



(22) Date de dépôt/Filing Date: 2004/08/10

(41) Mise à la disp. pub./Open to Public Insp.: 2006/02/10

(51) Cl.Int./Int.Cl. *H04L 9/00* (2006.01),
H04L 29/00 (2006.01), *H04L 12/54* (2006.01)

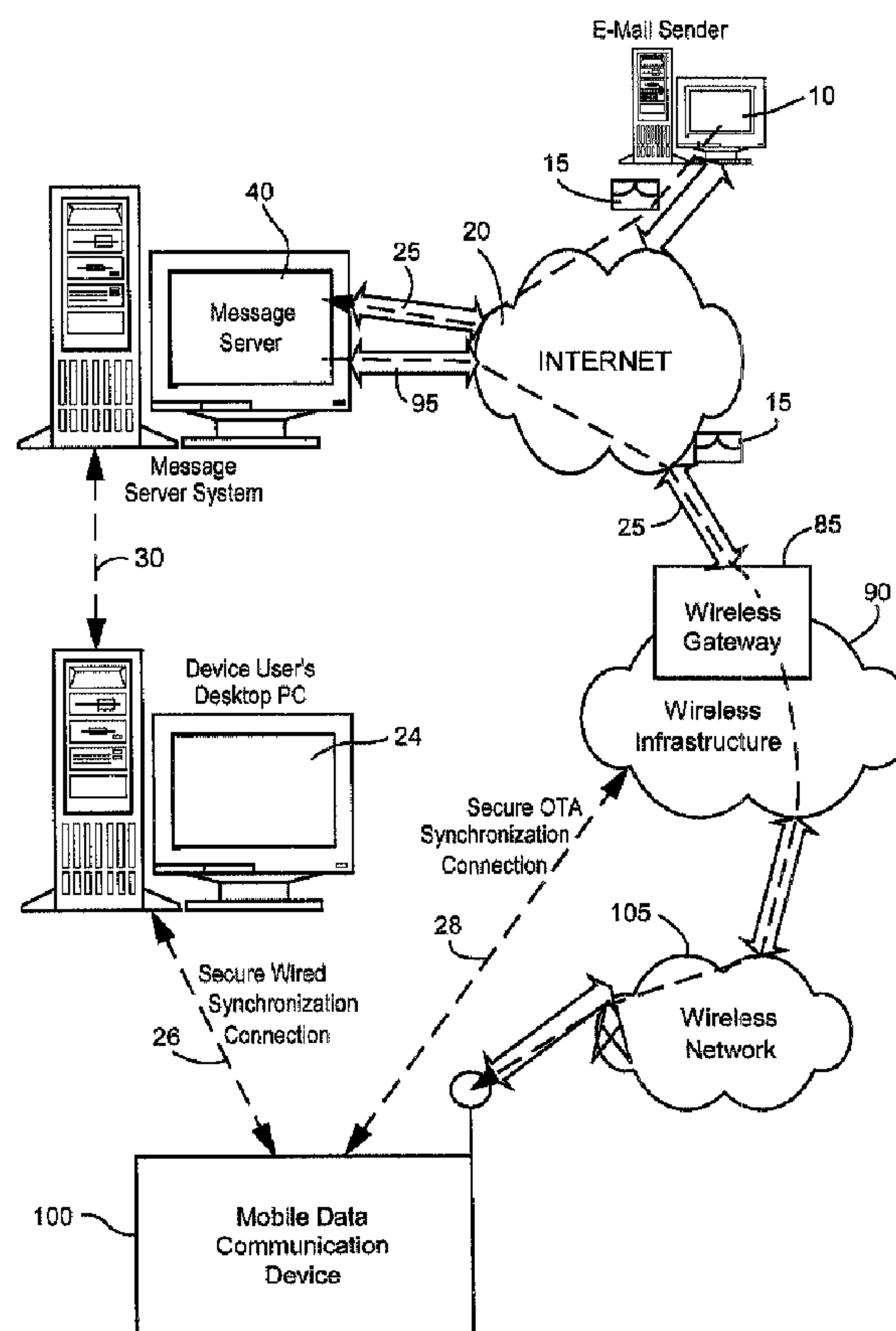
(71) Demandeur/Applicant:
RESEARCH IN MOTION LIMITED, CA

(72) Inventeurs/Inventors:
BROWN, MICHAEL K., CA;
BROWN, MICHAEL S., CA;
ADAMS, NEIL P., CA;
KIRKUP, MICHAEL G., CA;
LITTLE, HERBERT A., CA

(74) Agent: BORDEN LADNER GERVAIS LLP

(54) Titre : VERIFICATION DE MESSAGES ELECTRONIQUES SECURISES PAR UN SERVEUR

(54) Title: SERVER VERIFICATION OF SECURE ELECTRONIC MESSAGES



(57) Abrégé/Abstract:

Systems and methods for processing encoded messages within a wireless communications system are disclosed. A server within the wireless communications system determines whether the size of an encoded message is too large for a wireless



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

communications device. If the message is too large, the server removes part of the message and sends an abbreviated message to the wireless device, together with additional information relating to processing of the encoded message, such as, for example, hash context values, that assist the wireless communications device in verifying the abbreviated message.

ABSTRACT

Systems and methods for processing encoded messages within a wireless communications system are disclosed. A server within the wireless communications system determines whether the size of an encoded message is too large for a wireless communications device. If the message is too large, the server removes part of the message and sends an abbreviated message to the wireless device, together with additional information relating to processing of the encoded message, such as, for example, hash context values, that assist the wireless communications device in verifying the abbreviated message.

SERVER VERIFICATION OF SECURE ELECTRONIC MESSAGES

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to an electronic messaging system that is capable of processing encoded messages and information. In particular, the disclosure is directed to a system in which an electronic message server performs at least a portion of the verification functions typically performed by a mobile wireless communications device having secure electronic messaging capability, especially where an encoded message is too large for verification on the mobile wireless communications device.

2. Related Art

Exchanging cryptographically encoded secure electronic messages and data, such as, for example, e-mail messages, is well known. In many known electronic message exchange schemes, signatures, encryption or both are commonly used to ensure the integrity and confidentiality of information being exchanged between a sender and a recipient of the electronic messages. In an e-mail system, for example, the sender of an e-mail message may either sign the message, encrypt the message or both sign and encrypt the message. These actions may be performed using well-known standards, such as, for example, Secure Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy™ (PGP™), OpenPGP, and numerous other secure e-mail standards.

In general, secure e-mail messages are relatively large. For example, S/MIME can increase the size of an e-mail message by a factor of ten or more in some situations. This size augmentation presents difficulties, especially in devices that have a limit on the size of a message

that can be processed, such as, for example, a mobile wireless communications device. Such a device may also experience difficulty handling a message wherein only a portion of the message has been transferred to the device because of the above-mentioned size limitations.

For example, if a message is larger than the size limit of the device, then the entire message will never reach the device. If this large message is a signed or encoded message, then all the data required to verify the signature may not be sent to the device, and thus, the device may not be able to verify the signature.

BRIEF SUMMARY OF THE INVENTION

In view of the foregoing, we have now identified an efficient and easy to implement system and method for verifying secure electronic messages, wherein some of the processing overhead associated with decoding and/or verifying secure messages is distributed from a device having a size limit, such as, for example, a mobile wireless communications device, to a device having the ability to process much larger size messages, such as, for example, a server within the wireless communications system.

According to an exemplary embodiment of the present disclosure, a server within the wireless communications system has the ability to determine if a secure message is too large to be verified on a size-limited device. The server may make this determination by finding the point in the secure electronic message encoding where the message will be cut off due to the size constraints of the size-limited device. The server determines if the cut off point occurs in such a location that verification of the message will not be possible on the size-limited device, such as, for example, part way through the signed data or in the middle of the signature data. If the message is determined to be too long such that verification on the device is not possible, then the server can attempt to verify the signature on the message.

According to an exemplary embodiment of the disclosure, the server is operable to assist the size-limited device in verifying the message itself. For example, if a secure (e.g., signed and/or encrypted) message that is too large for the size-limited device is made up of three parts, A, B and C, where B is an attachment, the server may remove the attachment B from the message. Consequently, the attachment B will not be sent to the size-limited device. Because the attachment has been removed from the electronic message, the size-limited device will be unable to verify the signature. In order to assist the size-limited device in verifying the message, the server may apply a hashing function to parts A, B and C, in sequence. After each part has been hashed, the hashing function has a context associated therewith. The size-limited device, of course, only has parts A and C, so when it performs a hash, it will have the same context after hashing part A, but will have the incorrect starting context when it hashes part C. In a preferred embodiment, the hashing function applied to parts A, B and C may be the same as that used in signature generation.

In this situation, the server can insert the hash context after it hashed part A and the hash context after it hashed part B in place of the attachment B in the original message. Because the hash contexts are much smaller than the application data, the size-limited device should be able to accept this data. Accordingly, after the size-limited device performs its hash of part A, it can compare the hash context obtained from hashing part A with the hash context received from the server when it hashed part A. If these contexts match, the device can then substitute the hash context received from the server after it hashed part B, and the device can then continue to hash part C. This result can then be used to verify the signature.

In another exemplary embodiment of the disclosure, the server could alternatively insert the result of performing an exclusive OR function (XOR) of the context after hashing part A with

the context after hashing part B. The device would then perform a hash of part A, take this context and perform an XOR with the value the server provides. The device then takes the result of that XOR function and uses it as the context after hashing part B. This alternative further reduces the amount of data required to be sent to the size-limited device.

As a further alternative exemplary embodiment, the server may only verify levels of the message. For example, in S/MIME the actual steps involved in verifying a message involve taking multiple digests and then performing an actual signature verification calculation. In this embodiment, the server may verify that the digests match, but leave the signature verification calculation to the size-limited device.

The foregoing exemplary embodiments provide a solution to the problem of verifying secured electronic messages by a size-limited device by distributing the processing overhead to a server of the electronic messaging system, thereby enabling the sharing of system resources to assist the size-limited device in verifying secured electronic messages.

The advantages attendant with the various embodiments of the invention described above are provided by the method and system of automated key management disclosed and described herein with reference to the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of exemplary embodiments of the present invention will be better understood and appreciated in conjunction with the following detailed description of exemplary embodiments taken together with the accompanying drawings, in which:

FIG. 1 is an overall system wide schematic view of an exemplary wireless e-mail communication system incorporating a mobile wireless communications device with the descriptive error messaging in accordance with an exemplary embodiment of the present invention;

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

FIG. 3 is an illustrative schematic block diagram of an exemplary mobile wireless communications device;

FIG. 4 is a block diagram depicting components used in handling encoded messages;

FIG. 5 is an illustrative flow diagram of an exemplary operational scenario for processing encoded messages according to an exemplary embodiment of the invention; and

FIG. 6 is an illustrative flow diagram of an alternative exemplary operational scenario according to another exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

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), RFC822 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 at least one of 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 300, 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 300 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 300 is the message server 400, 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 400 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 400 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 400 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 300.

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 300 or a computer 35 within the system 300. 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 (IPV6) 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 400 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.

As depicted in FIG. 3, mobile communications device 100 includes a suitable RF antenna 102 for wireless communication to/from wireless network 20. Conventional RF, demodulation/modulation and decoding/coding circuits 104 are provided. As those in the art will appreciate,

such circuits may involve possibly many digital signal processors (DSPs), microprocessors, filters, analog and digital circuits and the like. However, since such circuitry is well known in the art, it is not further described herein.

The mobile communications device 100 will also typically include a main control CPU 106 that operates under the control of a stored program in program memory 108, and which has access to data memory 110. CPU 106 also communicates with a conventional keyboard 112 and display 114 (for example, a liquid crystal display or LCD) and audio transducer or speaker 116. A portion of the data memory 310 is available for storing data required for decrypting encrypted messages, such as, for example, private keys, digital certificates, and the like. Suitable computer program executable code is stored in portions of the program memory 108 to constitute stored program logic for receiving and using new or added private keys and/or digital certificates or the like as described below (for example, via a wired serial I/O port or the wireless RF antenna 102).

As depicted in FIG. 1, a secure wired synchronization connection 26 (for example, between serial I/O ports of the user's base unit 24 and the wireless device 100) is typically provided for normal data synchronization purposes (for example, to synchronize databases in the two devices with respect to such things as calendars, to-do lists, task lists, address books, etc.). Part of prior data synchronization processes has included a program logic such as Cert Sync for maintaining synchronization between cryptographic message certificates. If a secure over the air (OTA) synchronization connection 28 is available, it may also be used by Cert Sync to maintain synchronization of cryptographic message certificates.

As previously described, there is a communications link (for example, depicted in dotted lines at 30 in FIG. 1) typically found between the device user's base unit 24 and a system message server 14. Accordingly, there is an existing communication path that may be utilized

for passing synchronization data from the user's base unit 24 via channel 30, the server 14, Internet 12, wireless gateway 16 and wireless infrastructure 18 via the OTA synchronization connection 28.

E-mail messages generated using the S/MIME and PGP techniques may include encrypted information, a digital signature on the message contents, or both. In signed S/MIME operations the sender takes a digest of a message and signs the digest using the sender's private key. A digest is essentially a checksum, CRC or other preferably non-reversible operation such as a hash of the message, which is then signed. The signed digest is appended to the outgoing message, possibly along with the certificate of the sender and possibly any required certificates or CRLs. The receiver of this signed message must also take a digest of the message, compare this digest with the digest appended to the message, retrieve the sender's public key, and verify the signature on the appended digest. If the message content has been changed, the digests will be different or the signature on the digest will not verify properly. If the message is not encrypted, this signature does not prevent anyone from seeing the contents of the message, but does ensure that the message has not been tampered with and is from the actual person as indicated on the "from" field of the message.

The receiver may also verify the certificate and CRL if they were appended to the message. A certificate chain is a certificate along with a number of other certificates required to verify that the original certificate is authentic. While verifying the signature on a signed message, the receiver of the message will also typically obtain a certificate chain for the signing certificate and verify that each certificate in the chain was signed by the next certificate in the chain, until a certificate is found that was signed by a root certificate from a trusted source, such as, for example, a large Public Key Server (PKS) associated with a Certificate Authority (CA),

such as, for example, Verisign or Entrust, both prominent companies in the field of public key cryptography. Once such a root certificate is found, a signature can be verified and trusted, since both the sender and receiver trust the source of the root certificate.

In encrypted S/MIME message operations, a one-time session key is generated and used to encrypt the body of the message, typically with a symmetric cipher, such as, for example, Triple DES. The session key is then encrypted using the receiver's public key, typically with a public key encryption algorithm like RSA. If the message is addressed to more than one receiver, the same session key is encrypted using the public key of each receiver. The encrypted message body, as well as all encrypted session keys, is sent to every receiver. Each receiver must then locate its own session key, possibly based on a generated Recipient Info summary of the receivers that may be attached to the message, and decrypt the session key using its private key. Once the session key is decrypted, it is then used to decrypt the message body. The S/MIME Recipient Info attachment can also specify the particular encryption scheme that must be used to decrypt the message. This information is normally placed in the header of the S/MIME message. Those skilled in the art will appreciate that these operations relate to an illustrative example of S/MIME messaging and its associated encoding operations, namely encryption. It will also be understood that the instant disclosure is in no way limited thereto.

FIG. 4 illustrates a situation where encoded messages are provided to a mobile device 410 by a server 408 contained within a wireless connector system 406. With reference to FIG. 4, an encoded message 404 from a sender 402 is provided to the wireless connector system 406. The server 408 within the wireless connector system 406 analyzes the encoded message 404 with respect to its size. If the size is determined to be above some predetermined threshold, then the server 408 may notify the mobile device 410 with size related information 414. The server may

process the encoded message 412 before sending it to the mobile device such that the encoded message 412 is below the predetermined threshold size. Moreover, data item 412 may be further processed by the server 408 such that the message is partially decoded and the result of such processing sent to the mobile device 410.

As an exemplary operational scenario, current mobile device implementations typically have a limit on the message size that will reach the mobile device, such as, for example, 32 KB. If an S/MIME message is over 32 KB, then the entire message will not completely reach the mobile device. As such, if the message is signed, then it cannot be verified on the mobile device due to the size limitation. The server in this situation may send an indication to the mobile device that the message is too large to be verified by the mobile device and that verification has already been done by the server. The user receiving this message will then be aware that verification of the message has already been accomplished.

According to an exemplary embodiment of the present invention, as illustrated in FIG. 5, the server is operable to assist the size-limited mobile device in verifying the message itself. As an operational illustrative example, a secure (e.g., signed) message that is too large for the size-limited device may be made include an attachment. Start indication block 500 indicates that process block 502 has received a message at the server. Decision block 504 examines the message to determine if the size is above a predetermined threshold. The message size includes the size of any attachments that may be present. If the message size is not above the predetermined threshold, the message is provided to the size-limited device 506 after the server has performed any additional customary processing of the message. If the message is too large for the size-limited device, the server may perform additional steps to assist the size-limited device in verifying the message. For example, the server determines the point in the secure

electronic message encoding where the message will be cut off due to the size constraints of the size-limited device. The server determines if the cut off point occurs in such a location that verification of the message will not be possible on the size-limited device, such as, for example, part way through the signed data or in the middle of the signature data. If the message is determined to be too long such that verification is not possible on the device, then the server can attempt to verify the signature on the message.

As an operational example, assume that the message data is made up of three parts, A, B and C, where B is a large attachment. After determining that the message is too large for the size-limited device, the server may remove the attachment B from the message to prevent it from being sent to the size-limited device 508. Consequently, the attachment B will not be sent to the size-limited device. Because the attachment has been removed from the electronic message, the size-limited device will be unable to verify the signature. In order to assist the size-limited device in verifying the message, the server may apply a hashing function to parts A, B and C, in sequence 510. In a preferred embodiment, the hashing function applied to parts A, B and C is the same as that used in signature generation. After each part has been hashed, the hashing function has a context associated therewith. The size-limited device, of course, only has parts A and C, so when it performs a hash, it will have the same context after hashing part A, but will have the incorrect starting context when it hashes part C.

In this situation, the server can insert the hash context after it hashed part A and the hash context after it hashed part B in place of the attachment B in the original message 512. Because the hash contexts are much smaller than the application data, the size-limited device should be able to accept this data. Accordingly, after the size-limited device performs its hash of part A, it can compare the hash context obtained from hashing part A with the hash context received from

the server when it hashed part A. If these contexts match, the device can then substitute the hash context received from the server after it hashed part B, and the device can then continue to hash part C 514. This result can then be used to verify the signature 516.

Another example is illustrated in FIG. 6. In this example, steps 600, 602, 604, 606, 608 and 610 correspond substantially to steps 500, 502, 504, 506, 508 and 510 of FIG. 5. According to this example, the server could alternatively insert the result of performing an exclusive OR function (XOR) of the context after hashing part A with the context after hashing part B 612. The device would then perform a hash of part A, take this context and perform an XOR with the value the server provides for the context after hashing part B 614. The device then takes the result of that XOR function and uses it as the context after hashing part B 616, to verify the signature 618. This alternative further reduces the amount of data required to be sent to the size-limited device.

As yet another example, the server may only verify levels of the message. For example, in S/MIME the actual steps involved in verifying a message involve taking multiple digests and then performing an actual signature verification calculation. In this exemplary embodiment, the server may verify that the digests match, but leave the signature verification calculation to the size-limited device.

While the foregoing has been described in conjunction with specific exemplary embodiments, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the exemplary embodiments set forth herein are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as defined in the appended claims.

WHAT IS CLAIMED IS:

1. A method for processing encoded messages comprising:
 - receiving an encoded message at a server, the encoded message having a message size;
 - comparing the message size to a predetermined threshold;
 - sending said encoded message to a device when said message size is less than said predetermined threshold;
 - removing a portion of said encoded message and sending an abbreviated message to said device when said encoded message is larger than said predetermined threshold, said abbreviated message being said encoded message less the removed portion such that the abbreviated message has a size smaller than the predetermined threshold;
 - processing said encoded message in a predetermined sequence at said server and providing results of said processing to said device; and
 - processing said abbreviated message at said device using at least portions of the results of processing at the server received by the device to verify the message received by the device.
2. The method according to claim 1, wherein said device is a mobile wireless communications device.
3. The method according to claim 1, wherein said portion of said encoded message that is removed is an attachment to an encoded e-mail message.

4. The method according to claim 1, wherein said processing of said encoded message at said server comprises performing a sequential hashing function on predetermined portions of the encoded message to generate hash context values for said predetermined portions.

5. The method according to claim 4, wherein said processing of said abbreviated message comprises performing a sequential hashing function on predetermined portions of said abbreviated message and inserting appropriate hash context values received from the server where necessary to verify said abbreviated message.

6. The method according to claim 4, further comprising performing an exclusive OR function on predetermined hash context values and sending a result of said exclusive OR function to said device and said device processing said abbreviated message by performing an exclusive OR function on predetermined hash context values and comparing a result of said exclusive OR function to the result received from the server.

7. The method according to claim 2, wherein said processing of said encoded message at said server comprises verifying that digests of the encoded message match and said processing of said abbreviated message comprises verifying a signature of said abbreviated message based on the result of the processing of said encoded message at said server.

8. A method for processing encoded messages comprising:

receiving an encoded message at a server, the encoded message having a message size;

comparing the message size to a predetermined threshold;

removing a portion of said encoded message and sending an abbreviated message to said device when said encoded message is larger than said predetermined threshold, said abbreviated message being said encoded message less the removed portion such that the abbreviated message has a size smaller than the predetermined threshold;

processing said encoded message in a predetermined sequence at said server and providing results of said processing to said device; and

processing said abbreviated message at said device using at least portions of the results of processing at the server received by the device to verify the message received by the device.

9. The method according to claim 8, wherein said device is a mobile wireless communications device.

10. The method according to claim 8, wherein said portion of said encoded message that is removed is an attachment to an encoded e-mail message.

11. The method according to claim 8, wherein said processing of said encoded message at said server comprises performing a sequential hashing function on predetermined portions of the encoded message to generate hash context values for said predetermined portions.

12. The method according to claim 11, wherein said processing of said abbreviated message comprises performing a sequential hashing function on predetermined portions of said abbreviated message and inserting appropriate hash context values received from the server where necessary to verify said abbreviated message.

13. The method according to claim 11, further comprising performing an exclusive OR function on predetermined hash context values and sending a result of said exclusive OR function to said device and said device processing said abbreviated message by performing an exclusive OR function on predetermined hash context values and comparing a result of said exclusive OR function to the result received from the server.

14. The method according to claim 9, wherein said processing of said encoded message at said server comprises verifying that digests of the encoded message match and said processing of said abbreviated message comprises verifying a signature of said abbreviated message based on the result of the processing of said encoded message at said server.

15. A system for verifying encoded electronic messages, comprising:
a server for receiving an encoded message at a server, the encoded electronic message having a message size;
program logic resident on said server for comparing the message size to a predetermined threshold, removing a portion of said encoded message and sending an abbreviated message to said device when said encoded message is larger than said predetermined threshold, said abbreviated message being said encoded message less the removed portion such

that the abbreviated message has a size smaller than the predetermined threshold; processing said encoded message in a predetermined sequence at said server and providing results of said processing to said device; and

a wireless communications device for receiving messages from said server, said wireless communications device including program logic for processing said abbreviated message at said device using at least portions of the results of processing at the server received by the device to verify the message received at the device.

16. A system for verifying encoded electronic messages comprising:

a server;

a mobile wireless communications device;

means for receiving an encoded electronic message at a server, the encoded message having a message size;

means for comparing the message size to a predetermined threshold;

means for removing a portion of said encoded message and sending an abbreviated message to said mobile wireless communications device when said encoded message is larger than said predetermined threshold, said abbreviated message being said encoded message less the removed portion such that the abbreviated message has a size smaller than the predetermined threshold; and

means for processing said encoded message in a predetermined sequence at said server and providing results of said processing to said mobile wireless communications device;

means resident on said mobile wireless communications device for processing said abbreviated message at said device using at least portions of the results of processing at the server received by the device to verify the message received at the device.

17. A method for processing encoded messages comprising:
sending an abbreviated encoded electronic message from a server to a mobile device, the abbreviated message being at least a portion of an original encoded message received by the server; and
sending results of processing performed by the server on the encoded message to the mobile device for use in processing the abbreviated message to verify the abbreviated message.

18. The method according to claim 17, wherein said mobile device is a wireless communications device.

19. The method according to claim 17, wherein a portion of said encoded message that is removed to form the abbreviated message is an attachment to an encoded e-mail message.

20. The method according to claim 17, wherein said processing of said encoded message performed by said server comprises performing a sequential hashing function on predetermined portions of the encoded message to generate hash context values for said predetermined portions.

21. The method according to claim 20, wherein said processing of said abbreviated message comprises performing a sequential hashing function on predetermined portions of said abbreviated message and inserting appropriate hash context values received from the server where necessary to verify said abbreviated message.

22. The method according to claim 20, further comprising performing an exclusive OR function on predetermined hash context values and sending a result of said exclusive OR function to said device and said device processing said abbreviated message by performing an exclusive OR function on predetermined hash context values and comparing a result of said exclusive OR function to the result received from the server.

23. The method according to claim 18, wherein said processing of said encoded message by said server comprises verifying that digests of the encoded message match and said processing of said abbreviated message comprises verifying a signature of said abbreviated message based on the result of the processing of said encoded message at said server.

24. A system for verifying encoded messages for a mobile wireless communications device comprising:

a server operable to perform at least a portion of verification processing of said encoded message when said server determines that a size of the encoded message is too large for processing by the mobile wireless communications device alone.

25. The method according to claim 24, wherein said verification processing of said encoded message performed by said server comprises performing a sequential hashing function on predetermined portions of the encoded message to generate hash context values for said predetermined portions.

26. The method according to claim 25, wherein said mobile wireless communications device receives said hash context values from said server and uses said hash context values to perform verification processing of received portions of said encoded message.

27. The method according to claim 25, further comprising performing an exclusive OR function on predetermined hash context values and sending a result of said exclusive OR function to said mobile wireless communications device for use in verification processing of received portions of said encoded message at said mobile wireless communications device.

28. The method according to claim 24, wherein said verification processing of said encoded message by said server comprises verifying that digests of the encoded message match and verification processing of portions of the encoded message received by the mobile wireless communications device comprises verifying a signature of said message based on the result of the verification processing of said encoded message at said server.

1/6

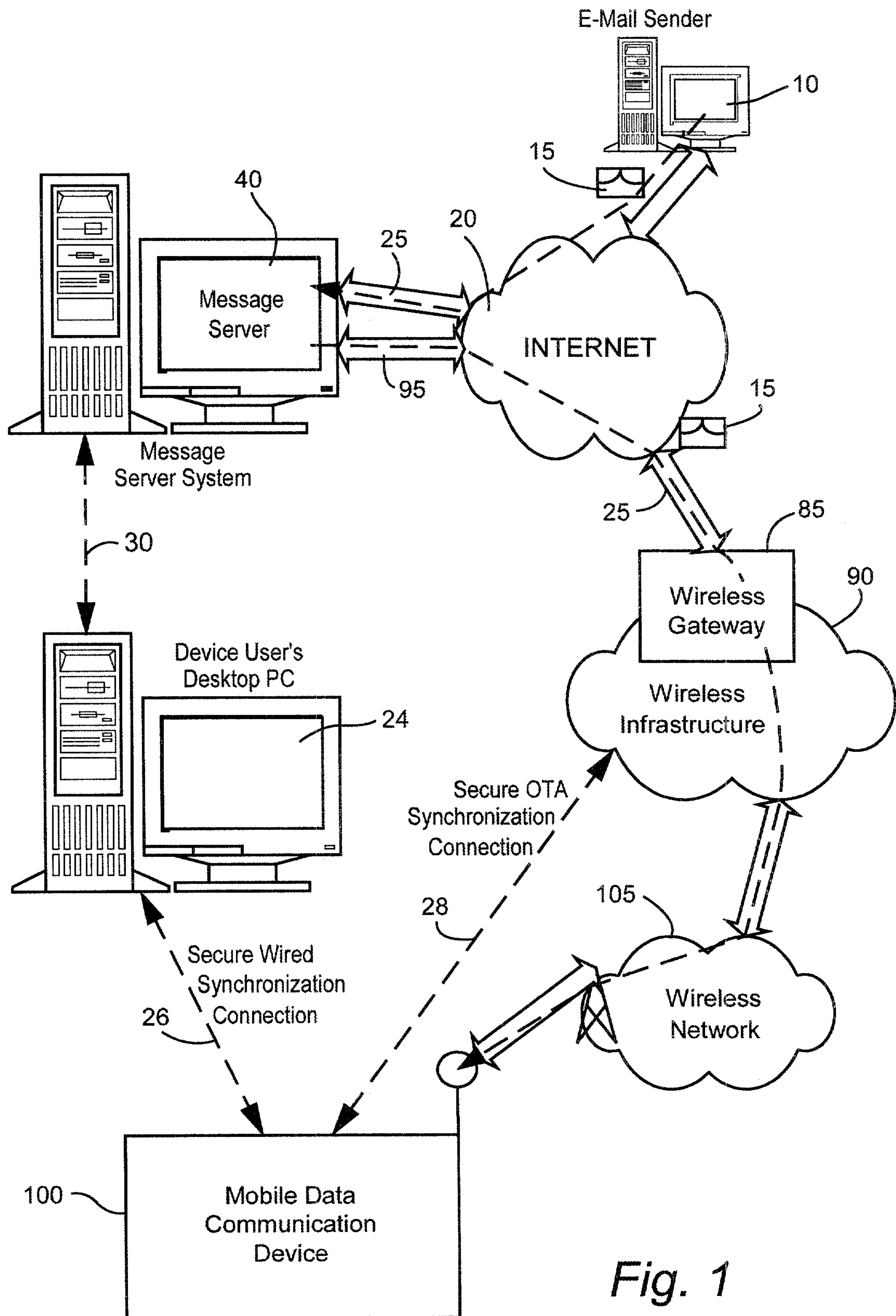


Fig. 1

2/6

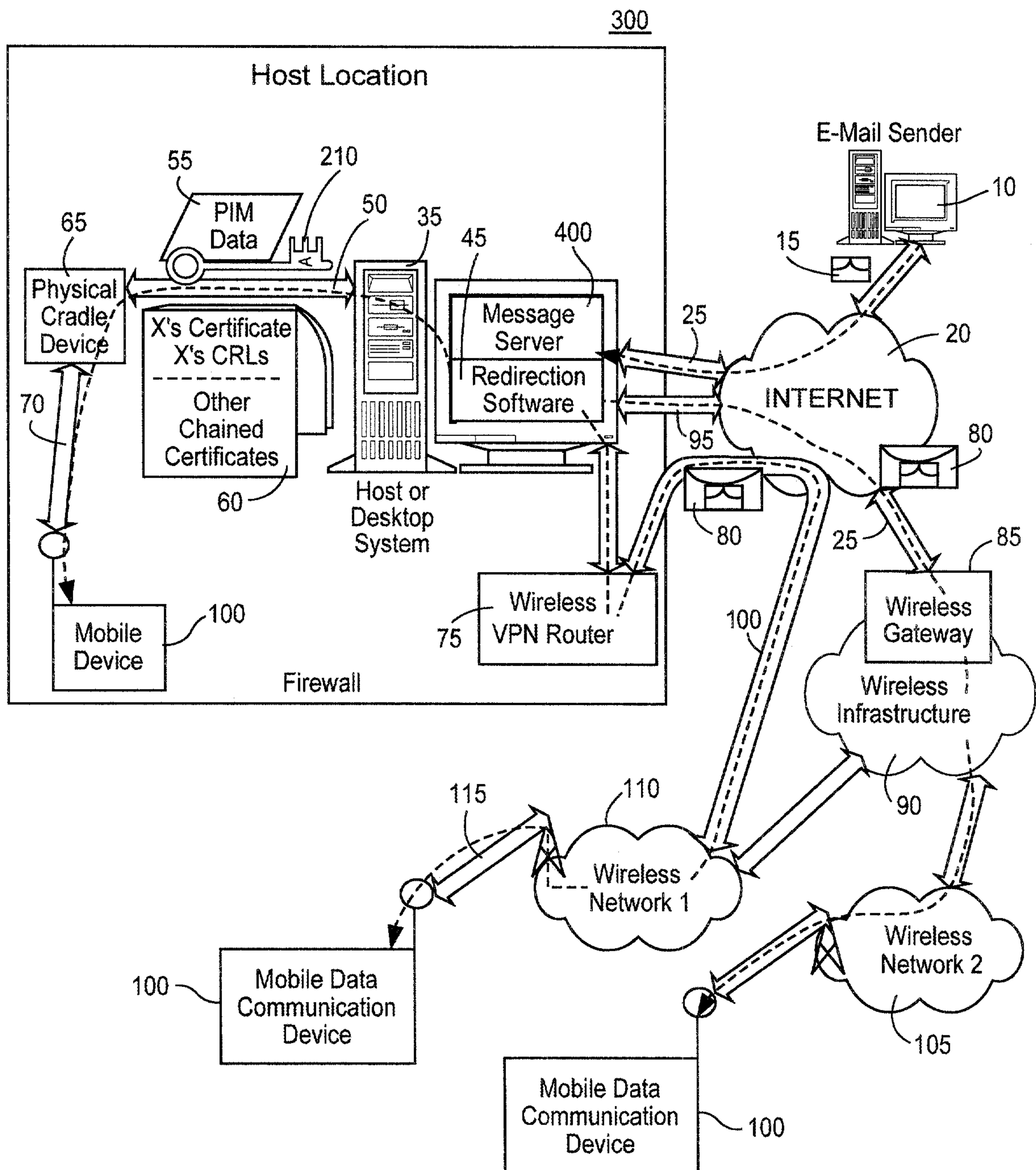
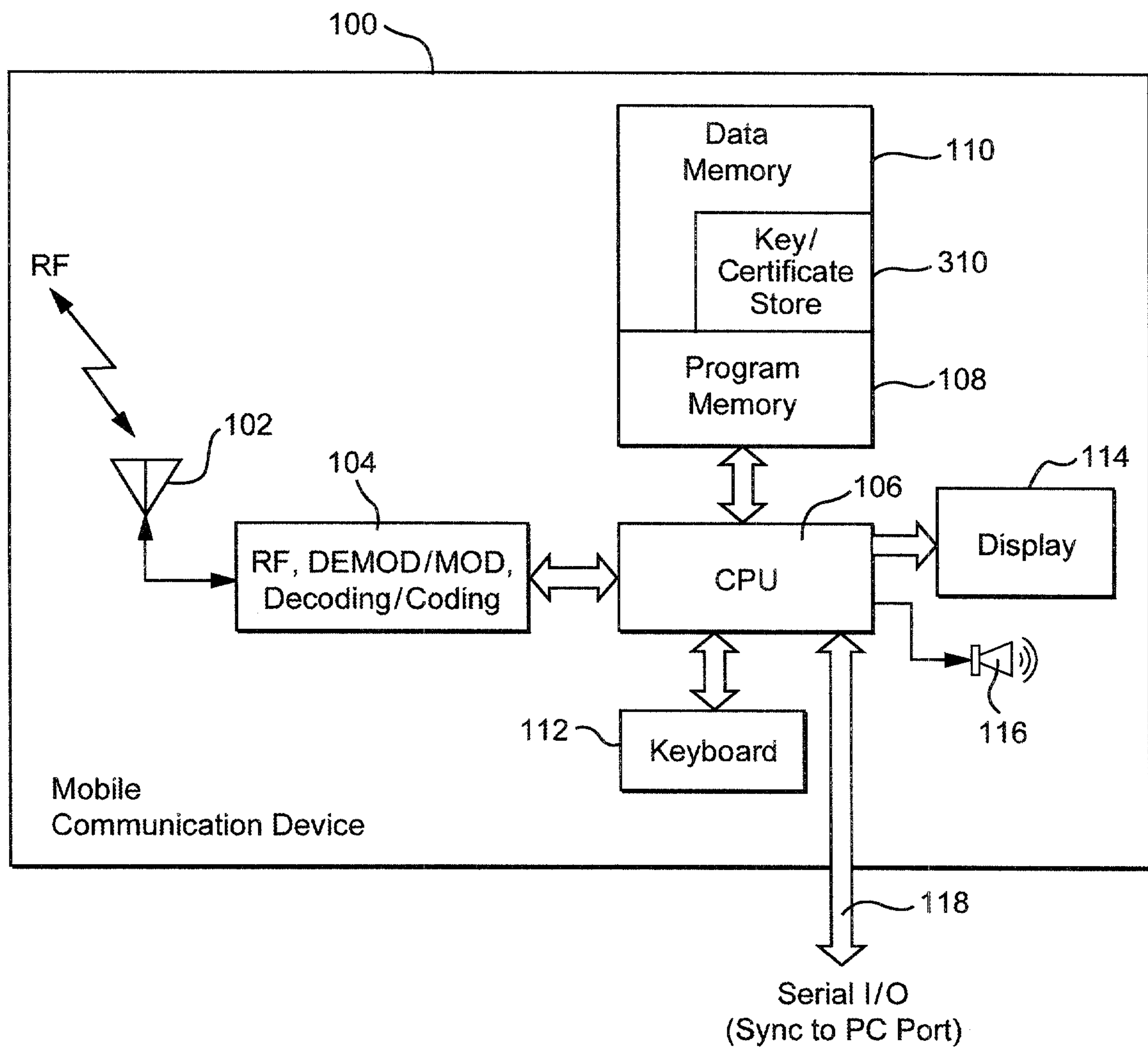
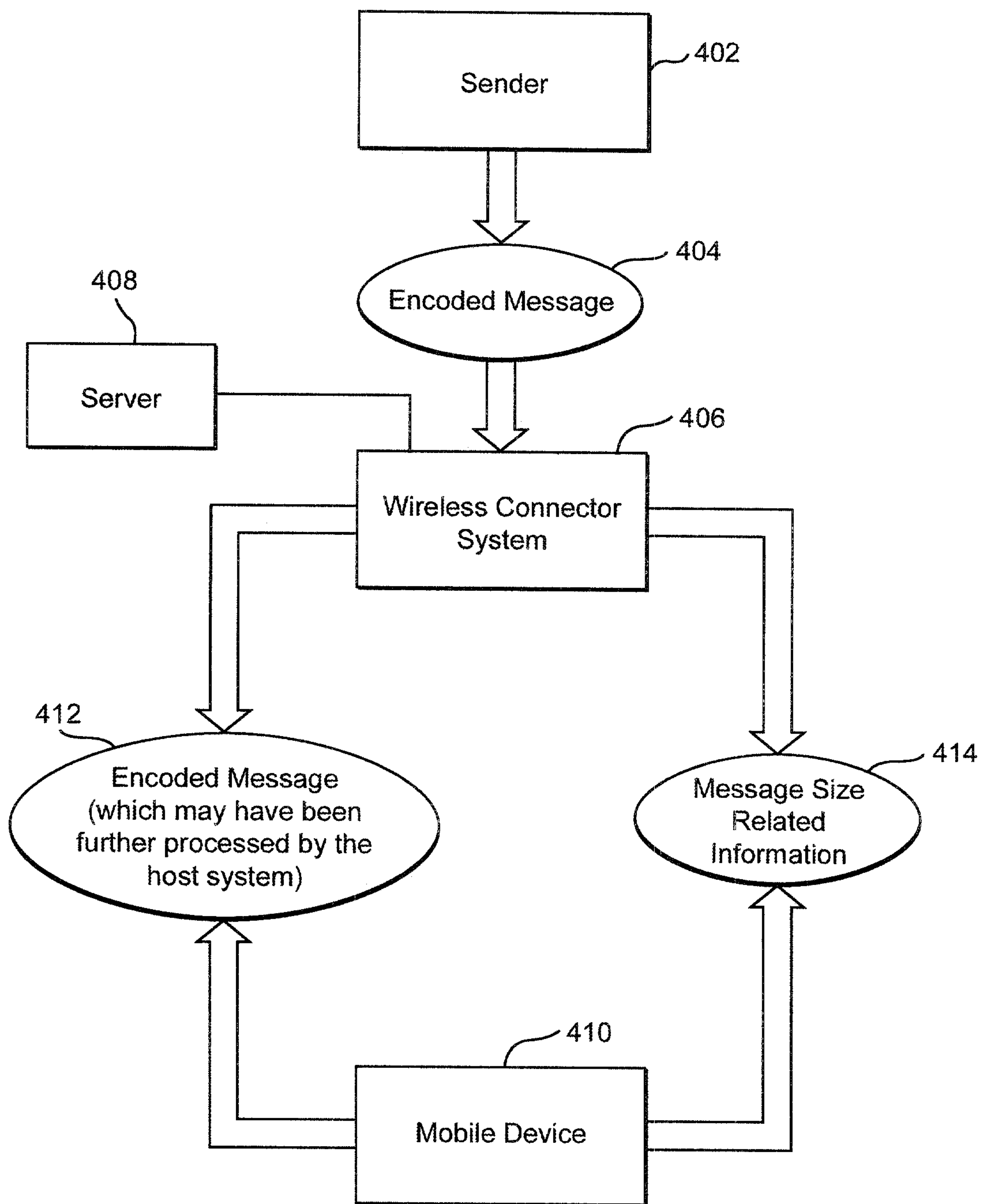


Fig. 2

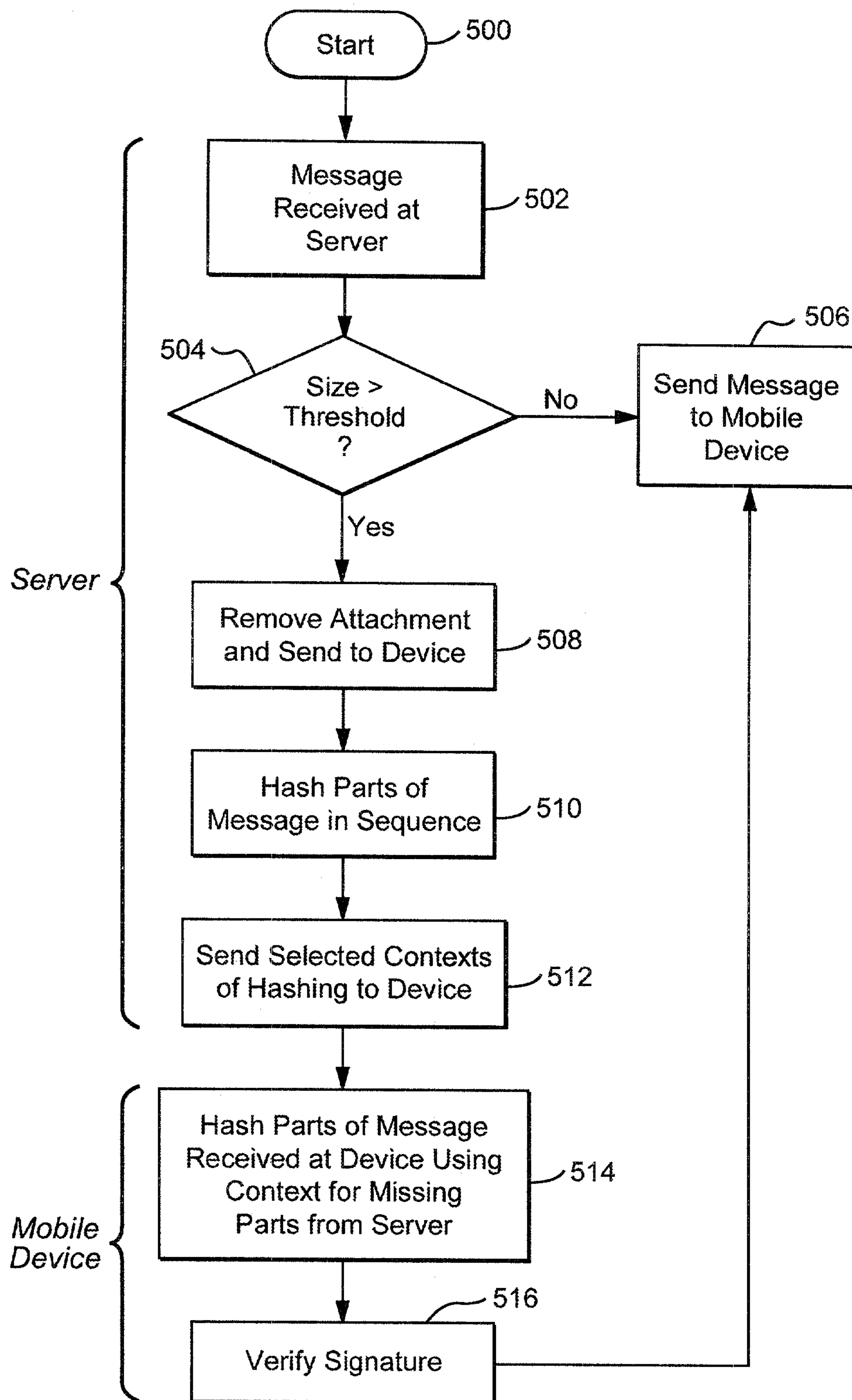
3/6

*Fig. 3*

4/6

*Fig. 4*

5/6

*Fig. 5*

6/6

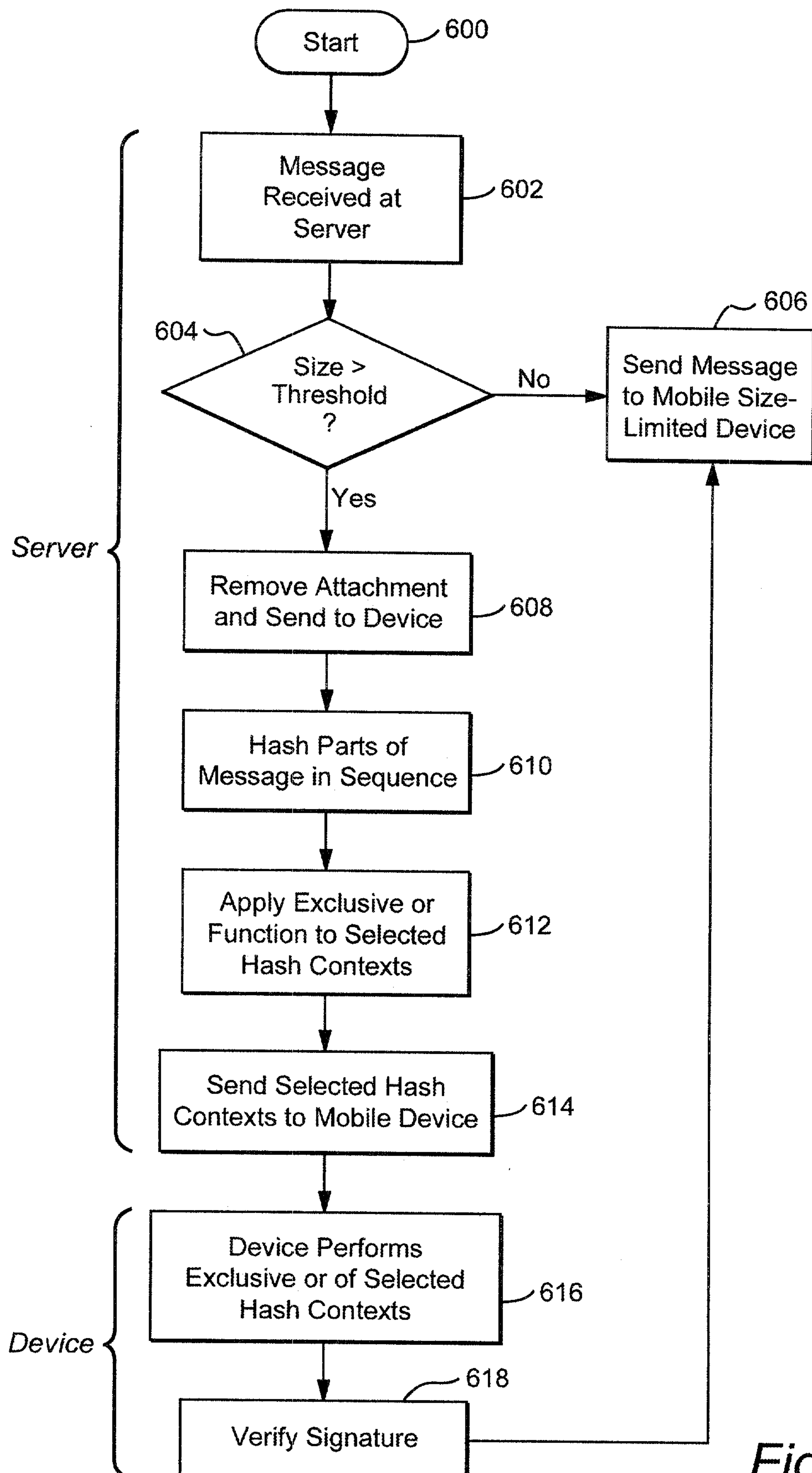


Fig. 6

