by the receiving party from the sending party, the second sub-session key in a second message, the second message including the receiving party digital signature; means for transmitting upon receipt of the second message, from the sending party to a trusted third party, a third cryptographic message with the second sub-session key, the second sub-session key encrypted with the trusted third party's public key; means for obtaining, by the trusted third party, the second sub-session key from the third cryptographic message and generating a fourth cryptographic message; means for publishing, by the trusted third party, the fourth cryptographic message on the trusted third party's web site; means for retrieving, by the receiving party, the fourth cryptographic message from the trusted third party's web site; and means for combining, by the receiving party, a predefined number of the plurality of sub-session keys into a required session key in order to retrieve encrypted product from the first cryptographic message.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this

specification, illustrate embodiments of the invention that together with the description serve to explain the principles of the invention.

In the drawings:

Fig. 1 illustrates a computer network in which the inventive non-repudiation protocol may be incorporated;

Fig. 2 illustrates the TCP/IP Layering Model Protocol used during communications between components on the computer network;

Fig. 3 illustrates a secret sharing technology which enables a sender to divide a session key into two keys;

Fig. 4 illustrates an alternate embodiment for dividing two session keys into two sub-session keys;

Fig. 5 illustrates a preferred embodiment of the inventive non-repudiation protocol; and

Fig. 6 illustrates the steps implemented according to the preferred embodiment of the inventive non-repudiation protocol in Fig. 5; and

Fig. 7 illustrates a security architecture in which the inventive non-repudiation protocol may be practiced.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. The present invention described below extends the functionality of the inventive non-repudiation

protocols and methods for utilizing the protocol in a system.

Fig. 1 is an example of a local area network (LAN) 100 that is configured to utilize a non-repudiation protocol. LAN 100 comprises a server 102, four computer systems 104-110, and peripherals, such as printers and other devices 112, that may be shared by components on LAN 100. Computer systems 104-110 may serve as clients for server 102 and/or as clients and/or servers for each other and/or for other components connected to LAN 100. Components on LAN 100 are preferably connected together by cable media, for example copper or fiber-optic cable and the network typology may be a token ring topology 114. It should be apparent to those of ordinary skill in the art that other media, for example, wireless media, such as optical and radio frequency, may also connect LAN 100 components. It should also be apparent that other network topologies, such as Ethernet, may be used.

Data may be transferred between components on LAN 100 in packets, i.e., blocks of data that are individually transmitted over LAN 100. Routers 120, 122 create an expanded network by connecting LAN 100 to other computer networks, such as the Internet, other LANs or Wide Area Networks (WAN). Routers are hardware devices that may include a conventional processor, memory, and separate I/O interface for each network to which it connects. Hence, components on the expanded network may share information and services with each other. In order for communications to occur between components of physically connected networks, all components on the expanded network and the routers that connect them must adhere to a standard protocol. Computer networks connected to the Internet and to other networks typically use TCP/IP Layering Model

Protocol. It should be noted that other internetworking protocols may be used.

As illustrated in Fig. 2, TCP/IP Layering Model comprises an application layer or (Layer 5) 202, a transport layer or (Layer 4) 204, an Internet layer or (Layer 3) 206, a network interface layer or (Layer 2) 208, and a physical layer or (Layer 1) 210.

Application layer protocols 202 specify how each software application connected to the network uses the network. Transport layer protocols 204 specify how to ensure reliable transfer among complex protocols. Internet layer protocols 206 specify the format of packets sent across the network as well as mechanisms used to forward packets from a computer through one or more routers to a final destination. Network interface layer protocols 208 specify how to organize data into frames and how a computer transmits frames over the network; and physical layer protocols 210 correspond to the basic network hardware. By using TCP/IP Layering model protocols, any component connected to the network can communicate with any other component connected directly or indirectly to one of the attached networks.

A browser application, such as Microsoft Explorer ™ or Netscape Internet Browser ™, connects users on computer systems 104-110 to the World Wide Web (Web) on the Internet. Most browser applications display information on computer 104-110 screens and permit a user to navigate through the Web using a mouse. Like other network applications, Web browsing uses the client-server paradigm. When given the Uniform Resource Locator (URL) of a document, the browser application becomes a client and it contacts the server specified in the URL to request the document. After receiving the document from the server, the browser application displays the document

for the user. When the browser application interacts with a Web server application, the two applications follow the HyperText Transport Protocol (HTTP). HTTP allows the browser application to request a specific item, which the server application then returns. To ensure that browser applications and server applications inter-operate unambiguously, HTTP defines the exact format for request sent from the browser application to the server application as well as the format of replies that the server application returns. It is apparent to those skilled in the art that other protocols may be used.

Currently, during an electronic commerce transaction on the Internet, one transacting party enters the URL of another transacting party and the browser application requests a web page associated with the URL from the appropriate server application. After displaying the web page, one transacting party may transmit a transaction to the other transacting party through the displayed web page and the browser application. For example, a buyer on the Internet, wishing to purchase a software application, may enter the URL of a seller into the browser application. The browser displays a corresponding web page and the buyer may order the software application through the web page. Upon receiving the order, the seller may transmit the software application through the seller's web page to the buyer. During transmission, however, a third party may intercept the transaction or the system may malfunction before all messages in the transaction are submitted to the buyer.

To ensure that security requirements of confidentiality, integrity, authenticity and authorization are fulfilled during each transmission, current encryption technologies are implemented. However one of the transacting parties may later deny that the transaction

actually occurred. For example, the buyer may subsequently deny receiving the already delivered software application. Moreover, if there was a system malfunction, the transmission of the software application to the buyer may be destroyed during the malfunction and the seller may request payment for the undelivered software application from the buyer. Thus, it is important that both the buyer and the seller have some evidence of a properly executed transaction to prevent subsequent repudiation by either party.

The present invention utilizes a secret sharing technology to prevent non-repudiation of origin and receipt. Secret sharing is a key distribution mechanism whereby multiple parties hold separate portions of a required key and a predefined number parties must combine their portions for the required key to be recovered. Secret sharing technology therefore ensures that the recipient of a product must obtain predefined part(s) of the required key that encrypts a product, from the sender or a third party, in order for the recipient to decrypt the product.

Fig. 3 illustrates a secret sharing technology that enables a sender to divide a session key into two sub-session keys. As illustrated in Fig. 3, the sender generates an original session key (K) and divides it into K1 302 and K2 304 by using the following formula:

$$K1 = (K + r*ID_R) \bmod 2^{64}$$

$$K2 = (K + r*ID_{TTP}) \bmod 2^{64}$$

Where r is a large random number generated by the sender; ID_R is the recipient's unique public identifier; and ID_{TTP} is a trusted third party's unique public identifier.

Fig. 4 illustrates an alternate embodiment for dividing two session keys into two sub-session keys. Using two session keys in a secret sharing technology ensure stronger security since a third party must obtain two keys in order to decrypt the desired product. As illustrated in Fig. 4, the sender generates two original session keys (K and K') and divides them into K1 402 and K2 404 by using the following formula:

$$K1 = (K + K'*ID_R) \bmod 2^{64}$$

$$K2 = (K + K'*ID_{TTP}) \bmod 2^{64}$$

Where K and K' can be recreated by the recipient when he/she obtains K1 from the sender and K2 from the trusted third party.

Fig. 5 illustrates a preferred embodiment of a non-repudiation protocol 500 where the trusted third party addresses only non-repudiation issues, thereby minimizing the cost associated with trusted third party processing. In protocol 500, sender 502 includes a product that is encrypted with the session key in message 508 and transmits message 508 to the recipient. Message 508 also includes sender's 502 digital signature and first sub-session key 302/402 that is encrypted with recipient's 504 public key. Recipient 504 may decrypt first sub-session key 302/402 with recipient's private key. However, recipient 504 is required to obtain the second sub-session key 304/404 in order to decrypt message 508 and retrieve the encrypted product. In order to obtain second sub-session key 304/404, recipient 504 must acknowledge receipt of message 508 to sender 502. If recipient 504 is no longer interested in encrypted message 508 after receiving it, recipient 504 is not required to request second sub-session key 304, and the protocol ends. If recipient 504 did not receive encrypted message 508 due to a system error and recipient

504 does not request second sub-session key 304/404, sender 502 is then alerted by the fact that recipient 504 did not request second sub-session key 304/404. Sender 502 may thereafter inquire why recipient 504 did not request the second sub-session key and may re-send encrypted message 508 when the system malfunction no longer exists.

Recipient 504 may use encrypted message 508 as evidence of non-repudiation of origin. Recipient 504 may request second sub-session key 304/404 from sender 502 in message 510. Message 510 includes recipient's 504 digital signature and sender 502 may use message 510 as evidence of non-repudiation of receipt. Upon receipt of the message 510, sender 502 encrypts second sub-session key 304/404 with a trusted third party's public key and includes encrypted sub-session key 304/404 in message 512. Sender 502 thereafter transmits messages 512 to trusted third party 506 who is responsible for resolving repudiation disputes between sender 502 and recipient 504.

Upon receipt of message 512, trusted third party 506 decrypts it with trusted third party's private key to obtain second sub-session key 304/404. Trusted third party 506 re-encrypts second sub-session key 304/404 with recipient's 504 public key. Then trusted third party 506 includes the re-encrypted second sub-session key 304/404 in message 514 and publishes message 514 in trusted third party's public key repository. Thereafter only recipient 504 can decrypt message 514 with recipient's private key. Recipient 504 and sender 502 need to actively retrieve message 514 from the trusted third party's site by using a persistent protocol such as HTTP or File Transfer Protocol (FTP). Recipient 504 then combines first and second sub-session keys 302/402 and 304/404 to retrieve the original session key and decrypt the product in message 508.

In this protocol, trusted third party 506 is responsible for taking care of the key repository 518 and publishing second sub-session key 304/404. By tracking activity on the trusted third party's site, trusted third party 506 can determine when recipient 504 retrieved second sub-session key 304/404. If recipient 504 later deny retrieving second sub-session key304/404, trusted third party 506 can prove to the appropriate authority that the key was actually published and retrieved. Moreover, if there is a dispute between sender 502 and recipient 504 about proper transmission of the product, sender 502 can transmit a fifth message with the first sub-session key 302/402 and the encrypted product in dispute to trusted third party 506. Trusted third party can then verify whether there was proper transmission from sender to recipient. Since trusted third party 506 is generally a disinterested and reputable party, it is easier for trusted third party to resolve disputes and repudiation issues.

Fig 6 illustrates the steps implemented in a preferred embodiment of the inventive protocol. In Step 610 of protocol 500, sender 502 sends encrypted message 508 with sender's 302 digital signature, the encrypted product and a first sub-session key to the recipient. In Step 620, recipient 504 may use encrypted message 508 as evidence of non-repudiation of origin. In Step 630, recipient 504 requests second sub-session key 304/404 from sender 502 in message 510 with recipient's 504 digital signature. Sender 502 may then use message 510 as evidence of non-repudiation of receipt. In Step 640, upon receipt of message 510, sender 502 transmits a third message 512 with the encrypted second sub-session key to trusted third party. In Step 650, trusted third party 506 decrypts third message 512, re-encrypts second sub-session key with recipient's public

key and stores re-encrypted second sub-session key in fourth message 514. Trusted third party 506 publishes the fourth message 514 in the public key repository 518 on trusted third party's 506 web site. In Step 660, recipient is responsible for retrieving fourth message 514 from the key repository, and sender 502 and recipient 504 may use message 514 as evidence in any later case of repudiation dispute.

Fig. 7 illustrates a security architecture 700 in which the inventive protocol may be practiced. At the base layer of security architecture 700 is a security hardware 702 that makes it more difficult for a third party to manipulate or steal secret information that is embedded in a software package. A secret key cryptography system 704 and a public key cryptography system 706 are built on security hardware 702 for providing additional security. Cryptographic algorithms 708 are built on cryptographic systems 704 and 706. The inventive non-repudiation protocol 710 and cryptographic protocols 712 are built on cryptographic algorithms 708. Encryption algorithms and protocols 714a- 714d that ensure confidentiality, integrity, authenticity and non-repudiation are built on cryptographic protocols 712 and non-repudiation protocol 710. Security administration 716, which includes key management, authorization and management of access control for a firewall and proxy server, is built on algorithms and protocol 714a-714d. HTTP 718 and S/MIME 720, the two most widely used protocols on the Web in electronic data interchange, are also built on algorithms and protocols 714a-714d. A directory service 722, which implements a key distribution mechanism to distribute public keys in a certificate authority 724, and certificate authority 724 are built upon security administration 716 and on algorithms and protocols 714a-714d. Examples of the

directory services include Microsoft Exchange™ directory, Lotus Notes™ directory, and Novell Netware™ Directory Service. The next layer includes public key infrastructure (PKI) 724, which is a comprehensive security infrastructure for enterprise-wide applications. PKI 724 combines digital certificates, public key cryptography, secret key cryptography, certificate authorities and directory services into one to make industry decisions about security easier. EDI INT 726, a standard making organization, is also in the layer with PKI 724. The final layer includes non-EDI applications 728 and EDI applications 730.

The foregoing description has been directed to specific embodiments of this invention. It will be apparent, however, that other variations and modifications may be made to the described embodiments, with the attainment of some or all of their advantages. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the invention.

WHAT IS CLAIMED:

1. A method for ensuring non-repudiation by transacting parties involved in an executed electronic transaction, the transacting parties using a trusted third party to resolve repudiation disputes, the method comprising the steps of:

generating, by a sending party, a session key and dividing the session key into a plurality of sub-session keys comprising a first sub-session key and a second sub-session key;

sending, by the sending party to a receiving party, a first cryptographic message, the first cryptographic message including a product that is encrypted with the session key, a digital signature of the sending party, and an encrypted first sub-session key;

requesting upon receipt of the first cryptographic message, by the receiving party from the sending party, the second sub-session key in a second message, the second message including the receiving party digital signature;

transmitting upon receipt of the second message, from the sending party to a trusted third party, a third cryptographic message with the encrypted second sub-session key, the second sub-session key encrypted with the trusted third party's public key;

obtaining, by the trusted third party, the second sub-session key from the third cryptographic message and generating a fourth cryptographic message;

publishing, by the trusted third party, the fourth cryptographic message on the trusted third party's web site;

retrieving, by the receiving party, the fourth cryptographic message from the trusted third party's web site; and

combining, by the receiving party, a predefined number of the plurality of sub-session keys into a required session key in order to retrieve encrypted product from the first cryptographic message.

2. The method of claim 1, comprising the step of using a plurality of keys as the session key.

3. The method of claim 2, wherein the step of combining a predefined number of the plurality of sub-session keys further comprising the step of combining the first and second sub-session keys into the required session key in order to retrieve encrypted product from the first cryptographic message.

4. The method of claim 3, wherein the step of obtaining further comprising the steps of:

decrypting, by the trusted third party, the second sub-session key in the third cryptographic message with the trusted third party's private key to obtain the second sub-session key; and

re-encrypting, by the trusted third party, the second sub-session key with the receiving party's public key and including the re-encrypting second sub-session key in the fourth cryptographic message;

5. The method of claim 4, wherein the step of publishing further comprising the step of storing, by the trusted third party, the fourth cryptographic message in a public key repository on the trusted third party's web site.

6. The method of claim 5, further comprising the step of encrypting, by the sending party, the first sub-session key in the first cryptographic message with the receiving party's public key.

7. The method of claim 6, further comprising the step of decrypting, by the receiving party, the first sub-session key in the first cryptographic message with the receiving party's private key.

8. The method of claim 7, further comprising the step of requiring a predefine number of the plurality of sub-session keys to retrieve information from the first cryptographic message.

9. The method of claim 8, further comprising the step of requiring the first and second sub-session keys to retrieve information from the first cryptographic message.

10. The method of claim 9, further comprising the step of using, by the receiving party, the first cryptographic message as evidence of non-repudiation of origin.

11. The method of claim 10, further comprising the step of using, by the sending party, the second cryptographic message as evidence of non-repudiation of receipt.

12. The method of claim 11, further comprising the step of retrieving, by the receiving and sending parties, the fourth cryptographic message from the trusted third party's web site by using a persistent protocol.

13. The method of claim 12, further comprising the step of auditing, by the trusted third party, the trusted third party's web site in order to determine when the receiving party retrieves the fourth cryptographic message.

14. The method of claim 13, further comprising the step of proving, by the trusted third party, receipt of the fourth cryptographic message by the receiving party through the step of auditing.

15. The method of claim 14, further comprising the step of using the fourth cryptographic message as evidence of non-repudiation of origin and receipt.

16. The method of claim 15, further comprising the step of sending, from the sending party to the trusted third party, a fifth cryptographic message to resolve a repudiation dispute between the sending party and the receiving party.

17. The method of claim 16, further comprising the step of including, by the sending party, the encrypted first sub-session key and the encrypted product in the fifth cryptographic message.

18. The method of claim 17 further comprising the step of verifying, by the trusted third party, proper transmission of the encrypted first sub-session key and the encrypted product from the sending party to the receiving party by using the fifth cryptographic message, and then resolving repudiation dispute between the sending party and receiving party.

19. The method of claim 18, further comprising the step of using hashing to create the first, second, third, fourth and fifth cryptographic messages.

20. The method of claim 18, further comprising the step of using encryption to create the first, second, third, fourth and fifth cryptographic messages.

21. The method of claim 18, further comprising the step of using encoding to create the first, second, third, fourth and fifth cryptographic messages.

22. A system for ensuring non-repudiation by transacting parties involved in an executed electronic transaction, the transacting parties using a trusted third party to resolve repudiation disputes, the system comprises:

means for generating, by a sending party, a session key and dividing the session key into a plurality of sub-session keys comprising a first sub-session key and a second sub-session key;

means for sending, by the sending party to a receiving party, a first cryptographic message, the first cryptographic message including a product that is encrypted with the session key, a digital signature of the sending party, and an encrypted first sub-session key;

means for requesting upon receipt of the first cryptographic message, by the receiving party from the sending party, the second sub-session key in a second message, the second message including the receiving party's digital signature;

means for transmitting upon receipt of the second message, from the sending party to a trusted third party, a third cryptographic message with the encrypted second sub-session key, the second sub-session key encrypted with the trusted third party's public key;

means for obtaining, by the trusted third party, the second sub-session key from the third cryptographic message and generating a fourth cryptographic message;

means for publishing, by the trusted third party, the fourth cryptographic message on the trusted third party's web site;

means for retrieving, by the receiving party, the fourth cryptographic message from the trusted third party's web site; and

means for combining, by the receiving party, a predefined number of the plurality of sub-session keys into a required session key in order to retrieve encrypted product from the first cryptographic message.

23. The method of claim 22, comprising means for using a plurality of keys as the session key.

24. The method of claim 23, further comprising means for combining the first and second sub-session keys into the required session key in order to retrieve encrypted product from the first cryptographic message.

25. The method of claim 24, further comprising:

means for decrypting, by the trusted third party, the second sub-session key in the third cryptographic message with the trusted third party's private key to obtain the second sub-session key; and

means for re-encrypting, by the trusted third party, the second sub-session key with the receiving party's public key and including the re-encrypted second sub-session key in the fourth cryptographic message;

26. The method of claim 25, further comprising means for storing, by the trusted third party, the fourth cryptographic message in a public key repository on the trusted third party's web site.

27. The method of claim 26, further comprising means for encrypting, by the sending party, the first sub-session key in the first cryptographic message with the receiving party's public key.

28. The method of claim 27, further comprising means for decrypting, by the receiving party, the encrypted first sub-session key in the first cryptographic message with the receiving party's private key.

29. The method of claim 28, further comprising means for requiring a predefine number of the plurality of sub-session keys to retrieve information from the first cryptographic message.

30. The method of claim 29, further comprising means for requiring the first and second sub-session keys to retrieve information from the first cryptographic message.

31. The method of claim 30, further comprising means for using, by the receiving party, the first cryptographic message as evidence of non-repudiation of origin.

32. The method of claim 30, further comprising means for using, by the sending party, the second cryptographic message as evidence of non-repudiation of receipt.

33. The method of claim 32, further comprising means for retrieving, by the receiving and sending parties, the fourth cryptographic message from the trusted third party's web site by using a persistent protocol.

34. The method of claim 33, further comprising means for auditing, by the trusted third party, the trusted third party's web site in order to determine when the receiving party retrieves the fourth cryptographic message.

35. The method of claim 34, further comprising means for proving, by the trusted third party, receipt of the fourth cryptographic message by the receiving party through the step of auditing.

36. The method of claim 35, further comprising means for using the fourth cryptographic message as evidence of non-repudiation of origin and receipt.

37. The method of claim 36, further comprising means for sending, from the sending party to the trusted third party, a fifth cryptographic message to resolve a repudiation dispute between the sending party and the receiving party.

38. The method of claim 37, further comprising means for including, by the sending party, the encrypted first sub-session key and the encrypted product in the fifth cryptographic message.

39. The method of claim 38 further comprising means for verifying, by the trusted third party, proper transmission of the encrypted first sub-session key and the encrypted product from the sending party to the receiving party by using the fifth cryptographic message, and then resolving repudiation dispute between the sending party and receiving party.

40. The system of claim 39, further comprising means for using hashing to create the first, second, third, fourth and fifth cryptographic messages.

41. The system of claim 39, further comprising means for using encryption to create the first, second, third, fourth and fifth cryptographic messages.

42. The method of claim 39, further comprising means for using encoding to create the first, second, third, fourth and fifth cryptographic messages.

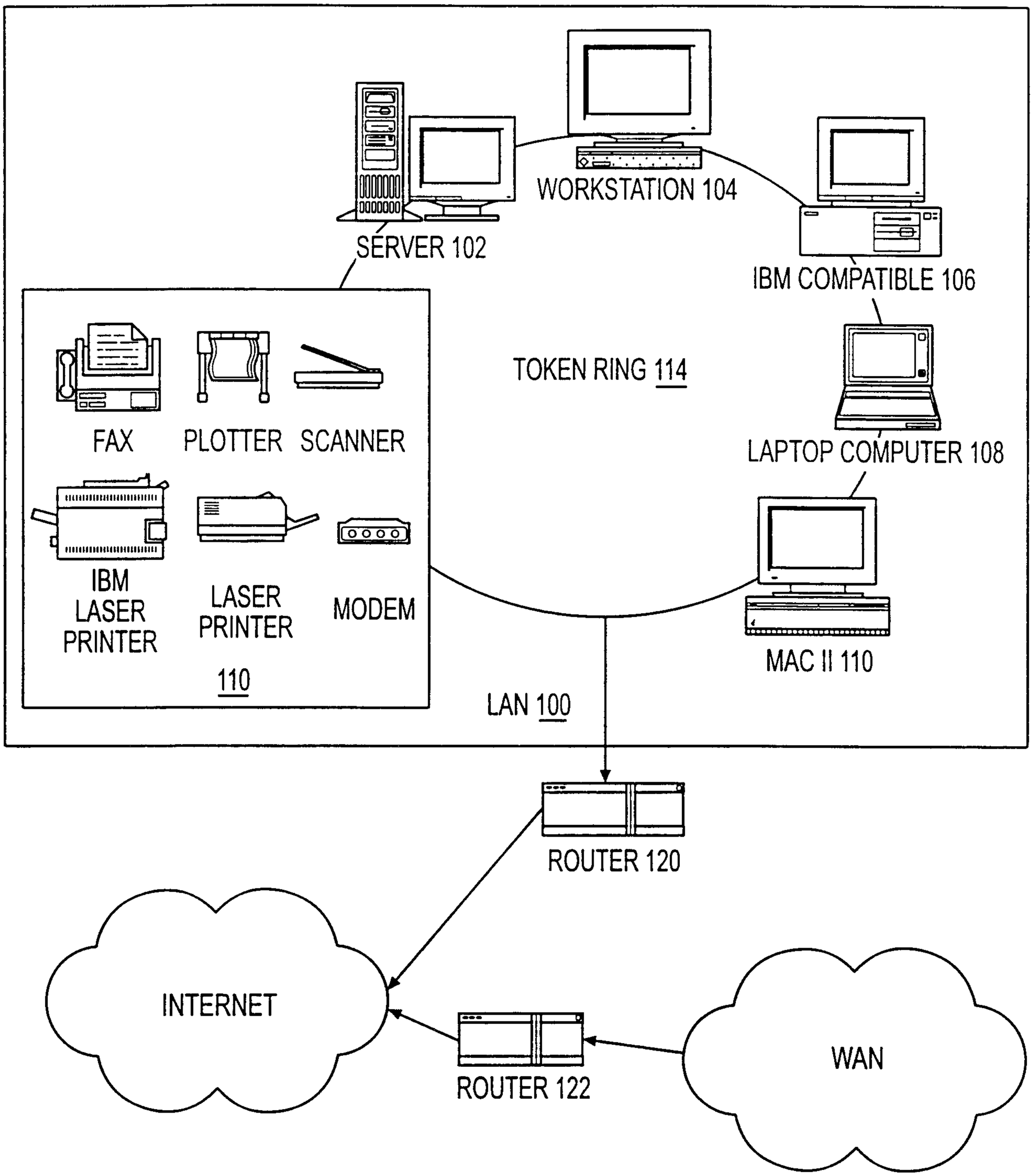
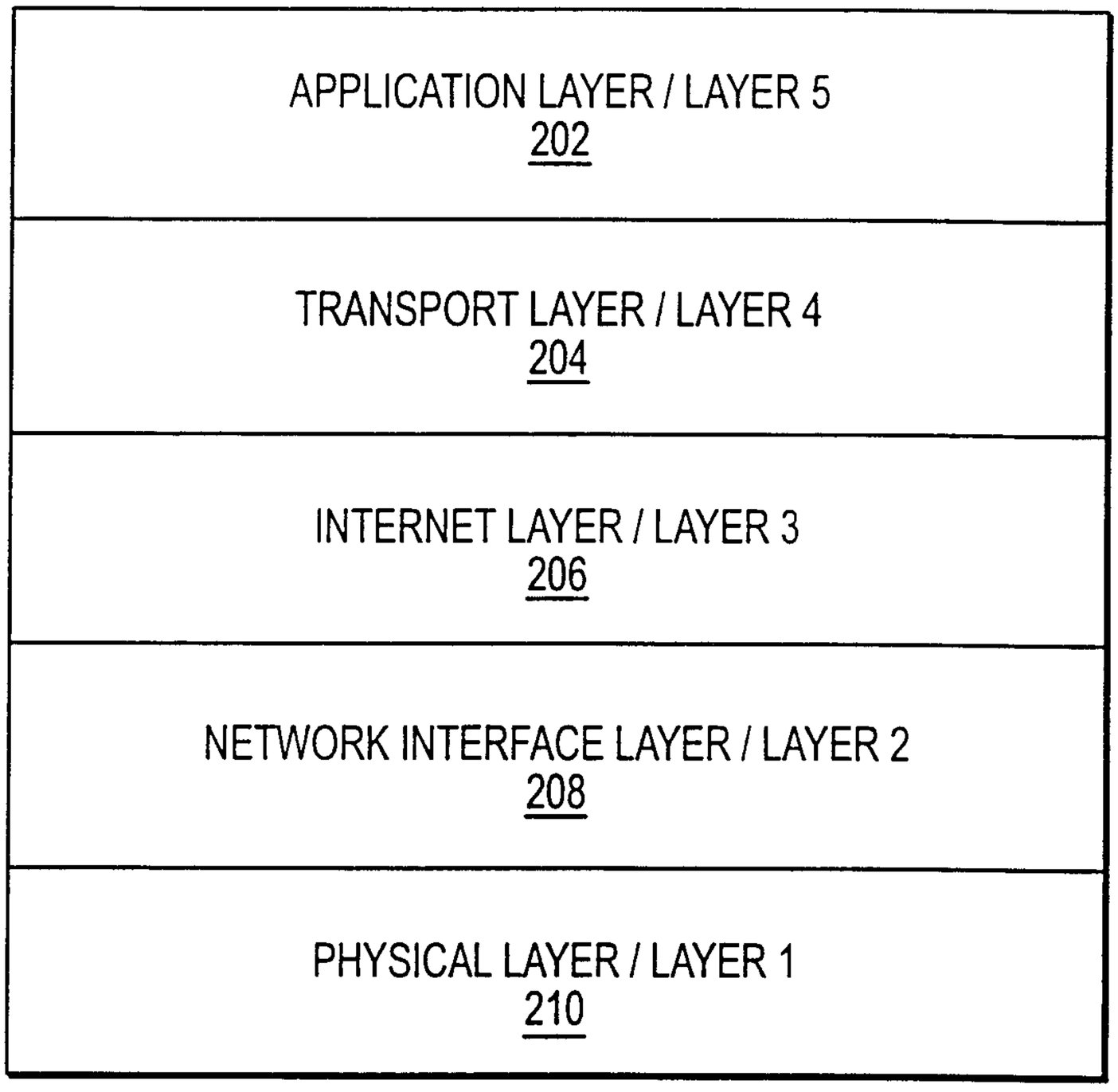

SERVER 102
WORKSTATION 104
IBM COMPATIBLE 106
LAPTOP COMPUTER 108
MAC II 110
TOKEN RING 114
FAX
PLOTTER
SCANNER
IBM LASER PRINTER
LASER PRINTER
MODEM
110
LAN 100
ROUTER 120
ROUTER 122
INTERNET
WAN

FIG. 1



TCP/IP LAYERING MODEL

FIG. 2

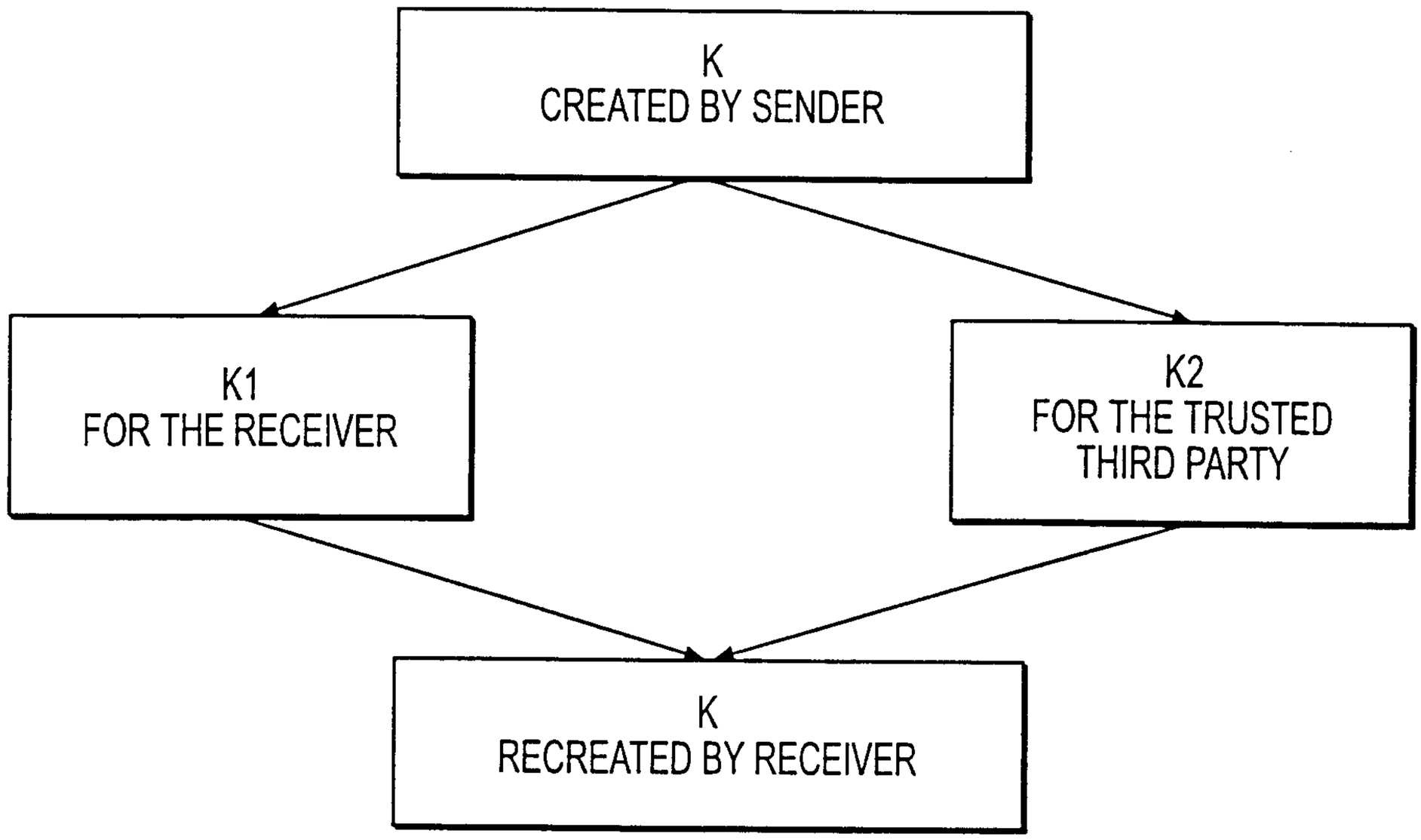

K
CREATED BY SENDER
K1
FOR THE RECEIVER
K2
FOR THE TRUSTED
THIRD PARTY
K
RECREATED BY RECEIVER

FIG. 3

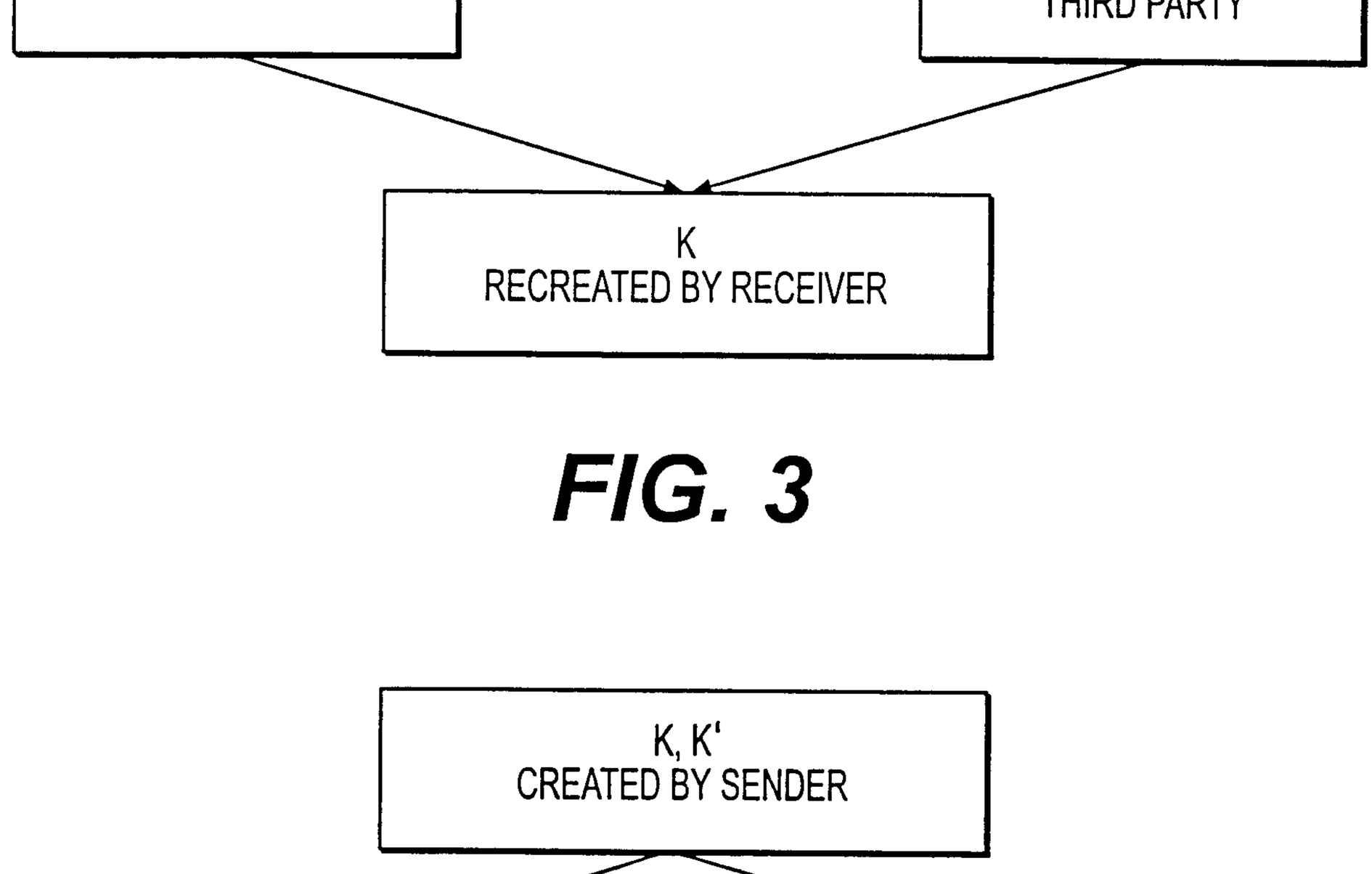
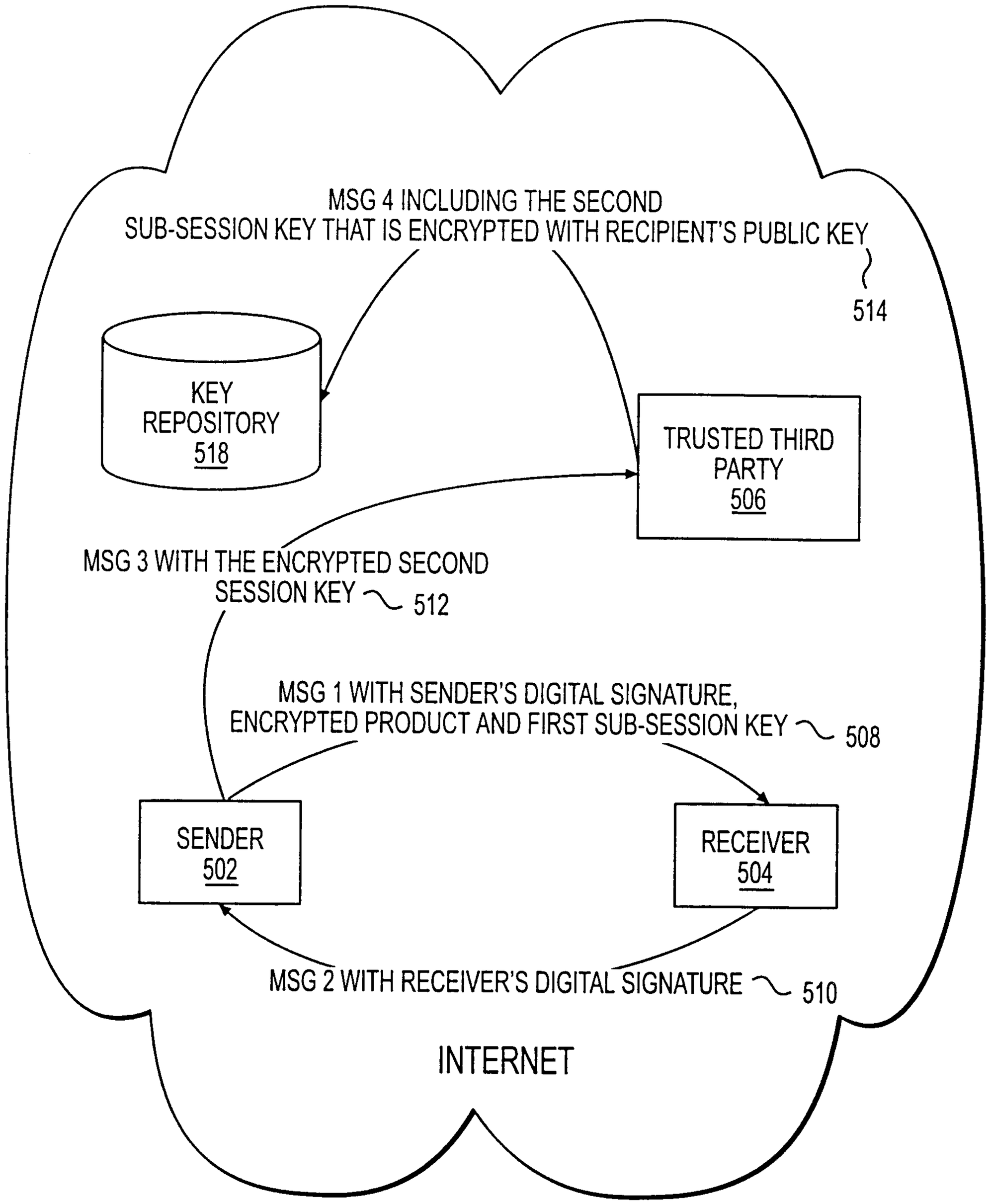
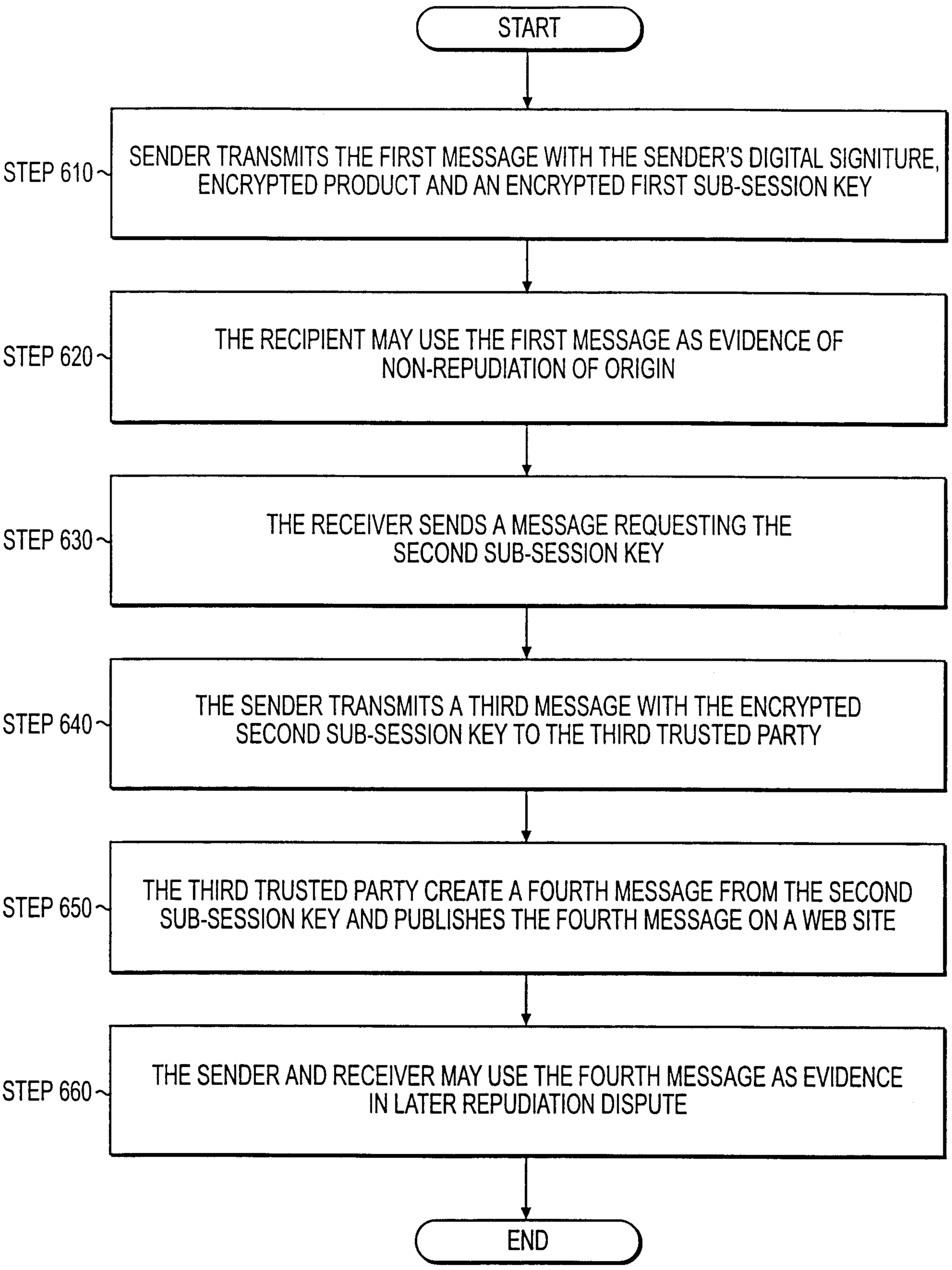

K, K'
CREATED BY SENDER
K1
FOR THE RECEIVER
K2
FOR THE TRUSTED
THIRD PARTY
K, K'
RECREATED BY RECEIVER

FIG. 4



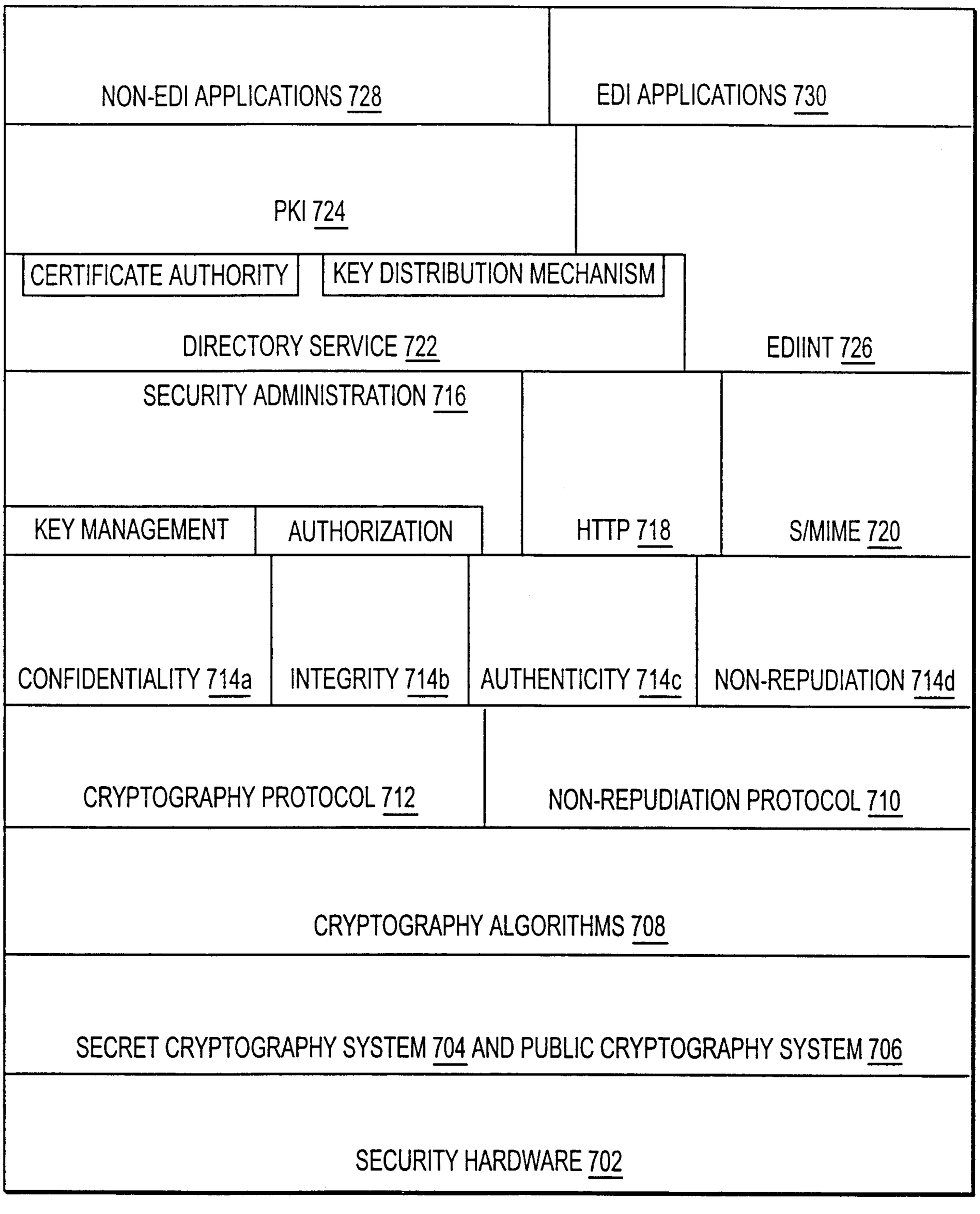
NON-REPUDIATION PROTOCOL 500

FIG. 5



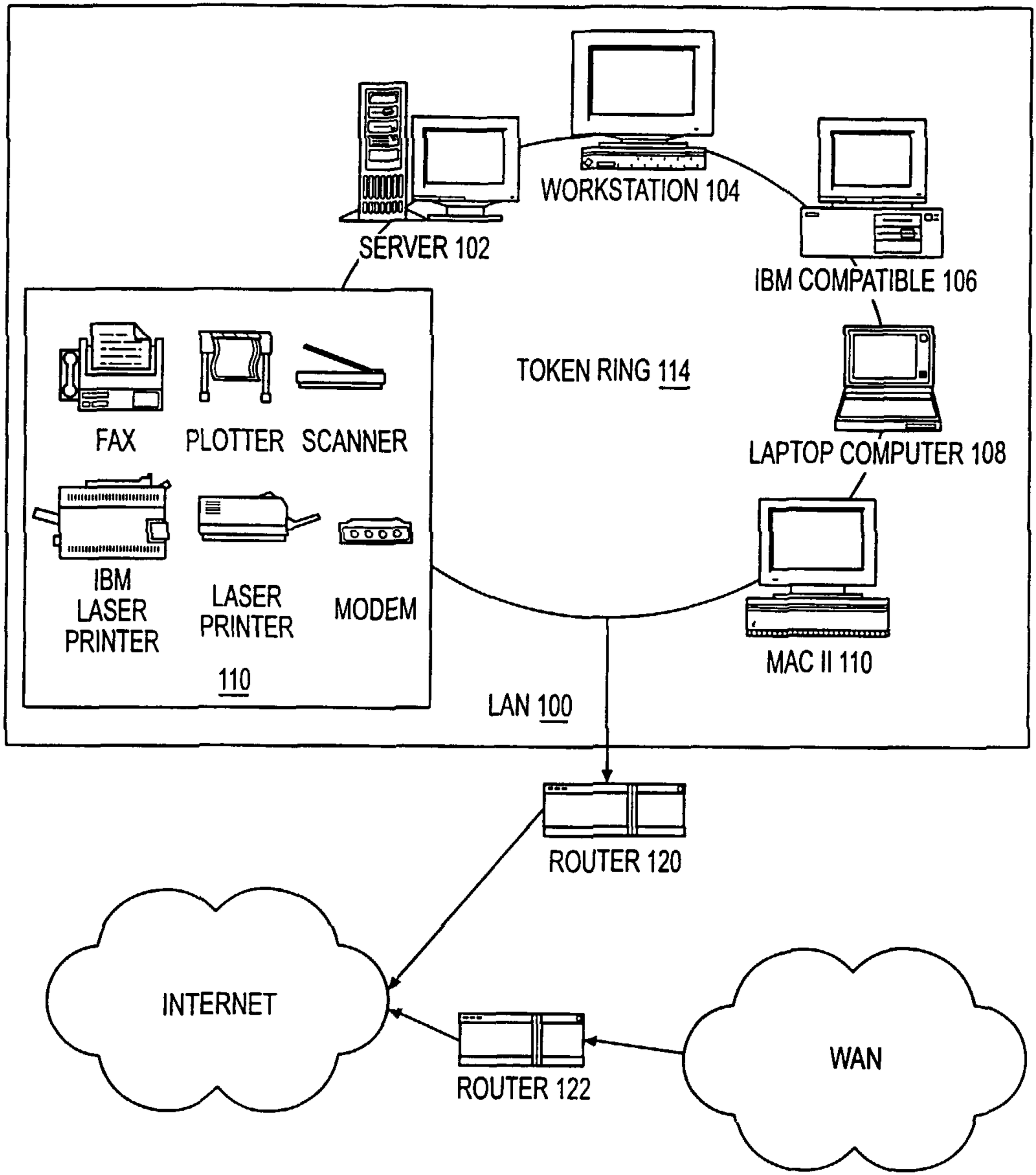
NON-REPUDIATION PROTOCOL 600

FIG. 6



SECURITY ARCHITECTURE 700

FIG. 7


SERVER 102
WORKSTATION 104
IBM COMPATIBLE 106
LAPTOP COMPUTER 108
MAC II 110
TOKEN RING 114
FAX
PLOTTER
SCANNER
IBM LASER PRINTER
LASER PRINTER
MODEM
110
LAN 100
ROUTER 120
ROUTER 122
INTERNET
WAN