

(51) International Patent Classification:
H04W 12/06 (2009.01)(21) International Application Number:
PCT/US2012/028611(22) International Filing Date:
9 March 2012 (09.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/450,956 9 March 2011 (09.03.2011) US
13/213,401 19 August 2011 (19.08.2011) US(71) Applicant (for all designated States except US): **QUALCOMM INCORPORATED** [US/US]; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **PA-LANIGOUNDER, Anand** [IN/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **TIEDEMANN, Edward George** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **NASIELSKI, John Wallace** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).(74) Agent: **KIM, Won Tae**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

- with international search report (Art. 21(3))

(54) Title: METHOD FOR AUTHENTICATION OF A REMOTE STATION USING A SECURE ELEMENT

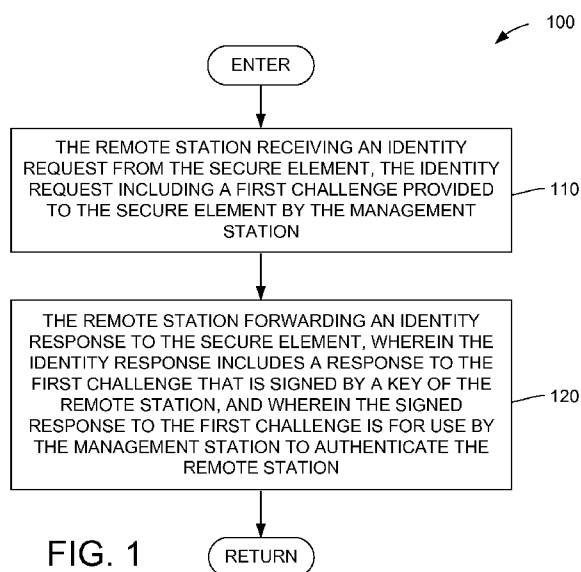


FIG. 1

(57) Abstract: Disclosed is a method for authentication of a remote station by a management station using a secure element. In the method, the remote station receives an identity request from the secure element. The identity request includes a first challenge provided to the secure element by the management station. The remote station forwards an identity response to the secure element. The identity response includes a response to the first challenge that is signed by a key of the remote station, and the signed response to the first challenge is for use by the management station to authenticate the remote station.

METHOD FOR AUTHENTICATION OF A REMOTE STATION USING A SECURE ELEMENT

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Application No. 61/450,956, filed March 9, 2011, which application is incorporated herein by reference.

BACKGROUND

Field

[0002] The present invention relates generally to authentication of a remote station.

Background

[0003] A remote station may host user services provided by a wireless network operator. In GSM, UMTS, LTE and cdma2000 systems, the user services may be enabled using a smart card. An example of a smart card may be a Universal Integrated Circuit Card (UICC). The UICC may be removable, allowing it to be moved to another station or device. The wireless network operator may desire to authenticate the hosting remote station, without undue expense.

[0004] There is therefore a need for an effective technique for authenticating a remote station.

SUMMARY

[0005] An aspect of the present invention may reside in a method for authentication of a remote station by a management station using a secure element. In the method, the remote station receives an identity request from the secure element. The identity request includes a first challenge provided to the secure element by the management station. The remote station forwards an identity response to the secure element. The identity response includes a response to the first challenge that is signed by a key of the remote station. The signed response to the first challenge is for use by the management station to authenticate the remote station.

[0006] In more detailed aspects of the invention, the secure element may be a smartcard that is embedded in the remote station, a smartcard that is removable from the remote station, or a Trusted Processor Module built into the remote station. The remote station

may be a wireless mobile device. The key of the remote station may be a private key that corresponds to a public key available to the management station, and the identity response may include a certificate that includes the public key. Alternatively, the key of the remote station may be a secret key shared by the management station. The identity response may include an identity value that is unique to the remote station. The first challenge may be a first nonce. Also, the identity response may include a second challenge generated by the remote station for use in authenticating the management station.

[0007] Another aspect of the invention may reside in a remote station which may include means for receiving an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station, and means for forwarding an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station.

[0008] Another aspect of the invention may reside in a remote station which may include a processor configured to receive an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station, and to forward an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station; and a memory configured to store the key of the remote station.

[0009] Another aspect of the invention may reside in a computer program product, comprising computer-readable storage medium, comprising code for causing a computer to receive an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station; and code for causing a computer to forward an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key associated with the computer, and wherein the signed response to the first challenge is for use by the management station to authenticate the computer.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0010] FIG. 1 is a flow diagram of a method for authentication of a remote station by a management station using a secure element, according to the present invention.
- [0011] FIG. 2 is a flow diagram of a call flow for authentication of a remote station by a management station using a secure element.
- [0012] FIG. 3 is a block diagram of a computer including a processor and a memory.
- [0013] FIG. 4 is a block diagram of an example of a wireless communication system.

DETAILED DESCRIPTION

- [0014] The word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments.
- [0015] With reference to FIGS. 1 and 2, an aspect of the present invention may reside in a method 100 for authentication of a remote station 210 by a management station 220 using a secure element 230. In the method, the remote station receives an identity request REQ ID from the secure element (step 110). The identity request includes a first challenge N1 provided to the secure element by the management station. The remote station forwards an identity response ID RES to the secure element (step 120). The identity response includes a response to the first challenge that is signed by a key K of the remote station. The signed response is for use by the management station to authenticate the remote station.
- [0016] In more detailed aspects of the invention, the secure element 230 may be a smartcard that is embedded in the remote station 210, a smartcard that is removable from the remote station, or a Trusted Processor Module built into the remote station. The remote station may comprise a mobile user equipment (UE) such as a wireless device. The key K of the remote station may be a private key K_{PRI} that corresponds to a public key available to the management station, and the identity response may include a certificate CERT that includes the public key. Alternatively, the key of the remote station may be a secret key K_{SH} shared by the management station 220. The identity response may include an identity value that is unique to the remote station, such as an International Mobile Equipment Identity (IMEI) or Mobile Equipment Identity (MEID) or any other identity that uniquely always identifies the remote station. Other examples of such identities may include, but are not limited to, hardware identifiers assigned by

IEEE such as EUI-48 or EUI-64 or assigned by the manufacturer of the remote station. The first challenge N1 may be a first nonce. Also, the identity response may include a second challenge, such as a second nonce, generated by the remote station for use in authenticating the management station.

[0017] With further reference to FIG. 3, another aspect of the invention may reside in a remote station 210 which may include means (processor 310) for receiving an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station, and means 310 for forwarding an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station.

[0018] Another aspect of the invention may reside in a remote station 210 which may include a processor 310 configured to receive an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station, and to forward an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station; and a memory configured to store the key of the remote station.

[0019] Another aspect of the invention may reside in a computer program product, comprising non-transitory computer-readable storage medium 320, comprising code for causing a computer 300 to receive an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station; and code for causing a computer to forward an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key associated with the computer, and wherein the signed response to the first challenge is for use by the management station to authenticate the computer.

[0020] The remote station 210 or apparatus may comprise a computer 300 that includes, a processor 310, a storage medium 320 such as memory and/or disk drives, a secure module 330, a display 340, an input device such as a keyboard 350, a microphone, speaker(s), a camera, and the like. The station may include a wireless connection 360. Further, the station may also include USB, Ethernet and similar interfaces.

[0021] With reference again to FIG. 2, a high level call flow 200 shows procedures for host remote station authentication by the management station 220. The secure element 230 may be a smart card attached to the remote station 210, and provisioned with addresses for management station. The remote station may be a host module such as a mobile equipment with a secure storage and execution environment 330, e.g., a trusted environment (TrE) such as 3GPP TS 33.320. The remote station may be provisioned with device credentials such as an IMEI as the device identity, and a securely stored device private key or a shared secret key. The public key corresponding to the device private key may be accessible (for example, from a certificate CERT) to anyone wanting to verify a signature made using the device private key. If used, the shared secret key likewise would be securely stored by the management station. The management station may be a secure element manager that provides network access applications (NAAs) to the secure element. NAAs are used to obtain service from access networks such as wireless or wireline networks.

[0022] For example, the secure element 230 may be a smartcard (e.g., SIM, UICC/eUICC or R-UIM) or a Trusted Processor Module (TPM) that may not be customized with network operator data before deployment. It may be desirable for the smartcard or TPM to verify that it is attached to a certified and/or authorized host (cellular module/mobile equipment) before the smartcard or TPM is provisioned with network access credential information. Also, a network operator may want to periodically verify that the smartcard or TPM is still attached to the host remote station 210. For example, the network operator may want to prevent the pairing of a smartcard or TPM with another unauthorized host remote station for illicitly receiving network access, or for avoiding tracking by the network operator or government authorities. Using the smartcard or TPM may allow authentication of the host remote station without requiring changes to certain transport access network (i.e., LTE/UMTS, cdma2000 or other such wireless or even wireline access network) protocols.

[0023] The host remote device's identity may be any device identity that may be associated with the device's private/public key pair, or with the shared secret key. In addition to the IMEI, other examples may include an MEID, EUI-64, EUI-48, or any other unique device identity.

[0024] The management station 220 may be the entity that operates an over-the-air (OTA) management platform for the secure element 230. The secure element may use

existing UICC/SIM card protocols specified by ETSI SCP/3GPP, or may use GlobalPlatform protocols or other suitable protocols.

[0025] In the call flow 200, the secure element 230 may open a connection with the remote station 210, and request the remote station to establish a transport connection with the management station 220 (step 250). The connection between the secure element and the remote station may be securely protected to prevent attack from an attacker inserted between the secure element and the remote station. The remote station selects a transport system 240 for establishing the transport connection with the management station (step 252). The transport system may be a wireless wide area access network WWAN (e.g., a cdma2000 or 3GPP access system such as GSM/GPRS/UMTS/LTE, etc.), a wireless local area network WLAN (e.g., an IEEE 802.11a/b/g/n wireless network), or a fixed IP service provided by a fixed network (e.g., PSTN, xDSL, Cable, Ethernet, Fiber, etc.). The transport connection may use IP or SMS or any such transport protocol. The transport connection is established (step 254). The secure element and the management station 220 may securely connect over the transport protocol for provisioning or management message exchanges (step 256). The messages transported between the secure element and the management station may be encrypted and integrity protected using, for example, authenticated HTTPS/TLS or SMS enhanced with encryption and/or integrity.

[0026] The management station 220 sends a request for a signed host remote station identity request REQ ID REQ to the secure element 230 (step 258). The request includes a nonce N1. The secure element sends a request for a signed host remote station identity, which includes the nonce N1, to the host remote station 210 (step 260). The remote station returns, to the secure element, a signed identity response ID RES that includes its identity (e.g., its IMEI), the nonce, and a signature (step 262). The signed identity response may further include a second nonce N2 as a challenge to authenticate the management station. The signature is for use by the management station for authenticating the remote station.

[0027] When using a private/public key pair, the remote station 210 hashes the message and encrypts it using the private key. The management station 220 decrypts the encrypted hash using the remote station's public key to authenticate the remote station (step 266). Message integrity is verified by re-hashing the received message and comparing it to the signature hash.

- [0028] When using a shared secret key, the remote station 210 generates the signature (MAC) using the shared key (MAC = HMAC (shared key, message)). The management station 220 re-generates the signature (MAC) using the shared key, and compares it with the received MAC (step 266). The host remote station is then identified by the received identity.
- [0029] After successful authentication of the host remote station 210, the management station 220 may then securely provision and activate the secure element 230 with NAAs or other credentials for providing services to the remote station (step 268). If the authentication of the host remote station fails, the management station may black list the remote station and not provision it with NAAs or other credentials information needed by the remote station to obtain service from a service provider. The management station may also instruct the secure element to disallow the use of network access credential information by the host remote station, if present on the secure element.
- [0030] The management station 220 may periodically request host remote station authentication. For example, the management station may request authentication during an on-going management session. Alternatively, the management station may configure a policy in the secure element 230 to perform the authentication steps at the end of a configured time, upon detection of a change in the host remote station (e.g., a new device is paired), or upon every power-up of the host remote station.
- [0031] With reference to FIG. 4, a wireless remote station (RS) 402 (or UE) may communicate with one or more base stations (BS) 404 of a wireless communication system 400. The RS may further pair with a wireless peer device. The wireless communication system 400 may further include one or more base station controllers (BSC) 406, and a core network 408. Core network may be connected to an Internet 410 and a Public Switched Telephone Network (PSTN) 412 via suitable backhauls. A typical wireless mobile station may include a handheld phone, or a laptop computer. The wireless communication system 400 may employ any one of a number of multiple access techniques such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), space division multiple access (SDMA), polarization division multiple access (PDMA), or other modulation techniques known in the art.
- [0032] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For

example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0033] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0034] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0035] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to

the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[0036] In one or more exemplary embodiments, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software as a computer program product, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code in the form of instructions or data structures and that can be accessed by a computer. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

[0037] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be

limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS:

CLAIMS

1. A method for authentication of a remote station by a management station using a secure element, comprising:

the remote station receiving an identity request from the secure element, the identity request including a first challenge provided to the secure element by the management station; and

the remote station forwarding an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station.

2. A method for authentication as defined in claim 1, wherein the secure element is a smartcard that is embedded in the remote station.

3. A method for authentication as defined in claim 1, wherein the secure element is a smartcard that is removable from the remote station.

4. A method for authentication as defined in claim 1, wherein the secure element is a Trusted Processor Module built into the remote station.

5. A method for authentication as defined in claim 1, wherein the remote station is a wireless mobile device.

6. A method for authentication as defined in claim 1, wherein the key of the remote station is a private key that corresponds to a public key available to the management station.

7. A method for authentication as defined in claim 6, wherein the identity response includes a certificate that includes the public key.

8. A method for authentication as defined in claim 1, wherein the key of the remote station is a secret key shared by the management station.

9. A method for authentication as defined in claim 1, wherein the identity response includes an identity value that is unique to the remote station.
10. A method for authentication as defined in claim 1, wherein the first challenge is a first nonce.
11. A method for authentication as defined in claim 1, wherein the identity response includes a second challenge generated by the remote station for use in authenticating the management station.
12. A remote station, comprising:
 - means for receiving an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station; and
 - means for forwarding an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station.
13. A remote station as defined in claim 12, wherein the secure element is a smartcard that is embedded in the remote station.
14. A remote station as defined in claim 12, wherein the secure element is a smartcard that is removable from the remote station.
15. A remote station as defined in claim 12, wherein the secure element is a Trusted Processor Module built into the remote station.
16. A remote station as defined in claim 12, wherein the remote station is a wireless mobile device.

17. A remote station as defined in claim 12, wherein the key of the remote station is a private key that corresponds to a public key available to the management station.

18. A remote station as defined in claim 17, wherein the identity response includes a certificate that includes the public key.

19. A remote station as defined in claim 12, wherein the key of the remote station is a secret key shared by the management station.

20. A remote station as defined in claim 12, wherein the identity response includes an identity value that is unique to the remote station.

21. A remote station as defined in claim 12, wherein the first challenge is a first nonce.

22. A remote station as defined in claim 12, wherein the identity response includes a second challenge generated by the remote station for use in authenticating the management station.

23. A remote station, comprising:

a processor configured to:

receive an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station, and

forward an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key of the remote station, and wherein the signed response to the first challenge is for use by the management station to authenticate the remote station; and

a memory configured to store the key of the remote station.

24. A remote station as defined in claim 23, wherein the secure element is a smartcard that is embedded in the remote station.

25. A remote station as defined in claim 23, wherein the secure element is a smartcard that is removable from the remote station.

26. A remote station as defined in claim 23, wherein the secure element is a Trusted Processor Module built into the remote station.

27. A remote station as defined in claim 23, wherein the remote station is a wireless mobile device.

28. A remote station as defined in claim 23, wherein the key of the remote station is a private key that corresponds to a public key available to the management station.

29. A remote station as defined in claim 28, wherein the identity response includes a certificate that includes the public key.

30. A remote station as defined in claim 23, wherein the key of the remote station is a secret key shared by the management station.

31. A remote station as defined in claim 23, wherein the identity response includes an identity value that is unique to the remote station.

32. A remote station as defined in claim 23, wherein the first challenge is a first nonce.

33. A remote station as defined in claim 23, wherein the identity response includes a second challenge generated by the remote station for use in authenticating the management station.

34. A computer program product, comprising:
computer-readable medium, comprising:
code for causing a computer to receive an identity request from a secure element, the identity request including a first challenge provided to the secure element by a management station; and
code for causing a computer to forward an identity response to the secure element, wherein the identity response includes a response to the first challenge that is signed by a key associated with the computer, and wherein the signed response to the first challenge is for use by the management station to authenticate the computer.
35. A computer program product as defined in claim 34, wherein the secure element is a smartcard.
36. A computer program product as defined in claim 34, wherein the secure element is a removable smartcard.
37. A computer program product as defined in claim 34, wherein the secure element is a Trusted Processor Module.
38. A computer program product as defined in claim 34, wherein the key is a private key that corresponds to a public key available to the management station.
39. A computer program product as defined in claim 34, wherein the key is a secret key shared by the management station.
40. A computer program product as defined in claim 34, wherein the first challenge is a first nonce.

1/3

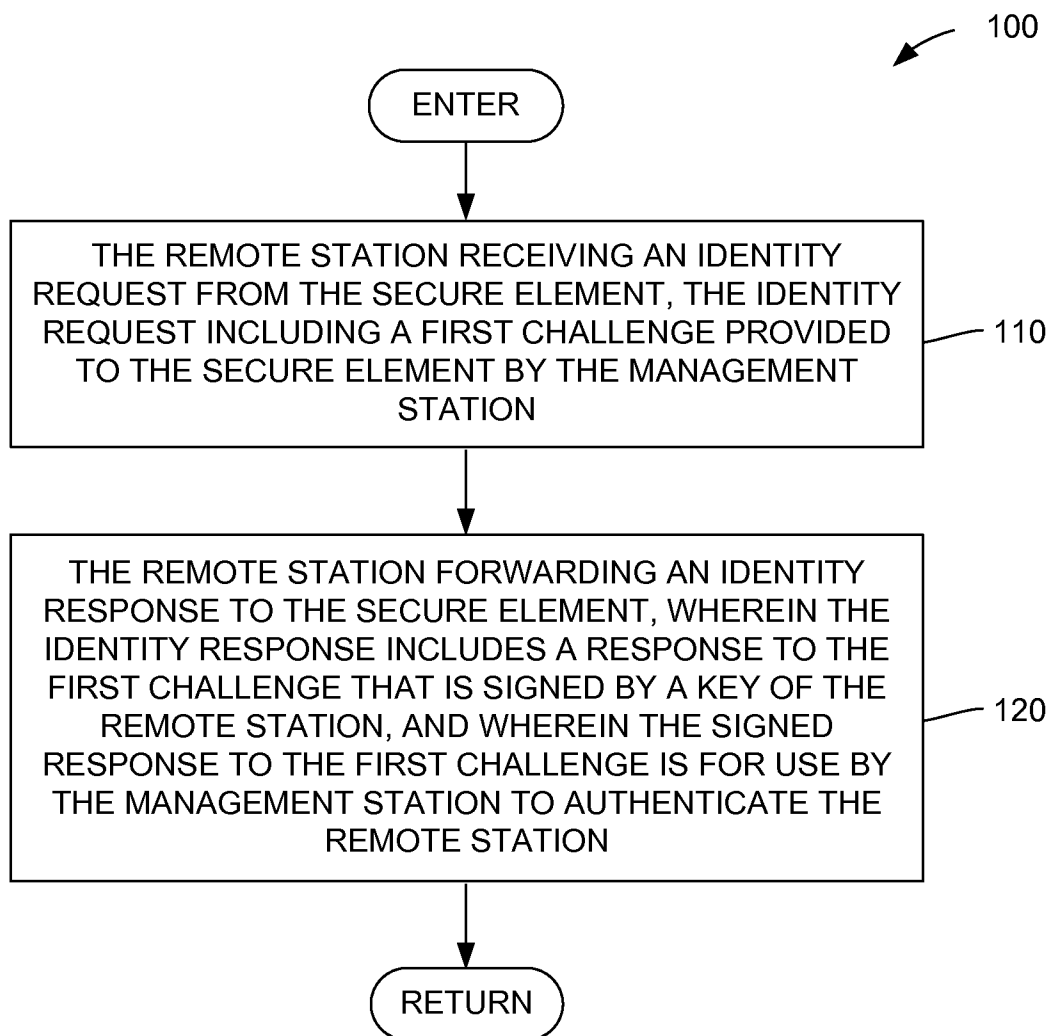


FIG. 1

2/3

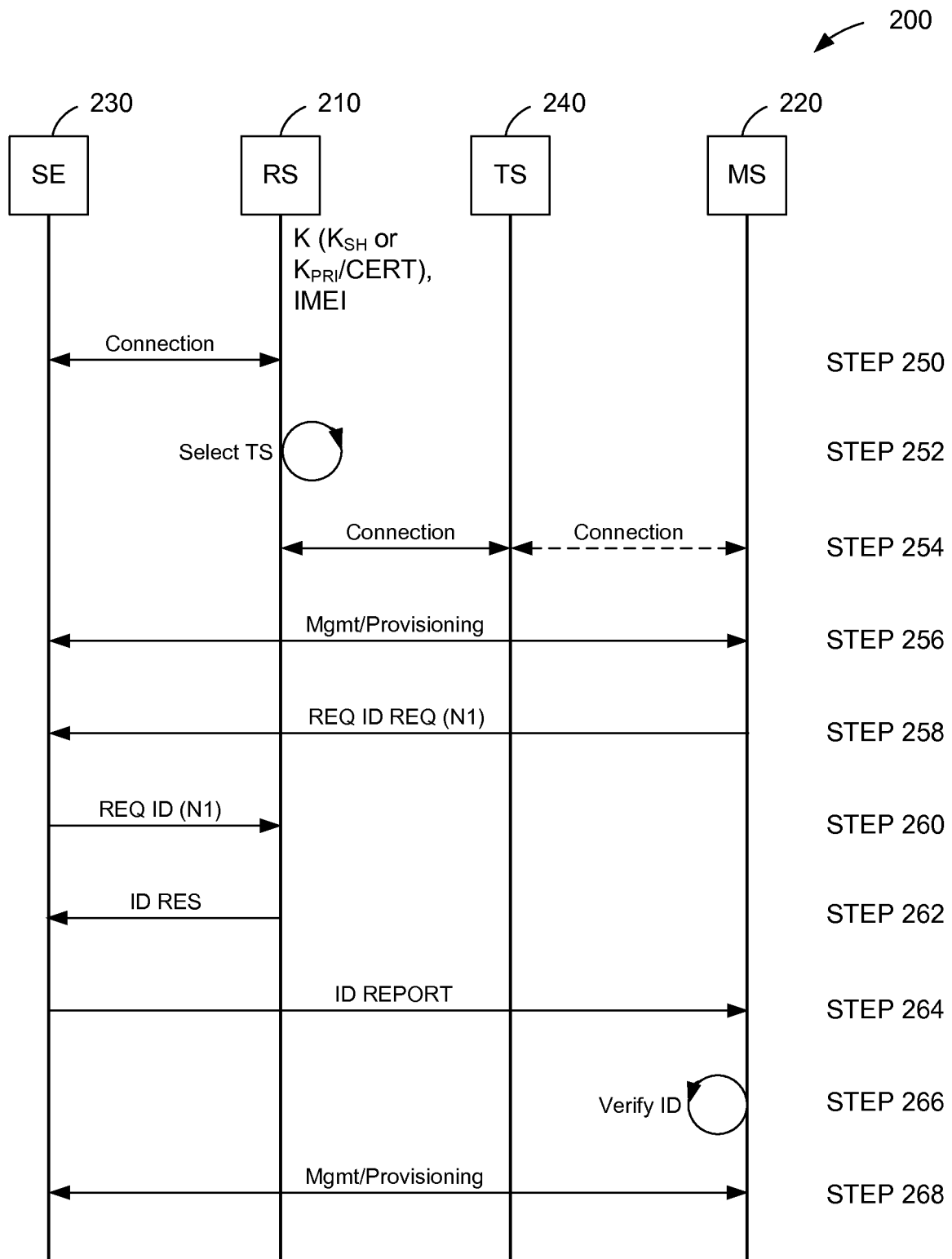


FIG. 2

3/3

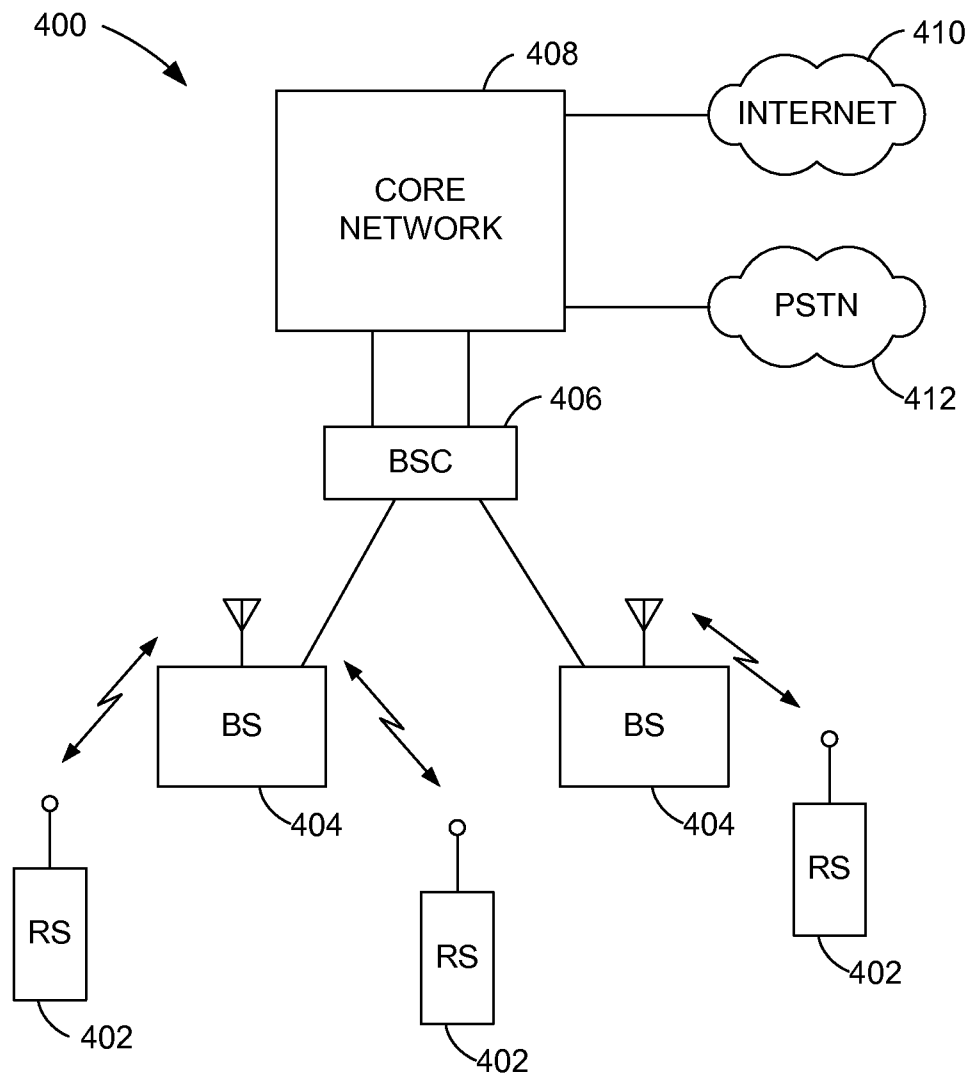


FIG. 4

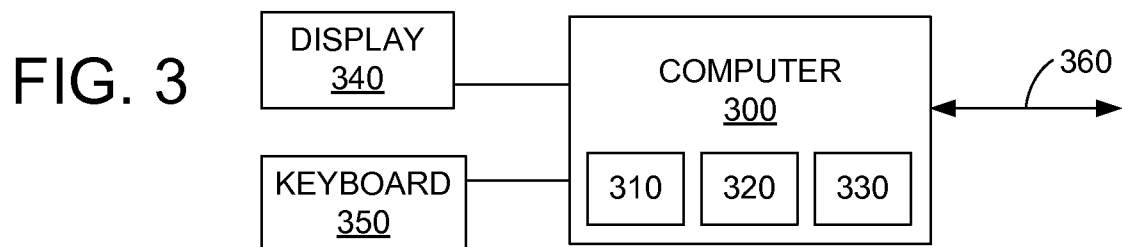


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2012/028611

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/06

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L H04Q G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/111616 A1 (ADI WAEL [DE]) 10 June 2004 (2004-06-10) paragraphs [0057], [0059] - [0068], [0073] - [0094] figures 1-6	1-40
X	US 2007/142086 A1 (BOURSIER CARINE [FR] ET AL) 21 June 2007 (2007-06-21) paragraphs [0026] - [0039] figures 1-2	1-40
X	EP 2 291 015 A1 (GEMALTO SA) 2 March 2011 (2011-03-02) paragraphs [0097] - [0103], [0108] - [0121] figures 1,2	1-40



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

2 May 2012

Date of mailing of the international search report

23/05/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ghomrasseni, Z

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/028611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004111616	A1	10-06-2004	DE 10026326 A1 29-11-2001
			EP 1290905 A2 12-03-2003
			JP 4819286 B2 24-11-2011
			JP 2003535497 A 25-11-2003
			US 2004111616 A1 10-06-2004
			WO 0191478 A2 29-11-2001
US 2007142086	A1	21-06-2007	AT 386408 T 15-03-2008
			DE 602004011836 T2 09-04-2009
			EP 1709827 A1 11-10-2006
			FR 2864410 A1 24-06-2005
			US 2007142086 A1 21-06-2007
			WO 2005069658 A1 28-07-2005
EP 2291015	A1	02-03-2011	EP 2291015 A1 02-03-2011
			WO 2011023819 A1 03-03-2011