US 20030014629A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0014629 A1

Zuccherato (43) Pub. Date: Jan. 16, 2003

(54) ROOT CERTIFICATE MANAGEMENT SYSTEM AND METHOD

(76) Inventor: Robert J. Zuccherato, Stittsville (CA)

Correspondence Address:
VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601 (US)

(21) Appl. No.: 09/906,504

(22) Filed: Jul. 16, 2001

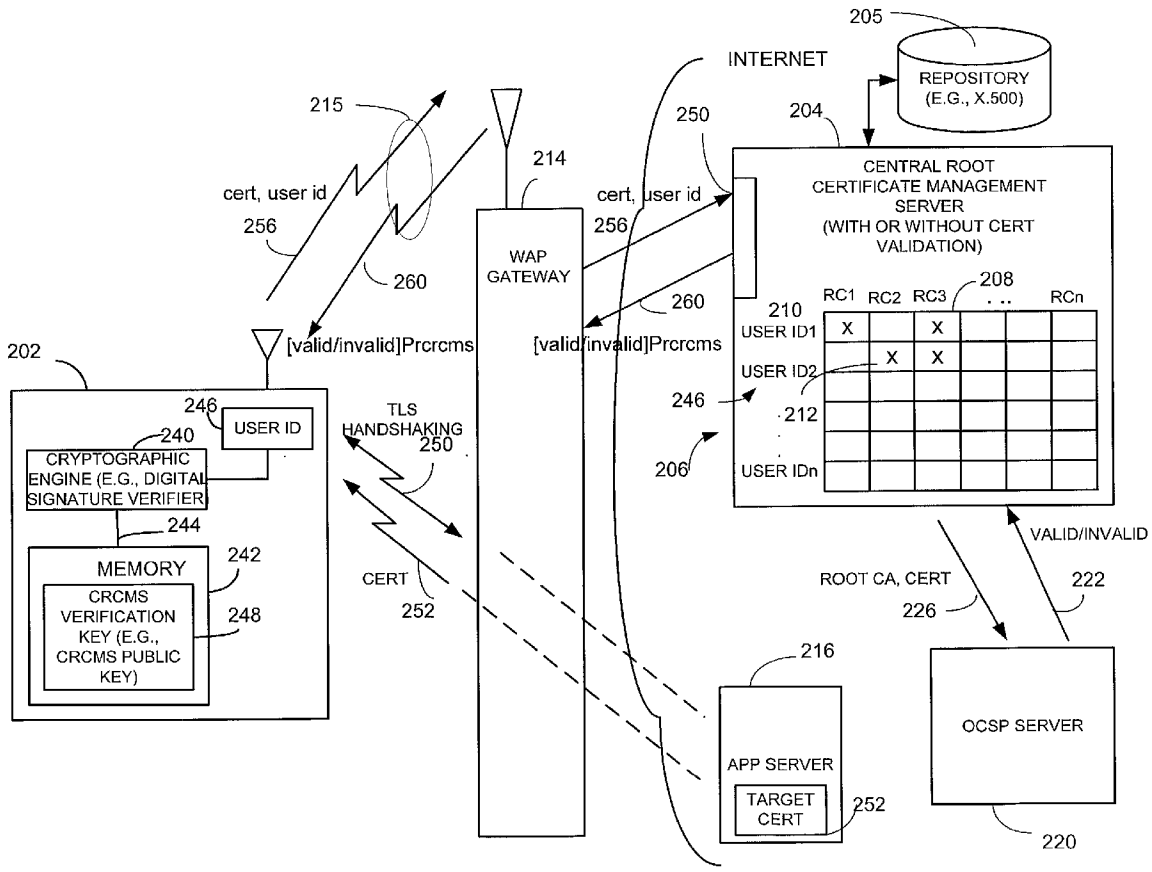
Publication Classification

(51) Int. Cl.[7] G06F 7/00

(52) U.S. Cl. 713/156

(57) ABSTRACT

A method and system for validating a certificate maintains a multi-subscriber root certificate store, containing subscriber identification data for a plurality of subscribers along with data representing a plurality of root certificates, such as an index to root certificates or the root certificates themselves, associated with each of the plurality of subscribers. In one example, a table is stored containing specified root CA certificates for a plurality of subscribers in a network such as stored by a network element in a wireless radiotelephone network, or any other suitable wireless network. Subscriber units do not have a root CA store that contains pre-stored root CA certificates. Accordingly, memory is saved in the subscriber units. In addition, a separate server that stores the multi-subscribers root certificate store preferably carries out certificate path validation on behalf of the mobile units so that the wireless mobile unit need not carry out certificate path construction. Instead, a wireless mobile unit simply sends a certificate to be validated along with its subscriber ID data identifying the mobile unit or application to the multi-subscriber root certificate store server and waits for a "yes" or "no" answer from the server to determine whether the certificate is valid.



IPR2025-01572
Apple EX1007 Page 1

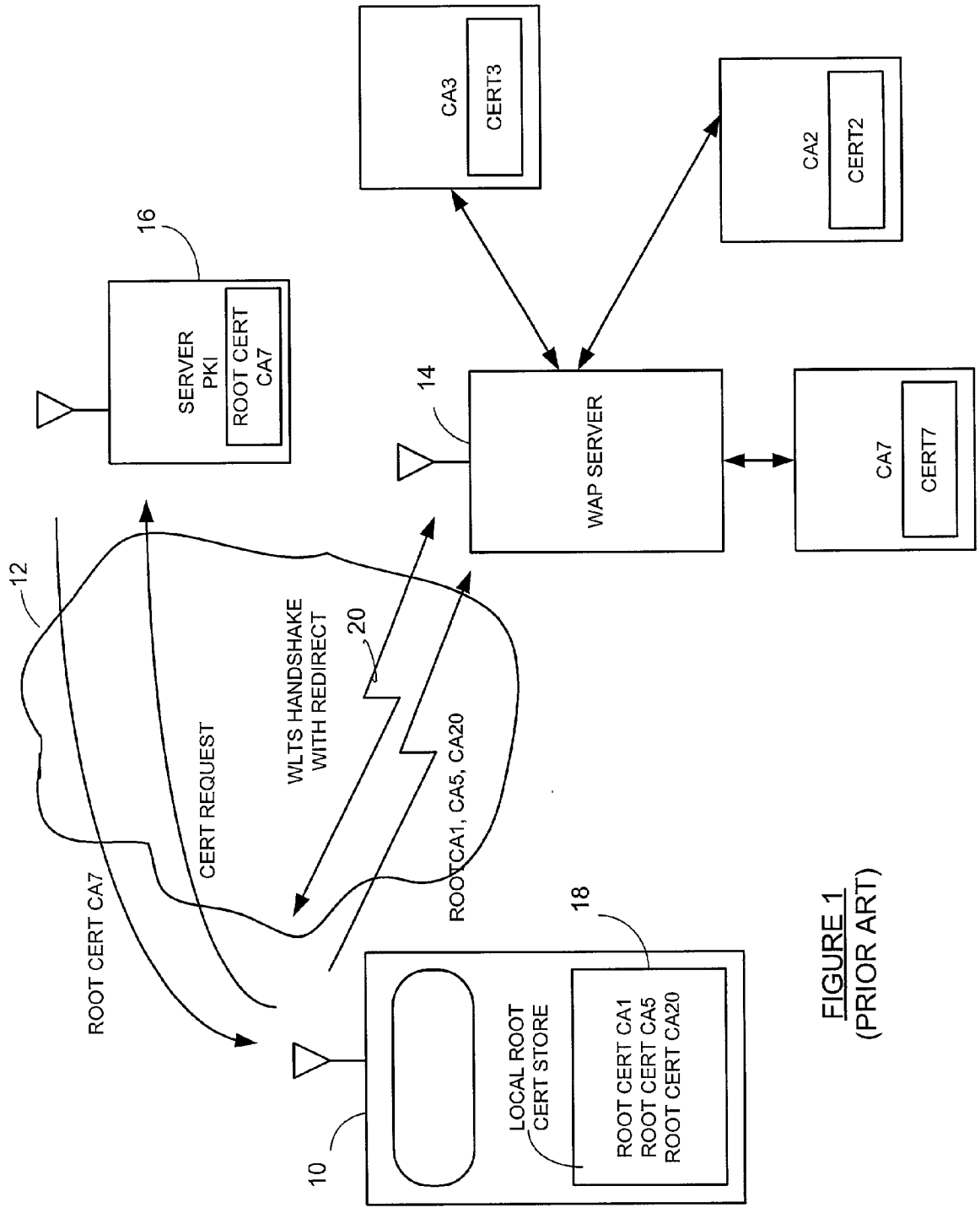


FIGURE 1
(PRIOR ART)

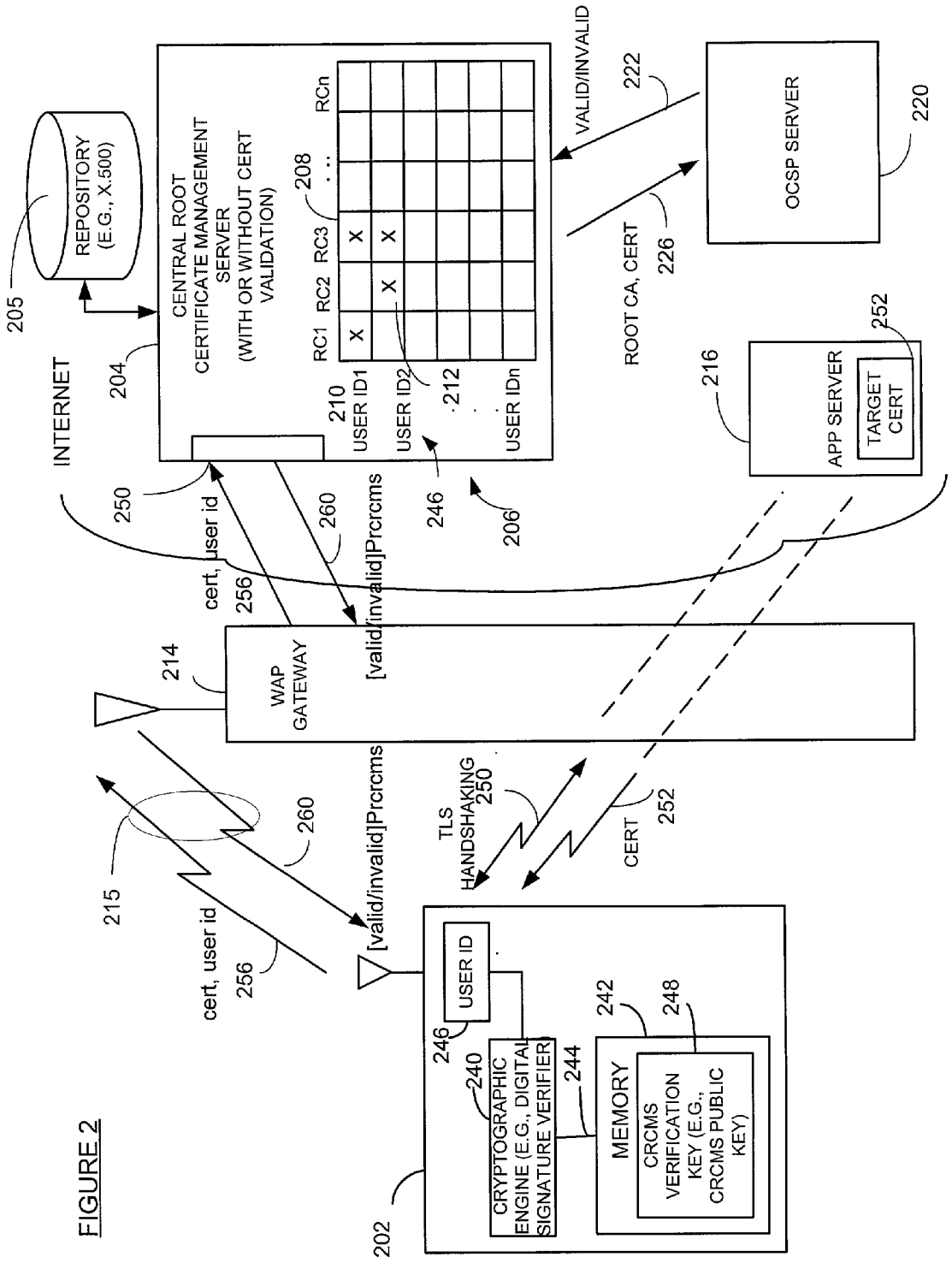

REPOSITORY (E.G., X.500)
205
INTERNET
204
CENTRAL ROOT CERTIFICATE MANAGEMENT SERVER (WITH OR WITHOUT CERT VALIDATION)
208
RC1 RC2 RC3 RCn
USER ID1
USER ID2
USER IDn
210
212
206
246
250
260
cert, user id
256
[valid/invalid]Prcrcms
VALID/INVALID
222
OCSP SERVER
220
ROOT CA, CERT
226
216
APP SERVER
TARGET CERT
252
WAP GATEWAY
214
TLS HANDSHAKING
CERT
215
USER ID
CRYPTOGRAPHIC ENGINE (E.G., DIGITAL SIGNATURE VERIFIER)
240
244
MEMORY
242
248
CRCMS VERIFICATION KEY (E.G., CRCMS PUBLIC KEY)
202

FIGURE 2

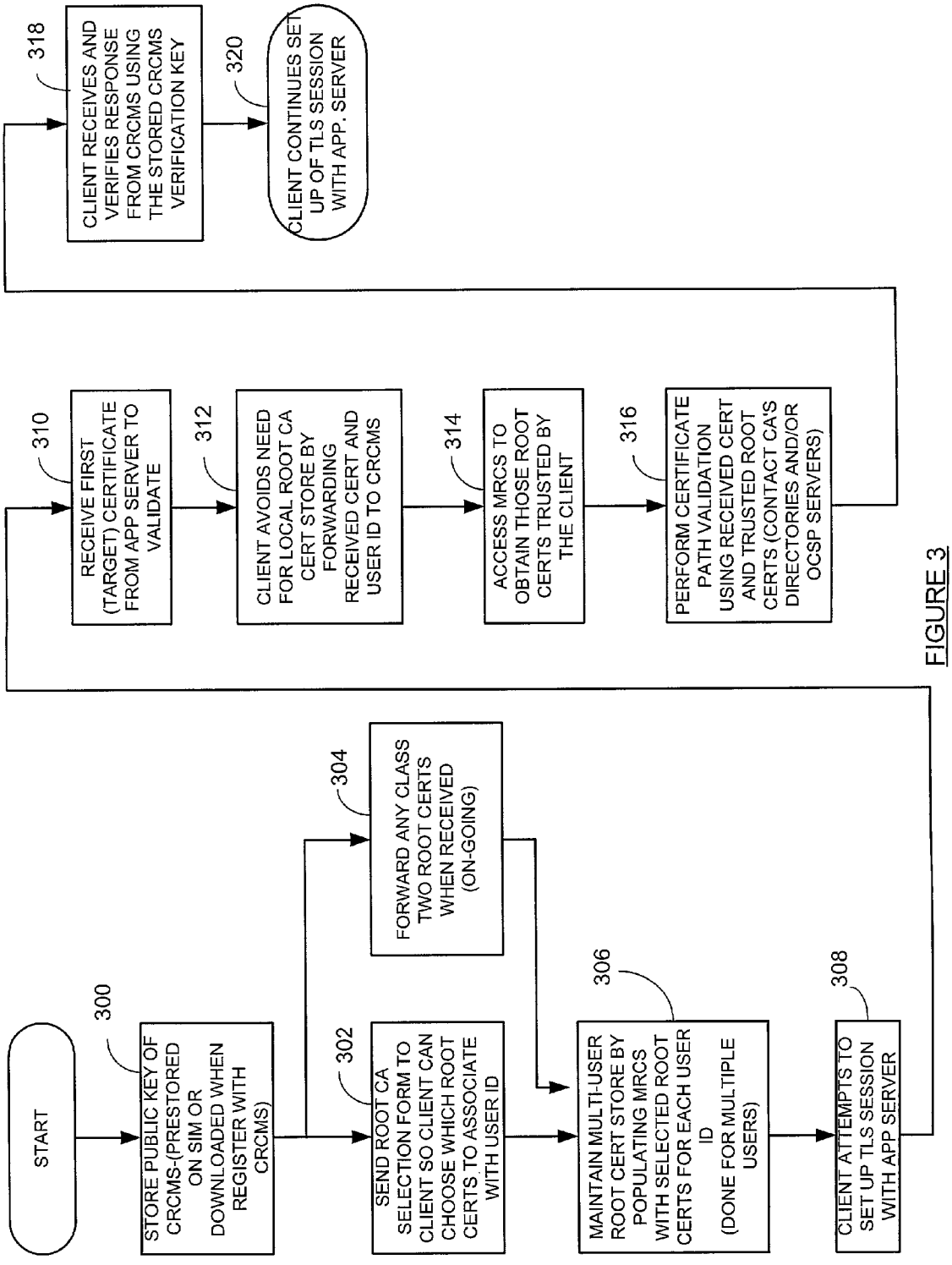

START
300
STORE PUBLIC KEY OF CRCMS-(PRESTORED ON SIM OR DOWNLOADED WHEN REGISTER WITH CRCMS)
302
SEND ROOT CA SELECTION FORM TO CLIENT SO CLIENT CAN CHOOSE WHICH ROOT CERTS TO ASSOCIATE WITH USER ID
304
FORWARD ANY CLASS TWO ROOT CERTS WHEN RECEIVED (ON-GOING)
306
MAINTAIN MULTI-USER ROOT CERT STORE BY POPULATING MRCS WITH SELECTED ROOT CERTS FOR EACH USER ID (DONE FOR MULTIPLE USERS)
308
CLIENT ATTEMPTS TO SET UP TLS SESSION WITH APP SERVER
310
RECEIVE FIRST (TARGET) CERTIFICATE FROM APP SERVER TO VALIDATE
312
CLIENT AVOIDS NEED FOR LOCAL ROOT CA CERT STORE BY FORWARDING RECEIVED CERT AND USER ID TO CRCMS
314
ACCESS MRCS TO OBTAIN THOSE ROOT CERTS TRUSTED BY THE CLIENT
316
PERFORM CERTIFICATE PATH VALIDATION USING RECEIVED CERT AND TRUSTED ROOT CERTS (CONTACT CA'S DIRECTORIES AND/OR OCSP SERVERS)
318
CLIENT RECEIVES AND VERIFIES RESPONSE FROM CRCMS USING THE STORED CRCMS VERIFICATION KEY
320
CLIENT CONTINUES SET UP OF TLS SESSION WITH APP. SERVER

FIGURE 3

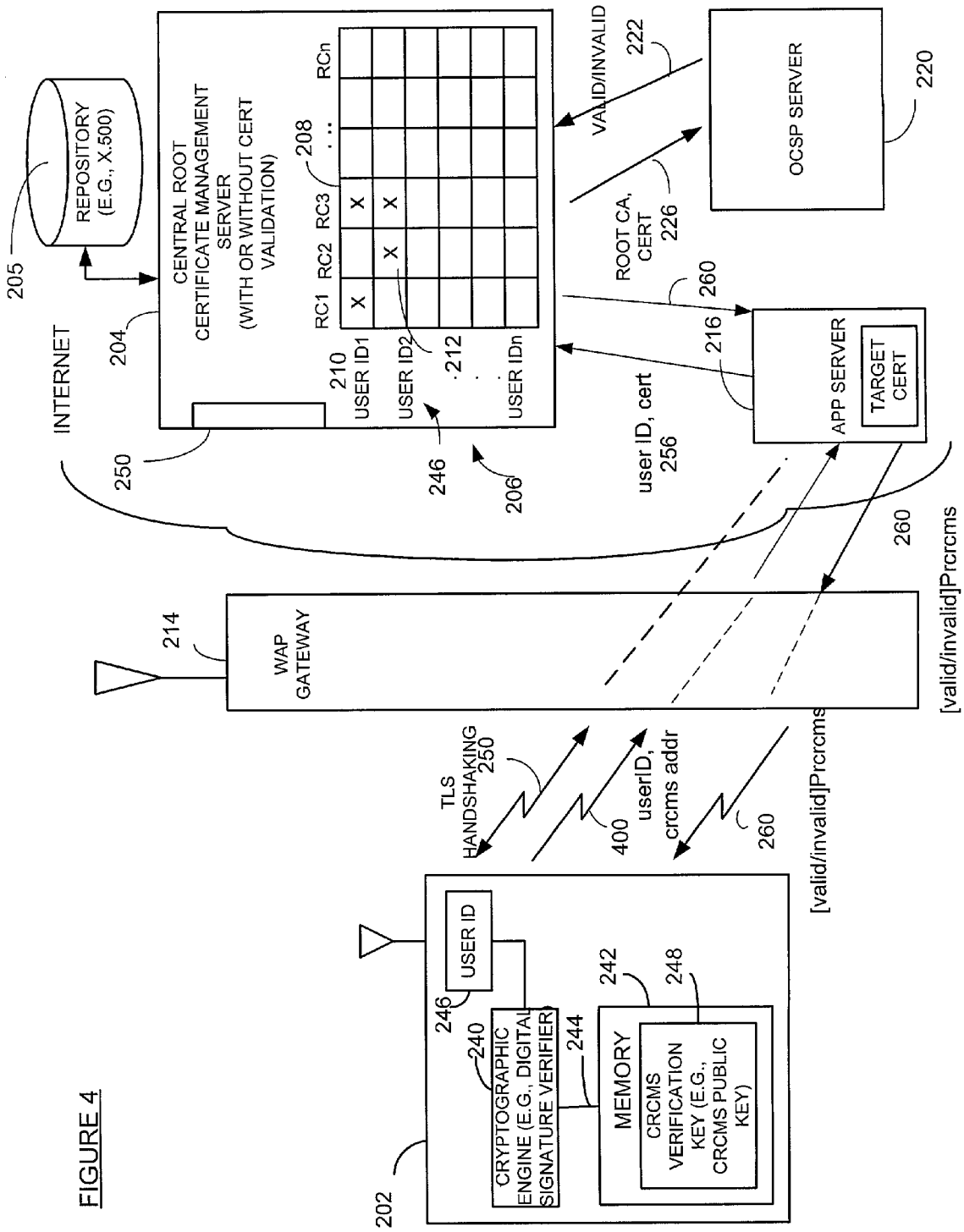

REPOSITORY (E.G., X.500)
205
CENTRAL ROOT CERTIFICATE MANAGEMENT SERVER (WITH OR WITHOUT CERT VALIDATION)
204
INTERNET
250
RC1 RC2 RC3 ... RCn
208
USER ID1
USER ID2
USER IDn
210
212
246
206
VALID/INVALID
222
OCSP SERVER
220
ROOT CA, CERT
226
260
216
APP SERVER
TARGET CERT
user ID, cert
256
WAP GATEWAY
214
TLS HANDSHAKING
250
400
userID, crcms addr
260
[valid/invalid]Prcrcms
[valid/invalid]Prcrcms
USER ID
246
240
CRYPTOGRAPHIC ENGINE (E.G., DIGITAL SIGNATURE VERIFIER)
244
MEMORY
242
248
CRCMS VERIFICATION KEY (E.G., CRCMS PUBLIC KEY)
202

FIGURE 4

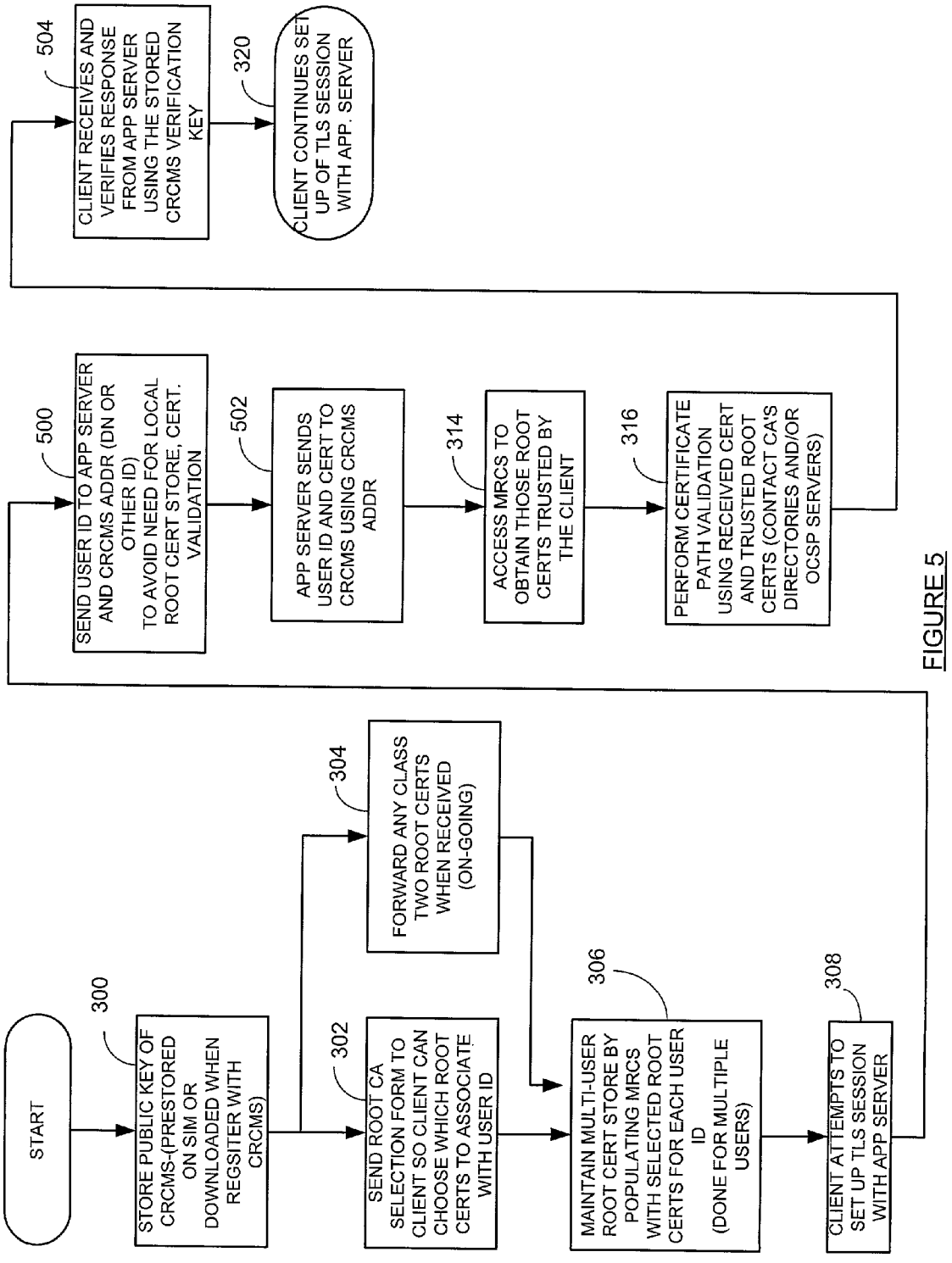
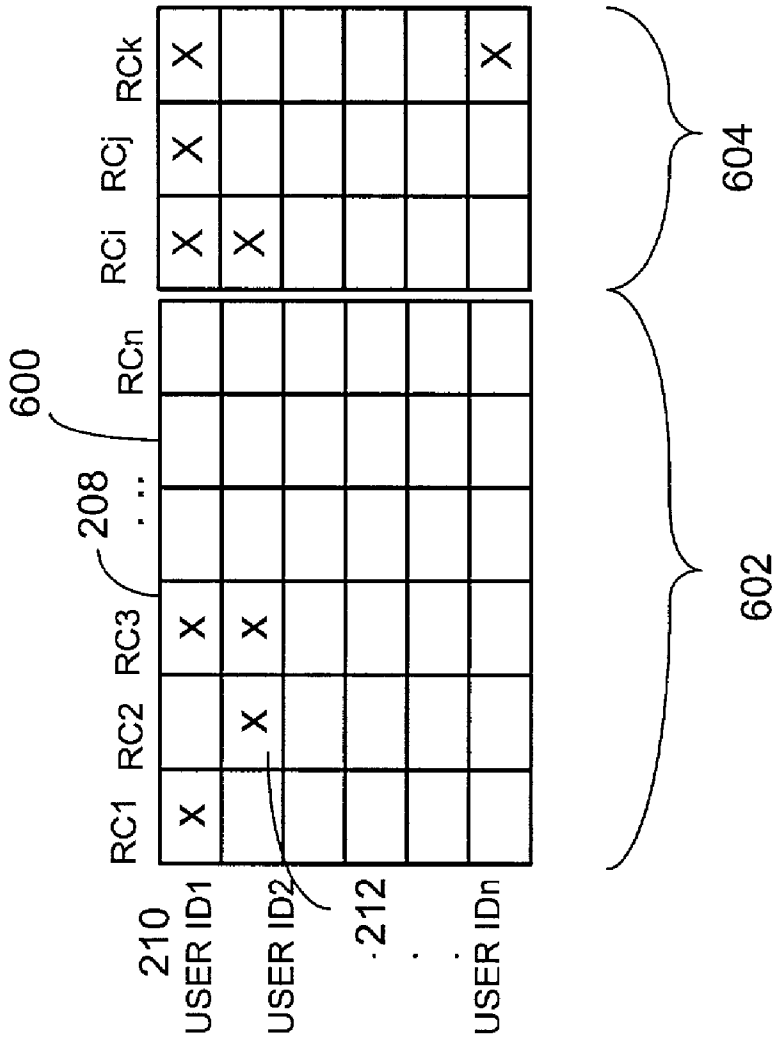

START
300
STORE PUBLIC KEY OF CRCMS-(PRESTORED ON SIM OR DOWNLOADED WHEN REGSITER WITH CRCMS)
302
SEND ROOT CA SELECTION FORM TO CLIENT SO CLIENT CAN CHOOSE WHICH ROOT CERTS TO ASSOCIATE WITH USER ID
304
FORWARD ANY CLASS TWO ROOT CERTS WHEN RECEIVED (ON-GOING)
306
MAINTAIN MULTI-USER ROOT CERT STORE BY POPULATING MRCS WITH SELECTED ROOT CERTS FOR EACH USER ID (DONE FOR MULTIPLE USERS)
308
CLIENT ATTEMPTS TO SET UP TLS SESSION WITH APP SERVER
500
SEND USER ID TO APP SERVER AND CRCMS ADDR (DN OR OTHER ID) TO AVOID NEED FOR LOCAL ROOT CERT STORE, CERT. VALIDATION
502
APP SERVER SENDS USER ID AND CERT TO CRCMS USING CRCMS ADDR
314
ACCESS MRCS TO OBTAIN THOSE ROOT CERTS TRUSTED BY THE CLIENT
316
PERFORM CERTIFICATE PATH VALIDATION USING RECEIVED CERT AND TRUSTED ROOT CERTS (CONTACT CA'S DIRECTORIES AND/OR OCSP SERVERS)
504
CLIENT RECEIVES AND VERIFIES RESPONSE FROM APP SERVER USING THE STORED CRCMS VERIFICATION KEY
320
CLIENT CONTINUES SET UP OF TLS SESSION WITH APP. SERVER

FIGURE 5

FIGURE 6


600
208
210
212
RC1
RC2
RC3
RCn
RCi
RCj
RCk
USER ID1
USER ID2
USER IDn
602
604

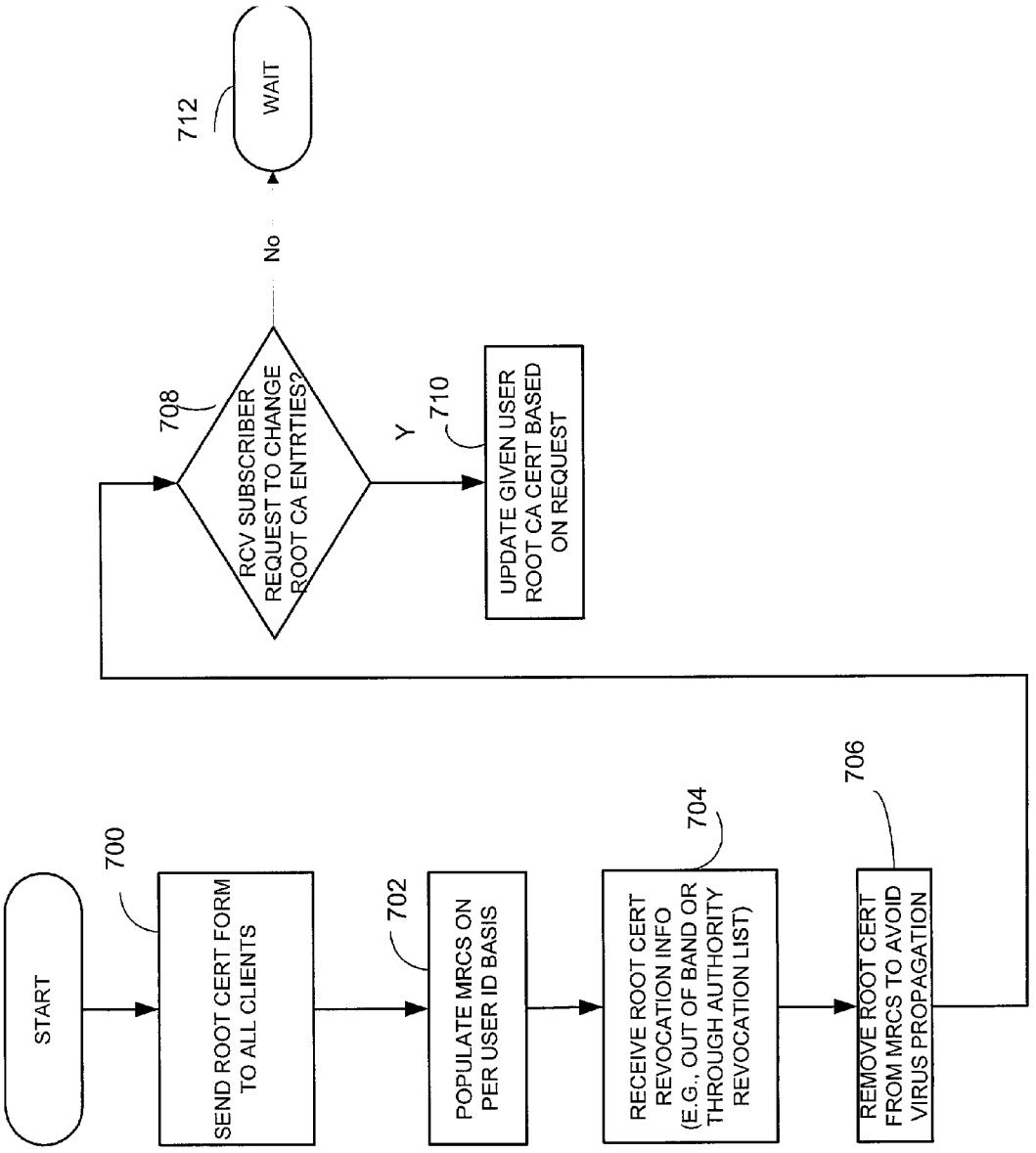

START
700
SEND ROOT CERT FORM TO ALL CLIENTS
702
POPULATE MRCS ON PER USER ID BASIS
704
RECEIVE ROOT CERT REVOCATION INFO (E.G., OUT OF BAND OR THROUGH AUTHORITY REVOCATION LIST)
706
REMOVE ROOT CERT FROM MRCS TO AVOID VIRUS PROPAGATION
708
RCV SUBSCRIBER REQUEST TO CHANGE ROOT CA ENTRTIES?
Y
710
UPDATE GIVEN USER ROOT CA CERT BASED ON REQUEST
No
712
WAIT

FIGURE 7

ROOT CERTIFICATE MANAGEMENT SYSTEM AND METHOD

FIELD OF THE INVENTION

[0001] The invention relates generally to information security systems employing cryptographic techniques, and more particularly to wireless information security systems that employ certificates.

BACKGROUND OF THE INVENTION

[0002] In typical public key cryptography systems, digital signature key pairs, having a private key and public key, are often used to authenticate a digital signature of a client using a software application in order to confirm the identity of the sender of the message. The software application executes on a processor, sometimes referred to as a cryptographic engine. A subscriber may generally be, for example, a network computer mode, an Internet appliance, wireless radiotelephone, a software application or a subscriber in the information security system. In addition to digital signature key pairs, encryption key pairs are also generally used to encrypt data being sent from one subscriber to another subscriber within the computer network or within a wireless network. Certificates are typically generated by a trusted certification authority for the public keys of the private/public key pair to certify that the keys are genuinely owned by a named subscriber. Standards, such as ISO 9594-8, available from the International Organization Standardization, define typical certificate content.

[0003] Certification authorities (CA), sometimes referred to as certificate issuing units, issue certificates for subscribers. Root certificates are those certificates issued by a root certification authority to itself. Thus, a root certificate is verified using the public key contained within it. Since any entity with access to any private/public key pair can produce such a root certificate, a legitimate root certificate must be protected for integrity and authenticity by another external mechanism. In conventional desktop devices, such as desktop computers and laptop computers, Web browsers have a long pre-stored list of trusted root certificates that have been issued by differing certification authorities. Accordingly, a local root certification authority certificate store is maintained by such conventional devices. The root CA certificates are typically used by the desktop device or other unit to validate certificates that accompany encrypted information or digitally signed information, such as with electronic transactions via the Internet. The stored long list of trusted root certificates allows a device to potentially trust a number of certificates from differing certification authorities allowing the Web browser to potentially transact business with subscribers in different trust domains. However, a problem arises with wireless mobile devices that have a limited amount of memory, battery life and limited processing capabilities. The limited amount of memory makes it difficult to store a long list of trusted root certificates, and a limited battery life and processing capabilities can reduce the processing capabilities to make it difficult for a wireless device to carry out conventional certificate validation operations.

[0004] For example, typically, a certificate verification module within a device attempts to find a sequence of certificates corresponding to a certification path starting with the trusted certification authority whose public key the subscriber trusts a priori (i.e., root CA), and ending at a target certification authority which has signed the certificate of the public key to be verified. If the search for trusted paths is carried out using conventional search techniques, such as a breadth first or depth first techniques as known in the art, then a problem by way of reduced system or device performance occurs when large numbers of certification authorities are in the community of interest, and many different combinations of links among certification authorities and various networks (or the same network) exist. In such systems, a verification unit may spend valuable processing time obtaining and verifying all combinations of links to determine whether a trusted path has been maintained with the certification authority of the verifying verification unit and the certificate issuing unit that issued the target certificate.

[0005] Due to the limited amount of memory in an Internet appliance, mobile wireless units, and other mobile devices, only a small number of trusted root certificates are typically stored on each device. Accordingly, the local root CA certificate store is made smaller. Extensions are then added to most protocols which use certificates allowing the subscriber device to specify which root certificates it trusts. By allowing a subscriber device to specify which roots it trusts, a Web server, or other suitable server, which also has the root certificates stored thereon, can choose the correct certificate (one trusted by the subscriber device) to send to the subscriber or to abandon the protocol if the server does not trust any of the root certificates specified by the subscriber. However, this arrangement requires the Web server, or other server, to possibly have numerous certificates for many different roots which may be trusted by subscribers. It also means that there will be potentially many failed attempts at establishing a transport layer security session when a match does not occur. Wireless application protocol (WAP) servers, for example, typically check a list of certificates that it trusts and compares that list to see if a root certificate that is identified by the subscriber is also on the list. If so, it will complete the transport layer security session. Otherwise, it will abandon the protocol.

[0006] **FIG. 1** illustrates a conventional wireless communication system with a mobile wireless device **10** that is in operative communication through a wireless network **12** with a wireless application protocol server **14** and, if desired, another public key infrastructure server **16**. The mobile wireless device **10** includes a root CA certificate store **18** that contains, in this example, root certificates from Certification Authority **1** (CA1), CA **5** and CA **20** and accordingly and will trust communications from subscribers or servers that also trust these root CAs. As shown, the WAP server **14** has been issued a certificate **7** from CA7, certificate **2** from CA **2**, and certificate **3** from CA3. In this example, the mobile wireless device **10** has received a communication in which a certificate from CA7 is used to digitally sign information. Through wireless transport security handshaking **20**, the wireless mobile unit **10** communicates with the WAP server and notifies the WAP server that it trusts certificates from CA1, CA5 and CA20 as indicated in the root CA store **18**. Since the digitally signed message uses a certificate from CA7, the WAP server may redirect the wireless mobile unit **10** to contact the server **16** which would provide a root certificate for CA7. However, since there is only enough memory to store, for example, three root certificates, the

IPR2025-01572
Apple EX1007 Page 9

subscriber must now determine which of the root certificates gets deleted in favor of the new root certificate from CA7. In addition, many mobile wireless devices may have slow or low bandwidth communication links such as slow modems which limit the amount of information that can be communicated. Moreover, persons owning the devices may typically have to pay for air time and thus minimizing the bandwidth requirements in wireless communications for purposes of information security is high desirable.

[0007] Alternative methods are known that allow devices to securely download lists of trusted root certificates from a server when the current list is insufficient for certain purposes. This allows a subscriber to manage the trusted roots available on the device according to applications commonly used. However, with a limited amount of memory, it may become difficult for subscribers to manage all of the root certificates required. Since air interface resource bandwidth may be limited for mobile wireless devices, typically it is not desirable to always be downloading new root certificates when the current list is insufficient.

[0008] In addition, many mobile devices as noted above, have limited processing capabilities and limited battery life. Thus, computationally intensive operations such as performing full certificate path validation may not be possible or may take prohibitively long periods of time. In order to deal with such a problem, extensions to the On-line Certificate Status Protocol (OCSP) are used. With this solution, a subscriber sends a target certificate (certificate to be validated) and the trusted root certificate to a third party OCSP server which constructs and validates the appropriate certificate path. The OCSP server indicates whether or not the target certificate is valid. However, such a methodology still requires a subscriber to trust and have available the same number of root certificates. For example, if a subscriber requires validation of a certificate, the client sends the target certificate and a root certificate to the OCSP server. If a valid certificate chain exists for the target certificate and the associated root certificate, the OCSP server responds that the certificate is "valid". If a valid certificate chain does not exist, the server responds that the certificate is "invalid". In this conventional method, a root certificate is sent by the wireless mobile unit in the request to the OCSP server. It would be desirable to avoid having to waste wireless resource bandwidth on sending root certificates. In addition, it would be desirable to avoid having to access or maintain a local root CA store.

[0009] If a root certification authority needs to be revoked because its security has been compromised, such that it is no longer trusted (or for any other reason), it is difficult often to relay this information to all subscribers and to get all subscribers to manually remove the appropriate certificates from a list of trusted root certificates. One solution has been to post the revocation information in widely available media along with instructions on how to delete the untrusted root certificate from the device or Web browser. An alternative solution has been for a trusted server to create a signed list of root certificates that are no longer trusted and to send this list to all subscribers or subscribers. However, with such approaches, not all subscribers may receive or act on the message. The compromise of a certification authority in any network and particularly a wireless network, such as if a virus is present, can allow an unscrupulous party to be allowed to digitally sign information. Moreover, with pre-stored root CA certificates, stored, for example, in memory of mobile devices, it is often difficult to determine which subscribers have which root certificates since different browsers may have different pre-stored sets and depending upon the browser version, differing root CAs may be present in any given mobile wireless device.

[0010] Consequently, a need exists for a method and apparatus that suitably reduces storage requirements of wireless mobile devices, improves use of wireless bandwidth resources, and also allows for a more efficient control of revoked root certification authority certificates.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] **FIG. 1** is block diagram illustrating one example of a wireless communication system employing the use of certificates in a conventional manner;

[0012] **FIG. 2** is a block diagram of a wireless communication system employing certificate validation in accordance with one embodiment of the invention;

[0013] **FIG. 3** is a flow chart illustrating one method for validating a certificate in accordance with one embodiment of the invention;

[0014] **FIG. 4** is a block diagram illustrating another embodiment of a wireless communication system employing the validation of a certificate in accordance with one embodiment of the invention;

[0015] **FIG. 5** is a flow chart illustrating one method for validating a certificate as carried out by the system of **FIG. 4**;

[0016] **FIG. 6** is a block diagram illustrating one example of the content of a multi-subscriber root certificate store in accordance with one embodiment of the invention; and

[0017] **FIG. 7** is a flow chart illustrating one example of maintenance of a multi-subscriber root certificate store in accordance with one embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0018] A method and system for validating a certificate maintains a multi-subscriber root certificate store, containing subscriber identification data for a plurality of subscribers along with data representing a plurality of root certificates, such as an index to root certificates or the root certificates themselves, associated with each of the plurality of subscribers. In one example, a table is stored containing specified root CA certificates for a plurality of subscribers in a network such as stored by a network element in a wireless radiotelephone network, or any other suitable wireless network. Subscriber units do not have a root CA store that contains pre-stored root CA certificates. Accordingly, memory is saved in the subscriber units. In addition, a separate server that stores the multi-subscribers root certificate store preferably carries out certificate path validation on behalf of the mobile units so that the wireless mobile unit need not carry out certificate path construction. Instead, a wireless mobile unit simply sends a certificate to be validated along with its subscriber ID data identifying the mobile unit or application to the multi-subscriber root certificate store server and waits for a "yes" or "no" answer from the server to determine whether the certificate is valid.

[0019] In one embodiment, the multi-subscriber root certificate management server obtains, based on received subscriber identification data, those root certificates trusted by the subscriber from the multi-root certificate store. The server then performs certificate path validation to validate the received certificate using the root certificates from the multi-root certificate store. Accordingly, a party other than the wireless mobile unit performs certificate validation. Hence, the cryptographic engine resident in the wireless mobile unit may be less sophisticated and need not require a certificate validation engine.

[0020] The multi-subscriber root certificate store may store the list of root certificates trusted by each subscriber or each group of subscribers. Accordingly, the root certificates trusted by each client or subscriber need not reside locally on the client device and hence need not take up valuable memory resources on the device. In addition, the multi-subscriber root certificate store allows each subscriber or group of subscribers to trust as many root certificates as required. The central multi-subscriber root certificate management server allows for central and effective control of root certificate revocation. The central root certificate management server is able to immediately remove any untrusted root certificate from any and all subscriber lists of trusted root certificates. This may be desirable where network operators wish to maintain control of their subscribers' trust relationships.

[0021] When a subscriber receives a certificate that it wishes to validate, it sends a request to the central root certificate management server with an indication of the subscriber's identity. The subscriber identification data may be a signature on the subscriber's identity. The subscriber identification data may be a signature on the request, the subscriber's ID number or subscriber's name or any other method of identifying the subscriber. The request does not include an indication of the roots trusted by the subscriber since the central root certificate management server already has this information (and the client does not). The central root certificate management server then validates the certificate with respect to the list of trusted roots stored for that particular subscriber. A response is then returned, indicating the validity (pass/fail) of the target certificate. The response is protected for integrity and authenticity either using a digital signature, a secure session, a MAC or any other method for providing integrity and authenticity. In order to verify the response, the subscriber device need only store a verification key required to verify the response. This can result in a substantial savings over having to store a list of trusted root CA certificates and requiring certification path verification. In addition to root certificates, the central root certificate management server may also store any policy information required to validate certificates within any particular certification authority domain.

[0022] As an alternative, when a subscriber receives digitally signed information that it wishes to validate, it could send a request to the central root certificate management server with the certificate and an indication of the subscriber's identity, as above, but also including the digital signature to be validated. The central root certificate management server then validates the certificate, as above, and also validates the digital signature. The digital signature can only be valid if the corresponding certificate is valid. The response from the central root certificate management server to the subscriber indicates the validity (pass/fail) of the signature.

[0023] **FIG. 2** illustrates one example of a system **200** for validating a certificate **252** in accordance with one embodiment of the invention. The system **200** includes a wireless mobile unit **202** and a server referred to as a central root certificate management server (CRCMS) **204**, that includes a central root certificate managing module, such as a software application that contains instructions that, when executed by a processing device resident in the server, causes the server to perform the operations described herein. However, it will be recognized that any suitable combination of hardware, software and firmware may be used. The central root certificate management server **204** includes memory **206**, such as a database or other suitable storage medium or structure that serves as a multi-subscriber root certificate store **208** which contains subscriber identification data **210** for a plurality of subscribers and data representing a plurality of root certificates **212** associated with each of the plurality of subscribers. The central root certificate managing module maintains the multi-subscriber root certificate store **208** by at least removing unacceptable root certificates determined to be, for example, invalid or otherwise untrustworthy, that are common for a plurality of subscribers. In this example, subscribers having subscriber ID **1** and subscriber ID**2** both have root certificate **3** (RC**3**) as trusted root certificates. Accordingly, if root certificate **3** is determined to be compromised, the central root certificate management server **204** will indicate that these root certificates are untrustworthy and remove them from the multi-subscriber root certificate store and, if desired, notify the subscriber the next time the subscriber requests validation of a certificate using the root certificate RC**3**.

[0024] The central root certificate management server **204** is operably coupled to wireless network through, for example, a wireless application protocol (WAP) gateway **214**. As shown, the central root certificate management server **204** is a server element within the Internet. However, the server may be in any suitable system. The mobile wireless unit **202** is in operative communication with the wireless application protocol gateway **214** through a suitable wireless communication link or network illustrated generally as **215**. The system **200** also includes an application server **216**, such as a Web server or other unit with which the wireless mobile device **202** wishes to communicate and which provides the target certificate **252**.

[0025] Also shown is a certificate repository **205**, which includes suitable certificate revocation lists, certificates, and any other suitable information as known in the art to facilitate the construction of trusted paths. The repository **205** may be, for example, an X.500 type repository, or any other suitable repository. Accordingly, the central root certificate management server **204** may also provide certificate validation as known in the art, by constructing the requisite paths to determine whether a certificate is valid. In an alternative embodiment, instead of the central root certificate management server **204** performing certificate validation, an OCSP server **220** performs certificate validation. In this embodiment, the central root certificate management server **204** sends a target certificate **252** to be validated and the root certificate **226** from the multi-subscriber root certificate store to the OCSP server. The OCSP server **220** then

performs path construction if desired or any other suitable processing necessary to determine whether the target certificate **252** is valid. The OCSP server then sends the validation status **222** back to the central root certificate management server **204** which can then communicate whether the certificate is valid back to the wireless mobile unit **202**. As shown, the wireless mobile unit **202** may be any suitable Internet appliance, a laptop computer with a wireless transceiver, a radiotelephone, or any other suitable device. The wireless mobile device **202** includes a cryptographic engine **240** which may be implemented, for example, by suitable programming of a processing device such as a microprocessor, DSP, or any other suitable device to perform cryptographic functions. In this example, the cryptographic engine **240** is configured to be a digital signature verifier.

[**0026**] The wireless mobile device **202** also includes memory **242** operably coupled to the cryptographic engine **240** via a suitable bus **244**. Subscriber identification data **246** is stored in the wireless mobile device **202** as well as, for example, a verification key **248** such as a public key certificate issued for the central root certificate management server. In an alternative embodiment, a MAC key of the central root certificate management server may also be used, or any other suitable verification key.

[**0027**] The cryptographic engine **240** determines whether the target certificate **252** or a received certificate received from, for example, the server **216** is valid, without referencing a local root certificate store. Preferably, no root certificates are stored in the wireless mobile unit **202** and instead are maintained by the central root certificate management server **204**.

[**0028**] The central root certificate management server **204** includes an interface **250** that is operative to communicate with the wireless access protocol-based gateway **214**. Also, if desired, the same interface, or other interface, can be used to communicate with the third party root certificate validation provider, namely the OCSP server **220**.

[**0029**] Referring to **FIGS. 2 and 3**, the operation of the system **200** will be described. As shown in block **300**, the verification key **248** is prestored in the wireless mobile device. This may be, for example, the public key associated with the central root certificate management server **204** as issued by itself serving as a certification authority. Alternatively, the information may be downloaded wirelessly when the wireless mobile device **202** is activated, as part of an initialization procedure. In order for the central root certificate management server **204** to populate the multi-subscriber root certificate store **208**, the central root certificate management server **204** sends a root CA certificate selection form containing a list of a plurality of root certification authority certificates to allow the client to identify which root CA certificates to associate with its subscriber identification data. This is shown in block **302**. This may be carried out as part of a set up procedure. The root certification authority certificate selection form may be an HTML form, or any data structure, applet or any other mechanism to allow choosing of desired root CA certificates by or through a client device.

[**0030**] As shown in block **304**, the method also includes the wireless mobile device **202** forwarding any root certificates that it receives from other sources, that are categorized in a different class from those placed in the selection form. For example, if the subscriber is a member of a plurality of different communities of trust, and associated root CA certificates are added periodically, the wireless mobile unit **202** forwards the new root certificates to the central root certificate management server for association with the particular subscriber ID for that device so that the device need not maintain the new root CA certificates.

[**0031**] As shown in block **306**, the method includes maintaining, such as by the central root certificate management server **204** , the multi-subscriber root certificate store **208** by populating the multi-subscriber root certificate store **208** with selected root CA certificates for the given subscriber ID as indicated in the form. This population is done for all subscribers in the network community as identified, for example, by a system operator or upon initialization with the system **200**. As shown in block **308**, the method includes the wireless mobile device **202** attempting to set up, for example, a transport layer security session with the application server **216**. This is shown as TLS handshaking **250**.

[**0032**] As shown in block **310**, the application server **216** sends the target certificate **252** to be validated, back to the wireless mobile unit **202** as indicated by communication **252**. In response to receiving the target certificate **252**, the wireless mobile device **202**, in this embodiment, merely forwards the received certificate along with the subscriber identification data **246** to the central root certificate management server **204** as shown by communication **256**. Accordingly, the wireless mobile unit **202** avoids a need for a local root certificate store, accessing of such a store, and avoids certificate validation processing, by merely forwarding the received certificate **252** and the subscriber ID **246** to the central root certificate management server **204**. This is shown in block **312**. The communication is considered a request **256** to validate the target certificate **252** which includes data representing the certificate to be validated. In this instance, it is the certificate itself. Alternatively, it can be the public key within the certificate, the subject name from the certificate, or an index to a repository indicating where to obtain the target certificate. The central root certificate management server **204** receives the request **256** to validate a certificate as shown in block **314** accesses the multi-subscriber root certificate store **208** using the user ID **246** to obtain those root certificates trusted by that particular client. Accordingly, the method includes obtaining, based on the received user identification data **246**, those root certificates trusted by the client as obtained from the multi-user root certificate store **208**. Assuming by way of example that the subscriber ID data corresponds to subscriber ID**1**, the root certificates that are trusted in this example are those from root certificate CA**1** and root certificate CA**3**.

[**0033**] As shown in block **316**, the central root certificate management server **204** performs validation of the target certificate **252** by constructing a certificate chain between the target certificate and a root certificate stored in the multi-subscriber root certificate store for that client. As known in the art this involves, for example, contacting the requisite certification authorities, directories, and/or if desired, a OCSP server. As shown in block **318**, the method includes receiving back, by the wireless mobile unit **202**, a trusted certificate validation response **260** indicating whether the target certificate **252** is valid based on the root certificates from the multi-subscriber root certificate store

containing the subscriber identification data for the plurality of subscribers. This is shown in block **318**. This includes, for example, the central root certificate management server **204** digitally signing the validation data that forms the trusted validation response **260** indicating, for example, whether the certificate is valid or not. This may be digitally signed, for example, by the private key of the central root certificate management server **204**. This validation response **260** is then passed to the WAP gateway, and the WAP gateway **214** then wirelessly passes the validation response **260** to the wireless mobile unit **202**. Upon receiving the validation response **260**, the wireless mobile device **202** uses the cryptographic engine **240** to verify the trusted validation response **260** to validate the digital signature on the response to determine whether the certificate is valid. This is done without accessing a local root certificate store. If the certificate is valid, the wireless mobile apparatus **202** continues set up of the TLS session with the application server **216** as shown in block **320**.

[**0034**] As shown in **FIG. 2**, maintaining the multi subscriber root certificate store **208** may include storing a table containing user identification data **210** for a plurality of subscribers, and data representing the plurality of different classes of root certificates associated with each of the plurality of subscribers. This may be done, for example, on a group of subscriber basis as well.

[**0035**] From the perspective of the wireless mobile unit **202**, the cryptographic engine **240** sends the data representing the certificate **252** to be validated (such as the certificate itself, the public key therefrom, the subject name from the certificate, or an index) as well as subscriber identification data **246**, representing a subscriber for the central root certificate managing server **204**. The cryptographic engine **240** receives the trusted validation response **260** indicating whether the target certificate **252** is valid based on the contents of multi-subscriber root certificate store. The cryptographic engine **240** then verifies the trusted certificate validation response **260** using the stored verification key **248** that is associated with the central root certificate management unit **204** indicating whether the target certificate is valid. This is done without accessing a local root certificate store.

[**0036**] Referring to **FIGS. 4 and 5**, an alternative embodiment is shown wherein wireless resource bandwidth is reduced. This is done, for example, by having the application server **216** be in communication with the central root certificate management server **204**. In contrast with the system and operation described in **FIGS. 2 and 3**, in this embodiment, the wireless mobile device **202**, namely the cryptographic engine **240**, instead of sending the target certificate **252**, sends data representing an address associated with the multi-subscriber root certificate store **208**, namely, an address such as an IP address or DN of the central root certificate management server **204** indicated as data **400** to the WAP gateway **214** which then forwards it to the application server **216**. The application server **216** includes a software routing module, such as a software application, which retrieves the target certificate **252** and sends the target certificate **252** along with the subscriber ID **246** as message **256** to the central root certificate management server **204**. Upon receipt of the response **260** from the central root certificate management server **204**, the application server **216** forwards the response to the wireless mobile device **202**. In this way, the target certificate **252** from the application server **216**, namely the target certificate to be validated, need not be communicated to the wireless mobile device **202** and hence reduces bandwidth. In addition, WAP gateway **214** need not be coupled to the central root certificate management server **204**.

[**0037**] Accordingly, as shown in **FIG. 5**, an alternate method includes sending the subscriber ID **246** to the application server **216** along with a central root certificate management server address **400** to avoid the need for local root certificate store and local certificate validation processing. As shown in block **502**, the method includes the application server **216** sending the subscriber ID **246** and the target certificate **252** to the central root certificate management server **204** using the address information **400**. As described above, the same steps **314** and **316** apply. However, instead of receiving the response **260** from the central root certificate management server **204** for the WAP gateway, the wireless mobile device **202** receives and verifies the response **260** as sent by the application server **216**. This is shown in block **504**.

[**0038**] **FIG. 6** illustrates the multi-root certificate store **208** showing a table **600** having root certificate classification divisions **602** and **604**. In this embodiment, each root certificate is classified as to widely used root certificates and less widely used root certificates. The widely used certificates are considered a Class 1 **602** and may be prestored in the central root certificate management server. The table **600** is preferably digitally signed by the central root certificate management server **204** to protect the integrity of the information. The class 2 root certificates **604** are those that are likely obtained and provided to the central root certificate management server **204** by each wireless mobile device as they are transmitted to such devices on a periodic basis.

[**0039**] With the central storing of root certificates for multiple subscribers, each subscriber can also send a request to the central root certificate management server **204** to remove a root CA association, if desired. In addition, the central root certificate management server **204** can revoke root CAs for all subscribers at the same time to avoid the spreading of a virus, for example.

[**0040**] **FIG. 7** is a flow chart illustrating one example of multi-subscriber root certificate store maintenance. As shown in block **700**, the method includes sending the root certificates from all clients to be stored and then populating the store **208** on a per-subscriber ID basis (or per group basis), as shown in block **702**. As noted above, each subscriber may select which certificates they desire in their list. As shown in block **704**, the central root certificate management server **204** receives the root certificate revocation information out of band at a later point in time to determine which root certificate should be revoked. As shown in block **706**, the central root certificate management server **204** removes the root CA from the multi-subscriber certificate store to avoid virus propagation. This is done for all subscribers in the system, namely those identified by the subscriber IDs in the table **600**. As shown in block **708**, the method includes determining whether a request has been received from wireless mobile device to change any root CA entries. If so, as shown in block **710**, the method includes updating the root CA certificates for the requesting subscriber based on the update request. If no such request has

been received, the method includes waiting, as shown in block **712**, to receive such a request at a later date.

[**0041**] In the above-described apparatus and methods, wireless mobile devices need not store any trusted root certificates and need only, for example, store a single verification key associated with the central root certificate management server **204**, to effect validation of all certificates. The wireless mobile units need not download trusted root certificates and do not need to implement certificate path validation. In addition, the above operations allow for more effective central 'control of a subscriber's trusted root certificate list. Other advantages will be recognized by those of ordinary skill in the art.

[**0042**] Implementations of the above apparatus and methods may include, for example, the use of software serving as executable instructions that when executed by one or more processing devices in the central root certificate management server and/or application server and/or WAP gateway and/or wireless mobile device, that causes the requisite devices to perform the operations described herein. As such, an implementation may have one or more storage mediums, such as CD ROMs, distributed storage to effect downloading of the software from remove servers, or any other suitable storage medium containing executable instructions that when executed by one or more processing devices, causes the one or more processing devices to act as described herein.

[**0043**] The processors may be a single processing entity or a plurality of processing entities. Such a processing entity may be a microprocessor, microcomputer, microcontroller, central processing units, digital signal processor, state machine, logic circuitry, and/or any device that manipulates information based on operational instructions. The memory may be a single memory device or a plurality of memory devices. Such a memory device may be a read-only memory, random access memory, floppy disk memory, hard disk memory, system memory, reprogrammable memory, magnetic tape memory, DVD memory, and/or any device that stores digital information. Note that if the processors implement one or more of their functions using a state machine or logic circuitry, the memory containing the corresponding operational instructions is embedded within the circuitry that comprises the state machine and/or logic circuitry.

[**0044**] It should be understood that the implementation of other variations and modifications of the invention in its various aspects will be apparent to those of ordinary skill in the art, and that the invention is not limited by the specific embodiments described. For example, although the examples above have been described with reference to a wireless environment, the disclosed methods and apparatus can be employed in a non-wireless environment such as conventional Web browsers. It is therefore contemplated to cover by the present invention, any and all modifications, variations, or equivalents that fall within the spirit and scope of the basic underlying principles disclosed and claimed herein.

What is claimed is:

1. A method for validating a certificate comprising:

maintaining a multi-subscriber root certificate store containing subscriber identification data for a plurality of subscribers and data representing a plurality of root certificates associated with each of the plurality of subscribers;

receiving data representing a first certificate to be validated;

receiving first user identification data in connection with a request to validate the first certificate for a first user; and

obtaining, based on the received first user identification data, those root certificates trusted by the first user from the multi-root certificate store.

2. The method of claim 1 including the step of providing data representing whether validation of the first certificate was successful based on a root certificate from those trusted by the first user as obtained from the multi-user root certificate store.

3. The method of claim 1 including the step of validating, by a party other than the first user, the first certificate using a first root certificate from those obtained from the multi-root certificate store.

4. The method of claim 3 wherein validating the first certificate includes constructing a certificate chain between the first certificate and the first root certificate and validating the integrity and correctness of each certificate in the chain.

5. The method of claim 1 including providing a trusted first certificate validation response indicating whether the first certificate is valid.

6. The method of claim 1 including the step of sending, by a client unit, user identification data for use in obtaining those root certificates trusted by the first user from the multi-root certificate store and sending the data representing a first certificate to be validated.

7. The method of claim 1 including the step of sending, by a client unit, user identification data for use in obtaining those root certificates trusted by the first user from the multi-root certificate store and sending data representing an address associated with the multi-user root certificate store.

8. The method of claim 1 wherein the step of maintaining the multi-user root certificate store containing user identification data for the plurality of subscribers and data representing the plurality of root certificates associated with each of the plurality of subscribers includes the step of storing a table containing user identification data for the plurality of subscribers and data representing the plurality of different classes of root certificates associated with each of the plurality of subscribers.

9. The method of claim 5 including the step of verifying, by the first user, the trusted first certificate validation response indicating whether the first certificate is valid, without accessing a local root certificate store.

10. The method of claim 5 wherein the trusted first certificate validation response is digitally signed by a server containing the multi-user root certificate store.

11. The method of claim 1 including the step of sending a root certification authority certificate selection form containing a list of a plurality of root certification authority certificates, to the first user to allow the first user to select which root certificates in the list should be associated with the identification data of the first user.

12. The method of claim 1 wherein the step of maintaining the multi-user root certificate store containing user identification data for the plurality of subscribers and data representing the plurality of root certificates associated with each

of the plurality of subscribers includes the step of removing common root certificates for a plurality of listed users in response to a compromise of the root certificate.

13. A method for validating a certificate comprising:

sending, by a first wireless mobile unit, data representing a first certificate to be validated and unit identification data representing the first wireless mobile unit;

receiving, by the first wireless mobile unit, a trusted first certificate validation response indicating whether the first certificate is valid based on a multi-user root certificate store containing user identification data for a plurality of wireless mobile units and data representing a plurality of root certificates associated with each of the wireless mobile units; and

verifying, by the first wireless mobile unit, the trusted first certificate validation response indicating whether the first certificate is valid, without accessing a local root certificate store.

14. A method for validating a certificate comprising:

maintaining a multi-user root certificate store containing user identification data for a plurality of subscribers and data representing a plurality of root certificates associated with each of the plurality of subscribers;

sending, by a first user, a request to validate a first certificate that includes data representing the first certificate to be validated and user identification data for the fist user;

receiving the request to validate the first certificate containing the data representing the first certificate to be validated and the user identification data;

obtaining, based on the received first user identification data, those root certificates trusted by the first user from the multi-root certificate store; and

receiving, by the first user, a trusted first certificate validation response indicating whether the first certificate is valid based on the multi-user root certificate store containing user identification data for a plurality of subscriber and data representing a plurality of root certificates associated with each of the users; and

verifying, by the first user, the trusted first certificate validation response to determine whether the first certificate is valid, without accessing a local root certificate store.

15. The method of claim 14 including the step of validating, by a party other than the first user, the first certificate using a first root certificate from those obtained from the multi-root certificate store.

16. The method of claim 15 wherein validating the first certificate includes constructing a certificate chain between the first certificate and the first root certificate and validating the integrity and correctness of each certificate in the chain.

17. The method of claim 14 wherein the step of maintaining the a multi-user root certificate store containing user identification data for the plurality of subscribers and data representing the plurality of root certificates associated with each of the plurality of subscribers includes the step of storing a table containing user identification data for the plurality of subscribers and data representing the plurality of different classes of root certificates associated with each of the plurality of subscribers.

18. The method of claim 14 wherein the trusted first certificate validation response is digitally signed by a server containing the multi-user root certificate store.

19. The method of claim 17 including the step of sending a root certification authority certificate selection form containing a list of a plurality of root certification authority certificates, to the first user to allow the first user to select which root certificates in the list should be associated with the identification data of the first user.

20. A server comprising:

a central root certificate managing module; and

memory containing a multi-user root certificate store containing user identification data for a plurality of subscribers and data representing a plurality of root certificates associated with each of the plurality of subscribers;

wherein the central root certificate managing module maintains the multi-user root certificate store by at least responding to subscriber requests to change root CA entries.

21. The server of claim 20 wherein the central root certificate managing module maintains the multi-user root certificate store by removing unacceptable root certificates that are common for a plurality of subscribers.

22. The server of claim 20 including an interface operative to communicate with a wireless access protocol based gateway.

23. The server of claim 20 including an interface operative to communicate with a third party root certificate validation provider.

24. A wireless mobile unit comprising:

a cryptographic engine operative to determine whether a received certificate is valid without referencing a local root certificate store; and

memory, operatively coupled to the cryptographic engine, containing at least data representing a verification key associated with a central root certificate managing unit.

25. The wireless mobile unit of claim 24 wherein the cryptographic engine includes a digital signature verifier and wherein the memory contains a public key certificate associated with the central root certificate managing unit.

26. The wireless mobile unit of claim 25 wherein the cryptographic engine sends data representing the certificate to be validated and unit identification data representing a user for the central root certificate managing unit; receives a trusted first certificate validation response indicating whether the first certificate is valid based on a multi-user root certificate store containing user identification data for a plurality of wireless mobile units and data representing a plurality of root certificates associated with each of the wireless mobile units; and verifies the trusted first certificate validation response using the stored verification key associated with the central root certificate managing unit indicating whether the first certificate is valid, without accessing a local root certificate store.

* * * * *