



(22) Date de dépôt/Filing Date: 2004/08/09

(41) Mise à la disp. pub./Open to Public Insp.: 2006/02/09

(51) Cl.Int./Int.Cl. *G06F 17/30* (2006.01),
H04L 12/16 (2006.01)

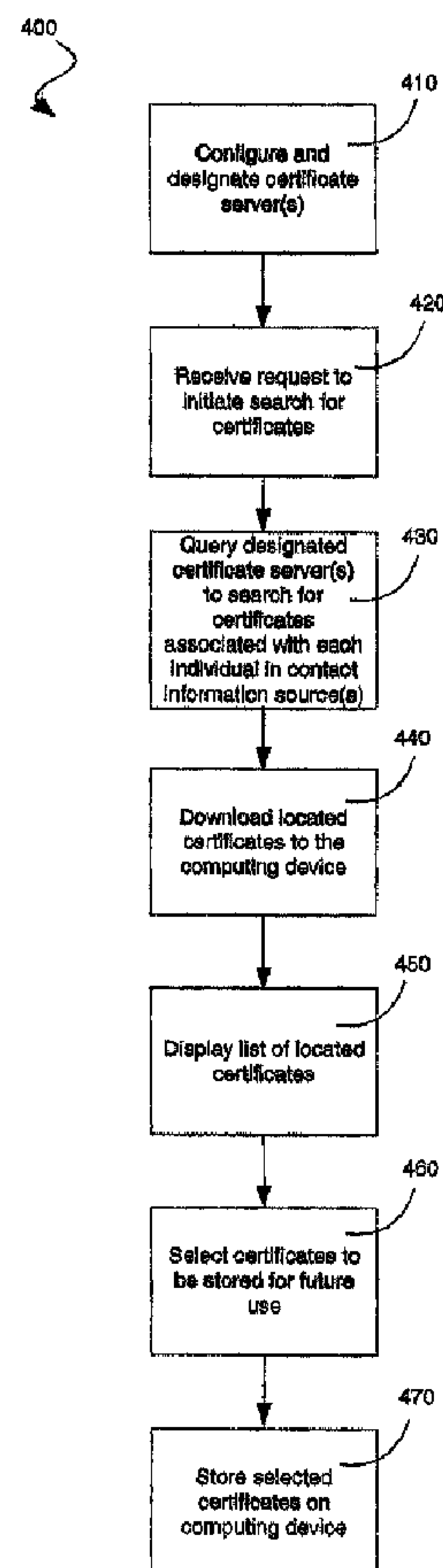
(71) Demandeur/Applicant:
RESEARCH IN MOTION LIMITED, CA

(72) Inventeurs/Inventors:
BROWN, MICHAEL S., CA;
ADAMS, NEIL P., CA;
TAPUSKA, DAVID F., CA;
LITTLE, HERBERT A., CA

(74) Agent: BERESKIN & PARR

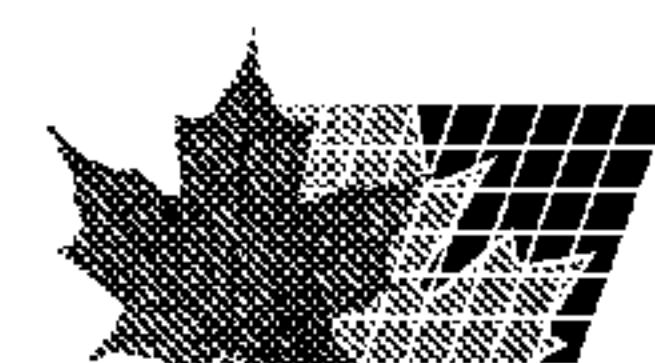
(54) Titre : SYSTÈME ET METHODE DE RECHERCHE ET DE RECUPERATION DE CERTIFICATS

(54) Title: SYSTEM AND METHOD FOR CERTIFICATE SEARCHING AND RETRIEVAL



(57) Abrégé/Abstract:

A system and method for searching and retrieving certificates, which may be used in the processing of encoded messages. In one embodiment, a certificate synchronization application is programmed to perform certificate searches by querying one or more



(57) **Abrégé(suite)/Abstract(continued):**

certificate servers using contact information stored on a computing device, from an address book for example. The invention allows certificates for contacts to be automatically searched for and retrieved from certificate servers, so that users need not manually search for certificates associated with each individual contact for which information is stored in a contact information source.

ABSTRACT OF THE DISCLOSURE

A system and method for searching and retrieving certificates, which may be used in the processing of encoded messages. In one embodiment, a certificate synchronization application is programmed to perform certificate searches by querying one or more certificate servers using contact information stored on a
5 computing device, from an address book for example. The invention allows certificates for contacts to be automatically searched for and retrieved from certificate servers, so that users need not manually search for certificates associated with each individual contact for which information is stored in a contact information source.

**Title: SYSTEM AND METHOD FOR CERTIFICATE SEARCHING AND
RETRIEVAL**

Field of the Invention

[0001] The invention relates generally to the processing of messages, such as e-mail messages, and more specifically to a system and method for searching and retrieving certificates used in the processing of encoded
5 messages.

Background of the Invention

[0002] Electronic mail ("e-mail") messages may be encoded using one of a number of known protocols. Some of these protocols, such as Secure Multiple
10 Internet Mail Extensions ("S/MIME") for example, rely on public and private encryption keys to provide confidentiality and integrity, and on a Public Key Infrastructure (PKI) to communicate information that provides authentication and authorization. Data encrypted using a private key of a private key/public key pair can only be decrypted using the corresponding public key of the pair, and vice-
15 versa. The authenticity of public keys used in the encoding of messages is validated using certificates. In particular, if a user of a computing device wishes to encrypt a message before the message is sent to a particular individual, the user will require a certificate for that individual. That certificate will typically comprise the public key of the individual, as well as other identification-related
20 information.

[0003] If the requisite certificate for the intended recipient is not already stored on the user's computing device, the certificate must first be retrieved. Searching for and retrieving a certificate for a specific recipient is a process that generally involves querying a certificate server by having the user manually enter
25 the name and/or e-mail address of the intended recipient in a search form displayed on the computing device. Certificates located in the search are then temporarily downloaded to the computing device for consideration, and a list of

- 2 -

located certificates may be displayed to the user. Selected certificates in the list may then be manually identified by a user for storage in a non-volatile store of the computing device, for potential future use.

[0004] Most computing devices provide software applications that allow
5 users to maintain a list of contacts and information associated with those
contacts. For example, an e-mail application may allow a user to manage an
address book that identifies selected individuals and stores information
associated with them in address book entries. If the user plans to communicate
10 messages, the certificates of these individuals will potentially need to be
obtained. However, manually entering search criteria for each individual
associated with an entry in the address book in querying one or more certificate
servers to obtain the potentially needed certificates can be time consuming, and
may be particularly cumbersome if the computing device on which the certificate
15 searches are initiated is small in size (e.g. a mobile device).

Summary of the Invention

[0005] Embodiments of the invention are generally directed to a system
and method for searching and retrieving certificates that automates at least some
20 of the tasks typically performed manually by users in known techniques, and
uses contact information, such as that stored in an address book for example, in
the searching of certificates.

[0006] In one broad aspect of the invention, there is provided a method for
searching and retrieving certificates associated with one or more contacts, the
25 method comprising the steps of: identifying one or more certificate servers to be
searched; identifying one or more contact information sources, each storing
contact information for at least one contact; for each contact of at least a subset
of the contacts for which contact information is stored in the one or more contact

- 3 -

information sources, searching each identified certificate server for certificates associated therewith by submitting at least one query constructed using at least some of the contact information for the respective contact to the respective certificate server, wherein the searching step is performed by a certificate
5 synchronization application; for each identified certificate server, downloading certificates satisfying the at least one query submitted thereto, to a computing device; and storing at least a subset of downloaded certificates in one or more certificate stores.

[0007] In another broad aspect of the invention, at least one of the one or
10 more contact information sources resides on a mobile device, and the searching step may be performed when the mobile device is coupled to the computing device.

[0008] In another broad aspect of the invention, at least one of the one or
15 more contact information sources is an address book, which may reside on the mobile device.

[0009] In another broad aspect of the invention, certificates stored in the storing step are stored in a certificate store on the computing device, a certificate store on the mobile device, or both.

[0010] In another broad aspect of the invention, the method further
20 comprises the steps of: generating a list of certificates identifying at least a subset of certificates downloaded to the computing device; displaying the list to a user; and receiving user selections of selected certificates identified in the list; wherein the at least a subset of certificates stored comprises the selected certificates.

25 **[0011]** In another broad aspect of the invention, the method further comprises the step of filtering out duplicate downloaded certificates prior to the storing step.

Brief Description of the Drawings

[0012] For a better understanding of embodiments of the invention, and to show more clearly how it may be carried into effect, reference will now be made, by way of example, to the accompanying drawings in which:

- 5 FIG. 1 is a block diagram of a mobile device in one example implementation;
FIG. 2 is a block diagram of a communication subsystem component of the mobile device of FIG. 1;
FIG. 3 is a block diagram of a node of a wireless network;
FIG. 4 is a block diagram illustrating components of a host system in one
10 example configuration;
FIG. 5 is a block diagram showing an example of a certificate chain;
FIG. 6 is a block diagram illustrating components of an example of an encoded message;
FIG. 7A is a flowchart illustrating steps in a method of searching and retrieving
15 certificates in an embodiment of the invention; and
FIG. 7B is a flowchart illustrating steps in a method of searching and retrieving certificates in another embodiment of the invention.

Detailed Description of Embodiments of the Invention

- 20 [0013] Some embodiments of the invention make use of a mobile station. A mobile station is a two-way communication device with advanced data communication capabilities having the capability to communicate with other computer systems, and is also referred to herein generally as a mobile device. A mobile device may also include the capability for voice communications.
25 Depending on the functionality provided by a mobile device, it may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication

- 5 -

device (with or without telephony capabilities). A mobile device communicates with other devices through a network of transceiver stations.

[0014] To aid the reader in understanding the structure of a mobile device and how it communicates with other devices, reference is made to FIGS. 1
5 through 3.

[0015] Referring first to FIG. 1, a block diagram of a mobile device in one example implementation is shown generally as 100. Mobile device 100 comprises a number of components, the controlling component being microprocessor 102. Microprocessor 102 controls the overall operation of mobile
10 device 100. Communication functions, including data and voice communications, are performed through communication subsystem 104. Communication subsystem 104 receives messages from and sends messages to a wireless network 200. In this example implementation of mobile device 100, communication subsystem 104 is configured in accordance with the Global
15 System for Mobile Communication (GSM) and General Packet Radio Services (GPRS) standards. The GSM/GPRS wireless network is used worldwide and it is expected that these standards will be superseded eventually by Enhanced Data GSM Environment (EDGE) and Universal Mobile Telecommunications Service (UMTS). New standards are still being defined, but it is believed that they will
20 have similarities to the network behaviour described herein, and it will also be understood by persons skilled in the art that the invention is intended to use any other suitable standards that are developed in the future. The wireless link connecting communication subsystem 104 with network 200 represents one or more different Radio Frequency (RF) channels, operating according to defined
25 protocols specified for GSM/GPRS communications. With newer network protocols, these channels are capable of supporting both circuit switched voice communications and packet switched data communications.

[0016] Although the wireless network associated with mobile device 100 is a GSM/GPRS wireless network in one example implementation of mobile device

- 6 -

100, other wireless networks may also be associated with mobile device 100 in variant implementations. Different types of wireless networks that may be employed include, for example, data-centric wireless networks, voice-centric wireless networks, and dual-mode networks that can support both voice and data
5 communications over the same physical base stations. Combined dual-mode networks include, but are not limited to, Code Division Multiple Access (CDMA) or CDMA2000 networks, GSM/GPRS networks (as mentioned above), and future third-generation (3G) networks like EDGE and UMTS. Some older examples of data-centric networks include the Mobitex™ Radio Network and the DataTAC™
10 Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM and Time Division Multiple Access (TDMA) systems.

[0017] Microprocessor 102 also interacts with additional subsystems such as a Random Access Memory (RAM) 106, flash memory 108, display 110,
15 auxiliary input/output (I/O) subsystem 112, serial port 114, keyboard 116, speaker 118, microphone 120, short-range communications 122 and other devices 124.

[0018] Some of the subsystems of mobile device 100 perform communication-related functions, whereas other subsystems may provide
20 "resident" or on-device functions. By way of example, display 110 and keyboard 116 may be used for both communication-related functions, such as entering a text message for transmission over network 200, and device-resident functions such as a calculator or task list. Operating system software used by microprocessor 102 is typically stored in a persistent store such as flash memory
25 108, which may alternatively be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 106.

- 7 -

[0019] Mobile device 100 may send and receive communication signals over network 200 after required network registration or activation procedures have been completed. Network access is associated with a subscriber or user of a mobile device 100. To identify a subscriber, mobile device 100 requires a
5 Subscriber Identity Module or "SIM" card 126 to be inserted in a SIM interface 128 in order to communicate with a network. SIM 126 is one type of a conventional "smart card" used to identify a subscriber of mobile device 100 and to personalize the mobile device 100, among other things. Without SIM 126, mobile device 100 is not fully operational for communication with network 200.
10 By inserting SIM 126 into SIM interface 128, a subscriber can access all subscribed services. Services could include: web browsing and messaging such as e-mail, voice mail, Short Message Service (SMS), and Multimedia Messaging Services (MMS). More advanced services may include: point of sale, field service and sales force automation. SIM 126 includes a processor and memory
15 for storing information. Once SIM 126 is inserted in SIM interface 128, it is coupled to microprocessor 102. In order to identify the subscriber, SIM 126 contains some user parameters such as an International Mobile Subscriber Identity (IMSI). An advantage of using SIM 126 is that a subscriber is not necessarily bound by any single physical mobile device. SIM 126 may store
20 additional subscriber information for a mobile device as well, including datebook (or calendar) information and recent call information.

[0020] Mobile device 100 is a battery-powered device and includes a battery interface 132 for receiving one or more rechargeable batteries 130. Battery interface 132 is coupled to a regulator (not shown), which assists battery
25 130 in providing power $V+$ to mobile device 100. Although current technology makes use of a battery, future technologies such as micro fuel cells may provide the power to mobile device 100.

[0021] Microprocessor 102, in addition to its operating system functions, enables execution of software applications on mobile device 100. A set of

- 8 -

applications that control basic device operations, including data and voice communication applications, will normally be installed on mobile device 100 during its manufacture. Another application that may be loaded onto mobile device 100 would be a personal information manager (PIM). A PIM has
5 functionality to organize and manage data items of interest to a subscriber, such as, but not limited to, e-mail, calendar events, voice mails, appointments, and task items. A PIM application has the ability to send and receive data items via wireless network 200. PIM data items may be seamlessly integrated, synchronized, and updated via wireless network 200 with the mobile device
10 subscriber's corresponding data items stored and/or associated with a host computer system. This functionality creates a mirrored host computer on mobile device 100 with respect to such items. This can be particularly advantageous where the host computer system is the mobile device subscriber's office computer system.

15 **[0022]** Additional applications may also be loaded onto mobile device 100 through network 200, auxiliary I/O subsystem 112, serial port 114, short-range communications subsystem 122, or any other suitable subsystem 124. This flexibility in application installation increases the functionality of mobile device 100 and may provide enhanced on-device functions, communication-related
20 functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using mobile device 100.

[0023] Serial port 114 enables a subscriber to set preferences through an external device or software application and extends the capabilities of mobile
25 device 100 by providing for information or software downloads to mobile device 100 other than through a wireless communication network. The alternate download path may, for example, be used to load an encryption key onto mobile device 100 through a direct and thus reliable and trusted connection to provide secure device communication.

- 9 -

[0024] Short-range communications subsystem 122 provides for communication between mobile device 100 and different systems or devices, without the use of network 200. For example, subsystem 122 may include an infrared device and associated circuits and components for short-range
5 communication. Examples of short range communication would include standards developed by the Infrared Data Association (IrDA), Bluetooth, and the 802.11 family of standards developed by IEEE.

[0025] In use, a received signal such as a text message, an e-mail message, or web page download will be processed by communication
10 subsystem 104 and input to microprocessor 102. Microprocessor 102 will then process the received signal for output to display 110 or alternatively to auxiliary I/O subsystem 112. A subscriber may also compose data items, such as e-mail messages, for example, using keyboard 116 in conjunction with display 110 and possibly auxiliary I/O subsystem 112. Auxiliary subsystem 112 may include
15 devices such as: a touch screen, mouse, track ball, infrared fingerprint detector, or a roller wheel with dynamic button pressing capability. Keyboard 116 is an alphanumeric keyboard and/or telephone-type keypad. A composed item may be transmitted over network 200 through communication subsystem 104.

[0026] For voice communications, the overall operation of mobile device
20 100 is substantially similar, except that the received signals would be output to speaker 118, and signals for transmission would be generated by microphone 120. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on mobile device 100. Although voice or audio signal output is accomplished primarily through speaker 118,
25 display 110 may also be used to provide additional information such as the identity of a calling party, duration of a voice call, or other voice call related information.

[0027] Referring now to FIG. 2, a block diagram of the communication subsystem component 104 of FIG. 1 is shown. Communication subsystem 104

- 10 -

comprises a receiver 150, a transmitter 152, one or more embedded or internal antenna elements 154, 156, Local Oscillators (LOs) 158, and a processing module such as a Digital Signal Processor (DSP) 160.

[0028] The particular design of communication subsystem 104 is dependent upon the network 200 in which mobile device 100 is intended to operate, thus it should be understood that the design illustrated in FIG. 2 serves only as one example. Signals received by antenna 154 through network 200 are input to receiver 150, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, and analog-to-digital (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in DSP 160. In a similar manner, signals to be transmitted are processed, including modulation and encoding, by DSP 160. These DSP-processed signals are input to transmitter 152 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over network 200 via antenna 156. DSP 160 not only processes communication signals, but also provides for receiver and transmitter control. For example, the gains applied to communication signals in receiver 150 and transmitter 152 may be adaptively controlled through automatic gain control algorithms implemented in DSP 160.

[0029] The wireless link between mobile device 100 and a network 200 may contain one or more different channels, typically different RF channels, and associated protocols used between mobile device 100 and network 200. A RF channel is a limited resource that must be conserved, typically due to limits in overall bandwidth and limited battery power of mobile device 100.

[0030] When mobile device 100 is fully operational, transmitter 152 is typically keyed or turned on only when it is sending to network 200 and is otherwise turned off to conserve resources. Similarly, receiver 150 is periodically

- 11 -

turned off to conserve power until it is needed to receive signals or information (if at all) during designated time periods.

[0031] Referring now to FIG. 3, a block diagram of a node of a wireless network is shown as 202. In practice, network 200 comprises one or more nodes 5 202. Mobile device 100 communicates with a node 202 within wireless network 200. In the example implementation of FIG. 3, node 202 is configured in accordance with General Packet Radio Service (GPRS) and Global Systems for Mobile (GSM) technologies. Node 202 includes a base station controller (BSC) 204 with an associated tower station 206, a Packet Control Unit (PCU) 208 10 added for GPRS support in GSM, a Mobile Switching Center (MSC) 210, a Home Location Register (HLR) 212, a Visitor Location Registry (VLR) 214, a Serving GPRS Support Node (SGSN) 216, a Gateway GPRS Support Node (GGSN) 218, and a Dynamic Host Configuration Protocol (DHCP) 220. This list of components is not meant to be an exhaustive list of the components of every 15 node 202 within a GSM/GPRS network, but rather a list of components that are commonly used in communications through network 200.

[0032] In a GSM network, MSC 210 is coupled to BSC 204 and to a landline network, such as a Public Switched Telephone Network (PSTN) 222 to satisfy circuit switched requirements. The connection through PCU 208, SGSN 20 216 and GGSN 218 to the public or private network (Internet) 224 (also referred to herein generally as a shared network infrastructure) represents the data path for GPRS capable mobile devices. In a GSM network extended with GPRS capabilities, BSC 204 also contains a Packet Control Unit (PCU) 208 that connects to SGSN 216 to control segmentation, radio channel allocation and to 25 satisfy packet switched requirements. To track mobile device location and availability for both circuit switched and packet switched management, HLR 212 is shared between MSC 210 and SGSN 216. Access to VLR 214 is controlled by MSC 210.

- 12 -

[0033] Station 206 is a fixed transceiver station. Station 206 and BSC 204 together form the fixed transceiver equipment. The fixed transceiver equipment provides wireless network coverage for a particular coverage area commonly referred to as a "cell". The fixed transceiver equipment transmits communication
5 signals to and receives communication signals from mobile devices within its cell via station 206. The fixed transceiver equipment normally performs such functions as modulation and possibly encoding and/or encryption of signals to be transmitted to the mobile device in accordance with particular, usually predetermined, communication protocols and parameters, under control of its
10 controller. The fixed transceiver equipment similarly demodulates and possibly decodes and decrypts, if necessary, any communication signals received from mobile device 100 within its cell. Communication protocols and parameters may vary between different nodes. For example, one node may employ a different modulation scheme and operate at different frequencies than other nodes.

15 **[0034]** For all mobile devices 100 registered with a specific network, permanent configuration data such as a user profile is stored in HLR 212. HLR 212 also contains location information for each registered mobile device and can be queried to determine the current location of a mobile device. MSC 210 is responsible for a group of location areas and stores the data of the mobile
20 devices currently in its area of responsibility in VLR 214. Further VLR 214 also contains information on mobile devices that are visiting other networks. The information in VLR 214 includes part of the permanent mobile device data transmitted from HLR 212 to VLR 214 for faster access. By moving additional information from a remote HLR 212 node to VLR 214, the amount of traffic
25 between these nodes can be reduced so that voice and data services can be provided with faster response times and at the same time requiring less use of computing resources.

[0035] SGSN 216 and GGSN 218 are elements added for GPRS support; namely packet switched data support, within GSM. SGSN 216 and MSC 210

- 13 -

have similar responsibilities within wireless network 200 by keeping track of the location of each mobile device 100. SGSN 216 also performs security functions and access control for data traffic on network 200. GGSN 218 provides internetworking connections with external packet switched networks and connects to one or more SGSN's 216 via an Internet Protocol (IP) backbone network operated within the network 200. During normal operations, a given mobile device 100 must perform a "GPRS Attach" to acquire an IP address and to access data services. This requirement is not present in circuit switched voice channels as Integrated Services Digital Network (ISDN) addresses are used for routing incoming and outgoing calls. Currently, all GPRS capable networks use private, dynamically assigned IP addresses, thus requiring a DHCP server 220 connected to the GGSN 218. There are many mechanisms for dynamic IP assignment, including using a combination of a Remote Authentication Dial-In User Service (RADIUS) server and DHCP server. Once the GPRS Attach is complete, a logical connection is established from a mobile device 100, through PCU 208, and SGSN 216 to an Access Point Node (APN) within GGSN 218. The APN represents a logical end of an IP tunnel that can either access direct Internet compatible services or private network connections. The APN also represents a security mechanism for network 200, insofar as each mobile device 100 must be assigned to one or more APNs and mobile devices 100 cannot exchange data without first performing a GPRS Attach to an APN that it has been authorized to use. The APN may be considered to be similar to an Internet domain name such as "myconnection.wireless.com".

[0036] Once the GPRS Attach is complete, a tunnel is created and all traffic is exchanged within standard IP packets using any protocol that can be supported in IP packets. This includes tunneling methods such as IP over IP as in the case with some IPSecurity (IPsec) connections used with Virtual Private Networks (VPN). These tunnels are also referred to as Packet Data Protocol (PDP) Contexts and there are a limited number of these available in the network

- 14 -

200. To maximize use of the PDP Contexts, network 200 will run an idle timer for each PDP Context to determine if there is a lack of activity. When a mobile device 100 is not using its PDP Context, the PDP Context can be deallocated and the IP address returned to the IP address pool managed by DHCP server
5 220.

[0037] Referring now to FIG. 4, a block diagram illustrating components of a host system in one example configuration is shown. Host system 250 will typically be a corporate office or other local area network (LAN), but may instead be a home office computer or some other private system, for example, in variant
10 implementations. In this example shown in FIG. 4, host system 250 is depicted as a LAN of an organization to which a user of mobile device 100 belongs.

[0038] LAN 250 comprises a number of network components connected to each other by LAN connections 260. For instance, a user's desktop computer 262a with an accompanying cradle 264 for the user's mobile device 100 is
15 situated on LAN 250. Cradle 264 for mobile device 100 may be coupled to computer 262a by a serial or a Universal Serial Bus (USB) connection, for example. Other user computers 262b are also situated on LAN 250, and each may or may not be equipped with an accompanying cradle 264 for a mobile device. Cradle 264 facilitates the loading of information (e.g. PIM data, private
20 symmetric encryption keys to facilitate secure communications between mobile device 100 and LAN 250) from user computer 262a to mobile device 100, and may be particularly useful for bulk information updates often performed in initializing mobile device 100 for use. As will be discussed in further detail below, the information downloaded to mobile device 100 may include certificates used in
25 the exchange of messages. It will be understood by persons skilled in the art that user computers 262a, 262b will typically be also connected to other peripheral devices not explicitly shown in FIG. 4.

[0039] Embodiments of the invention relate generally to the processing of messages, such as e-mail messages, and the communication of such messages

- 15 -

to and from mobile device 100. Accordingly, only a subset of network components of LAN 250 are shown in FIG. 4 for ease of exposition, and it will be understood by persons skilled in the art that LAN 250 will comprise additional components not explicitly shown in FIG. 4, for this example configuration. More
5 generally, LAN 250 may represent a smaller part of a larger network [not shown] of the organization, and may comprise different components and/or be arranged in different topologies than that shown in the example of FIG. 4.

[0040] In this example, mobile device 100 communicates with LAN 250 through a node 202 of wireless network 200 and a shared network infrastructure
10 224 such as a service provider network or the public Internet. Access to LAN 250 may be provided through one or more routers [not shown], and computing devices of LAN 250 may operate from behind a firewall or proxy server 266.

[0041] In a variant implementation, LAN 250 comprises a wireless VPN router [not shown] to facilitate data exchange between the LAN 250 and mobile
15 device 100. The concept of a wireless VPN router is new in the wireless industry and implies that a VPN connection can be established directly through a specific wireless network to mobile device 100. The possibility of using a wireless VPN router has only recently been available and could be used when the new Internet Protocol (IP) Version 6 (IPV6) arrives into IP-based wireless networks. This new
20 protocol will provide enough IP addresses to dedicate an IP address to every mobile device, making it possible to push information to a mobile device at any time. An advantage of using a wireless VPN router is that it could be an off-the-shelf VPN component, not requiring a separate wireless gateway and separate wireless infrastructure to be used. A VPN connection would preferably be a
25 Transmission Control Protocol (TCP)/IP or User Datagram Protocol (UDP)/IP connection to deliver the messages directly to mobile device 100 in this variant implementation.

[0042] Messages intended for a user of mobile device 100 are initially received by a message server 268 of LAN 250. Such messages may originate

- 16 -

from any of a number of sources. For instance, a message may have been sent by a sender from a computer 262b within LAN 250, from a different mobile device [not shown] connected to wireless network 200 or to a different wireless network, or from a different computing device or other device capable of sending
5 messages, via the shared network infrastructure 224, and possibly through an application service provider (ASP) or Internet service provider (ISP), for example.

[0043] Message server 268 typically acts as the primary interface for the exchange of messages, particularly e-mail messages, within the organization and over the shared network infrastructure 224. Each user in the organization that
10 has been set up to send and receive messages is typically associated with a user account managed by message server 268. One example of a message server 268 is a Microsoft Exchange™ Server. In some implementations, LAN 250 may comprise multiple message servers 268. Message server 268 may also be adapted to provide additional functions beyond message management, including
15 the management of data associated with calendars and task lists, for example.

[0044] When messages are received by message server 268, they are typically stored in a message store [not explicitly shown], from which messages can be subsequently retrieved and delivered to users. For instance, an e-mail client application operating on a user's computer 262a may request the e-mail
20 messages associated with that user's account stored on message server 268. These messages would then typically be retrieved from message server 268 and stored locally on computer 262a.

[0045] When operating mobile device 100, the user may wish to have e-mail messages retrieved for delivery to the handheld. An e-mail client application
25 operating on mobile device 100 may also request messages associated with the user's account from message server 268. The e-mail client may be configured (either by the user or by an administrator, possibly in accordance with an organization's information technology (IT) policy) to make this request at the

- 17 -

direction of the user, at some pre-defined time interval, or upon the occurrence of some pre-defined event. In some implementations, mobile device 100 is assigned its own e-mail address, and messages addressed specifically to mobile device 100 are automatically redirected to mobile device 100 as they are
5 received by message server 268.

[0046] To facilitate wireless communication of messages and message-related data between mobile device 100 and components of LAN 250, a number of wireless communications support components 270 may be provided. In this example implementation, wireless communications support components 270
10 comprise a message management server 272, for example. Message management server 272 is used to specifically provide support for the management of messages, such as e-mail messages, that are to be handled by mobile devices. Generally, while messages are still stored on message server 268, message management server 272 can be used to control when, if, and how
15 messages should be sent to mobile device 100. Message management server 272 also facilitates the handling of messages composed on mobile device 100, which are sent to message server 268 for subsequent delivery.

[0047] For example, message management server 272 may: monitor the user's "mailbox" (e.g. the message store associated with the user's account on
20 message server 268) for new e-mail messages; apply user-definable filters to new messages to determine if and how the messages will be relayed to the user's mobile device 100; compress and encrypt new messages (e.g. using an encryption technique such as Data Encryption Standard (DES) or Triple DES) and push them to mobile device 100 via the shared network infrastructure 224
25 and wireless network 200; and receive messages composed on mobile device 100 (e.g. encrypted using Triple DES), decrypt and decompress the composed messages, re-format the composed messages if desired so that they will appear to have originated from the user's computer 262a, and re-route the composed messages to message server 268 for delivery.

[0048] Certain properties or restrictions associated with messages that are to be sent from and/or received by mobile device 100 can be defined (e.g. by an administrator in accordance with IT policy) and enforced by message management server 272. These may include whether mobile device 100 may
5 receive encrypted and/or signed messages, minimum encryption key sizes, whether outgoing messages must be encrypted and/or signed, and whether copies of all secure messages sent from mobile device 100 are to be sent to a pre-defined copy address, for example.

[0049] Message management server 272 may also be adapted to provide
10 other control functions, such as only pushing certain message information or pre-defined portions (e.g. "blocks") of a message stored on message server 268 to mobile device 100. For example, when a message is initially retrieved by mobile device 100 from message server 268, message management server 272 is adapted to push only the first part of a message to mobile device 100, with the
15 part being of a pre-defined size (e.g. 2 KB). The user can then request more of the message, to be delivered in similar-sized blocks by message management server 272 to mobile device 100, possibly up to a maximum pre-defined message size.

[0050] Accordingly, message management server 272 facilitates better
20 control over the type of data and the amount of data that is communicated to mobile device 100, and can help to minimize potential waste of bandwidth or other resources.

[0051] It will be understood by persons skilled in the art that message management server 272 need not be implemented on a separate physical server
25 in LAN 250 or other network. For example, some or all of the functions associated with message management server 272 may be integrated with message server 268, or some other server in LAN 250. Furthermore, LAN 250 may comprise multiple message management servers 272, particularly in variant implementations where a large number of mobile devices need to be supported.

[0052] Embodiments of the invention relate generally to the processing of encoded messages, such as e-mail messages that are encrypted and/or signed. While Simple Mail Transfer Protocol (SMTP), RFC822 headers, and Multipurpose Internet Mail Extensions (MIME) body parts may be used to define the format of a typical e-mail message not requiring encoding, Secure/MIME (S/MIME), a version of the MIME protocol, may be used in the communication of encoded messages (i.e. in secure messaging applications). S/MIME enables end-to-end authentication and confidentiality, and protects data integrity and privacy from the time an originator of a message sends a message until it is decoded and read by the message recipient. Other known standards and protocols may be employed to facilitate secure message communication, such as Pretty Good Privacy™ (PGP), OpenPGP, and others known in the art.

[0053] Secure messaging protocols such as S/MIME rely on public and private encryption keys to provide confidentiality and integrity, and on a Public Key Infrastructure (PKI) to communicate information that provides authentication and authorization. Data encrypted using a private key of a private key/public key pair can only be decrypted using the corresponding public key of the pair, and vice-versa. Private key information is never made public, whereas public key information is shared.

[0054] For example, if a sender wishes to send a message to a recipient in encrypted form, the recipient's public key is used to encrypt a message, which can then be decrypted only using the recipient's private key. Alternatively, in some encoding techniques, a one-time session key is generated and used to encrypt the body of a message, typically with a symmetric encryption technique (e.g. Triple DES). The session key is then encrypted using the recipient's public key (e.g. with a public key encryption algorithm such as RSA), which can then be decrypted only using the recipient's private key. The decrypted session key can then be used to decrypt the message body. The message header may be used to specify the particular encryption scheme that must be used to decrypt the

- 20 -

message. Other encryption techniques based on public key cryptography may be used in variant implementations. However, in each of these cases, only the recipient's private key may be used to facilitate decryption of the message, and in this way, the confidentiality of messages can be maintained.

5 **[0055]** As a further example, a sender may sign a message using a digital signature. A digital signature is a digest of the message (e.g. a hash of the message) encrypted using the sender's private key, which can then be appended to the outgoing message. To verify the signature of the message when received, the recipient uses the same technique as the sender (e.g. using the same
10 standard hash algorithm) to obtain a digest of the received message. The recipient also uses the sender's public key to decrypt the digital signature, in order to obtain what should be a matching digest for the received message. If the digests of the received message do not match, this suggests that either the message content was changed during transport and/or the message did not
15 originate from the sender whose public key was used for verification. By verifying a digital signature in this way, authentication of the sender and message integrity can be maintained.

[0056] An encoded message may be encrypted, signed, or both encrypted and signed. The authenticity of public keys used in these operations is validated
20 using certificates. A certificate is a digital document issued by a certificate authority (CA). Certificates are used to authenticate the association between users and their public keys, and essentially, provides a level of trust in the authenticity of the users' public keys. Certificates contain information about the certificate holder, with certificate contents typically formatted in accordance with
25 an accepted standard (e.g. X.509).

[0057] Consider FIG. 5, in which an example certificate chain 300 is shown. Certificate 310 issued to "John Smith" is an example of a certificate issued to an individual, which may be referred to as an end entity certificate. End entity certificate 310 typically identifies the certificate holder 312 (i.e. John Smith

- 21 -

in this example) and the issuer of the certificate 314, and includes a digital signature of the issuer 316 and the certificate holder's public key 318. Certificate 310 will also typically include other information and attributes that identify the certificate holder (e.g. e-mail address, organization name, organizational unit name, location, etc.). When the individual composes a message to be sent to a recipient, it is customary to include that individual's certificate 300 with the message.

[0058] For a public key to be trusted, its issuing organization must be trusted. The relationship between a trusted CA and a user's public key can be represented by a series of related certificates, also referred to as a certificate chain. The certificate chain can be followed to determine the validity of a certificate.

[0059] For instance, in the example certificate chain 300 shown in FIG. 5, the recipient of a message purported to be sent by John Smith may wish to verify the trust status of certificate 310 attached to the received message. To verify the trust status of certificate 310 on a recipient's computing device (e.g. computer 262a of FIG. 4) for example, the certificate 320 of issuer ABC is obtained, and used to verify that certificate 310 was indeed signed by issuer ABC. Certificate 320 may already be stored in a certificate store on the computing device, or it may need to be retrieved from a certificate source (e.g. LDAP server 284 of FIG. 4 or some other public or private LDAP server). If certificate 320 is already stored in the recipient's computing device and the certificate has been designated as trusted by the recipient, then certificate 310 is considered to be trusted since it chains to a stored, trusted certificate.

[0060] However, in the example shown in FIG. 5, certificate 330 is also required to verify the trust of certificate 310. Certificate 330 is self-signed, and is referred to as a "root certificate". Accordingly, certificate 320 may be referred to as an "intermediate certificate" in certificate chain 300; any given certificate chain to a root certificate, assuming a chain to the root certificate can be determined for

- 22 -

a particular end entity certificate, may contain zero, one, or multiple intermediate certificates. If certificate 330 is a root certificate issued by a trusted source (from a large certificate authority such as Verisign or Entrust, for example), then certificate 310 may be considered to be trusted since it chains to a trusted
5 certificate. The implication is that both the sender and the recipient of the message trust the source of the root certificate 330. If a certificate cannot be chained to a trusted certificate, the certificate may be considered to be "not trusted".

[0061] Certificate servers store information about certificates and lists
10 identifying certificates that have been revoked. These certificate servers can be accessed to obtain certificates and to verify certificate authenticity and revocation status. For example, a Lightweight Directory Access Protocol (LDAP) server may be used to obtain certificates, and an Online Certificate Status Protocol (OCSP) server may be used to verify certificate revocation status.

15 **[0062]** Standard e-mail security protocols typically facilitate secure message transmission between non-mobile computing devices (e.g. computers 262a, 262b of FIG. 4; remote desktop devices). Referring again to FIG. 4, in order that signed messages received from senders may be read from mobile device 100 and encrypted messages be sent to those senders, mobile device
20 100 is adapted to store certificates and associated public keys of other individuals. Certificates stored on a user's computer 262a will typically be downloaded from computer 262a to mobile device 100 through cradle 264, for example.

[0063] Certificates stored on computer 262a and downloaded to mobile
25 device 100 are not limited to certificates associated with individuals but may also include certificates issued to CAs, for example. Certain certificates stored in computer 262a and/or mobile device 100 can also be explicitly designated as "trusted" by the user. Accordingly, when a certificate is received by a user on mobile device 100, it can be verified on mobile device 100 by matching the

- 23 -

certificate with one stored on mobile device 100 and designated as trusted, or otherwise determined to be chained to a trusted certificate.

[0064] Mobile device 100 may also be adapted to store the private key of the public key/private key pair associated with the user, so that the user of mobile
5 device 100 can sign outgoing messages composed on mobile device 100, and decrypt messages sent to the user encrypted with the user's public key. The private key may be downloaded to mobile device 100 from the user's computer 262a through cradle 264, for example. The private key is preferably exchanged between the computer 262a and mobile device 100 so that the user may share
10 one identity and one method for accessing messages.

[0065] User computers 262a, 262b can obtain certificates from a number of sources, for storage on computers 262a, 262b and/or mobile devices (e.g. mobile device 100). These certificate sources may be private (e.g. dedicated for use within an organization) or public, may reside locally or remotely, and may be
15 accessible from within an organization's private network or through the Internet, for example. In the example shown in FIG. 4, multiple PKI servers 280 associated with the organization reside on LAN 250. PKI servers 280 include a CA server 282 for issuing certificates, an LDAP server 284 used to search for and download certificates (e.g. for individuals within the organization), and an
20 OCSP server 286 used to verify the revocation status of certificates.

[0066] Certificates may be retrieved from LDAP server 284 by a user computer 262a, for example, to be downloaded to mobile device 100 via cradle 264. However, in a variant implementation, LDAP server 284 may be accessed directly (i.e. "over the air" in this context) by mobile device 100, and mobile
25 device 100 may search for and retrieve individual certificates through a mobile data server 288. Similarly, mobile data server 288 may be adapted to allow mobile device 100 to directly query OCSP server 286 to verify the revocation status of certificates.

- 24 -

[0067] In variant implementations, only selected PKI servers 280 may be made accessible to mobile devices (e.g. allowing certificates to be downloaded only from a user's computer 262a, 262b, while allowing the revocation status of certificates to be checked from mobile device 100).

- 5 **[0068]** In variant implementations, certain PKI servers 280 may be made accessible only to mobile devices registered to particular users, as specified by an IT administrator, possibly in accordance with an IT policy, for example.

[0069] Other sources of certificates [not shown] may include a Windows certificate store, another secure certificate store on or outside LAN 250, and
10 smart cards, for example.

[0070] Referring now to FIG. 6, a block diagram illustrating components of an example of an encoded message, as may be received by a message server (e.g. message server 268 of FIG. 4), is shown generally as 350. Encoded message 350 typically includes one or more of the following: a header portion
15 352, an encoded body portion 354, optionally one or more encoded attachments 356, one or more encrypted session keys 358, and signature and signature-related information 360. For example, header portion 352 typically includes addressing information such as "To", "From", and "CC" addresses, and may also include message length indicators, and sender encryption and signature scheme
20 identifiers, for example. Actual message content normally includes a message body or data portion 354 and possibly one or more attachments 356, which may be encrypted by the sender using a session key. If a session key was used, it is typically encrypted for each intended recipient using the respective public key for each recipient, and included in the message at 358. If the message was signed,
25 a signature and signature-related information 360 are also included. This may include the sender's certificate, for example.

[0071] The format for an encoded message as shown in FIG. 6 is provided by way of example only, and persons skilled in the art will understand that

- 25 -

embodiments of the invention will be applicable to encoded messages of other formats. Depending on the specific messaging scheme used, components of an encoded message may appear in a different order than shown in FIG. 6, and an encoded message may include fewer, additional, or different components, which
5 may depend on whether the encoded message is encrypted, signed or both.

[0072] Embodiments of the invention are generally directed to a system and method for searching and retrieving certificates that automates at least some of the tasks typically performed manually by users in known techniques for searching certificates, and uses contact information, such as that stored in an
10 address book for example, in the searching of certificates.

[0073] In one embodiment of the invention, a certificate synchronization application is provided on a user's computing device. The certificate synchronization application is programmed to allow users to initiate certificate searches of one or more certificate servers (e.g. an LDAP server, such as LDAP
15 server 284 of FIG. 4) using contact information stored on the computing device.

[0074] In one embodiment of the invention, the certificate synchronization application executes and resides on a user's desktop computer (e.g. computer 262a of FIG. 4) to which a cradle (e.g. cradle 264 of FIG. 4) for a mobile device (e.g. mobile device 100 of FIG. 4) is connected. However, in variant
20 embodiments of the invention, the certificate synchronization application may execute and reside on a desktop computer not equipped with a cradle for a mobile device, or on some other computing device. For example, the certificate synchronization application may execute and reside on a mobile device, which may have direct access to certificate servers (e.g. through mobile data server
25 288 of FIG. 4). By way of further example, the certificate synchronization application need not be executing on the same computing device to which certificates would typically be downloaded. For example, the certificate synchronization application may execute on a central server, such as a message management server (e.g. message management server 272 of FIG. 4) or

- 26 -

message server (e.g. message server 268 of FIG. 4), for example. Moreover, the certificate synchronization application need not be a stand-alone application, and the functions of the certificate synchronization application described herein may be integrated with the functions of some other application, residing and
5 executing on a computing device such as a desktop computer, a mobile device, a message management server, a message server, or some other computing device.

[0075] In one embodiment of the invention, the contact information is stored in an address book of the user. However, in variant embodiments of the
10 invention, the contact information may originate from other contact information sources, and may include contact management application data and calendar application data, for example. Recipient lists within one or more received e-mail messages and files containing contact data are further examples of possible contact information sources. These sources may reside on the user's computing
15 device or one or more other computing devices coupled to the user's computing device. Contact information associated with other users (e.g. data associated with another individual's address book, etc.) may also be used.

[0076] Referring to FIG. 7A, a flowchart illustrating steps in a method of searching and retrieving certificates in an embodiment of the invention is shown
20 generally as 400. The method facilitates at least partial automation of a pre-loading of certificates, so that users do not have to manually search for a certificate for each individual contact associated with an entry in a contact information source.

[0077] In this embodiment of the invention, at least some steps of the
25 method are performed by a certificate synchronization application that executes and resides on a desktop computer. In variant embodiments, the certificate synchronization application may be residing and executing on a computing device such as a mobile device, a message management server, a message server, or some other computing device.

- 27 -

[0078] At step 410, one or more certificate servers (e.g. LDAP server 284 of FIG. 4) that will be used for certificate searches are configured for access. Of those configured certificate servers, one or more certificate servers may be designated for certificate searching in accordance with an embodiment of the invention.

[0079] Typically, information required to configure a certificate server may include, for example, a host name, a host address or uniform resource locator (URL), a port number (e.g. for LDAP servers), a default base query, a query limit (i.e. the maximum number of certificates to be returned), and/or an indication of whether certificate information is to be compressed for transmission. In one implementation, such configuration information can be input by a user, and default values for certain inputs may be set in the certificate synchronization application. In other implementations, such configuration information may already be pre-defined in the certificate synchronization application, possibly by an IT administrator in accordance with an IT policy. Still other implementations may permit some configuration information to be input or modified by users, while not permitting other configuration information to be user-modified.

[0080] Similarly, in one implementation, the certificate synchronization application may permit users to manually designate specific certificate servers that will be queried and searched in accordance with an embodiment of the invention. In other implementations, the certificate synchronization application may automatically designate certain pre-identified specific certificate servers to be searched, possibly as directed by an IT administrator in accordance with an IT policy. Still other implementations may permit some degree of user configuration, by allowing a user to designate specific certificate servers but only from a pre-defined set defined by an IT administrator in accordance with an IT policy, for example.

- 28 -

[0081] At step 420, a request is received by the certificate synchronization application from the user to initiate a search for certificates in the servers designated at step 410.

[0082] At step 430, the certificate synchronization application searches for
5 certificates by automatically querying each designated certificate server, for certificates issued to each individual associated with an entry in one or more contact information sources. This information may be provided in a user's address book, for example, with each entry in the address book providing a name and/or e-mail address of an individual.

10 **[0083]** The certificate synchronization application is pre-configured [step not explicitly shown] to identify the location(s) of the contact information source(s) to be used, possibly as defined by the user upon initial configuration of the certificate synchronization application. One or more default contact information sources (e.g. the address book of the user's primary e-mail application) may also
15 be defined.

[0084] In variant embodiments of the invention, information identifying the contact information source(s) to be used may be explicitly requested from the user prior to commencement of the search.

[0085] In variant embodiments of the invention, the certificate
20 synchronization application may be adapted to search for and locate possible contact information sources on the user's computing device. The located sources can then be automatically used for the certificate search at step 430, or a list of the located sources can be displayed to the user prior to searching so that the user can explicitly select the sources to be used.

25 **[0086]** The form of the query used to search for certificates can differ in different implementations. For example, the certificate synchronization application may search only for certificates that match both the full name and e-mail address associated with each contact entry (e.g. address entry) in the

- 29 -

contact information source(s) being used. Alternatively, the certificate synchronization application may search for certificates that match either the full name or e-mail address associated with a contact entry, or that match only the last name and e-mail address associated with the contact entry, for example.

5 Where a designated certificate server supports wild-card type queries (e.g. entering one or more initial characters for a particular attribute being searched results in all certificates containing an attribute value beginning with those initial characters to be retrieved), these queries may also be employed in the certificate search. Other types of data that may be provided in a contact information source

10 that is also a searchable attribute in a certificate server being searched may also be employed in certificate search queries. A combination of different types of queries may also be employed to locate a certificate for a specific contact (e.g. if no certificates are found for a contact using a full name and e-mail address type query, one or more additional queries may be used to progressively broaden the

15 search in an attempt to locate a certificate for the contact). It will be understood by persons skilled in the art that many different variations of search queries and search algorithms may be employed without departing from the scope of the invention.

[0087] At step 440, located certificates resulting from the queries

20 performed at step 430 are downloaded to the computing device. In this embodiment, these certificates are stored temporarily on the computing device, and only a subset of certificates as selected by a user is stored for future use. This allows the user to filter the search results and discard unwanted or irrelevant certificates. However, in a variant implementation, all located certificates may be

25 automatically stored for future use on the computing device at step 440 without being filtered by the user. In this case, the remaining steps of method 400 would not be performed.

[0088] At step 450, a list of located certificates downloaded to the computing device at step 440 is displayed to the user.

- 30 -

- [0089]** At step 460, a subset of certificates may be selected by the user from the list displayed at step 450, to be stored for future use.
- [0090]** At step 470, the certificates selected at step 460 are stored in a certificate store on the computing device.
- 5 **[0091]** While only end entity certificates will typically be searched for and located in this embodiment of the invention, in a variant embodiment, a contact information source may also store information that can be used to locate root and/or intermediate certificates issued to certificate authorities, and the certificate synchronization application may be adapted to search for those certificates.
- 10 **[0092]** In a variant embodiment of the invention, method 400 further comprises a step of filtering out duplicate certificates that have been downloaded to the computing device. The list of located certificates displayed at step 450 may be generated to reflect the filtered results.
- [0093]** In a variant embodiment of the invention, method 400 further
15 comprises steps of determining and filtering out duplicate contacts for the search, prior to querying the designated certificate servers.
- [0094]** Referring to FIG. 7B, a flowchart illustrating steps in a method of searching and retrieving certificates in another embodiment of the invention is shown generally as 400b. Method 400b is similar to method 400, except that this
20 embodiment of the invention applies more specifically to systems in which the computing device is one that can be coupled to a mobile device (e.g. computer 262a to mobile device 100 of FIG. 4). The coupling can be facilitated by a cradle connected to the computing device (e.g. cradle 264 of FIG. 4), although other coupling techniques may be employed in variant implementations.
- 25 **[0095]** In this embodiment of the invention, the certificate search need not be explicitly requested by the user, but instead is automatically initiated upon detecting that the mobile device is coupled to the computing device, as shown at step 420b. Accordingly, at step 430, one of the contact information sources that

- 31 -

can be used in the certificate search is the address book on the mobile device. A certificate synchronization manager residing on the desktop computing device for example, may read entries from the address book on the mobile device, and use the read information to perform the certificate search. Other contact information
5 sources residing on the mobile device may be similarly accessed.

[0096] Furthermore, at step 470b, the certificates selected at step 460 may be stored in a certificate store on the (e.g. desktop) computing device, downloaded to the mobile device coupled to the computing device for storage in a certificate store on the mobile device, or both.

10 **[0097]** In a variant embodiment of the invention, step 420b comprises detecting that the mobile device is coupled to the computing device, but the certificate search is not automatically initiated at this step. Instead, data may be uploaded from one or more contact information sources on the mobile device and stored on the computing device to be retrieved later by the certificate
15 synchronization application, at some future time. Accordingly, data can be retrieved from the mobile device when coupled to the computing device, but the certificate search may be deferred.

[0098] The steps of a method of searching and retrieving certificates in embodiments of the invention may be provided as executable software
20 instructions stored on computer-readable media, which may include transmission-type media.

[0099] The invention has been described with regard to a number of embodiments. However, it will be understood by persons skilled in the art that other variants and modifications may be made without departing from the scope
25 of the invention as defined in the claims appended hereto.

Claims:

1. A method for searching and retrieving certificates associated with one or more contacts, the method comprising the steps of:
 - a) identifying one or more certificate servers to be searched;
 - 5 b) identifying one or more contact information sources, each storing contact information for at least one contact;
 - c) for each contact of at least a subset of the contacts for which contact information is stored in the one or more contact information sources, searching each identified certificate server for certificates
10 associated therewith by submitting at least one query constructed using at least some of the contact information for the respective contact to the respective certificate server, wherein the searching step is performed by a certificate synchronization application;
 - d) for each identified certificate server, downloading certificates
15 satisfying the at least one query submitted thereto, to a computing device; and
 - e) storing at least a subset of certificates downloaded at step d) in one or more certificate stores.
2. The method of claim 1, wherein the certificate synchronization application
20 executes and resides on the computing device.
3. The method of claim 1, wherein at least one of the one or more contact information sources is an address book.
4. The method of claim 1, wherein at least one of the one or more contact information sources resides on a mobile device.
- 25 5. The method of claim 4, wherein step c) is performed when the mobile device is coupled to the computing device.

- 33 -

6. The method of claim 4, wherein at least one of the one or more contact information sources is an address book residing on the mobile device.
7. The method of claim 4, wherein each of the one or more certificate stores is selected from the following group: a certificate store on the computing device;
5 and a certificate store on the mobile device.
8. The method of claim 1, further comprising the steps of: generating a list of certificates identifying at least a subset of certificates downloaded to the computing device at step d); displaying the list to a user; and receiving user selections of selected certificates identified in the list; wherein the at least a
10 subset of certificates stored at step e) comprises the selected certificates.
9. The method of claim 1, further comprising the step of filtering out duplicate downloaded certificates prior to the step e).
10. The method of claim 1, wherein the one or more certificate servers comprises one or more LDAP servers.
- 15 11. A software application comprising a plurality of instructions stored on a computer-readable medium, the instructions for a method of searching and retrieving certificates associated with one or more contacts, the method comprising the steps of:
- 20 a) identifying one or more certificate servers to be searched;
- b) identifying one or more contact information sources, each storing contact information for at least one contact;
- c) for each contact of at least a subset of the contacts for which contact information is stored in the one or more contact information sources, searching each identified certificate server for certificates
25 associated therewith by submitting at least one query constructed using at least some of the contact information for the respective

- 34 -

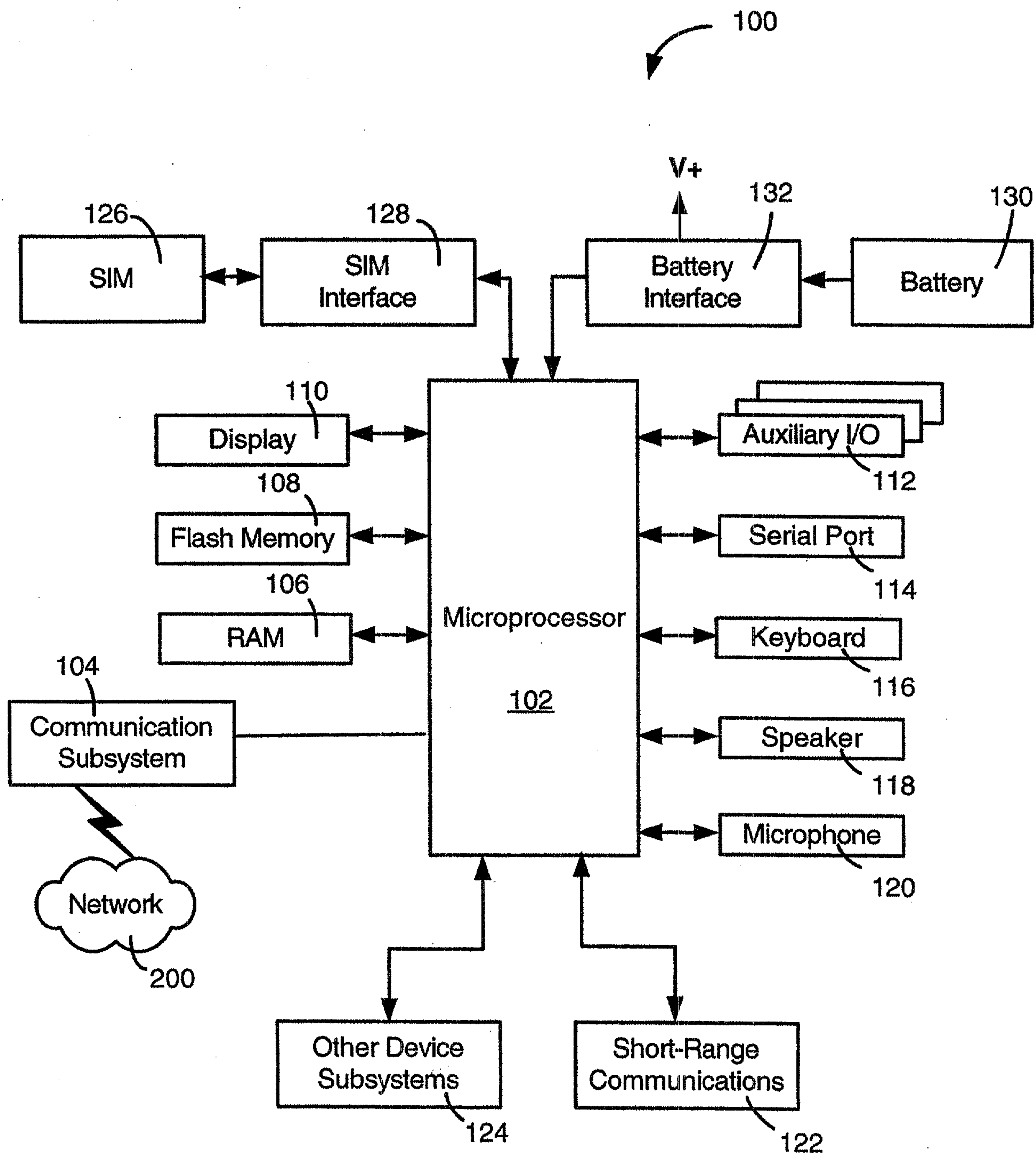
contact to the respective certificate server, wherein the searching step is performed by the software application;

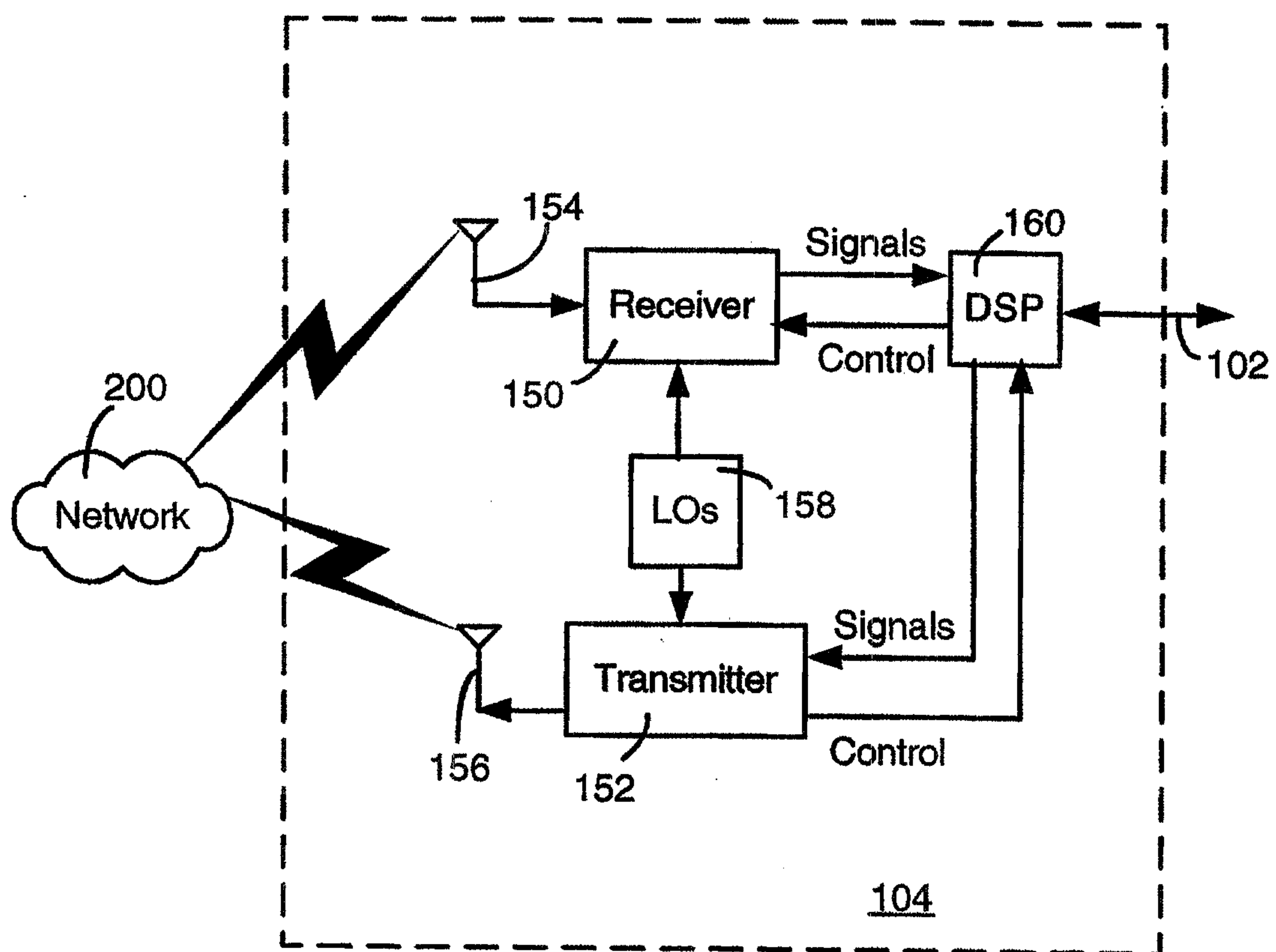
- d) for each identified certificate server, downloading certificates satisfying the at least one query submitted thereto, to a computing device; and
- e) storing at least a subset of certificates downloaded at step d) in one or more certificate stores.

12. A system for searching and retrieving certificates associated with one or more contacts comprising at least one computing device, wherein a certificate synchronization application executes and resides on a computing device of the at least one computing device, the certificate synchronization application programmed to:

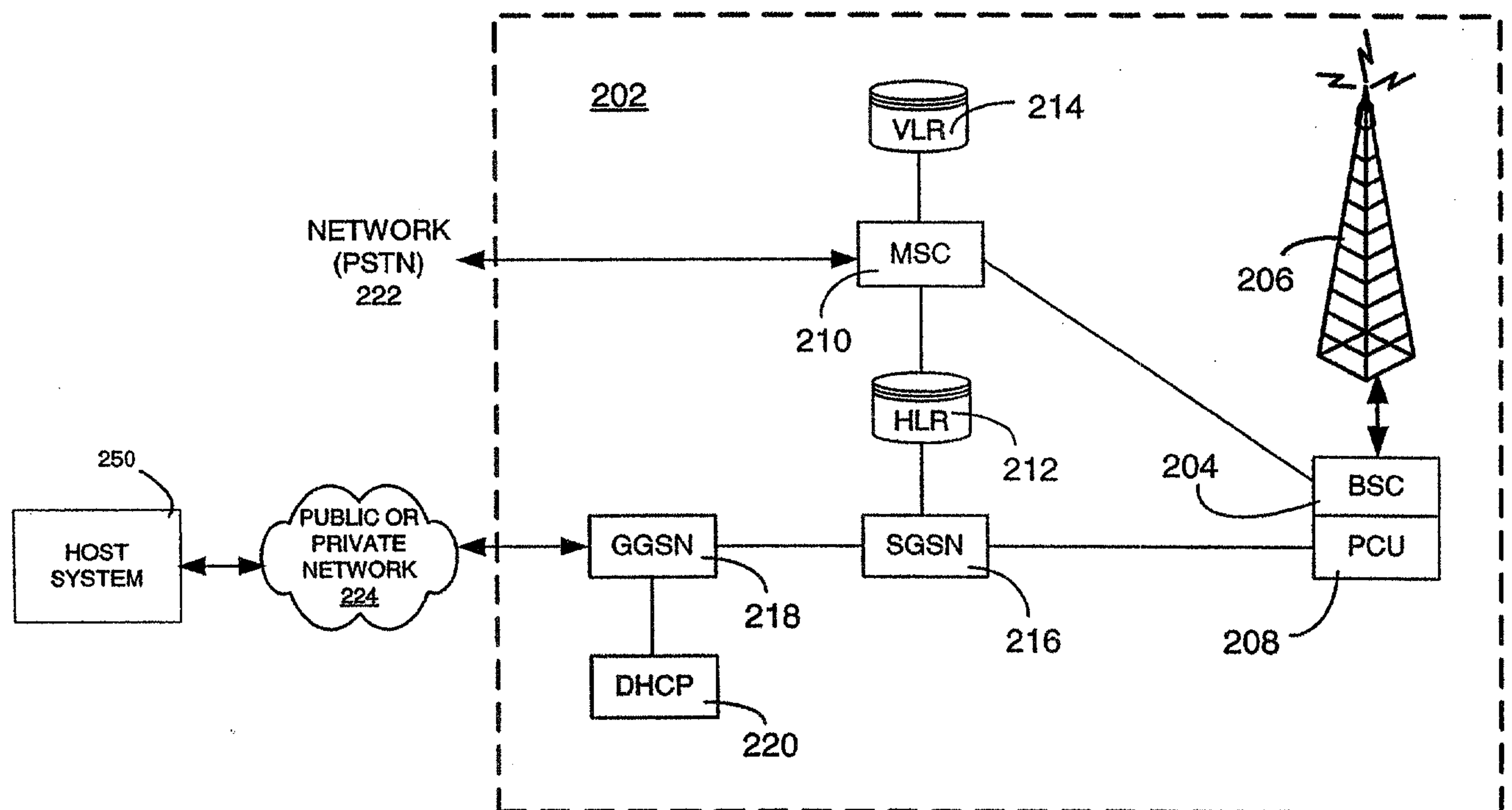
- a) identify one or more certificate servers to be searched;
- b) identify one or more contact information sources, each storing contact information for at least one contact;
- c) for each contact of at least a subset of the contacts for which contact information is stored in the one or more contact information sources, search each identified certificate server for certificates associated therewith by submitting at least one query constructed using at least some of the contact information for the respective contact to the respective certificate server, wherein the searching is performed by the certificate synchronization application;
- d) for each identified certificate server, download certificates satisfying the at least one query submitted thereto, to one of the at least one computing device; and
- e) store at least a subset of downloaded certificates in one or more certificate stores.

1/7

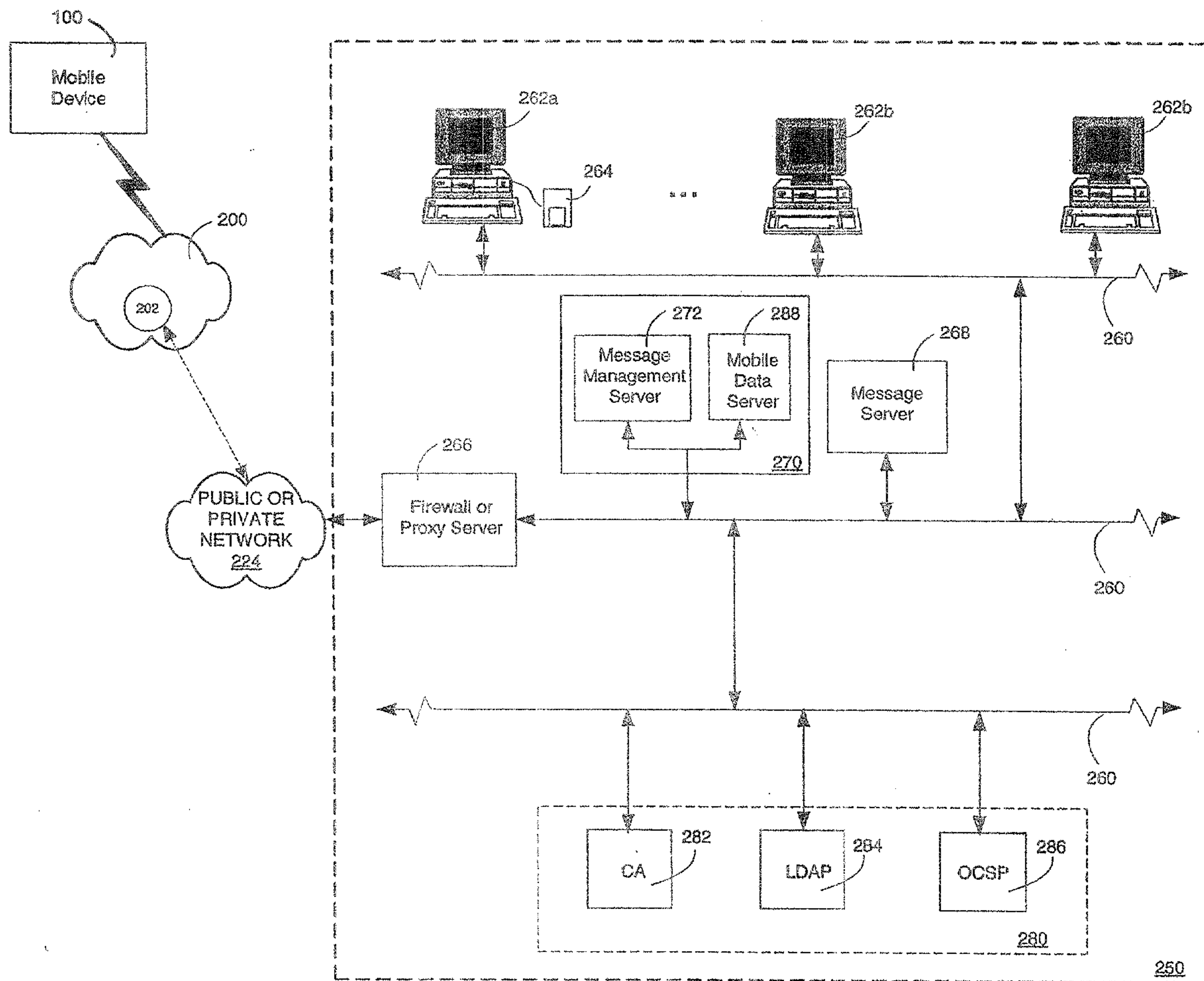
**FIG. 1**

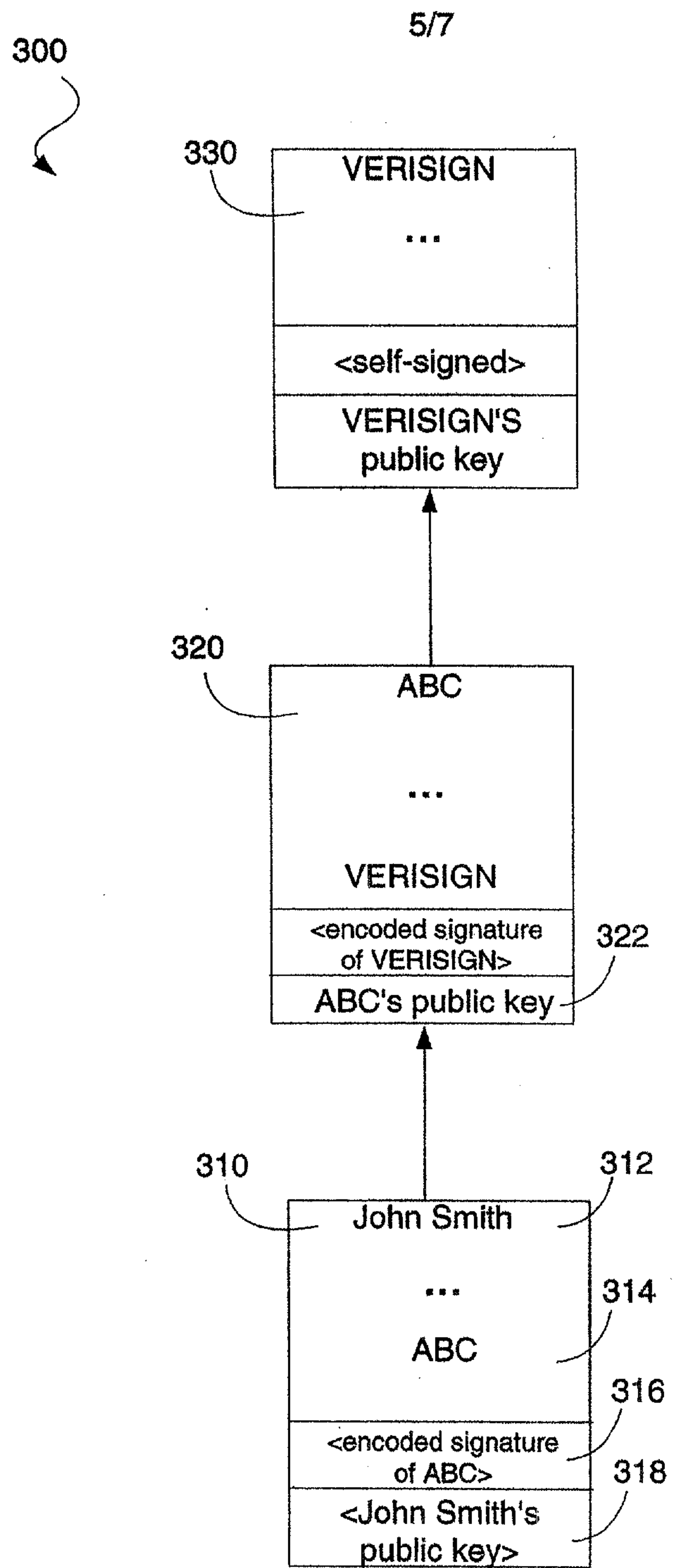
**FIG. 2**

3/7

**FIG. 3**

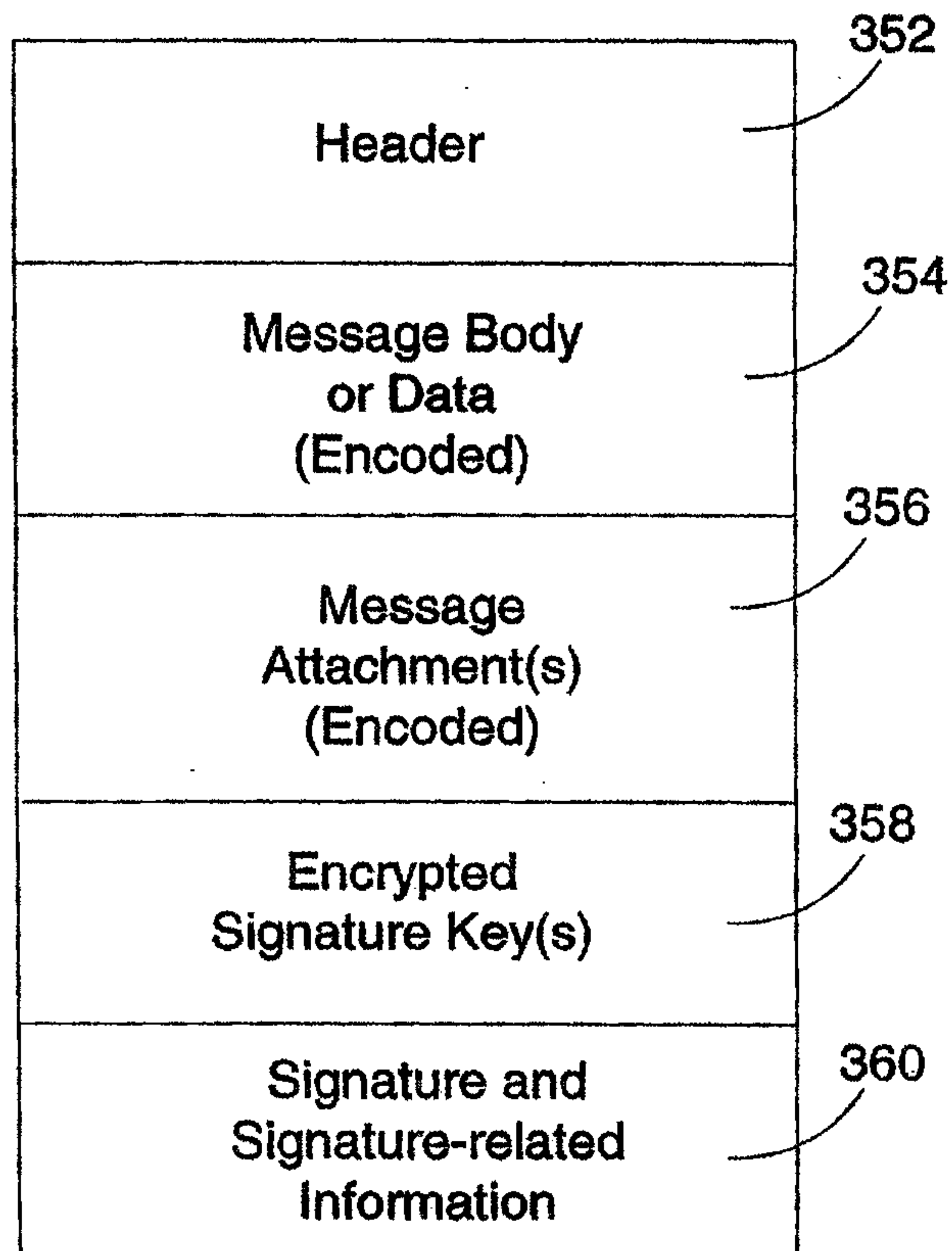
4/7

**FIG. 4**

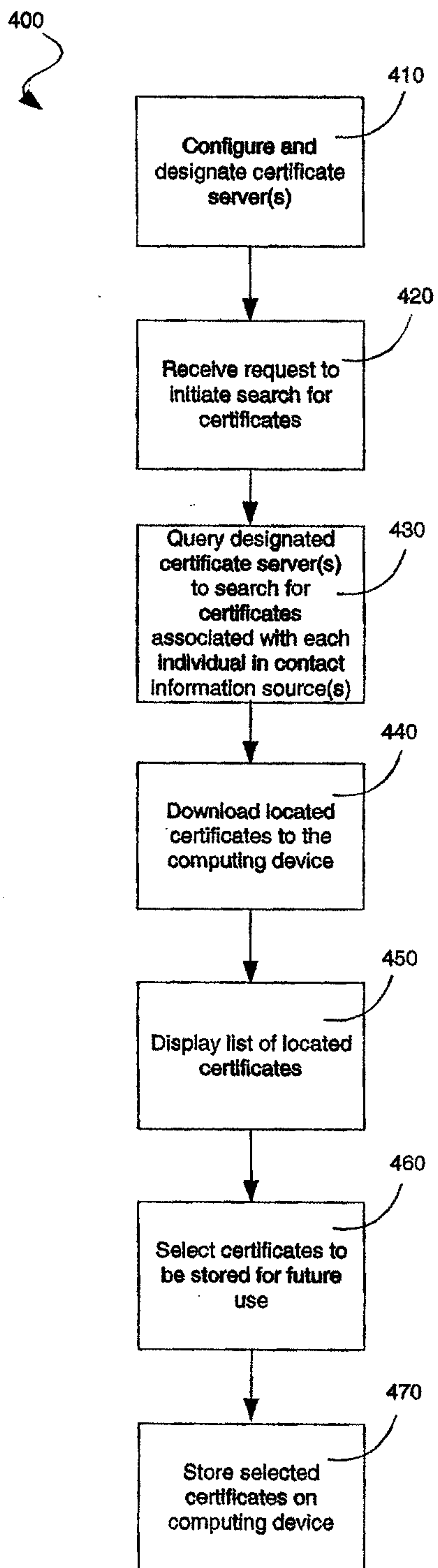
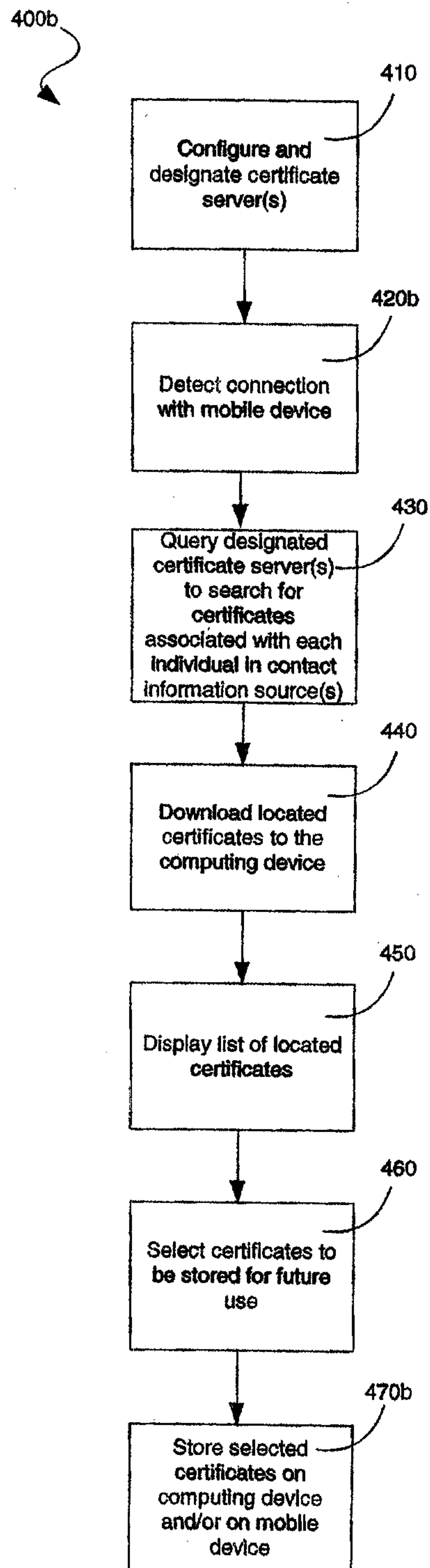
**FIG. 5**

6/7

350

**FIG. 6**

7/7

**FIG. 7A****FIG. 7B**

400

