



(22) Date de dépôt/Filing Date: 2008/08/26

(41) Mise à la disp. pub./Open to Public Insp.: 2009/03/04

(45) Date de délivrance/Issue Date: 2013/05/14

(30) Priorité/Priority: 2007/09/04 (EP07115678.0)

(51) Cl.Int./Int.Cl. *H04W 4/12* (2009.01),
H04L 9/28 (2006.01), *H04W 12/02* (2009.01),
H04W 88/02 (2009.01)

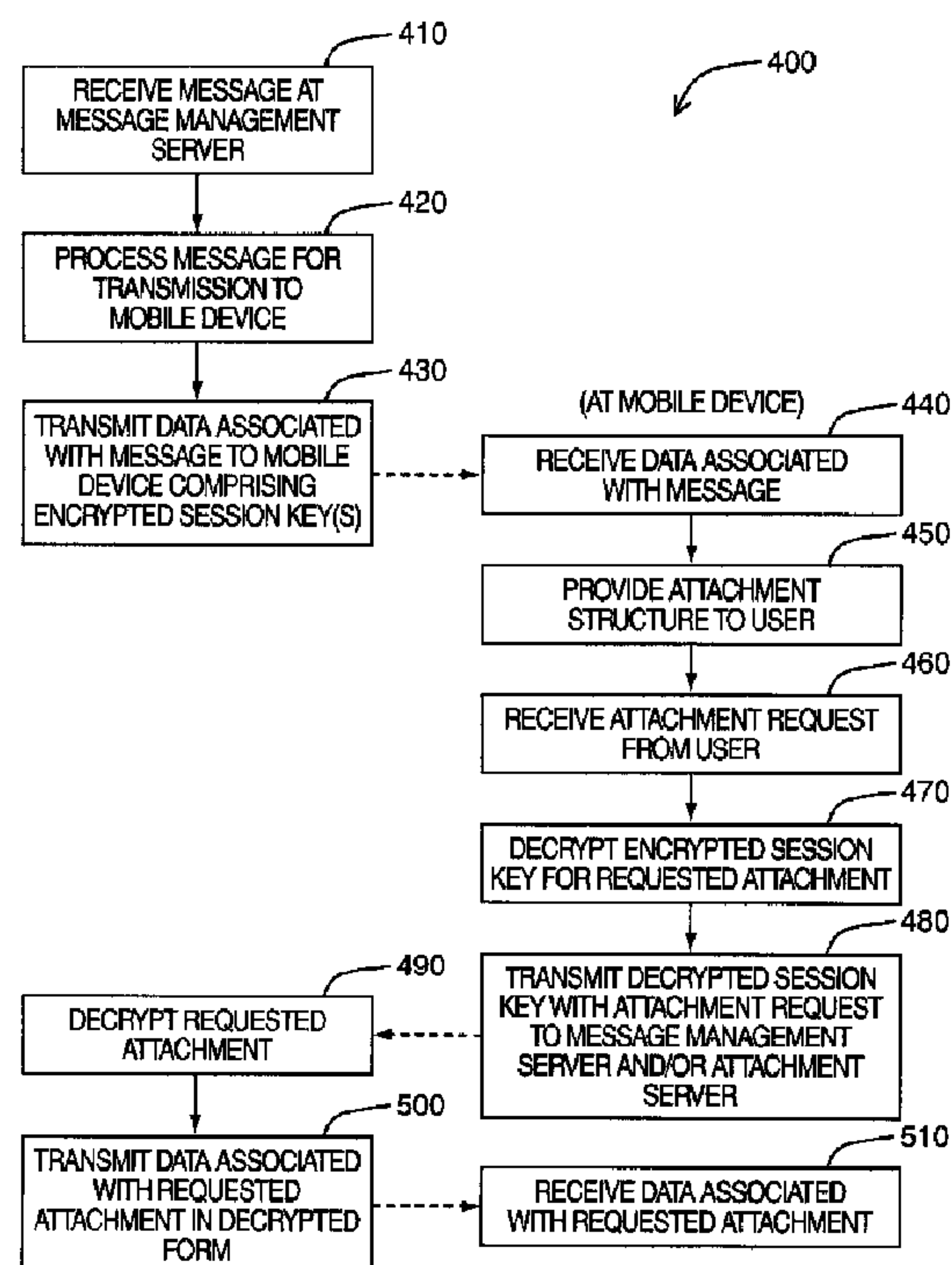
(72) Inventeurs/Inventors:
BROWN, MICHAEL K., CA;
KIRKUP, MICHAEL G., CA;
BROWN, MICHAEL S., CA

(73) Propriétaire/Owner:
RESEARCH IN MOTION LIMITED, CA

(74) Agent: BERESKIN & PARR LLP/S.E.N.C.R.L.,S.R.L.

(54) Titre : SYSTEME ET METHODE DE TRAITEMENT DE PIECES JOINTES AUX MESSAGES ENVOYES A UN
APPAREIL MOBILE

(54) Title: SYSTEM AND METHOD FOR PROCESSING ATTACHMENTS TO MESSAGES SENT TO A MOBILE DEVICE



(57) Abrégé/Abstract:

A system and method for processing attachments to messages sent to a mobile device is described herein. Embodiments described herein apply to encrypted messages comprising multiple message parts, in which different encryption keys (e.g. session keys) have been used to encrypt the different message parts. In at least one example embodiment, the encrypted session keys for every message content part comprising an attachment is received at the mobile device. In one embodiment, all of the encrypted session keys are stored together in a main message header. The mobile device may then decrypt the encrypted session key associated with a user requested attachment, and transmits the decrypted session key to one or more remote servers in an attachment request for use in decrypting the requested attachment. Data associated with the requested attachment, in decrypted form, is returned to the mobile device.



ABSTRACT

A system and method for processing attachments to messages sent to a mobile device is described herein. Embodiments described herein apply to encrypted
5 messages comprising multiple message parts, in which different encryption keys (e.g. session keys) have been used to encrypt the different message parts. In at least one example embodiment, the encrypted session keys for every message content part comprising an attachment is received at the mobile device. In one
10 embodiment, all of the encrypted session keys are stored together in a main message header. The mobile device may then decrypt the encrypted session key associated with a user requested attachment, and transmits the decrypted session key to one or more remote servers in an attachment request for use in decrypting the requested attachment. Data associated with the requested attachment, in decrypted form, is returned to the mobile device.

SYSTEM AND METHOD FOR PROCESSING ATTACHMENTS TO MESSAGES SENT TO A MOBILE DEVICE

[0001] Embodiments described herein relate generally to the processing of messages, such as e-mail messages, and more specifically to a system and
5 method for processing messages with attachments that are sent to a mobile device.

[0002] Many mobile devices are adapted to permit users to view data associated with message attachments, in some form, on their mobile device. Some of these mobile devices are not equipped with native attachment viewers.
10 In those cases, a message attachment is typically processed initially by a remote server. The remote server retrieves and potentially reformats attachment data, which is then transmitted to the mobile device. The data associated with the attachment that is received at the mobile device is in a form suitable for processing by applications residing on the mobile device, and rendered as
15 needed.

[0003] For example, messages addressed to a user of a mobile device may arrive at a message server and may then be routed to a message management server. The message management server is typically configured to convert data associated with a message into a wireless device-friendly format before the
20 message data is transmitted to the mobile device. However, in order to conserve bandwidth, the message management server may also be configured to not send message attachments to the mobile device.

[0004] Instead, the message management server may analyze the message and provide data to the mobile device that indicates the existence of one
25 or more attachments to the message. Subsequently, the user of the mobile device may request a specific attachment. The request is sent to the message management server or an attachment server that is configured to process the message, retrieve the requested attachment, and send data associated with the attachment (e.g. text, images) to the mobile device, typically in a device-friendly
30 format.

General

[0005] In one broad aspect, there may be provided a system and method for processing attachments to messages sent to a mobile device (e.g. mobile device 100 of FIG. 1), the method comprising: after a message addressed to a user of the mobile device is received by one or more remote servers, receiving data associated with the message at the mobile device from the one or more remote servers (e.g. message management server 272 of FIG. 4); wherein the message addressed to the user comprises a plurality of message content parts, at least one of the plurality of message content parts comprising an attachment; wherein each message content part has been encrypted using a different one of a plurality of session keys, and each session key has been encrypted using an encryption key associated with the user; wherein the one or more remote servers (e.g. message management server 274) are configured to initially withhold transmission of data associated with an attachment to the mobile device, and transmit data associated with the attachment to the mobile device only if a request therefor is received; and wherein the data received at said receiving comprises data identifying an attachment structure for the message, and further comprises an encrypted session key for at least one message content part comprising an attachment; and outputting the attachment structure (e.g. to the user of the mobile device).

Brief Description of the Drawings

[0006] For a better understanding of embodiments described herein, and to show more clearly how they may be carried into effect, reference will now be made, by way of example, to the accompanying drawings in which:

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 example configuration;

FIG. 5 is a block diagram illustrating components of an example of an encrypted message comprising a plurality of message content parts; and

FIG. 6 is a flowchart illustrating steps in a method of processing attachments to a message sent to a mobile device in accordance with at least one embodiment.

Description of Preferred Embodiments

- 5 **[0007]** Some embodiments described herein make use of a mobile station. A mobile station generally comprises a two-way communication device with advanced data communication capabilities having the capability to communicate with other devices, and is also referred to herein generally as a mobile device. A mobile device may also include the capability for voice communications.
- 10 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 device (with or without telephony capabilities). A mobile device may communicate with other devices through a network of transceiver stations.
- 15 **[0008]** 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 through 3.
- 20 **[0009]** 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 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
- 25 one example implementation of mobile device 100, communication subsystem 104 may be configured in accordance with the Global 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 may be supplemented or superseded eventually by newer standards
- 30 such as Enhanced Data GSM Environment (EDGE), Universal Mobile Telecommunications Service (UMTS), and Ultra Mobile Broadband (UMB), etc. New standards are still being defined, but it is believed that they will have similarities to the network behaviour described herein, and it will also be

understood by persons skilled in the art that the embodiments of the present disclosure are 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 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.

[0010] Although the wireless network associated with mobile device 100 is a GSM/GPRS wireless network in one example implementation of mobile device 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 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™ Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM and Time Division Multiple Access (TDMA) systems.

[0011] Other network communication technologies that may be employed include, for example, Integrated Digital Enhanced Network (iDEN™), Evolution-Data Optimized (EV-DO), and High Speed Packet Access (HSPA), etc.

[0012] Microprocessor 102 also interacts with additional subsystems such as a Random Access Memory (RAM) 106, flash memory 108, display 110, auxiliary input/output (I/O) subsystem 112, serial port 114, keyboard 116, speaker 118, microphone 120, short-range communications subsystem 122 and other subsystems 124.

[0013] Some of the subsystems of mobile device 100 perform communication-related functions, whereas other subsystems may provide “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 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.

[0014] 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 may provide for a Subscriber Identity Module ("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. By inserting SIM 126 into SIM interface 128, a subscriber can access all subscribed services. Services may include without limitation: web browsing and messaging such as e-mail, voice mail, instant messaging, peer-to-peer messaging, Short Message Service (SMS), and Multimedia Messaging Services (MMS). More advanced services may include without limitation: point of sale, field service and sales force automation. SIM 126 includes a processor and memory 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 additional subscriber information for a mobile device as well, including datebook (or calendar) information and recent call information.

[0015] Mobile device 100 may be a battery-powered device and may include a battery interface 132 for receiving one or more rechargeable batteries 130. Battery interface 132 may be coupled to a regulator (not shown), which assists battery 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. In some embodiments, mobile device 100 may be solar-powered.

[0016] Microprocessor 102, in addition to its operating system functions, enables execution of software applications on mobile device 100. A set of applications that control basic device operations, including data and voice communication applications, may be installed on mobile device 100 during its manufacture. Another application that may be loaded onto mobile device 100 is a personal information manager (PIM). A PIM has 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 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.

[0017] 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 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.

[0018] Serial port 114 enables a subscriber to set preferences through an external device or software application and extends the capabilities of mobile 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.

[0019] 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 include standards developed by the Infrared Data Association (IrDA), Bluetooth, and the 802.11 family of standards (Wi-Fi®) developed by IEEE.

[0020] In use, a received signal such as a text message, an e-mail message, or web page download is processed by communication subsystem 104
10 and input to microprocessor 102. Microprocessor 102 then processes 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 devices such
15 as: a touch screen, mouse, track ball, infrared fingerprint detector, or a roller wheel with dynamic button pressing capability. Keyboard 116 may comprise an alphanumeric keyboard and/or telephone-type keypad. A composed item may be transmitted over network 200 through communication subsystem 104.

[0021] For voice communications, the overall operation of mobile device
20 100 is substantially similar, except that the received signals may be processed and output to speaker 118, and signals for transmission may 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
25 118, 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.

[0022] Referring now to FIG. 2, a block diagram of the communication
subsystem component 104 of FIG. 1 is shown. Communication subsystem 104
30 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.

[0023] 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
5 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
10 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
15 gains applied to communication signals in receiver 150 and transmitter 152 may be adaptively controlled through automatic gain control algorithms implemented in DSP 160.

[0024] The wireless link between mobile device 100 and a network 200 may contain one or more different channels, typically different RF channels, and
20 associated protocols used between mobile device 100 and network 200. A RF channel is a limited resource, typically due to limits in overall bandwidth and limited battery power of mobile device 100.

[0025] When mobile device 100 is fully operational, transmitter 152 may be typically keyed or turned on only when it is sending to network 200 and may
25 otherwise be turned off to conserve resources. Similarly, receiver 150 may be periodically turned off to conserve power until it is needed to receive signals or information (if at all) during designated time periods.

[0026] 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
30 202. 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 GPRS and GSM technologies; however, in other embodiments, different standards may be implemented as discussed in more detail above.

Node 202 includes a base station controller (BSC) 204 with an associated tower station 206, a Packet Control Unit (PCU) 208 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 node 202 within a GSM/GPRS network, but rather a list of components that are commonly used in communications through network 200.

10 **[0027]** 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 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
15 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 satisfy packet switched requirements. To track mobile device location and availability for both circuit switched and packet switched management, HLR 212 is
20 shared between MSC 210 and SGSN 216. Access to VLR 214 is controlled by MSC 210.

[0028] 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
25 referred to as a "cell". The fixed transceiver equipment transmits communication 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
30 predetermined, communication protocols and parameters, under control of its 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.

[0029] 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 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 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.

[0030] SGSN 216 and GGSN 218 are elements added for GPRS support; namely packet switched data support, within GSM. SGSN 216 and MSC 210 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 performs a "GPRS Attach" to acquire an IP address and to access data services. This normally is not present in circuit switched voice channels as Integrated Services Digital Network (ISDN) addresses are used for routing incoming and outgoing calls. Currently, 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
5 APN may be considered to be similar to an Internet domain name such as "myconnection.wireless.com".

[0031] 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
10 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 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
15 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 220.

[0032] 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
20 be a home office computer or some other private system, for example, in variant 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.

[0033] LAN 250 comprises a number of network components connected to each other by LAN connections 260. For instance, a user's desktop computer
25 262a with an accompanying cradle 264 for the user's mobile device 100 is 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
30 device. Cradle 264 facilitates the loading of information (e.g. PIM data, private 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. The information downloaded to mobile device 100 may include certificates used in 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.

5 4.

[0034] Furthermore, 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 generally, LAN 250 may represent a
10 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.

[0035] In this example, mobile device 100 communicates with LAN 250 through a node 202 of wireless network 200 and a shared network infrastructure
15 224 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.

[0036] In a variant implementation, LAN 250 comprises a wireless VPN router [not shown] to facilitate data exchange between the LAN 250 and mobile
20 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
25 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 may include, for example, a
30 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.

[0037] Messages intended for a user of mobile device 100 are initially received by a message server 268 of LAN 250. Such messages may originate 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
5 [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 messages, via the shared network infrastructure 224, and possibly through an application service provider (ASP) or Internet service provider (ISP), for example.

[0038] Message server 268 typically acts as the primary interface for the
10 exchange of messages, particularly e-mail messages, within the organization and over the shared network infrastructure 224. Each user in the organization that 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
15 comprise multiple message servers 268. Message server 268 may also be adapted to provide additional functions beyond message management, including the management of data associated with calendars and task lists, for example.

[0039] When messages are received by message server 268, they are typically stored in a message store [not explicitly shown], from which messages
20 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 messages associated with that user's account stored on message server 268. These messages may then typically be retrieved from message server 268 and stored locally on computer 262a.

[0040] 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 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
25 organization's information technology (IT) policy) to make this request at the 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
30

100 are automatically redirected to mobile device 100 as they are received by message server 268.

[0041] To facilitate the 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 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 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.

[0042] For example, message management server 272 may: monitor the user's "mailbox" (e.g. the message store associated with the user's account on 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 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.

[0043] 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 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.

[0044] Message management server 272 may also be adapted to provide 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 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.

[0045] Accordingly, message management server 272 facilitates better 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.

[0046] It will be understood by persons skilled in the art that message management server 272 need not be implemented on a separate physical server 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 is supported.

[0047] Embodiments described herein generally related to the processing of encoded messages, such as e-mail messages that are encrypted. 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 standards and protocols may be employed to

facilitate secure message communication, such as Pretty Good Privacy™ (PGP) and variants of PGP such as OpenPGP, for example. It will be understood that where reference is generally made to “PGP” herein, the term is intended to encompass any of a number of variant implementations based on the more
5 general PGP scheme.

[0048] Secure messaging protocols such as S/MIME and PGP-based protocols rely on public and private encryption keys to provide confidentiality and integrity. Data encoded using a private key of a private key/public key pair can only be decoded using the corresponding public key of the pair, and data encoded
10 using a public key of a private key/public key pair can only be decoded using the corresponding private key of the pair. It is intended that private key information never be made public, whereas public key information may be shared.

[0049] 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
15 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
20 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 message. Other encryption techniques based on public key cryptography may be used in variant implementations. However, in each of these cases, only the
25 recipient’s private key may be used to facilitate decryption of the message, and in this way, the confidentiality of messages can be maintained.

[0050] As a further example, a sender may sign a message using a digital signature. A digital signature generally comprises a digest of the message (e.g. a hash of the message) encoded using the sender’s private key, which can then be
30 appended to the outgoing message. To verify the digital signature of the message when received, the recipient uses the same technique as the sender (e.g. using the same standard hash algorithm) to obtain a digest of the received message. The recipient also uses the sender’s public key to decode 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 originate from the sender whose public key was used for verification. Digital
5 signature algorithms are designed in such a way that only someone with knowledge of the sender's private key should be able to encode a signature that the recipient will decode correctly using the sender's public key. Therefore, by verifying a digital signature in this way, authentication of the sender and message integrity can be maintained.

10 **[0051]** An encoded message may be encrypted, signed, or both encrypted and signed. Where used in this disclosure, "signed and/or encrypted" means signed or encrypted or both. The authenticity of public keys used in these operations may be validated using certificates. A certificate is a digital document issued by a certificate authority (CA). Certificates are used to authenticate the
15 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 an accepted standard (e.g. X.509).

[0052] In PGP-based systems, a PGP key is used, which is like an S/MIME
20 certificate in that it contains public information including a public key and information on the key holder or owner. Unlike S/MIME certificates, however, PGP keys are not generally issued by a certificate authority, and the level of trust in the authenticity of a PGP key typically requires verifying that a trusted individual has vouched for the authenticity of a given PGP key.

25 **[0053]** 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). In order that signed messages received from senders may be read from mobile device 100 and encrypted
30 messages be sent to those senders, mobile device 100 is adapted to store public keys (e.g. in S/MIME certificates, PGP keys) of other individuals. Keys stored on a user's computer 262a may be downloaded from computer 262a to mobile device 100 through cradle 264, for example.

[0054] 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 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 may be exchanged between the computer 262a and mobile device 100 so that the user may share one identity and one method for accessing messages.

[0055] User computers 262a, 262b can obtain S/MIME certificates and PGP keys from a number of sources, for storage on computers 262a, 262b and/or mobile devices (e.g. mobile device 100), in a key store, for example. The sources of these certificates and keys may be private (e.g. dedicated for use within an organization) or public, may reside locally or remotely, and may be accessible from within an organization's private network or through the Internet, for example. In the example shown in FIG. 4, multiple public key infrastructure (PKI) servers 280 associated with the organization reside on LAN 250. PKI servers 280 include a CA (certificate authority or certification authority) server 282 for issuing S/MIME certificates, a Lightweight Directory Access Protocol (LDAP) server 284 used to search for and download certificates and/or PGP keys (e.g. for individuals within the organization), and an Online Certificate Status Protocol (OCSP) server 286 used to verify the revocation status of S/MIME certificates, for example.

[0056] Certificates and/or PGP keys 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 device 100 may search for and retrieve individual certificates and PGP keys 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 S/MIME certificates.

[0057] 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).

[0058] 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.

[0059] Other sources of certificates and PGP keys [not shown] may include
5 a Windows® certificate or key store, another secure certificate store on or outside LAN 250, and smart cards, for example.

[0060] Embodiments of the system and method described herein are generally applicable to encrypted messages comprising multiple message parts, in which different encryption keys (e.g. session keys) have been used to encrypt
10 the different message parts. Such encrypted messages may be formatted in accordance with a protocol that permits different message parts to be encrypted with different encryption keys, such as a PGP Partitioned encoding format, for example. One example of such a message is shown in FIG. 5.

[0061] Referring to FIG. 5, a block diagram illustrating components of an
15 example of an encrypted message, as may be received by a message server (e.g. message server 268 of FIG. 4), is shown generally as 350.

[0062] In the present example, encrypted message 350 includes various message parts. For example, encrypted message 350 includes a main message header part 352, wherein header portion 352 typically includes addressing
20 information such as "To", "From", and "CC" addresses, and may also include message length indicators, and sender encryption and signature scheme identifiers, for example.

[0063] Encoded message 350 may also include a message body part 356 containing message content. Encoded message 350 may also include a first
25 attachment 360 to message 350. Encoded message 350 may also include a second attachment 364 to message 350. Encoded message 350 may also include a footer (not shown).

[0064] Encoded message 350 may also include a session key 354 provided within, for example, the data contained in message body part 356, where session
30 key 354 has been used to encrypt data in message body part 356 and has subsequently been encrypted with an encryption key associated with the user (e.g. a public key of a public key/private key pair associated with the user). Session key 354 will typically immediately precede the data of message body part

356 in encoded message 350. However, session key 354 is shown separately from message body part 356 in FIG. 5 to facilitate understanding of this example.

[0065] Encoded message 350 may also include a first attachment-specific session key 358 provided within, for example, the data contained in the message part comprising the first attachment 360, where the first attachment-specific session key 358 has been used to encrypt the first attachment 360 and has subsequently been encrypted with the encryption key associated with the user. Attachment-specific session key 358 will typically immediately precede the data of the first attachment 360 in encoded message 350. However, attachment-specific session key 358 is shown separately from the data of the first attachment 360 in FIG. 5 to facilitate understanding of this example.

[0066] Encoded message 350 may also include a second attachment-specific session key 362 provided within, for example, the data contained in the message part comprising the second attachment 364, where the second attachment-specific session key 362 has been used to encrypt the second attachment 364 and has subsequently been encrypted with the encryption key associated with the user. Attachment-specific session key 362 will typically immediately precede the data of the second attachment 364 in encoded message 350. However, attachment-specific session key 362 is shown separately from the data of the second attachment 364 in FIG. 5 to facilitate understanding of this example.

[0067] Persons skilled in the art will understand that the example message 350 is provided for illustrative purposes only, and that different messages may have a fewer or a greater number of components than shown in FIG. 5. For example, a message may have no attachments. Alternatively, the message may have only one attachment, two attachments as shown, or more than two attachments. For each attachment, an associated session key may or may not be provided for the respective attachment. As a further example, the message body itself may comprise multiple message parts. For each message part of the message body, an associated session key may or may not be provided for the respective message part of the message body. The message may also comprise signature and signature-related information (not shown). It will also be understood by persons skilled in that art that if the message has multiple

recipients, there may be multiple encrypted session keys associated with a given message part (e.g. a message body part and/or an attachment), with typically one encrypted session key being provided for each recipient.

[0068] Known systems are generally adapted to deal only with messages which provide a single session key per message (e.g. a typical S/MIME message), and not with messages comprising multiple message parts encrypted with different session keys (e.g. PGP Partitioned messages). For example, if an encrypted PGP Partitioned message is received at a mobile device not equipped with an on-device attachment viewer, the user will not be able to view attachments to the message that it might receive at the mobile device using the same methods as it would to view attachments to an encrypted S/MIME message.

[0069] Consider the previous example where a message management server analyzes a message for attachments. Suppose that the mobile device is not equipped with an attachment viewer. The message management server does not send any attachments to the message directly. Instead, the message management server provides data to the mobile device that indicates the existence of one or more attachments to the message. The user can then consider this data (i.e. the message's "attachment structure") and subsequently request data associated with a specific attachment that can be rendered on the mobile device.

[0070] Where the message comprises multiple attachments that have been encrypted using different encryption keys (e.g. as in a PGP partitioned message), it may be possible for the message management server to determine the general attachment structure for the message even though it cannot decrypt the attachments themselves or view the contents of those attachments.

[0071] When data associated with a specific attachment is requested by the user, the attachment will need to be decrypted. To facilitate this, one or more remote servers (e.g. a message management server and/or attachment server) may be provided with a copy of the mobile device user's private key, so that the session key for the specific attachment can be decrypted, and the data associated with the attachment retrieved as required. However, as this would involve control of the private key to be relinquished by the user, the security risks associated with such an implementation would generally be considered undesirable. Moreover, in

some circumstances, the private key simply cannot be sent to the server. For example, if the key is stored on a smart card, it cannot be copied from the physical card.

[0072] At least some embodiments described herein relate generally to a system and method wherein encrypted session keys for at least one attachment to a message are transmitted from a remote server to a mobile device. The session key for a user requested attachment can be decrypted at the mobile device, and the decrypted session key can be transmitted by the mobile device to a remote server so that the message can be processed in order to retrieve data associated with the user requested attachment. Data associated with the user-requested attachment in a form that can be rendered at the mobile device is then transmitted to the mobile device. These embodiments may be particularly applicable to mobile devices that do not provide for an on-device ("native") attachment viewer capable of processing message attachments in their original form within a received message, although they may be applied for use with other mobile devices as well.

[0073] In one broad aspect, there is provided a system and method for processing attachments to messages sent to a mobile device (e.g. mobile device 100 of FIG. 1), the method comprising: after a message addressed to a user of the mobile device is received by one or more remote servers, receiving data associated with the message at the mobile device from the one or more remote servers (e.g. message management server 272 of FIG. 4); wherein the message addressed to the user comprises a plurality of message content parts, at least one of the plurality of message content parts comprising an attachment; wherein each message content part has been encrypted using a different one of a plurality of session keys, and each session key has been encrypted using an encryption key associated with the user; wherein the one or more remote servers (e.g. message management server 274) are configured to initially withhold transmission of data associated with an attachment to the mobile device, and transmit data associated with the attachment to the mobile device only if a request therefor is received; and wherein the data received at said receiving comprises data identifying an attachment structure for the message, and further comprises an encrypted

session key for at least one message content part comprising an attachment; and outputting the attachment structure (e.g. to the user of the mobile device).

[0074] In another broad aspect, the data received at said receiving comprises the encrypted session key for every message content part comprising an attachment.

[0075] In another broad aspect, the method further comprises: receiving an attachment request at the mobile device, the attachment request identifying an attachment to the message; decrypting the encrypted session key at the mobile device for the message content part comprising the attachment identified in the attachment request to determine a decrypted session key; transmitting the decrypted session key with the attachment request from the mobile device to the one or more remote servers (e.g. message management server 272 and /or an attachment server [not explicitly shown in FIG. 4]); wherein the one or more remote servers are configured to retrieve the attachment identified in the attachment request by decrypting the message content part comprising the attachment identified in the attachment request using the decrypted session key, and to transmit data associated with the attachment in decrypted form to the mobile device; and receiving data associated with the attachment identified in the attachment request in decrypted form at the mobile device.

[0076] In another broad aspect, the message addressed to the user comprises a main message header, wherein the data identifying an attachment structure for the message and the encrypted session key for each message content part comprising an attachment have been stored in the main message header; and wherein the data associated with the message received at the mobile device comprises data stored in the main message header. In one example embodiment, the one or more remote servers (e.g. message management server 272) are configured to retrieve, for the message addressed to a user of the mobile device received by the one or more remote servers, an encrypted session key for each message content part comprising an attachment, and to store each encrypted session key in the main message header. In another example embodiment, the encrypted session key for each message content part comprising an attachment has been stored in the main message header at a sender's computing device from which the message originates.

[0077] In another broad aspect, the message addressed to the user comprises a main message header and at least one message part associated with each message content part comprising an attachment, wherein an encrypted session key for each message content part comprising an attachment has been
5 stored in the associated one of the at least one message part, and wherein at least one encrypted session key is received at the mobile device.

[0078] In another broad aspect, the message is more specifically a message formatted in accordance with a format in which each encrypted attachment has a different session key, such as, for example, a PGP Partitioned
10 encoding format.

[0079] These and other aspects and features of various embodiments will be described in greater detail below.

[0080] Referring now to FIG. 6, a flowchart illustrating steps in a method of processing attachments to a message sent to a mobile device in accordance with
15 at least one embodiment is shown generally as 400. Additional details of some of the features described below in respect of the steps of method 400 have been described earlier in the present description.

[0081] To facilitate better understanding of the flow of method steps of method 400, certain steps may be performed remotely from a mobile device and
20 other steps may be performed at the mobile device (e.g. mobile device 100 of FIG. 1). In one embodiment, at least some of these steps performed at the mobile device are performed by a messaging application that executes and resides on the mobile device. The messaging application need not be a stand-alone application, and the functionality of the messaging application may be
25 implemented in one or more applications executing and residing on the mobile device.

[0082] At step 410, a message addressed to a user of the mobile device is received by one or more remote servers. In one example embodiment, the one or more remote servers comprise a message management server (e.g. message
30 management server 272 of FIG. 4). The message is of the type that comprises multiple message content parts, wherein each message content part has been encrypted (e.g. at a sender's computing device from which the message originates) with a different one of a plurality of session keys, and wherein each

session key was then subsequently encrypted with an encryption key associated with the recipient (i.e. with the user of mobile device 100 in this example).

[0083] The encryption key associated with the user that is used to encrypt the session keys is typically a public key associated with the user. However, in
5 variant embodiments, a symmetric key may be employed.

[0084] By way of example, the message received at step 410 may be similar to message 350 as described with reference to FIG. 5. For example, the message may be a PGP Partitioned message.

[0085] At step 420, the message management server processes the
10 message to prepare the message for transmission to the mobile device, and data associated with the message as a result of the processing is then transmitted to the mobile device at step 430. By way of example, data associated with the message as transmitted to the mobile device may be provided as one or more data blocks.

15 **[0086]** As previously noted, in various embodiments described herein, attachments (in their original form in the received message) are not sent to the mobile device at step 430. The message management server is configured to initially withhold transmission of attachments to the mobile device. Data associated with an attachment (e.g. in a form that does not require the mobile
20 device to be equipped with a native attachment viewer) is transmitted to the mobile device if a request for the data by way of an attachment request is received from the user.

[0087] However, where the message comprises multiple separately encrypted message parts, it may be possible to determine a general attachment
25 structure for the message. Data identifying the attachments (e.g. a file name) as may be provided in a message part headers associated with the attachments may be used to facilitate a determination of the attachment structure that may be made when processing the message at step 420.

[0088] The data transmitted to the mobile device at step 430 comprises
30 data identifying the attachment structure. The data transmitted at step 430 further comprises an encrypted session key for each message content part that comprises an attachment. Typically, the data transmitted at step 430 will also

comprise data associated with a main message header, an encrypted message body and the associated encrypted session key.

[0089] In some instances, not all of the encrypted session keys for every message content part that comprises an attachment may have been transmitted to the mobile device at step 430, due to data transmission limits for example. In that event, if an attachment is later requested by the user for which the associated encrypted session key has not yet been transmitted to the mobile device, the associated encrypted session key may be required to first be transmitted to the mobile device for decryption (step not shown).

[0090] In one example embodiment, in processing the message at step 420, the message management server retrieves the encrypted session key for each message content part comprising an attachment, and optionally, the encrypted session key associated with the message body. All of the retrieved keys are stored in a main message header, which is transmitted to the mobile device at step 430. Accordingly, all of the encrypted session keys for the message content parts that comprise an attachment may then be typically received at the mobile device, even if the mobile device receives only a small part of the entire message, as data in the main message header is typically provided before other message data when message data is transmitted from the message management server to the mobile device.

[0091] In another example embodiment, the message management server need not process the message to retrieve the encrypted session keys for storage in the main message header when the encrypted session keys for each message content part comprising an attachment have already been pre-stored in the main message header. The encrypted session keys may have been pre-stored in the main message header at a sender's computing device from which the message received at step 410 originates.

[0092] In another example embodiment, the encrypted session keys for each message content part comprising an attachment may be placed within associated individual message parts, each individual message part immediately preceding or contained within the respective message content part, when data for the message is transmitted to the mobile device at step 430. In this manner, the

encrypted session keys are transmitted in an order reflecting their original positions within the message, as received by the mobile device.

[0093] At step 440, the data that is transmitted by the message management server at step 430 is received at the mobile device.

5 **[0094]** At step 450, the attachment structure for the message is provided as output to the user based on the data received at step 440. The user may be informed of the attachment structure through the use of a messaging application.

[0095] In use, if after considering the attachment structure, the user wishes to request a specific attachment for the message, steps 460 to 510 are performed.

10 **[0096]** At step 460, an attachment request that identifies one or more requested attachments is received from the user.

[0097] At step 470, the encrypted session key associated with each requested attachment as identified in the attachment request is decrypted. A private key associated with the user, which typically resides on the mobile device,
15 may be used for this purpose, where the encrypted session keys of the message have been encrypted (e.g. at the sender's computing device) using the corresponding public key associated with the user.

[0098] In a variant embodiment, the encrypted session key may be decrypted with a symmetric key at step 470, where the encrypted session keys of
20 the message have been encrypted (e.g. at the sender's computing device) using a symmetric key.

[0099] At step 480, each session key decrypted at step 470 is transmitted with the attachment request to one or more remote servers. For example, the attachment request may be transmitted to an attachment server, either directly or
25 via another remote server such as the message management server. In variant embodiments, the functions of the attachment server may be provided by the message management server.

[00100] At step 490, the attachment request is received by the one or more remote servers, and the requested attachment(s) are decrypted using the
30 decrypted session key(s) received from the mobile device.

[00101] At step 500, decrypted data associated with the requested attachment(s) is transmitted to the mobile device, and subsequently received at the mobile device at step 510. The data transmitted by the one or more remote

servers and received at the mobile device is typically device-friendly, and may be provided as text and images that can be processed by a messaging application residing and executing on the mobile device for rendering to a user.

[00102] In one example embodiment, the message management server may
5 decrypt the requested attachment(s) at step 490, and then forward the decrypted attachment(s) to an attachment server for further processing, in order to generate data associated with the attachment(s) in a format suitable for rendering on the mobile device (e.g. a mobile device not equipped with a native attachment viewer).

10 **[00103]** In variant embodiments, the decryption of attachments and the subsequent processing thereof may be performed by the same server.

[00104] In the case where a message is addressed to a plurality of recipients, there may be a plurality of encrypted session keys associated with each message content part. For example, there may be one encrypted session
15 key per recipient for each message content part. In such a case, the message management server may transmit all encrypted session keys for each part to the mobile device, and allow the mobile device to determine which of the encrypted session keys it is capable of decrypting. Alternatively, if the message management server has knowledge of which private keys are stored on the
20 mobile device, it may choose to send only one or more of the encrypted session keys that were encrypted with public keys corresponding to the private keys stored on the mobile device.

[00105] Persons skilled in the art will understand that certain steps of method 400 may be repeated. For example, method 400 may be repeated when
25 another message intended for a user of the mobile device is to be processed. As a further example, steps 460 to 510 may be repeated when the user submits a further attachment request in respect of the same message for which an attachment request was previously made.

[00106] The steps of a method of processing attachments in accordance
30 with any of the embodiments described herein may be provided as executable software instructions stored on computer-readable media, which may include transmission-type media.

[00107] As used herein, the wording “and/or” is intended to represent an inclusive-or. That is, “X and/or Y” is intended to mean X or Y or both. Moreover, “X, Y, and/or Z” is intended to mean X or Y or Z or any combination thereof.

[00108] The present disclosure has been described with regard to a number
5 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 of the invention as defined in the claims appended hereto.

CLAIMS:

1. A method of processing attachments to messages sent to a mobile device, the method comprising:

after a message to be sent to the mobile device is received by one or more remote servers, receiving data associated with the message at the mobile device from the one or more remote servers;

wherein the message comprises a plurality of encrypted attachments;

wherein each encrypted attachment has been encrypted using a different one of a plurality of session keys;

wherein each of said plurality of session keys has been encrypted using an encryption key;

wherein the one or more remote servers initially withholds transmission of each encrypted attachment and subsequently transmits an identified encrypted attachment in decrypted form to the mobile device if a request for the identified encrypted attachment is received; and

wherein the data received at the mobile device comprises data identifying an attachment structure for the message, and further comprises one or more of the plurality of session keys in encrypted form;

outputting the attachment structure at the mobile device;

receiving an attachment request at the mobile device, the attachment request identifying a selected encrypted attachment of the plurality of encrypted attachments;

if the one or more of the plurality of session keys in encrypted form does not include the session key that encrypted the selected encrypted attachment, transmitting the session key in encrypted form that encrypted the selected encrypted attachment from the one or more remote servers to the mobile device;

decrypting the session key, of the plurality of session keys in encrypted form, that encrypted the selected encrypted attachment, to produce a decrypted session key for the selected encrypted attachment at the mobile device;

transmitting the decrypted session key for the selected encrypted attachment with the attachment request, from the mobile device to the one or more remote servers; and

receiving a decrypted attachment corresponding to the selected encrypted attachment identified in the attachment request at the mobile device, the decrypted attachment being in a form that can be rendered at the mobile device;

wherein the one or more remote servers is configured to decrypt the selected encrypted attachment identified in the attachment request using the decrypted session key to produce a decrypted attachment, process the decrypted attachment to place it in a form that can be rendered at the mobile device, and transmit the decrypted attachment in a form that can be rendered at the mobile device to the mobile device.

2. The method of claim 1,
wherein the message comprises a main message header and the plurality of encrypted attachments; and
wherein each of the plurality of session keys in encrypted form is stored with its corresponding encrypted attachment in an associated message part.
3. The method of claim 1 or claim 2, wherein the one or more remote servers comprises a message management server.
4. The method of any one of claims 1 to 3, where the one or more remote servers comprises an attachment server.
5. The method of any one of claims 1 to 4, wherein the message comprises a message formatted in accordance with a Pretty Good Privacy 'PGP' Partitioned encoding format.
6. The method of any one of claims 1 to 4, wherein the message comprises an e-mail message, an instant message or a peer-to-peer message.
7. The method of any one of claims 1 to 6, wherein each of the plurality of encrypted attachments is formatted in accordance with a PGP Partitioned encoding format.

8. A computer-readable medium comprising instructions executable on a processor of a computing device for causing the computing device to implement the method of any one of claims 1 to 7.

9. A mobile device comprising processing means configured to:

after a message to be sent to a mobile device is received by one or more remote servers, receive data associated with the message at the mobile device from the one or more remote servers;

wherein the message comprises a plurality of encrypted attachments;

wherein each encrypted attachment has been encrypted using a different one of a plurality of session keys;

wherein each of said plurality of session keys has been encrypted using an encryption key;

wherein the one or more remote servers initially withholds transmission of each encrypted attachment and subsequently transmits an identified encrypted attachment in decrypted form to the mobile device if a request for the identified encrypted attachment is received; and

wherein the data received at the mobile device comprises data identifying an attachment structure for the message, and further comprises one or more of the plurality of session keys in encrypted form;

output the attachment structure at the mobile device;

receive an attachment request at the mobile device, the attachment request identifying a selected encrypted attachment of the plurality of encrypted attachments;

if the one or more of the plurality of session keys in encrypted form does not include the session key that encrypted the selected encrypted attachment, transmit the session key in encrypted form that encrypted the selected encrypted attachment from the one or more remote servers to the mobile device;

decrypt the session key, of the plurality of session keys in encrypted form, that encrypted the selected encrypted attachment, to produce a decrypted session key for the selected encrypted attachment at the mobile device;

transmit the decrypted session key for the selected encrypted attachment with the attachment request, from the mobile device to the one or more remote servers; and

receive a decrypted attachment corresponding to the selected encrypted attachment identified in the attachment request at the mobile device, the decrypted attachment being in a form that can be rendered at the mobile device;

wherein the one or more remote servers is configured to decrypt the selected encrypted attachment identified in the attachment request using the decrypted session key to produce a decrypted attachment, process the decrypted attachment to place it in a form that can be rendered at the mobile device, and transmit the decrypted attachment in a form that can be rendered at the mobile device to the mobile device.

10. The mobile device of claim 9,

wherein the message comprises a main message header and the plurality of encrypted attachments; and

wherein each of the plurality of session keys in encrypted form is stored with its corresponding encrypted attachment in an associated message part.

11. The mobile device of claim 9 or claim 10, wherein the one or more remote servers comprises a message management server.

12. The mobile device of any one of claims 9 to 11, where the one or more remote servers comprises an attachment server.

13. The mobile device of any one of claims 9 to 12, wherein the message comprises a message formatted in accordance with a Pretty Good Privacy 'PGP' Partitioned encoding format.

14. The mobile device of any one of claims 9 to 12, wherein the message comprises an e-mail message, an instant message or a peer-to-peer message.

15. The mobile device of claim 13, wherein each of the plurality of encrypted attachments is formatted in accordance with a PGP Partitioned encoding format.

16. A system for processing attachments to messages, the system comprising:

a mobile device comprising at least a processor and a memory;
wherein one or more remote servers are configured to transmit data associated with a message to the mobile device; and
wherein the mobile device is configured to execute an application module programmed to perform the method of any one of claims 1 to 7.

17. A mobile device configured to process a message comprising a plurality of encrypted attachments received from a sender via one or more remote servers, wherein the mobile device comprises a processor and memory, and wherein the processor is configured to perform acts comprising:

receiving, from the one or more remote servers, data associated with the message, wherein the one or more remote servers are configured to initially withhold transmission of each encrypted attachment of the plurality of encrypted attachments to the mobile device until a request for the attachment is made by the mobile device, and wherein the data received from the one or more remote servers identifies an attachment structure for the message and comprises at least one encrypted session key of a plurality of session keys; and

outputting the attachment structure;

wherein the message as sent from the sender comprises the plurality of encrypted attachments, wherein each of the plurality of encrypted attachments is encrypted using a different one of the plurality of session keys, and wherein each session key of the plurality of session keys is encrypted such that the session key is decryptable with a key accessible to the mobile device but not to the one or more remote servers.

18. The device of claim 17, wherein the data associated with the message received at the mobile device comprises an encrypted session key for each of the plurality of encrypted attachments.

19. The device of claim 18, wherein the processor is further configured to:

receive an attachment request via a user interface of the mobile device, the attachment request identifying a specific encrypted attachment of the plurality of encrypted attachments;

decrypt the encrypted session key for the specific encrypted attachment to produce a decrypted session key;
transmit the decrypted session key with the attachment request to the one or more remote servers, wherein the one or more remote servers are configured to decrypt the specific encrypted attachment using the decrypted session key and to transmit data associated with the specific encrypted attachment in decrypted form to the mobile device; and
receive data associated with the specific encrypted attachment in decrypted form from the one or more remote servers.

20. The device of claim 19, wherein the device is not equipped with a native attachment viewer.

21. The device of claim 19, wherein the data associated with the specific encrypted attachment received in decrypted form from the one or more remote servers comprises text and images, which are processed by a messaging application residing and executing on the mobile device for rendering in the user interface.

22. The device of claim 18, wherein the encrypted session key for each of the plurality of encrypted attachments is provided in a message header.

23. The device of claim 22, wherein the one or more remote servers are configured to retrieve the encrypted session key for each of the plurality of encrypted attachments, and to store the encrypted session key for each of the plurality of encrypted attachments in the message header.

24. The device of claim 22, wherein the encrypted session key for each of the plurality of encrypted attachments has been stored in the message header at a computing device of the sender.

25. The device of claim 18, wherein the encrypted session key for each of the plurality of encrypted attachments is provided with its corresponding encrypted attachment in an associated message part, within the data received from the one or more remote servers.
26. The device of any one of claims 17 to 25, wherein the one or more remote servers comprises a message management server.
27. The device of any one of claims 17 to 25, where the one or more remote servers comprises an attachment server.
28. The device of any one of claims 17 to 27, wherein the message comprises a message formatted in accordance with a PGP Partitioned encoding format.
29. The device of any one of claims 17 to 28, wherein the message comprises an e-mail message.
30. The device of any one of claims 17 to 28, wherein the message comprises an instant message.
31. The device of any one of claims 17 to 28, wherein the message comprises a peer-to-peer message.
32. The device of any one of claims 17 to 31, wherein each of the plurality of encrypted attachments is formatted in accordance with a PGP Partitioned encoding format.
33. The device of claim 17 or claim 18, wherein the device is not equipped with an attachment viewer.
34. The device of any one of claims 17 to 33, wherein the key accessible to the mobile device is stored on a smart card.

35. The device of any one of claims 17 to 34, wherein the key accessible to the mobile device comprises a public key of a public key and private key pair.

36. The device of any one of claims 17 to 34, wherein the key accessible to the mobile device comprises a symmetric encryption key.

37. A method of processing attachments to messages sent to a mobile device, the method comprising:

after a message to be sent to the mobile device is received by one or more remote servers, receiving data associated with the message at the mobile device from the one or more remote servers;

wherein the message comprises a plurality of encrypted attachments;

wherein each encrypted attachment has been encrypted using a different one of a plurality of session keys, and each session key has been encrypted with a further encryption key such that the session key is decryptable with the further encryption key that resides on the mobile device and is not available to the remote server;

wherein the one or more remote servers are configured to initially withhold transmission of each attachment to the mobile device, and are configured to subsequently transmit an identified attachment to the mobile device if a request for the identified encrypted attachment is received; and

wherein the data received at the mobile device comprises data identifying an attachment structure for the message that identifies each of the plurality of attachments by a filename, and further comprises at least one encrypted session key; and outputting the attachment structure at the mobile device.

38. The method of claim 37, wherein the data received at the mobile device comprises an encrypted session key for each encrypted attachment.

39. The method of claim 37 or claim 38, further comprising:

receiving an attachment request at the mobile device, the attachment request identifying an attachment to the message;

decrypting the encrypted session key for the attachment identified in the attachment request to produce a decrypted session key;
transmitting the decrypted session key with the attachment request from the mobile device to the one or more remote servers;
wherein the one or more remote servers are configured to decrypt the attachment identified in the attachment request using the decrypted session key, and to transmit data associated with the attachment in decrypted form to the mobile device; and
receiving data associated with the attachment identified in the attachment request in decrypted form at the mobile device.

40. The method of any one of claims 37 to 39,
wherein the message comprises a main message header;
wherein each encrypted session key for each encrypted attachment has been inserted into the main message header; and
wherein the data associated with the message received at the mobile device comprises data in the main message header.

41. The method of any one of claims 37 to 40, wherein the one or more remote servers are configured to retrieve, for the message received by the one or more remote servers, each encrypted session key for each encrypted attachment, and to store each encrypted session key in the main message header.

42. The method of any one of claims 37 to 40, wherein at a sender's computing device from which the message originates, each encrypted session key for each encrypted attachment has been stored in the main message header.

43. The method of any one of claims 37 to 39,
wherein the message comprises a main message header;
wherein an encrypted session key for each encrypted attachment is stored with its corresponding encrypted attachment in an associated message part; and
wherein at least one encrypted session key is received at the mobile device.

44. The method of any one claims 37 to 43, wherein the one or more remote servers comprises a message management server.
45. The method of any one of claims 37 to 44, where the one or more remote servers comprises an attachment server.
46. The method of any one of claims 37 to 45, wherein the message comprises a message formatted in accordance with a PGP Partitioned encoding format.
47. The method of any one of claims 37 to 46, wherein the message comprises an e-mail message.
48. The method of any one of claims 37 to 46, wherein the message comprises an instant message.
49. The method of any one of claims 37 to 46, wherein the message comprises a peer-to-peer message.
50. The method of any one of claims 37 to 49, wherein each of the plurality of encrypted attachments is formatted in accordance with a PGP Partitioned encoding format.
51. A computer-readable medium comprising instructions executable on a processor of a mobile device, wherein the processor is configured to implement a method of processing attachments to messages sent to the mobile device, the method comprising:
after a message to be sent to the mobile device is received by one or more remote servers,
receiving data associated with the message at the mobile device from the one or more remote servers;
wherein the message comprises a plurality of encrypted attachments;
wherein each encrypted attachment has been encrypted using a different one of a plurality of session keys, and each session key has been encrypted with a further

encryption key such that the session key is decryptable with the further encryption key that resides on the mobile device and is not available to the remote server;
wherein the one or more remote servers are configured to initially withhold transmission of each attachment to the mobile device, and are configured to subsequently transmit an identified attachment to the mobile device if a request for the identified encrypted attachment is received; and
wherein the data received at the mobile device comprises data identifying an attachment structure for the message that identifies each of the plurality of attachments by a filename, and further comprises at least one encrypted session key; and
outputting the attachment structure at the mobile device.

52. A system for processing attachments to messages, the system comprising:

a mobile device comprising at least a processor and a memory;
wherein one or more remote servers are configured to transmit data associated with a message to the mobile device;
wherein the processor is configured to:
after a message to be sent to the mobile device is received by one or more remote servers, receive data associated with the message at the mobile device from the one or more remote servers;
wherein the message comprises a plurality of encrypted attachments;
wherein each encrypted attachment has been encrypted using a different one of a plurality of session keys, and each session key has been encrypted with a further encryption key such that the session key is decryptable with the further encryption key that resides on the mobile device and is not available to the remote server;
wherein the one or more remote servers are configured to initially withhold transmission of each attachment to the mobile device, and are configured to subsequently transmit an identified attachment to the mobile device if a request for the identified encrypted attachment is received; and
wherein the data received at the mobile device comprises data identifying an attachment structure for the message that identifies each of the plurality of attachments by a filename, and further comprises at least one encrypted session key; and

output the attachment structure at the mobile device.

53. The system of claim 52, wherein the one or more remote servers comprises a message management server.

54. The system of claim 52 or claim 53, where the one or more remote servers comprises an attachment server.

55. The system of any one of claims 52 to 54, wherein the message comprises a message formatted in accordance with a PGP Partitioned encoding format.

56. The system of any one of claims 52 to 55, wherein the message comprises an e-mail message.

57. The system of any one of claims 52 to 55, wherein the message comprises an instant message.

58. The system of any one of claims 52 to 55, wherein the message comprises a peer-to-peer message.

59. A mobile device configured to process a message comprising a plurality of encrypted attachments addressed to a plurality of recipients received from a sender via one or more remote servers, wherein the mobile device comprises a processor and memory, and wherein the processor is configured to perform acts comprising:

receiving, from the one or more remote servers, data associated with the message, wherein the one or more remote servers are configured to initially withhold transmission of each encrypted attachment of the plurality of encrypted attachments to the mobile device until a request for the attachment is made by the mobile device, and wherein the data received from the one or more remote servers identifies an attachment structure for the message and comprises, for each of the plurality of encrypted attachments, an encrypted session key for each of the plurality of recipients;

outputting the attachment structure;

wherein for each of the plurality of encrypted attachments, the encrypted session key for the recipient associated with the mobile device is decryptable with a key accessible to the mobile device but not to the one or more remote servers, and the encrypted session key for recipients not associated with the mobile device cannot be decrypted with the key accessible to the mobile device but not to the one or more remote servers;

receiving an attachment request via a user interface of the mobile device, the attachment request identifying a specific encrypted attachment of the plurality of encrypted attachments;

decrypting the encrypted session key that is for the specific encrypted attachment and that is for the recipient associated with the mobile device to produce a decrypted session key;

transmitting the decrypted session key with the attachment request to the one or more remote servers, wherein the one or more remote servers are configured to decrypt the specific encrypted attachment using the decrypted session key and to transmit data associated with the specific encrypted attachment in decrypted form to the mobile device; and

receiving data associated with the specific encrypted attachment in decrypted form from the one or more remote servers.

60. The device of claim 59, wherein the device is not equipped with a native attachment viewer.

61. The device of claim 59 or claim 60, wherein the data associated with the specific encrypted attachment received in decrypted form from the one or more remote servers comprises text and images, which are processed by a messaging application residing and executing on the mobile device for rendering in the user interface.

62. The device of any one of claims 59 to 61, wherein the encrypted session key for each of the plurality of recipients, for each of the plurality of encrypted attachments, as received from the one or more remote servers is provided in a message header.

63. The device of any one of claims 59 to 61, wherein the encrypted session key for each of the plurality of recipients, is provided with their corresponding encrypted attachment in an associated message part, within the data received from the one or more remote servers.

64. The device of any one of claims 59 to 63, wherein the one or more remote servers comprises a message management server.

65. The device of any one of claims 59 to 64, where the one or more remote servers comprises an attachment server.

66. The device of any one of claims 59 to 65, wherein the message comprises a message formatted in accordance with a PGP Partitioned encoding format.

67. The device of any one of claims 59 to 66, wherein the message comprises an e-mail message.

68. The device of any one of claims 59 to 66, wherein the message comprises an instant message.

69. The device of any one of claims 59 to 66, wherein the message comprises a peer-to-peer message.

70. The device of any one of claims 59 to 69, wherein each of the plurality of encrypted attachments is formatted in accordance with a PGP Partitioned encoding format.

71. The device of any one of claims 59 to 70, wherein the device is not equipped with an attachment viewer.

72. The device of any one of claims 59 to 71, wherein the key accessible to the mobile device is stored on a smart card.

73. The device of any one of claims 59 to 72, wherein the key accessible to the mobile device comprises a public key of a public key and private key pair.

74. The device of any one of claims 59 to 72, wherein the key accessible to the mobile device comprises a symmetric encryption key.

75. A method of processing, on a mobile device, a message comprising a plurality of encrypted attachments addressed to a plurality of recipients received from a sender via one or more remote servers, the method comprising:

receiving, from the one or more remote servers, data associated with the message, wherein the one or more remote servers are configured to initially withhold transmission of each encrypted attachment of the plurality of encrypted attachments to the mobile device until a request for the attachment is made by the mobile device, and wherein the data received from the one or more remote servers identifies an attachment structure for the message and comprises, for each of the plurality of encrypted attachments, an encrypted session key for each of the plurality of recipients;

outputting the attachment structure;

wherein for each of the plurality of encrypted attachments, the encrypted session key for the recipient associated with the mobile device is decryptable with a key accessible to the mobile device but not to the one or more remote servers, and the encrypted session key for recipients not associated with the mobile device cannot be decrypted with the key accessible to the mobile device but not to the one or more remote servers;

receiving an attachment request via a user interface of the mobile device, the attachment request identifying a specific encrypted attachment of the plurality of encrypted attachments;

decrypting the encrypted session key that is for the specific encrypted attachment and that is for the recipient associated with the mobile device to produce a decrypted

session key;

transmitting the decrypted session key with the attachment request to the one or more remote servers, wherein the one or more remote servers are configured to decrypt the specific encrypted attachment using the decrypted session key and to transmit data associated with the specific encrypted attachment in decrypted form to the mobile device; and

receiving data associated with the specific encrypted attachment in decrypted form from the one or more remote servers.

76. A computer-readable medium comprising instructions executable by a processor, said instructions for implementing, on a mobile device, a method of processing a message comprising a plurality of encrypted attachments addressed to a plurality of recipients received from a sender via one or more remote servers, the method comprising:

receiving, from the one or more remote servers, data associated with the message, wherein the one or more remote servers are configured to initially withhold transmission of each encrypted attachment of the plurality of encrypted attachments to the mobile device until a request for the attachment is made by the mobile device, and wherein the data received from the one or more remote servers identifies an attachment structure for the message and comprises, for each of the plurality of encrypted attachments, an encrypted session key for each of the plurality of recipients;

outputting the attachment structure;

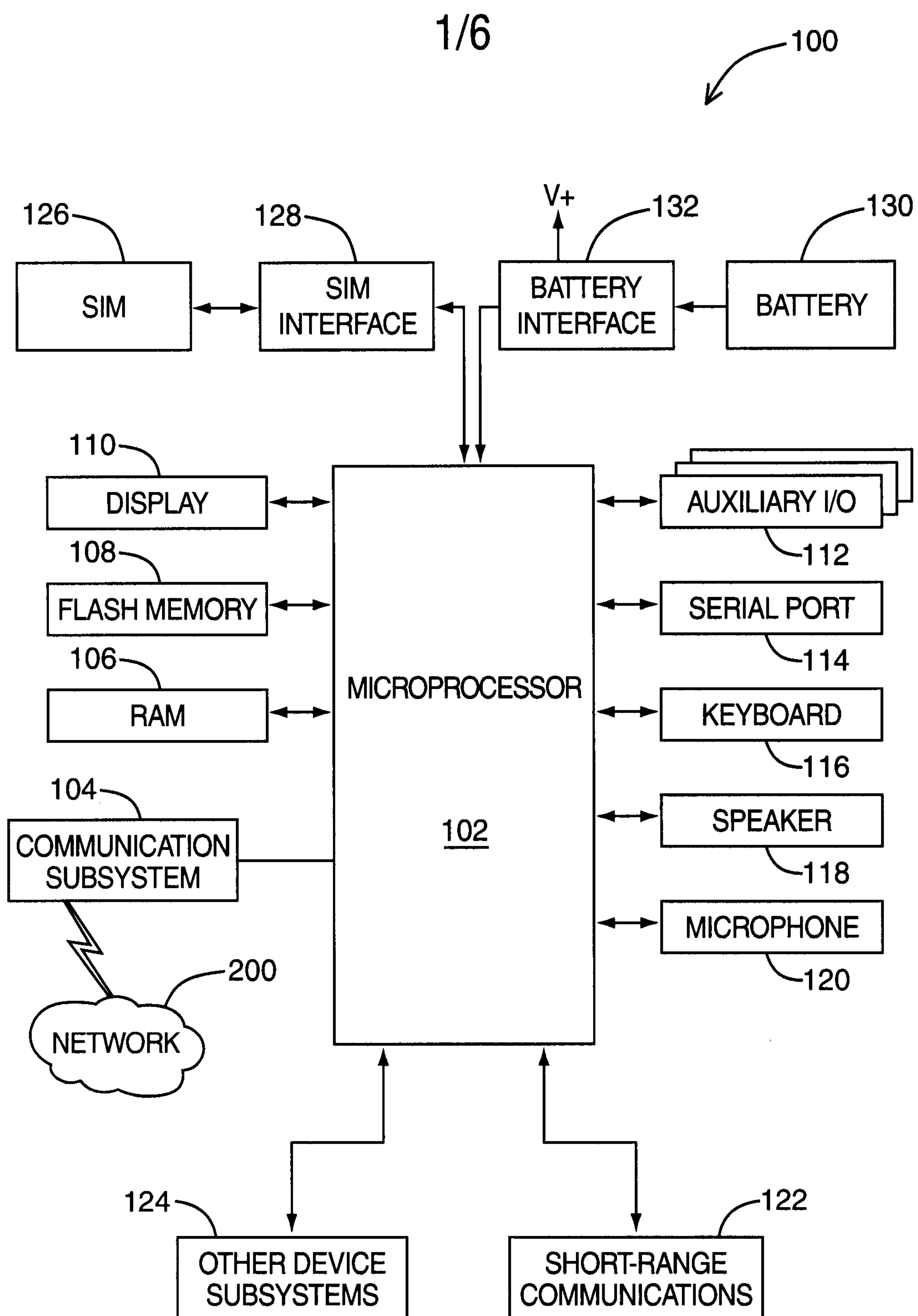
wherein for each of the plurality of encrypted attachments, the encrypted session key for the recipient associated with the mobile device is decryptable with a key accessible to the mobile device but not to the one or more remote servers, and the encrypted session key for recipients not associated with the mobile device cannot be decrypted with the key accessible to the mobile device but not to the one or more remote servers;

receiving an attachment request via a user interface of the mobile device, the attachment request identifying a specific encrypted attachment of the plurality of encrypted attachments;

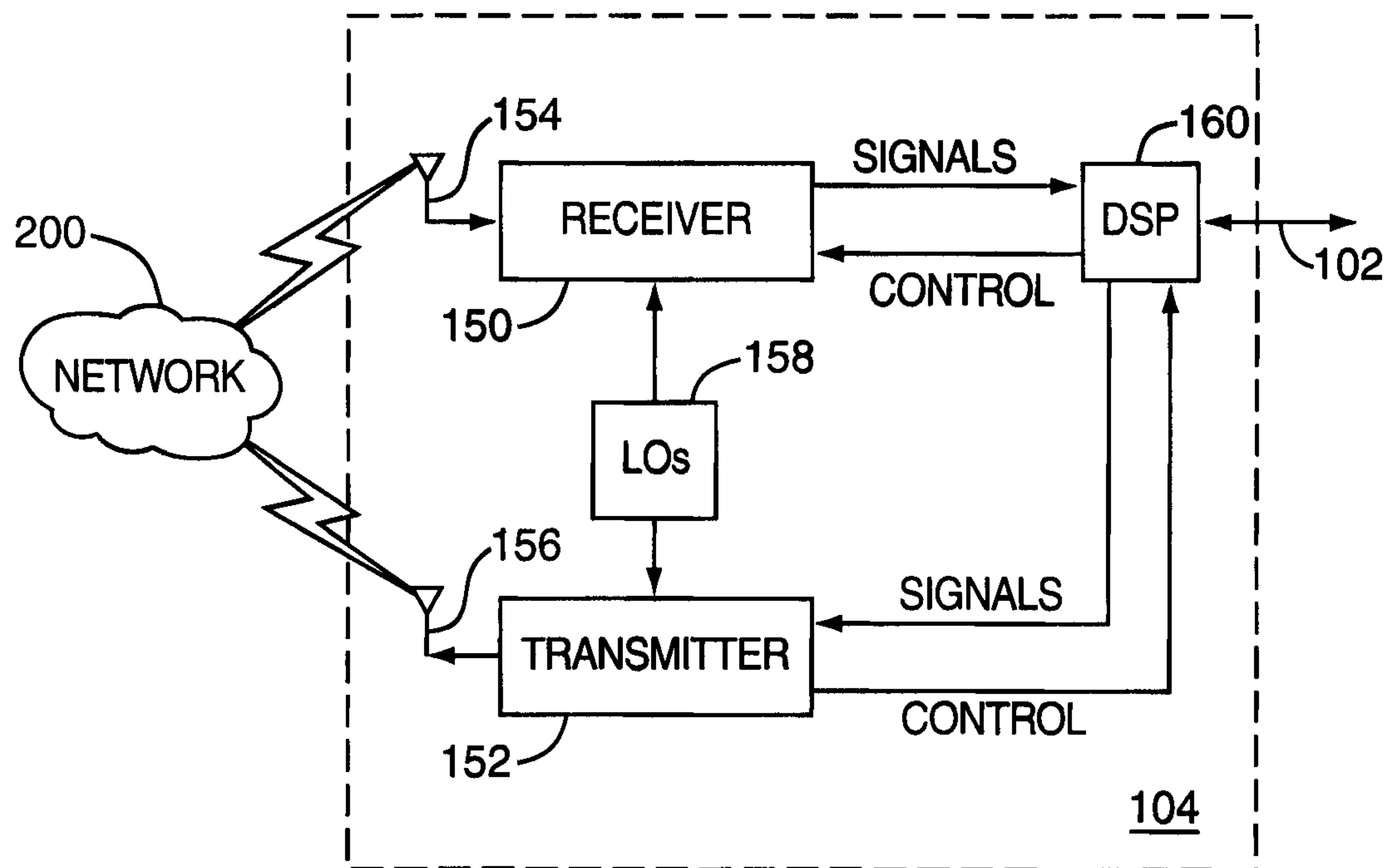
decrypting the encrypted session key that is for the specific encrypted attachment and that is for the recipient associated with the mobile device to produce a decrypted session key;

transmitting the decrypted session key with the attachment request to the one or more remote servers, wherein the one or more remote servers are configured to decrypt the specific encrypted attachment using the decrypted session key and to transmit data associated with the specific encrypted attachment in decrypted form to the mobile device; and

receiving data associated with the specific encrypted attachment in decrypted form from the one or more remote servers.

FIG. 1

2/6

FIG. 2

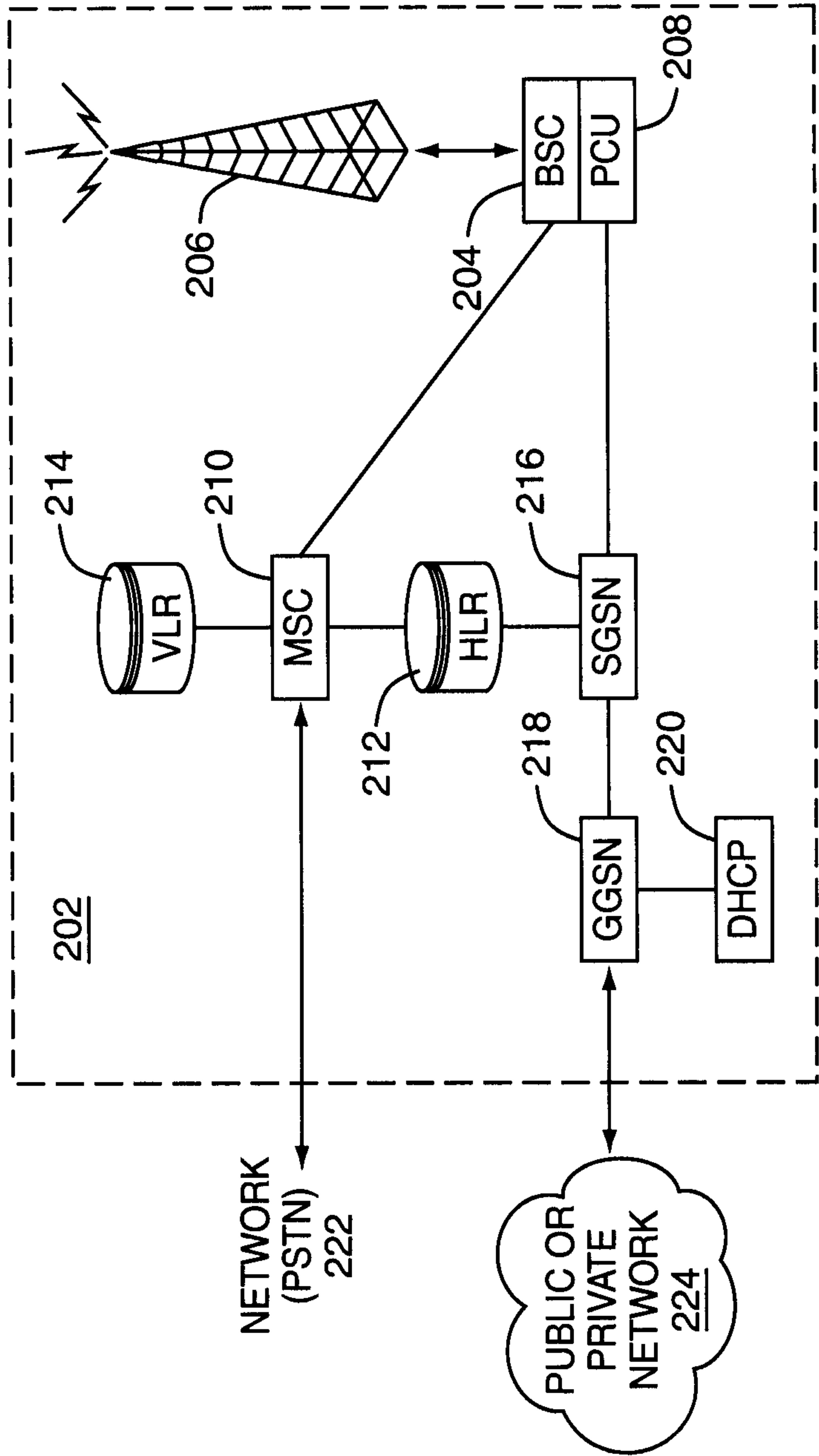


FIG. 3

4/6

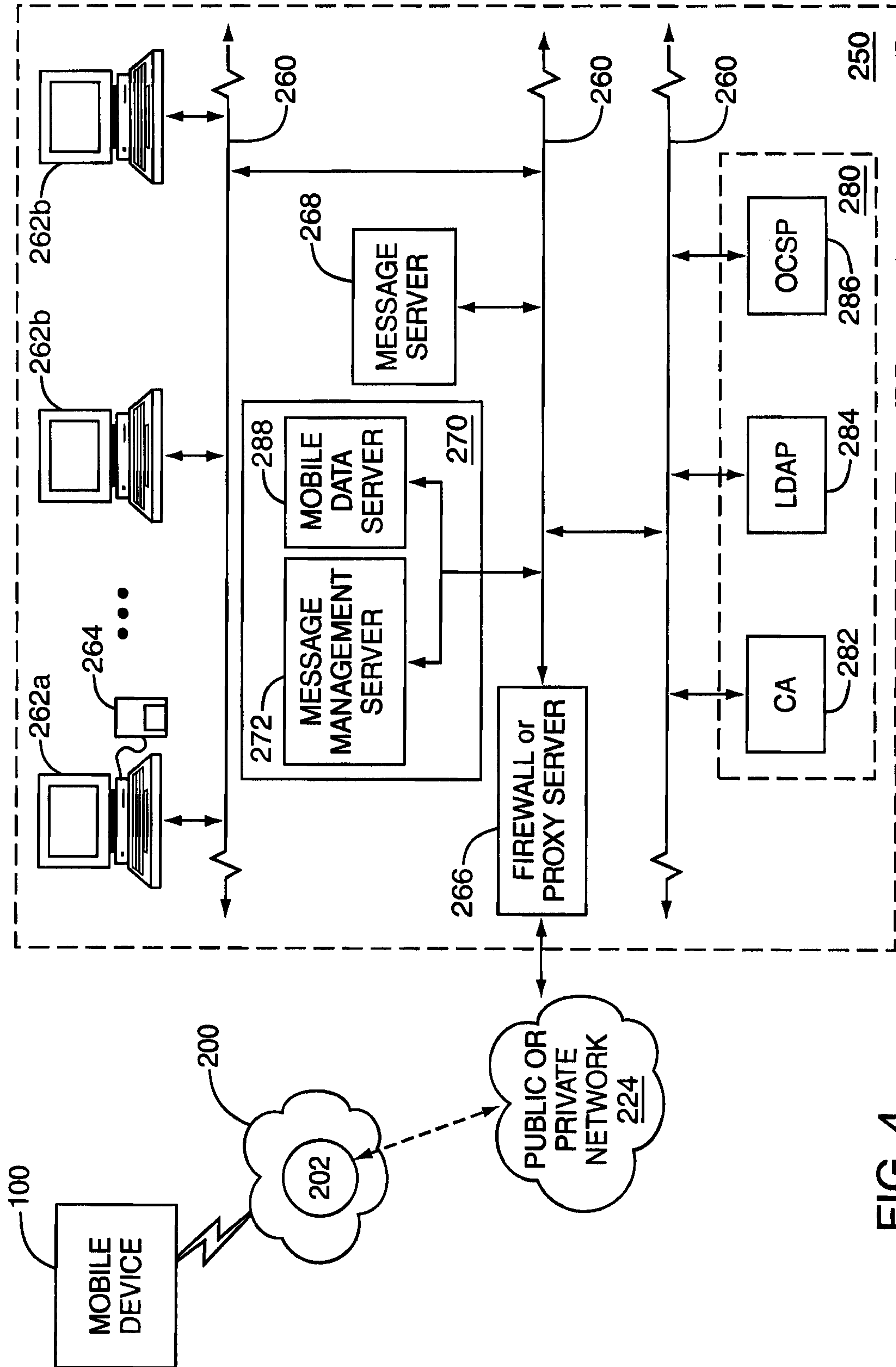
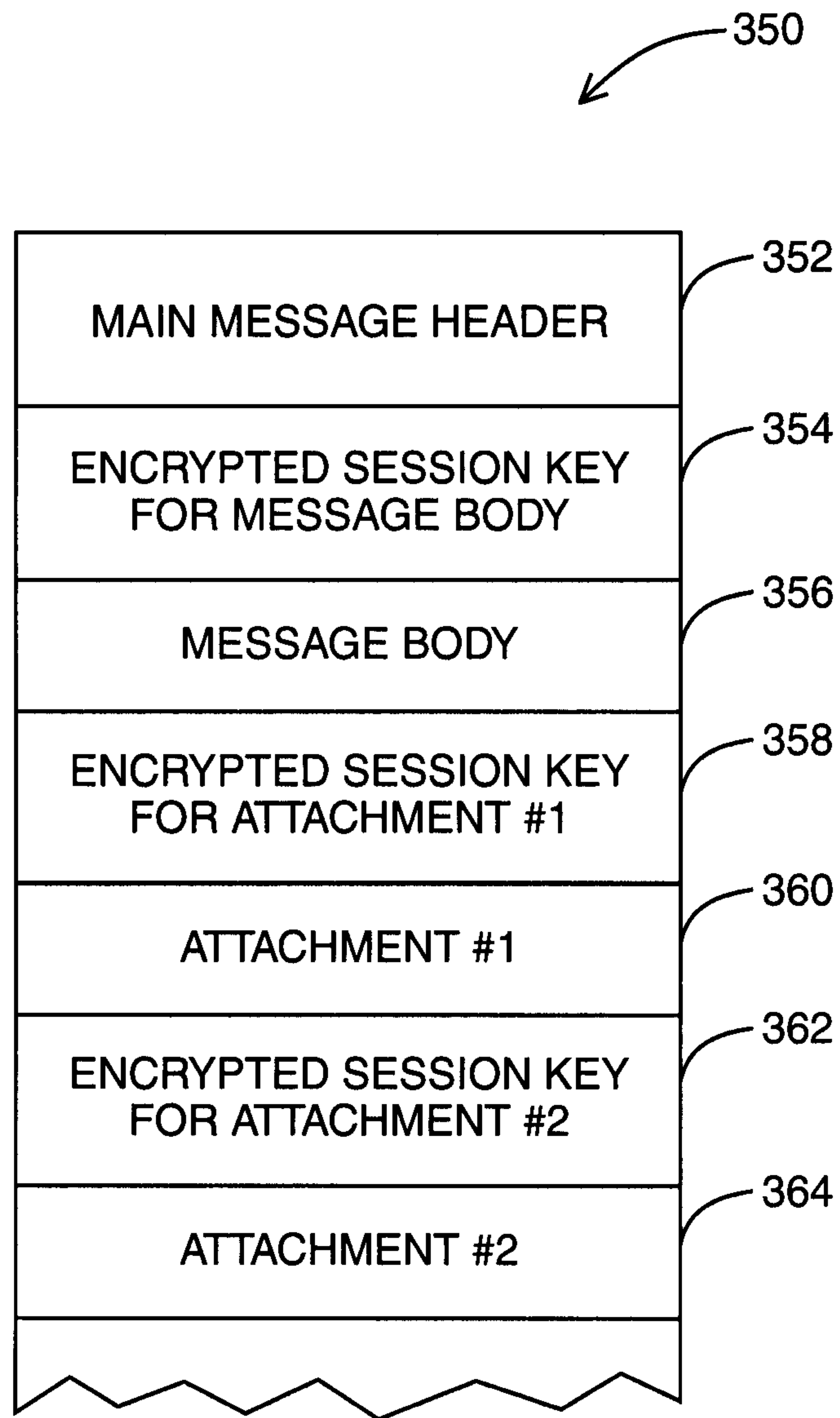


FIG. 4

5/6

FIG. 5

6/6

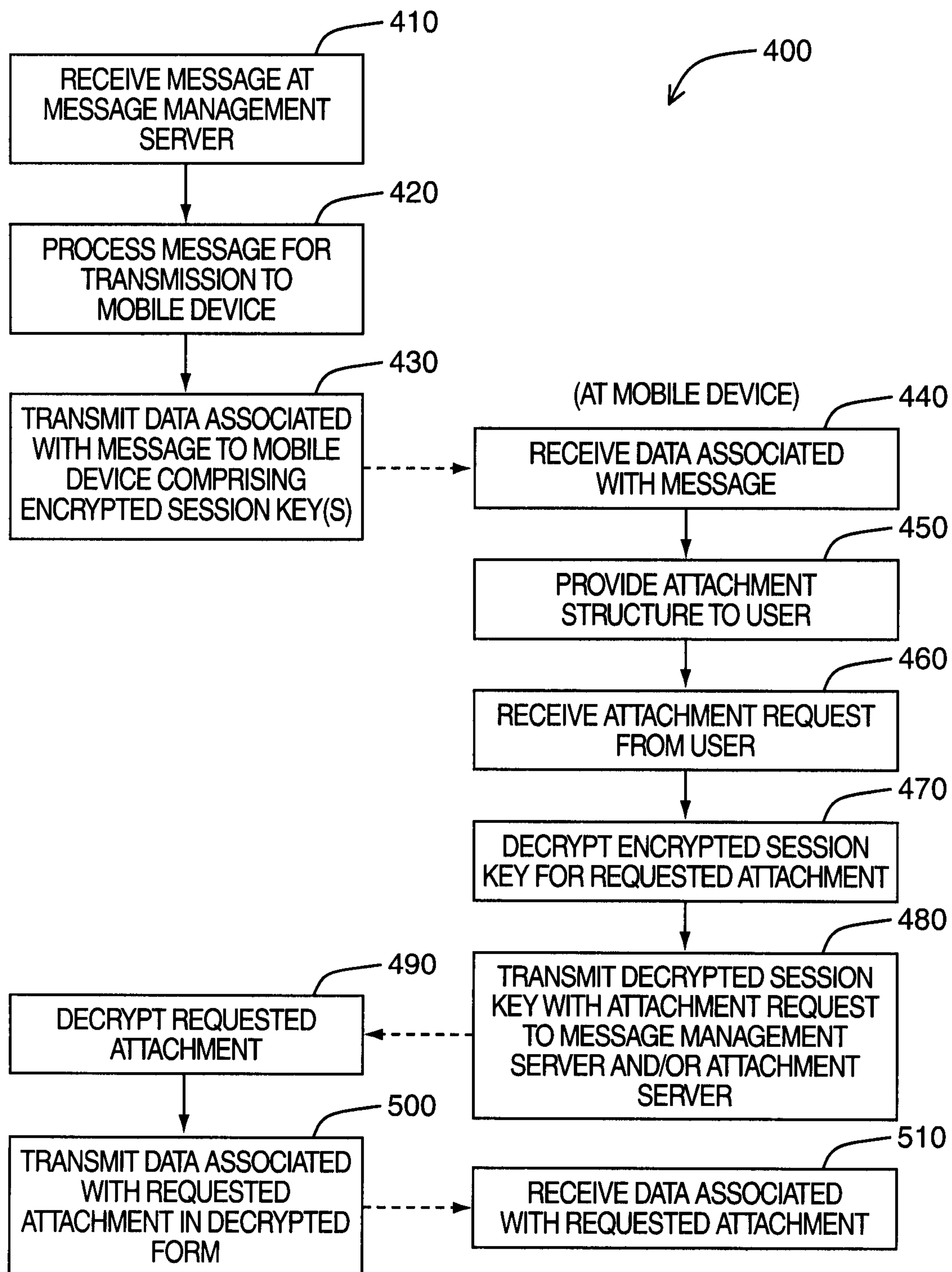


FIG. 6

