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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2005 (29.12.2005)

PCT

(10) International Publication Number
WO 2005/125115 A1

(51) International Patent Classification[7]: H04L 12/54, H04Q 7/32

(21) International Application Number: PCT/CA2005/000962

(22) International Filing Date: 21 June 2005 (21.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/581,644 21 June 2004 (21.06.2004) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED?** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

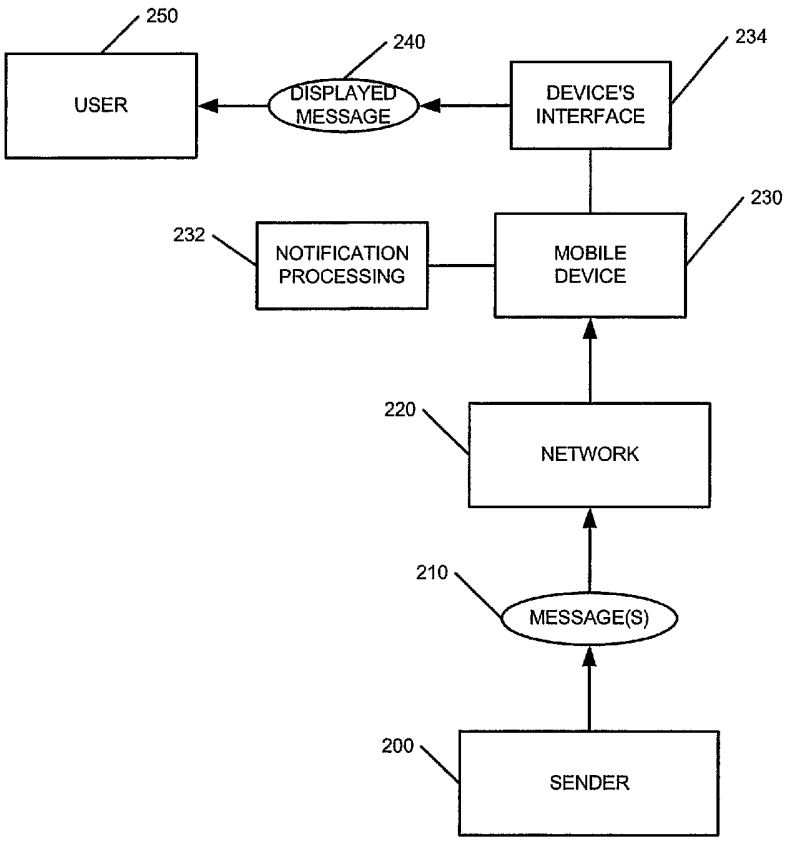
(72) Inventors: **ADAMS, Neil, P.**; 550 Little Dover Crescent, Waterloo, Ontario N2K 4E4 (CA). **LITTLE, Herbert, A.**; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA). **BROWN, Michael, K.**; 1938 Mapleridge Drive, Peterborough, Ontario K9K 2E4 (CA). **BROWN, Michael, S.**; 350 University Downs Crescent, Waterloo, Ontario N2K 4B1 (CA).

(74) Agents: **BEHMANN, Curtis, B.** et al.; Borden Ladner Gervais LLP, World Exchange Plaza, Suite 1100, 100 Queen Street, Ottawa, Ontario K1P 1J9 (CA).

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR HANDLING MESSAGE RECEIPT NOTIFICATION



(57) Abstract: Systems and methods for operation upon a wireless mobile device to handle message notifications. A method can include receiving a message by the wireless mobile device over a wireless communications network. The received message is processed so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender.

WO 2005/125115 A1

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

Published:
— *with international search report*
— *with amended claims*

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

SYSTEM AND METHOD FOR HANDLING MESSAGE RECEIPT NOTIFICATION

BACKGROUND

Technical Field

This document relates generally to the field of communications, and in particular to handling messages on mobile wireless communications devices.

Description of the Related Art

Mobile wireless devices are configured to send and receive messages, such as e-mail messages. Typically a signed receipt is sent before a user is allowed to view a message. Additionally, a message may have to be verified before the signed receipt is sent. To verify the message typically all of the message has to be present. This can be difficult to perform on a constrained device, such as a mobile device, because it may take a while to receive enough of the message on the device to verify. In fact, a device may never receive the entire message, such as when the message is relatively long or in other situations (e.g., when the message is received and viewed in portions or chunks). Additionally in some situations, there may not be a mechanism to receive the entire message until a user starts to view the message (e.g., when a user has to request additional message chunks while viewing a message).

SUMMARY

In accordance with the teachings disclosed herein, systems and methods are provided for providing signed receipt notifications. An example of a system and method includes a mobile device being able to send a signed receipt notification although the entire message may not have been received yet.

As another example, a system and method can include receiving a message by the wireless mobile device over a wireless communications network, wherein a sender composed the message intended for receipt by at least one recipient. The received message is processed so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender.

As another example, a system and method can be configured to include notification processing instructions that can process a message received by the wireless mobile device

over a wireless communications network, wherein a sender composed the message intended for receipt by at least one recipient. Signed receipt generation instructions are used to generate a signed receipt based upon the received message. The notification processing instructions are configured to process the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before the generated signed receipt is provided to the sender. The signed receipt can be used at least in part to confirm whether the specific recipient had received the sender's message.

As will be appreciated, the systems and methods disclosed herein are capable of other and different embodiments, and its several details are capable of modifications in various respects, all without departing from the spirit of the techniques disclosed herein. Accordingly, the drawings and description set forth herein are to be regarded as illustrative in nature and not restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an overview of an example communication system in which a wireless communication device may be used.

FIG. **2** is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices.

FIG. **3** is a block diagram depicting a system for handling messages received over a network.

FIG. **4** is a block diagram depicting a system for providing signed receipt notifications.

FIG. **5** is a block diagram depicting a system that interacts with a user in order to provide signed receipt notifications.

FIG. **6** is a block diagram depicting use of signed receipt generation functionality in order to generate a signed receipt.

FIG. **7** is a user interface that provides one or more indicators regarding a signed receipt notification.

FIG. **8** is a flowchart depicting an example operational scenario wherein a message that is received by a mobile device is processed in order to generate a signed receipt.

FIG. **9** is a flowchart depicting an example operational scenario that illustrates interaction with a user in order to provide signed receipt notifications.

FIG. **10** is a block diagram of an example mobile device.

DETAILED DESCRIPTION OF THE DRAWINGS

FIG. **1** is an overview of an example communication system in which a wireless communication device may be used. One skilled in the art will appreciate that there may be hundreds of different topologies, but the system shown in FIG. **1** helps demonstrate the operation of the encoded message processing systems and methods described in the present application. There may also be many message senders and recipients. The simple system shown in FIG. **1** is for illustrative purposes only, and shows perhaps the most prevalent Internet e-mail environment where security is not generally used.

FIG. **1** shows an e-mail sender **10**, the Internet **20**, a message server system **40**, a wireless gateway **85**, wireless infrastructure **90**, a wireless network **105** and a mobile communication device **100**.

An e-mail sender system **10** may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system **10** has an account, located within a company, possibly connected to a local area network (LAN), and connected to the Internet **20**, or connected to the Internet **20** through a large ASP (application service provider) such as America Online (AOL). Those skilled in the art will appreciate that the systems shown in FIG. **1** may instead be connected to a wide area network (WAN) other than the Internet, although e-mail transfers are commonly accomplished through Internet-connected arrangements as shown in FIG. **1**.

The message server **40** may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet **20**. Although other messaging systems might not require a message server system **40**, a mobile device **100** configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are Microsoft Exchange™ and Lotus Domino™. These products are often used in conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. **1**, as they do not directly play a role in the secure message processing described below. Message servers such as server **40** typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation.

The wireless gateway **85** and infrastructure **90** provide a link between the Internet **20** and wireless network **105**. The wireless infrastructure **90** determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. A message is then delivered to the mobile device **100** via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network **105** to the mobile device **100**. The particular network **105** may be virtually any wireless network over which messages may be exchanged with a mobile communication device.

As shown in FIG. **1**, a composed e-mail message **15** is sent by the e-mail sender **10**, located somewhere on the Internet **20**. This message **15** is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC**822** headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message **15** arrives at the message server **40** and is normally stored in a message store. Most known messaging systems support a so-called "pull" message access scheme, wherein the mobile device **100** must request that stored messages be forwarded by the message server to the mobile device **100**. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device **100**. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device **100** are redirected from the message server **40** to the mobile device **100** as they are received.

Regardless of the specific mechanism controlling the forwarding of messages to the mobile device **100**, the message **15**, or possibly a translated or reformatted version thereof, is sent to the wireless gateway **85**. The wireless infrastructure **90** includes a series of connections to wireless network **105**. These connections could be Integrated Services Digital Network (ISDN), Frame Relay or T1 connections using the TCP/IP protocol used throughout the Internet. As used herein, the term "wireless network" is intended to include three different types of networks, those being (**1**) data-centric wireless networks, (**2**) voice-centric wireless networks and (**3**) 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, (**1**) Code Division Multiple Access (CDMA) networks, (**2**) the Groupe Special Mobile or the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) networks, and (**3**)

future third-generation (3G) networks like Enhanced Data-rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS). Some older examples of data-centric network 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 TDMA systems.

FIG. **2** is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices. The system of FIG. **2** is substantially similar to the FIG. **1** system, but includes a host system **30**, a redirection program **45**, a mobile device cradle **65**, a wireless virtual private network (VPN) router **75**, an additional wireless network **110** and multiple mobile communication devices **100**. As described above in conjunction with FIG. **1**, FIG. **2** represents an overview of a sample network topology. Although the encoded message processing systems and methods described herein may be applied to networks having many different topologies, the network of FIG. **2** is useful in understanding an automatic e-mail redirection system mentioned briefly above.

The central host system **30** will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system **30** is the message server **40**, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet **20**. In the system of FIG. **2**, the redirection program **45** enables redirection of data items from the server **40** to a mobile communication device **100**. Although the redirection program **45** is shown to reside on the same machine as the message server **40** for ease of presentation, there is no requirement that it must reside on the message server. The redirection program **45** and the message server **40** are designed to co-operate and interact to allow the pushing of information to mobile devices **100**. In this installation, the redirection program **45** takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices **100**. A more detailed description of the redirection software **45** may be found in the commonly assigned United States Patent **6,219,694** ("the '**694** Patent"), entitled "System and Method for Pushing Information From A Host System To A Mobile Data Communication Device Having A Shared Electronic Address," and issued to the assignee of the instant application on April **17, 2001**, which is hereby incorporated into the present application by reference. This push technique may

use a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device, thus effectively extending the security firewall to include each mobile device **100** associated with the host system **30**.

As shown in FIG. **2**, there may be many alternative paths for getting information to the mobile device **100**. One method for loading information onto the mobile device **100** is through a port designated **50**, using a device cradle **65**. This method tends to be useful for bulk information updates often performed at initialization of a mobile device **100** with the host system **30** or a computer **35** within the system **30**. The other main method for data exchange is over-the-air using wireless networks to deliver the information. As shown in FIG. **2**, this may be accomplished through a wireless VPN router **75** or through a traditional Internet connection **95** to a wireless gateway **85** and a wireless infrastructure **90**, as described above. The concept of a wireless VPN router **75** is new in the wireless industry and implies that a VPN connection could be established directly through a specific wireless network **110** to a mobile device **100**. The possibility of using a wireless VPN router **75** has only recently been available and could be used when the new Internet Protocol (IP) Version **6** (IPV**6**) arrives into IP-based wireless networks. This new protocol will provide enough IP addresses to dedicate an IP address to every mobile device **100** and thus make it possible to push information to a mobile device **100** at any time. A principal advantage of using this wireless VPN router **75** is that it could be an off-the-shelf VPN component, thus it would not require a separate wireless gateway **85** and wireless infrastructure **90** to be used. A VPN connection would preferably be a Transmission Control Protocol (TCP)/IP or User Datagram Protocol (UDP)/IP connection to deliver the messages directly to the mobile device **100**. If a wireless VPN **75** is not available then a link **95** to the Internet **20** is the most common connection mechanism available and has been described above.

In the automatic redirection system of FIG. **2**, a composed e-mail message **15** leaving the e-mail sender **10** arrives at the message server **40** and is redirected by the redirection program **45** to the mobile device **100**. As this redirection takes place the message **15** is re-enveloped, as indicated at **80**, and a possibly proprietary compression and encryption algorithm can then be applied to the original message **15**. In this way, messages being read on the mobile device **100** are no less secure than if they were read on a desktop workstation such as **35** within the firewall. All messages exchanged between the redirection program **45** and the mobile device **100** preferably use this message

repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the "from" field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device **100** allows the received message to appear as though the message originated from the user's desktop system **35** rather than the mobile device **100**.

With reference back to the port **50** and cradle **65** connectivity to the mobile device **100**, this connection path offers many advantages for enabling one-time data exchange of large items. For those skilled in the art of personal digital assistants (PDAs) and synchronization, the most common data exchanged over this link is Personal Information Management (PIM) data **55**. When exchanged for the first time this data tends to be large in quantity, bulky in nature and requires a large bandwidth to get loaded onto the mobile device **100** where it can be used on the road. This serial link may also be used for other purposes, including setting up a private security key **111** such as an S/MIME or PGP specific private key, the Certificate (Cert) of the user and their Certificate Revocation Lists (CRLs) **60**. The private key is preferably exchanged so that the desktop **35** and mobile device **100** share one personality and one method for accessing all mail. The Cert and CRLs are normally exchanged over such a link because they represent a large amount of the data that is required by the device for S/MIME, PGP and other public key security methods.

FIG. **3** depicts a mobile device **230** (e.g., a wireless mobile communications device) receiving one or more messages **210** from a sender **200** over a network **220**. The messages **210** can be e-mail messages or another type of communication from the sender **200**. In the example of FIG. **3**, the sender **200** has requested that a signed receipt be sent back from the mobile device **230**.

To handle the processing of the received message **210** and the requested signed receipt, the mobile device **230** includes notification processing instructions **232**. The notification processing instructions **232** process the received message **210** so that at least a portion **240** of the sender's message is displayed on the device's interface **234** to the user **250**.

FIG. **4** shows more specifically that the notification processing instructions **232** allows a received message (or the message portion(s) that have been received thus far) to be displayed on the device's interface **234** to the user **250** before a notification **260** (e.g., a

signed receipt) is provided to the sender. Accordingly, this allows the notification **260** to be sent while also allowing the user **250** to view the displayed message **240** on the mobile device **230**.

FIG. **5** illustrates that the device **230** on which the user **250** is viewing a received message can send the notification **260** in many different ways, such as manually or automatically. For example, the user **250** can be prompted through prompt **310** to send a signed receipt **300** when the user **250** exits the displayed message **234** irrespective of whether the entire message of the sender has been sent to the device **230**. The user **250** can provide any information needed to handle the viewing and sending of the signed receipt **300** by supplying input **320** to the device **230**. The user **250** can also be prompted for any additional information as well, such as their password, for use in generating a digitally signed receipt **300**.

FIG. **6** depicts that the notification processing instruction **232** can have access to functionality or instructions **350** to handle generation of a signed receipt. The signed receipt generation instructions **350** can be configured such that the notification process occurs in an automatic manner. For example, if a user's private key(s) were encrypted with a low security password that would not require prompting the user, the signed receipt can be automatically sent without user intervention.

Other approaches may be used as well, such as the device **230** prompting at **310** the user **250** for their password to decrypt the private key in order to sign the message, at which point the user could cancel and the signed receipt would not be sent. The user may also not have to supply their password before they exit the message since the user has already been shown the message.

An interface can provide one or more indicators regarding a message's notification process status. For example, the device can display an icon indicating whether notification has been sent. This can be helpful since the signed receipt may or may not have been sent for a particular message. A menu item can also be provided to force the receipt to be sent before exiting the message if that is desired. An indication can also be shown within a sent message that a signed receipt was requested. (It is noted that in a typical desktop implementation, such an indication is not needed because it is assumed that the signed receipt has been sent before the user views the message because the desktop computer has the entire message.) FIG. **7** provides an illustration of an indication **410** being provided through interface **400** that a signed receipt is requested.

FIG. **8** depicts an example operational scenario wherein a message is received by a mobile device at step **500** over a network. The entire message or a portion of the sent message may have been received by the mobile device. At step **502**, the message is viewed by the user. When the notification can be generated, the notification is sent to the sender at step **504**.

The systems and methods disclosed herein are presented only by way of example and are not meant to limit the scope of the invention. Other variations of the systems and methods described above will be apparent to those skilled in the art and as such are considered to be within the scope of the invention. For example, FIG. **9** illustrates that after the message is being displayed at step **502** to the user, the user can elect to exit the message **550**, whereupon the user can be prompted via prompt **554** as to whether to send the signed receipt and/or, if needed, to provide a password via prompt **556**. If the user has indicated that the signed receipt is to be sent and the necessary information to generate the signed receipt has been provided, then the signed receipt is generated and sent to the sender at step **558**. The sender receives the message and validates that it contains a signed receipt for the original message.

In this operational scenario, the signed receipt can be generated in different ways, such as through software instructions (e.g., signed receipt generation instructions **350** of FIG. **6**) that have been configured to digitally sign a receipt for use in acknowledging that the message was successfully delivered and verified.

As another example of the wide scope of the systems and methods disclosed herein, a system and method could be configured to handle the sending of a signed receipt when receiving the message in pieces or chunks at a time. In a resource constrained device, a device can request to receive chunks of the message upon request of the user to view more of the message. The device can send a signed receipt when the last more message chunk arrives which allows a mobile device to verify the message and thus send the signed receipt (or the receipt can be sent as otherwise disclosed herein).

The systems and methods may be provided on many different types of computer-readable media including computer storage mechanisms (e.g., CD-ROM, diskette, RAM, flash memory, computer's hard drive, etc.) that contain instructions for use in execution by a processor to perform the methods' operations and implement the systems described herein. Illustrations of the systems and methods include but are not limited to a mobile device being able to send a signed receipt notification although the entire message may not

have been received yet. As another illustration, a system and method can include receiving a message by the wireless mobile device over a wireless communications network, wherein a sender composed the message intended for receipt by at least one recipient. The received message is processed so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender. As another illustration, a system and method can be configured to include notification processing instructions that can process a message received by the wireless mobile device over a wireless communications network, wherein a sender composed the message intended for receipt by a specific recipient. Signed receipt generation instructions are used to generate a signed receipt based upon the received message. The notification processing instructions are configured to process the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before the generated signed receipt is provided to the sender. The signed receipt can be used at least in part to confirm whether the specific recipient had received the sender's message.

As another example of the wide scope of the systems and methods disclosed herein, the systems and methods may be used with many different computers and devices, such as a wireless mobile communications device shown in FIG. **10**. With reference to FIG. **10**, the mobile device **100** is a dual-mode mobile device and includes a transceiver **611**, a microprocessor **638**, a display **622**, non-volatile memory **624**, random access memory (RAM) **626**, one or more auxiliary input/output (I/O) devices **628**, a serial port **630**, a keyboard **632**, a speaker **634**, a microphone **636**, a short-range wireless communications sub-system **640**, and other device sub-systems **642**.

The transceiver **611** includes a receiver **612**, a transmitter **614**, antennas **616** and **618**, one or more local oscillators **613**, and a digital signal processor (DSP) **620**. The antennas **616** and **618** may be antenna elements of a multiple-element antenna, and are preferably embedded antennas. However, the systems and methods described herein are in no way restricted to a particular type of antenna, or even to wireless communication devices.

The mobile device **100** is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device **100** may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks

are depicted in FIG. **10** by the communication tower **619**. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network.

The transceiver **611** is used to communicate with the network **619**, and includes the receiver **612**, the transmitter **614**, the one or more local oscillators **613** and the DSP **620**. The DSP **620** is used to send and receive signals to and from the transceivers **616** and **618**, and also provides control information to the receiver **612** and the transmitter **614**. If the voice and data communications occur at a single frequency, or closely-spaced sets of frequencies, then a single local oscillator **613** may be used in conjunction with the receiver **612** and the transmitter **614**. Alternatively, if different frequencies are utilized for voice communications versus data communications for example, then a plurality of local oscillators **613** can be used to generate a plurality of frequencies corresponding to the voice and data networks **619**. Information, which includes both voice and data information, is communicated to and from the transceiver **611** via a link between the DSP **620** and the microprocessor **638**.

The detailed design of the transceiver **611**, such as frequency band, component selection, power level, etc., will be dependent upon the communication network **619** in which the mobile device **100** is intended to operate. For example, a mobile device **100** intended to operate in a North American market may include a transceiver **611** designed to operate with any of a variety of voice communication networks, such as the Mobitex or DataTAC mobile data communication networks, AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device **100** intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with a mobile device **100**.

Depending upon the type of network or networks **619**, the access requirements for the mobile device **100** may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if

any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network **619**, other than any legally required operations, such as '**911**' emergency calling.

After any required network registration or activation procedures have been completed, the mobile device **100** may the send and receive communication signals, including both voice and data signals, over the networks **619**. Signals received by the antenna **616** from the communication network **619** are routed to the receiver **612**, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP **620**. In a similar manner, signals to be transmitted to the network **619** are processed, including modulation and encoding, for example, by the DSP **620** and are then provided to the transmitter **614** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network **619** via the antenna **618**.

In addition to processing the communication signals, the DSP **620** also provides for transceiver control. For example, the gain levels applied to communication signals in the receiver **612** and the transmitter **614** may be adaptively controlled through automatic gain control algorithms implemented in the DSP **620**. Other transceiver control algorithms could also be implemented in the DSP **620** in order to provide more sophisticated control of the transceiver **611**.

The microprocessor **638** preferably manages and controls the overall operation of the mobile device **100**. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP **620** could be used to carry out the functions of the microprocessor **638**. Low-level communication functions, including at least data and voice communications, are performed through the DSP **620** in the transceiver **611**. Other, high-level communication applications, such as a voice communication application **624**A, and a data communication application **624**B may be stored in the non-volatile memory **624** for execution by the microprocessor **638**. For example, the voice communication module **624**A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device **100** and a plurality of other voice or dual-mode devices via the network **619**. Similarly, the data communication module **624**B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files,

organizer information, short text messages, etc., between the mobile device **100** and a plurality of other data devices via the networks **619**.

The microprocessor **638** also interacts with other device subsystems, such as the display **622**, the RAM **626**, the auxiliary input/output (I/O) subsystems **628**, the serial port **630**, the keyboard **632**, the speaker **634**, the microphone **636**, the short-range communications subsystem **640** and any other device subsystems generally designated as **642**.

Some of the subsystems shown in FIG. **10** perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as the keyboard **632** and the display **622** may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor **638** is preferably stored in a persistent store such as non-volatile memory **624**. The non-volatile memory **624** may be implemented, for example, as a Flash memory component, or as battery backed-up RAM. In addition to the operating system, which controls low-level functions of the mobile device **610**, the non-volatile memory **624** includes a plurality of software modules **624**A-**624**N that can be executed by the microprocessor **638** (and/or the DSP **620**), including a voice communication module **624**A, a data communication module **624**B, and a plurality of other operational modules **624**N for carrying out a plurality of other functions. These modules are executed by the microprocessor **638** and provide a high-level interface between a user and the mobile device **100**. This interface typically includes a graphical component provided through the display **622**, and an input/output component provided through the auxiliary I/O **628**, keyboard **632**, speaker **634**, and microphone **636**. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM **626** for faster operation. Moreover, received communication signals may also be temporarily stored to RAM **626**, before permanently writing them to a file system located in a persistent store such as the Flash memory **624**.

An exemplary application module **624**N that may be loaded onto the mobile device **100** is a personal information manager (PIM) application providing PDA functionality, such as calendar events, appointments, and task items. This module **624**N may also

interact with the voice communication module **624**A for managing phone calls, voice mails, etc., and may also interact with the data communication module for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module **624**A and the data communication module **624**B may be integrated into the PIM module.

The non-volatile memory **624** preferably also provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules **624**A, **624**B, via the wireless networks **619**. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless networks **619**, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

Context objects representing at least partially decoded data items, as well as fully decoded data items, are preferably stored on the mobile device **100** in a volatile and non-persistent store such as the RAM **626**. Such information may instead be stored in the non-volatile memory **624**, for example, when storage intervals are relatively short, such that the information is removed from memory soon after it is stored. However, storage of this information in the RAM **626** or another volatile and non-persistent store is preferred, in order to ensure that the information is erased from memory when the mobile device **100** loses power. This prevents an unauthorized party from obtaining any stored decoded or partially decoded information by removing a memory chip from the mobile device **100**, for example.

The mobile device **100** may be manually synchronized with a host system by placing the device **100** in an interface cradle, which couples the serial port **630** of the mobile device **100** to the serial port of a computer system or device. The serial port **630** may also be used to enable a user to set preferences through an external device or software application, or to download other application modules **624**N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network **619**. Interfaces for other wired download paths may be provided in the mobile device **100**, in addition to or instead of the serial port **630**. For example, a USB port would provide an interface to a similarly equipped personal computer.

Additional application modules **624**N may be loaded onto the mobile device **100** through the networks **619**, through an auxiliary I/O subsystem **628**, through the serial port **630**, through the short-range communications subsystem **640**, or through any other suitable subsystem **642**, and installed by a user in the non-volatile memory **624** or RAM **626**. Such flexibility in application installation increases the functionality of the 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 the mobile device **100**.

When the mobile device **100** is operating in a data communication mode, a received signal, such as a text message or a web page download, is processed by the transceiver module **611** and provided to the microprocessor **638**, which preferably further processes the received signal in multiple stages as described above, for eventual output to the display **622**, or, alternatively, to an auxiliary I/O device **628**. A user of mobile device **100** may also compose data items, such as e-mail messages, using the keyboard **632**, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device **100** is further enhanced with a plurality of auxiliary I/O devices **628**, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the communication networks **619** via the transceiver module **611**.

When the mobile device **100** is operating in a voice communication mode, the overall operation of the mobile device is substantially similar to the data mode, except that received signals are preferably be output to the speaker **634** and voice signals for transmission are generated by a microphone **636**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile device **100**. Although voice or audio signal output is preferably accomplished primarily through the speaker **634**, the display **622** may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor **638**, in conjunction with the voice communication module and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display **622**.

A short-range communications subsystem **640** is also included in the mobile device **100**. The subsystem **640** may include an infrared device and associated circuits and components, or a short-range RF communication module such as a Bluetooth™ module or an **802.11** module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "Bluetooth" and "**802.11**" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.

It is further noted that the systems and methods may be implemented on various types of computer architectures and data signals to/from a device may be conveyed via fiber optic medium, carrier waves, wireless networks, etc. for communication among multiple devices. The systems' and methods' data may be stored in one or more data stores. The data stores can be of many different types of storage devices and programming constructs, such as RAM, ROM, Flash memory, programming data structures, programming variables, etc. It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program.

The computer components, software modules, functions and data structures described herein may be connected directly or indirectly to each other in order to allow the flow of data needed for their operations. It is also noted that a module or processor includes but is not limited to a unit of code that performs a software operation, and can be implemented for example as a subroutine unit of code, or as a software function unit of code, or as an object (as in an object-oriented paradigm), or as an applet, or in a computer script language, or as another type of computer code, such as Java.

CLAIMS:

1. A method for operation upon a wireless mobile device to handle message notifications, comprising:

receiving a message by the wireless mobile device over a wireless communications network;

wherein a sender composed the message intended for receipt by at least one recipient;

processing the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender;

wherein the signed receipt is used at least in part to confirm whether the intended recipient had received the sender's message.

2. The method of claim 1, wherein the signed receipt provides an indication to the sender that the message has been verified by the intended recipient of the message.

3. The method of claim 1, wherein generation of the signed receipt includes verifying the message;

wherein after the message is verified, the signed receipt is provided to the sender.

4. The method of claim 3, wherein a substantial portion or the entire message is needed before the message can be verified.

5. The method of claim 4, wherein the device is a constrained device.

6. The method of claim 5, wherein the message is provided to the wireless mobile device in portions.

7. The method of claim 6, wherein the user of the wireless mobile device provides a request for an additional portion of the message to be provided to the wireless mobile device.

8. The method of claim 7, wherein the user provides the request while viewing at least a portion of the message.

9. The method of claim 1, wherein the signed receipt is digitally signed by the recipient through use of a private key of the recipient.

10. The method of claim 1, wherein the message is an email message.

11. The method of claim 1, wherein, without said processing of the received message, the signed receipt is to be sent before the message is displayed.

12. The method of claim 1, wherein the signed receipt notification is provided to the sender although the entire message has not have been received by the wireless mobile device.

13. The method of claim 1, wherein the user is prompted to send the signed receipt when the user exits the displayed message irrespective of whether the entire message of the sender has been sent to the device; wherein the user is prompted for the user's password for use in generating a digitally signed receipt.

14. The method of claim 1, wherein interface indicators are provided to indicate the status with respect to a signed receipt.

15. The method of claim 1, wherein the wireless mobile device is a wireless mobile communications device.

16. The method of claim 1, wherein the wireless mobile device is a personal digital assistant (PDA).

17. A data signal that is transmitted using the wireless network, wherein the data signal includes the generated signed receipt of claim 1.

18. Computer-readable medium capable of causing a computing device to perform the method of claim 1.

19. A system for operation upon a wireless mobile device to handle message notifications, comprising:

notification processing instructions configured to process a message received by the wireless mobile device over a wireless communications network;

wherein a sender composed the message intended for receipt by at least one recipient;

signed receipt generation instructions configured to generate a signed receipt based upon the received message;

wherein the notification processing instructions are configured to process the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before the generated signed receipt is provided to the sender;

wherein the signed receipt is used at least in part to confirm whether the intended recipient had received the sender's message.

20. A system for operation upon a wireless mobile device to handle message notifications, comprising:

means for receiving a message by the wireless mobile device over a wireless communications network;

wherein a sender composed the message intended for receipt by at least one recipient;

means for processing the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender;

wherein the signed receipt is used at least in part to confirm whether the intended recipient had received the sender's message.

AMENDED CLAIMS

received by the International Bureau on 07 November 2005 (07.11.2005): original claims 1-20 have been replaced by amended claims 1-20.

1. A method for operation upon a wireless mobile device to handle message notifications, comprising:

receiving a message by the wireless mobile device over a wireless communications network;

wherein a sender composed the message intended for receipt by at least one recipient;

processing the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender;

wherein the signed receipt is used at least in part to confirm whether the intended recipient had received the sender's message.

2. The method of claim 1, wherein the signed receipt provides an indication to the sender that the message has been verified by the intended recipient of the message.

3. The method of claim 1, wherein in the processing of the received message, at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is generated and provided to the sender;

wherein the generation of the signed receipt includes verifying the message;

wherein after the message is verified, the signed receipt is provided to the sender.

4. The method of claim 3, wherein at least a portion or the entire message is needed before the message can be verified.

5. The method of claim 4, wherein the device is a constrained device.

6. The method of claim 5, wherein the message is provided to the wireless mobile device in portions.

7. The method of claim 6, wherein the user of the wireless mobile device provides a request for an additional portion of the message to be provided to the wireless mobile device.

8. The method of claim 7, wherein the user provides the request while viewing at least a portion of the message.

9. The method of claim 1, wherein the signed receipt is digitally signed by the recipient through use of a private key of the recipient.

10. The method of claim 1, wherein the message is an email message.

11. The method of claim 1, wherein, with said processing of the received message the signed receipt is to be sent after at least a portion of the message is displayed;

wherein without said processing of the received message, the signed receipt is to be sent before the message is displayed.

12. The method of claim 1, wherein a signed receipt notification is provided to the sender although the entire message has not been received by the wireless mobile device.

13. The method of claim 1, wherein the user is prompted to send the signed receipt when the user exits the displayed message irrespective of whether the entire message of the sender has been sent to the device; wherein the user is prompted for the user's password for use in generating a digitally signed receipt.

14. The method of claim 1, wherein interface indicators are provided to indicate status with respect to a signed receipt.

15. The method of claim 1, wherein the wireless mobile device is a wireless mobile communications device.

16. The method of claim 1, wherein the wireless mobile device is a personal digital assistant (PDA).

17. A data signal that is transmitted using the wireless communications network, wherein the data signal includes the generated signed receipt of claim 1.

18. A computer-readable medium having recorded thereon instructions which, when executed by a computing device, cause the computing device to perform the method of claim 1.

19. A system for operation upon a wireless mobile device to handle message notifications, comprising:

notification processing instructions configured to process a message received by the wireless mobile device over a wireless communications network;

wherein a sender composed the message intended for receipt by at least one recipient;

signed receipt generation instructions configured to generate a signed receipt based upon the received message;

wherein the notification processing instructions are configured to process the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before the generated signed receipt is provided to the sender;

wherein the signed receipt is used at least in part to confirm whether the intended recipient had received the sender's message.

20. A system for operation upon a wireless mobile device to handle message notifications, comprising:

means for receiving a message by the wireless mobile device over a wireless communications network;

wherein a sender composed the message intended for receipt by at least one recipient;

means for processing the received message so that at least a portion of the sender's message is displayed to a user of the wireless mobile device before a signed receipt is provided to the sender;

wherein the signed receipt is used at least in part to confirm whether the intended recipient had received the sender's message.

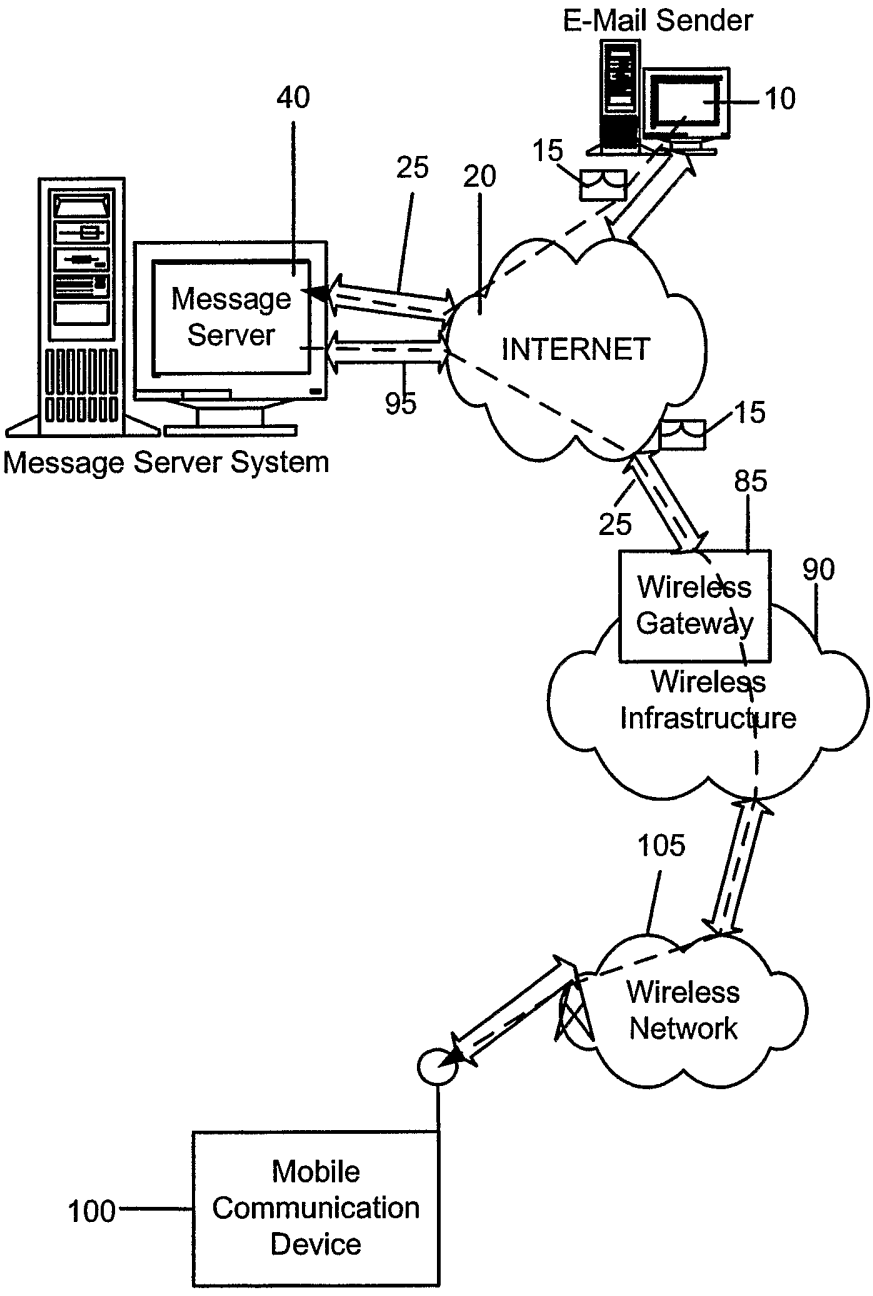

E-Mail Sender
10
40
15
25
20
Message Server
INTERNET
95
15
Message Server System
85
25
90
Wireless Gateway
Wireless Infrastructure
105
Wireless Network
100
Mobile Communication Device

FIG. 1

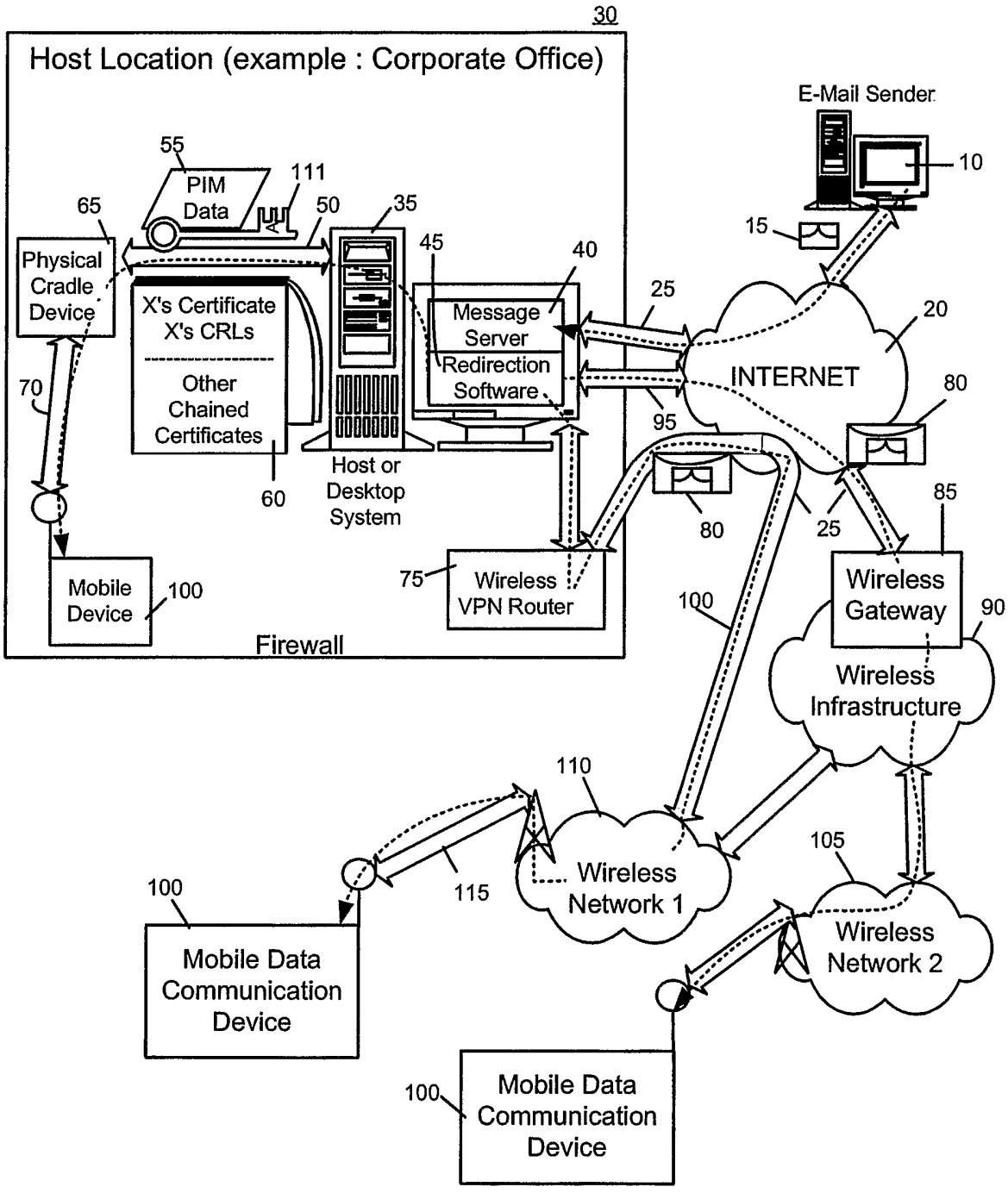

30
Host Location (example : Corporate Office)
E-Mail Sender
10
55
PIM Data
111
50
35
65
Physical Cradle Device
45
40
15
X's Certificate
X's CRLs
Other Chained Certificates
Message Server
Redirection Software
25
20
INTERNET
70
80
95
60
Host or Desktop System
80
25
85
Mobile Device
100
75
Wireless VPN Router
Firewall
100
Wireless Gateway
90
Wireless Infrastructure
110
105
Wireless Network 1
Wireless Network 2
115
100
Mobile Data Communication Device
100
Mobile Data Communication Device

FIG. 2

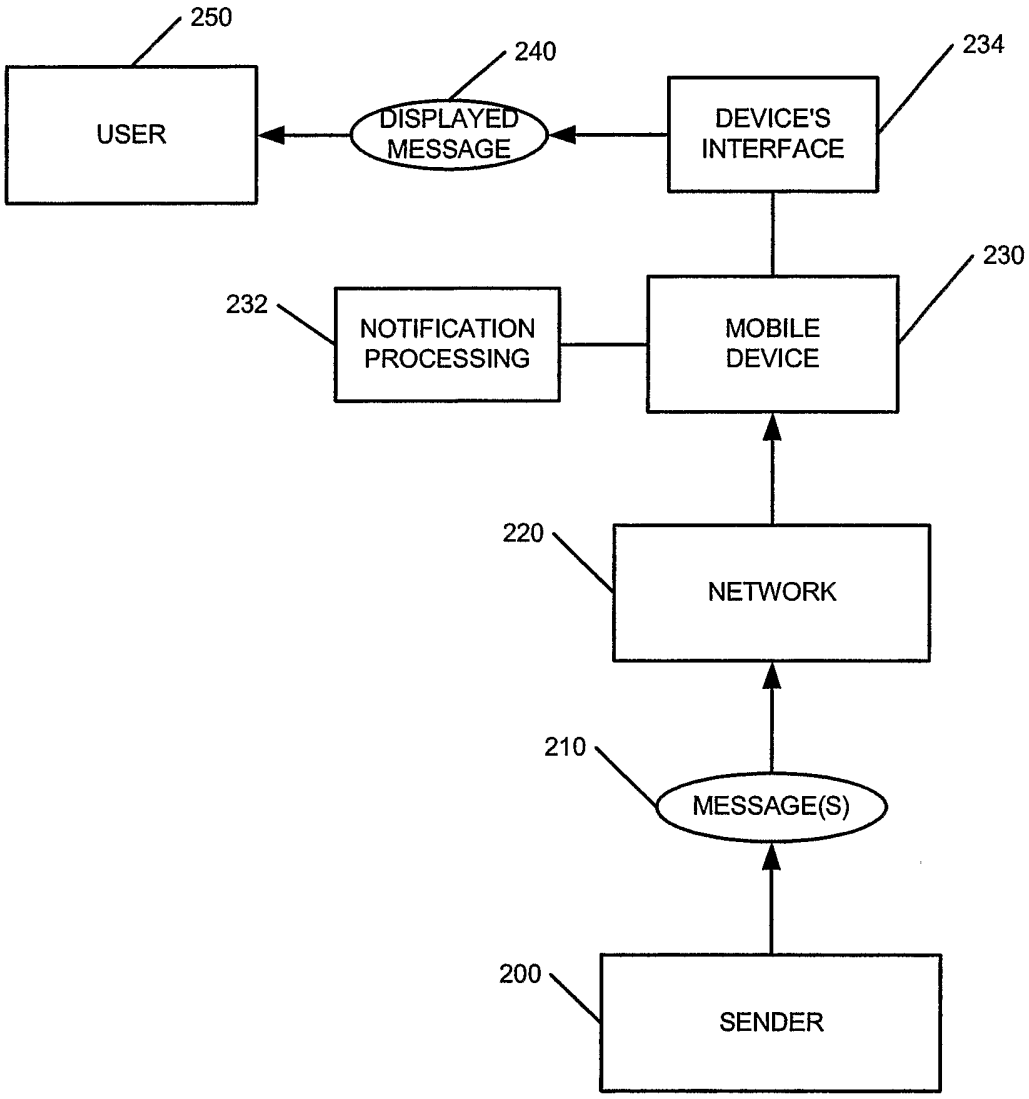

250
USER
240
DISPLAYED MESSAGE
234
DEVICE'S INTERFACE
232
NOTIFICATION PROCESSING
230
MOBILE DEVICE
220
NETWORK
210
MESSAGE(S)
200
SENDER

FIG. 3

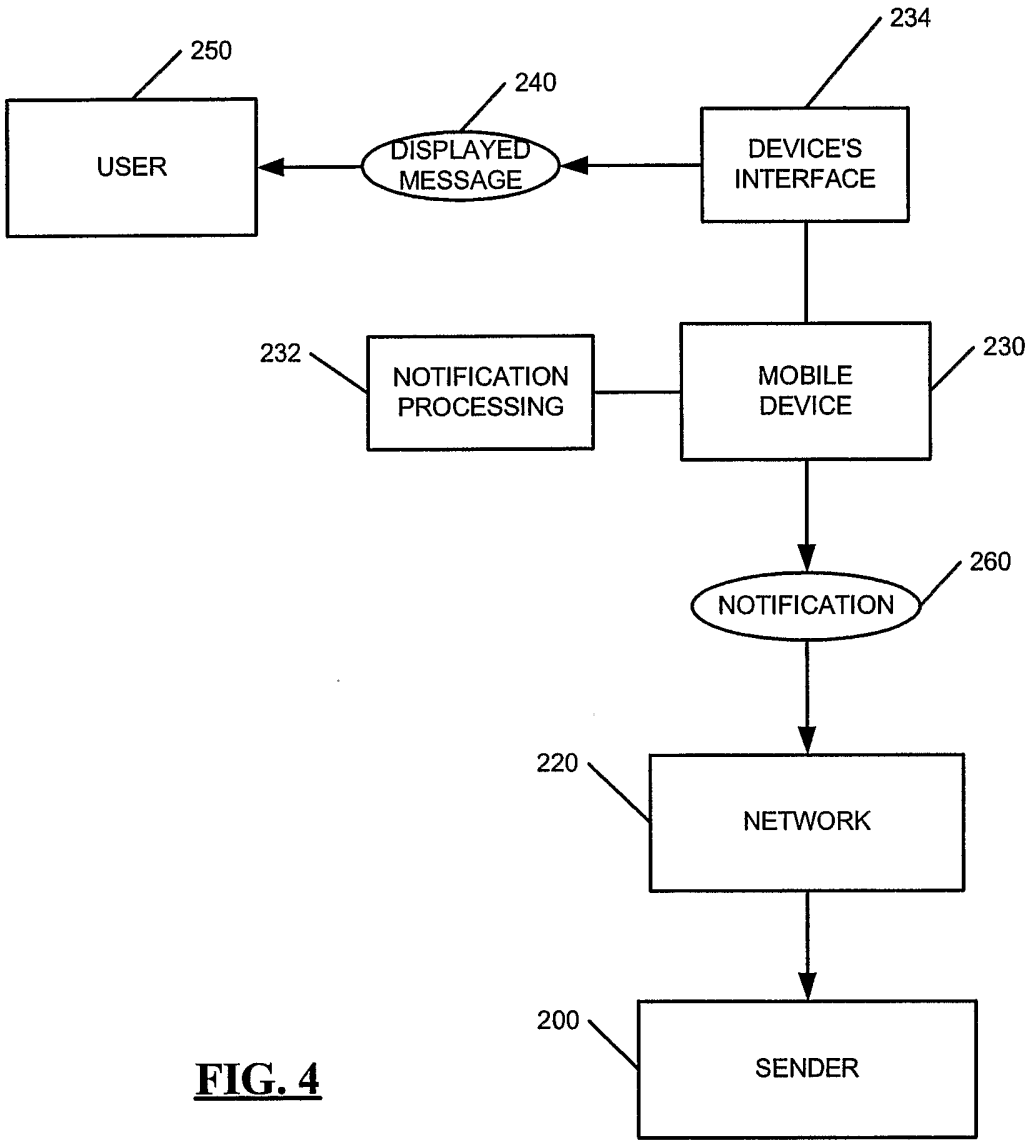

250
USER
240
DISPLAYED MESSAGE
234
DEVICE'S INTERFACE
232
NOTIFICATION PROCESSING
230
MOBILE DEVICE
260
NOTIFICATION
220
NETWORK
200
SENDER

FIG. 4

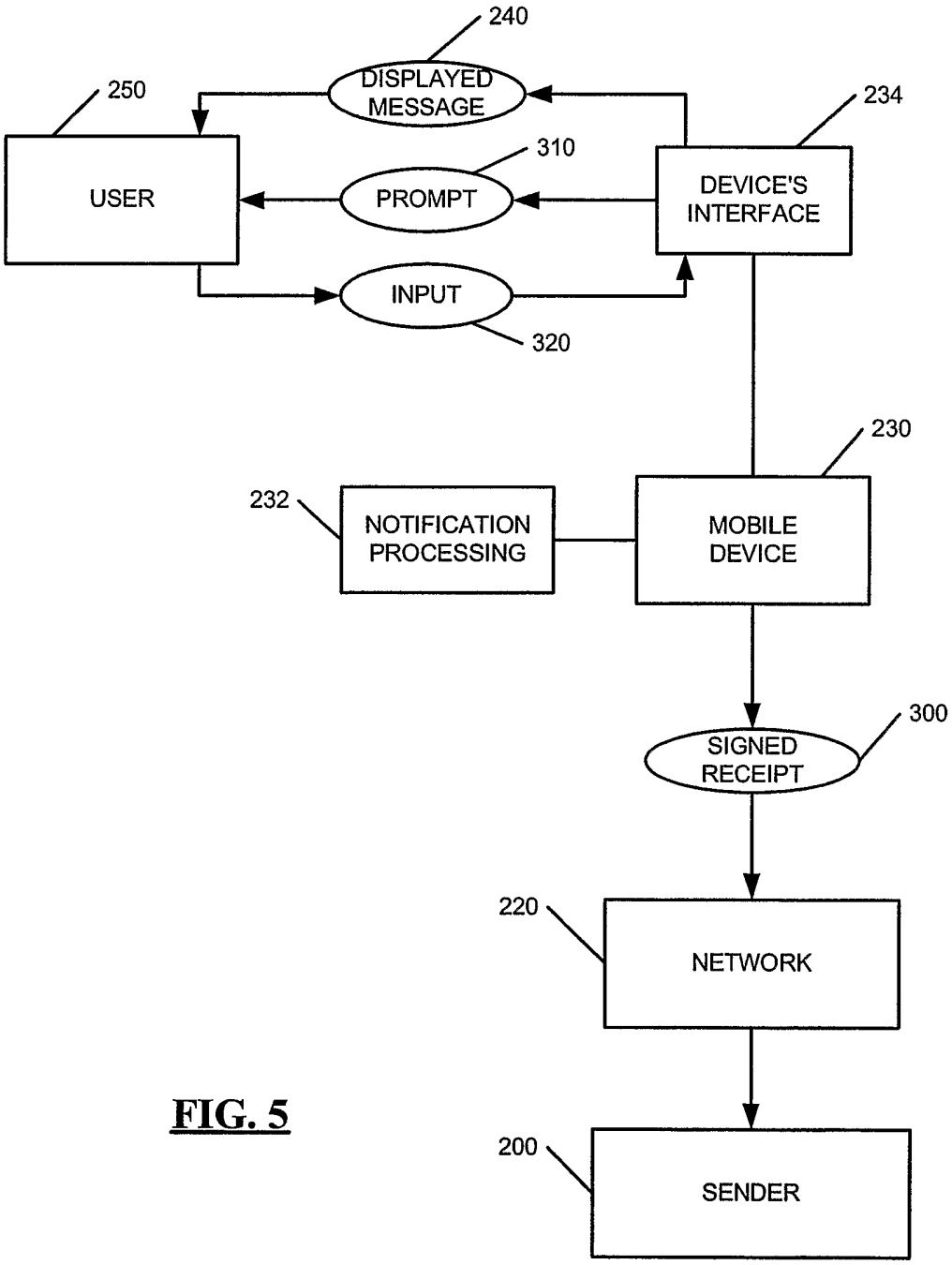

240
DISPLAYED MESSAGE
250
USER
310
PROMPT
234
DEVICE'S INTERFACE
INPUT
320
230
232
NOTIFICATION PROCESSING
MOBILE DEVICE
300
SIGNED RECEIPT
220
NETWORK
200
SENDER

FIG. 5

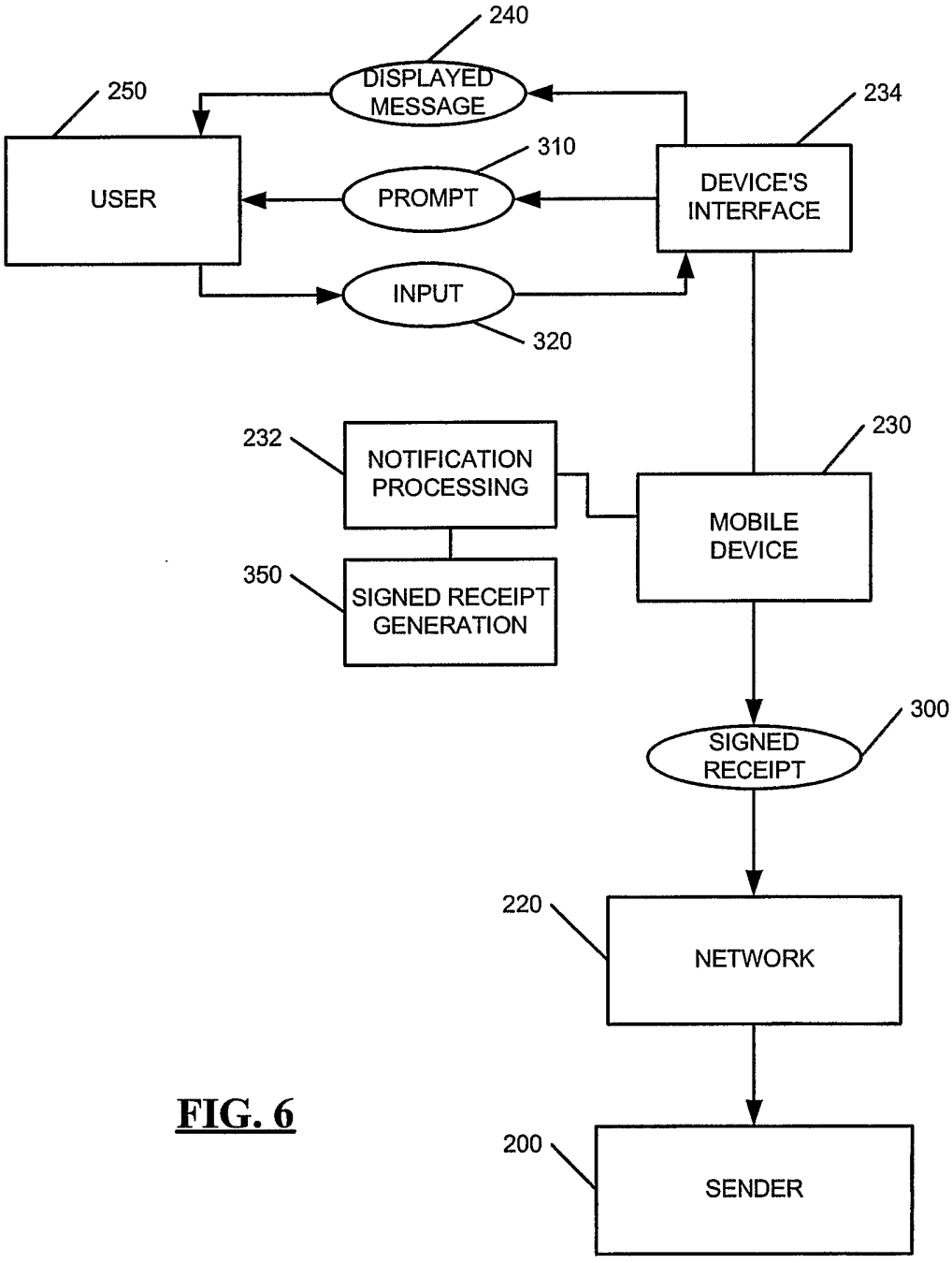

240
DISPLAYED MESSAGE
250
USER
234
DEVICE'S INTERFACE
310
PROMPT
INPUT
320
232
NOTIFICATION PROCESSING
230
MOBILE DEVICE
350
SIGNED RECEIPT GENERATION
300
SIGNED RECEIPT
220
NETWORK
200
SENDER

FIG. 6

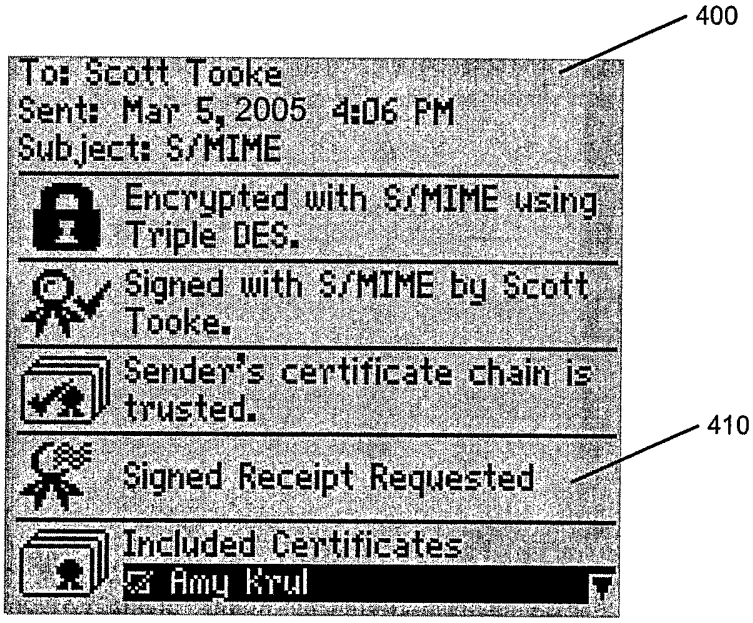

400
To: Scott Tooke
Sent: Mar 5, 2005 4:06 PM
Subject: S/MIME
Encrypted with S/MIME using Triple DES.
Signed with S/MIME by Scott Tooke.
Sender's certificate chain is trusted.
410
Signed Receipt Requested
Included Certificates
Amy Krul

FIG. 7

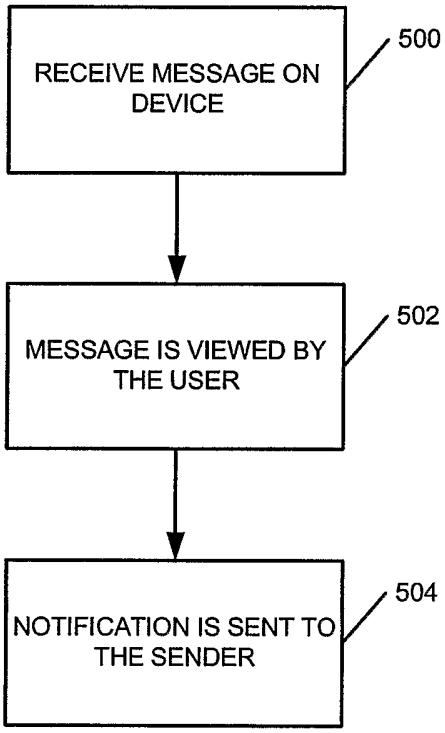

RECEIVE MESSAGE ON DEVICE
500
MESSAGE IS VIEWED BY THE USER
502
NOTIFICATION IS SENT TO THE SENDER
504

FIG. 8

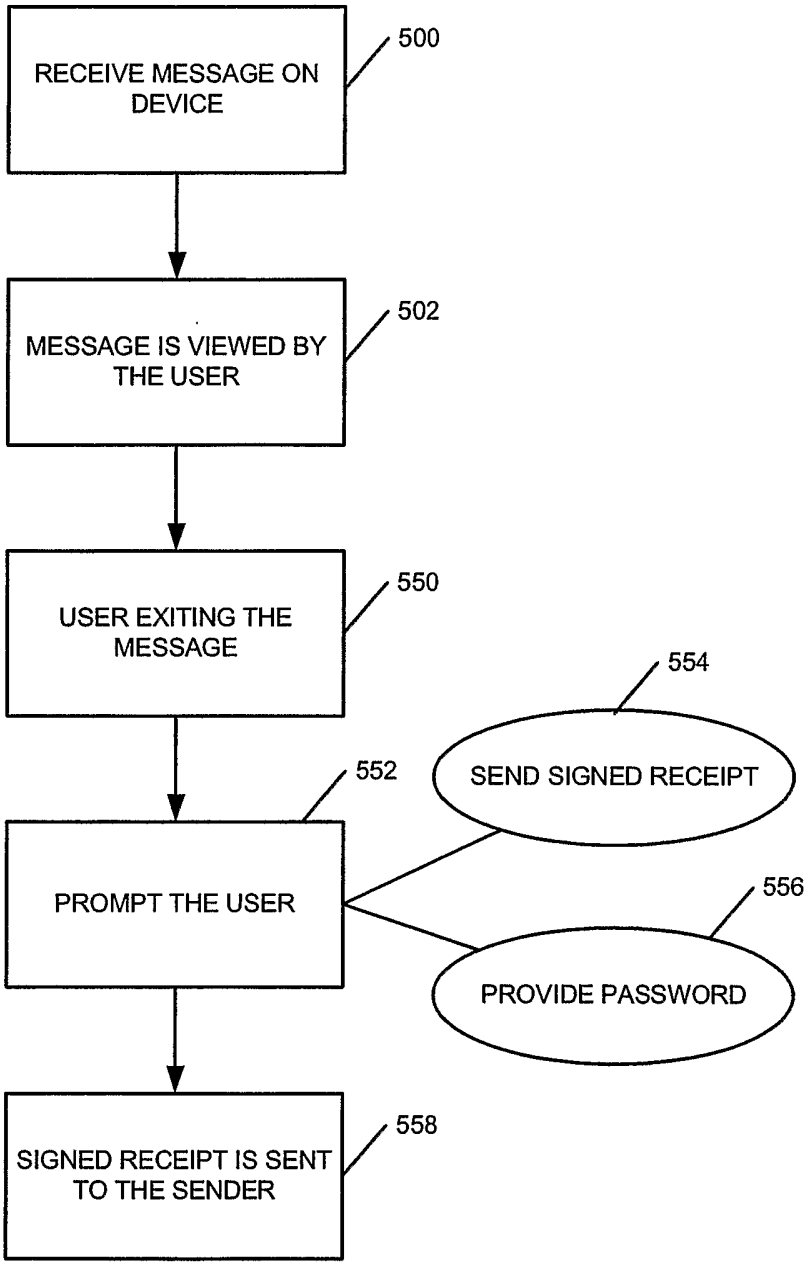

RECEIVE MESSAGE ON DEVICE
500
MESSAGE IS VIEWED BY THE USER
502
USER EXITING THE MESSAGE
550
554
SEND SIGNED RECEIPT
552
PROMPT THE USER
556
PROVIDE PASSWORD
SIGNED RECEIPT IS SENT TO THE SENDER
558

FIG. 9

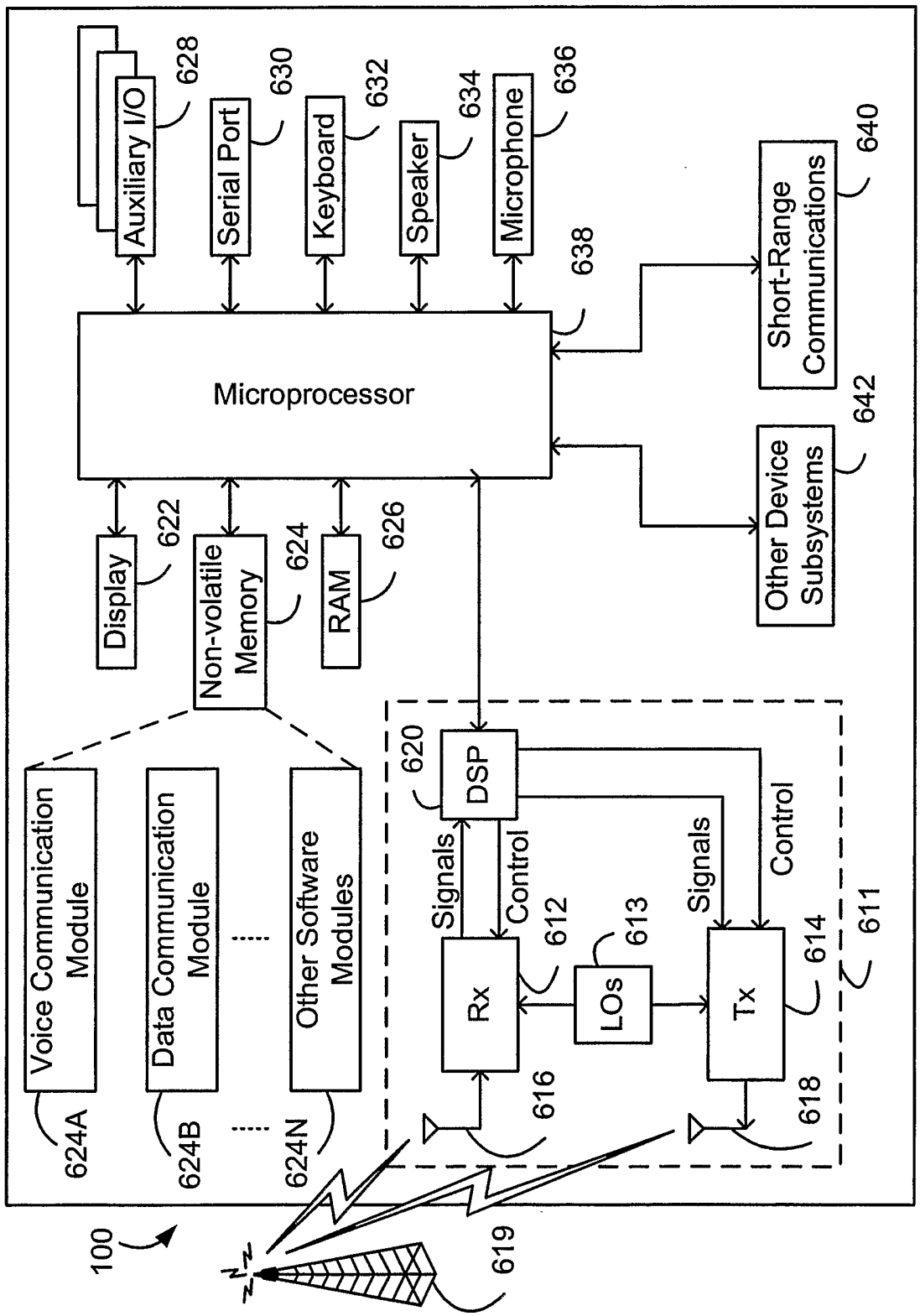

Auxiliary I/O
628
Serial Port
630
Keyboard
632
Speaker
634
Microphone
636
638
Microprocessor
Short-Range Communications
640
Other Device Subsystems
642
Display
622
Non-volatile Memory
624
RAM
626
Voice Communication Module
Data Communication Module
Other Software Modules
624A
624B
624N
DSP
620
Signals
Control
Rx
612
LOs
613
Tx
614
611
616
618
619
100

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000962

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7): H04L 12/54, H04Q 7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC (7): H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Derwent, Canadian Patent Database, IEEE Xplore, Google, Qweb-PlusPat. Some keywords used: sender/creator/originator, receiver/recipient, response/acknowledgment/receipt/notification, message/mail/email/e-mail/electronic mail/electronic message, mobile/wireless/portable/radio/handheld/PDA, portion/part*/fraction/fragment/piece, display/view/open, signed/signature, encrypt/secure.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/49766 A1 (Vatanen et al.) 24 August 2000 (24-08-2000) *abstract* *page 3, line 24 - page 4, line 21* *page 4, line 32 - page 5, line 26*	1-3, 9, 19, 20
A	P. Hoffman: "Enhanced Security Services for S/MIME" Internet Mail Consortium, June 1999. Retrieved from the internet at www.apps.ietf.org/rfc/rfc2634.html *page 10, section 2 - page 24, section 2.11*	1-3, 9, 10, 19, 20
A	WO 01/17165 A2 (Smith et al.) 8 March 2001 (08-03-2001) *page 6, line 26 - page 12, line 1* *Figures 3A-3B*	1, 19, 20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 August 2005 (16-08-2005)	7 September 2005 (07-09-2005)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Georges Matar (819) 994-6366

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000962

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 629 982 A (Micali) 13 May 1997 (13-05-1997) *abstract* *column 3, lines 51 - 67* *column 6, line 34 - column 9, line 15* *column 11, line 60 - column 13, line 8*	1, 19, 20
A	CA 2 141 900 A1 (Mandelbaum et al.) 8 September 1995 (08-09-1995) *abstract* *page 2, line 24 - page 3, line 29*	1, 19, 20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2005/000962

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO0049766 A1	24-08-2000	AU2674600 A	04-09-2000
		EP1153495 A1	14-11-2001
		FI107205B B1	15-06-2001
		US2003078058 A1	24-04-2003
WO0117165 A2	08-03-2001	AU6910500 A	26-03-2001
		CA2383000 A1	08-03-2001
		EP1212880 A2	12-06-2002
		JP2003535386 T	25-11-2003
		NO20020963 A	19-04-2002
		US6725381 B1	20-04-2004
		US2004153645 A1	05-08-2004
US5629982 A	13-05-1997	CA2215908 A1	26-09-1996
		CA2261947 A1	12-02-1998
		EP0815671 A1	07-01-1998
		EP0917781 A1	26-05-1999
		JP2000515649 T	21-11-2000
		US5553145 A	03-09-1996
		US5666420 A	09-09-1997
		US6134326 A	17-10-2000
		US6137884 A	24-10-2000
		US6141750 A	31-10-2000
		WO9629795 A1	26-09-1996
		WO9806198 A1	12-02-1998
CA2141900 A1	08-09-1995	EP0671830 A2	13-09-1995
		JP7298065 A	10-11-1995
		NO313850B B1	09-12-2002
		SG28196 A1	01-04-1996
		US5552897 A	03-09-1996