



(22) Date de dépôt/Filing Date: 2007/06/22

(41) Mise à la disp. pub./Open to Public Insp.: 2007/12/23

(45) Date de délivrance/Issue Date: 2012/03/27

(30) Priorité/Priority: 2006/06/23 (EP06253267.6)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
H04L 12/54 (2006.01)

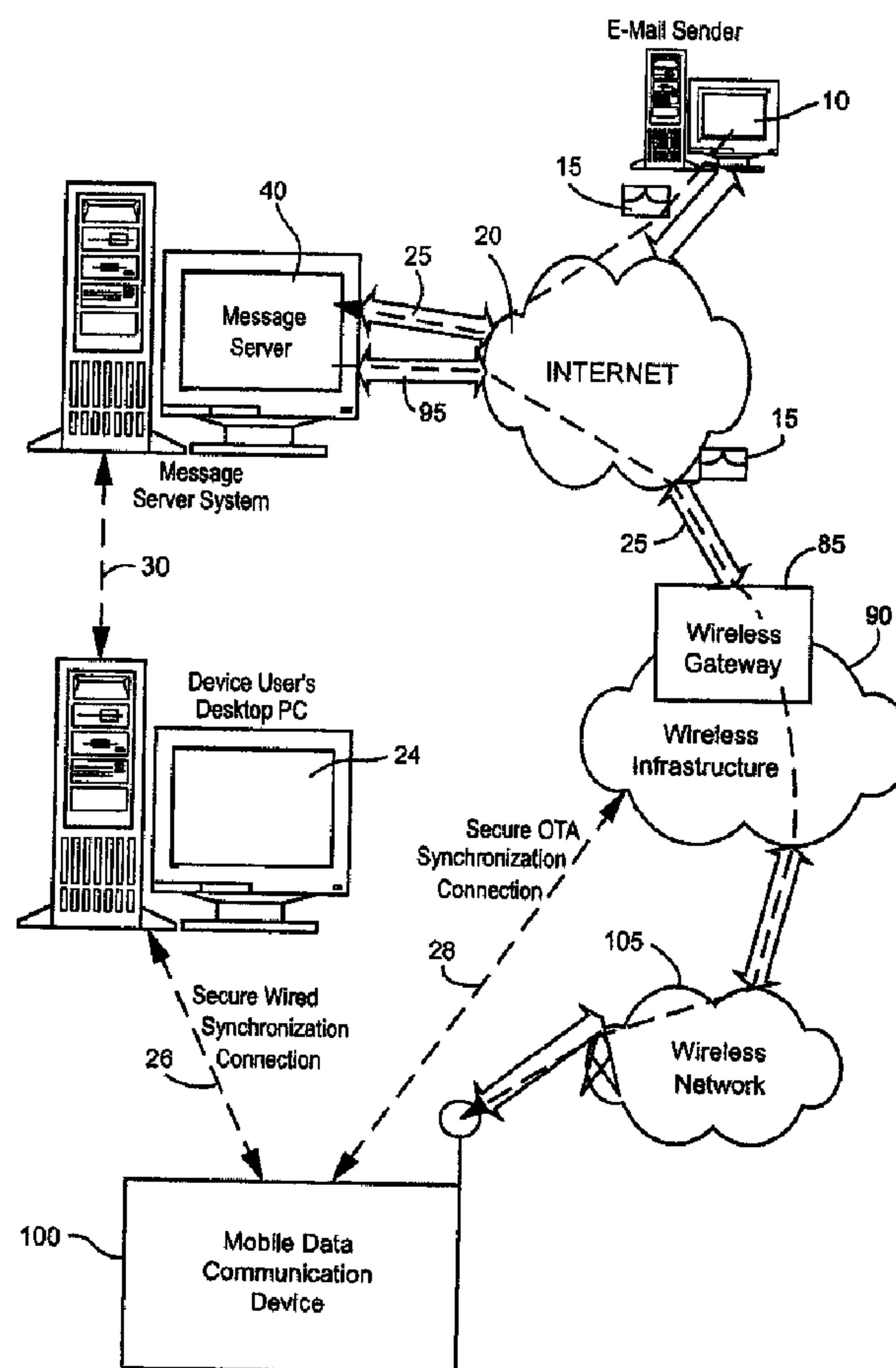
(72) Inventeurs/Inventors:
BROWN, MICHAEL K., CA;
BROWN, MICHAEL S., CA;
SEGATO, TIMOTHY, CA

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

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

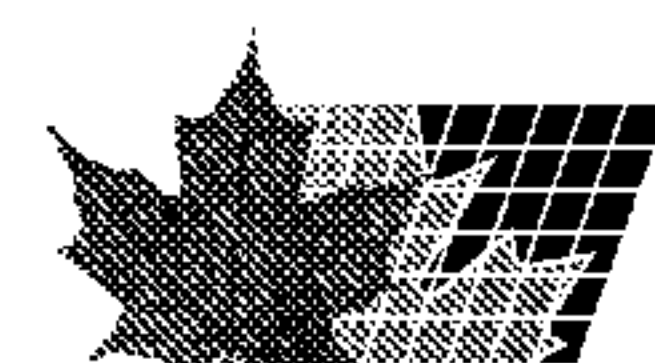
(54) Titre : SYSTEME ET METHODE PERMETTANT DE TRAITER LES DISCORDANCES DU COURRIEL

(54) Title: SYSTEM AND METHOD FOR HANDLING ELECTRONIC MAIL MISMATCHES



(57) Abrégé/Abstract:

A system and method for handling e-mail address mismatches between the address contained within a user's certificate or certificate chain, and the account address actually being used is disclosed. In order to resolve address mismatches a canonical or



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

generic domain name or user name may, for example, be used as a lifelong address of a user that is contained in the user's certificate. Upon detection of an address mismatch, the system and method disclosed herein may automatically re-check the certificate or search for a certificate containing the canonical or generic domain name and/or user name to attempt to resolve the mismatch. This mismatch resolution is preferably transparent to the user and occurs automatically. The canonical or generic domain and/or user names that are available to the device may be typically controlled by IT policy that is in place on the system for the device. While this system is suitable for any type of electronic messaging system, it has particular applicability to systems that use mobile wireless communication devices with electronic messaging capability.

ABSTRACT

A system and method for handling e-mail address mismatches between the address contained within a user's certificate or certificate chain, and the account address actually being used is disclosed. In order to resolve address mismatches a canonical or generic domain name or user name may, for example, be used as a lifelong address of a user that is contained in the user's certificate. Upon detection of an address mismatch, the system and method disclosed herein may automatically re-check the certificate or search for a certificate containing the canonical or generic domain name and/or user name to attempt to resolve the mismatch. This mismatch resolution is preferably transparent to the user and occurs automatically. The canonical or generic domain and/or user names that are available to the device may be typically controlled by IT policy that is in place on the system for the device. While this system is suitable for any type of electronic messaging system, it has particular applicability to systems that use mobile wireless communication devices with electronic messaging capability.

SYSTEM AND METHOD FOR HANDLING ELECTRONIC MAIL MISMATCHES

BACKGROUND

Technical Field

The present disclosure relates generally to the processing of secure electronic messages and information. In particular, the instant disclosure is directed to a system and method for resolving mismatches that may occur between, for example, an e-mail address contained in the certificate of a sender or recipient of an electronic message, and the e-mail address actually used in the sender or recipient field of an e-mail.

Related Art

Exchanging secured electronic messages and data, such as, for example, e-mail messages, is well known. Secure electronic messaging may involve the use of digital signatures, encryption, or the like. For example, a recipient of an electronic message may verify that the sender of an electronic message is trusted by comparing the address of the sender to an address that may be contained in a certificate or certificate chain of the sender.

Some organizations, such as, for example, government agencies like the Department of Defense, are moving to systems in which a user has an e-mail address that they will keep for the life of their tenure with that organization. This sort of lifelong address will typically be contained within the user's certificate. As a user moves around within the organization, the address for their account may change, for example, based on location. For example, the lifelong address may appear as John.Doe@agency.gov, while the address being used when the user is working at a particular site within the organization may change to reflect the location of the user, for example, John.Doe@locationA.agency.gov. Thus, in this example, as John Doe moves about throughout the agency, the lifelong address of John Doe will not change, but John Doe's Outlook® address may change based on John Doe's location.

This arrangement can create many problems with signed electronic messages, such as, for example, S/MIME, because it depends on the e-mail address found in the user's certificate matching the e-mail address of the account for verification. In this example, if

someone wants to send an e-mail to John Doe when he is stationed at location A, the system would search for the certificate containing the address John.Doe@locationA.agency.gov, but the address contained in John Doe's lifelong certificate is John.Doe@agency.gov. This difference will result in a mismatch. Similarly, if John Doe were to send a signed e-mail to someone, when the recipient attempts to verify it, the recipient will see the originating address is John.Doe@locationA.agency.gov, but the address in the certificate is John.Doe@agency.gov. Again, this will result as an e-mail mismatch error.

What is needed is a system and method for resolving the potential mismatch errors, for example, those that might occur in organizations that use lifelong e-mail addresses and shorter term addresses that are used as the user moves around within the organization.

BRIEF SUMMARY

In view of the foregoing, we have now identified an efficient, accurate and easy to implement system and method for handling e-mail address mismatches between the address contained within a user's certificate or certificate chain, and the account address actually being used. In order to resolve address mismatches one or more canonical, e.g., generic, domain name(s) may, for example, be used as a lifelong address of a user that is contained in the user's certificate. Upon detection of an address mismatch, the system and method disclosed herein may automatically re-check the certificate or search for a certificate containing the canonical or generic domain or user name to attempt to resolve the mismatch. This mismatch resolution is preferably transparent to the user and occurs automatically. The canonical or generic domain or user names that are available to the device may be typically controlled by IT policy that is in place on the system for the device. While this system is suitable for any type of electronic messaging system, it has particular applicability to systems that use mobile wireless communication devices with electronic messaging capability.

According to an exemplary embodiment, if a search for a recipient's certificate, or when performing an address mismatch check when receiving a signed message, a canonical or generic domain name may be included in the search. Thus, if someone is trying to send an e-mail to John.Doe@locationA.agency.gov, and a matching certificate is not found, the search may be retried using a canonical or generic domain name, such as, for example, John.Doe@agency.gov. The system may be preferably configured to

automatically retry a certificate search of a recipient using the canonical or generic domain name, or in the case of an address mismatch when attempting to verify a received message, retry the check substituting the canonical or generic domain name(s). A faster and perhaps even more efficient approach when searching for a certificate or attempting to resolve a mismatch, is to automatically check certificates for both the address of the account being used and canonical or generic domain name simultaneously, and transparently provide the user with the matching result. While it is preferred in this example to perform these certificate checks at the device level, it is also envisioned that a server or service resident on a server within the system, such as, for example, an e-mail server may perform these checks thereby increasing the speed and efficiency of the search, while alleviating processor overhead of the device. As with the device, a server-based implementation, the canonical or generic domain names that are available to the device via the server may be typically controlled by IT policy that is in place on the system.

According to another exemplary embodiment, the system may be configured to search for a generic name that includes canonical or generic user name(s) in place of (or in addition to) a canonical or generic domain name to search for a certificate or to resolve a mismatch. Typically, e-mail addresses are composed of two main parts - the user name and the domain name, for example, user name@domain name. The examples set forth above are described with respect to using a canonical or generic domain name when searching for a certificate or when attempting to resolve a mismatch. However, it is also contemplated that a canonical or generic user name may be used to search for a certificate or resolve a mismatch. For example, the user name may change as an employee moves or is assigned to different departments within an agency. For instance, the lifelong address may be John.Doe@agency.gov, but the user name may change as John Doe is assigned to different offices or departments within the agency, for example, John.Doe_Legal@agency.gov, John.Doe_accounting@agency.gov, John.Doe_Solicitor@agency.gov, etc. In this example, to search for a certificate or to resolve a mismatch, the system may utilize a canonical or generic user name, e.g., by truncating the portion of the user name following the underscore in the examples set forth above. The system administrator would be able to set the rules for using canonical or generic user names or domain names based on the structure of the address via IT policy.

In yet a further exemplary implementation, using a combination of canonical or generic domain names and user names to search for a certificate or to resolve a mismatch may also be used to provide a more robust solution.

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 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 abbreviated schematic diagram of hardware included within an exemplary mobile wireless communications device;

FIG. 4 is an abbreviated schematic functional diagram of the hardware/software utilized in an exemplary mobile wireless communication device in the exemplary embodiment of FIG. 1;

FIG. 5 is an exemplary abbreviated flow diagram of a method used in a system for handling electronic mail mismatches in a recipient address;

FIG. 6 is another exemplary abbreviated flow diagram of a method used in a system for handling electronic mail mismatches in a recipient address;

FIG. 7 is an exemplary abbreviated flow diagram of a method used in a system for handling electronic mail mismatches in a sender's address;

FIG. 8 is another exemplary abbreviated flow diagram of a method used in a system for handling electronic mail mismatches in a sender's address; and

FIG. 9 is an exemplary screen shot illustrating an exemplary administrator screen that may be used to assign a generic or canonical name to a user's certificate.

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), integrated Digital Enhanced Network (iDEN), Evolution Data Optimized (EvDO), High-Speed Downlink Packet Access (HSDPA), Universal Mobile Telecommunications Systems (UMTS) or the like. Some older examples of data-centric network include the MobitexTM Radio Network and the DataTACTM 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. 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. However, there are situations where a user does not have the ability to establish such a link to their desktop 35 in order to update the key store of the mobile device 100 with the appropriate private keys. In these situations, the system and method described herein allow the secure transfer of cryptographic information over a wireless link.

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 20 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.

As depicted in FIG. 4, the user's base unit 24 may be used to update the mobile wireless communications device 100 with information including, for example, private key information and digital certificate information. The user's base station 24 is typically a desktop PC, and may be of conventional hardware and operating system design. It will typically include desktop manager program logic 304 (in the form of, for example, executable computer program logic) for managing, among other things, a normal data synchronization connection to device 100. As previously mentioned, in the environment of mobile wireless communications systems, such a desktop manager may typically include logic for synchronizing cryptographic message certificates. Such logic is denoted here as Cert Sync.

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. 5 is an exemplary abbreviated flow diagram of a method for use in a system for handling electronic mail mismatches when searching for a recipient's certificate using a recipient address. According to this exemplary illustration, a user first enters an electronic messaging application 501 resident on or accessible to the device being used by the user. Such devices may include, for example, a mobile wireless communication device that is capable of supporting electronic mail functions, as discussed above. The user then enters a recipient address 503 in the appropriate field of the electronic mail message to be sent. The system then conducts a search for the recipient's certificate by attempting to locate the recipient address in certificates resident on the device 507. Alternatively, the system may be configured to search certificates stored on a server of the system. If the recipient address is found in a certificate available to the device 509, the user may continue with the electronic mailing process using the recipient's certificate 511. On the other hand, if no certificate containing the recipient address is found 509, the system and method according to an exemplary embodiment then searches for the recipient certificate using a canonical or generic domain name and/or a canonical or generic user name 513. For simplicity, the examples described herein refer generally to a canonical or generic domain name. However, it will be understood that the application applies equally to the use of a canonical or generic user name in place of a generic or canonical domain name, and to a combination of canonical or generic domain and user names. As described above, the canonical or generic domain name may be, for example, a lifelong address that is assigned to a person for the duration of their tenure with a specific agency, organization, company, or the like. If the certificate is found using the canonical or generic domain name 515, the user may continue the messaging process 511. If no certificate is found 515, a notification may be provided to the user that no certificate match for the address was found 517. While the electronic mail handling system and method is described herein with respect to processing at the electronic mail device itself, it will be understood that the

system and method may be implemented by any suitable means, such as, for example, an e-mail server, or the like, and that the disclosure is directed to a system and method for handling electronic mail mismatches regardless of where the certificates are stored or which device(s) in the system implement the method.

FIG. 6 is an exemplary abbreviated flow diagram of an alternative method for use in a system for handling electronic mail mismatches when searching for a recipient's certificate using a recipient address. The exemplary method illustrated in FIG. 6 is similar to that of FIG. 5. However, in the FIG. 6 embodiment, the search for the recipient certificate is conducted using the recipient address and canonical or generic domain name concurrently. According to this exemplary embodiment, the user enters the electronic messaging application 601, and enters recipient e-mail address in the appropriate field 603. The system then conducts a search for the recipient's certificate by attempting to locate the recipient address in certificates resident on or accessible to the device and by attempting to locate a canonical or generic domain name associated with the recipient concurrently 605. If a certificate is found 607, the user may continue the messaging process 609. If no match is found 607, a notification may be provided to the user of a mismatch 611. As discussed above, searching for both the recipient address and a canonical or generic domain name associated with the recipient concurrently may provide efficiencies of speed and processing overhead.

FIG. 7 is an exemplary abbreviated flow diagram of a method used in a system for handling electronic mail mismatches when searching for a sender's certificate using a sender's address. The process illustrated in FIG. 7 is similar to that illustrated in FIG. 5, with the certificate search being based on the sender's e-mail address or canonical or generic domain name associated with the sender. According to this exemplary embodiment, after a user receives an electronic message 701, the system institutes a search for the sender's certificate based on the sender's e-mail address that was used to send the message 703. If a corresponding certificate is found based on the sender's address 705, the user may continue the process of verifying the user's information, such as, for example, the user's digital signature 709. If no certificate corresponding to the sender is found 705, the system may then search for the sender certificate using a canonical or generic domain name associated with the sender's lifelong address 711. If a certificate associated with the sender is found 713, the user may then continue the processing of the received mail 709. If no match is found 713, the user may be notified of a mismatch 715.

While the electronic mail handling system and method is described herein with respect to processing at the electronic mail device itself, it will be understood that the system and method may be implemented by any suitable means, such as, for example, an e-mail server, or the like, and that the disclosure is directed to a system and method for handling electronic mail mismatches regardless of where the certificates are stored or which device(s) in the system implement the method.

FIG. 8 is an exemplary abbreviated flow diagram of an alternative method for use in a system for handling electronic mail mismatches when searching for a sender's certificate using a sender's address. The exemplary method illustrated in FIG. 8 is similar to that of FIG. 7. However, in the FIG. 8 embodiment, the search for the sender's certificate is conducted using the sender's address and canonical or generic domain name concurrently. According to the example illustrated in FIG. 8, the user receives an electronic message 801. The system then conducts a search for the sender's certificate by attempting to locate the sender's address in certificates resident on or accessible to the device and by attempting to locate a canonical or generic domain name associated with the sender concurrently 803. If a certificate is found 805, the user may continue the messaging process 809. If no match is found 805, a notification may be provided to the user of a mismatch 807. As discussed above, searching for both the sender's address and a canonical or generic domain name associated with the sender concurrently may provide efficiencies of speed and processing overhead.

As discussed herein, the device within the system that provides the electronic message mismatch handling as described with respect to the illustrative embodiments discussed in detail above, may be any device within the system, including, but not limited to the electronic messaging device itself, a server within the system, or the like.

Furthermore, as discussed above, the system may be configured to search for a canonical or generic user name in place of (or in addition to) a canonical or generic domain name to search for a certificate or to resolve a mismatch. Typically, e-mail addresses are composed of two main parts - the user name and the domain name, for example, user name@domain name. The examples set forth above are described with respect to using a canonical or generic domain name when searching for a certificate or when attempting to resolve a mismatch. However, it is also contemplated that a canonical or generic user name may be used to search for a certificate or resolve a mismatch. For example, the user name may change as an employee moves or is assigned to different

departments within an agency. For instance, the lifelong address may be John.Doe@agency.gov, but the user name may change as John Doe is assigned to different offices or departments within the agency, for example, John.Doe_Legal@agency.gov, John.Doe_accounting@agency.gov, John.Doe_Solicitor@agency.gov, etc. In this example, to search for a certificate or to resolve a mismatch, the system may utilize a canonical or generic user name, e.g., by truncating the portion of the user name following the underscore in the examples set forth above. The system administrator would be able to set the rules for using canonical and/or generic user names or domain names based on the structure of the address via IT policy. FIG. 9 is an exemplary screen shot illustrating an exemplary administrator screen that may be used to assign a generic or canonical name to a user's certificate. As illustrated in this exemplary screen shot, the system administrator, for example, may be provided with the ability to enter data in a field that reflects a long-lived (e.g., canonical or generic name) associated with a particular user. The screen shot also provides a rule associated with the field relating to the use of canonical or generic names for long-lived addresses.

In yet a further exemplary implementation, using a combination of canonical or generic domain names and user names to search for a certificate or to resolve a mismatch may also be used to provide a more robust solution.

It will be understood that the methods described herein for locating a certificate of a sender or recipient of an electronic message may be embodied in executable program logic. The executable program logic may reside on the device or on a server within the system that processes electronic messages. Moreover, the executable program logic may be transmitted or received by various devices and circuits within devices of the system on a carrier wave modulated by a signal representing the corresponding program logic or executable code, or the like, or any other suitable communication medium.

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.

CLAIMS:

1. A method for locating a certificate in an electronic messaging system, wherein acts of the method are performed by a processor of a computing device, and wherein the method comprises:

5 obtaining a recipient address for an electronic message to be sent by the electronic messaging system, said recipient address comprising a first user name and a first domain name;

 searching for a certificate of the recipient based on a match with the recipient address;

10 automatically searching for the certificate of the recipient based on a canonical name associated with the recipient address if no match occurs based on the recipient address, wherein the canonical name is the recipient address with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name; and

15 providing an indication of whether the certificate of the recipient has been found.

2. The method according to claim 1, wherein the automatically searching for the certificate of the recipient based on the canonical name associated with the recipient address comprises:

20 first searching for the certificate of the recipient based on the recipient address with the first domain name truncated to identify the second domain name, and if no matching certificate is found then searching for the certificate of the recipient based on the recipient address with the first user name truncated to identify the second user name.

25 3. The method according to claim 1, wherein the automatically searching for the certificate of the recipient based on the canonical name associated with the recipient address comprises:

searching for the certificate of the recipient based on the recipient address with the first domain name truncated to identify the second domain name, and searching for the certificate of the recipient based on the recipient address with the first user name truncated to identify the second user name, concurrently.

- 5 4. The method according to any one of claims 1 to 3, wherein the electronic messaging system resides on a mobile wireless communication device.
5. The method according to claim 4, wherein said searching for the certificate of the recipient based on the match with the recipient address, and said automatically searching for the certificate of the recipient based on the canonical name
10 associated with the recipient address if no match occurs based on the recipient address are conducted on said mobile wireless communication device.
6. The method according to any one of claims 1 to 3, wherein said searching for the certificate of the recipient based on the match with the recipient address, and said automatically searching for the certificate of the recipient based on the
15 canonical name associated with the recipient address if no match occurs based on the recipient address are conducted on a server associated with said electronic messaging system.
7. The method according to any one of claims 1 to 6, wherein said canonical name comprises at least one of multiple canonical domain names and multiple
20 canonical user names.
8. A method for locating a certificate for an electronic messaging system, wherein acts of the method are performed by a processor of a computing device, and wherein the method comprises:

25 searching for a certificate of a recipient of an electronic message based on a canonical name associated with a recipient address of the recipient;

wherein the recipient address comprises at least a first user name and at least a first domain name, and wherein the canonical name is the recipient address

with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name.

9. The method according to claim 8, wherein said canonical name comprises at least one of multiple canonical domain names and multiple canonical user names.

5 10. The method according to claim 8 or claim 9, wherein the searching for the certificate of the recipient of the electronic message based on the canonical name associated with the recipient address comprises:

first searching for the certificate of the recipient based on the recipient address with the first domain name truncated to identify the second domain name,
10 and if no matching certificate is found then searching for the certificate of the recipient based on the recipient address with the first user name truncated to identify the second user name.

11. The method according to claim 8 or claim 9, wherein the searching, for the certificate of the recipient of the electronic message based on the canonical name
15 associated with the recipient address comprises:

searching for the certificate of the recipient based on the recipient address with the first domain name truncated to identify the second domain name, and searching for the certificate of the recipient based on the recipient address with the first user name truncated to identify the second user name, concurrently.

20 12. The method according to any one of claims 8 to 11, wherein the electronic messaging system resides on a mobile wireless communication device, and wherein the searching is conducted on at least one of said mobile wireless communication device and a server associated with said electronic messaging system.

25 13. A method for locating a certificate in an electronic messaging system, wherein acts of the method are performed by a processor of a computing device, and wherein the method comprises:

obtaining a sender address for an electronic message received by the electronic messaging system, said sender address comprising a first user name and a first domain name;

5 searching for a certificate of the sender based on a match with the sender address;

10 automatically searching for the certificate of the sender based on a canonical name associated with the sender address if no certificate of the sender is found based on a match with the sender address, wherein the canonical name is the sender address with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name; and

providing an indication of whether the certificate of the sender has been found.

14. The method according to claim 13, wherein the automatically searching for the certificate of the sender based on the canonical name associated with the sender address comprises:

20 first searching for the certificate of the sender based on the sender address with the first domain name truncated to identify the second domain name, and if no matching certificate is found then searching for the certificate of the sender based on the first user name truncated to identify the second user name.

15. The method according to claim 13, wherein the automatically searching for the certificate of the sender based on the canonical name associated with the sender address comprises:

25 searching for the certificate of the sender based on the sender address with the first domain name truncated to identify the second domain name, and searching for the certificate of the sender based on the first user name truncated to identify the second user name, concurrently.

16. The method according to any one of claims 13 to 15, wherein said searching for the certificate of the sender based on the match with the sender address, and said automatically searching for the certificate of the sender based on the canonical name associated with the sender address if no certificate of the sender is found based on the match with the sender address are conducted on a mobile wireless communication device.

17. The method according to any one of claims 13 to 15, wherein said searching for the certificate of the sender based on the match with the sender address, and said automatically searching for the certificate of the sender based on the canonical name associated with the sender address if no certificate of the sender is found based on the match with the sender address are conducted on a server of the messaging system.

18. The method according to any one of claims 13 to 17, wherein said canonical name comprises at least one of multiple canonical domain names and multiple canonical user names.

19. A method for locating a certificate for an electronic messaging system, wherein acts of the method are performed by a processor of a computing device, the acts comprising:

searching for a certificate of a sender of an electronic message based on a canonical name associated with a sender address of the sender, wherein the sender address comprises at least a first user name and at least a first domain name and wherein the canonical name is the sender address with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name.

20. The method according to claim 19, wherein said canonical name comprises at least one of multiple canonical domain names and multiple canonical user names.

21. The method according to claim 19 or claim 20, wherein the searching for the certificate of the sender of the electronic message based on the canonical name associated with the sender address of the sender comprises:

5 first searching for the certificate of the sender based on the sender address with the first domain name truncated to identify the second domain name, and if no matching certificate is found then searching for the certificate of the sender based on the sender address with the first user name truncated to identify the second user name.

10 22. The method according to any one of claims 19 to 20, wherein the searching for the certificate of the sender of the electronic message based on the canonical name associated with the sender address of the sender comprises:

15 searching for the certificate of the sender based on the sender address with the first domain name truncated to identify the second domain name, and searching for the certificate of the sender based on the sender address with the first user name truncated to identify the second user name, concurrently.

20 23. The method according to any one of claims 19 to 22, wherein the electronic messaging system resides on a mobile wireless communication device, and wherein the searching is conducted on at least one of said mobile wireless communication device and a server associated with said electronic messaging system.

24. A method for locating a certificate for an electronic messaging system, wherein acts of the method are performed by a processor of a computing device, and wherein the method comprises:

25 obtaining a recipient address of a recipient of an electronic message to be sent by the electronic messaging system, said recipient address comprising a first user name and a first domain name;

searching for a certificate of the recipient based on a match with the recipient address, and automatically searching for the certificate of the recipient based on a canonical name associated with the recipient address concurrently with said searching for the certificate of the recipient based on the recipient address, wherein the canonical name is the recipient address with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name;

and providing an indication of whether the certificate of the recipient has been found.

25. A method for locating a certificate for an electronic messaging system, wherein acts of the method are performed by a processor of a computing device, and wherein the method comprises:

receiving a sender address for an electronic message received by the electronic messaging system, said sender address comprising a first user name and a first domain name;

searching for a certificate of the sender based on a match with the sender address, and automatically searching for the certificate of the sender based on a canonical name associated with the sender address concurrently with said searching for the certificate of the sender based on the sender address, wherein the canonical name is the sender address with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name; and

providing an indication of whether the certificate of the sender has been found.

26. A system for locating a certificate in an electronic messaging system, comprising:

a plurality of devices capable of sending and receiving electronic messages;

a server for processing at least some electronic messages;

program logic executable by a processor and operable to locate a certificate of a sender or a recipient of an electronic message based on a canonical name associated with the sender or the recipient respectively, wherein said program logic operates to search for the certificate based on an address of the sender or recipient of the message, said address comprising a first user name and a first domain name, and if no certificate is found, wherein said program logic further operates to automatically search for the certificate of the sender or the recipient based on the canonical name associated with the address of the sender or the recipient of the message, and provide an indication of whether the certificate of the sender or the recipient has been found, wherein the canonical name is the address of the sender or the recipient with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name.

27. The system according to claim 26, wherein said program logic is resident on at least one of said plurality of devices capable of sending and receiving electronic messages.

28. The system according to claim 26, wherein said program logic is resident on said server.

29. The system according to any one of claims 26 to 28, wherein said plurality of devices comprises a mobile wireless communication device.

30. A computer-readable medium for storing the program logic of the system according to any one of claims 26 to 29, the program logic comprising instructions executable by the processor.

31. A system for locating a certificate for an electronic messaging system, comprising:

a plurality of devices capable of sending and receiving electronic messages;

a server for processing at least some electronic messages;

program logic executable by a processor and operable to search for a certificate of a sender or a recipient of an electronic message based on a canonical name associated with an address of the sender or the recipient respectively, wherein the address of the sender or the recipient comprises at least a first user name and at least a first domain name, and wherein the canonical name is the address of the sender or the recipient with the first domain name truncated to identify a second domain name and the first user name truncated to identify a second user name.

32. The system according to claim 31, wherein said program logic is resident on at least one of said plurality of devices capable of sending and receiving electronic messages.

33. The system according to claim 31, wherein said program logic is resident on said server.

34. The system according to any one of claims 31 to 33, wherein said plurality of devices comprises a mobile wireless communication device.

35. The system according to any one of claims 31 to 34, wherein before searching for the certificate of the sender or the recipient based on the canonical name associated with the address of the sender or the recipient respectively, said program logic operates to obtain the address of the sender or the recipient and to search for a certificate of the sender or the recipient based on a match with the address of the sender or the recipient respectively, wherein the program logic operates to automatically perform said searching for the certificate of the sender or the recipient based on the canonical name associated with the address of the sender or the recipient respectively if no match occurs when searching based on the address of the sender or the recipient, and provide an indication of whether the certificate of the sender or the recipient has been found.

36. The system according to any one of claims 31 to 34, wherein when searching for the certificate of the sender or the recipient based on the canonical name associated with the address of the sender or the recipient respectively address, the program logic operates to first search for the certificate of the sender or the recipient based on the address of the sender or the recipient with the first domain name truncated to identify the second domain name, and if no matching certificate is found then searching for the certificate of the sender or the recipient based on the address of the sender or the recipient with the first user name truncated to identify the second user name.

37. The system according to any one of claims 31 to 34, wherein when searching for the certificate of the sender or the recipient based on the canonical name associated with the address of the sender or the recipient respectively, the program logic operates to concurrently search for the certificate of the sender or the recipient based on the address of the sender or the recipient with the first domain name truncated to identify the second domain name and the first user name truncated to identify the second user name.

38. The system according to any one of claims 31 to 37, wherein said canonical name comprises at least one of multiple canonical domain names and multiple canonical user names.

39. A computer-readable medium for storing the program logic of the system according to any one of claims 31 to 38, the program logic comprising instructions executable by the processor.

40. A method of locating a certificate, the method performed by a processor of a computing device, the method comprising:

identifying an e-mail address, said e-mail address comprising a user name and a name of a first domain;

truncating the name of the first domain to identify the name of a second domain; and

searching for one or more certificates associated with an address comprising the user name and the name of the second domain, wherein the first domain is a subdomain of the second domain.

5 41. The method of claim 40, further comprising providing an indication of a result of said searching, wherein said indication indicates whether at least one certificate associated with an address comprising the user name and the name of the second domain was found as a result of said searching.

10 42. The method of claim 40 or claim 41, further comprising searching for one or more certificates associated with the e-mail address comprising the user name and the name of the first domain.

15 43. The method of claim 42, wherein the searching for one or more certificates associated with the address comprising the user name and the name of the second domain is performed upon determining that no certificates associated with the e-mail address comprising the user name and the name of the first domain are found.

20 44. The method of claim 42, wherein said searching for one or more certificates associated with the e-mail address comprising the user name and the name of the first domain and said searching for one or more certificates associated with the address comprising the user name and the name of the second domain are performed concurrently.

45. The method of any one of claims 40 to 44, further comprising truncating the user name to identify a second user name, and searching for one or more certificates associated with an address comprising the second user name and the name of the second domain.

25 46. The method of any one of claims 40 to 45, wherein the computing device comprises a mobile device.

47. The method of any one of claims 40 to 46, wherein the searching comprises searching certificates resident on the computing device.

48. The method of any one of claims 40 to 46, wherein the searching comprises searching certificates stored on a server.

5 49. The method of any one of claims 40 to 48, wherein the identified e-mail address is associated with a recipient of an e-mail message to be sent from the computing device.

50. The method of any one of claims 40 to 48, wherein the identified e-mail address is associated with a sender of an e-mail message received at the
10 computing device.

51. A computing device configured to locate a certificate, wherein a processor of the computing device is configured to:

identify an e-mail address, said e-mail address comprising a user name and a name of a first domain;

15 truncate the name of the first domain to identify the name of a second domain; and

search for one or more certificates associated with an address comprising the user name and the name of the second domain, wherein the first domain is a subdomain of the second domain.

20 52. The device of claim 51, wherein the processor is further configured to provide an indication of a result of said searching, and wherein said indication indicates whether at least one certificate associated with an address comprising the user name and the name of the second domain was found as a result of said searching.

53. The device of claim 51 or claim 52, wherein the processor is further configured
25 to search for one or more certificates associated with the e-mail address comprising the user name and the name of the first domain.

54. The device of claim 53, wherein the search for one or more certificates associated with the address comprising the user name and the name of the second domain is performed upon determining that no certificates associated with the e-mail address comprising the user name and the name of the first domain are found.

55. The device of claim 53, wherein the search for one or more certificates associated with the e-mail address comprising the user name and the name of the first domain and the search for one or more certificates associated with the address comprising the user name and the name of the second domain are performed concurrently.

56. The device of any one of claims 51 to 55, wherein the processor is further configured to truncate the user name to identify a second user name, and search for one or more certificates associated with an address comprising the second user name and the name of the second domain.

57. The device of any one of claims 51 to 56, wherein the device comprises a mobile device.

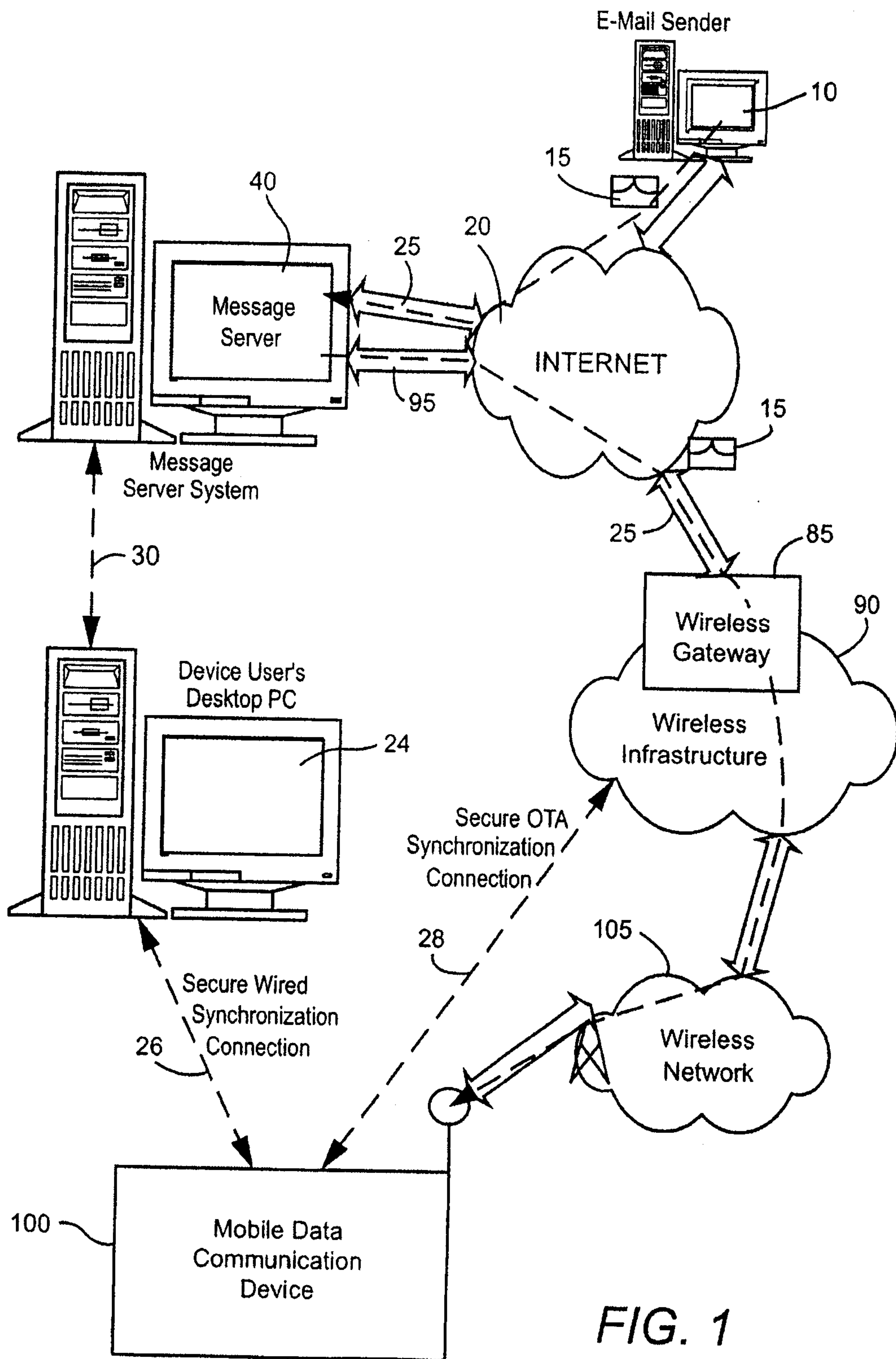
58. The device of any one of claims 51 to 57, wherein the processor is configured to search for certificates resident on the computing device.

59. The device of any one of claims 51 to 57, wherein the processor is configured to search for certificates stored on a server.

60. The device of any one of claims 51 to 59, wherein the identified e-mail address is associated with a recipient of an e-mail message to be sent from the computing device.

61. The device of any one of claims 51 to 59, wherein the identified e-mail address is associated with a sender of an e-mail message received at the computing device.

1/9



2/9

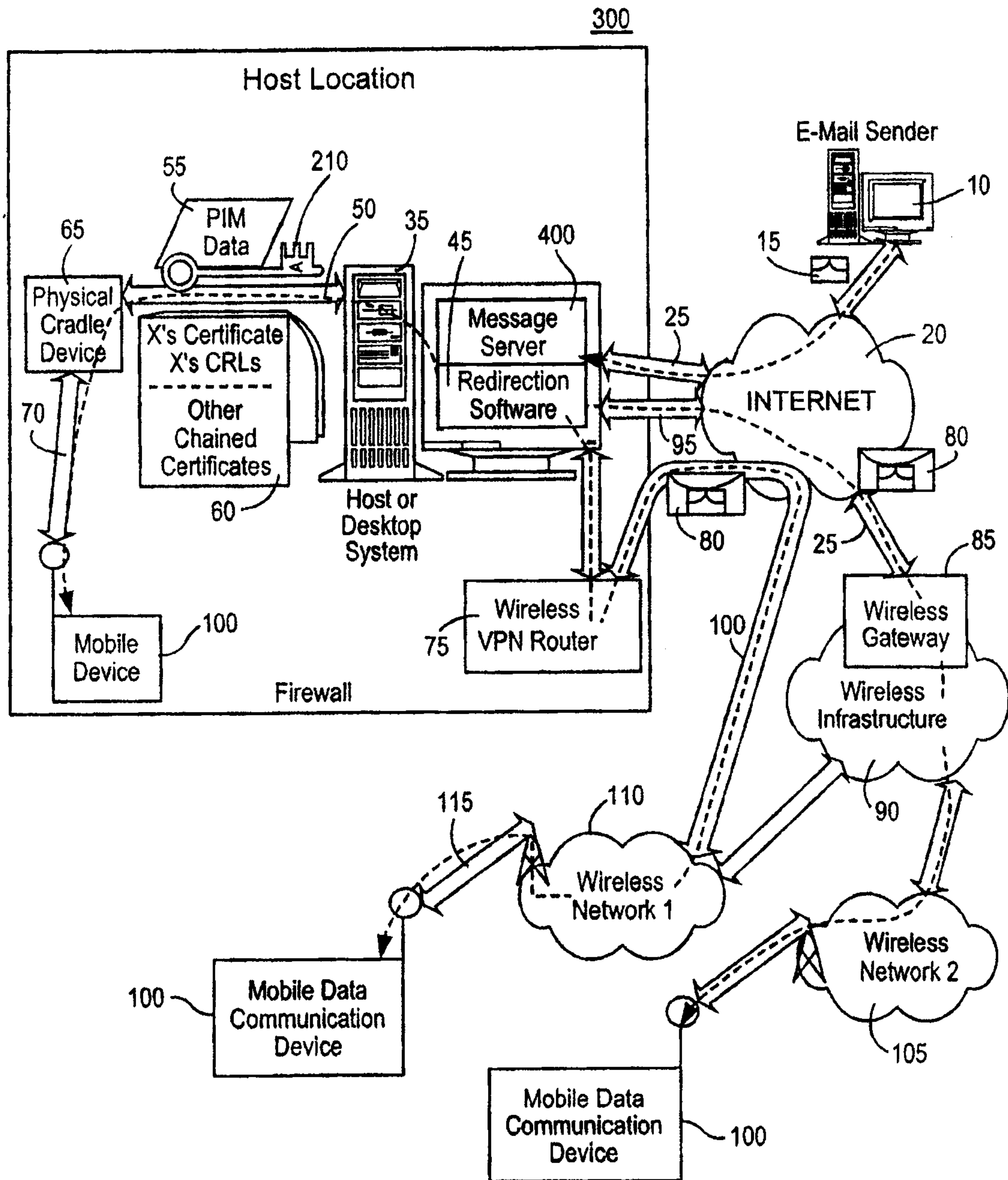


FIG. 2

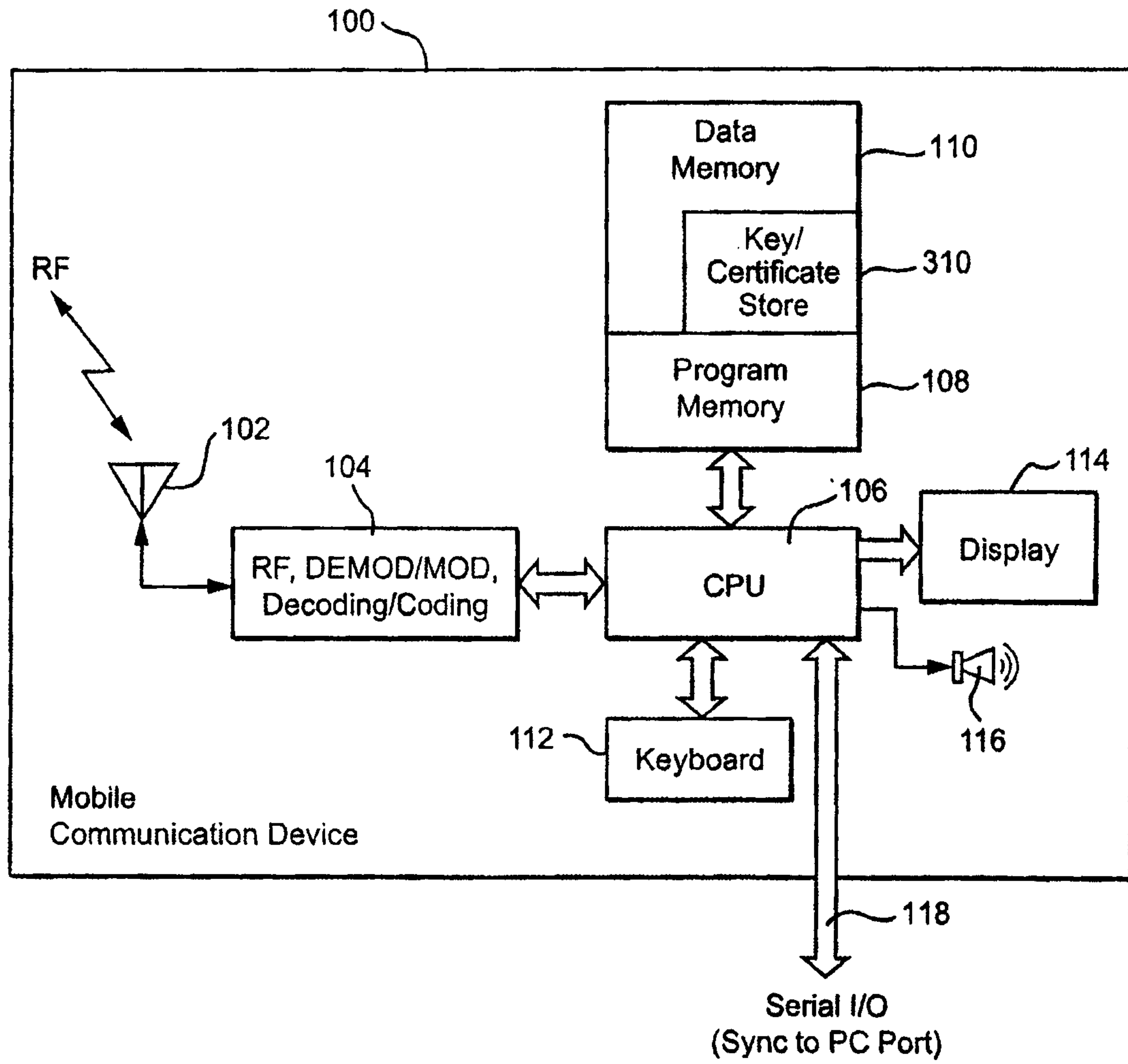


FIG. 3

4/9

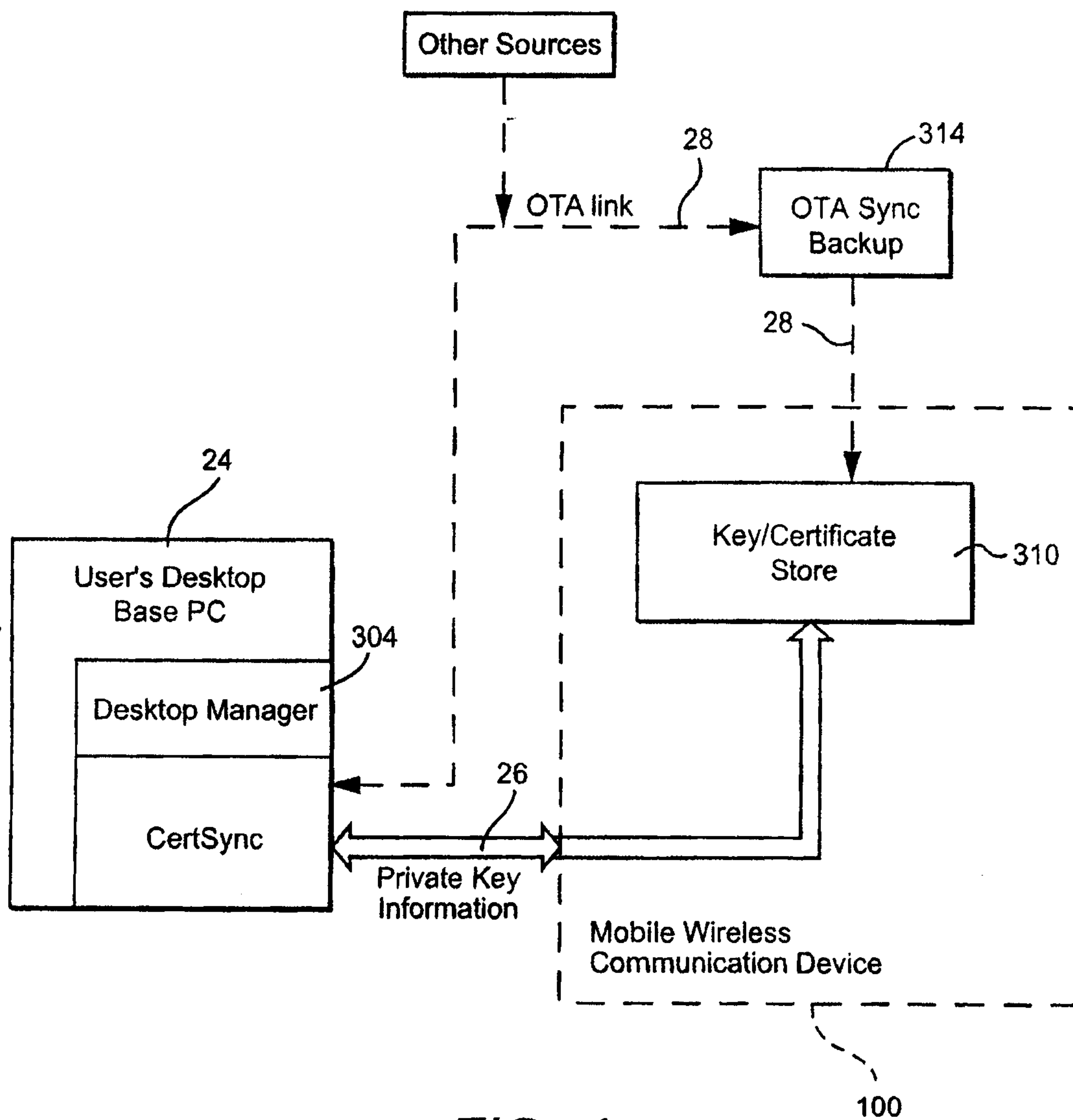
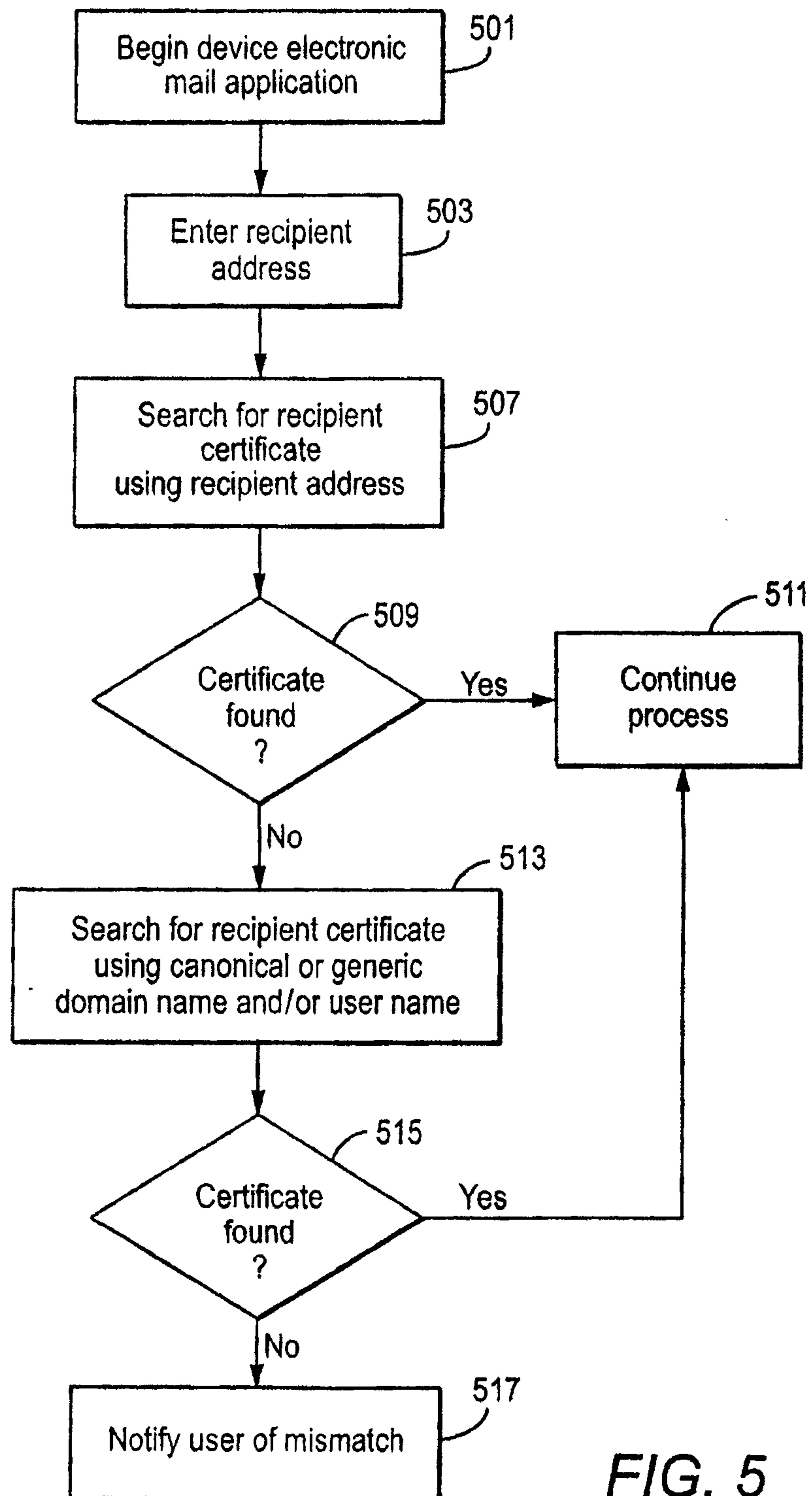
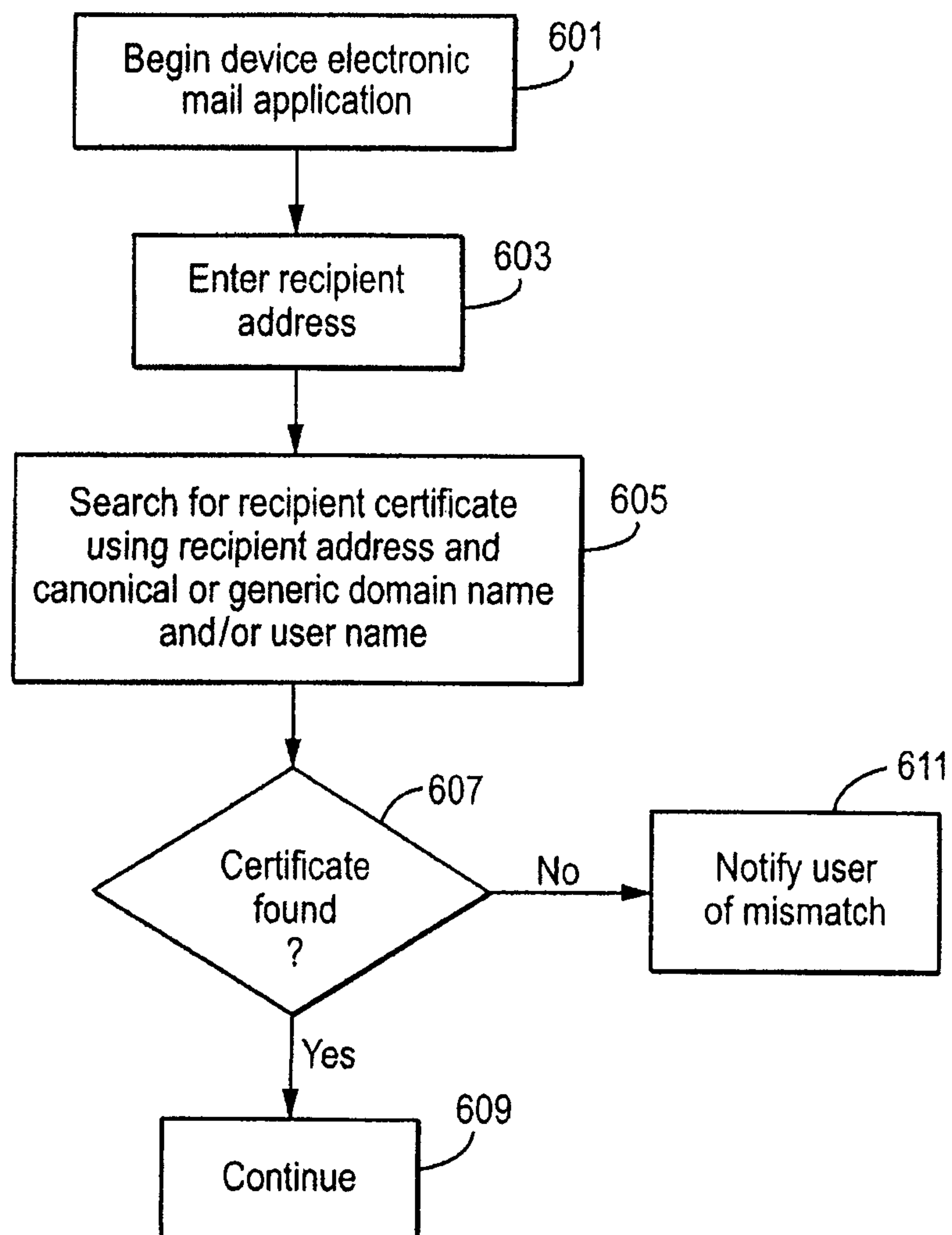


FIG. 4

5/9

**FIG. 5**

6/9

**FIG. 6**

7/9

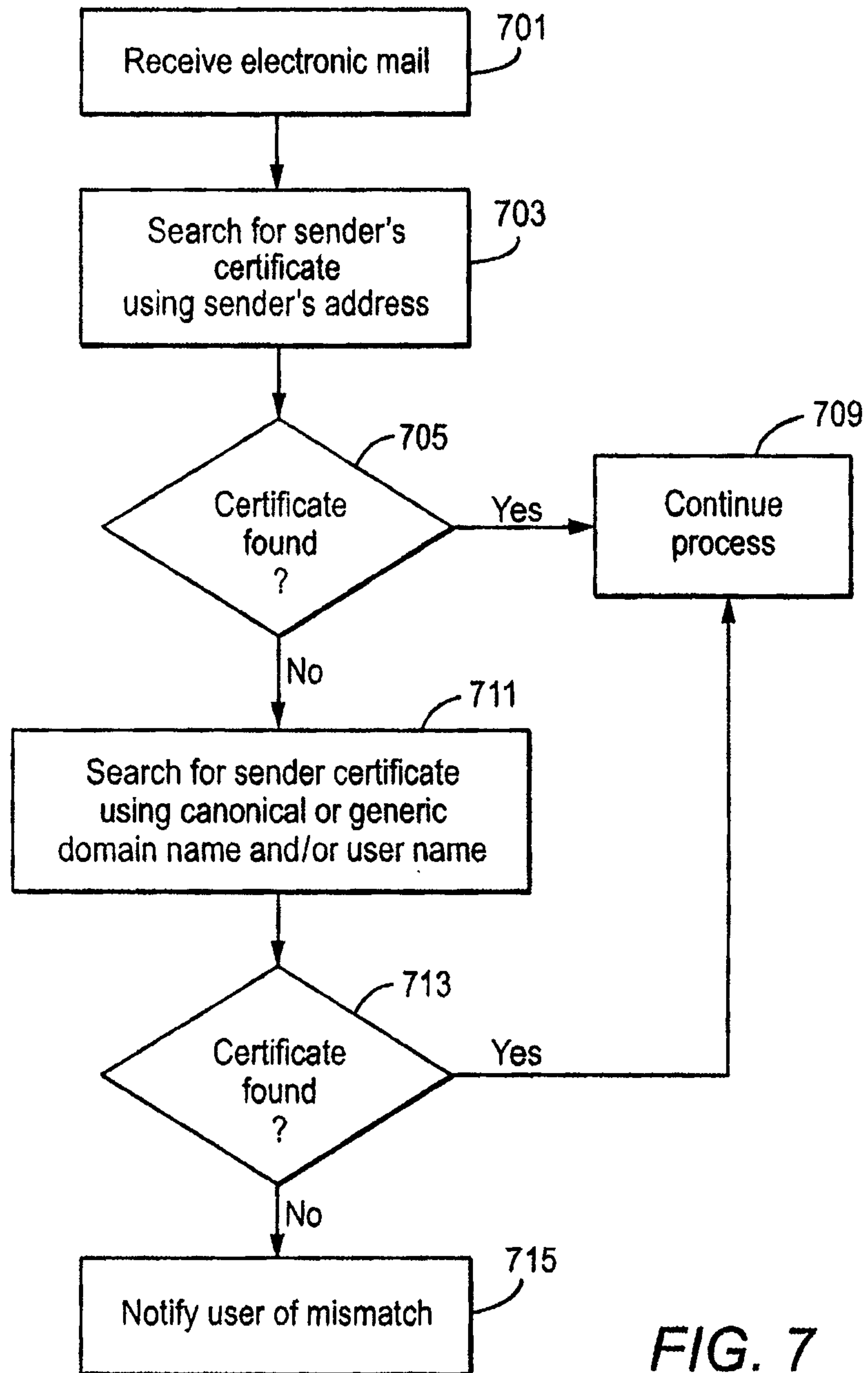


FIG. 7

8/9

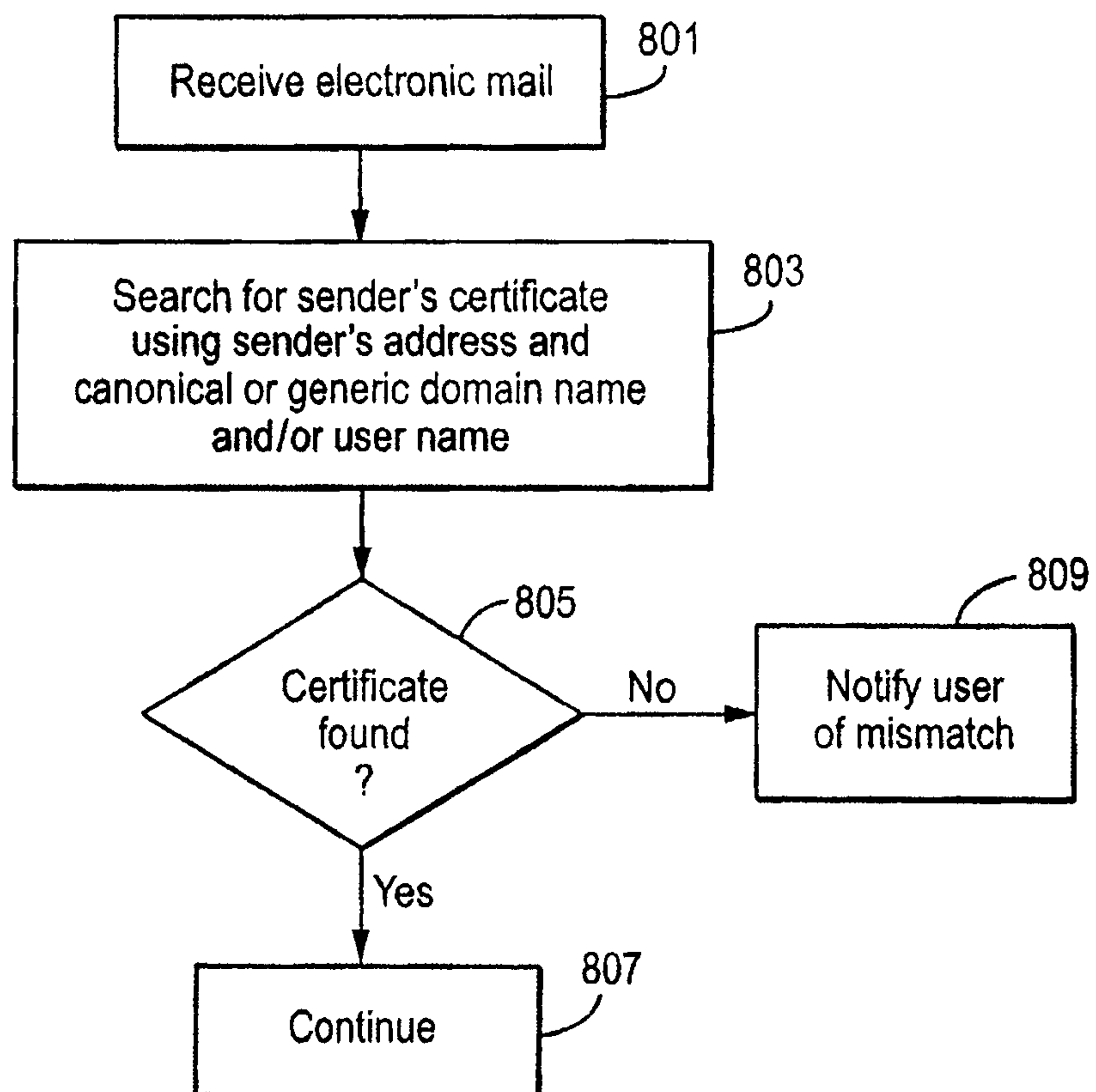


FIG. 8

Default

Security Policy Group

SMIME Application Policy Group

PGP Application Policy Group

Memory Cleaner Policy Group

TLS Application Policy Group

WTLS Application Policy Group

Browser Policy Group

SIM Application Toolkit

TCP Policy Group

PIM Sync Policy Group

Bluetooth Policy Group

VoIP Policy Group

Smart Dialing Policy Group

VPN Policy Group

WLAN Policy Group

On-Device Help Policy Group

Bluetooth Smart Card Reader

MDS Policy Group

Secure Email Policy Group

Desktop Policy Group

Service Exclusivity Policy Group

Certificate Ssync Policy Group

BlackBerry Messenger Policy Group

User Defined Items

Disable Certificate Address Checks

Canonical Certificate Domain Name

agency.gov

Canonical Certificate Domain Name

Specify the domain name that is used for the email addresses contained in certificates issued within the organization. This rule is intended for use in organizations where users' certificates contain a long-lived email address but they typically send email from a shorter-lived email address with the

OK

Cancel

Apply

FIG. 9

