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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 November 2003 (06.11.2003)

PCT

(10) International Publication Number
WO 03/091858 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US03/07574

(22) International Filing Date: 13 March 2003 (13.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/376,100 26 April 2002 (26.04.2002) US

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46, Quai Le Gallo, F-92648 Boulogne (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ZHANG, Junbiao** [US/US]; 1003 Sunny Slope Road, Bridgewater, NJ 08807 (US). **WANG, Charles, Chuanming** [US/US]; 1504 Spearmint Circle, Jamison, PA 18929 (US). **LI, Jun** [CN/US]; 26 Orchid Drive, Plainsboro, NJ 08536 (US).

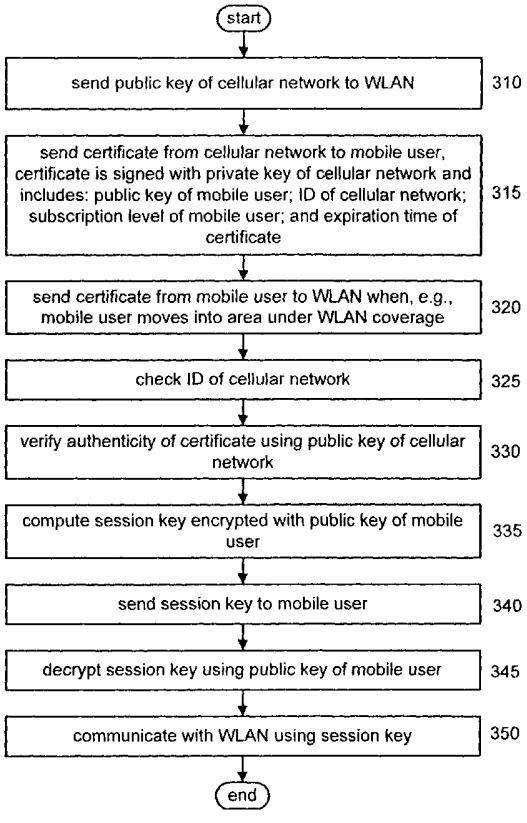
(74) Agents: **TRIPOLI, Joseph, S** et al.; Thomson Licensing, Inc., Two Independence Way, Princeton, NJ 08540 (US).

(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, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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,

[Continued on next page]

(54) Title: CERTIFICATE BASED AUTHENTICATION AUTHORIZATION ACCOUNTING SCHEME FOR LOOSE COUPLING INTERWORKING



(57) Abstract: A method for Authentication Authorization and Accounting (AAA) in an interworking between first and second networks that do not belong in the same administrative domain, using certificate based transactions. In the method according to the invention, the second network sends a public key to the first network, and a certificate to a mobile device. The certificate includes information regarding the subscription level of the mobile device and is signed with a private key of the second network. Upon detection of the first network the mobile device transmits the certificate and the first network authenticates the certificate using the public and private keys of the second network, and authorizes access to the network in response. The first network then sends a session key encrypted with a public key of the mobile device. The mobile device decrypts the session key with a private key and access the first network using the session key. In this manner, interworking is implemented without requiring the deployment of a special interworking function to bridge between the two different types of networks.

WO 03/091858 A2

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

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.

CERTIFICATE BASED AUTHENTICATION AUTHORIZATION ACCOUNTING SCHEME FOR LOOSE COUPLING INTERWORKING

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention generally relates to networking and, more particularly, to a certificate based Authentication Authorization and Accounting (AAA) scheme for loose coupling interworking between two different access networks.

Related Art

Typically, Authentication, Authorization and Accounting (AAA) are required to access and utilize networks such as cellular networks and Wireless Local Area Networks (WLANs). However, the implementing of AAA can be difficult as well as requiring additional software and/or hardware in the case of interworking between two different radio access networks that do not belong to the same administrative domain and do not share the same AAA schemes.

There are two main types of interworking between cellular networks and WLANs: tight coupling and loose coupling. In a loose coupling scenario, the WLAN and the cellular network have independent data paths but the AAA for WLAN users relies on cellular network AAA functions. However, the cellular network AAA protocols (MAP/SS7) are incompatible with Internet Protocol (IP) based protocols used by WLAN users. Two approaches have been proposed. In the first approach, an AAA interface is provided in the cellular network Home Location Register (HLR). This requires either duplicating HLR data or providing a protocol converter between Radius/Diameter and MAP. In the second approach, if the Mobile Terminal (MT) uses a Subscriber Identity Module (SIM) card based authentication mechanism (e.g., NOKIA's wireless operator LAN), then the AAA will follow the cellular procedure. An AAA InterWorking Function (IWF) is necessary to interface with the HLR and an MT. Functionality wise, it is similar to a Serving GPRS (General Packet Radio Service) Support Node (SGSN) or Mobile Switching Center (MSC) from the AAA perspective except AAA traffic is carried through IP.

With both approaches, special interworking functions or gateways need to be deployed by the cellular operators. With the second approach, users are required to have a SIM card for WLAN access, but most WLAN users do not have SIM cards available on their laptops or Personal Digital Assistants (PDAs).

Accordingly, it would be desirable and highly advantageous to have an Authentication Authorization and Accounting (AAA) scheme for the case of interworking between two different networks that do not belong to the same administrative domain and do not share the same AAA schemes, where the AAA scheme does not require the deployment of a special interworking function to bridge between the two different types of networks.

SUMMARY OF THE INVENTION

The problems stated above, as well as other related problems of the prior art, are solved by the present invention, a certificate based Authentication, Authorization and Accounting (AAA) scheme for an interworking between different access networks.

Advantageously, the present invention can operate without interaction with the cellular core network during authentication. Compared with existing schemes, the proposed scheme does not require the cellular operators to adapt their Home Location Register (HLR) interfaces to provide authentication for WLAN users through Internet protocols.

According to an aspect of the present invention, there is provided a method for Authentication Authorization and Accounting (AAA) in an interworking between at least two networks. The at least two networks include a first network and a second network. A user of the first network is verified based on a certificate, by the second network. A session key is sent from the second network to a mobile device of the user when the user is verified. The session key is used for encrypting communication between the mobile device and the second network.

These and other aspects, features and advantages of the present invention will become apparent from the following detailed description of preferred embodiments, which is to be read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a computer system 100 to which the present invention may be applied, according to an illustrative embodiment of the present invention;

FIG. 2 is a block diagram illustrating a combination of access networks to which the present invention may be applied, according to an illustrative embodiment of the present invention;

FIG. 3 is a flow chart illustrating a certificate based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to an illustrative embodiment of the present invention; and

FIG. 4 is a flow chart illustrating a certificate based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to another illustrative embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is directed to a certificate based Authentication Authorization and Accounting (AAA) scheme for loose coupling interworking. It is to be appreciated that the present invention is applicable to any combination of access networks (such as, e.g., an interworking between a Community Access Television (CATV) network and a Wireless Local Area Network (WLAN)). However, the present invention is particularly applicable to a cellular network and WLAN in a loose interworking arrangement.

It is to be understood that the present invention may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof, for example, within a mobile terminal, access point, or a cellular network. Preferably, the present invention is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM), and input/output (I/O) interface(s). The computer platform also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the application program (or a combination thereof), which is executed via the operating system. In addition, various other peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying Figures are preferably

implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the present invention is programmed. Given the teachings herein, one of ordinary skill in the related art will be able to contemplate these and similar implementations or configurations of the present invention.

FIG. 1 is a block diagram illustrating a computer system 100 to which the present invention may be applied, according to an illustrative embodiment of the present invention. The computer processing system 100 may be embodied in a mobile device used to access a cellular network or a WLAN. The computer processing system 100 includes at least one processor (CPU) 102 operatively coupled to other components via a system bus 104. A read only memory (ROM) 106, a random access memory (RAM) 108, a display adapter 110, an I/O adapter 112, a user interface adapter 114, a sound adapter 199, and a network adapter 198, are operatively coupled to the system bus 104.

A display device 116 is operatively coupled to system bus 104 by display adapter 110. A disk storage device (e.g., a magnetic or optical disk storage device) 118 is operatively coupled to system bus 104 by I/O adapter 112.

A mouse 120 and keyboard 122 are operatively coupled to system bus 104 by user interface adapter 114. The mouse 120 and keyboard 122 are used to input and output information to and from system 100.

At least one speaker (herein after "speaker") 197 is operatively coupled to system bus 104 by sound adapter 199.

A (digital and/or analog) modem 196 is operatively coupled to system bus 104 by network adapter 198.

FIG. 2 is a block diagram illustrating a combination of access networks to which the present invention may be applied, according to an illustrative embodiment of the present invention. In the illustrative embodiment of FIG. 2, the combination of access networks includes a cellular network 210 and three Wireless Local Area Network (WLAN) 220a, 220b, and 220c. Mobile terminal 200, cellular network 210 and WLANs 220 may communicate with each other as indicated. The present invention provides a certificate based scheme to provide AAA services to WLAN users. As noted above, the present invention may be applied to any combination of networks, including different numbers and different types of networks.

FIG. 3 is a flow diagram illustrating a certificate based method for

Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to an illustrative embodiment of the present invention. The access networks include a cellular network and a Wireless Local Area Network (WLAN), such as those shown in Fig. 2. The cellular network is associated with at least a mobile user. It is to be appreciated that while the illustrative embodiment of FIG. 3 (as well as the illustrative embodiment of FIG. 4 below) is described with respect to a cellular network and a WLAN, any combination of networks, including the preceding and other types of networks as well as different numbers of networks, may be readily employed in accordance with the present invention while maintaining the spirit and scope of the present invention.

Initially, a public key K_{pub_cn} associated with the cellular network is sent from the cellular network to the WLAN, which has an interworking contract with the cellular network (step 310). In the event that the cellular network has an interworking contract with more than one WLAN, then the cellular network could send the cellular network public key K_{pub_cn} to all of the WLANs with which it has a contract. It is preferable, but not mandatory, that the cellular network public key K_{pub_cn} is distributed through a secure channel so that the recipient WLAN can be sure that K_{pub_cn} is indeed a valid public key associated with the cellular network.

A certificate is then sent from the cellular network to the mobile user (step 315). The certificate includes, but is not limited to, the following: public key K_{pub_u} associated with the mobile user; ID of cellular network; subscription level of the mobile user, for example, whether the mobile user has subscribed for WLAN service, for authorization/verification purposes; expiration time of the certificate; and ID of the mobile user. The certificate is signed with a private key K_{pri_cn} of the cellular network. It is preferable, but not mandatory, that the certificate is sent to the mobile user when the mobile user signs up with the cellular network for WLAN interworking service.

The various keys and the certificate are used as follows. When the mobiel user moves into an area under WLAN coverage, the certificate is sent from the mobile user to the WLAN (step 320). The WLAN then: checks the ID of the cellular network included in the certificate (step 325); checks the ID of the mobile user included in the certificate (e.g., for an authorization/verification purpose(s)) (step 327); verifies the authenticity of the certificate using the public key K_{pub_cn} of the cellular network (step 330); upon verification, computes a session key for the mobile user that is encrypted with a public key K_{pub_u} of the mobile user that was included in

the certificate (step 335); and sends the session key to the mobile user (step 340). The session key may be, but is not limited to, a per user Wired Equivalent Privacy (WEP) key.

Upon receiving the session key, the mobile user decrypts the session key using his/her private key K_{pri_u} (step 345) and communicates with the WLAN using the session key (i.e., all subsequent communication between the mobile device and the WLAN is encrypted with the session key) (step 350). Thus, the mobile user is authenticated by the WLAN since only that specific mobile user has the necessary private key K_{pri_u} to decrypt the session key.

FIG. 4 is a flow diagram illustrating a certificate based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to another illustrative embodiment of the present invention. The access networks include a cellular network and a Wireless Local Area Network (WLAN). The cellular network is associated with at least a mobile user. The method of FIG. 4 allows for mutual authentication between the mobile user and the WLAN, so that the mobile user can also verify that he/she is indeed communicating with a legitimate WLAN (to prevent, e.g., messages from being snooped).

A public key K_{pub_cn} of the cellular network is sent from the cellular network to the WLAN, which has an interworking contract with the cellular network (step 310). In the event that the cellular network has an interworking contract with more than one WLAN, then the cellular network could send the public key K_{pub_cn} of the cellular network to all of these WLANs. It is preferable, but not mandatory, that the public key K_{pub_cn} is distributed through a secure channel so that the WLAN can be sure that K_{pub_cn} is indeed the public key of the cellular network.

The public key K_{pub_cn} of the cellular network is also sent from the cellular network to the mobile user (step 412).

A first certificate is sent from the cellular network to the mobile user (step 315). The first certificate includes, but is not limited to, the following: public key K_{pub_u} of the mobile user; ID of cellular network; subscription level of the mobile user (whether the mobile user has subscribed for WLAN service); expiration time of the first certificate; and ID of mobile user. The first certificate is signed with a private key K_{pri_cn} of the cellular network. It is preferable, but not mandatory, that the first certificate is sent to

the mobile user when the mobile user signs up with the cellular network for WLAN interworking service.

A second certificate is also sent from the cellular network to each WLAN (that has a contract agreement with the cellular network) (step 417). The second certificate includes, but is not limited to, a public key K_{pub_w} of the WLAN. The second certificate is signed with the private key K_{pri_cn} of the cellular network.

The first certificate is sent from the mobile user to the WLAN (e.g., an Access Point (AP) or other entity), e.g., when the mobile user moves into an area under WLAN coverage (step 320). In response, the WLAN checks the ID of the cellular network included in the first certificate (step 325), checks the ID of the mobile user included in the first certificate (e.g., for an authorization/verification purpose(s)) (step 327), and verifies the authenticity of the first certificate using the public key K_{pub_cn} of the cellular network (step 330). Upon verification, the WLAN computes a session key for the mobile user that is encrypted with the public key K_{pub_u} of the mobile user (that was included in the first certificate) and that is signed with the private key K_{pri_w} of the WLAN (step 435), and sends the session key and the second certificate to the mobile user (step 440). The session key may be, but is not limited to, a per user Wired Equivalent Privacy (WEP) key.

Upon receiving the session key and the second certificate, the mobile user verifies that the second certificate is valid using the public key K_{pub_cn} of the cellular network (step 441). If it is valid, then the public key K_{pub_w} of the WLAN is extracted from the second certificate (step 442). The mobile user then verifies that the session key actually comes from the WLAN by using the public key K_{pub_w} of the WLAN to verify the signature on the session key (step 443). If the encrypted session key is verified to come from the WLAN, the mobile user then decrypts the session key using his/her private key K_{pri_u} (step 345) and communicates with the WLAN using the session key. All subsequent communication between the mobile device and the WLAN is encrypted with the session key starts using the session key for communicating with the WLAN (step 350).

Thus, a primary advantage of the present invention as compared with the prior art is that the present invention does not require any physical interworking functions in order for the WLAN to interact with the cellular network for the purpose of user authentication. In fact, by using certificates, the WLANs do not need any interaction with the cellular network at the time the mobile terminal requests access to the

network in order to grant user access. Since the certificate includes the identity of the mobile user, accounting functions can be easily performed using this information, including the user identity.

Although the illustrative embodiments have been described herein with reference to the accompanying drawings, it is to be understood that the present invention is not limited to those precise embodiments, and that various other changes and modifications may be affected therein by one skilled in the art without departing from the scope or spirit of the invention. All such changes and modifications are intended to be included within the scope of the invention as defined by the appended claims.

WHAT IS CLAIMED IS:

1. A method for providing Authentication, Authorization and Accounting (AAA) in a first network for a mobile device that is associated with a second network, the first and second networks having respective AAA schemes, comprising the steps of:

receiving a first key from the second network;

receiving a certificate from a mobile device; and

authenticating the certificate using the key, and if the certificate is authenticated,

generating a session key, transmitting the session key to the mobile device, and allowing the mobile device to access the first network using the session key.

2. The method according to claim 1, wherein the certificate includes a public key associated with the mobile device, an ID associated with the second network, and a signature comprising a second key of the second network.

3. The method according to claim 2, wherein the authenticating step comprises authenticating the certificate in response to the first and second keys of the second network.

4. The method according to claim 2, wherein the generating step comprises the steps of computing the session key and encrypting the session key using the public key associated with the mobile device.

5. The method according to claim 1, wherein the certificate includes a subscription level associated with the mobile device that indicates whether the device is subscribed to an interworking service, and performing the generating step if the mobile device has subscribed to the interworking service.

6. The method according to claim 1, wherein the certificate includes an expiration time that indicates when the certificate expires, and further comprising the step of checking the certificate to determine whether the certificate has expired.

7. The method according to claim 1, wherein the certificate includes an ID associated with the mobile device, and further comprising the step of generating accounting information based on the usage of the first network by the mobile device following the authentication.

8. The method according to claim 1, further comprising the step of receiving from the second network a second certificate, which includes a public key associated with the first network and is signed with a second key of the second network, and wherein the transmitting step comprises transmitting the session key and the second certificate to the mobile device, whereby the mobile device can verify that the session key was transmitted from the first network in response to the second certificate.

9. A method for accessing a first network using a mobile device associated with a second network, including authentication, authorization, and accounting (AAA) via the first network, comprising the steps of:

receiving a certificate from a second network that has an existing interworking relationship with the first network;

in response to detection of the first network, transmitting the certificate to the first network, whereby AAA may be performed in response to the certificate and a first key transmitted from the second network to the first network;

receiving a session key from the first network upon authentication; and

accessing the first network using the session key.

10. The method according to claim 9, wherein the certificate includes a public key associated with the mobile device, an ID associated with the second network, and a signature comprising a second key of the second network.

11. The method according to claim 10, wherein the receiving step comprises receiving a session key encrypted using the public key of the mobile device, and further comprising the step of decrypting the session key using a private key associated with the mobile device.

12. The method according to claim 9, wherein the certificate includes a subscription level associated with the mobile device that indicates whether the device has subscribed to an interworking service.

13. The method according to claim 9, wherein the certificate includes an expiration time that indicates when the certificate expires.

14. The method according to claim 9, wherein the certificate includes an ID associated with the mobile device, whereby accounting information based on the usage of the first network by the mobile device may be generated by the first network in response to the ID and transmitted to the second network.

15. The method according to claim 9, further comprising the step of

receiving from the first network a second certificate issued by the second network; and

verifying that the session key was sent by the first network in response to the second certificate.

16 The method according to claim 15, wherein the second certificate includes a public key associated with the first network.

17. An apparatus for accessing a first network, including authentication, authorization, and accounting via the first network, and for associating with a second network, comprising:

means for receiving a certificate from the second network, which has an existing interworking relationshipt with the first network;

means for storing the certificate;

means for detecting the presence of the first network, and transmitting the certificate to the first network in response to the detection of the first network, whereby AAA can be performed by the first network in response to the certificate and a key provided by the second network;

means for receiving a session key from the first network; and

means for accessing the first network using the session key.

18. The apparatus according to claim 17, wherein the certificate includes a public key, ID of the second network, subscription level, and subscription expiration time associated with the apparatus.

19. The apparatus according to claim 18, further comprising means for decrypting the session key using a private key associated with the apparatus.

20. The apparatus according to claim 19, further comprising means for receiving from the first network a second certificate issued by the second network, and means for verifying that the session key was sent by the first network in response to the second certificate.

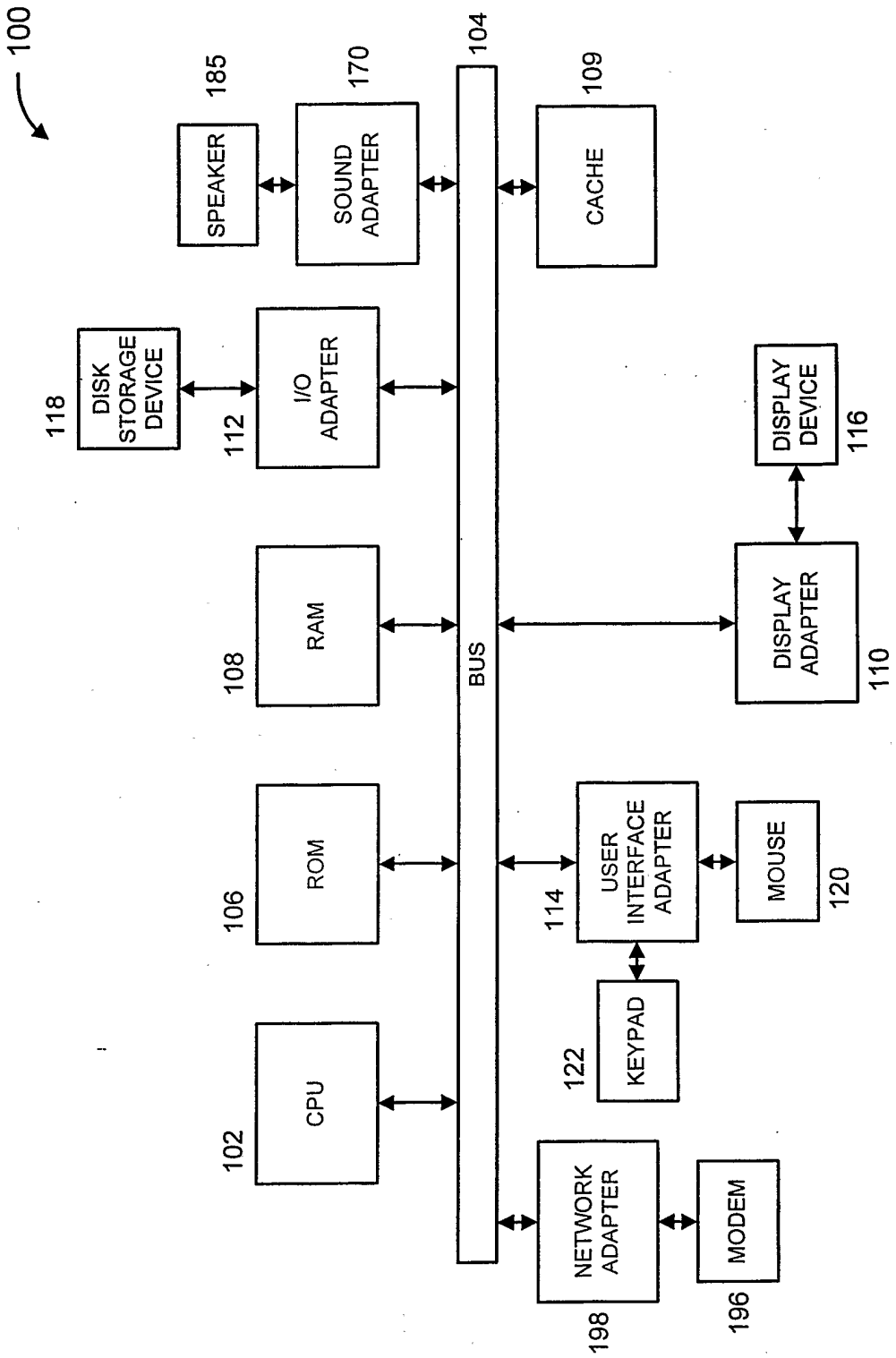

100
SPEAKER
185
SOUND ADAPTER
170
CACHE
109
104
DISK STORAGE DEVICE
118
I/O ADAPTER
112
DISPLAY DEVICE
116
RAM
108
BUS
DISPLAY ADAPTER
110
ROM
106
USER INTERFACE ADAPTER
114
MOUSE
120
KEYPAD
122
CPU
102
NETWORK ADAPTER
198
MODEM
196

FIG. 1

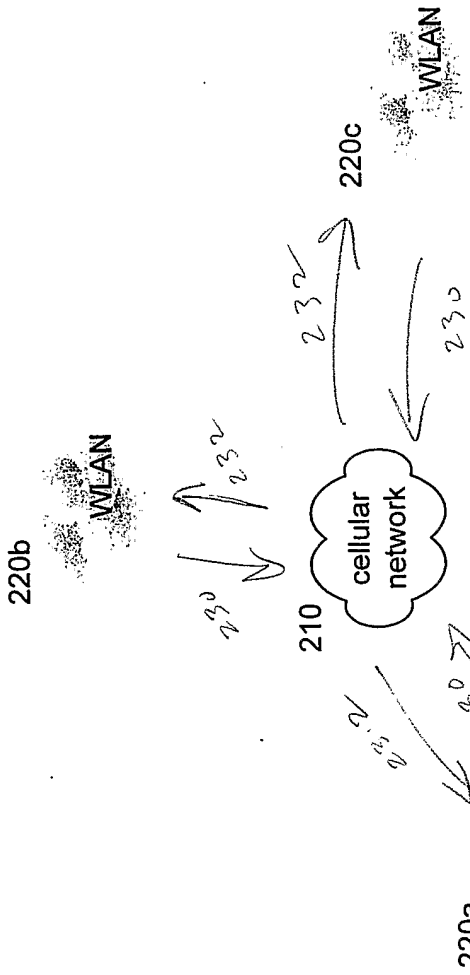


FIG. 2

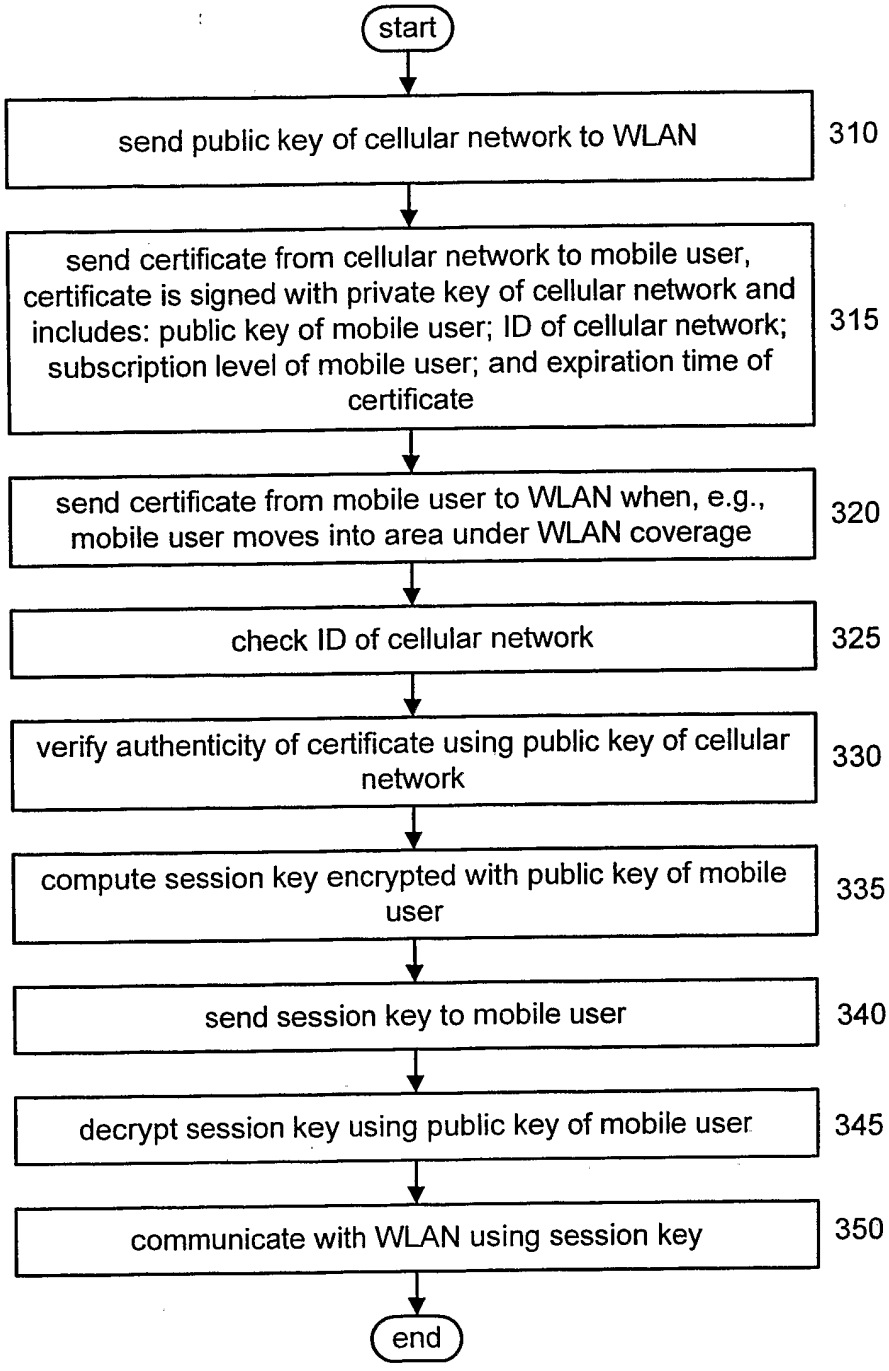

start
send public key of cellular network to WLAN
310
send certificate from cellular network to mobile user, certificate is signed with private key of cellular network and includes: public key of mobile user; ID of cellular network; subscription level of mobile user; and expiration time of certificate
315
send certificate from mobile user to WLAN when, e.g., mobile user moves into area under WLAN coverage
320
check ID of cellular network
325
verify authenticity of certificate using public key of cellular network
330
compute session key encrypted with public key of mobile user
335
send session key to mobile user
340
decrypt session key using public key of mobile user
345
communicate with WLAN using session key
350
end

FIG. 3

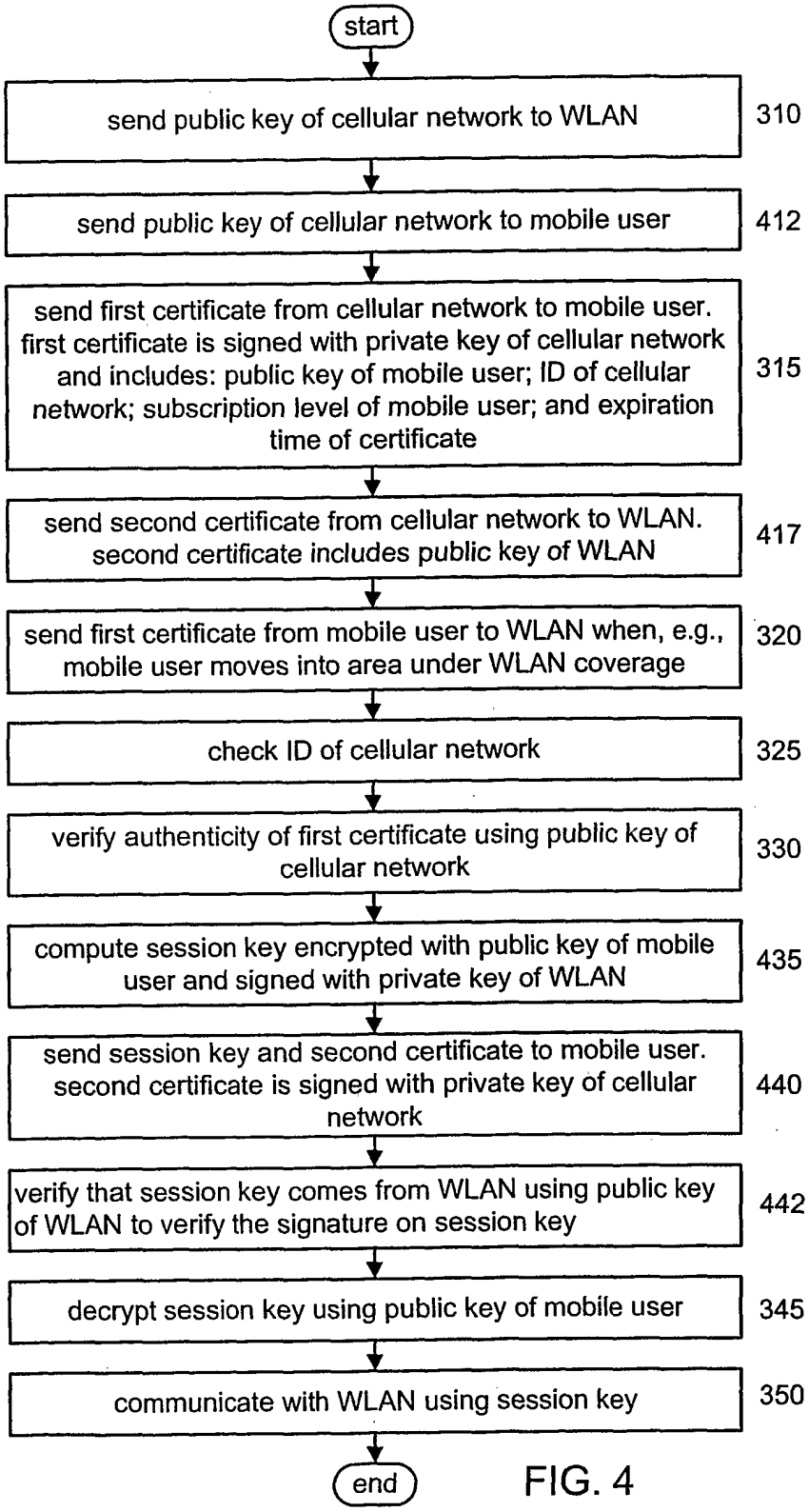

start
send public key of cellular network to WLAN
310
send public key of cellular network to mobile user
412
send first certificate from cellular network to mobile user. first certificate is signed with private key of cellular network and includes: public key of mobile user; ID of cellular network; subscription level of mobile user; and expiration time of certificate
315
send second certificate from cellular network to WLAN. second certificate includes public key of WLAN
417
send first certificate from mobile user to WLAN when, e.g., mobile user moves into area under WLAN coverage
320
check ID of cellular network
325
verify authenticity of first certificate using public key of cellular network
330
compute session key encrypted with public key of mobile user and signed with private key of WLAN
435
send session key and second certificate to mobile user. second certificate is signed with private key of cellular network
440
verify that session key comes from WLAN using public key of WLAN to verify the signature on session key
442
decrypt session key using public key of mobile user
345
communicate with WLAN using session key
350
end

FIG. 4