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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 April 2006 (27.04.2006)

PCT

(10) International Publication Number
WO 2006/045102 A2

(51) International Patent Classification:
H04L 9/28 (2006.01)

(21) International Application Number:
PCT/US2005/038135

(22) International Filing Date: 20 October 2005 (20.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/620,889 20 October 2004 (20.10.2004) US

(71) Applicant *(for all designated States except US)*: **SEVEN NETWORKS, INC.** [US/US]; 901 Marshall Street, 1st floor, Redwood City, CA 94063 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **FIATAL, Trevor** [US/US]; 4550 Meyer Park Circle, Fremont, CA 94536 (US). **SUTARIA, Jay** [US/US]; 800 High School Way #231, Mountain View, CA 94041 (US). **NANJUNDESWARAN, Sridhar** [IN/US]; 415 Mountain Laurel Court, Mountain View, CA 94043 (US). **BAVADEKAR, Shailesh** [US/US]; 2945 Hancock Drive, Fremont, CA 94538 (US).

(74) Agents: **FORD, Stephen, S.** et al.; Marger Johnson & McCollom, P.C., 210 S.W. Morrison Street, Suite 400, Portland, OR 97204 (US).

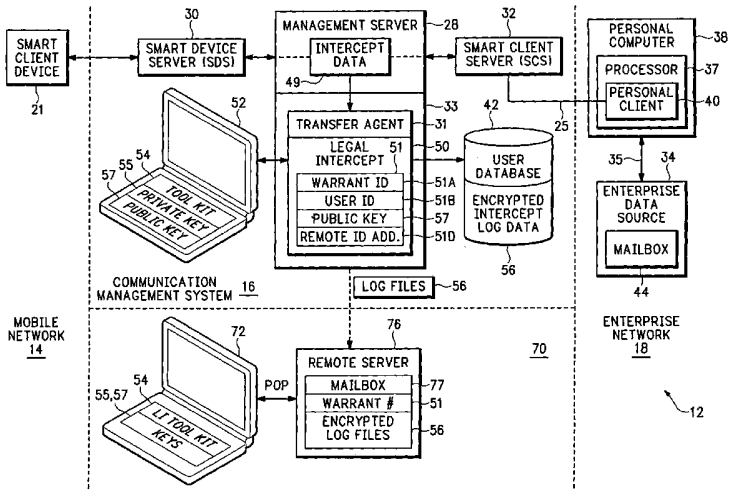
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

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

(54) **Title:** METHOD AND APPARATUS FOR INTERCEPTING EVENTS IN A COMMUNICATION SYSTEM



(57) **Abstract:** An intercept system provides more effective and more efficient compliance with legal intercept warrants. The intercept system can provide any combination of operations that include near-real-time intercept, capture of intercepted data in structured authenticated form, clear text intercept for communications where there is access to encryption keys, cipher text intercept for communications where there is no access to encryption keys, provision of transactional logs to the authorized agency, interception without altering the operation of the target services, and encryption of stored intercepted information.

WO 2006/045102 A2

METHOD AND APPARATUS FOR INTERCEPTING EVENTS IN A COMMUNICATION SYSTEM

Background

Wireless digital communication systems wirelessly transport electronic mail (email), text messages, text files, images, Voice Over Internet Protocol (VoIP) data, and any other types of digital data and communications to wireless devices. Wireless communication system providers are facing the prospects of having to comply with a variety of legal-intercept (wiretap) requirements. Authorization for a legal intercept may include warrants for "wiretap/interception", "search and seizure", or both. For example, the requirements outlined in CALEA (US Communications Assistance for Law Enforcement Act of 1994, http://www.askcalea.net/) may have to be met by any proposed solution. In another example, the requirements outlined by the Australian Communications Authority (http://www.aca.gov.au) in the Australia Telecommunications Act of 1997 may have to be met by any proposed solution.

There are several technical challenges complying with these legal intercept requirements that may not exist in conventional telephone systems. For example, the intercepted data may be encrypted. The wireless network provider must be able to intercept the encrypted data, and any other non-encrypted information, without tipping off the intercept target that the wiretap is taking place.

The wiretap warrant may require the communication system provider to provide any intercepted information in substantially real-time or may require the communication system provider to intercept and store communications in an automated manner for later retrieval and

analysis by the law enforcement agency. Evidentiary problems exist with information intercepted outside the presence and control of the enforcement agency. For example, the intercepted communications could be either intentionally or inadvertently deleted. A system malfunction could also prevent some communications from being intercepted. There is also the evidentiary issue of whether or not someone has tampered with the intercepted information. It may also be necessary to prevent technicians operating the communication system from accessing or viewing the intercepted information.

The invention addresses these and other problems with the present technology.

Summary of the Invention

An intercept system provides more effective and more efficient compliance with legal intercept warrants. The intercept system can provide any combination of operations that include near-real-time intercept, capture of intercepted data in structured authenticated form, clear text intercept for communications where there is access to encryption keys, cipher text intercept for communications where there is no access to encryption keys, provision of transactional logs to the authorized agency, interception without altering the operation of the target services, and encryption of stored intercepted information.

The foregoing and other objects, features and advantages of the invention will become more readily apparent from the following detailed description of a preferred embodiment of the invention which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a communication management system that operates a legal intercept system.

FIG. 2 is a diagram of an example log file generated for intercepted data.

FIG. 3 is a flow diagram showing in more detail how the log files in FIG. 2 are generated.

FIG. 4 is another block diagram showing how the legal intercept system operates with different types of encryption.

FIG. 5 is a diagram showing how intercepted data with different encryptions is converted into a log file.

FIG. 6 is a flow diagram showing in more detail how different types of encrypted data are formatted into a log file.

FIG. 7 is a diagram showing how a common transport is used for sending encrypted data.

FIG. 8 is a block diagram showing how an encryption schema in the communication management system is used in cooperation with the intercept system.

DETAILED DESCRIPTION

In the description below, an intercept event refers to an event where an agency issues a warrant requesting data interception for a targeted user. A targeted user is identified by a unique label, such as a username or account number, that corresponds to a user who is under intercept. A communication event, transaction, or intercept data is any message either sent or received by the targeted user. The intercept data can include synchronization messages, email data, calendars, contacts, tasks, notes, electronic documents, files or any other type of data passing through the communication management system.

Communication Management System

FIG. 1 shows an example of a communication network 12 that may operate similarly to the networks described in U.S. Patent Application, Ser. No. 10/339,368 entitled: CONNECTION ARCHITECTURE FOR A MOBILE NETWORK, filed January 8, 2003, and U.S. Patent Application Ser. No. 10/339,368 entitled: SECURE TRANSPORT FOR MOBILE COMMUNICATION NETWORK, filed January 8, 2003, which are both herein incorporated by reference.

The communication system 12 in one implementation is used for intercepting data pursuant to legal search warrants. For example, a law enforcement agency may require the operator of communication system 12 to intercept all messages sent to and from a mobile device 21. It should be understood that this is just one example of a communication system 12 and that the legal intercept system described in more detail below can operate with any communication network that is required to provide legal interception.

The communication system 12 includes a mobile network 14, an enterprise network 18, and a communication management system 16 that manages communications between the mobile network 14 and the enterprise network 18. The mobile network 14 includes mobile devices 21 that communicate with an IP infrastructure through a wireless or landline service provider. Since mobile networks 14 are well known, they are not described in further detail.

The enterprise network 18 can be any business network, individual user network, or local computer system that maintains local email or other data for one or more users. In the embodiment shown in FIG. 1, the enterprise network 18 includes an enterprise data source 34 that contains a user mailbox 44 accessible using a Personal Computer (PC) 38. In one example, the enterprise data source 34 may be a Microsoft® Exchange® server and the PC 38 may access the mailbox 44 through a Microsoft® Outlook® software application. The

mailbox 44 and data source 34 may contain emails, contact lists, calendars, tasks, notes, files, or any other type of data or electronic document.

The PC 38 is connected to the server 34 over a Local Area Network (LAN) 35. The PC 38 includes memory (not shown) for storing local files that may include personal email data as well as any other types of electronic documents. Personal client software 40 is executed by a processor 37 in the PC 38. The personal client 40 enables the mobile device 21 to access email, calendars, and contact information as well as local files in enterprise network 18 associated with PC 38.

The communication management system 16 includes one or more management servers 28 that each include a processor 33. The processor 33 operates a transfer agent 31 that manages the transactions between the mobile device 21 and the enterprise network 18. A user database 42 includes configuration information for different users of the mobile communication service. For example, the user database 42 may include login data for mobile device 21.

While referred to as a communication management system 16 and management server 28, this can be any intermediary system that includes one or more intermediary servers that operate between the mobile network 14 and the enterprise or private network 18. For example, a separate Smart Device Server (SDS) 30 may be used in management system 16 for handling communications with mobile devices in mobile network 14. Correspondingly, a SEVEN Connection Server (SCS) 32 may be used for handling communications with personal clients in enterprise networks 18.

Legal Interception

A Legal Intercept (LI) software module 50 is operated by the processor 33 and communicates with the transfer agent 31 in order to capture intercept data 49 associated with targeted user 51B. An operator sets up a configuration file 51 that is then used by the legal intercept module to automatically intercept communications for a particular target user and then format the intercepted communications into self authenticating log files.

An operator runs a toolkit utility 54 from a computer terminal 52 to configure the management server 28 for capturing intercept data 49. The toolkit utility 54 is used for creating and loading the configuration file 51 into memory in management server 28 and can also display detected intercept data 49. To initiate an intercept, an entry is loaded into the configuration file 51. To stop capturing intercept data 49, the system administrator deletes the entry or configuration file 51 from memory. Changes to the configuration file 51 of management server 28 may be automatically replicated to other management servers that are part of the communication management system 16. The toolkit utility 54 may have tightly controlled access that only allows operation by a user with an authorized login and password.

The toolkit 54 allows the operator to view, add, modify, and delete a warrant sequence number 51A, user identifier (ID) 51B, and encryption key 57 in the configuration file 51. The warrant identifier may be the actual sequence number for a wiretap or search warrant issued by a court of law and presented to the operator of communication management system 16 by a federal, state, or municipal government agency. The user ID 51B for example may be an identifier used by communication management system 16 to uniquely identify different mobile clients 21.

The public encryption key 57 may be the public key component of a public/private key pair, such as a Pretty Good Privacy (PGP) or GNU Privacy Guard (GPG) public key, for

encrypting the intercept data 49. In one embodiment, the legal intercept module 50 may not allow the management server 28 to start an interception process until a valid public key 57 is loaded into configuration file 51. This ensures that the intercepted data 49 can be immediately encrypted while being formatted into a log file 56. If this encryption fails for any reason, the legal intercept module 50 may shut down the intercept process ensuring that no intercept data 49 is stored in the clear.

The configuration file 51 may also include one or more entries defining a transport protocol, destination, and associated configuration values for the transmission of intercepted data via a network. In one embodiment, this could include a destination email address associated with a Simple Mail Transfer Protocol (SMTP) host and port number or other Internet Protocol (IP) destination address that is used by the legal intercept module 50 to automatically transmit the intercept data 49 to mail box 77 on a remote server 76 that is accessible by the agency issuing the warrant.

After the configuration file 51 is enabled, the legal intercept module 51 starts intercepting data 49 associated with the targeted user identified by user ID 51B. As mentioned above, this can include any emails, calendar information, contacts, tasks, notes, electronic documents, files or any other type of control or content data associated with user ID 51B. The intercepted data can include any type of communications such as email sent or received, calendar items sent or received, and other data sent/received by and from the targeted smart device 21. The captured intercept data 49 may then be encrypted using the encryption key 57 contained in the configuration file 51. The encrypted copy of the captured intercept data 49 may then be formatted and written to log file 56.

Data Delivery

The legal intercept module 50 running on each management server 28 may periodically poll the directory or location containing the encrypted intercept log files 56 for each user ID under intercept for the presence of new files or data. The poll period in one example is approximately every minute. Of course this is only one example and any user configurable time period can be used. New intercept data 49 which has been stored in one or more log files 56 and identified by the legal intercept module 50 during the polling process may be automatically reprocessed and/or transmitted according to the specification in configuration file 51. As an alternative to storing encrypted intercept data 49 in log file 56 on a file system, intercept data may be stored in database 42. Also, as shown in FIG. 4, the log file 56 may be stored in an alternative file system 53 located within the management server 28. The agency issuing the warrant can then access the data contained in log files 56 or database 42 in one of many different ways.

In one implementation, an official from the agency physically sits at terminal 52 at the location of communication management system 16. The agency official then reads the log files 56 in semi-real-time as the intercept events 49 are being detected in the management server 49. The agency official then uses terminal 52 to store or copy the log files 56 onto a portable storage medium, such as a Compact Disc (CD), memory stick, etc. In this implementation, the legal intercept log files 56 may not reside in user database 42 at all, or may only reside in database 42 for some relatively brief period of time while being transferred onto the portable storage media.

A copy of the log files may be stored onto the portable storage medium while the same log files remain in the communication management system 16. The copy of the log

files in the management system 16 could then be used, if necessary, for evidentiary purposes when admitting the copy under control of the agency official into evidence.

In an alternative implementation, the legal intercept module 50 may automatically send the log files 56 for the intercepted events to an email mailbox 77 operated in a remote server 76. The remote server 76 may be located in a wireless service provider network or may be located at the facilities of the enforcement agency issuing the warrant. In this implementation, a terminal 72 at the remote location 70 may include a toolkit utility 54 that has some of the same functionality as toolkit 54. The utility 54 only allows authorized users to decrypt and access the log files 56 received from communication management system 16.

For example, the toolkit utility 54 may include public and private PGP or GPG encryption keys 57 and 55, respectively, that are associated with the public encryption key 57 previously loaded into configuration file 51. Only personnel having authorized access to the toolkit 54 can decrypt and read the log files 56 previously generated and encrypted by legal intercept module 50. This provides additional privacy of the intercept data 49 from technical personnel of the communication management system 16 that may not be authorized to view the intercept data 49.

The intercept module 50 may transfer each captured log file 56 to a SMTP email server 76 via the Simple Mail Transfer Protocol (SMTP). The SMTP server 76 stores each log file 56 in an inbox of mailbox 77. The name of the mailbox 77 may be the same as the warrant sequence number @ the agency's domain name. For example, warrant123@LAPD.com. The warrant sequence number may correspond with the warrant identifier 51A in configuration file 51 and the domain name may correspond with the IP address 51D in configuration file 51. Once transmitted and accepted by the SMTP email server 76, the log file 56 may be automatically deleted from user database 42.

The agency issuing the warrant can retrieve the captured log files 56 in remote server 76 for a particular user ID under interception using for example the Post Office Protocol (POPv3). The agency is given the name of email server 76, POP and SMTP port numbers, the mailbox id (warrant sequence number 51) and a password to access the mailbox 77. The agency then retrieves log files 56 in mailbox 77 using POP. Once a file is downloaded from the mailbox 77 to an agency terminal 72, the log file 56 may be automatically deleted from the mailbox 77.

Log Files

Referring to FIGS. 1 and 2, the legal intercept software 50 generates log files 56 in a structured manner that provides more secure and reliable data authentication. In this example, an intercept directory 60 is loaded with log files 56 generated to account for every minute of a particular time period, such as an entire day. The legal intercept 50 may generate a name for directory 60 that identifies the contents as legal intercepts, for a particular user ID and for a particular day. Of course this is just one naming convention that can be used to more efficiently organize log files.

The log files 56 stored in directory 60 may indicate the number of events intercepted for the targeted device during each minute. For example, a first log file 56A is identified by the following log file name: fe0-2005/09/23-00:00.ASC, containing a single line that reads as follows: "0 events logged in the last minute". This indicates that a management server fe0 on September 23rd, 2005, at 12:00 midnight logged zero intercept events for a particular user ID during the specified time period. A second log file 56B is named to identify a next minute of the intercept period and indicates that between 12:00 A.M and 12:01 A.M, on the same day, no intercept events were logged.

The first detected intercept events for this particular user ID for this particular day were detected in log file 56C identified by the log file name: fe0- 2005/09/23-00:02.ASC, the first and/or last line of which reads "3 events logged in the last minute". Log file 56C indicates that 3 intercept events were detected on September 23rd, 2005, between 12:01 A.M. and 12:02 A.M. The legal intercept 50 generates this contiguous set of log files 56 that cover each minute or other configured interval of the intercept period.

The legal intercept 50 may also load a first entry into the log file directory 60 that lists the warrant id 51A, PGP key 57, etc. The legal intercept 50 may also generate a log file 56 that indicates any management server status-change events. For example, if the management server 28 conducts a graceful shutdown, a log file 56 may be generated that indicates when the shut down occurred and possibly the cause of the shutdown.

This highly structured log file format provides the agency official a quick indicator of when intercept events are detected for a particular target user. Further, as shown above, the log files are created contiguously for predetermined time periods over a particular intercept period even when no intercept events are detected. This provides further verification that the legal intercept 50 was actually in operation and continuously monitoring for intercept events during the intercept period.

As described above, the log files 56 may be stored into a portable storage media that can be transported by an agency official. Alternatively, the log files 56 may be stored in the user database 42 in the communication management system 16 for later retrieval by the agency official via toolkit 54. In another implementation, the log files 56 may be sent to the mailbox 77 in a server 76 in a mobile operator infrastructure which is accessible by the agency official.

FIG. 3 explains in further detail how the legal intercept module 50 might generate the log files. In operation 61, communications are monitored for a particular targeted user for predetermined time periods over an intercept period. In one example as described above, the predetermined time period may be one minute. Of course, time periods of less than one minute or more than one minute may also be used. The duration of these time periods may also be configurable by setting a parameter in configuration file 51. If no intercept events are detected during the predetermined time period in operation 62, an empty log file is generated for that time period in operation 63.

When intercept events are detected, all the intercepted data for that time period is formatted into a same log file 56 in operation 64. The log file is encrypted in operation 65 using the encryption key 57 (FIG. 1) loaded by the toolkit 54 into configuration file 51. All of the encrypted log files 56 associated with a particular targeted user for a particular intercept period are stored in a same intercept directory 60 (FIG. 2). For example, all log files generated for a particular user ID for a same day are stored in the same intercept directory. If the current day of legal interception is not completed in operation 66, further monitoring and interception is performed in operation 61.

When interception for a current interception period is completed, a Cyclic Redundancy Check (CRC) value, or some other type of digital certificate/signature, may be generated in operation 67. The CRC can be used to verify that the contents of intercept directory 60 have not been tampered with or deleted after their initial generation. The CRC may be encrypted in operation 68 and then separately emailed to the agency or separately stored for later validation. As discussed above, the encrypted log files may then either be emailed to a mailbox or stored locally for later retrieval by the enforcement agency.

Thus, the individual log file encryption in operation 65 ensures the authenticity of intercepted events for a particular time period and the CRC generated in operation 67 ensures that none of the individual log files have been removed or replaced.

Encrypted Intercept Data

Referring to FIG. 4, as described above, the log files 56 may be stored in database 42 or in a file system 53 within the management server 28. A single or multi-tiered encryption scheme may be used in network 12. For example, the personal client 40 may make an outbound connection 25 to the management server 28. The personal client 40 registers the presence of a particular user to the management server 28 and negotiates a security association specifying a cryptographic ciphersuite (including encryption cipher, key length, and digital signature algorithm) and a unique, secret point-to-point encryption key 29 over connection 25. In one example, the key 29 is an Advanced Encryption Standard (AES) key. Of course, encryption ciphers other than AES can also be used. The encryption key 29 enables secure communication between management server 28 and PC 38 over connection 25.

The mobile device 21 also negotiates a point-to-point security association, specifying a cryptographic ciphersuite and a unique encryption key 27, with the management server 28. In one example, the point-to-point encryption key 27 is also an AES encryption key. The negotiated security association that includes encryption key 27 enables secure point-to-point communication between the mobile device 21 and the management server 28 over connection 23. Each different mobile device 21 negotiates a different security association that includes a unique encryption key 27 with the management server 28.

The point-to-point encryption key 27 may be used for encrypting control data that needs to be transferred between the mobile device 21 and management server 28. The point-to-point encryption key 29 may be used for encrypting control data that needs to be transferred between the management server 28 and personal client 40. For example, the control data may include login information and transaction routing information.

An end-to-end security association, specifying a cryptographic ciphersuite and a unique encryption key 46, is negotiated between the mobile device 21 and the personal client 40. In one example, the end-to-end encryption key 46 is also an AES encryption key. The end-to-end encryption key 46 in one example is used for encrypting transaction payloads transferred between personal client 40 and mobile device 21. For example, the end-to-end encryption key 46 may be used for encrypting the content of emails, files, file path names, contacts, notes, calendars, electronic documents and any other type of data transferred between mobile device and the PC. The end-to-end encryption key 46 is only known by the mobile device 21 and the personal client 40. Data encrypted using the end-to-end key 46 cannot be decrypted by the management server 28.

Referring to FIGS. 4 and 5, the legal intercept module 50 can produce log files 56 from intercept data 49 that have any combination of unencrypted data 49A sent in the clear, point-to-point encrypted data 49B encrypted using the point-to-point encryption keys 27 or 29, and end-to-end encrypted data 49C encrypted using the end-to-end encryption key 46.

The communication management system 16 has access to the point-to-point encryption keys 27 and 29 used for encrypting the point-to-point encrypted information 49B. Therefore, the management system 16 can automatically decrypt the point-to-point encrypted information 49B before it is reformatted into log file 56.

The end-to-end encryption keys 46 are only shared between the endpoints 21 and 38 and are unknown to the communication management system 16. Therefore, the agency issuing the warrant may be required to extract the end-to-end encryption keys 46 either at the mobile device 21 or at the enterprise server 34 or personal computer 38. The end-to-end encrypted information 49C may then be decrypted at a later time separately from the point-to-point encrypted information 49B.

For example, after receiving and decrypting the log file 56, the enforcement agency may then independently conduct a seizure of the end-to-end encryption key 46 from either the enterprise network 18 or the mobile device 21. The enforcement agency could then separately decrypt information 56B in log file 56 with the seized end-to-end encryption key 46.

FIG. 6 explains in more detail how the legal intercept module 50 handles the decryption and reformatting of intercept data into log files. In operation 80, the management server 28 is configured to conduct a legal intercept for a particular user ID as described above in FIG. 1. Accordingly, the management server 28 begins intercepting data for the identified user ID in operation 82.

In operation 84, any point-to-point encrypted portion 49B of the intercepted data 49 (FIG. 5) is decrypted. In operation 86, the decrypted point-to-point data is combined with any information 49A in the intercept data 49 received in the clear. The unencrypted data is then formatted into an unencrypted portion 56A of the log file 56 in FIG. 5. Any end-to-end encrypted data 49C is then combined in the same log file 56 as section 56B in operation 88. The log file 56 is then possibly encrypted in operation 90 and then either stored in a local database or automatically sent to a remote server.

Detecting Different Types of Intercept Data

FIGS. 7 and 8 explain in more detail how a particular data format used by the communication system 12 can be used to identify point-to-point and end-to-end encrypted intercept data. FIG. 7 shows how encryption can be performed differently for different types of data or for data associated with different destinations. Intercept data 102 includes content data 108 such as the contents of an email message, an electronic document, or any other type of information that should only be accessed by two endpoints. The content data 108 in this example is encrypted using an end-to-end encryption key.

A second portion 106 of intercept data 102 may include control information that only needs to be processed by one particular server. In this case, control data 106 may be encrypted using a first point-to-point encryption key. A third portion 104 of intercept data 102 may have other control information, for example, error checking data, that needs to be processed by a different server. Accordingly, the error checking data 104 is encrypted using a second point-to-point encryption key different than either of the other two encryption keys used for encrypting data 108 and 106.

FIG. 8 shows in more detail an encryption schema 112 is used by the mobile device 21, management server 28, and personal client 40 when processing transactions between a source and a target device. In the example below, the mobile device 21 is operating as a source for sending a transaction 110. The transaction 110 requests personal client 40 to send a document 114 located in a personal directory in local memory 116 of PC 38. The personal client 40 operates as a target for the transaction 110 and the management server 28 operates as the transfer agent for transferring the transaction 110 from the mobile device 21 to the personal client 40.

It should be understood that this is only an example, and the devices shown in FIG. 8 can process many different types of transactions. For example, the transaction 110 may request synchronization of emails in the PC 38 with emails in the mobile device 21. Further, any device can operate as a source or target for the transaction. For example, the personal client 40 operates as a source and the mobile device 21 operates as a target when a transaction 111 is sent as a reply to request 110.

The mobile device 21, management server 28, and the personal client 40 are all configured with an encryption schema 112 that identifies how specific items in the transaction 110 are to be encrypted. Each device is also configured with different security associations as described above in FIG. 4. For example, the mobile device 21 has both Point-to-Point (PP) key 27 and End-to-End (EE) key 46. Management server 28 has PP key 27 and PP key 29, and the PC 38 has PP key 29 and EE key 46.

The mobile device 21 forms the request transaction 110. One example of a request is as follows.

```
Request:    {auth_token = "abc",
             device_id = "xyz",
             method_id = "GetDocument",
             args = {path = "/docs"}
             }
```

Mobile device 21 attaches an auth_token to transactions sent to the management server 28. For example, the mobile device 21 may be required to authenticate to the management server 28 by transmitting a username and password prior to being permitted to submit other transactions for processing. The management server 28 issues the mobile device 21 an auth_token after successfully validating the username and password against information in the user database 42. The mobile device 21 then attaches the auth_token to subsequent transactions sent to the management server 28. The management server 28 uses

the auth_token to identify and authenticate the source of each transaction and to determine where to route the transaction.

The device_id identifies the particular mobile device 21 sending the request 110. The device_id may be necessary, for example, when a user has more than one mobile device. The personal client 40 can use different device_id values to track when synchronization information was last sent to each of multiple different mobile devices. The device_id can also be used by either the management server 28 or the personal client 40 to determine how to format data sent to particular types of mobile devices 21. For example, data may need to be formatted differently for a cell phone as opposed to a personal computer. The device_id can also be used to correlate a known security association with a particular mobile device.

The method_id item in the example identifies a particular function GetDocument associated with request 110. The method_id item also requires the inclusion of related argument items that identify the parameters for the GetDocument function. For example, the argument items might include the expression path="/docs" identifying the pathname where the requested documents are located.

In order to prepare the request 110 for transmission, the mobile device 21 performs a pattern match of the request 110 using the encryption schema 112. This pattern match separates the items in request 110 into different channels. One example of the different channels is shown below. In this example, the items in each channel are associated with predefined security associations: clear, pp, and ee.

```
Channels:
        {clear = { device_id = "xyz"}
        pp = {auth_token = "abc", method_id = "GetDocument"}
        ee = {args = {path = {path = "/docs"}}}
        }
```

The channel contents are encoded (via a process commonly known as serialization) into arrays of bits or bytes referred to as data groups. These groupings of bits or bytes are referred to generally below as arrays, but can be any type of partition, group, etc.

The contents of the clear channel are encoded into an array of bits referred to as data_group_1, the contents of the pp channel are encoded into an array of bits referred to as data_group_2, and the contents of the ee channel are encoded into an array of bits referred to as data_group_3. The contents of each channel need to be encoded into bit arrays so that they can be encrypted. The contents of the channels after being encoded into bit arrays are represented as follows.

Encoded
Channels: {clear = data_group_1
pp = data_group_2
ee = data_group_3}

The bit arrays are then encrypted according to the security association parameters for each channel. According to the encryption schema 112, bits in the clear channel (data_group_1) are not encrypted. The bits in the pp channel data_group_2 are encrypted using the point-to-point security association between mobile device 21 and management server 28, using PP key 27, and are referred to after encryption as pp_data_group_2. The bits in the ee channel data_group_3 are encrypted using the end-to-end security association between mobile device 21 and personal client 40, using EE key 46, and are referred to after encryption as ee_data_group_3. The data groups are represented as follows after encryption:

Encrypted
Channels: {clear = data_group_1
pp = pp_data_group_2
ee = ee_data_group_3}

The bits making up the encrypted and unencrypted channels are then encoded into one or more packets. For clarity, the description below will refer to a single packet, however, the data from the channels may be contained in multiple packets. Some of the contents of the packet are shown below.

Packet:

Header	length
	version
	flags
Payload	count = 3
	"clear"
	data_group_1
	"pp"
	pp_data_group_2
	"ee"
	ee_data_group_3

Information in the packet header may include the packet length, a version number, and other flags. The packet payload includes a count identifying 3 pairs of items. The three items include the non-encrypted contents in the clear channel, the pp encrypted contents of the pp channel, and the ee encrypted contents of the ee channel. The packet is then transported by mobile device 21 to the management server 28.

The transfer agent operating in server 28 receives the packet. The bits in the packet are separated into the different channels clear = data_group_1, pp=pp_data_group_2, and ee = ee_data_group_3.

The data in the clear channel does not need to be decrypted. The transfer agent decrypts the only bits in channels for which it has a known security association. The transfer

agent, as a member of the point-to-point security association between mobile device 21 and management server 28, possesses the PP key 27 and therefore decrypts the contents of the pp channel. The transfer agent is not a member of the end-to-end security association between mobile device 21 and personal client 40, does not have the EE key 46 and therefore does not decrypt the data in the ee channel. Decryption produces the following data groups: clear = data_group_1, pp = data_group_2, and ee = ee_data_group_3.

The transfer agent decodes the contents of the clear and pp channels. The contents of the encrypted ee channel are not decoded, but instead are maintained in an unmodified state for eventual transport to the personal client 40. Decoding produces the following contents.

```
Decoded
Channels:    {clear = {device_id = "xyz"}
             pp = {auth_token = "abc", method_id = "GetDocument"}
             ee=ee_data_group_3
             }
```

A partial request is formed by merging the items of the clear and pp channels. The partial request in this example could look similar to the following:

```
Partial Request:    {auth_token = "abc",
                    device_id = "xyz",
                    method_id = "GetDocument",
                    args = { }
                    encrypted = {ee=ee_data_group_3}
                    }
```

The transfer agent 31 in the management server 28 processes the partial request. In this example, the transfer agent may verify the request is authorized by matching the value of auth_token ("abc") with contents in the user database 42 (FIG. 8). The auth_token and the

method_id ("GetDocument") indicate that the transaction 110 is a document request directed to the personal client 40.

The transfer agent may identify a user_id = "joe" associated with the auth_token = "abc" and generate the following new request.

```
New Request:    {user_id = "joe",
                device_id = "xyz",
                method_id = "GetDocument",
                args = { }
                encrypted = {ee=ee_data_group_3}
                }
```

The legal intercept 50 in FIG. 1 may come into play at this point, or earlier in the encryption schema 112. For example, the legal intercept 50 checks the user_id in the request with the user id 51B in the intercept configuration file 51. In this example, if "joe" matches the user_id 51B in configuration file 51, then the contents in the request are formatted into a log file 56 as described above. As can be seen, at this point the new request has already decrypted the auth_token = "abc" and method_id = "GetDocument". Further, the device_id = "xyz" was received in the clear. The legal intercept 50 simply has to format these different channels into a log file.

The end-to-end encrypted data in group 3 remains encrypted and therefore may not provide all of the information desired for the enforcement agency. However, the decrypted information does provide enough information to adequately indicate that the intercepted data is associated with a particular user_id. The intercepted unencrypted data may also provide further evidence that the enforcement agency can then use to obtain another warrant to seize the ee encryption key from the targeted user.

As described above in FIG. 2, the legal intercept 50 may then attach appropriate time/date stamp headers to this raw data frame to authenticate the time and date when the data was intercepted.

End-to-End Encrypted Data

As described above, the communication management system 16 may not have access to the end-to-end encryption keys 46 (FIG 2). However, as shown in FIG. 8, the management server 28 is still capable of identifying data streams belonging to users targeted for interception, as this identifying information is required for routing the datagrams shown above. Thus, the legal intercept module 50 can still intercept data that cannot be immediately decrypted.

The intercept logs 56 can therefore contain data encrypted using encryption keys known only to the endpoints. For example, a mobile device 21 and a desktop connector running on personal computer 38 (FIG. 1). The toolkit 54 in FIG. 1 can facilitate the recovery of the end-to-end keys 46.

In order to make use of this functionality, the enforcement agency seeking the information may need to obtain both an intercept warrant, and either a search-and-seizure warrant authorizing the extraction of the configuration data from the smart device client in the mobile device 21 or a search-and-seizure warrant authorizing the extraction of the end-to-end encryption key from the desktop connector in the PC 38 (FIG. 1).

After the authorized agency has executed the necessary warrants, the toolkit 54 is used by the agency to facilitate the recovery of the end-to-end key 46. The toolkit utility 54 then uses the end-to-end key 46 to decrypt the end-to-end encrypted information in the log files 56.

The system described above can use dedicated processor systems, micro controllers, programmable logic devices, or microprocessors that perform some or all of the operations. Some of the operations described above may be implemented in software and other operations may be implemented in hardware.

For the sake of convenience, the operations are described as various interconnected functional blocks or distinct software modules. This is not necessary, however, and there may be cases where these functional blocks or modules are equivalently aggregated into a single logic device, program or operation with unclear boundaries. In any event, the functional blocks and software modules or features of the flexible interface can be implemented by themselves, or in combination with other operations in either hardware or software.

Having described and illustrated the principles of the invention in a preferred embodiment thereof, it should be apparent that the invention may be modified in arrangement and detail without departing from such principles. Claim is made to all modifications and variation coming within the spirit and scope of the following claims.

Claims

1. A communication management device, comprising:

a processor configured to operate as a legal intercept for intercepting data associated with a target user pursuant to a legal warrant.

2. The device according to claim 1 wherein the processor is configured to intercept the data according to an intercept configuration file that includes, but is not limited to, a unique intercept identifier and a user ID identifying the target user subject to a legal intercept operation.

3. The device according to claim 1 wherein the processor is configured to automatically format the intercepted data into log files.

4. The device according to claim 3 wherein the processor automatically sends the log files to a remote server accessible by an enforcement agency issuing the legal warrant.

5. The device according to claim 3 wherein the processor generates multiple log files that identify any intercepted data for associated contiguous predetermined time periods extending over a continuous intercept period.

6. The device according to claim 5 wherein the processor generates the individual log files for back-to-back time periods that each either contain intercepted data for the associated time period or indicate that no data was intercepted during the associated time period.

7. The device according to claim 3 wherein the processor is configured to derive one or more digital signatures for the log files in the intercept directory.

8. The device according to claim 3 wherein the processor is configured to encrypt the log files according to an encryption key known by an enforcement agency issuing the warrant.

9. The device according to claim 1 wherein the processor is configured to identify a first portion of the intercepted data encrypted using a first known security association for which the processor has knowledge of the encryption key and identify a second portion of the intercepted data encrypted using a second unknown security association, the processor decrypting and storing the first portion of the intercepted data into a log file and combining the encrypted second portion of the intercepted data with the decrypted first portion of the intercepted data in the same log file.

10. The device according to claim 9 wherein the first portion of the intercepted data is encrypted with a known point-to-point encryption key and the second portion of the intercepted data is encrypted with an unknown end-to-end encryption key.

11. The device according to claim 10 wherein the processor is configured to encrypt both the decrypted first portion of the intercepted data and the second encrypted portion of the intercepted data.

12. The device according to claim 9 wherein the first portion of the intercepted data includes transaction authentication and routing information and the second portion of the intercepted data includes the contents of email messages, electronic files, or other electronic data.

13. The device according to claim 1 wherein the processor operates in a management server that manages communications between a local device operating in an enterprise or local network and a mobile wireless device that synchronizes with a portion of the data in the local device.

14. A method for intercepting data, comprising:

receiving a warrant identifier for a warrant authorizing a legal intercept;

receiving a user identifier identifying an intercept target for the legal intercept associated with the warrant; and

automatically intercepting data received and/or sent by the intercept target identified by the user identifier.

15. The method according to claim 14 wherein the intercept target is a mobile device and the intercept data are messages that update email information between the mobile device and a corresponding local device operating in an enterprise or local network.

16. The method according to claim 14 including:

identifying a first portion of the intercepted data encrypted using a first known security association;

identifying a second portion of the intercepted data encrypted using a second unknown security association;

decrypting the first portion of the intercepted data and formatting the decrypted first portion of the intercepted data into a log file; and

combining the encrypted second portion of the intercepted data with the decrypted first portion of the intercepted data in the same log file.

17. The method according to claim 14 including:

managing the transfer of contents between a computer operating in an enterprise or network and a mobile device associated with the intercept target;

receiving authorization via the warrant identifier and user identifier to intercept communications between the computer and/or mobile device;

automatically intercepting data transferred between the computer and the mobile device pursuant to the warrant identifier and the user identifier; and

storing the intercepted data in a structure format that identifies when data was intercepted and at the same time provides authentication that the stored intercepted data has not been altered or deleted.

18. The method according to claim 17 including monitoring communications between the computer and the mobile device for multiple contiguous time periods.

19. The method according to claim 18 including:

generating the log files over an intercept period that encompasses multiple contiguous time periods;

storing the log files in a same intercept directory;

inserting the warrant identifier into the intercept directory; and

generating a name for the intercept directory that identifies the intercept target and the intercept period over which the log files were generated.

20. The method according to claim 19 including:

encrypting the log files in the intercept directory with an encryption scheme known by an agency issuing the warrant; and

sending the encrypted intercept directory to an electronic mailbox accessible by the agency.

21. The method according to claim 20 including:

generating a Cyclic Redundancy Check (CRC) or other digital signature value for all of the log files in the intercept directory;

encrypting the resulting generated value; and

providing the encrypted generated value to the enforcement agency separately from the encrypted intercept directory to verify that the log files have not been altered.

22. The method according to claim 14 including:

reading an intercept configuration file that contains the warrant identifier, the user identifier, an enforcement agency known encryption key and an electronic mailbox address;

upon reading the intercept configuration file automatically intercepting data received and/or sent by a device corresponding with the user identifier;

formatting any intercepted data into log files that identify when the data was intercepted; and

encrypting the log files using the encryption key.

23. The method according to claim 14 including:

identifying a first portion of the intercepted data encrypted with a known encryption key;

decrypting the first portion of the intercepted data using the known encryption key;

storing the decrypted first portion of the intercepted data in a log file;

identifying a second portion of the intercepted data encrypted with an unknown encryption key; and

combining the decrypted first portion of the intercepted data with the encrypted second portion of the intercepted data in the same log file.

24. A communication management system, comprising:

a management server used for managing communications between a computer in an enterprise or local network and a mobile device;

the management server configurable to operate as an interception device for intercepting the communications between the computer and the mobile device pursuant to a warrant from an enforcement agency.

25. The communication management system according to claim 24 including a software utility operating on a terminal that configures the management server for intercepting the communications between the computer and the mobile device.

26. The communication management system according to claim 25 wherein the software utility modifies a configuration file in the management server to include a warrant identifier and a user identifier for a targeted mobile device for the intercepted communications.

27. The communication system according to claim 26 wherein the software utility is configured to access end-to-end encryption keys located in either the target computer or the mobile device pursuant to a legal seizure warrant.

28. The communication system according to claim 25 wherein the software utility contains an encryption key used for decrypting log files generated by the management server that contain encrypted intercepted communications between the computer and the mobile device.

29. A communication management system, comprising:

a processor configured to operate as a legal intercept for intercepting data associated with a target user pursuant to a legal warrant,

the processor configured to identify a first unencrypted portion of the intercepted data and identify a second encrypted portion of the intercepted data encrypted using an unknown security association, and

the processor further configured to store the first portion of the intercepted data into a log file and combine the encrypted second portion of the intercepted data with the first portion of the intercepted data in the same log file.

30. The system according to claim 29 wherein the second portion of the intercepted data is encrypted with an unknown end-to-end encryption key.

31. The system according to claim 30 wherein the processor is configured to encrypt the first and second portion of the intercepted data stored in the log file.

32. The system according to claim 29 wherein the first portion of the intercepted data includes transaction authentication and routing information and the second portion of the intercepted data includes the contents of email messages, electronic files, or other electronic data.

33. The system according to claim 29 wherein the processor is configured to identify a third portion of the intercepted data encrypted using a known security association, decrypt the third portion of the intercepted data, and combine the decrypted third portion of the intercepted data with the first and second portion of the data in the same log file.

34. The system according to claim 33 wherein the processor is configured to encrypt the first, second and third portion of the intercepted data before being stored in the log file.

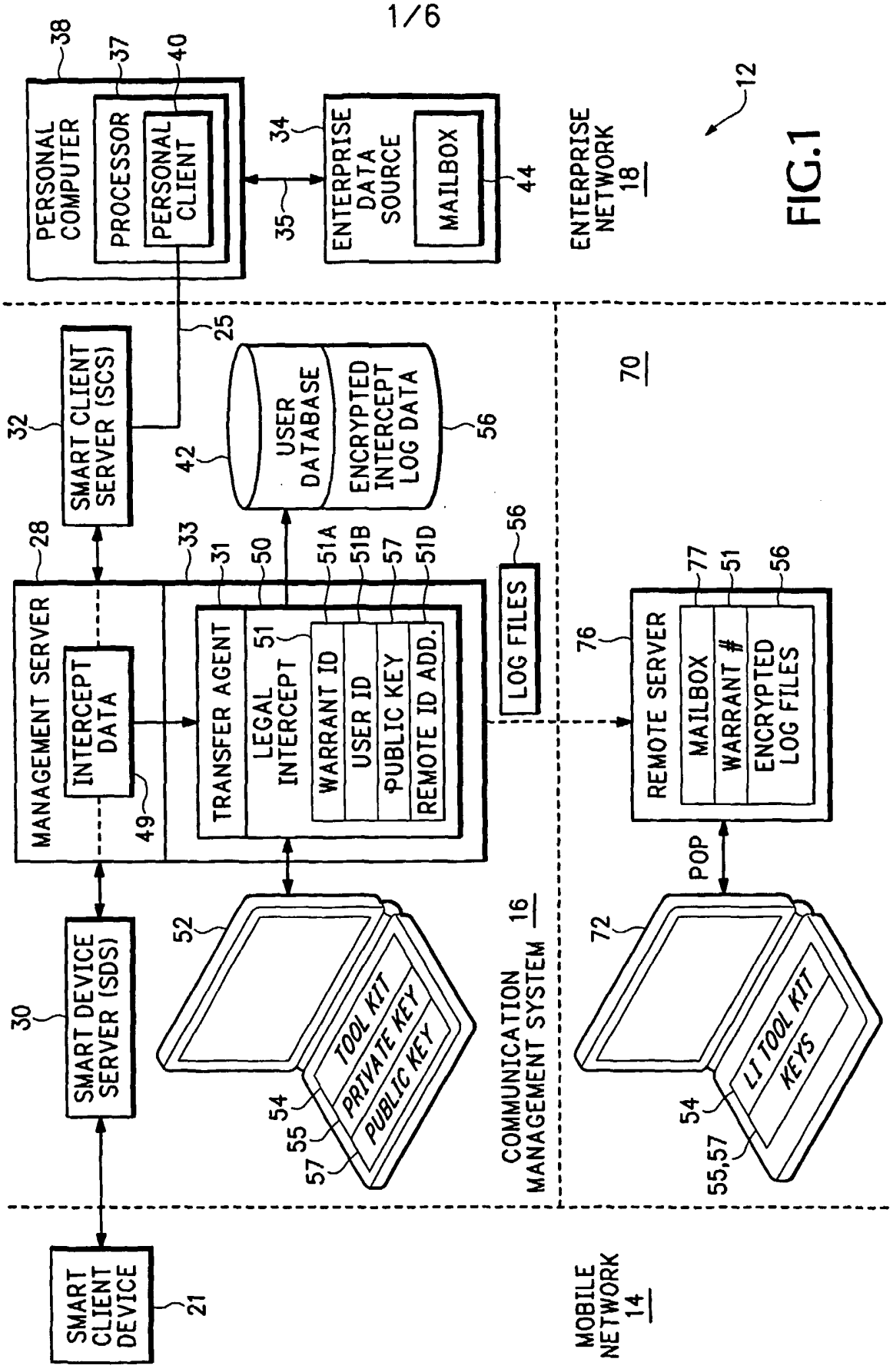

PERSONAL COMPUTER
38
PROCESSOR
37
PERSONAL CLIENT
40
34
35
ENTERPRISE DATA SOURCE
MAILBOX
44
ENTERPRISE NETWORK 18
12
25
SMART CLIENT SERVER (SCS)
32
USER DATABASE
42
ENCRYPTED INTERCEPT LOG DATA
56
70
28
MANAGEMENT SERVER
INTERCEPT DATA
49
33
31
50
TRANSFER AGENT
51
LEGAL INTERCEPT
WARRANT ID
USER ID
PUBLIC KEY
REMOTE ID ADD.
51A
51B
57
51D
LOG FILES
56
76
REMOTE SERVER
77
51
MAILBOX
WARRANT #
ENCRYPTED LOG FILES
56
POP
SMART DEVICE SERVER (SDS)
30
52
TOOL KIT
PRIVATE KEY
PUBLIC KEY
54
55
57
COMMUNICATION MANAGEMENT SYSTEM 16
72
LI TOOL KIT
KEYS
54
55,57
SMART CLIENT DEVICE
21
MOBILE NETWORK 14

FIG.1

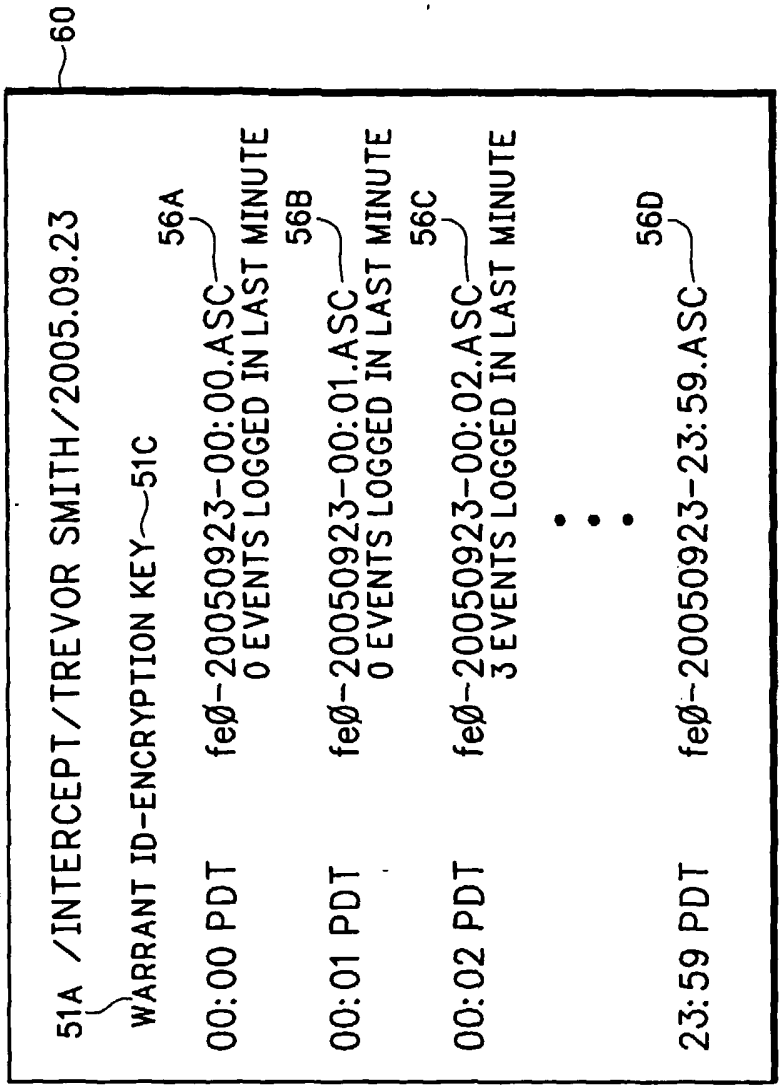

60
LEGAL INTERCEPT LOG FILE DIRECTORY
51A /INTERCEPT/TREVOR SMITH/2005.09.23
WARRANT ID-ENCRYPTION KEY
51C
00:00 PDT
fe0-20050923-00:00.ASC
56A
0 EVENTS LOGGED IN LAST MINUTE
00:01 PDT
fe0-20050923-00:01.ASC
56B
0 EVENTS LOGGED IN LAST MINUTE
00:02 PDT
fe0-20050923-00:02.ASC
56C
3 EVENTS LOGGED IN LAST MINUTE
23:59 PDT
fe0-20050923-23:59.ASC
56D

FIG.2

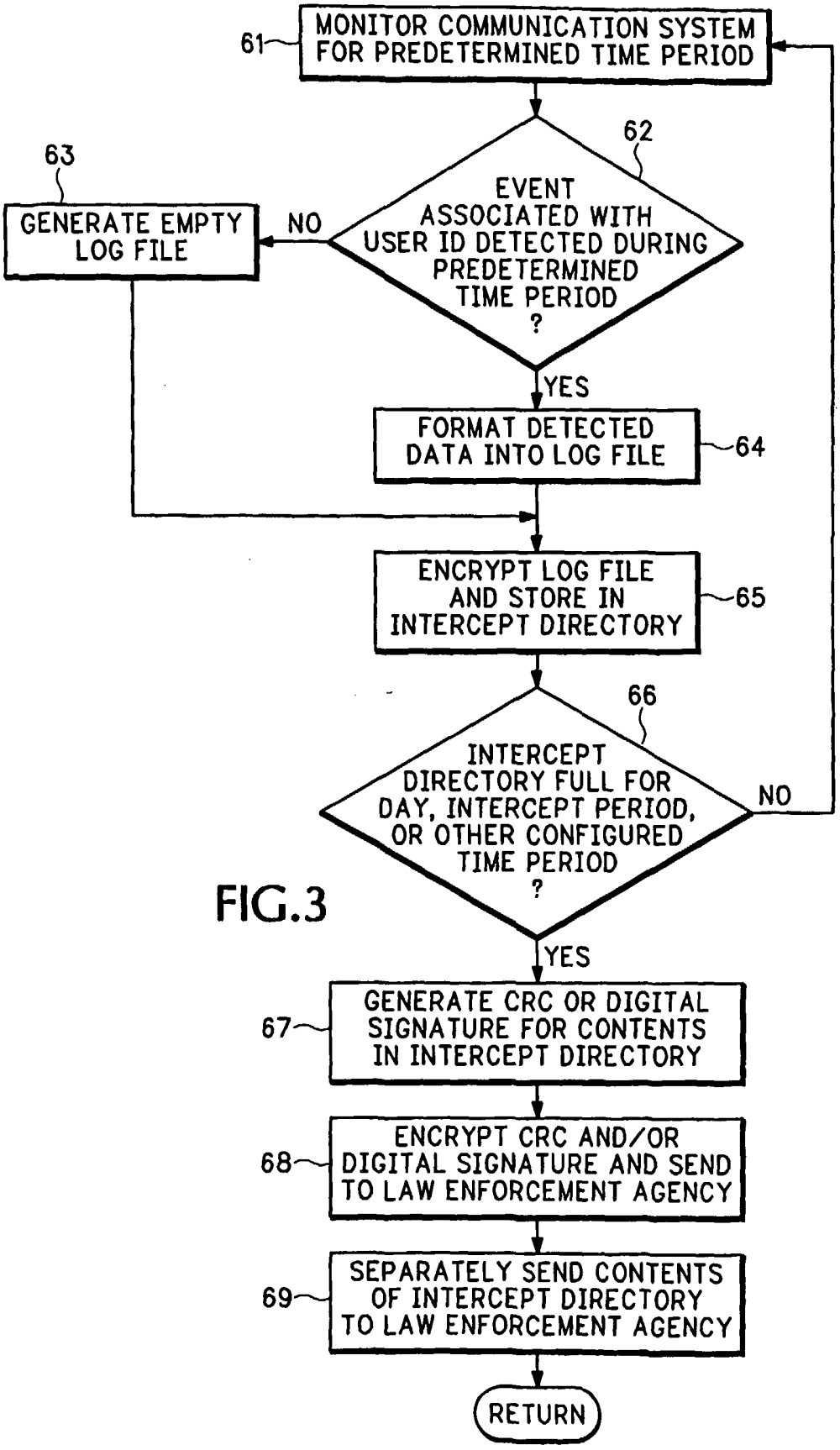

61
MONITOR COMMUNICATION SYSTEM FOR PREDETERMINED TIME PERIOD
62
EVENT ASSOCIATED WITH USER ID DETECTED DURING PREDETERMINED TIME PERIOD ?
NO
63
GENERATE EMPTY LOG FILE
YES
FORMAT DETECTED DATA INTO LOG FILE
64
ENCRYPT LOG FILE AND STORE IN INTERCEPT DIRECTORY
65
66
INTERCEPT DIRECTORY FULL FOR DAY, INTERCEPT PERIOD, OR OTHER CONFIGURED TIME PERIOD ?
NO
YES
67
GENERATE CRC OR DIGITAL SIGNATURE FOR CONTENTS IN INTERCEPT DIRECTORY
68
ENCRYPT CRC AND/OR DIGITAL SIGNATURE AND SEND TO LAW ENFORCEMENT AGENCY
69
SEPARATELY SEND CONTENTS OF INTERCEPT DIRECTORY TO LAW ENFORCEMENT AGENCY
RETURN

FIG.3

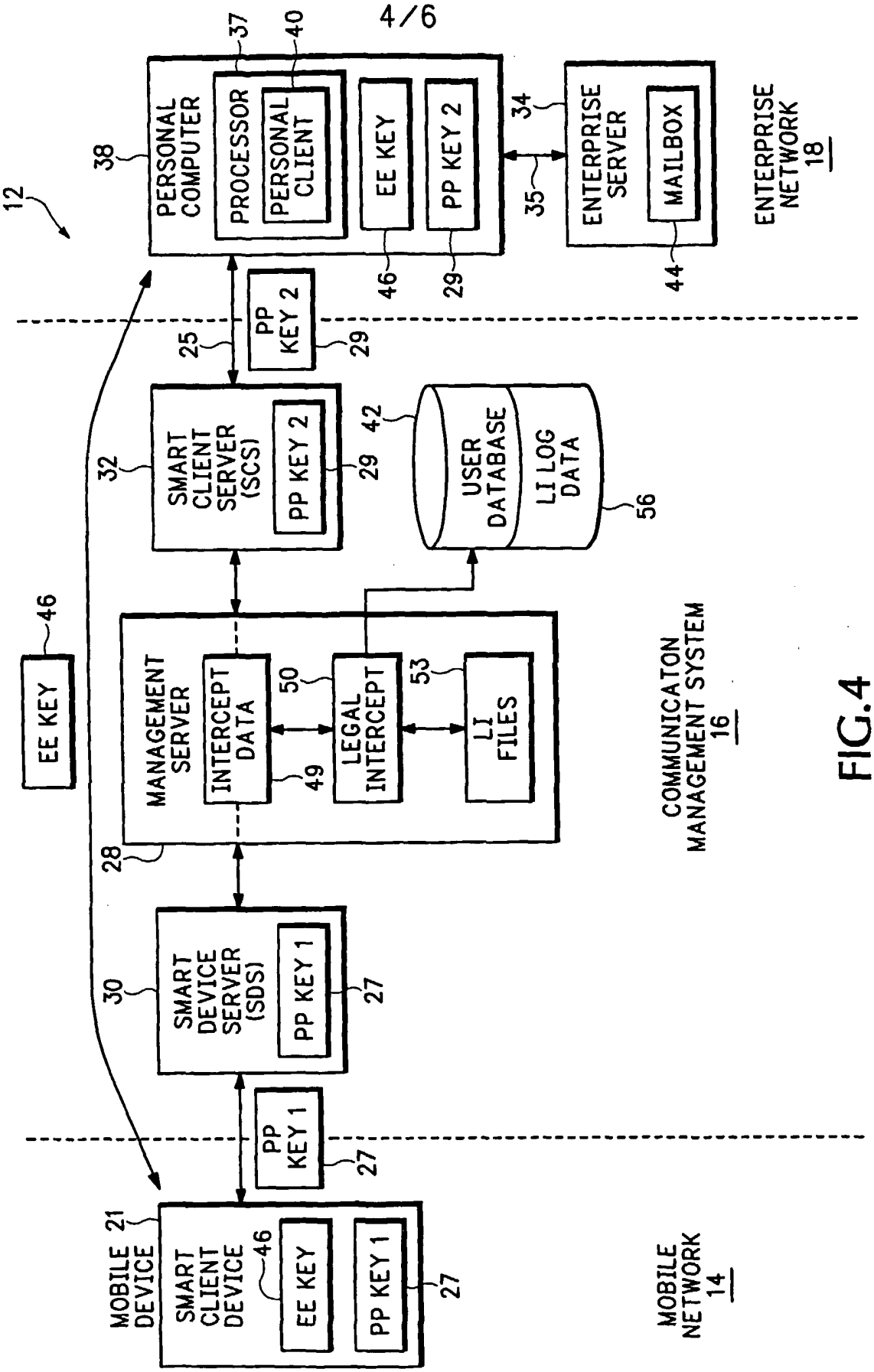

12
PERSONAL COMPUTER
38
PROCESSOR
37
PERSONAL CLIENT
40
EE KEY
46
PP KEY 2
29
34
35
ENTERPRISE SERVER
MAILBOX
44
ENTERPRISE NETWORK 18
PP KEY 2
29
25
SMART CLIENT SERVER (SCS)
32
PP KEY 2
29
42
USER DATABASE
LI LOG DATA
56
EE KEY
46
MANAGEMENT SERVER
28
INTERCEPT DATA
50
49
LEGAL INTERCEPT
53
LI FILES
COMMUNICATON MANAGEMENT SYSTEM 16
SMART DEVICE SERVER (SDS)
30
PP KEY 1
27
PP KEY 1
27
MOBILE DEVICE
21
SMART CLIENT DEVICE
46
EE KEY
PP KEY 1
27
MOBILE NETWORK 14

FIG.4

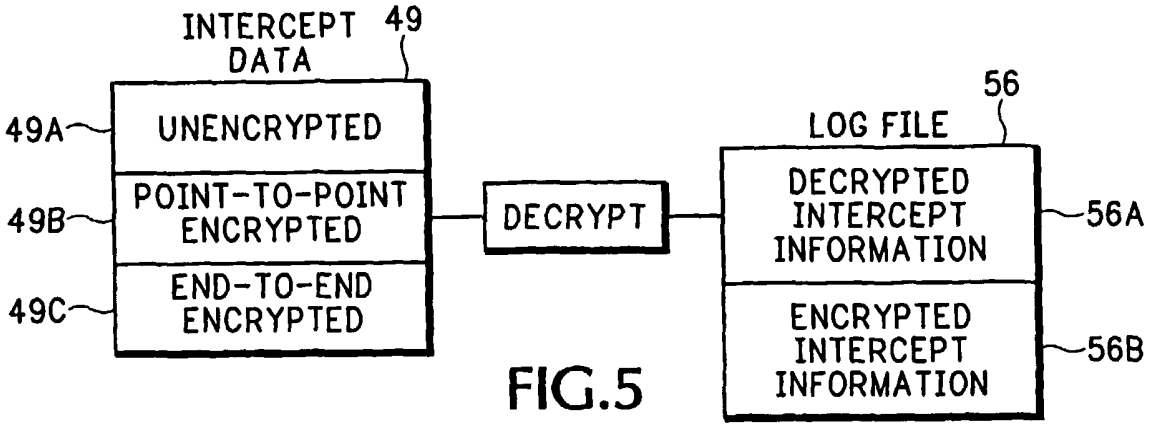

INTERCEPT DATA
49
49A
UNENCRYPTED
49B
POINT-TO-POINT ENCRYPTED
49C
END-TO-END ENCRYPTED
DECRYPT
56
LOG FILE
DECRYPTED INTERCEPT INFORMATION
56A
ENCRYPTED INTERCEPT INFORMATION
56B

FIG.5

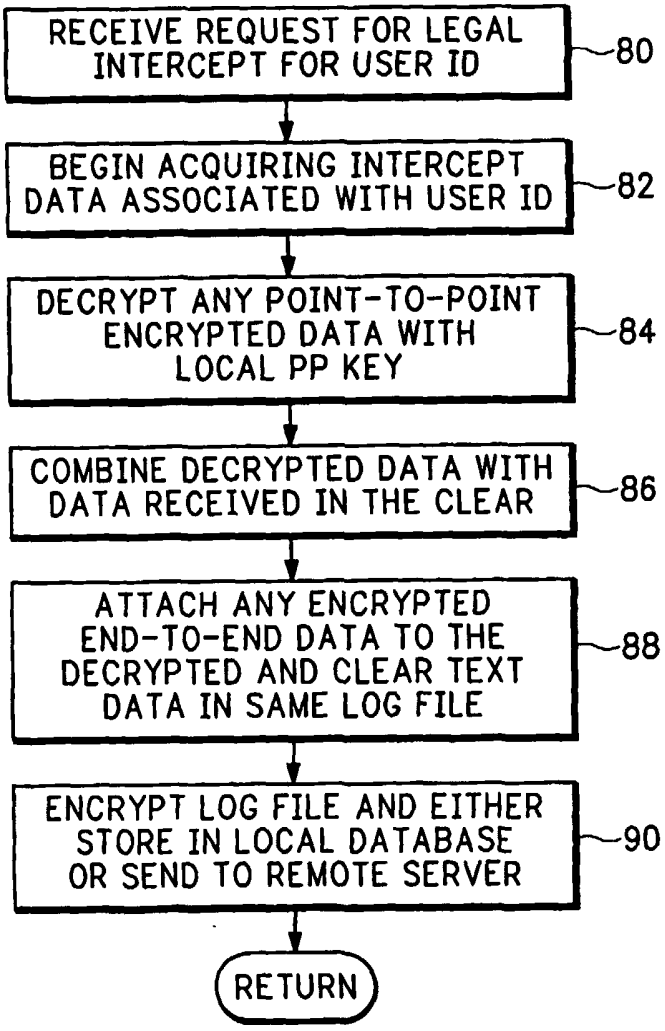

RECEIVE REQUEST FOR LEGAL INTERCEPT FOR USER ID
80
BEGIN ACQUIRING INTERCEPT DATA ASSOCIATED WITH USER ID
82
DECRYPT ANY POINT-TO-POINT ENCRYPTED DATA WITH LOCAL PP KEY
84
COMBINE DECRYPTED DATA WITH DATA RECEIVED IN THE CLEAR
86
ATTACH ANY ENCRYPTED END-TO-END DATA TO THE DECRYPTED AND CLEAR TEXT DATA IN SAME LOG FILE
88
ENCRYPT LOG FILE AND EITHER STORE IN LOCAL DATABASE OR SEND TO REMOTE SERVER
90
RETURN

FIG.6

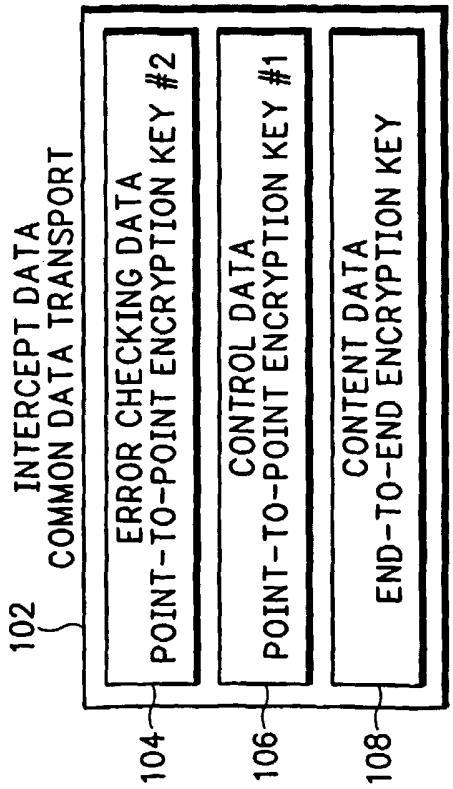

INTERCEPT DATA
COMMON DATA TRANSPORT
102
ERROR CHECKING DATA
POINT-TO-POINT ENCRYPTION KEY #2
CONTROL DATA
POINT-TO-POINT ENCRYPTION KEY #1
CONTENT DATA
END-TO-END ENCRYPTION KEY
104
106
108

FIG.7

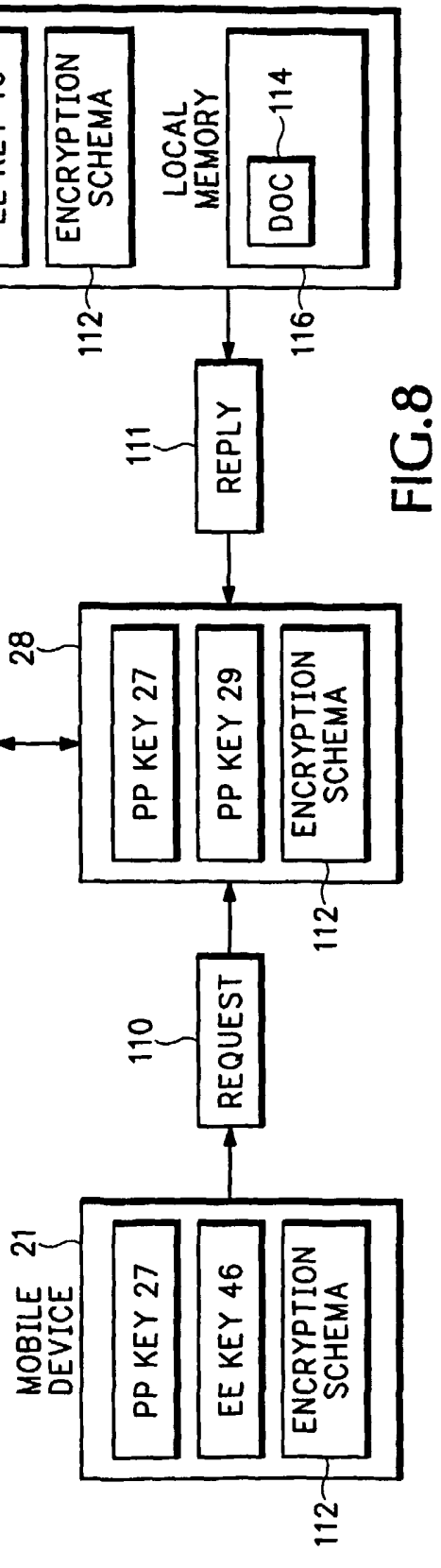

12
38
PERSONAL CLIENT
PP KEY 29
EE KEY 46
ENCRYPTION SCHEMA
LOCAL MEMORY
DOC
114
40
112
116
111
REPLY
42
USER DATABASE
28
PP KEY 27
PP KEY 29
ENCRYPTION SCHEMA
112
110
REQUEST
MOBILE DEVICE
21
PP KEY 27
EE KEY 46
ENCRYPTION SCHEMA
112

FIG.8