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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2009 (15.01.2009)

PCT

(10) International Publication Number
WO 2009/008641 A2

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/KR2008/003969

(22) International Filing Date: 4 July 2008 (04.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2007-0068080 6 July 2007 (06.07.2007) KR

(71) Applicant *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161, Gajeong-dong, Yusong-gu, Daejeon-city 305-350 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KIM, Kwihoon** [KR/KR]; 110-1103 Nokwon Apt., Dunsan2-dong, Seo-gu, Daejeon-city 305-732 (KR). **LEE, Hyun-Woo** [KR/KR]; 105-203 HANA Apt., Shinseong-dong, Yuseong-gu, Daejeon-city 305-721 (KR). **JO, Seng-Kyoun** [KR/KR]; 280-16 Pugkajwa2-dong, Seodaemun-gu, Seoul 120-812 (KR). **AHN, Jae-Young** [KR/KR]; #301, 210-40, Shinseong-dong, Yuseong-gu, Daejeon-city 305-805 (KR). **RYU, Won** [KR/KR]; #202, 111-12, Eoeun-dong, Yuseong-gu, Daejeon-city 305-807 (KR). **LEE, Byung-Sun** [KR/KR]; 107-1104 Hanbit Apt., Eoeun-dong, Yusong-gu, Daejeon-city 305-755 (KR). **JUN, Kyung-Pyo** [KR/KR]; 117-1502 Hanvit Apt., Eoeun-dong, Yuseong-gu, Daejeon-city 305-755 (KR).

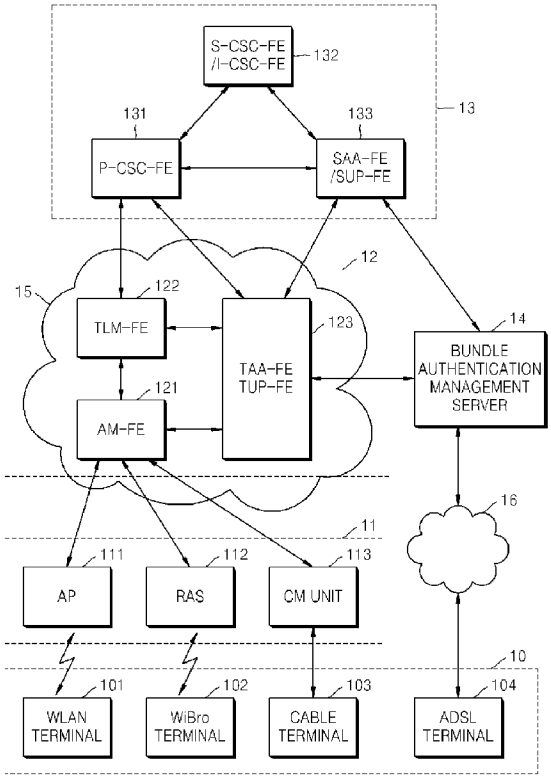
(74) Agent: **Y.P.LEE, MOCK & PARTNERS**; 1575-1, Seocho-dong, Seocho-gu, Seoul 137-875 (KR).

(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, 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,

[Continued on next page]

(54) Title: NODE AUTHENTICATION AND NODE OPERATION METHODS WITHIN SERVICE AND ACCESS NETWORKS IN NGN ENVIRONMENT

FIG. 1



(57) Abstract: Provided are node authentication and node operation methods within service and access networks for bundle authentication between the service and access networks in a next generation network (NGN) . A method of authentication processing of a node (S-CSC-FE/I-CSC-FE (Serving Call Session Control Functional Entity/Interrogating Call Session Control Functional Entity)) within a service network for bundle authentication between service and access networks, the method including: receiving first authentication information about access authentication of a terminal from a first node within the service networks; requesting to receive second authentication information from a second node within the service network based on the first authentication information; and comparing the first authentication information with the second authentication information to authenticate the terminal.

WO 2009/008641 A2

IL, IN, IS, JP, KE, KG, KM, KN, KP, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (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*

Description

NODE AUTHENTICATION AND NODE OPERATION METHODS WITHIN SERVICE AND ACCESS NETWORKS IN NGN ENVIRONMENT

[1] This application claims the benefit of Korean Patent Application No. 10-2007-0068080, filed on July 6, 2007, in the Korean Intellectual Property Office, the disclosure of which is incorporated herein in its entirety by reference.

Technical Field

[2] The present invention relates to node authentication and node operation methods, and more particularly, node authentication and node operation methods within service and access networks for bundle authentication between the service and access networks in a next generation network (NGN) when a subscriber subscribes to the service and access networks.

[3] This work was partly supported by the IT R&D program of MIC/IITA [2005-S-058-02, Development of Network/Service Control Technology in ALL-IP based Converged network].

Background Art

[4] It is assumed that an access provider and a service provider share physical line information previously in an NGN environment of conventional ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) and TISPAN (The Telecoms & Internet converged Services & Protocols for Advanced Networks). In this case, when a subscriber has access to an access network and network connection authentication succeeds, a subscriber having the same line information is authenticated in a service network without a special authentication key exchange mechanism.

[5] Currently, in documents of ITU-T and TISPAN, SCF (Service Control Function) which takes charge in control, registration, authentication, and authorization of session at a service level needs NACFs (Network Attachment Control Functions) which provides an identification/authentication function of a network level to subscribers who try to access to an NGN service for registration function, to retrieve line information using an IP (Internet Protocol) address as a key in order to obtain physical line information. In normal cases, various NACFs exist in one SCF. However, there is no special mention on which NACF the SCF selects.

[6] According to conventional SCF-NACF bundle authentication, when access authentication that is managed by a specific NACF only for fixed subscribers, succeeds and when a terminal requests a service user ID (Identifier), i.e., PUID (PUblic user ID) or

PRID (PRivate user ID), subscribed to SCF-NACF bundle authentication, using an IP address and a realm in which access authentication succeed, service authentication also succeeds. This is because of the following four conditions.

[7] When access authentication succeeds, one IP address and one realm are allocated to a subscriber ID that succeeds access network connection for each line ID. P-CSC-FE (Proxy Call Session Control Functional Entity) obtains an IP and a realm which are a service user ID, from a terminal and obtains a line ID from TLM-FE (Transport Location Management Functional Entity) using the IP and realm. When predetermined SCF and NACF are bundle-subscribed to SUP-FE (Service User Profile Functional Entity), a line ID of the NACF is stored previously for a service user ID (a predetermined line ID is fixed to a fixed subscriber). S-CSC-FE (Service Call Session Control Functional Entity) determines for authentication whether the line ID received from P-CSC-FE and the line ID received from SUP-FE are the same or not.

[8] Furthermore, an NACF-SCF bundle authentication scheme in documents of ITU-T and TISPAN is based on lines and thus can be applied only to a fixed network such as xDSL. Thus, the NACF-SCF bundle authentication scheme cannot be used in WLAN (wireless LAN) or WiBro network in which the terminal is moved.

Disclosure of Invention

Technical Problem

[9] The present invention provides node authentication and node operation methods within service and access networks for SCF-NACF bundle authentication by registering a TLM-FE address of NACF in P-CSC-FE.

Technical Solution

[10] According to an aspect of the present invention, there is provided a method of authentication processing of a node (S-CSC-FE/I-CSC-FE (Serving Call Session Control Functional Entity/Interrogating Call Session Control Functional Entity)) within a service network for bundle authentication between service and access networks, the method including: receiving first authentication information about access authentication of a terminal from a first node within the service networks; requesting to receive second authentication information from a second node within the service network based on the first authentication information; and comparing the first authentication information with the second authentication information to authenticate the terminal.

[11] According to another aspect of the present invention, there is provided a method of operating a node (TAA-FE (Transport Authentication & Authorization Functional Entity)/TUP-FE (Transport User Profile Functional Entity)) within an access network for bundle authentication between service and access networks, the method including :

performing access authentication on a terminal that tries to access the access network; determining whether or not the terminal subscribes to a bundle of the service and access networks; and when it is checked that the terminal subscribes to the bundle of the service and access networks, transmitting first and second authentication information to the access network and the service network, respectively.

[12] According to another aspect of the present invention, there is provided a method of operating a node (P-CSC-FE (Proxy Call Session Control Functional Entity)) within a service network for bundle authentication between service and access networks, the method including : receiving authentication information when access authentication is performed on a terminal in the access network; determining whether or not the authentication information corresponding to the terminal exists when the terminal accesses the service network; and when it is determined that the authentication information does not exit, requesting the authentication information to the access network and receiving the authentication information.

Advantageous Effects

[13] According to the present invention, NACF-SCF bundle authentication can be performed regardless of a wired or wireless access in an NGN. The prior art is capable of NACF-SCF bundle authentication only at a wired access. On the other hand, the present invention can be applied to wired or wireless subscribers. Furthermore, by using the present invention, when a subscriber subscribes to NACF-SCF authentication in an NGN, if access authentication in NACF succeeds, an additional authentication procedure is simplified, and due to a simplified service authentication procedure, a service user can omit an operation of additionally inputting a password.

Description of Drawings

[14] The above and other features and advantages of the present invention will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings in which:

[15] FIG. 1 illustrates a configuration of a system to which embodiments of the present invention are applied;

[16] FIG. 2 is a flowchart illustrating a method of bundle authentication of a wired or wireless terminal between service and access networks in a next generation network (NGN) according to an embodiment of the present invention; and

[17] FIG. 3 is a flowchart illustrating a method of bundle authentication of a wired or wireless terminal between service and access networks using a bundle authentication management server in a next generation network (NGN).

Mode for Invention

[18] FIG. 1 illustrates a configuration of a system to which embodiments of the present

invention are applied.

[19] Referring to FIG. 1, the system comprises an NGN terminal unit 10, a connection unit 11, an NACF unit 12, and an SCF unit 13. The system may further comprise a bundle authentication server manager 14, if necessary. Reference numerals 15 and 16 denote wired or wireless communication networks. There may be a plurality of wired or wireless communication network 15 and 16 and thus, there may be a plurality of NACF units 12 and SCF units 13.

[20] The NGN terminal unit 10 comprises a WLAN terminal 101, a WiBro terminal 102, a cable terminal 103, and an asymmetric digital subscriber line (ADSL) terminal 104.

[21] The connection unit 11 comprises an access point (AP) 111 connected to the WLAN terminal 101, a remote access server (RAS) 112 connected to the WiBro terminal 102, and a cable modem (CM) unit 113 connected to the cable terminal 103 and comprising a CM and a cable modem termination system (CMTS), which are devices for packet connection of each NGN terminal. The ADSL terminal 104 is connected to the wired or wireless communication network 16 via an ADSL line.

[22] The NACF unit 12 which is an access control network, takes charge in IP address allocation and connection authentication for connection. The NACF unit 12 comprises AM-FE (Access Management Functional Entity) 121 for access management, TLM-FE (Transport Location Management Functional Entity) 122 for transport location management, and TAA-FE (Transport Authentication & Authorization Functional Entity)/TUP-FE (Transport User Profile Functional Entity) 123 for authentication.

[23] The SCF unit 13 which is a service control network, takes charge in service routing and service authentication. The SCF unit 13 comprises P-CSC-FE (Proxy Call Session Control Functional Entity) 131, S-CSC-FE/I-CSC-FE (Serving Call Session Control Functional Entity/Interrogating Call Session Control Functional Entity) 132, SAA-FE (Service Authentication & Authorization Functional Entity)/SUP-FE (Service User Profile Functional Entity) 133.

[24] The bundle authentication management server 14 takes charge in authentication information exchange between the NACF unit 12 and the SCF unit 13 and stores a service user ID corresponding to a subscriber ID when a subscriber subscribes to a bundle.

[25] FIG. 2 is a flowchart illustrating a method of bundle authentication of a wired or wireless terminal between service and access networks in a next generation network (NGN) according to an embodiment of the present invention.

[26] First, a terminal of the NGN terminal unit 10 is access-authenticated by the TAA-FE/TUP FE 123 through the AM FE 121 (operation 20). If authentication succeeds, the TAA-FE/TUP FE 123 determines whether the corresponding subscriber subscribes to an NACF-SCF bundle service (operation 21) or not. If the subscriber subscribes to the

NACF-SCF bundle service, the TAA-FE/TUP FE 123 transfers authentication information to the TLM-FE 122 using a global IP address as a key, and the TLM-FE 122 sends the authentication information and its own address to the P-CSC-FE 131 (operation 22). In addition, the TAA-FE/TUP FE 123 sends the authentication information to the SAA-FE/SUP FE 133 using a subscriber ID as a key (operation 37). Here, the SAA-FE/SUP FE 133 stores a service user ID corresponding to the subscriber ID when the subscriber subscribes to a bundle.

[27] If the subscriber also subscribes to NGN SCF and tries service registration authentication, a subscriber terminal transfers a session initiation protocol (SIP) register message to the P-CSC-FE 131 (operation 23).

[28] The P-CSC-FE 131 inspects whether the service user subscribes to an NACF-SCF bundle (operation 24) or not. The inspection operation is performed by determining whether there is effective access authentication information to be mapped to the global IP address of the terminal or not. If there is no effective access authentication information, the P-CSC-FE 131 requests authentication information to the TLM-FE 122 using an address of the TLM-FE 122 (operation 25) and obtains the authentication information from the TLM-FE 122 (operation 26).

[29] The P-CSC-FE 131 inserts the authentication information to an SIP register message and sends the SIP register message to the S-CSC-FE/I-CSC-FE 132 (operation 27). In this case, the SIP register message comprises PUID and PRID obtained from the subscriber when the subscriber subscribes to the bundle.

[30] The S-CSC-FE/I-CSC-FE 132 sends an MAR (Multimedia Authentication Request) message requesting bundle authentication and authentication information registered in the SAA-FE/SUP-FE 133 to the SAA-FE/SUP-FE 133 using PUID and PRID included in the SIP register message as a key (operation 28) and obtains an MAA (Multimedia Authentication Answer) message including the authentication information (operation 29).

[31] The S-CSC-FE/I-CSC-FE 132 compares to determine whether the authentication information obtained from the TLM-FE 122 and the authentication information obtained from the SAA-FE/SUP-FE 133 are the same or not (operation 30). If two authentication information are not the same, it is determined that authentication fails and failure of the terminal authentication is notified to the terminal of the NGN terminal unit 10 through the P-CSC-FE 131 (operation 31). If the authentication succeeds, the S-CSC-FE/I-CSC-FE 132 registers S-CSC-FE information to which a user terminal belongs, in the SAA-FE/SUP-FE 133 using an SAR (Server Assignment Request) message (operation 32) and receives a profile and billing information of the service user from the SAA-FE-SUP-FE 133 using an SAA (Server Assignment Answer) message (operation 33).

[32] The S-CSC-FE/I-CSC-FE 132 sends a service registration success message for the SIP register to the subscriber terminal through the P-CSC-FE 131 (operation 34).

[33] FIG. 3 is a flowchart illustrating a method of bundle authentication of a wired or wireless terminal between service and access networks using a bundle authentication management server in a NGN. In FIG. 3, operations having the same reference numerals as those of FIG. 2 are the same as operations of FIG. 2. Thus, a detailed description thereof will be omitted, and only operations having different reference numerals will now be described.

[34] In operation 22 of FIG. 2, the TAA-FE/TUP-FE 123 transfers the authentication information to a bundle authentication management server 14 using a subscriber ID as a key (operation 45). The TAA-FE/TUP FE 123 sends the authentication information to the bundle authentication management server 14 using the subscriber ID as the key (operation 46). Here, the bundle authentication management server 14 stores a service user ID corresponding to the subscriber ID received when a subscriber subscribes to a bundle.

[35] Furthermore, in operation 28 of FIG. 2, if the S-CSC-FE/I-CSC-FE 132 requests a result of whether the bundle authentication is performed and the authentication information to the SAA-FE/SUP-FE 133 using an MAR message, the SAA-FE/SUP-FE 133 transmits PRID or PUID to the bundle authentication management server 14 and requests the authentication information (operation 40). The bundle authentication management server 14 transfers the authentication information for the corresponding subscriber to the SAA-FE/SUP-FE 133, and the SAA-FE/SUP-FE 133 inserts the authentication information to an MAA message and sends the MAA message to the S-CSC-FE/I-CSC-FE 132 (operation 41).

[36] The S-CSC-FE/I-CSC-FE 132 compares to determine whether the authentication information obtained from the TLM-FE 122 and the authentication information obtained from the bundle authentication management server 14 are the same or not (operation 42). If two authentication information are not the same, it is determined that authentication fails and failure of terminal authentication is notified to the terminal of the NGN terminal unit 10 through the P-CSC-FE 131 (operation 31). If the authentication succeeds, the S-CSC-FE/I-CSC-FE 132 registers S-CSC-FE information to which a user terminal belongs, in the SAA-FE/SUP-FE 133 using an SAR message (operation 43) and receives a profile and billing information of the service user from the SAA-FE-SUP-FE 133 using an SAA message (operation 44).

[37] The S-CSC-FE/I-CSC-FE 132 sends a service registration success message for an SIP register to the subscriber terminal through the P-CSC-FE 131 (operation 34).

[38] The following Table 1 shows an example in which a subscriber ID, an IP address, a Realm, bundle information between access and service networks, an access authen-

tication scheme, an authentication context, and a line ID are stored in a database of the TAA-FE/TUP-FE 123 of FIG. 1.

[39] Table 1

[40] [Table 1]

[Table]

Subscriber ID	IP Address	Realm	Bundle Information	Access Authentication Scheme	Authentication Context	Line ID
sub1@etri.re.kr	123.456.789.123	etri.com	Line-based SCF-NACF	EAP-AKA	RAND||AUTN||XRES||CK||IK	xDSL line
sub1@etri.re.kr	123.456.789.124	etri.com	Authentication information-based SCF-NACF		nonce||response	
sub2@etri.re.kr	123.456.789.124	etri.com	Unsubscribed		RAND||AUTN||XRES||CK||IK	
…	…	…	…	…	…	…

[41] According to Table 1, one subscriber ID and authentication-related information are matched in the format of a lookup table.

[42] The following Table 2 shows an example in which PRID, PUID, an IP address, a Realm, bundle information between access and service networks, a service authentication scheme, an authentication context, a line ID, and effective time are stored in a database of P-CSC-FE 131 of FIG. 1.

[43] Table 2

[44]

[Table 2]

[Table]

PRID	PUID	IPAddress	Realm	Bundle Information	Service Authentication Scheme	Authentication Context	Line ID	Effective Time
user1@etri.re.kr	sip:user1@etri.re.kr	123.456.789.123	etri.com	Line-based SCF-NACF	Line-based SCF-NACF		xDSL line	60
user1@etri.re.kr	tel:01123456789	123.456.789.124	etri.com	Authentication information-based SCF-NACF	Authentication Information-based SCF-NACF	RAND||AUTN||XRES||CK||IK		50
user2@etri.re.kr	sip:user2@etri.re.kr	123.456.789.124	etri.com	Unsubscribed	Digest-MD5			
…	…	…	…	…	…	…	…	…

[45] In Table 2, PRID and PUID are keys.

[46] The following Table 3 shows an example in which PRID, PUID, a subscriber ID, an IP address, an Realm, bundle information between access and service scheme, a service authentication method, an authentication context, a line ID, and effective time are stored in a database of S-CSC-FE/I-CSC-FE 132 of FIG. 1.

[47] Table 3

[48]

[Table 3]

[Table]

PRID	PUID	Bundle Information	Service Authentication Scheme	Authentication Context	Line ID	Effective Time
user1@etri.re.kr	sip:user1@etri.re.kr	Line-based SCF-NACF	Line-based SCF-NACF		xDSL line	60
user1@etri.re.kr	tel:01123456789	Authentication Information-based SCF-NACF	Authentication Information-based SCF-NACF	RAND||AUTN||XRES||CK||IK		50
user2@etri.re.kr	sip:user2@etri.re.kr	Unsubscribed	Digest-MD5			
…	…	…	…	…	…	…

[49] The following Table 4 shows an example in which PRID, PUID, a subscriber ID, a Realm, bundle information between access and service networks, a service authentication method, an authentication context, a line ID, and effective time are stored in a database of S-CSC-FE/I-CSC-FE 132 of FIG. 1.

[50] Table 4

[51]

[Table 4]

[Table]

PRID	PUID	Subscriber ID	Bundle Information	Service Authentication Scheme	Authentication Context	Line ID	Effective Time
user1@etri.re.kr	sip:user1@etri.re.kr	sub1@etri.re.kr	Line-based SCF-NACF	Line-based SCF-NACF		xDSL line	60
user1@etri.re.kr	tel:01123456789	sub1@etri.re.kr	Authentication Information-based SCF-NACF	Authentication Information-based SCF-NACF	RAND||AUTN| XRES||CK||IK		50
user2@etri.re.kr	sip:user2@etri.re.kr	sub2@etri.re.kr	Unsubscribed	Digest-MD5			
…	…	…	…	…	…	…	…

[52] The following Table 5 shows an example in which PRID, PUID, a subscriber ID, a Realm, bundle information between access and service networks, an access authentication method, an authentication context, a line ID, and effective time are stored in a database of the bundled authentication management server 14 of FIG. 1.

[53] Table 5

[54]

[Table 5]

[Table]

PRID	PUID	Subscriber ID	Bundle Information	Access Authentication Scheme	Authentication Context	Line ID	Effective Time
user1@etri.re.kr	sip:user1@etri.re.kr	sub1@etri.re.kr	Line-based SCF-NACF	EAP-AKA	RAND||AUTN||XRES||CK||IK	XDSL line	60
user1@etri.re.kr	tel:01123456789	sub1@etri.re.kr	Authentication Information-based SCF-NACF	EAP-AKA	RAND||AUTN||XRES||CK||IK		50
user2@etri.re.kr	sip:user2@etri.re.kr	sub2@etri.re.kr	Unsubscribed				
…	…	…	…	…	…	…	…

[55] The invention can also be embodied as computer readable codes on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data which can be thereafter read by a computer system. Examples of the computer readable recording medium include read-only memory (ROM), random-access memory (RAM), CD-ROMs, magnetic tapes, floppy disks, optical data storage devices, and carrier waves (such as data transmission through the Internet). The computer readable recording medium can also be distributed over network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

[56] While this invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the appended claims. Therefore, the scope of the invention is defined only by the appended claims, and all differences within the scope will be construed as being included in the present invention.

Claims

[1] A method of authentication processing of a node (S-CSC-FE/I-CSC-FE (Serving Call Session Control Functional Entity/Interrogating Call Session Control Functional Entity)) within a service network for bundle authentication between service and access networks, the method comprising:
receiving first authentication information about access authentication of a terminal from a first node within the service networks;
requesting to receive second authentication information from a second node within the service network based on the first authentication information; and
comparing the first authentication information with the second authentication information to authenticate the terminal.

[2] The method of claim 1, wherein, in the first authentication information, a a global IP (Internet Protocol) address of the terminal is used as a key, and in the second authentication information, a subscriber ID is used as a key.

[3] A method of operating a node (TAA-FE (Transport Authentication & Authorization Functional Entity)/TUP-FE (Transport User Profile Functional Entity)) within an access network for bundle authentication between service and access networks, the method comprising :
performing access authentication on a terminal that tries to access the access network;
determining whether or not the terminal subscribes to a bundle of the service and access networks; and
when it is checked that the terminal subscribes to the bundle of the service and access networks, transmitting first and second authentication information to the access network and the service network, respectively.

[4] The method of claim 3, wherein the first and second authentication information are outputted using a global IP (Internet Protocol) address of the terminal as a key and using a subscriber ID as a key, respectively.

[5] A method of operating a node (P-CSC-FE (Proxy Call Session Control Functional Entity)) within a service network for bundle authentication between service and access networks, the method comprising :
receiving authentication information when access authentication is performed on a terminal in the access network;
determining whether or not the authentication information corresponding to the terminal exists when the terminal accesses the service network; and
when it is determined that the authentication information does not exit, requesting the authentication information to the access network and receiving the

authentication information

[6] The method of claim 5, wherein the authentication information is access authentication information that is outputted using a global IP (Internet Protocol) address of the terminal as a key and is mapped to the global IP address.

FIG. 1

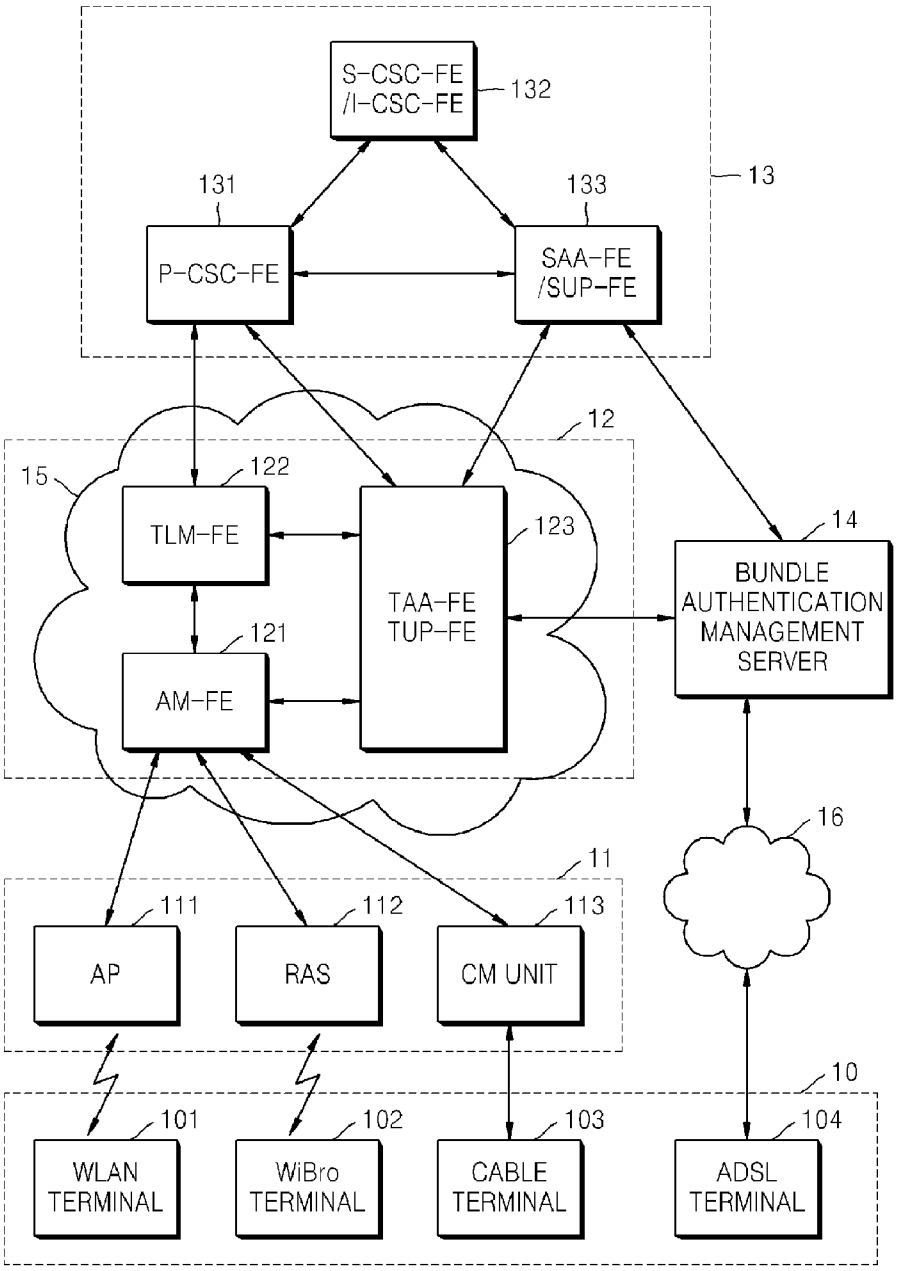

S-CSC-FE
/I-CSC-FE
132
131
133
13
P-CSC-FE
SAA-FE
/SUP-FE
12
15
122
TLM-FE
123
14
BUNDLE
AUTHENTICATION
MANAGEMENT
SERVER
TAA-FE
TUP-FE
121
AM-FE
16
11
111
112
113
AP
RAS
CM UNIT
10
101
102
103
104
WLAN
TERMINAL
WiBro
TERMINAL
CABLE
TERMINAL
ADSL
TERMINAL

FIG. 2

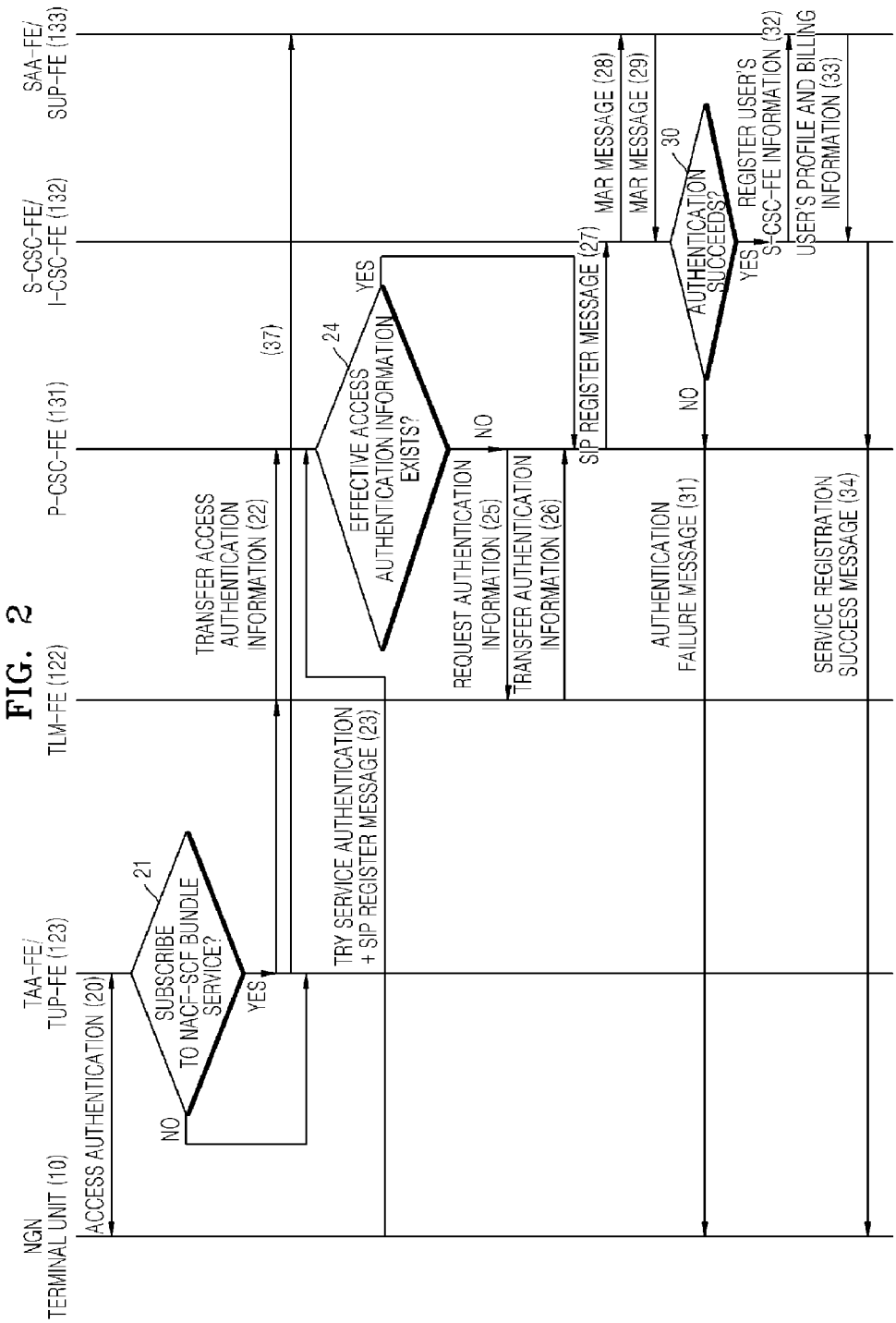
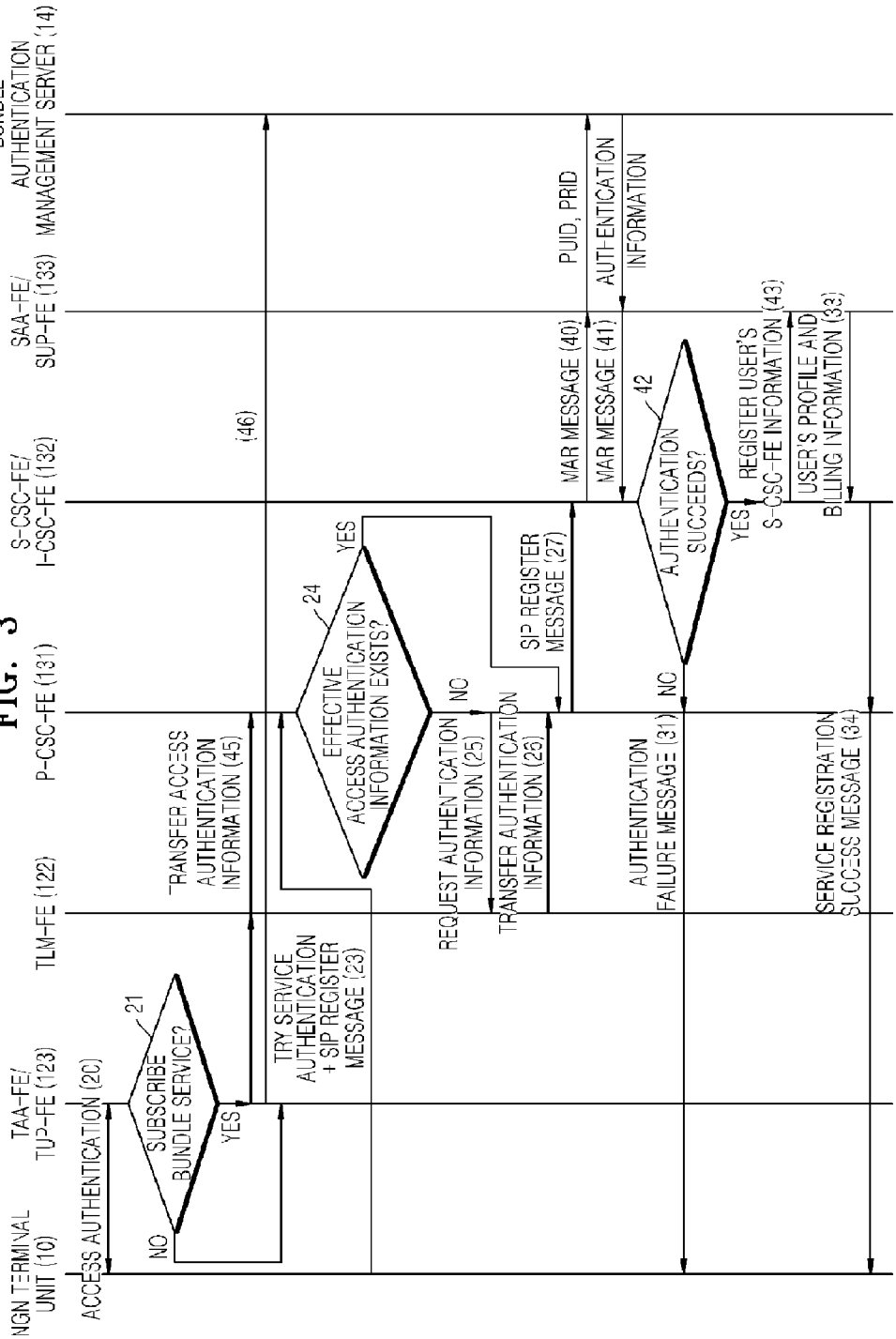

NGN TERMINAL UNIT (10)
TAA-FE/ TUP-FE (123)
TLM-FE (122)
P-CSC-FE (131)
S-CSC-FE/ I-CSC-FE (132)
SAA-FE/ SUP-FE (133)
ACCESS AUTHENTICATION (20)
21
SUBSCRIBE TO NACF-SCF BUNDLE SERVICE?
NO
YES
TRANSFER ACCESS AUTHENTICATION INFORMATION (22)
TRY SERVICE AUTHENTICATION + SIP REGISTER MESSAGE (23)
(37)
24
EFFECTIVE ACCESS AUTHENTICATION INFORMATION EXISTS?
YES
NO
REQUEST AUTHENTICATION INFORMATION (25)
TRANSFER AUTHENTICATION INFORMATION (26)
SIP REGISTER MESSAGE (27)
MAR MESSAGE (28)
MAR MESSAGE (29)
30
AUTHENTICATION SUCCEEDS?
NO
YES
AUTHENTICATION FAILURE MESSAGE (31)
REGISTER USER'S S-CSC-FE INFORMATION (32)
USER'S PROFILE AND BILLING INFORMATION (33)
SERVICE REGISTRATION SUCCESS MESSAGE (34)

FIG. 3


NGN TERMINAL UNIT (10)
TAA-FE/ TUP-FE (123)
TLM-FE (122)
P-CSC-FE (131)
S-CSC-FE/ I-CSC-FE (132)
SAA-FE/ SUP-FE (133)
BUNDLE AUTHENTICATION MANAGEMENT SERVER (14)
ACCESS AUTHENTICATION (20)
21
SUBSCRIBE BUNDLE SERVICE?
NO
YES
TRANSFER ACCESS AUTHENTICATION INFORMATION (45)
TRY SERVICE AUTHENTICATION + SIP REGISTER MESSAGE (23)
24
EFFECTIVE ACCESS AUTHENTICATION INFORMATION EXISTS?
YES
NO
REQUEST AUTHENTICATION INFORMATION (25)
TRANSFER AUTHENTICATION INFORMATION (26)
SIP REGISTER MESSAGE (27)
(46)
PUID, PRID
MAR MESSAGE (40)
MAR MESSAGE (41)
AUTHENTICATION INFORMATION
42
AUTHENTICATION SUCCEEDS?
YES
NO
REGISTER USER'S S-CSC-FE INFORMATION (43)
USER'S PROFILE AND BILLING INFORMATION (33)
AUTHENTICATION FAILURE MESSAGE (31)
SERVICE REGISTRATION SUCCESS MESSAGE (34)