(11) Application No. AU 2003257282 B2

(19) AUSTRALIAN PATENT OFFICE

(54) Title

System, method and computer product for delivery and receipt of S/MIME encrypted data

(51)[6] International Patent Classification(s)

G06F 13/00 (2006.01) 0BMJP H04L
G09C 1/00 (2006.01) 12/22
H04L 12/22 (2006.01) 20060101ALI2006031
H04L 12/58 (2006.01) 0BMJP H04L
H04L 29/06 (2006.01) 12/58
G06F 13/00 20060101ALI2005100
20060101AFI2006031 8BMEP H04L
0BMJP G09C 29/06
1/00 20060101ALI2005100
20060101ALI2006031 8BMEP
PCT/CA2003/001102

(21) Application No: 2003257282 (22) Application Date: 2003.07.23

(87) WIPO No: WO04/010661

(30) Priority Data

(31) Number	(32) Date	(33) Country
2,394,451	2002.07.23	CA

(43) Publication Date : 2004.02.09

(43) Publication Journal Date : 2004.03.18

(71) Applicant(s)

Echoworx Corporation

(72) Inventor(s)

Roberts, Michael; Waugh, Donald; Viatcheslav, Ivanov

(74) Agent/Attorney

Wrays, Ground Floor 56 Ord Street, West Perth, WA, 6005

(56) Related Art

WO 2000/042748
WO 2001/097089
US 6356937
STALLINGS, XP 000774260

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010661 A1

(51) International Patent Classification[7]: H04L 12/58, 29/06

(21) International Application Number: PCT/CA2003/001102

(22) International Filing Date: 23 July 2003 (23.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,394,451 23 July 2002 (23.07.2002) CA

(71) Applicant (*for all designated States except US*): **E-WITNESS INC.** [CA/CA]; 2950 Keele Street, Unit C, Toronto, Ontario M3M 2H2 (CA).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **WAUGH, Donald** [CA/CA]; 433 Canterbury Crescent, Oakville, Ontario L6J 5K8 (CA). **ROBERTS, Michael** [CA/CA]; 56 Mountfield Crescent, Thornhill, Ontario L4J 7E6 (CA). **VIATCHESLAV, Ivanov** [CA/CA]; 101 Joanna Crescent, Thornhill, Ontario L4J 5G1 (CA).

(74) Agent: **GIERCZAK, Eugene, J., A.**; c/o Miller Thomson, LLP, 20 Queen Street West, Suite 2500, Toronto, Ontario M5H 3S1 (CA).

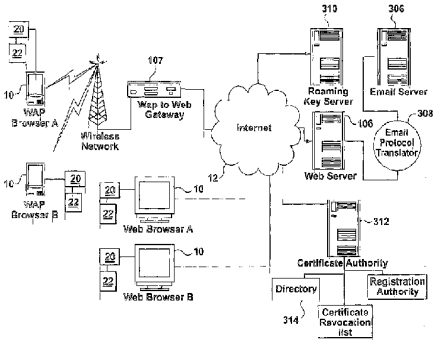
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH,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

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

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEM, METHOD AND COMPUTER PRODUCT FOR DELIVERY AND RECEIPT OF S/MIME ENCRYPTED DATA



(57) Abstract: A system for encrypting and decrypting S/MIME messages using a browser in either a web or wireless device for transmission to or from a web server on the Internet connected to an email server. The S/MIME encryption and decryption is conducted using a standard web browser on a personal computer or a mini browser on a wireless device such that email transmitted to the web or wireless browser from the web server can be completed and encrypted and signed by the user of the browser with such encrypted and signed data can be sent back to the web server. A method for delivering and using private keys in a browser and to ensure that such keys are destroyed after use is also provided. A method of transmitting encrypted S/MIME compliant messages to a web or wireless browser and decrypting and verifying such messages using the browser on the wireless device is also disclosed. A method for authenticating the sender/user of the browser, and a method for verifying and retrieving the certificates of the intended recipient of such messages in accordance with the public key infrastructure.

WO 2004/010661 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

SYSTEM, METHOD AND COMPUTER PRODUCT FOR DELIVERY AND RECEIPT OF S/MIME ENCRYPTED DATA

Field of the Invention

The invention relates generally to secure delivery and receipt of data in a public key infrastructure (PKI). This invention relates more particularly to secure delivery and receipt of S/MIME encrypted data (such as electronic mail) using web and WAP browsers connected to the Internet.

Throughout the specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Further, throughout the specification, unless the context requires otherwise, the word "include" or variations such as "includes" or "including", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Background of the Invention

Each document, reference, patent application or patent cited in this text is expressly incorporated herein in their entirety by reference, which means that it should be read and considered by the reader as part of this text. That the document, reference, patent application, or patent cited in this text is not repeated in this text is merely for reasons of conciseness.

Reference to cited material or information contained in the text should not be understood as a concession that the material or information was part of the common general knowledge or was known in Australia or any other country.

In the past 10 years, email (electronic mail) has taken on unparalleled use, as email has generally become an invaluable tool that enables parties to communicate work products quickly, easily, and efficiently. While email is very convenient, the security of data communicated using email is generally becoming an increasing concern as corporate correspondence moves from paper to digital form and hackers become more proficient at penetrating email systems. As 60% of a company's intellectual property can be found in digital form somewhere in its email message system (as some reports state), the need for secure email messaging is a valid concern, particularly in the case of sensitive business information.

In order to address this need for email security, S/MIME (Secure Multipurpose Internet Mail Extension) protocol was established by RSA Data Security and other software vendors approximately in 1995. The goal of S/MIME was to provide message integrity, authentication, non-repudiation and privacy of email messages through the use of PKI (Public Key Infrastructure) encryption and digital signature technologies. Email applications that support S/MIME are assured that third parties, such as network administrators and ISPs, cannot intercept, read or alter their messages. S/MIME functions primarily by building security on top of the common MIME protocol, which defines the manner in which an electronic message is organized, as well as the manner in which the electronic message is supported by most email applications.

Currently, the most popular version of S/MIME is V3 (version three), which was introduced in July 1999. Further information on S/MIME standardization and related documents can be found on the Internet Mail Consortium web site (**www.imc.org**) and the IETF S/MIME working group (**www.ietf.org/html.charters/smime-charter.html**).

The S/MIME V3 Standard consists generally of the following protocols:

- Cryptographic Message Syntax (RFC 2630)
- S/MIME Version 3 Message Specification (RFC 2633)
- S/MIME Version 3 Certificate Handling (RFC 2632)
- Diffie-Hellman Key Agreement Method (RFC 2631)

Enhanced Security Services (RFC 2634) is another protocol for S/MIME, and is a set of extensions which allows signed receipts, security labels, and secure mailing lists. The extensions for signed receipts and security labels will work with either S/MIME V2 or S/MIME v3, whereas the extension for secure mailing lists will only work with S/MIME V3. S/MIME messages are exchanged between users by requiring that the email software prepare an S/MIME file in accordance with the S/MIME specifications. The S/MIME file is sent as an attachment to an email message. Once this message reaches the recipient, it can only be processed if the recipient possesses a comparable version of an S/MIME email reader.

There are a number of challenges in exchanging email messages with the current S/MIME standards, including the following. If the recipient does not have S/MIME software capabilities, then the S/MIME message cannot be accessed and will be stored unopened, on the recipient's computer. An S/MIME encrypted message can similarly not be read if either the sender or the recipient was not enrolled with a Certificate Authority. The same result would occur if there were incompatibility between the S/MIME versions used by the sender and the recipient. This is a particularly important problem in that the S/MIME standards contemplate a general scale update of the then current S/MIME version to a modified S/MIME version in the event of a detected security breach. S/MIME email exchange would also be hindered if there was incompatibility between the email software used by each of the sender or recipient. S/MIME encrypted email exchange would also effectively be prevented if the S/MIME compatible email software was corrupt or if the sender's or recipient's keys have expired.

In order to remedy many of these problems, recipients usually upgrade or obtain their S/MIME email reader to take advantage of the most recent standardized version of the S/MIME protocol. The difficulty with this solution is the fact that it requires the user to download relatively large additional software packages that require constant updating in addition to taking up system resources.

Deployment of S/MIME encryption for secure email messaging using browsers is one possible solution to the aforesaid problems. A number of prior art solutions employing web or WAP browser technology have been proposed.

For example, Application No. WO00/42748, published on July 20, 2000, inventors Dmitry Dolinsky and Jean-Christophe Bandini, assigned to Tumbleweed Communications Corp. (the "Tumbleweed" reference), discloses a prior solution for secure web based email which is stated to eliminate the need for the user and the recipient to download S/MIME software packages through the use of an intermediary host server, separate from the email software applications. In this solution, the intermediary host server intercepts emails sent by the sender and then passes a message on to the recipient's email account informing them that a secure email is waiting for them. This message also contains the link to the decrypted message located on the intermediary host server. The decrypted message is presented to the recipient in an SSL session.

This prior art solution has a number of disadvantages. Relatively speaking, the use of an intermediary host server generally complicates the secure transactions overall and increases the infrastructure costs of providing secure email messaging. Another disadvantage of the Tumbleweed technology is that because the sender's computer does not have cryptographic capability, the solution overall bears the relative risks associated with a relatively porous network environment. Also, the nature of the solution proposed in the Tumbleweed reference overall does not readily provide for deployment over wired and wireless networks.

Another prior art solution, namely W/O 01/97089 A (Cook David P: Zixit Corp (US)) 20 December 2001 (2001-12-20) and Stallings W: "S/MIME: E-mail Gets Secure" Byte, McGraw-Hill Inc. St. Peterborough, US, vol. 23, no.7, 1 July 1998 (1998-07-01), pages 41-42, XP000774260 ISSN: 0360-5280 discloses a solution for sending/receiving S/MIME communications wherein the communications are encrypted/decrypted by a forwarding system consisting of a server based solution that enables the creation and decyphering of S/MIME communications. A browser linked to a network-connected device establishes a secure session with the forwarding system for the purpose of downloading

decrypted S/MIME communications, and also creating S/MIME communications, by operation of the forwarding system. This prior art solution has a number of disadvantages.

The ZIXIT approach integrates with a standard email client software such as Outlook. The user has all the assurances for the security of their email but they do not have any computer anywhere capability. They must always use the computer which has the ZIXIT thick email client and so they are not mobile. The aspect of ZIXIT which uses a browser is to deliver messages securely to recipients who are not using the ZIXIT software. In this scenario when the email author sends the email to a non ZIXIT user the message is stored to a message server and a pick up notice is sent to the recipient with a URL link to the message. The recipient clicks on the link and the message is downloaded to the browser using SSL.

In this way ZIXIT does not provide an S/MIME solution that leverages the pervasive nature of browser technology by enabling users to send and receive S/MIME compliant messages via a browser without the need of a message server linked to PKI infrastructure. Encryption at the client without the need for a thick client enables better utilization of resources at the client while providing pervasive security.

What is needed therefore is a web-based system, computer product and method for communicating data (including emails) on a secure basis using S/MIME that is easy to deploy using web and WAP browsers. What is further needed is an aforesaid system, computer product and method that is easily deployed, and at a relatively low cost, in that the cryptographic resources required for S/MIME encrypted messaging is provided at the network-connected devices themselves. What is also needed is a web-based system, computer product and method whereby the S/MIME encryption persists throughout the communication of data.

Disclosure of the Invention

In accordance with a first aspect of the present invention, there is provided a system for exchanging S/MIME compliant communications electronically comprising:

(a) at least one network-connected device for communicating with one or more remote devices via a communication network, said network-connected device comprising:

(b) a browser linked to the network-connected device;

(c) an encryption/decryption facility linked to the browser so as to enable PKI transactions to be conducted in the browser; and

(d) an S/MIME facility linked to the browser and the encryption/decryption facility that enables the network-connected device to exchange S/MIME compliant communications with remote network-connected devices via the browser in cooperation with the encryption/decryption facility.

Preferably, the system also comprises:

(a) a key storage means for storing a plurality of keys, each being usable by an associated user in a public key infrastructure to encrypt and decrypt data; and

(b) a user authentication means for determining whether a prospective user of a key in the plurality of keys is the associated user for the key;

wherein the encryption/decryption facility is linked to the key storage means and the user authentication means such that the encryption/decryption facility encrypts and decrypts data using the plurality of keys when the user authentication means authenticates a user of the network-connected device.

Preferably, the system further comprises an email server, and wherein the encryption/decryption facility and the S/MIME facility enable S/MIME compatible messages to be exchanged between the network-connected device and the email server.

Preferably, the user authentication means communicates with a Certificate Authority to authenticate the prospective user.

Preferably, the user authentication means comprises a roaming key server that authenticates the sender of an S/MIME compliant communication and transmits the sender's private key and certificate to the network-connected device via the remote server.

In accordance with a second aspect of the present invention, there is provided a computer program product operable on a network-connected device for enabling S/MIME compliant communications between the network-connected device and remote devices via a communication network, the computer program product comprising:

(a) a browser;

(b) an encryption/decryption facility linked to the browser so as to enable PKI transactions to be conducted in the browser; and

(c) an S/MIME facility linked to the browser and the encryption/decryption facility that enables the network-connected device to exchange S/MIME compliant communications with the remote device via the browser in cooperation with the encryption/decryption facility.

Preferably, the computer product further comprises:

(a) a key storage means for storing a plurality of keys, each key being usable by an associated user in a public key infrastructure to encrypt and decrypt data; and

(b) a user authentication means for determining whether a prospective user of a key in the plurality of keys is the associated user for the key; wherein the encryption/decryption facility is linked to the key storage means and the user authentication means such that the encryption/decryption facility encrypts and decrypts data using the plurality of keys when the user authentication means authenticates a user of the network-connected device.

Preferably, the S/MIME facility is an S/MIME browser extension.

Preferably, the S/MIME facility enables encryption and signature of electronic messages and attachments.

Preferably, the S/MIME facility is provided such that security of cryptographic operations in the computer product is maintained.

In accordance with a third aspect of the present invention, there is provided a method of sending S/MIME compliant communications electronically comprising:

(a) providing an encryption/decryption facility and an S/MIME facility, linked to a browser, loaded on a network-connected device associated with a sender;

(b) authenticating the sender with a remote server by means of a user authentication means linked to the network-connected device;

(c) the sender requesting an S/MIME compliant communication with a recipient from the remote server;

(d) the remote server communicating the recipient's public key and certificate to the S/MIME facility;

(e) the network-connected device contacting a Certificate Authority to verify the recipient's public key and certificate, by means of the encryption/decryption facility; and

(f) creating an S/MIME compliant communication by signing and encrypting a communication in the browser using the private key of the sender and the public key of the recipient, by means of the encryption/decryption facility and the S/MIME facility.

In accordance with a fourth aspect of the present invention, there is provided a method of retrieving and deciphering S/MIME compliant communications electronically comprising:

(a) providing an encryption/decryption facility and an S/MIME facility , linked to a browser, loaded on a network-connected device;

(b) requesting the retrieval of an S/MIME compliant communication from the network-connected device;

(c) authenticating a recipient associated with the network-connected device with a remote server;

(d) the remote server communicating the sender's public key and certificate to the S/MIME facility;

(e) the remote server sending the requested S/MIME compliant communication to the network-connected device;

(f) the encryption/decryption facility authenticating the recipient's private key and certificate against the private key and certificate stored to a key/certificate store accessible from the network-connected device whereby upon authentication thereof the private key and certificate are released to the S/MIME facility, thereby enabling the S/MIME compliant communication to be deciphered in the browser.

In accordance with a fifth aspect of the present invention, there is provided a system for exchanging S/MIME messages, said system comprising:

at least one network-connected device for communicating with a user via a communication network;

said at least one network-connected device comprising,

a browser,

said browser having an S/MIME extension,

said browser comprising an encryption/decryption component, and said encryption/decryption component comprising a key component for obtaining a key associated with said user; and

said S/MIME extension component being responsive to said encryption/decryption component for encrypting/decrypting an S/MIME message based on the key associated with said user.

Preferably, the system further comprises a key storage for storing a plurality of keys, said keys being usable by an associated user in a public key infrastructure to encrypt and decrypt data; a user authentication component for determining whether a prospective user of one of said plurality of keys is the associated user for said key, wherein said encryption/decryption facility is responsive to said user authentication component for encrypting and decrypting an S/MIME message based on the key for said associated user.

Preferably, the system further comprises an email server for exchanging said encrypted/decrypted S/MIME message between the network-connected device and the email server.

Preferably, said user authentication component comprises a roaming key server that authenticates the sender of an S/MIME compliant communication and transmits the sender's private key and certificate to said network-connected device via said remote server.

Preferably, said user authentication component comprises a communication component for communicating with a Certificate Authority for authenticating said prospective user.

In accordance with a sixth aspect of the present invention, there is provided a computer program product operable on a network-connected device for enabling S/MIME compliant communications between the network-connected device and a remote device via a communication network, the computer program product comprising:

a browser;

said browser comprising an S/MIME extension,

said browser comprising an encryption/decryption component, and said encryption/decryption component comprising a component for obtaining a key associated with a user in a public key infrastructure; and

said S/MIME extension component being responsive to said encryption/decryption component for encrypting/decrypting an S/MIME message intended for said remote device based on the key associated with said user.

Preferably, the computer product further comprises a key storage component for storing a plurality of keys, each key being useable by an associated user in said public key infrastructure to encrypt and decrypt data; and a user authentication component for determining whether a prospective user of a key in the plurality of keys is the associated user for the key, and wherein said encryption/decryption facility is responsive to said user authentication component for encrypting and decrypting an S/MIME message based on the key for said associated user.

Preferably, said S/MIME extension comprises a signature component.

2003257282 29 May 2009

In accordance with a seventh aspect of the present invention, there is provided a system for exchanging S/MIME compliant email via a communication network, said system comprising:

a network-connected device configured for communication with a remote device via the communication network;

said network-connected device comprising a browser, and said browser comprising an authentication component configured to authenticate one or more credentials associated with a user of said network-connected device, and said browser comprising a component responsive to said user for composing an email message;

said browser comprising an encryption/decryption component configured for PKI transactions, and an S/MIME component linked to said encryption/decryption component and configured for converting said email message into an S/MIME compliant email;

an email server comprising an email server software component that receives, stores and transmits S/MIME compliant email, said email server operatively connected to the communication network for receiving the S/MIME compliant email addressed to said remote device; and

said remote device comprising a browser configured for retrieving the S/MIME compliant email from said email server and comprising an S/MIME component configured for deciphering the S/MIME compliant email at said remote device.

Preferably, the system further comprises, a key storage component configured for storing a plurality of keys, each of said plurality of keys being associated with a user in a public key infrastructure to encrypt and decrypt data; and

said authentication component being configured for determining whether a prospective user of a key in the plurality of keys is the associated user for the key, and said encryption/decryption component being linked to said key storage component and said authentication component and said encryption/decryption component being responsive to said authentication component for encrypting/decrypting data using said plurality of keys when said authentication component authenticates a user of the network-connected device.

2003257282 29 May 2009

Preferably, said authentication component is configured to communicate with a Certificate Authority to authenticate a prospective user.

Preferably, the system further comprises a roaming key server configured for authenticating the sender of an S/MIME compliant email and transmitting the sender's private key and certificate to said network-connected device.

In accordance with an eighth aspect of the present invention, there is provided a computer program product operable on a network-connected device for enabling S/MIME compliant email messages between the network-connected device and remote devices via a communication network, the computer program product comprising:

a browser;

a component for composing an email message;

an encryption/decryption component linked to said browser and configured for performing PKI transactions in the browser; and

an S/MIME component linked to said browser and said encryption/decryption component and configured for converting said email message into an S/MIME compliant email message for exchange with the remote device via an email server comprising an email server software component that receives, stores and transmits S/MIME compliant email, said email server connected to the communication network.

Preferably, the computer program product further comprises:

a key storage component configured for storing a plurality of keys, each of said keys being associated with a user in a public key infrastructure for encrypting and decrypting data; and

a user authentication component configured for determining whether a prospective user of a key in the plurality of keys is the associated user for the key.

In accordance with a ninth aspect of the present invention, there is provided a device for creating and exchanging S/MIME compliant email messages via a communication network, said device comprising:

a browser;

2003257282 29 May 2009

a component for composing an email message;

said browser comprising an S/MIME extension component;

said browser comprising an encryption/decryption component, and said encryption/decryption component comprising a key component for obtaining a key associated with said user;

said S/MIME extension component being responsive to said encryption/decryption component for converting said email message into an S/MIME compliant email message based on the key associated with said user; and

a component configured for transferring said S/MIME compliant email message to an email server comprising an email server software component that receives, stores and transmits S/MIME compliant email, said email server operatively coupled to the communication network.

Preferably, the device further comprises a key storage component configured for storing a plurality of keys, said keys being usable by an associated user in a public key infrastructure to encrypt and decrypt data; a user authentication component for determining whether a prospective user of one of said plurality of keys is the associated user for said key, wherein said encryption/decryption facility is responsive to said user authentication component for encrypting and decrypting an S/MIME message based on the key for said associated user.

[The next page is page 11]

Embodiments of the system, computer product and method of the present invention may enable users to access their email account on an email server and to create or read S/MIME messages through any browser without the need to install client based email software. From a software distribution and user support perspective this generally may eliminate the need to support client based email and may thus reduce the cost of user and software support as well as addressing the need to support user mobility.

In another embodiment of the present invention, users may be enabled to remotely access private keys and digital certificates over the Internet from any network-connected device. This generally may eliminate the need for location specific private key and digital certificate storage.

Brief Description of the Drawings

A detailed description of the preferred embodiment(s) is (are) provided herein below by way of example only and with reference to the following drawings, in which:

Figure **1** is a schematic System Architectural Component Diagram of the S/MIME browser based email system.

Figure **1a** is a program resource chart illustrating the resources of the application of the present invention.

Figure **2** is a flow chart which depicts the steps in receiving, verifying, and decrypting an S/MIME message from an email server for display in a browser.

Figure **3** is a flow chart which depicts the steps for creating, signing and encrypting an S/MIME message in a browser for transmission to a web server to an email server.

Figure **4** is a schematic illustration of the detailed steps involved with creating, signing, and encrypting an unencrypted message.

Figure **5** is a schematic illustration of the detailed steps involved with retrieving and decrypting an encrypted message.

Figure **6** is a schematic System Resource Chart which illustrates the overall system for deploying PKI enablement of data in relation to a wireless network according to the Co-Pending Application.

Figure **7A** is a flow chart which illustrates the two stages involved in posting PKI enabled data in accordance with the Co-Pending Application: a) from a WAP device to the Server, and b) from the Web browser to the Server.

Figure **7B** is a flow chart which illustrates the two stages involved in retrieving posted PKI enabled data in accordance with the Co-Pending Application: a) from the Server to the WAP device, and b) from the Server to the Web browser.

Figure **8** is a schematic diagram illustrating the flow of PKI enabled data from the Server to a wireless device according to the Co-Pending Application.

Figure **9** is a schematic diagram illustrating the flow of PKI enabled data from the Server to a Web browser according to the Co-Pending Application.

Figure **10** is a schematic diagram illustrating the flow of PKI enabled data from a wireless device browser to a Web server according to the Co-Pending Application.Figure 11 is a schematic diagram illustrating the flow of PKI enabled data from a wired Web browser to a Web server according to the Co-Pending Application.

In the drawings, preferred embodiments of the invention are illustrated by way of example. It is to be expressly understood that the description and drawings are only for the purpose of illustration and as an aid to understanding, and are not intended as a definition of the limits of the invention.

Best Mode(s) for Carrying Out the Invention

Detailed Description of the Preferred Embodiment

As illustrated in Fig. **1**, at least one known network-connected device **10** is provided. Network-connected devices **10** may include a number of digital devices that provide connectivity to a network of computers. For example, network-connected device **10** may include a known personal computer or a known WAP device, cell phone, PDA or the like.

The network-connected device **10** is connected to the Internet **12** in a manner that is known. Specifically in relation to Fig. **1**, the connection of a network-connected device **10** that is a known WAP device to the Internet is illustrated, whereby a known WAP to WEB gateway **107** is provided, in a manner that is also known.

Each of the network-connected devices **10** also includes a browser **20**. The browser can be a standard Internet based browser, such as Netscape's Navigator™ or Microsoft's Internet Explorer™ or a known mini browser for wireless products such as cell phones or PDAs.

Each of the network-connected devices **10** also includes the application **22** of embodiments of the present invention. The particulars of this application, and the manner in which it permits PKI enabled communications over wired and wireless networks is disclosed in the co-pending application U.S. Application No. 10/178,224 (the "Co-Pending Application").

In one particular embodiment of application **22**, a browser extension or plug-in is provided in a manner that is known. Specifically, the application **22** and the browser **20** inter-operate by means of, for example, customized HTML tags. As opposed to using an intermediate host server, or a relatively large computer program, application **22** preferably provides necessary resources, as particularized below, to function with any third party PKI system, including for example, ENTRUST™, MICROSOFT™, BALTIMORE™, RSA™ and so forth. It should also be understood that the functions of the application **22** described

herein can also be provided as an "ACTIVE X OBJECT" in a manner that is known, or integrated within a browser.

Each of the network-connected devices **10** also includes a browser **20**. The browser can be a standard Internet based browser, such as Netscape's Navigator™ or Microsoft's Internet Explorer™ or a known mini browser for wireless products such as cell phones or PDAs.

Each of the network-connected devices **10** also includes the application **22** of the present invention. In one particular embodiment of the present invention, application **22** is best understood as a browser extension or plug-in that is provided in a manner that is known. Specifically, the application **22** and the browser **20** inter-operate by means of, for example, customized HTML tags.

It should also be understood, however, that the resources of the application **22** could also be provided by integration of the features of the application **22** in a browser or mini-browser, as opposed to a standalone application.

Application **22** preferably provides necessary resources, as particularized below, to function with any third party PKI system, including for example, ENTRUST™, MICROSOFT™, BALTIMORE™, RSA™ and so forth.

Application **22** includes a cryptographic utility **24**, provided in a manner that is known, that is adapted to perform at network-connected device **10** a series of cryptographic operations, including but not limited to:

- Digital signature of data in form fields;
- Encryption of data in form fields;
- Decryption of data in form fields;
- Verification of signature of data in form fields;
- Digital signature and encryption of data in form fields;
- Verification of Digital signature and decryption of data in form fields;
- Digital signature of full pages;

- Verification of digital signature of full pages;
- Encryption of full pages; and
- File attachment encryption and signing.

Specifically, application **22** includes a Crypto Library **300**, provided in a manner that is known. In one particular embodiment of the present invention, the application **22** also includes a User Certificate and Private Key Store **302** which contains the cryptographic data required to encrypt and/or digitally sign data included in data communications (including email) contemplated by the present invention. For example, in one particular implementation of the present invention, namely one whereby Entrust™ acts as the Certificate Authority, the .EPF file required to authenticate both the sender and the recipient is downloaded to the network-connected device **10**. The .EPF file is an encrypted file which is used to access the user credentials and private key required to process cryptographic operations.

Application **22** of the present invention also includes a PKI browser extension, and specifically an S/MIME browser extension **304**. The S/MIME browser extension permits the encryption and decryption of data communications (including email) in a browser, as particularized herein. This has the advantage of broad-based deployment as browser technology is commonplace. This also has the advantage of deployment across wireless and wired networks as the application **22** of the present invention, including the S/MIME browser extension, can be associated with a web browser or a WAP browser, as shown in Fig. **1**. In addition, the invention disclosed herein, which requires only a browser and the associated application **22** at each network-connected device **10** S/MIME encrypted communications are possible without the resources usually required to run a full S/MIME encryption program/email reader on the network-connected device **10**.

The S/MIME browser extension **304** is provided in a manner known by a skilled programmer. However, it is desirable for the S/MIME browser extension **304** of the present invention to have a number of attributes. First, as a result of the method of the present invention detailed below, it is desirable that the S/MIME browser extension **304** be able to add an attachment to an email message, and also sign and encrypt both the email message

and the attachment such that the email message overall is an S/MIME message. Second, the encryption and decryption of data in accordance with the S/MIME standard described herein involves a potential security risk if the S/MIME browser extension **304** is not designed properly. Specifically, it is necessary to ensure that browser memory is utilized in the course of the cryptographic operations such that security is not compromised. In one particular embodiment of the present invention, this is achieved by using the "TEMP" memory space of the browser **20**, in a manner known by a skilled programmer. Third, the S/MIME browser extension **304** further includes a CLEANUP ROUTINE in a manner that is known that eliminates any remnants from the memory associated with the browser, or otherwise with the network-connected device **10**, of either the message, or the user credential or private key that is part of the User Certificate and Private Key Store **302**, in order to maintain confidentiality.

In addition, the present invention contemplates that the S/MIME browser extension **304** facilitates the acceptance of digital certificates issued by an entity not related to the vendor of the application of the present invention, and also that is not "cross-certified", in a manner that is known. More particularly, the S/MIME browser extension **304** is adapted to permit the user of the application **22** of the present invention to store the digital certificates and public keys of users who are not related to the vendor of the application **22**.

Also connected to the Internet **12**, is a web server **106** which is provided using known hardware and software utilities so as to enable provisioning of the network-connected device **10**, in a manner that is known. The Web server **106** includes a web application **16**. The web application **16** is adapted to execute the operations, including PKI operations, referenced below.

Two of the embodiments of the present invention include, a system, computer product and method for:

1. Creating and delivering an S/MIME compliant email message to an email server; and

2. Retrieving and deciphering an S/MIME compliant email message from an email server.

In order to achieve the foregoing, the system, computer product and method of the embodiment of the present invention relies on aspects of the Co-Pending Application for engaging in PKI enabled transactions. Specifically, the email messages are created and delivered in accordance with the present invention in a manner that is analogous with the "POSTING DATA ON A SECURE BASIS" described in the Co-Pending Application. An email message is retrieved and deciphered in a manner that is analogous with the "RETRIEVING OF DATA ON A SECURE BASIS" also described in the Co-Pending Patent Application. Regarding the details of the manner in which cryptographic operations are processed by the application **22** of the present invention, reference is made to the Co-Pending Patent Application.

Aspects of the Co-Pending Application are disclosed below:

Posting Data on a Secure Basis

FIGS. 7A, 10 and 11 illustrate operation according to the Co-Pending Application in relation to PKI enabled data transactions as between a network-connected device 10, namely a WAP device or Web browser, on the one hand, and web server 106 on the other.

User, on a network-connected device 10, requests web page 18 from the web server 106 by connecting to web server application 16. Web application 16 presents a specific web page 18 responsive to the request from the network-connected device 10. The web page 18 is downloaded to the User through network-connected device 10. Specifically in relation to a network-connected device 10 that is a WAP device, web page 18 is downloaded to the WAP device's browser through the WAP to Web gateway 107 as illustrated in FIG. 6, in a manner that is known. WAP to Web gateway 107 functions as a translator in that it converts wireless device requests to web protocol (HTTP) requests. This translation enables User on the WAP device to access the web page 18 via the wireless network 108, again as illustrated in FIG. 6.

It should be understood, that the Co-Pending Application also contemplates PKI enabled data communications with other users associated with other network connected devices 10. One or more of these other network-connected devices 10 may be a typical personal computer having a known web browser, and connected to the Internet 12 in a manner that is known, as also illustrated in FIG. 6.

In one particular embodiment of the Co-Pending Application, web page 18 includes a web form 26 in a known format preferably including a plurality of fields. The Co-Pending Application contemplates a series of web forms 26, each being identified by a "SUBJECT" or equivalent, depending on the function of the web form 26, as explained below. In one particular embodiment of the web form 26 of the Co-Pending Application, web form 26 comprises mark-up language representing the required input from User, and instructions for cryptographic utility 24 to conduct certain specific cryptographic operations for the particular web form 26, as described below. One aspect of a particular embodiment of the Co-Pending Application is that certain of these instructions, and resultant cryptographic operations, may apply to specific fields included in the web form 26.

The web form 26 is also provided, in a manner that is known, with triggers or instructions that are received by web application 16 for executing functions using the data provided by User to the web form 26, as also particularized below. Again, these triggers or instructions may result in operations by web application 16 involving data contained in particular fields of web form 26. These operations effectively permits PKI enabled Internet provisioning in accordance with the Co-Pending Application.

User provides the data requested by web form 26 and then either the application 22 or the User will determine the location of the Recipient of this data. It should be understood that in some implementations of the Co-Pending Application, the Recipient will be web server 106. In other implementations of the Co-Pending Application, the Recipient will be one or more remote network-connected devices 10, also including the application 22 of the Co-Pending Application. Or the Recipient may be both one or more remote network-connected devices 10 and web server 106. User and Recipient may also

be individuals, for example, a doctor communicating with a patient for the purposes of secure on-line approval of a prescription.

In either case, the User submits the web form 26, typically by clicking on a "SUBMIT" button or equivalent, for sending the contents thereof to the Recipient. The cryptographic utility 24 is responsive to this action to perform a number of functions which are described below. It should be understood that the steps or functions described below could be combined into a lesser number of steps or functions, or expanded to a greater number of steps or functions, without departing from the scope of the Co-Pending Application.

Cryptographic utility 24 gathers from the memory 28 certain cryptographic operation parameters corresponding to the "SUBJECT" of the particular web form 26, including common name, distinguished name, email address or other information of User and/or Recipient; cryptographic mode, and the specific web form 26 fields to operate on.

Cryptographic utility 24 contacts a known Certificate Authority 103 via the communication facility (not shown) provided by network-connected device 10 to obtain information required to provide PKI enabled data to web server 106. Specifically, Certificate Authority 103 controls a Directory 105 that is also connected to the Internet that functions in a manner that is known. Cryptographic utility 24 retrieves certificates for the Recipient from Directory 105 associated with Certificate Authority 103.

Cryptographic utility 24 also interfaces with a known Certificate Revocation List 34, also associated with the Certificate Authority 103, to validate the Recipient's certificate, check for expiration, check for revocation, and also to obtain key usage data to permit use of the Recipient's certificate to conduct a PKI process.

Cryptographic utility 24 authenticates the User for PKI transaction, including for the purpose of preparing for use of the User's private key for digitally signing data included in web form 26 (as explained below).

Cryptographic utility 24 then conducts a series of cryptographic operations which generally include signing data included in web form 26 and/or encryption thereof. It

should be understood that in the Co-Pending Application, cryptographic utility 24 is adapted to perform specific cryptographic operations in relation to specific fields of web form 26 because they are marked for processing by the coding included in web form 26. For example, a particular web form 26 may call for each specified data element to be encoded in PKCS#7 format, or using some other custom data format involving digitally signing and/or encrypting. Data in other fields may remain unmodified.

This permits fields with sensitive data, for example, to be processed on an encrypted and/or digitally signed basis, while other fields with less sensitive data may remain unencrypted and unsigned. This conserves bandwidth, as well as memory resources wherever the data included in the web form 26 may be received. This also allows flexibility in terms of data management in that less sensitive data can be "mined" while protecting sensitive data.

Cryptographic utility 24 then builds a Web compliant "POST" data structure in a manner that is known (HTTP 1.1 for example), comprising for example a field name and clear or cipher text value pairs. This "POST" data structure is then sent to the web server 106. Web application 16 is then adapted to process the data in web form 26 in a manner that is known, in accordance with the particular processes associated with a particular "SUBJECT" defined web form 26. This may involve confirming digital signatures associated with particular fields, decrypting and processing data in particular fields. One important aspect of a particular embodiment of the Co-Pending Application is that the web application 16 in accordance with the Co-Pending Application is adapted to store data in particular fields in an encrypted format to database 14. This improves the security that the Co-Pending Application provides overall in that third parties cannot obtain data sent in accordance with the Co-Pending Application, even by hacking into web server or database 14.

Retrieving Data on a Secure Basis

In another aspect of the Co-Pending Application, retrieval of data stored in database 14 at one or more network-connected devices 10 is provided on a PKI enabled basis.

It should be understood that the steps or functions described below could be combined into a lesser number of steps or functions, or expanded to a greater number of steps or functions, without departing from the scope of the Co-Pending Application.

Generally the retrieval of data on a secure basis in accordance with the Co-Pending Application will involve a Recipient of the data, but also a Sender of the data.

Recipient, on a network-connected device 10, requests web page 18 from the web server 106 by connecting to web server application 16. Web application 16 presents a specific web page 18 responsive to the request from the network-connected device 10. The web page 18 is downloaded to the user through network-connected device 10. As stated earlier, specifically in relation to a network-connected device 10 that is a WAP device, web page 18 is downloaded to the WAP device's browser through the WAP to Web gateway 107 as illustrated in FIG. 6, in a manner that is known. WAP to Web gateway 107 functions as a translator in that it converts wireless device requests to web protocol (HTTP) requests. This translation enables user on the WAP device to access the web page 18 via the wireless network 108, again as illustrated in FIG. 6.

It should be understood, that the Co-Pending Application also contemplates PKI enabled data communications with other users associated with other network connected devices 10. One or more of these other network-connected devices 10 may be a typical personal computer having a known web browser, and connected to the Internet 12 in a manner that is known, as also illustrated in FIG. 6.

The Co-Pending Application contemplates that secure data from web server 106 will come in numerous different forms, depending on the precise nature of the implementation of the Co-Pending Application. Each such particular form will also generally be identified by a "SUBJECT" or equivalent, depending on the use of the data received at the particular network-connected device 10.

In one particular embodiment of the web page 18 containing secure data, the web page 18 also comprises mark-up language representing the output, and instructions for cryptographic utility 24 to conduct certain specific cryptographic operations in relation to

the web page 18, as described below. One aspect of a particular embodiment of the Co-Pending Application is that certain of these instructions, and resultant cryptographic operations, may apply to specific data included in web page 18.

Once the web page 18 is loaded to browser 20, the cryptographic utility 24 is engaged such that cryptographic functions described below are processed.

Cryptographic utility 24 gathers from the memory 28 certain cryptographic operation parameters corresponding to the "SUBJECT" of the particular web page 18, including common name, distinguished name, email address or other information of User and/or Recipient; cryptographic mode, and the specific web mark up tags to operate on, thereby identifying specific data in the web page 18 for cryptographic processing.

Cryptographic utility 24 contacts Certificate Authority 103 via the communication facility (not shown) provided by network-connected device 10 to obtain the PKI enabled data included in web page 18.

As mentioned earlier, Certificate Authority 103 operates a Directory 105 that is connected to the Internet. Cryptographic utility 24 retrieves certificates for the Sender and the Recipient from the Directory 105 in a manner that is known.

Cryptographic utility 24 also interfaces with a known Certificate Revocation List 34, also associated with the Certificate Authority 103, to retrieve the Certificate Revocation List 34.

Cryptographic utility 24 then authenticates the Recipient for PKI transaction, and in preparation for use of the Recipient's private key for decryption.

The cryptographic utility 24 then validates the Recipient's certificate, checks for expiration, checks for revocation, and also obtains key usage data to permit use of the Recipient's certificate to conduct a PKI process. The cryptographic utility 24 also validates the certificate of the Sender, and the integrity of the Sender's public key and appropriate usage of such public key to permit the PKI operations referenced below. All of this is provided in a manner that is known.

Cryptographic utility 24 then conducts a series of cryptographic operations which generally include decryption of data, and digital signature verification. It should be understood that in the Co-Pending Application, cryptographic utility 24 is adapted to perform specific cryptographic operations in relation to specific batches of data included in the web page 18 marked for processing in the mark-up language included in the web page 18. In this manner, each specified data element could be decoded in PKCS#7 format, or using some other custom data format involving decryption and/or signature verification. Also, cryptographic utility 24 permits cipher-text in the web page 18 to be selectively decoded and displayed in clear text.

It should be understood that the data in relation to which the cryptographic operations referenced above are conducted may include all forms of data, including for example images such as gifs or jpgs. Therefore, another aspect of the Co-Pending Application is, a system, computer product and method for decrypting and displaying images, including at a wireless device.

This permits fields with sensitive data, for example, to be retrieved on an encrypted and/or digitally signed basis, while other fields with less sensitive data may remain unencrypted and unsigned. This conserves bandwidth, as well as memory resources wherever the data included in the web form 26 may be received. This also encourages flexibility in data management procedures such that less sensitive data can be mined, while sensitive data is stored on a secure basis.

When considered together, FIGS. 8 to 11 illustrate that the basic architecture of the system of the Co-Pending Application is designed to promote interoperability between wireless and web based wired devices. Therefore the Co-Pending Application permits PKI enabled data to be transmitted and received from one wireless device to another, from a wireless device to a wired web device, and conversely from a wired web device to a wireless device.

As illustrated in Fig. **1**, one embodiment of the system of the present invention also includes a known email server **306**. The email server **306** sends and receives emails in a manner that is well known. The email server **306** is provided by known hardware and

software utilities. Also as illustrated in Fig. **1**, one embodiment of the system of the present invention includes an email protocol translator **308**. The email protocol translator **308** is a known utility which permits the web server **106** and the email server **306** to communicate by translating messages sent by the web server **106** to the particular email protocol understood by the email server **306** such as for example POP3 or IMAP4.

Creating and Delivering an S/MIME Compliant Email Message to an Email Server

Fig. **3** illustrates the creation and delivery of an S/MIME compliant email message to an email server in accordance with an embodiment of the present invention.

A user associated with a network-connected device **10** who desires to create and send an email on a secure basis (the "Sender") requests a page on the web server **106** using the browser **20** loaded on the network-connected device **10**.

The web server **106**, and specifically in co-operation with the web application **16** loaded on the web server **106**, responds to the network-connected device **10** by presenting a web page that is a web form requesting that the user associated with the network-device **10** provide authentication in order to gain access to the web application **16**, and specifically a web email application (not shown) that is included in the web application **16**.

The Sender supplies information in the authentication form fields (such as username and password) on the web page and concludes with submitting the form, typically by pressing a 'SUBMIT' button or equivalent.

The authentication credentials are passed to the web server **106**. The web server **106** in turn delivers the authentication credentials to the email server **306** via the email protocol translator **308**.

Specifically in accordance with the embodiment of the present invention whereby the roaming key server **310** is used to access the User Certificate and Private Key Store **302**, the web server **106** also transfers the user credentials to the roaming key server **310**.

The email server **306** authenticates the Sender and then passes back, through the email protocol translator **308**, message waiting lists and other pertinent information about the Sender's email account to the web server **106** for transmission display in the Sender's browser **20** and establishes an email session typically using a cookie, in a manner that is known.

Again, in accordance with the embodiment of the present invention utilizing the roaming key server **310**, the roaming key server **310** authenticates the Sender and transmits the Sender's private key and certificate through the web server **106** to the S/MIME browser extension **304**. In accordance with the embodiment of the present invention whereby the User Certificate and Private Key Store resides on the network-connected device **10**, the private key and certificate is accessed by the S/MIME browser extension **304**.

The Sender prepares an email message by completing the appropriate fields of the web form referred to, including for example the message subject, body and intended recipients fields. In one particular embodiment of the present invention, the application **22** also provides the recipients passwords.

The Certificate Authority **312** is contacted whereby the recipient's public keys and certificates are verified and retrieved from the associated directory **314**.

The message form data is passed to the application **22**, including the S/MIME browser extension **304**, for signing and encrypting the message and any attachments using the private key of the Sender and the public key of the recipients, and also so as to form an S/MIME compliant email message.

The message is returned to the browser **20** and sent from the browser **20** to the web server **106**, and using the email protocol translator **308** to the email server **306** for forwarding to the identified recipients.

Retrieving and Deciphering an S/MIME compliant email message from an email server

Fig. **2** illustrates the receipt, verification, decryption and display of an S/MIME compliant message from an email server in accordance with an embodiment of the present invention.

A user associated with a network-connected device **10** who desires to display a secure S/MIME compliant that they have received on a secure basis (the "Recipient") requests a page on the web server **106** using the browser **20** loaded on the network-connected device **10**.

The web server **106**, and specifically in co-operation with the web application **16** loaded on the web server **106**, responds to the network-connected device **10** by presenting a web page that is a web form requesting that the Recipient provide authentication in order to gain access to the web application **16**, and specifically a web email application (not shown) that is included in the web application **16**.

The Recipient supplies information in the authentication form fields (such as username and password) on the web page and concludes with submitting the form, typically by pressing a 'SUBMIT' button or equivalent.

The authentication credentials are passed to the web server **106**. The web server **106** in turn delivers the authentication credentials to the email server **306** via the email protocol translator **308**.

Specifically in accordance with the embodiment of the present invention whereby the roaming key server **310** is used to access the User Certificate and Private Key Store **302**, the web server **106** also transfers the user credentials to the roaming key server **310**.

The email server **306** authenticates the Recipient and then passes back, through the email protocol translator **308**, message waiting lists and other pertinent information about the Recipient's email account to the web server **106** for transmission display in the

Recipient's browser **20** and establishes an email session typically using a cookie, in a manner that is known.

The email server authenticates the Recipient and then passes back, through the email protocol translator **308**, message waiting lists and other pertinent information about the Recipient's email account to the web server **106** for transmission display in the Recipient's browser **20** and establishes an email session typically using a cookie.

Again, in accordance with the embodiment of the present invention utilizing the roaming key server **310**, the roaming key server **310** authenticates the Recipient and transmits the Recipient's private key and certificate through the web server **106** to the S/MIME browser extension **304**. In accordance with the embodiment of the present invention whereby the User Certificate and Private Key Store resides on the network-connected device **10**, the private key and certificate is accessed by the S/MIME browser extension **304**.

The Recipient requests a message to read which request is sent to the web server **106** through the email protocol translator **308** to the email server **306** with the message request.

The email server **306** retrieves the message and transmits the message to the Recipient through the web server **106** using the email protocol translator **308** to the Recipient's browser **20**.

The application **22** authenticates against its User Certificate Private Key Store **302** and thereby the key is released to the S/MIME browser extension **304** component thereof where upon the message signature can be verified and the message decrypted for display in the Recipient's browser **20**. Alternatively, in accordance with the embodiment of the present invention utilizing the roaming key server **310**, the authentication happens against data provided by the roaming key server **310** whereby the message signature can be verified and the message decrypted by the S/MIME browser extension **304**.

In another embodiment of the present invention, the persistent field level encryption disclosed in the Co-Pending Application is used for the purposes of the present invention to maintain the confidentiality of the identities of users (and for example their clients with whom they communicate on a secure basis in accordance with the present invention) and other personal information, by encrypting related data and storing the data in an encrypted form at a database (not shown) associated with the web server **106**.

The embodiment of the system of the present invention is best understood as the overall system including the network connected device **10** and the resources thereof, including the application **22**, and also the web server **106** and the email server **306**, as well as the resources of these as well. The embodiment of the computer product of the present invention is the application **22** on the one hand, but also the web application **16**, on the other. Another embodiment of the present invention includes the remote key server **310**.

The embodiment of the method of the present invention is best understood as a process for exchanging PKI S/MIME messages through a browser, whether a web browser or WAP browser. An embodiment of the method of the present invention should also be understood as a method for integrating wireless devices with Internet secure messaging using S/MIME. Another embodiment of the method of the present invention is a method for delivering private keys and certificates through the Internet or a wireless network. Yet another embodiment of the method of the present invention, is a method for eliminating the "man in the middle" security hole of proxy based gateways between the Internet and wireless networks by providing persistent secure data communication using S/MIME. A still other embodiment of the present invention is a method for allocating data resources as between the web server and a wireless device such that PKI is provided on the wireless device so as to provide S/MIME encryption on a persistent basis.

Embodiments of the present invention also provide for persistent field level encryption using S/MIME on a selective basis throughout an Internet-based data process. This promotes efficient utilization of resources by invoking PKI operations in relation to

specific elements of an Internet-based data process where security/authentication is most needed.

Embodiments of the present invention also provide a set of tools whereby PKI S/MIME capability is added to a browser in an efficient manner.

Embodiments of the present invention should also be understood as a set of tools for complying with legal digital signature requirements, including in association with a wireless device using a web mail system incorporating S/MIME.

A still other embodiment of the present invention is a method for permitting secure email messaging between wireless and Internet based or other networks using S/MIME.

Modifications and variations such as would be apparent to a skilled addressee are deemed to be within the scope of the present invention.

2003257282 29 May 2009

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS

1. A system for exchanging S/MIME compliant email via a communication network, said system comprising:

a network-connected device configured for communication with a remote device via the communication network;

said network-connected device comprising a browser, and said browser comprising an authentication component configured to authenticate one or more credentials associated with a user of said network-connected device, and said browser comprising a component responsive to said user for composing an email message;

said browser comprising an encryption/decryption component configured for PKI transactions, and an S/MIME component linked to said encryption/decryption component and configured for converting said email message into an S/MIME compliant email;

an email server comprising an email server software component that receives, stores and transmits S/MIME compliant email, said email server operatively connected to the communication network for receiving the S/MIME compliant email addressed to said remote device; and

said remote device comprising a browser configured for retrieving the S/MIME compliant email from said email server and comprising an S/MIME component configured for deciphering the S/MIME compliant email at said remote device.

2. The system as claimed in claim 1, further comprising, a key storage component configured for storing a plurality of keys, each of said plurality of keys being associated with a user in a public key infrastructure to encrypt and decrypt data; and

said authentication component being configured for determining whether a prospective user of a key in the plurality of keys is the associated user for the key, and said encryption/decryption component being linked to said key storage component and said authentication component and said encryption/decryption component being responsive to said authentication component for encrypting/decrypting data using said plurality of keys when said authentication component authenticates a user of the network-connected device.

2003257282 29 May 2009

3. The system as claimed in claim 2, wherein said authentication component is configured to communicate with a Certificate Authority to authenticate a prospective user.

4. The system as claimed in claim 3, further comprising a roaming key server configured for authenticating the sender of an S/MIME compliant email and transmitting the sender's private key and certificate to said network-connected device.

5. A computer program product operable on a network-connected device for enabling S/MIME compliant email messages between the network-connected device and remote devices via a communication network, the computer program product comprising:

a browser;

a component for composing an email message;

an encryption/decryption component linked to said browser and configured for performing PKI transactions in the browser; and

an S/MIME component linked to said browser and said encryption/decryption component and configured for converting said email message into an S/MIME compliant email message for exchange with the remote device via an email server comprising an email server software component that receives, stores and transmits S/MIME compliant email, said email server connected to the communication network.

6. The computer program product as claimed in claim 5, further comprising:

a key storage component configured for storing a plurality of keys, each of said keys being associated with a user in a public key infrastructure for encrypting and decrypting data; and

a user authentication component configured for determining whether a prospective user of a key in the plurality of keys is the associated user for the key.

7. A device for creating and exchanging S/MIME compliant email messages via a communication network, said device comprising:

a browser;

a component for composing an email message;

2003257282 29 May 2009

said browser comprising an S/MIME extension component;

said browser comprising an encryption/decryption component, and said encryption/decryption component comprising a key component for obtaining a key associated with said user;

said S/MIME extension component being responsive to said encryption/decryption component for converting said email message into an S/MIME compliant email message based on the key associated with said user; and

a component configured for transferring said S/MIME compliant email message to an email server comprising an email server software component that receives, stores and transmits S/MIME compliant email, said email server operatively coupled to the communication network.

8. The device as claimed in claim 7, further comprising a key storage component configured for storing a plurality of keys, said keys being usable by an associated user in a public key infrastructure to encrypt and decrypt data; a user authentication component for determining whether a prospective user of one of said plurality of keys is the associated user for said key, wherein said encryption/decryption facility is responsive to said user authentication component for encrypting and decrypting an S/MIME message based on the key for said associated user.

9. A system for exchanging S/MIME compliant email via a communication network substantially as hereinbefore described with reference to the accompanying drawings.

10. A computer program product substantially as hereinbefore described with reference to the accompanying drawings.

11. A device for creating and exchanging S/MIME compliant email messages via a communication network substantially as hereinbefore described with reference to the accompanying drawings.

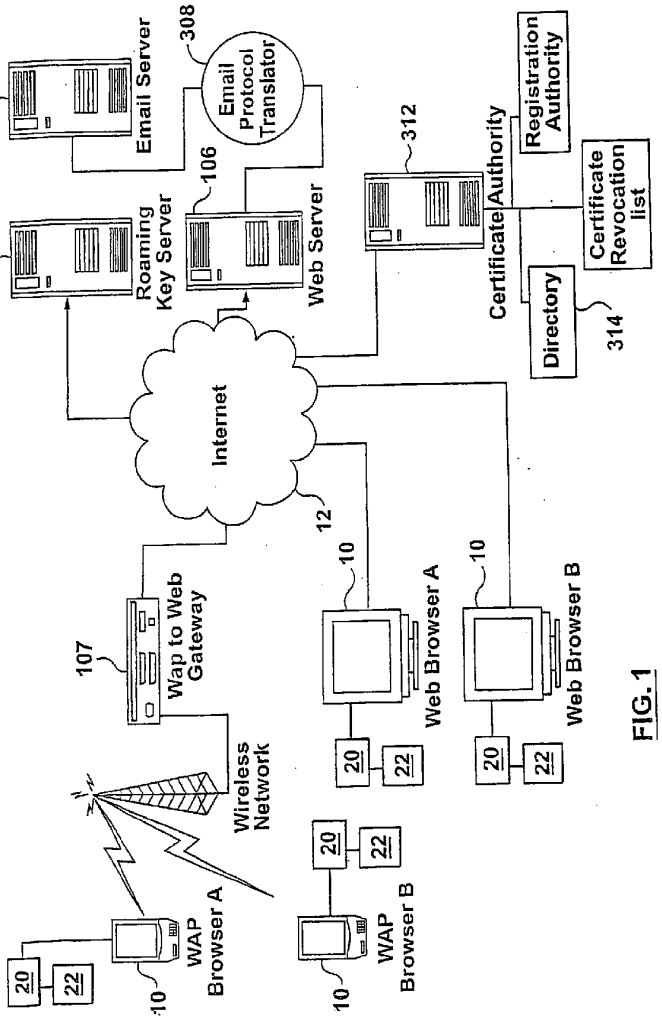

306
Email Server
308
Email Protocol Translator
310
Roaming Key Server
106
Web Server
312
Certificate Authority
Registration Authority
Certificate Revocation list
Directory
314
Internet
12
107
Wap to Web Gateway
Wireless Network
10
Web Browser A
10
Web Browser B
20
22
10
WAP Browser A
20
22
10
WAP Browser B

FIG. 1

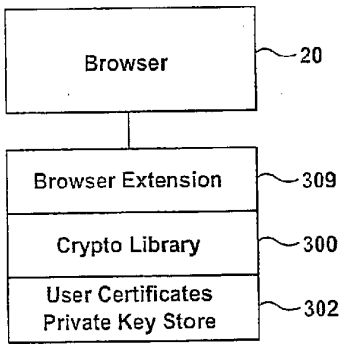

Browser
20
Browser Extension
309
Crypto Library
300
User Certificates
Private Key Store
302

FIG. 1A

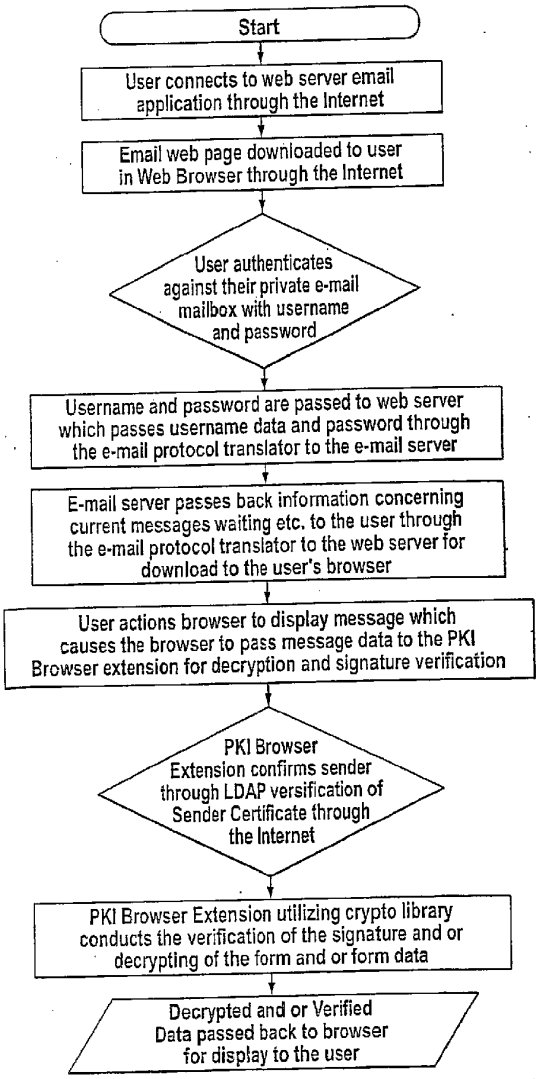

Start
User connects to web server email application through the Internet
Email web page downloaded to user in Web Browser through the Internet
User authenticates against their private e-mail mailbox with username and password
Username and password are passed to web server which passes username data and password through the e-mail protocol translator to the e-mail server
E-mail server passes back information concerning current messages waiting etc. to the user through the e-mail protocol translator to the web server for download to the user's browser
User actions browser to display message which causes the browser to pass message data to the PKI Browser extension for decryption and signature verification
PKI Browser Extension confirms sender through LDAP versification of Sender Certificate through the Internet
PKI Browser Extension utilizing crypto library conducts the verification of the signature and or decrypting of the form and or form data
Decrypted and or Verified Data passed back to browser for display to the user

FIG. 2

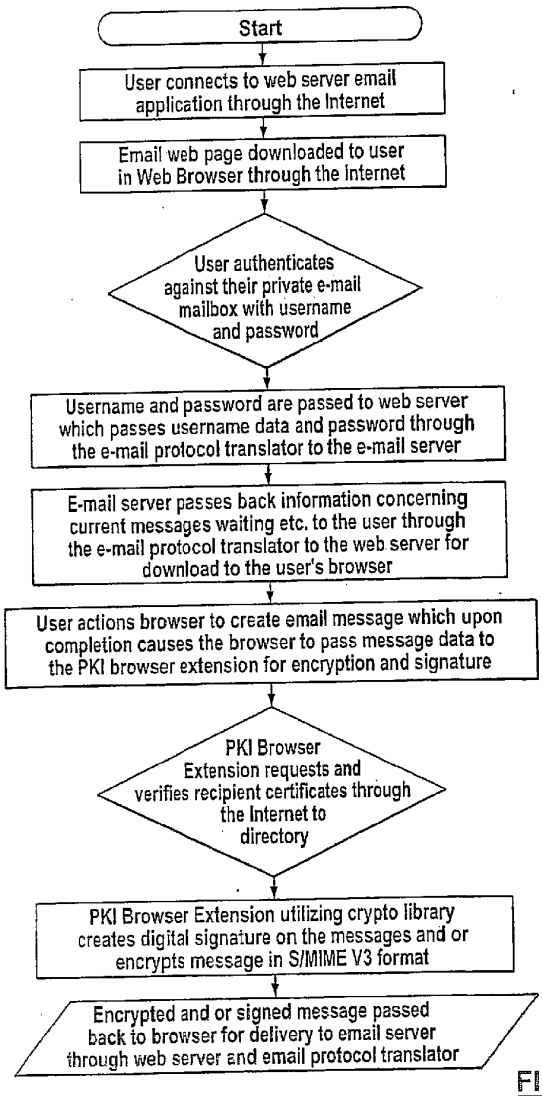

Start
User connects to web server email application through the Internet
Email web page downloaded to user in Web Browser through the Internet
User authenticates against their private e-mail mailbox with username and password
Username and password are passed to web server which passes username data and password through the e-mail protocol translator to the e-mail server
E-mail server passes back information concerning current messages waiting etc. to the user through the e-mail protocol translator to the web server for download to the user's browser
User actions browser to create email message which upon completion causes the browser to pass message data to the PKI browser extension for encryption and signature
PKI Browser Extension requests and verifies recipient certificates through the Internet to directory
PKI Browser Extension utilizing crypto library creates digital signature on the messages and or encrypts message in S/MIME V3 format
Encrypted and or signed message passed back to browser for delivery to email server through web server and email protocol translator

FIG. 3

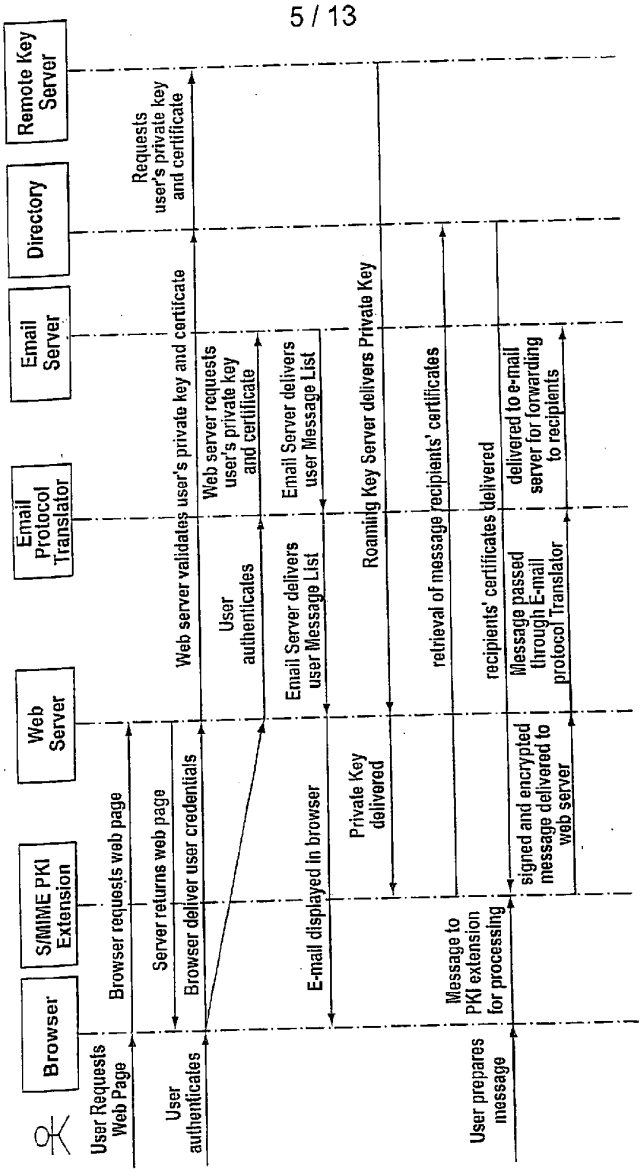

Browser
S/MIME PKI Extension
Web Server
Email Protocol Translator
Email Server
Directory
Remote Key Server
User Requests Web Page
Browser requests web page
Server returns web page
User authenticates
Browser deliver user credentials
Web server validates user's private key and certificate
Web server requests user's private key and certificate
Requests user's private key and certificate
User authenticates
Email Server delivers user Message List
Email Server delivers user Message List
E-mail displayed in browser
Private Key delivered
Roaming Key Server delivers Private Key
retrieval of message recipients' certificates
Message to PKI extension for processing
recipients' certificates delivered
User prepares message
signed and encrypted message delivered to web server
Message passed through E-mail protocol Translator
delivered to e-mail server for forwarding to recipients

FIG. 4

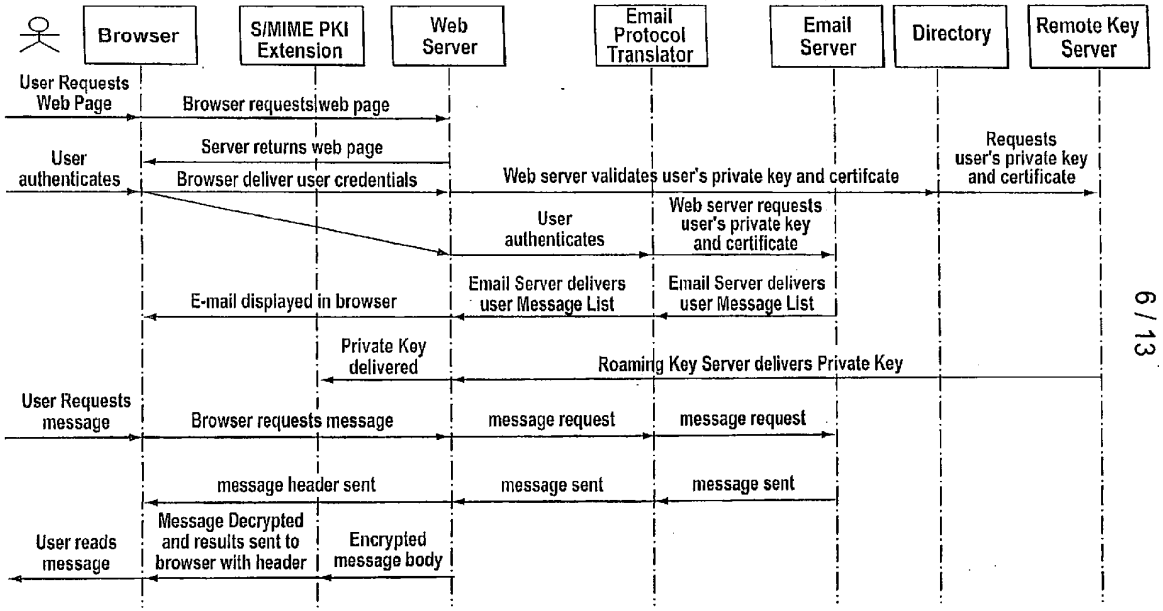

Browser
S/MIME PKI Extension
Web Server
Email Protocol Translator
Email Server
Directory
Remote Key Server
User Requests Web Page
Browser requests web page
Server returns web page
User authenticates
Browser deliver user credentials
Web server validates user's private key and certifcate
Requests user's private key and certificate
User authenticates
Web server requests user's private key and certificate
Email Server delivers user Message List
Email Server delivers user Message List
E-mail displayed in browser
Private Key delivered
Roaming Key Server delivers Private Key
User Requests message
Browser requests message
message request
message request
message header sent
message sent
message sent
User reads message
Message Decrypted and results sent to browser with header
Encrypted message body

FIG. 5

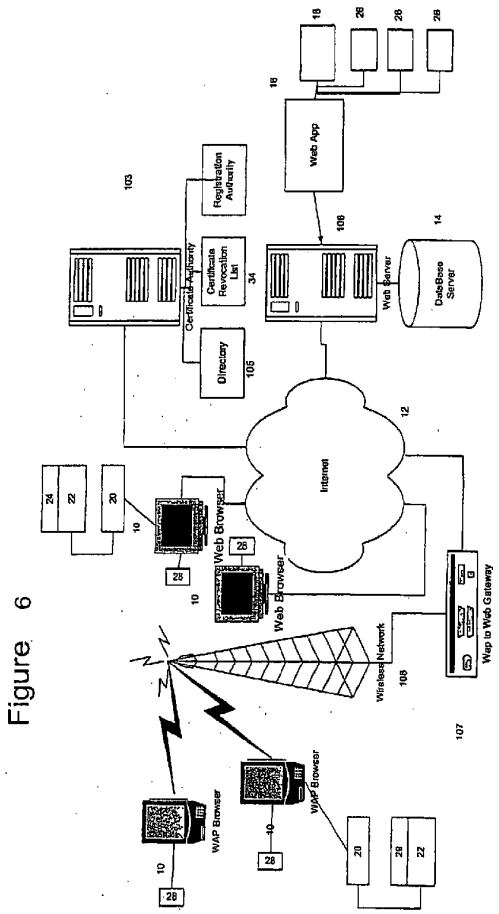
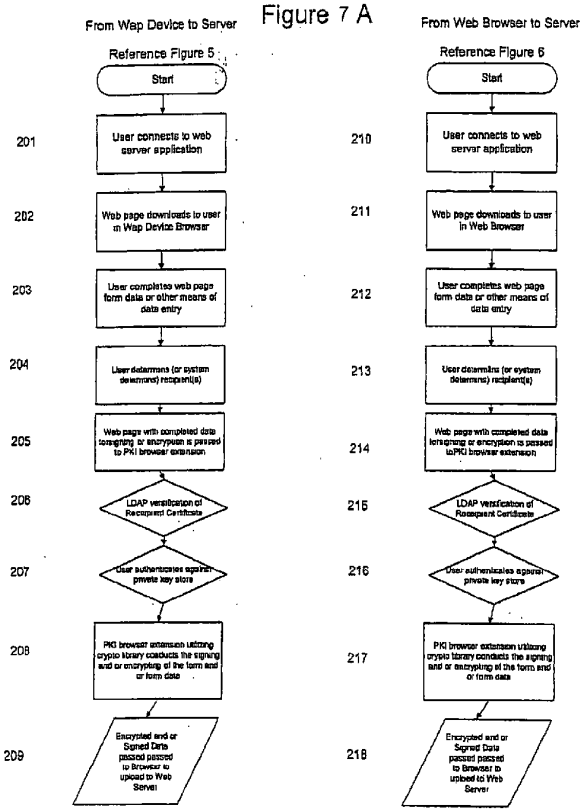

Web App
Registration Authority
Certificate Revocation List
Certificate Authority
Directory
Web Server
DataBase Server
Internet
Web Browser
Web Browser
WAP Browser
WAP Browser
Wireless Network
Wap to Web Gateway

Figure 6

2003257282 04 May 2009

Figure 7 A



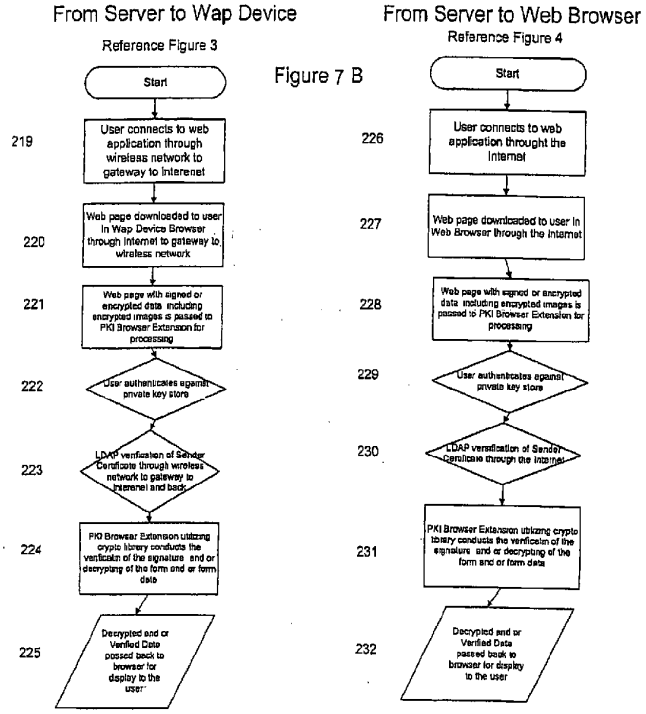

From Server to Wap Device
Reference Figure 3
From Server to Web Browser
Reference Figure 4
Start
219
User connects to web application through wireless network to gateway to Interenet
220
Web page downloaded to user in Wap Device Browser through Internet to gateway to wireless network
221
Web page with signed or encrypted data including encrypted images is passed to PKI Browser Extension for processing
222
User authenticates against private key store
223
LDAP verification of Sender Certificate through wireless network to gateway to Internet and back
224
PKI Browser Extension utilizing crypto library conducts the verification of the signature and or decrypting of the form and or form data
225
Decrypted and or Verified Data passed back to browser for display to the user
Start
226
User connects to web application throught the Internet
227
Web page downloaded to user in Web Browser through the Internet
228
Web page with signed or encrypted data including encrypted images is passed to PKI Browser Extension for processing
229
User authenticates against private key store
230
LDAP verification of Sender Certificate through the Internet
231
PKI Browser Extension utilizing crypto library conducts the verification of the signature and or decrypting of the form and or form data
232
Decrypted and or Verified Data passed back to browser for display to the user

Figure 7 B

Figure 8

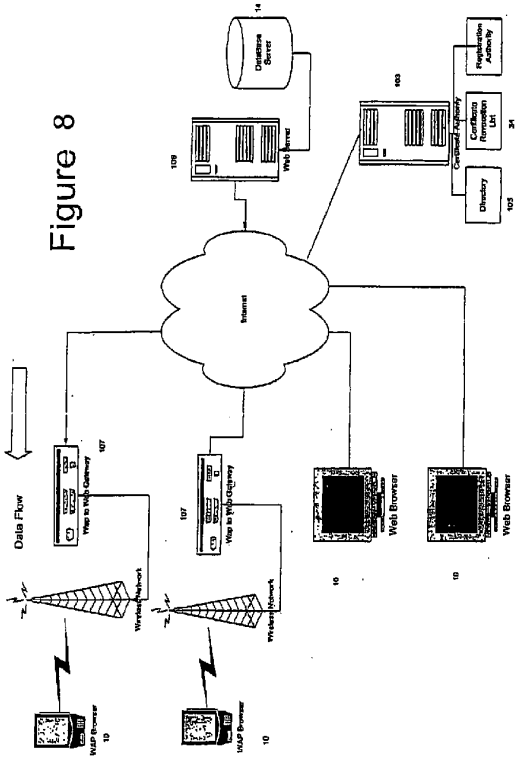


Figure 9

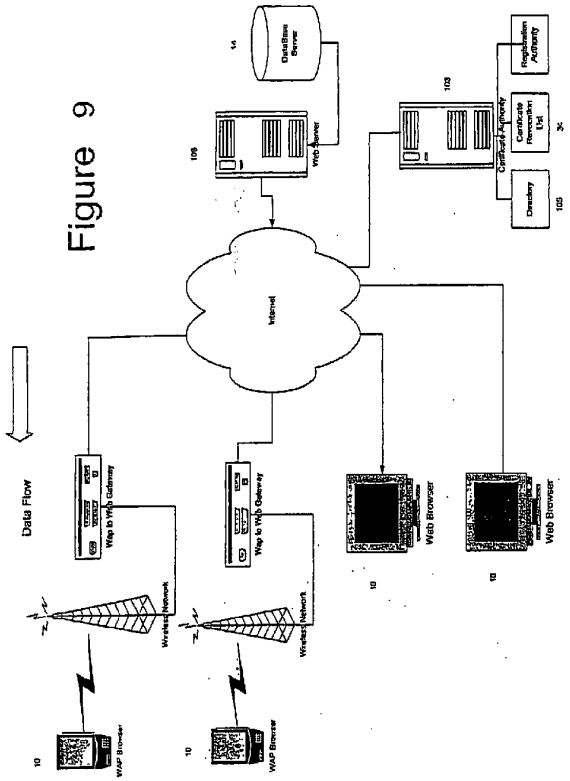


Figure 10

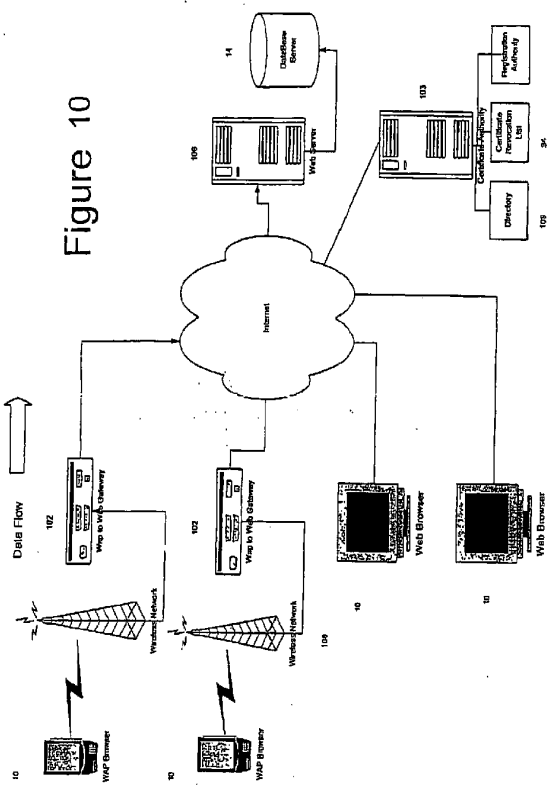
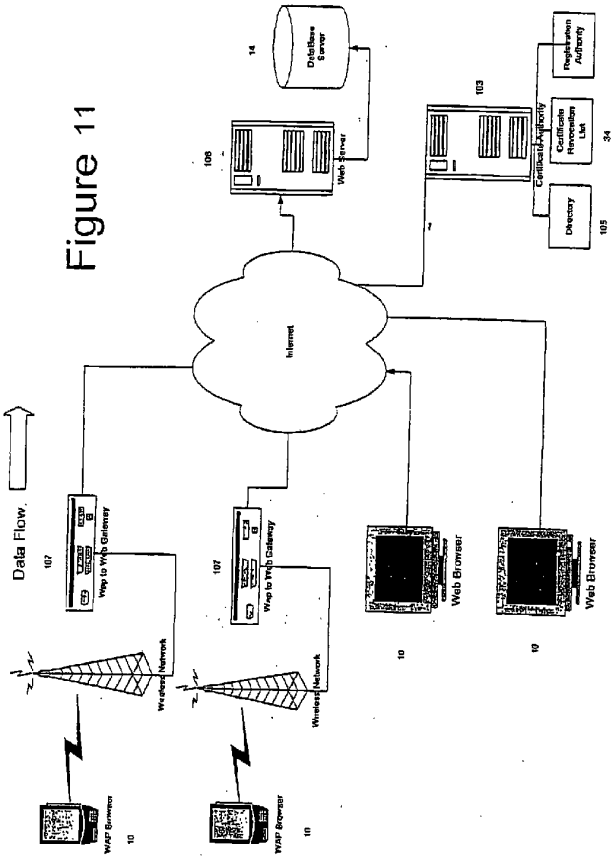

Data Flow
Internet
Web Server
Database Server
Registration Authority
Certificate Revocation List
Directory
Certificate Authority
Wap to Web Gateway
Wap to Web Gateway
Wireless Network
Wireless Network
WAP Browser
WAP Browser
Web Browser
Web Browser

Figure 11


Data Flow
Internet
Web Server
Database Server
Certificate Authority
Registration Authority
Certificate Revocation List
Directory
Wap to Web Gateway
Wireless Network
WAP Browser
Web Browser