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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 September 2010 (16.09.2010)

PCT

(10) International Publication Number
WO 2010/104283 A2

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)

(21) International Application Number:
PCT/KR2010/001356

(22) International Filing Date:
4 March 2010 (04.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2009-0020096 10 March 2009 (10.03.2009) KR
10-2009-0058150 29 June 2009 (29.06.2009) KR

(71) Applicant *(for all designated States except US)*: **KT CORPERATION** [KR/KR]; 206, Jungja-dong, Bundang-gu, Seongnam-city, Kyeonggi-do 463-711 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LEE, Duc-Key** [KR/KR]; 17, Umyeon-dong, Seocho-gu, Seoul 137-900 (KR). **BANG, Jung-Hee** [KR/KR]; 17, Umyeon-dong, Seocho-gu, Seoul 137-900 (KR).

(74) Agent: **SHINSUNG PATENT FIRM**; ID Tower #601, Jungdaero 105, (99-7 Garak-dong), Songpa-gu, Seoul 138-805 (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, 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, 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, RO, RS, RU, 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.

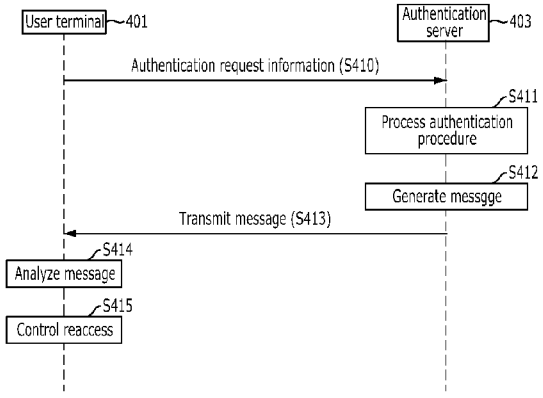
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, 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 (Rule 48.2(g))*

(54) Title: METHOD FOR USER TERMINAL AUTHENTICATION AND AUTHENTICATION SERVER AND USER TERMINAL THEREOF

[Fig. 4]



(57) Abstract: Provided are a method for user terminal authentication and authentication server and user terminal thereof. The method includes receiving authentication request information for accessing a network from the user terminal, processing a EAP authentication procedure according to the authentication request information, transmitting a message related to the EAP authentication procedure to the user terminal, wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

WO 2010/104283 A2

Description

Title of Invention: METHOD FOR USER TERMINAL AUTHENTICATION AND AUTHENTICATION SERVER AND USER TERMINAL THEREOF

Technical Field

[1] The present invention relates to a method for user terminal authentication; and more particularly, to a method for user terminal authentication, and an interface server and a user terminal using the same.

[2]

Background Art

[3] Due to the development of a communication system, various types of networks have been realized. An environment including multiple types of networks is referred to as a multi-network environment. In the multi-network environment, a user terminal may access one of networks such as a Wireless Local Area Network (WLAN) network, a Code Division Multiple Access (CDMA) network, and a World Interoperability for Microwave Access (WiMAX) network.

[4] Hereinafter, the WiMAX network will be exemplary described as one of the representative communication networks. The WiMAX network provides a communication service that enables a user to access the Internet at a high speed and to receive data or multimedia contents not only in an indoor place but also at the outside and even during travelling using various types of user terminals such as a personal computer, a notebook computer, a personal digital assistant (PDA), a portable multimedia player (PMP), a handset, and a smart phone.

[5] Such a WiMAX service enables a user to use the Internet even in the outdoor place such as streets, parks, and vehicles in travelling unlike a high speed internet service that enables a user to use the Internet only at an indoor place with an internet cable is installed such as home, a school, and an office.

[6] A WiMAX forum has been established by communication service providers, communication equipments manufacturers, and semiconductor manufacturers in order to secure comparability among equipment employing a WiMAX technology. The WiMAX forum uses an Institute of Electrical and Electronics Engineers (IEEE) standard 802.16 of a wide band wireless access technology as a fundamental technology. The WiMAX forum has been trying to advance a related technology from a stationary standard 802.16d to a mobile standard 802.16e.

[7] The WiMAX network is a wireless metropolitan area network (WMAN) technology based on IEEE 802.16 standard. In general, the WiMAX network includes an access

service network (ASN) and a connectivity service network (CSN). The access service network (ASN) includes a user terminal such as a mobile station (MS) which is a client, a base station (BS), and an access service network gateway (ASN-GW). The connectivity service network (CSN) includes logical entities such as a policy function (PF) entity, an authentication authorization and accounting (AAA) server, and an application function (AF) entity.

[8] Hereinafter, a logical structure of a WiMAX network will be described.

[9] The mobile station (MS) is referred to as a WiMAX terminal that accesses the ASN through a wireless link. An IEEE 802.16D/E standard WMAN access technology is mainly used at a wireless side of a WiMAX network.

[10] The ASN guarantees establishing connection between a WiMAX terminal and a WiMAX base station (BS). The ASN manages wireless resources, finds a network, selects an optimal a network service provider (NSP) for a WiMAX subscriber, operates as a proxy server for controlling authentication authorization and accounting (AAA) of a WiMAX subscriber in a proxy mobile intern protocol (MIP), and accesses an application through a WiMAX terminal.

[11] The CSN allocates an Internet protocol (IP) address for a session of a WiMAX subscriber, provides access for Internet, operates as an AAA proxy or an AAA server, performs a policy and controls access based on the subscribing data of a subscriber, supports establishing a tunnel between the ASN and the CSN, generates an invoice for a WiMAX subscriber, supports a policy of a WiMAX service through an operator, supports forming a loaming tunnel between CSNs, supports mobility between ASNs, provides a location based service, provides an end-to-end service, and supports various WiMAX services such as multimedia broadcast service and a multimedia broadcast multicast service (MBMS).

[12] Fig. 1 is a diagram illustrating a network system according to the related art.

[13] Referring to Fig. 1, the network system according to the related art includes a user terminal 110, a communication system 120, an Internet network 130, and an application service provider 140.

[14] The user terminal 110 is any devices that can access a network including a communication system. For example, the user terminal 110 may be a notebook computer, a personal computer, a personal digital assistant (PDA), a hand set, or a personal multimedia player (PMP).

[15] The communication system 120 includes a base station 121 or a radio access station (RAS) for controlling connection of a physical communication channel, an Access Service Network Gate Way (ASN-GW) 122 or Base Station Controller/Serving GPRS Supporting Node (BSC/SGSN) for controlling Medium Access Control (MAC) of an access network, Connectivity Service Network (CSN) 123 or Packet Data Service

Node/ Gateway GPRS Support Node (PDSN/GGSN) for controlling connection of a network layer. The communication system 120 may further include a location information server (LIS), a device capability server, a user profile server, a quality of service server (QoS), and a billing server.

[16] The application service provider 140 has servers for providing a predetermined service to the user terminal 110. The application service provider 140 may include an Internet Protocol Television (IPTV) server for providing an Internet based television programs to a user terminal 110 accessing the Internet network 130, a contents server for providing music/video contents in real time, a search engine server for providing a result of a search inquiry in response to a request of the user terminal 110, an advertisement server for providing advertisement, and a service server 139 for providing services.

[17] Extensible Authentication Protocol (EAP) is defined in a Request for Comments or Remote Function Call (RFC) standard by Internet Engineering Task Force (IETF). EAP is a protocol for performing authentication when a user terminal accesses the Internet. EAP has been widely used in various types of networks such as a wireless local area network and a WiBRO (WiMAX) network. An EAP authentication server authenticates a user terminal using various EAP methods such as TLS, TTLS, and AKA. In case of the success of authentication, the EAP authentication server transfers an EAP-Success message to a user terminal through a Network Access Server (NAS) disposed between the user terminal and the authentication server. In case of the failure of authentication, the EAP authentication server transfers an EAP-Failure message to the user terminal.

[18] When the EAP-failure message is received, the user terminal is denied to access the Internet by a network access server (NAS). In general, the user terminal automatically retries access to the Internet several times. When the user terminal finally fails to access the Internet, the user terminal enters to a waiting state for waiting input from a user. Since there is no standard defined for re-access after authentication failure, the number of retry times for re-access or an interval for re-access in a user terminal is determined by an algorithm or a policy defined by a user terminal manufacturer.

[19] According to causes of authentication failure, a user terminal may finally grant authentication through retrying re-access. However, a user terminal could continuously fail to grant authentication through numerous re-access tries. When the authentication failure repeats because the user terminal automatically tires re-access, it may generate significantly large load in related networks and authentication servers.

[20] In general, the user terminal is not informed why an authentication server denies the network access of the user terminal. Therefore, the user terminal automatically tires re-accessing in case of authentication failure. Therefore, if the user terminal is informed

of a reason of network access failure with instructions for re-access from the authentication server, it is possible to significantly reduce load in the networks and the authentication servers.

[21]

Disclosure of Invention

Technical Problem

[22] An embodiment of the present invention is directed to providing a method for user terminal authentication that provides network access denying reasons to a user terminal.

[23] An embodiment of the present invention is directed to providing a method for user terminal authentication that provides reaccess instructions to a user terminal according to network access denying reasons in order to reduce unnecessary re-access tries and significantly reduce load in an authentication server.

[24] An embodiment of the present invention is directed to providing a method for user terminal authentication that prevents a serious security problem when network access denying reasons and reaccess instructions are forged or modulated.

[25] Other objects and advantages of the present invention can be understood by the following description, and become apparent with reference to the embodiments of the present invention. Also, it is obvious to those skilled in the art of the present invention that the objects and advantages of the present invention can be realized by the means as claimed and combinations thereof.

[26]

Solution to Problem

[27] In accordance with an aspect of the present invention, there is provided a method for authenticating a user terminal, including: receiving authentication request information for accessing a network from the user terminal; processing a EAP authentication procedure according to the authentication request information; and transmitting a message related to the EAP authentication procedure to the user terminal, wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[28] In accordance with another aspect of the present invention, there is provided an apparatus for authenticating a user terminal, including: a receiver configured to receive authentication request information from the user terminal to access a network; an EAP authentication procedure processor configured to process an authentication procedure according to the authentication request information; and a transmitter configured to transmit a message related to the EAP authentication procedure to the user terminal,

wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for a user terminal to cope with the network rejection.

[29] In accordance with another aspect of the present invention, there is provided a method for authenticating a user terminal, including: transmitting authentication request information for accessing a network to an authentication server; and receiving a message related to an EAP authentication procedure processed according to the authentication request information from the authentication server, wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[30] In accordance with another aspect of the present invention, there is provided an apparatus apparatus for authenticating a user terminal, including: a transmitter configured to transmit authentication request information for accessing a network to an authentication server; and a receiver configured to receive a message related to an EAP authentication procedure processed according to the authentication request information from the authentication server, wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[31] In accordance with another aspect of the present invention, there is provided a method for authenticating a user terminal, including: receiving authentication request information for accessing a network from the user terminal; processing an EAP-TLS authentication procedure according to the authentication request information; and transmitting a EAP-Request/Notification message related to the EAP-TLS authentication procedure to the user terminal, wherein the EAP-Request/Notification message includes the network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[32] In accordance with another aspect of the present invention, there is provided a method for authenticating a user terminal, including: receiving authentication request information for accessing a network from the user terminal; processing an EAP-TTLS authentication procedure according to the authentication request information; and transmitting a EAP-Request/Notification message related to the EAP-TTLS authentication procedure to the user terminal, wherein the EAP-Request/Notification message includes the network rejection information when network rejection related to authentication failure or authorization failure is triggered during the the EAP-TTLS authen-

tication procedure, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[33] In accordance with another aspect of the present invention, there is provided a method for authenticating a user terminal, including: receiving authentication request information for accessing a network from the user terminal; processing an EAP-AKA authentication procedure according to the authentication request information; and transmitting a EAP-Request/Notification message related to the EAP-AKA authentication procedure to the user terminal, wherein the EAP-Request/Notification message includes the network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[34] In accordance with another aspect of the present invention, there is provided a computer readable recording medium storing a method for authenticating a user terminal, the method including: processing an EAP authentication procedure according to authentication request information from a user terminal for accessing a network; and generating a message including result information according to the EAP authentication procedure, wherein the result information includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[35] In accordance with another aspect of the present invention, there is provided a computer readable recording medium storing a method for authenticating a user terminal, the method including: generating authentication request information for accessing a network; and analyzing a message including result information of an EAP authentication procedure processed according to the authentication request information received from the authentication server, wherein the result information includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

Advantageous Effects of Invention

[36] A method for user terminal authentication according to the present invention can reduce load in a network and an authentication server by effectively controlling accessing a network when a user terminal fails to grant authentication of accessing a network.

[37] Further, the method for user terminal authentication according to the present invention can provide integrity protection as solution to overcome a serious security

problem that may be caused by forging or modulating network access denying reasons and reaccess instructions provided to a user terminal.

[38]

Brief Description of Drawings

[39] Fig. 1 is a diagram illustrating a network system according to the related art.

[40] Fig. 2 is a diagram illustrating a procedure of a user terminal for accessing a network.

[41] Fig. 3 is a diagram illustrating a procedure of a user terminal for accessing a network in case of authentication failure.

[42] Fig. 4 is a diagram illustrating a network access rejection procedure in an EAP authentication process when a user terminal is failed to be authenticated for accessing a network.

[43] Fig. 5 is a diagram illustrating an authentication server in accordance with an embodiment of the present invention.

[44] Fig. 6 is a diagram illustrating a user terminal in accordance with an embodiment of the present invention.

[45] Fig. 7 is a diagram illustrating a network access rejection procedure in EAP-TLS.

[46] Fig. 8 is a diagram illustrating a network access rejection procedure in EAP-TTLS.

[47] Fig. 9 is a diagram illustrating a network access rejection procedure in EAP-AKA.

[48]

Best Mode for Carrying out the Invention

[49] Following description exemplifies only the principles of the present invention. Even if they are not described or illustrated clearly in the present specification, one of ordinary skill in the art can embody the principles of the present invention and invent various apparatuses within the concept and scope of the present invention. The use of the conditional terms and embodiments presented in the present specification are intended only to make the concept of the present invention understood, and they are not limited to the embodiments and conditions mentioned in the specification.

[50] Also, all the detailed description on the principles, viewpoints and embodiments and particular embodiments of the present invention should be understood to include structural and functional equivalents to them. The equivalents include not only currently known equivalents but also those to be developed in future, that is, all devices invented to perform the same function, regardless of their structures.

[51] For example, block diagrams of the present invention should be understood to show a conceptual viewpoint of an exemplary circuit that embodies the principles of the present invention. Similarly, all the flowcharts, state conversion diagrams, pseudo codes and the like can be expressed substantially in a computer-readable media, and whether or not a computer or a processor is described distinctively, they should be un-

derstood to express various processes operated by a computer or a processor.

[52] Functions of various devices illustrated in the drawings including a functional block expressed as a processor or a similar concept can be provided not only by using hardware dedicated to the functions, but also by using hardware capable of running proper software for the functions. When a function is provided by a processor, the function may be provided by a single dedicated processor, single shared processor, or a plurality of individual processors, part of which can be shared.

[53] The apparent use of a term, 'processor', 'control' or similar concept, should not be understood to exclusively refer to a piece of hardware capable of running software, but should be understood to include a digital signal processor (DSP), hardware, and ROM, RAM and non-volatile memory for storing software, implicatively. Other known and commonly used hardware may be included therein, too.

[54] In the claims of the present specification, an element expressed as a means for performing a function described in the detailed description is intended to include all methods for performing the function including all formats of software, such as combinations of circuits for performing the intended function, firmware/microcode and the like.

[55] To perform the intended function, the element is cooperated with a proper circuit for performing the software. The present invention defined by claims includes diverse means for performing particular functions, and the means are connected with each other in a method requested in the claims. Therefore, any means that can provide the function should be understood to be an equivalent to what is figured out from the present specification.

[56] Hereinafter, a procedure of a user terminal for accessing a network will be described.

[57] Fig. 2 is a diagram illustrating a procedure of a user terminal for accessing a network. In order to describe the procedure of a user terminal for accessing a network, a WiMAX network is exemplarily described in Fig. 2. Fig. 2 describes the procedure of a user terminal for accessing a network based on an EAP authentication procedure between a user terminal and a network when a user terminal initially accesses a network.

[58] As shown in Fig. 2, the network includes a mobile station (MS) 201, a base station (BS) 203, an access network gateway (ASN-GW) 205, and an authentication server 207. The mobile station (MS) 201 may be any device that can access a network. The mobile station (MS) 201 is a user terminal such as a notebook computer, a personal computer, a personal digital assistant (PDA), a hand set, or a personal multimedia player (PMP). The authentication server 207 authenticates the network access of the mobile station 201. The authentication server 207 may be an Authentication Authorization Accounting (AAA) server. The AAA server may perform authentication, au-

thorization, and accounting for accessing resources and providing services. In general, the AAA server interacts with database and directories storing user information through accessing a network and interacting with a gateway server. In order to perform such operations, the AAA server employs protocol such as a Remote Authentication Dial-In User Service (RADIUS) and DIAMETER.

[59] Each operation in the procedure of a user terminal for accessing a network will be described in detail with reference to Fig. 2.

[60] (1) A user terminal acquires down-link (DL), performs Medium Access Control (MAC) synchronization, and obtains up-link (UL) channel parameters.

[61] (2) A user terminal performs initial ranging and physical layer (PHY) adjustment. In order to process such operations, the user terminal exchanges a Ranging Request (RNG-REQ) message and a Ranging Response (RNG-RSP).

[62] (3) The mobile station (MS) 201 transmits a PSS Basic Capability Request (SBC-REQ) message to the base station (BS) 203.

[63] (4) The base station (BS) 203 transmits an MS_PreAttachment_Req message to the ASN-GW 205 in order to inform that a new mobile station 201 enters a network.

[64] (5) The ASN-GW 205 transmits a MS_PreAttachment_Rsp message to the BS 203 as a response to the MS_PreAttachment_Req message.

[65] (6) After the ASN-GW 205 and the BS 203 exchange the MS_PreAttachment_Req message and the MS_PreAttachment_Rsp message, the BS 203 transmits a PSS Basic Capability Response (SBC-RSP) message to the MS 201.

[66] (7) Simultaneously, the BS 203 transmits a MS_PreAttachment_Ack message to the ASN-GW 205.

[67] (8) After completing MS_PreAttachment, the ASN-GW 205 starts an EAP authentication procedure. The ASN-GW 205 transmits an EAP Request/Identity message to the BS 203 using an Authentication Relay protocol (AR_EAP_Transfer).

[68] (9) The BS 203 relays the EAP Request/ Identity payload to the MS 201 through a PKMv2 (Privacy Key Management Version2)-RSP/EAP-Transfer message.

[69] (10) The MS 201 transmits a network access identifier (NAI) to the BS 203 using the PKMv2-REQ/EAP-Transfer message in response to the EAP Request/Identity.

[70] (11) The BS 203 transmits EAP payload included in the PKMv2-REQ/EAP-Transfer message to the ASN-GW 205 using Authentication Relay protocol (AR_EAP_Transfer).

[71] (12) The ASN-GW 205 analyzes the NAI and transmits the EAP payload to the authentication server 207. The MS 201 and the authentication server 207 perform the EAP authentication process.

[72] (13) The ASN-GW 205 receives an authentication result.

[73] (14) The ASN-GW 205 transmits the authentication result to the BS 203 using the

Authentication Relay protocol (AR_EAP_Transfer).

[74] (15) The BS 203 relays the EAP payload to the MS 201 using the PKMv2 EAP-Transfer/PKM-RSP message.

[75] (16) The ASN-GW 205 transmits a Key_Change_Directive message to the BS 203 in order to inform the completion of the EAP authentication process.

[76] (17) The BS 203 transmits a Key_Change_Ack message to the ASN-GW 205 as a response to the Key_Change_Directive message.

[77] (18-20) The BS 203 and the MS 201 perform a PKMv2 3-way handshake. While performing the PKMv2 3-way handshake, SA-TEK-Challenge/Request/Response messages are exchanged.

[78] (21-22) The MS 201 obtains valid TEK keys by exchanging PKMv2 Key-Request/Reply messages between the BS 203 and the MS 201.

[79] (23) After completing the PKMv2 3-way handshake, the MS 201 transmits a registration request (REG REQ) message to the BS 203. The REG REQ message includes information about CS capabilities, Mobility parameters, and Handover support.

[80] (24-25) The BS 203 transmits a MS_Attachment_Req message to the ASN-GW 205. The ASN-GW 205 transmits a MS_Attachment_Rsp message to the BS 203 as a response to the MS_Attachment_Req message.

[81] (26) The BS 203 transmits a registration response (REG RSP) message to the MS 201.

[82] (27) The BS 203 transmits a MS_Attachment_Ack message to the ASN-GW 205 after transmiting a registration response (REG RSP) message to the MS 201.

[83] (28-29) The ASN-GW 205 generates Initial service flow (ISF), builds a data path to the BS 203 and the MS 201, and establishes connection thereto.

[84] Hereinafter, a procedure of a user terminal for accessing a network in case of authentication failure will be described.

[85] Fig. 3 is a diagram illustrating a procedure of a user terminal for accessing a network in case of authentication failure. Like the network of Fig. 2, a network shown in Fig. 3 includes a mobile station (MS) 301, a base station (BS) 303, an access network gateway (ASN-GW) 305, and an authentication server 307.

[86] A user terminal searches a wireless signal, acquires a channel, and accesses a network access server. These processes are equivalent to the operations (1) to (11) of Fig. 2. Therefore, the operations (1) to (11) are identically applied to the procedure of Fig. 3.

[87] (12) The ASN-GW 305 analyzes the NAI and transmits the EAP payload to the authentication server 307. The MS 301 and the authentication server 307 perform the EAP authentication process. When the MS 301 is rejected to access the network, the authentication server 307 transmits network rejection information to the MS 301. The

ASN-GW 305 may relay an EAP message and payload from the BS 303.

[88] (13) The MS 301, the BS 303, and the ASN-GW 305 perform a disconnection procedure.

[89] Hereinafter, the EAP authentication process in case of user terminal authentication failure will be described in more detail.

[90] Fig. 4 is a diagram illustrating a network access rejection procedure in an EAP authentication process when a user terminal is failed to be authenticated for accessing a network. That is, Fig. 4 describes a network access rejection procedure performed when a user terminal fails to be authenticated for accessing a network. The network access rejection procedure will be described in detail based on a MS 401 and an authentication server 403.

[91] It is preferable that the network access rejection procedure according to the present embodiment is performed in an EAP authentication process. However, the network access rejection procedure according to the present embodiment may be applied to a general authentication process that authenticates a user terminal 401 for accessing a network. Here, the user terminal 401 may include a mobile station (MS).

[92] The network access rejection procedure according to the present embodiment provides network access rejection reasons to the user terminal 401 when the user terminal 401 is rejected to access a network. The network access rejection reasons are reasons why the user terminal 401 is rejected to access the network. Therefore, the user terminal 401 is enabled to perform a proper operation corresponding to the received network access rejection reasons.

[93] Referring to Fig. 4, the user terminal 401 transmits authentication request information to the authentication server 403 for authenticating accessing a network. At step S411, the authentication server 403 performs an authentication procedure according to the authentication request information received from the user terminal 401. The authentication procedure may include an EAP authentication procedure. In case of the EAP authentication procedure, the authentication procedure may be performed by selecting one of specific EAP authentication methods such as EAP-TLS, EAP-TTLS, and EAP-AKA. Each of EAP-TLS, EAP-TTLS, and EAP-AKA authentication methods will be described in later.

[94] When an authentication failure reason of the user terminal 401 is found during the authentication procedure, the authentication procedure is terminated by EAP. Here, the authentication failure may be reason by rejecting a user terminal to access a network. When a reason of rejection the user terminal to access a network is found, the authentication server 403 generates a message including authentication failure reason information and control information according to the authentication failure reason at step S412 and transmits the generated message to the user terminal 401 at step S413.

[95] In detail, when a network access rejection reason is found, the authentication server 403 generates a message according to a result of an authentication procedure before the authentication procedure ends. Particularly, when authentication of the user terminal 401 is rejected, the message includes network rejection information. The network rejection information includes authentication failure reason information and control information for coping with the authentication failure reason. The control information is about instructions for the user terminal 401 to cope with network access rejection according to the network rejection information after disconnecting the user terminal 401 from the network according to the network access rejection procedure. For example, the control information includes information about coping with the authentication failure, such as reaccess-try information or access-standby information after disconnection from a network.

[96] Here, the message may be an EAP message in case of an EAP based authentication. In detail, authentication failure reason information and control information for the user terminal 401 may be transmitted to the user terminal 401 using an EAP-Notification Request message.

[97] In a conventional EAP standard, an authentication server uses an EAP-Notification Request message to send a character string in a UTF-8 format to a user terminal. Further, a user terminal uses the EAP-Notification Request message to display the character string on a display unit. In the present embodiment, the EAP-Notification Request message expands to add access rejection reason information in a Type-Length-Value (TLV) format after the character string. Accordingly, the user terminal 401 analyzes the access rejection information and performs corresponding operations according to the analysis result. The EAP-Notification Request message will be described in more detail in later.

[98] Meanwhile, the network rejection information further includes rejection reason authentication information for integrity protection of the network rejection information. For example, Rejection Message Authentication Code (RMAC) may be the rejection reason authentication information.

[99] The rejection reason authentication information may be generated using a master session key (MSK) or an extended master session key (EMSK). Since the MSK or the MESK is for generating the rejection reason authentication information for protecting the network rejection information, the MSK or the EMSK must be generated in the authentication server 403 before the authentication server 403 transmits messages related to the authentication procedure to the user terminal 401. Therefore, the message related to the authentication procedure can be generated anytime after the MSK or the EMSK are generated.

[100] Here, the integrity protection may be performed by comparing the rejection reason

authentication information with rejection reason authentication information of the user terminal, which is generated using the MSK or the EMSK of the user terminal 401.

[101] At step S414, the user terminal 401 analyzes a message transmitted from the authentication server 403. The user terminal 401 also generates rejection reason authentication information of the user terminal 401 using the MSK or the EMSK of the user terminal 401 for integrity protection. The user terminal 401 protects the network rejection information from malicious attack such as forge or modulation by comparing the rejection reason authentication information generated by the authentication server 401 with the rejection reason authentication information generated by the user terminal 403. For example, the user terminal 401 and the authentication server 403 generate a MSK or an EMSK having the same value and use the same algorithm to calculate RMAC in case of RMAC. Therefore, RMAC values generated by the user terminal 401 and the authentication server 403 become identical except forged or modulated RMAC. The user terminal 401 ignores the received network rejection information when the network rejection information does not include a RMAC value or when a RMAC value generated by the user terminal 401 is not identical to a RMAC value calculated by the authentication server 403.

[102] Hereinafter, an EAP-Notification Request message will be described in more detail.

[103] The EAP-Notification Request message includes network rejection information. The network rejection information includes authentication failure reason information and control information for a user terminal to cope with authentication failure according to the authentication failure reason information.

[104] Meanwhile, the EAP-Notification Request may further include delimiter information and character strings for displaying. The delimiter information enables to identify a general EAP-Notification Request message from an EAP-Notification Request message having network rejection information. In case of using an EAP-Notification message to transfer the network access rejection information, the EAP-Notification Request message includes a delimiter and network access rejection information. The character string may be added prior to a NULL text which is a delimiter. Since the NULL text is not included in an EAP-Notification message in a conventional EAP standard, the user terminal 401 can determine that the EAP-Notification message includes the network rejection information if the EAP-Notification message includes the NULL text. The user terminal 401 determines a received EAP-Notification message as a conventional standard EAP-Notification message if the received EAP-Notification message does not include the NULL text but character string for displaying.

[105] Table 1 shows formation of a Type-Data field of an EAP-Notification message.

[106] Table 1

[Table 1]

[Table]

Element Name	Length in octets	Description
Human Readable String	Variable	If required, UTF-8 encoded human readable message MAY be included prior to the NULL character. Then, the MS SHOULD displays this message to the user if the integrity check succeeds.
Delimiter	1	The NULL character (0x00)
Network Rejection Information string	Variable	ASCII string that is BASE64-encoded from the Network Rejection Information TLV. The MS SHOULD NOT display this string to the user as it is, without proper translation.

[107]

[108] Hereinafter, network rejection information will be described.

[109] The network rejection information may be coded into Type-Length-Value (TLV). TLV coded network rejection information is human unreadable format. When the TLV coded network rejection information is not converted into a human readable format, the TVL coded network rejection information is not outputted through a display device of a user terminal. The TLV coded network rejection information is include a Type-Data field of the EAP-Notification Request message and transferred to the user terminal 401.

[110] The network rejection information may include authentication failure reason information and control information for a user terminal 401 to cope with authentication failure according to the authentication failure reason. Here, the authentication failure reason information may be classified by control information. The classified information may be expressed as a predetermined code.

[111] Table 2 shows the network rejection information in detail.

[112] Table 2

[Table 2]

[Table]

Type	3 for Network Rejection information		
Length in Octets	Variable		
Description	The Network Rejection Information is coded as follows		
Elements(Sub-TLVs)	**TLV Name**	**Description**	**M/0**
	Rejection Code		M
	Received NAI		M
	Emergency Services Overrride		0
	Allowed Location Information		0
	RMAC (Rejection Message Authentication Code) Value		M

[113]

[114] In Table 2, "Rejection Code" means a rejection code where authentication failure reason information is separated from control information. The network rejection information may include a rejection code, and the rejection code may be classified by a rejection class which is control information. Table 3 shows the rejection class in detail.

[115] Table 3

[Table 3]

[Table]

Rejection Class	Rejection Duration/Criteria	Applicability of Visited/Home AAA	Scope of Rejection
A	Until Manual Retry	Home AAA	All NAPs
B	Until Manual Retry	Visited/Home AAA	V-NSP
C	Until Power Cycle	Home AAA	All NAPs
D	Until Power Cycle	Visited/Home AAA	V-NSP
E	Until Timer Expiry	Home AAA	All NAPs
F	Until Timer Expiry	Visited/Home AAA	V-NSP
G	Until Location Criteria met	Home AAA	All NAPs
H	Until Location Criteria met	Visited/Home AAA	V-NSP

[116]

[117] In Table 3, the rejection class is classified from A to H. "Rejection Duration/Criteria"

classifies operations of the user terminal 401 by the network rejection information. For example, "Until manual Retry" is control information that control the user terminal 401 not to access a network until a user of the user terminal 401 manually request re-access. "Until Power Cycle" is control information that controls a user terminal 401 not to access a network until a user of the user terminal 401 manually applies the power of the user terminal 401 again. "Until Timer Expiry" is control information for controlling a user terminal 401 not to access a network until a predetermined time is passed. "Until Location Criteria met" is control information for controlling a user terminal 401 not to access a network until a user terminal arrives at an allowed location of a base station.

[118] Hereinafter, relation between a rejection code and a rejection class will be described.

[119] The rejection code is classified by a rejection class. Table 4 exemplary shows the relation of the rejection code and the rejection class. Here, Table 4 shows rejection classes from A to C among the rejection classes shown in Table 3.

[120] Table 4

[Table 4]

[Table]

Type	4 for Rejection Code
Length in Octects	2
	The Rejection Code value is defined as follows:**Rejection Class A** -Rejection Codes in the range 0x0000 - 0x00FF 0x0000 = Rejection Class A -General Error 0x0001 = Invalid Subscription Information 0x0002 = Major Network Problem 0x0003 = Unpaid Bills 0x0004 = Illegal Mobile Equipment 0x0005 = Device Type not supported by NSP 0x0006 = Misbehaving MS EquipmentAll other Rejection codes in Rejection Class A are undefined.**Rejection Class B** -Rejection Codes in the range 0x0100 - 0x01FF 0x0100 = Rejection Class B -General Error 0x0101 = No Roaming Agreement existing with the Home or the Visited Network 0x0102 = Illegal Mobile Equipment 0x0103 = Device Type not supported by NSP 0x0104 = Invalid Subscription/Configuration 0x0105 = Misbehaving MS EquipmentAll other Rejection codes in Rejection Class B are undefined.**Rejection Class C** -Rejection Codes in the range 0x0200 - 0x02FF 0x0200 = Rejection Class C -General Error 0x0201 = Invalid Subscription Information 0x0202 = Major Network Problem 0x0203 = Unpaid Bills 0x0204 = Illegal Mobile Equipment 0x0205 = Device Type not supported by NSP 0x0206 = Misbehaving MS EquipmentAll other Rejection codes in Rejection Class C are undefined.

[121]

[122] Hereinafter, RMAC will be described in detail. Table 5 exemplarily shows RMAC in detail. As shown in Table 5, 32-byte RMAC-Value is calculated using an EMSK value that is generated as the same value in both of the user terminal 401 and the authentication server 403 in an EAP authentication procedure. While calculating the RMAC-Value, a Value field of RMAC TLV included in Rejection Information TLV is filled with 0. After calculating, the Value field of RMAC TLV is replaced with the RMAC-Value. It is not necessary to share a security key value between the user terminal 401 and the authentication server 403 by using a 512-bit Extended Master Session Key (EMSK) value which is generated as the same value in the user terminal 401 and the authentication server 403 during the EAP standard authentication procedure.

[123] Table 5

[Table 5]

[Table]

Type	8 for RMAC (Rejection Message Authentication Code) Value
Length in octets	32
Value	32 octet RMAC Value SHALL be generated from the EMSK using the following formula:RMAC-Value = HMAC-SHA256(RMAC Key, Network Rejection Information TLV)where:RMAC-1 = HMAC-SHA256(EMSK , usage-data | 0x01)RMAC-2 = HMAC-SHA256(EMSK, RMAC-1 | usage data | 0x02)RMAC-Key = RMAC-1 | RMAC-2where:usage-data = key label + "\0" + lengthkey label = rmac-key@wimaxforum.org in ASCIIlength = 0x0200 the length in bits of the RMAC-Key expressed as a 2 byte unsigned integer in network order.RMAC-Value is a 32 octet HMAC-SHA256 digest value, where the RMAC-Key is used for the key and the whole Network Rejection Information TLV is used for the data, except that the value field of the RMAC Value TLV included in the Rejection Information is set to zero when calculating the RMAC-Value. After calculation, the value field of the RMAC Value TLV included in the Network Rejection Information TLV is replaced with the calculated RMAC-Value.

[124]

[125] Hereinafter, an authentication method according to embodiments of the present invention will be described in detail.

[126]

[127] <First user terminal authentication method>

[128] A user terminal authentication method in accordance with an embodiment of the present invention will be described with reference to Fig. 4. The user terminal authentication method according to the present embodiment denotes an authentication method performed by an authentication server 403.

[129] The user terminal authentication method according to the present embodiment includes receiving authentication request information for accessing a network from a user terminal 401; processing an authentication procedure according to the authentication request information; and transmitting a message according to the authentication procedure to the user terminal 401. When the authentication of the user terminal fails, the message includes network rejection information, and the network rejection information includes an authentication failure reason information and control

information for a user terminal 401 to cope with authentication failure according to the authentication failure reason.

[130] The authentication procedure may be an Extensible Authentication Protocol (EAP) based authentication procedure. Here, the message may be an EAP message. The EAP message further includes delimiter information.

[131] The network rejection information may be a Type-Length-Value (TLV) code. TLV coded network rejection information is in a human unreadable format. The TLV coded network rejection information cannot be displayed on a display unit of the user terminal 401 if it is not converted in a human readable format. Meanwhile, the TLV coded network rejection information may be included in a Type-Data field of the EAP message. The authentication failure reason information may be classified by control information.

[132] The network rejection information may further include rejection reason authentication information for integrity protection for the network rejection information. Here, rejection reason authentication information may be generated by using a Master Session Key (MSK) or an Extended Master Session Key (EMSK). The integrity protection may be performed by comparing rejection reason authentication information generated by the authentication server 403 with rejection reason authentication reason information of a user terminal 401, which is generated by using an MSK or an EMSK of the user terminal 401.

[133]

[134] <Second user terminal authentication method>

[135] Hereinafter, a user terminal authentication method according to another embodiment of the present invention will be described with reference to Fig. 4. Here, the user terminal authentication method according to the present embodiment denotes an authentication method performed by a user terminal 401.

[136] The user terminal authentication method according to the present embodiment includes: transmitting authentication request information for accessing a network to an authentication server 403; and receiving messages related to an authentication procedure processed according to the authentication request information from the authentication server 403. If the authentication of the user terminal 401 is failed as the result of the authentication procedure, the message includes network rejection information. The network rejection information includes authentication fail reason information and control information for a user terminal 401 to cope with the authentication failure according to the authentication failure reason.

[137] The user terminal authentication method according to the present embodiment further includes performing operations according to the control information.

[138] The authentication procedure may be an Extensible Authentication Protocol (EAP)

based authentication procedure. Here, the message may be an EAP message. The EAP message may further include delimiter information. The network rejection information may be coded as Type-Length-Value (TLV) code. The TLV coded network rejection information is in a human unreadable format. If it is not transformed into a human readable format, the TLV coded network rejection information may not be displayed on a display device of a user terminal 401. Meanwhile, the TLV coded network rejection information may be included in a Type-Data field of an EAP message, and the authentication failure reason information may be classified by control information.

[139] The network rejection information may further include rejection reason authentication information for integrity protection for network rejection information. The rejection reason authentication information may be generated using a Master Session Key (MSK) or an Extended Master Session Key (EMSK). The integrity protection may be performed by comparing rejection reason authentication information generated in a user terminal 401 with rejection reason authentication information of the authentication server 403, which is generated using a MSK or an EMSK of the authentication server 403.

[140]

[141] <Authentication Sever>

[142] An authentication server employing a method for authenticating a user terminal according to an embodiment of the present invention will be described, hereinafter.

[143] Fig. 5 is a diagram illustrating an authentication server in accordance with an embodiment of the present invention. Referring to Fig. 5, the authentication server 501 according to the present embodiment includes a receiver 503, a transmitter 505, and an authentication procedure processor 507.

[144] The receiver 503 receives authentication request information from a user terminal to access a network. The authentication procedure processor 507 processes authentication procedure according to the authentication request information. The transmitter 505 transmits messages generated by the authentication procedure to the user terminal. If the authentication of a user terminal fails, the message includes network rejection information. The network rejection information includes authentication failure reason information and control information for a user terminal to cope with the authentication failure according to the authentication failure reason.

[145] Here, the authentication procedure may be an Extensible Authentication Protocol (EAP) based authentication procedure. Here, the message may be an EAP message. The EAP message may further include delimiter information. The network rejection information may be coded as Type-Length-Value (TLV) code. The TLV coded network rejection information is in a human unreadable format. If it is not transformed into a human readable format, the TLV coded network rejection information may not be

displayed on a display device of a user terminal. Meanwhile, the TLV coded network rejection information may be included in a Type-Data field of an EAP message, and the authentication failure reason information may be classified by control information.

[146] The network rejection information may further include rejection reason authentication information for integrity protection for network rejection information. In this case, the authentication server 501 may further include an authentication information generator 509. The rejection reason authentication information may be generated using a Master Session Key (MSK) or an Extended Master Session Key (EMSK). The integrity protection may be performed by comparing rejection reason authentication information generated by the authentication server 501 with rejection reason authentication information of a user terminal, which is generated using a MSK or an EMSK of the user terminal.

[147]

[148] <User Terminal>

[149] A user terminal employing a method for authentication a user terminal according to an embodiment of the present invention will be described, hereinafter.

[150] Fig. 6 is a diagram illustrating a user terminal in accordance with an embodiment of the present invention. Referring to Fig. 6, the user terminal 601 includes a receiver 603 and a transmitter 605.

[151] The transmitter 605 transmits authentication request information for accessing a network to an authentication server. The receiver 605 receives a message related to an authentication procedure processed according to the authentication request information from the authentication server. If the authentication of the user terminal 601 fails, the message may include network rejection information. The network rejection information includes authentication failure reason information and control information for a user terminal 601 to cope with the authentication failure according to the authentication failure reason.

[152] The user terminal 601 may further include a controller 607 for performing control operations according to the control information.

[153] The authentication procedure may be an Extensible Authentication Protocol (EAP) based authentication procedure. Here, the message may be an EAP message. The EAP message may further include delimiter information. The network rejection information may be coded as Type-Length-Value (TLV) code. The TLV coded network rejection information is in human unreadable format. If it is not transformed into a human readable format, the TLV coded network rejection information may not be displayed on a display device of a user terminal 601. Meanwhile, the TLV coded network rejection information may be included in a Type-Data field of an EAP message, and the authentication failure reason information may be classified by control information.

[154] The network rejection information may further include rejection reason authentication information for integrity protection for network rejection information. In this case, the user terminal 601 may further include an authentication information generator 609. The rejection reason authentication information may be generated using a Master Session Key (MSK) or an Extended Master Session Key (EMSK). The integrity protection may be performed by comparing rejection reason authentication information generated by the user terminal 601 with rejection reason authentication information of an authentication server, which is generated using a MSK or an EMSK of the authentication server.

[155] The method of the present invention described above can be realized as a program and stored in a computer-readable recording medium such as CD-ROM, RAM, ROM, floppy disks, hard disks, magneto-optical disks and the like. Since the process can be easily implemented by those skilled in the art to which the present invention pertains, further description will not be provided herein. Particularly, the method of the present invention can be realized as a computer readable recoding medium storing a method for user terminal authentication where the method including processing an authentication procedure according to authentication request information from a user terminal for accessing a network an d generating a message including result information according to the authentication procedure. When the user terminal fails to be authenticated, the result information includes network rejection information. The network rejection information includes authentication failure reason information and control information for the user terminal to cope with the authentication failure based on the authentication failure reason information. Further, the method of the present invention can be realized as a computer readable recording medium for storing a method for user terminal authentication where the method including generating authentication request information for accessing a network and analyzing a message including a result of authentication procedure processed according to the authentication request information received from the authentication server. When the user terminal fails to be authenticated, the result information includes network rejection information. The network rejection information includes authentication failure reason information and control information for the user terminal to cope with the authentication failure according to the authentication failure reason.

[156] Hereinafter, exemplary applications of the present invention will be described. Particularly, a network access rejection procedure in an EAP-TLS, an EAP-TTLS, and an EAP-AKA will be described.

[157]

[158] <Network access rejection procedure in EAP-TLS>

[159] An EAP-TLS authentication protocol is an Xl.509 certificate based authentication

protocol. Here, EAP stands for Extensible Authentication Protocol and TLS denotes Transport Level Security. The EAP-TLS authentication protocol includes a procedure that an authentication server authenticates a user terminal using a certificate of a user terminal and a procedure that a user terminal authenticates an authentication server using a certificate of the authentication server. A user who wants to use an Internet service needs to be authenticated before using the Internet service. Here, mutual authentication may be performed between a user terminal and an authentication server.

[160] A Master Session Key (MSK) or an Extended MSK (EMSK) may be generated like Eq. 1.

[161]

[162] [Eq. 1]

[163] MSK(0,63) = TLS-PRF-64(master secret, "client EAP encryption", random)

[164] EMSK(0,63) = second 64 octets of: TLS-PRF-128(master secret, "client EAP encryption", random)

[165]

[166] In Eq. 1, master secret denotes a value shared in a TLS handshake procedure as a method defined in a TLS protocol. Random denotes client.random||server.random.

[167] Fig. 7 is a diagram illustrating a network access rejection procedure in EAP-TLS. Referring to Fig. 7, at step S710, a user terminal, a base station, and an ASN-GW acquire a channel and access a network access server. The network access rejection procedure will be described based on connection between the user terminal and the authentication server.

[168] The user terminal receives an EAP-Request/Identity message from the authentication server to request an identity of a user terminal. A Network Access Identifier (NAI) value is set as an Identity value of the EAP-Request/Identity message as a response to the EAP-Request/Identity message and the set NAI value is transmitted to the authentication server at step S711.

[169] The authentication server generates an EAP-Request/TLS-Start message when receiving the EAP-Response/Identity and transmits the generated EAP-Request/TLS-Start message to the user terminal at step S712.

[170] When the user terminal receives the EAP-Request/TLS-Start message, the user terminal generates an EAP-Response/TLS(client_hello) message and transmits the generated EAP-Response/TLS(client_hello) message to the authentication server at step S713.

[171] When the authentication server receives the EAP-Response/TLS(client_hello) message, the authentication server generates and transmits an EAP-Request/TLS(server_hello, certificate, [server_key_exchange], [certificate_request], server_hello_done) message to the user terminal at step S714.

[172] When the user terminal receives the EAP-Request/TLS(server_hello, certificate, [server_key_exchange], [certificate_request], server_hello_done) message and receives EAP-Response/EAP-TLS.client_hello messasge, the user terminal transmits the EAP-Response/TLS(certificate, client_key_ exchange], [certificate_verify], change_chiper_spec, finish) message to the authentication server at step S715.

[173] When the authentication server receives EAP-Response/TLS(certificate, client_key_exchange], [certificate_ verify], change_chiper_spec, finish) message, the authentication server transmits an EAP-Request/TLS(change_ chiper_spec, finish) message to the user terminal at step S716. The user terminal authenticates the authentication server by verifying TLS finished and transmits related message to the authentication server at step S717.

[174] Meanwhile, the authentication server includes an AAA-Key (MSK) into an AVP of a Diameter(RADIUS)/EAP-Transfer message and transmits the Diameter(RADIUS)/EAP-Transfer message to an Access Control Router (ACR). Then, the ACR safely stores the received AAA-Key (MSK).

[175] When the authentication server denies the access or the authentication of the user terminal, the authentication server transmits an EAP-Request/Notification (Displayable message/ Rejection Information) message to the user terminal at step S718.

[176] It was described with reference to Fig. 4. The user terminal transmits the EAP-Response/Notification message to the authentication server as a response to the EAP-Request/Notification message at step S719.

[177] The authentication server transmits a message informing authentication failure to the user terminal at step S720 and releases connection to the user terminal, the base station, and the ASN-GW at step S721.

[178]

[179] <Network access rejection procedure in EAP-TTLS>

[180] An EAP-TTLS (Tunneled TLS) Authentication Protocol is the extension of an EAP-TLS authentication protocol. The EAP-TTLS authentication protocol includes a first phase that a user terminal authenticates an authentication server using certificate of an authentication server and establishes a TLS (Transport Level Security) tunnel and a second phase that the authentication server authenticates the user terminal or a user on the safe TLS tunnel.

[181] The Master Session Key (MSK) and the Extended MSK (EMSK) may be generated like Eq. 2.

[182]

[183] [Eq. 2]

[184] MSK(0,63) = TLS-PRF-64(SecurityParameter.master_secret, "ttls key material",random)

[185] EMSK(0,63) = second 64 octets of: TLS-PRF-128(SecurityParameter.master_secret, "ttls keying material", random)

[186]

[187] In Eq. 2, SecurityParameter denotes each parameter exchanged in a TTLS handshake procedure. master_secret denotes a value negotiated in a TTLS handshake procedure in a method defined in a TLS protocol. Random denotes Security-Parameter.client_hello.random||SecurityParameter.server_hello.random.

[188] Fig. 8 is a diagram illustrating a network access rejection procedure in EAP-TTLS. Referring to Fig. 8, a user terminal, a base station, and an ASN-GW acquire a channel and access a network access server at step S811. The network access rejection procedure will be described based on connection between the user terminal and the authentication server.

[189] The user terminal receives an EAP-Request/Identity message that asks the identity of the user terminal from the authentication server, sets a Network Access Identifier (NAI) value of the user terminal as an Identity value of the EAP-Response/Identity message, and transmits the NAI of the user terminal to the authentication server at step S812.

[190] When the authentication server receives the EAP-Response/Identity message, the authentication server generates and transmits an EAP-Request/TTLS-Start message to the user terminal at step S813.

[191] The user terminal and the authentication server perform a TLS Handshake procedure at step S814.

[192] The above procedure is the first phase that the user terminal authenticates the authentication server using the certificate of the authentication server and establishes the TLS tunnel.

[193] Hereinafter, the second phase that the authentication server authenticates the user terminal or a user on the TLS tunnel will be described.

[194] The user terminal generates an EAP-Response/EAP-TTLS.MSCHAP-V2 message formed of user-name, MS-CHAPChallenge, and MS-CHAP2-Response and transmits the EAP-Response/EAP-TTLS.MSCHAP-V2 message to the authentication server at step S815.

[195]

[196] The authentication server performs user authentication using an MSCHAPv2 algorithm. In case of authentication success, the authentication server generates an EAP-Request/EAP-TTLS(MS-CHAP-V2-Success) message with MS-CHAP2-Success set and transmits the EAP-Request/EAP-TTLS(MS-CHAP-V2-Success) message to the user terminal at step S816. Then, the user responses to the authentication server at step S817.

[197] When the authentication server rejects the access or the authentication of the user terminal, the authentication server transmits an EAP-Request/Notification (Displayable message/ Rejection Information) to the user terminal at step S818. It was already described with reference to Fig. 4. The user terminal transmits an EAP-Response/Notification message as a response to the EAP-Request/Notification message to the authentication server at step S819.

[198] The authentication server transmits a message of an authentication failure to the user terminal at step S820 and releases the connections to the user terminal, the base station, and the ASN-GW at step S821.

[199]

[200] <Network Access rejection procedure in EAP-AKA>

[201] An EAP-AKA Authentication Protocol is an EAP authentication method for authenticating a user terminal and distributing a session key using an AKA procedure in an UMTS. AKA stands for Authentication and Key Agreement.

[202] Fig. 9 is a diagram illustrating a network access rejection procedure in EAP-AKA. Referring to Fig. 9, a user terminal, a base station (BS), and an ASN-GW obtain a channel and access a network access server at step S910. The network access rejection procedure will be described based on connection between a user terminal and an authentication server.

[203] The user terminal receives an EAP-Request/Identity message requiring identity of a user terminal from the authentication server, sets a Network Access Identifier (NAI) of the user terminal with the Identity value of the EAP-Request/Identity message, and transmits the NAI to the authentication server at step S911.

[204] The authentication server transmits an EAP-Request/AKA-Challenge message to the user terminal at step S912, and the user terminal transmits an EAP-Response/AKA-Challenge message to the authentication server at step S913.

[205] When the authentication server denies access or authentication of the user terminal, the authentication server transmits an EAP-Request/Notification (Displayable message/ Rejection Information) message to the user terminal at step S 914. This procedure is already described with reference to Fig. 4. The user terminal transmits an EAP-Response/Notification message to the authentication server as a response to the EAP-Request/Notification message at step S915.

[206] The authentication server transmits an EAP-Request/ AKA-Notification message to the user terminal at step S916, and the user terminal transmits an EAP-Response/AKA-Notification message to the authentication server as a response to the EAP-Request/ AKA-Notification message at step S917.

[207] The authentication server transmits an authentication result, that is, an authentication failure message, to the user terminal at step S918 and releases connections to the user

terminal, to the base station, and the ANS-GW at step S919.

[208] While the present invention has been described with respect to the specific embodiments, it will be apparent to those skilled in the art that various changes and modifications may be made without departing from the spirit and scope of the invention as defined in the following claims.

[209]

Industrial Applicability

[210] A method for user terminal authentication according to the present invention is applied to a communication system using a network. Particularly, the method for user terminal authentication according to the present invention is used for an authentication procedure.

[211]

Claims

[Claim 1] A method for authenticating a user terminal, comprising:
receiving authentication request information for accessing a network from the user terminal;
processing an EAP authentication procedure according to the authentication request information; and
transmitting a message related to the EAP authentication procedure to the user terminal,
wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[Claim 2] The method of claim 1, wherein the message is an EAP message and further includes delimiter information.

[Claim 3] The method of claim 2, wherein the network rejection information is coded by a Type-Length-Value (TLV).

[Claim 4] The method of claim 3, wherein the TLV coded network rejection information is in a human-unreadable format and is not displayed through a display device of the user terminal unless the TLV coded network rejection information is converted into a human-readable format.

[Claim 5] The method of claim 3, wherein the TLV coded network rejection information is included in a Type-Data field of the EAP message.

[Claim 6] The method of claim 1, wherein the network rejection information further includes rejection reason authentication information for integrity protection for the network rejection information.

[Claim 7] The method of claim 6, wherein the rejection reason authentication information is generated using a Master Session Key (MSK) or an Extended Master Session Key (EMSK).

[Claim 8] The method of claim 7, wherein the integrity protection is performed by comparing the rejection reason authentication information with rejection reason authentication information of the user terminal, which is generated using a MSK or an EMSK of the user terminal.

[Claim 9] An apparatus for authenticating a user terminal, comprising:
a receiver configured to receive authentication request information from the user terminal to access a network;
an EAP authentication procedure processor configured to process an authentication procedure according to the authentication request in-

formation; and

a transmitter configured to transmit a message related to the EAP authentication procedure to the user terminal,

wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for a user terminal to cope with the network rejection.

[Claim 10] A method for authenticating a user terminal, comprising:

transmitting authentication request information for accessing a network to an authentication server; and

receiving a message related to an EAP authentication procedure processed according to the authentication request information from the authentication server,

wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[Claim 11] The method of claim 10, further comprising performing control operations according to the control information.

[Claim 12] The method of claim 10, wherein the message is an EAP message and further includes delimiter information.

[Claim 13] The method of claim 12, wherein the network rejection information is coded by a Type-Length-Value (TLV).

[Claim 14] The method of claim 13, wherein the TLV coded network rejection information is in a human unreadable format and is not displayed through a display device of the user terminal if is not converted into a human readable format.

[Claim 15] The method of claim 13, wherein the TLV coded network rejection information is included in a Type-Data field of the EAP message.

[Claim 16] The method of claim 10, wherein the network rejection information further includes authentication rejection reason information for integrity protection for the network rejection information.

[Claim 17] The method of claim 16, wherein the rejection reason authentication information is generated using a Master Session Key (MSK) or an Extended Master Session Key (EMSK).

[Claim 18] The method of claim 17, wherein the integrity protection is performed by comparing the rejection reasons authentication information with rejection reason authentication server of the authentication server,

which is generated using a MSK or an EMSK of the authentication server.

[Claim 19] An apparatus for authenticating a user terminal, comprising:
a transmitter configured to transmit authentication request information for accessing a network to an authentication server; and
a receiver configured to receive a message related to an EAP authentication procedure processed according to the authentication request information from the authentication server,
wherein the message includes network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[Claim 20] A method for authenticating a user terminal, comprising:
receiving authentication request information for accessing a network from the user terminal;
processing an EAP-TLS authentication procedure according to the authentication request information; and
transmitting a EAP-Request/Notification message related to the EAP-TLS authentication procedure to the user terminal,
wherein the EAP-Request/Notification message includes the network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[Claim 21] A method for authenticating a user terminal, comprising:
receiving authentication request information for accessing a network from the user terminal;
processing an EAP-TTLS authentication procedure according to the authentication request information; and
transmitting a EAP-Request/Notification message related to the EAP-TTLS authentication procedure to the user terminal,
wherein the EAP-Request/Notification message includes the network rejection information when network rejection related to authentication failure or authorization failure is triggered during the the EAP-TTLS authentication procedure, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

[Claim 22] A method for authenticating a user terminal, comprising:

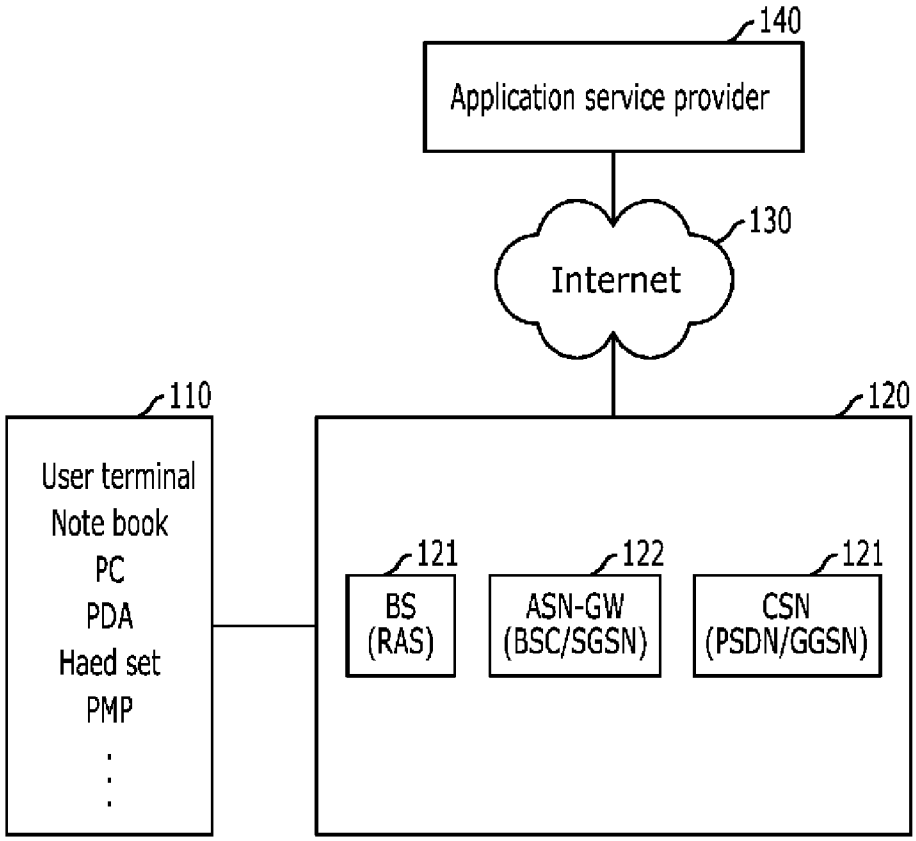
receiving authentication request information for accessing a network from the user terminal;

processing an EAP-AKA authentication procedure according to the authentication request information; and

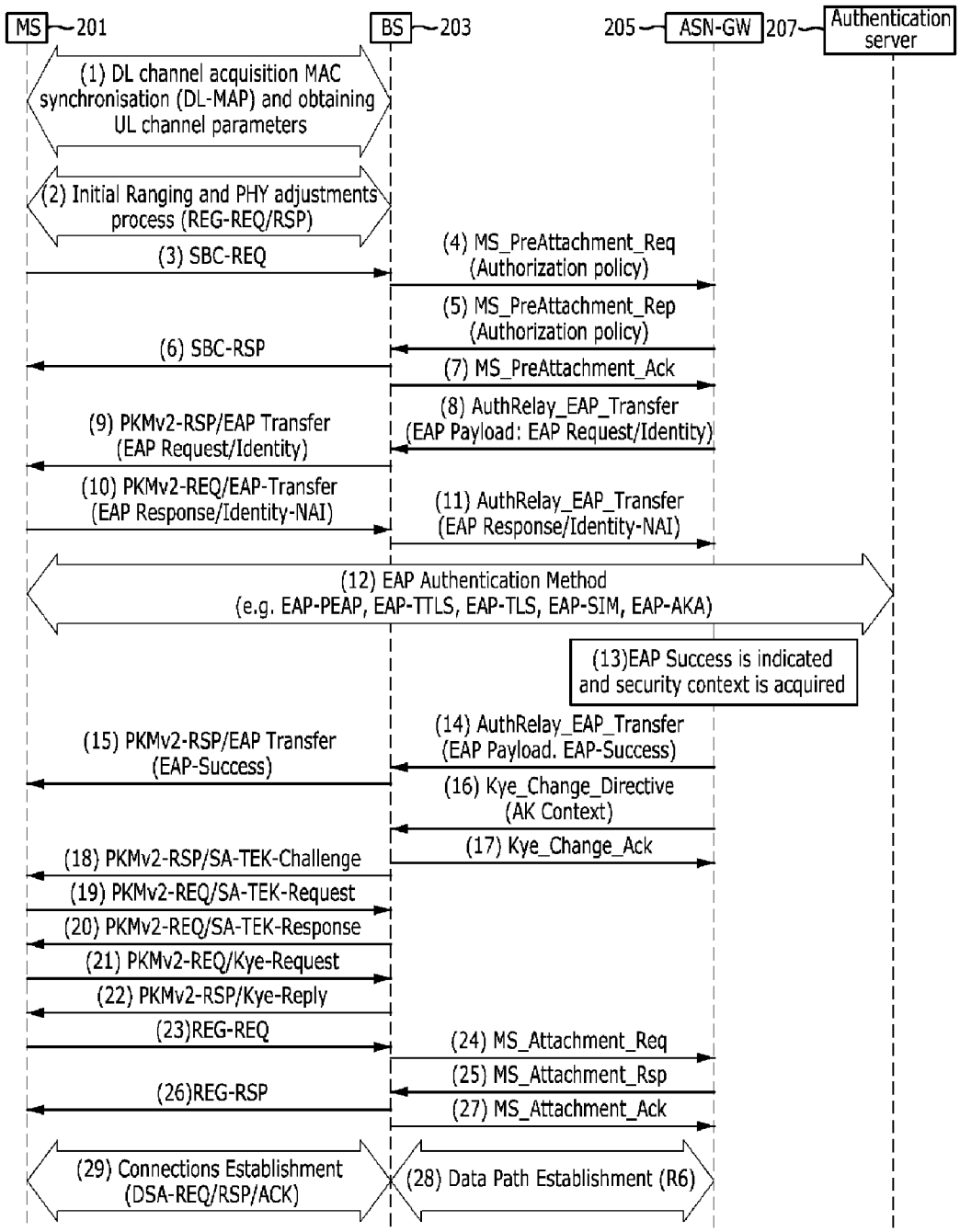
transmitting a EAP-Request/Notification message related to the EAP-AKA authentication procedure to the user terminal,

wherein the EAP-Request/Notification message includes the network rejection information when network rejection is triggered, and the network rejection information includes network rejection reason information and control information for the user terminal to cope with the network rejection.

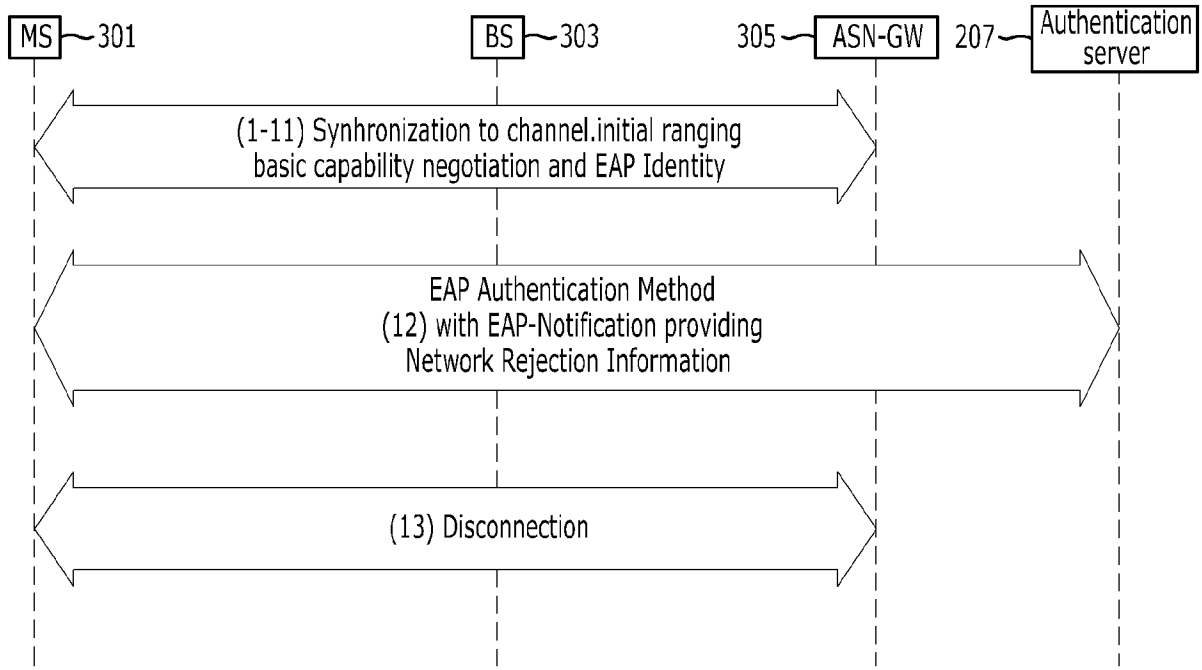
[Fig. 1]


140
Application service provider
130
Internet
110
User terminal
Note book
PC
PDA
Haed set
PMP
120
121
BS
(RAS)
122
ASN-GW
(BSC/SGSN)
121
CSN
(PSDN/GGSN)

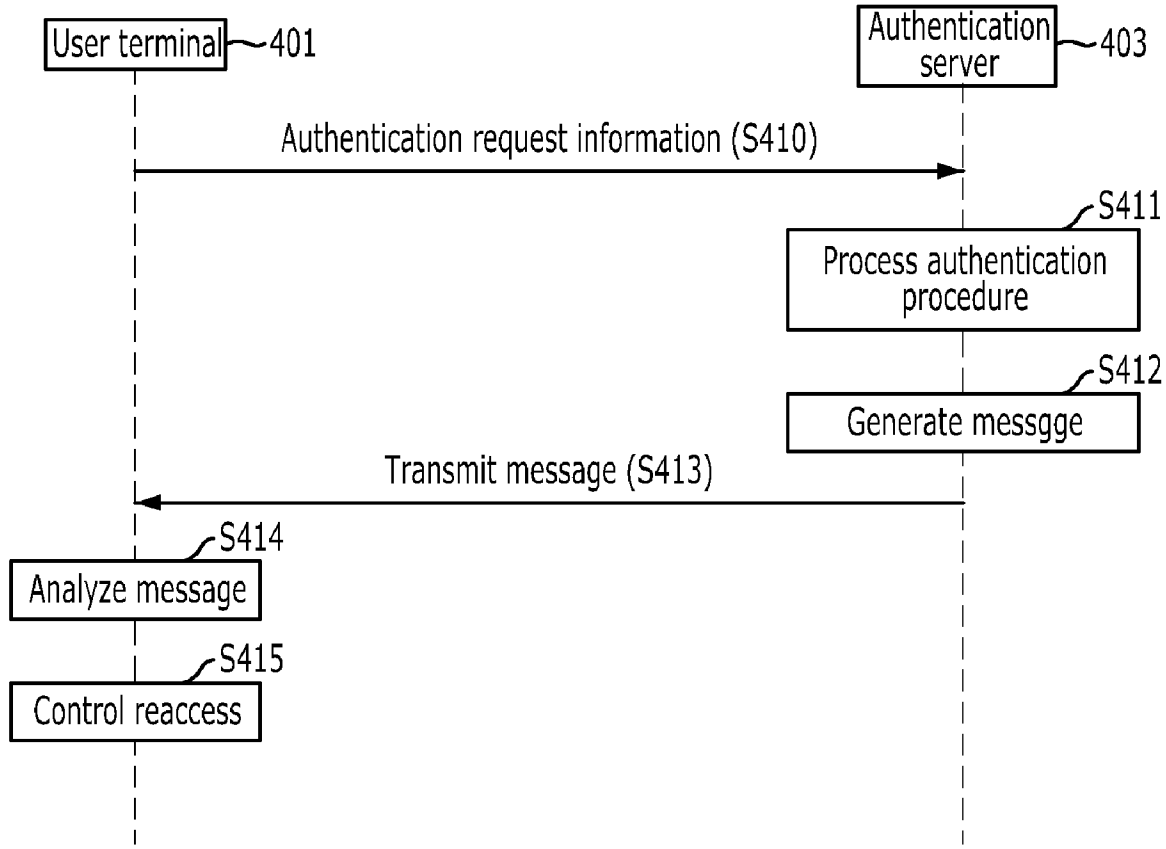
[Fig. 2]


MS
201
BS
203
205
ASN-GW
207
Authentication server
(1) DL channel acquisition MAC synchronisation (DL-MAP) and obtaining UL channel parameters
(2) Initial Ranging and PHY adjustments process (REG-REQ/RSP)
(3) SBC-REQ
(4) MS_PreAttachment_Req (Authorization policy)
(5) MS_PreAttachment_Rep (Authorization policy)
(6) SBC-RSP
(7) MS_PreAttachment_Ack
(8) AuthRelay_EAP_Transfer (EAP Payload: EAP Request/Identity)
(9) PKMv2-RSP/EAP Transfer (EAP Request/Identity)
(10) PKMv2-REQ/EAP-Transfer (EAP Response/Identity-NAI)
(11) AuthRelay_EAP_Transfer (EAP Response/Identity-NAI)
(12) EAP Authentication Method (e.g. EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA)
(13)EAP Success is indicated and security context is acquired
(14) AuthRelay_EAP_Transfer (EAP Payload. EAP-Success)
(15) PKMv2-RSP/EAP Transfer (EAP-Success)
(16) Kye_Change_Directive (AK Context)
(17) Kye_Change_Ack
(18) PKMv2-RSP/SA-TEK-Challenge
(19) PKMv2-REQ/SA-TEK-Request
(20) PKMv2-REQ/SA-TEK-Response
(21) PKMv2-REQ/Kye-Request
(22) PKMv2-RSP/Kye-Reply
(23)REG-REQ
(24) MS_Attachment_Req
(25) MS_Attachment_Rsp
(26)REG-RSP
(27) MS_Attachment_Ack
(29) Connections Establishment (DSA-REQ/RSP/ACK)
(28) Data Path Establishment (R6)

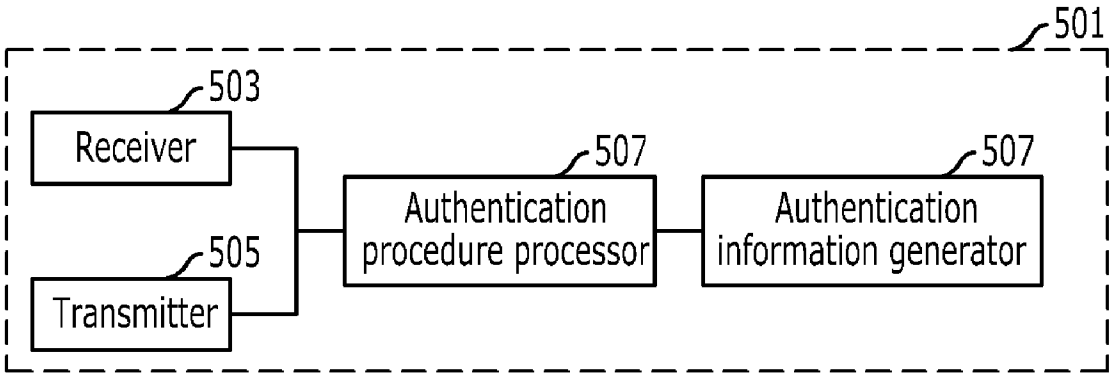
[Fig. 3]


MS
301
BS
303
305
ASN-GW
207
Authentication server
(1-11) Synhronization to channel.initial ranging
basic capability negotiation and EAP Identity
EAP Authentication Method
(12) with EAP-Notification providing
Network Rejection Information
(13) Disconnection

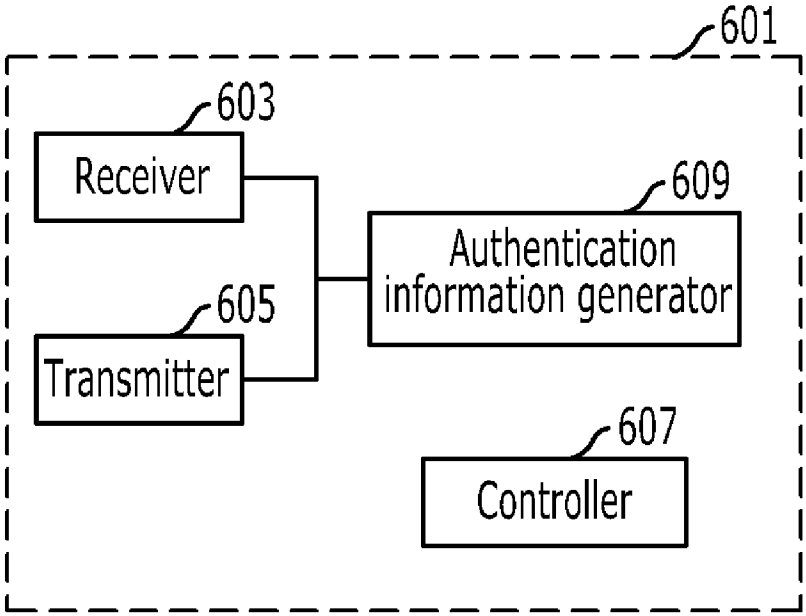
[Fig. 4]


User terminal
401
Authentication server
403
Authentication request information (S410)
S411
Process authentication procedure
S412
Generate messgge
Transmit message (S413)
S414
Analyze message
S415
Control reaccess

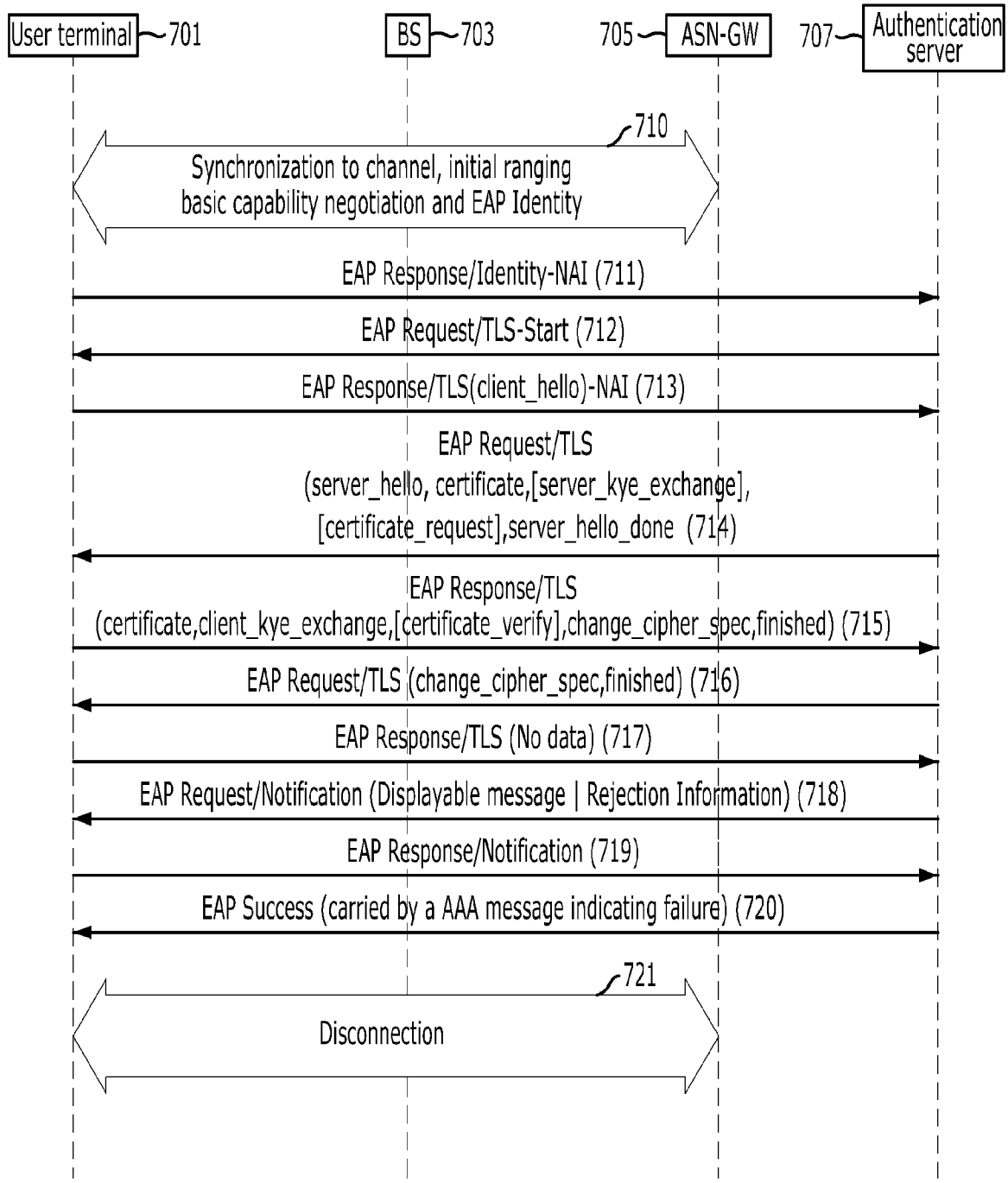
[Fig. 5]


501
503
Receiver
505
Transmitter
507
Authentication procedure processor
507
Authentication information generator

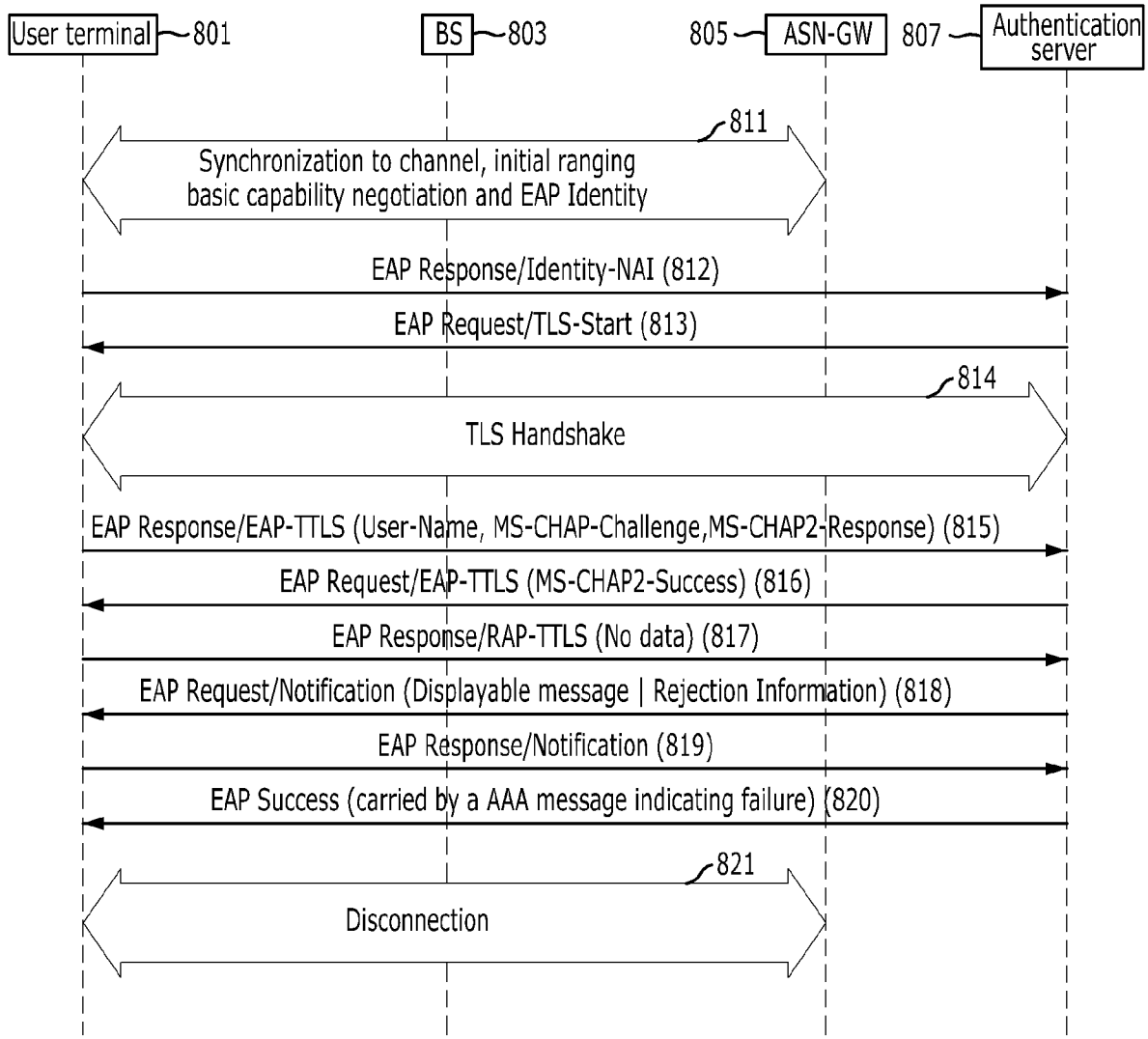
[Fig. 6]


601
603
Receiver
605
Transmitter
609
Authentication information generator
607
Controller

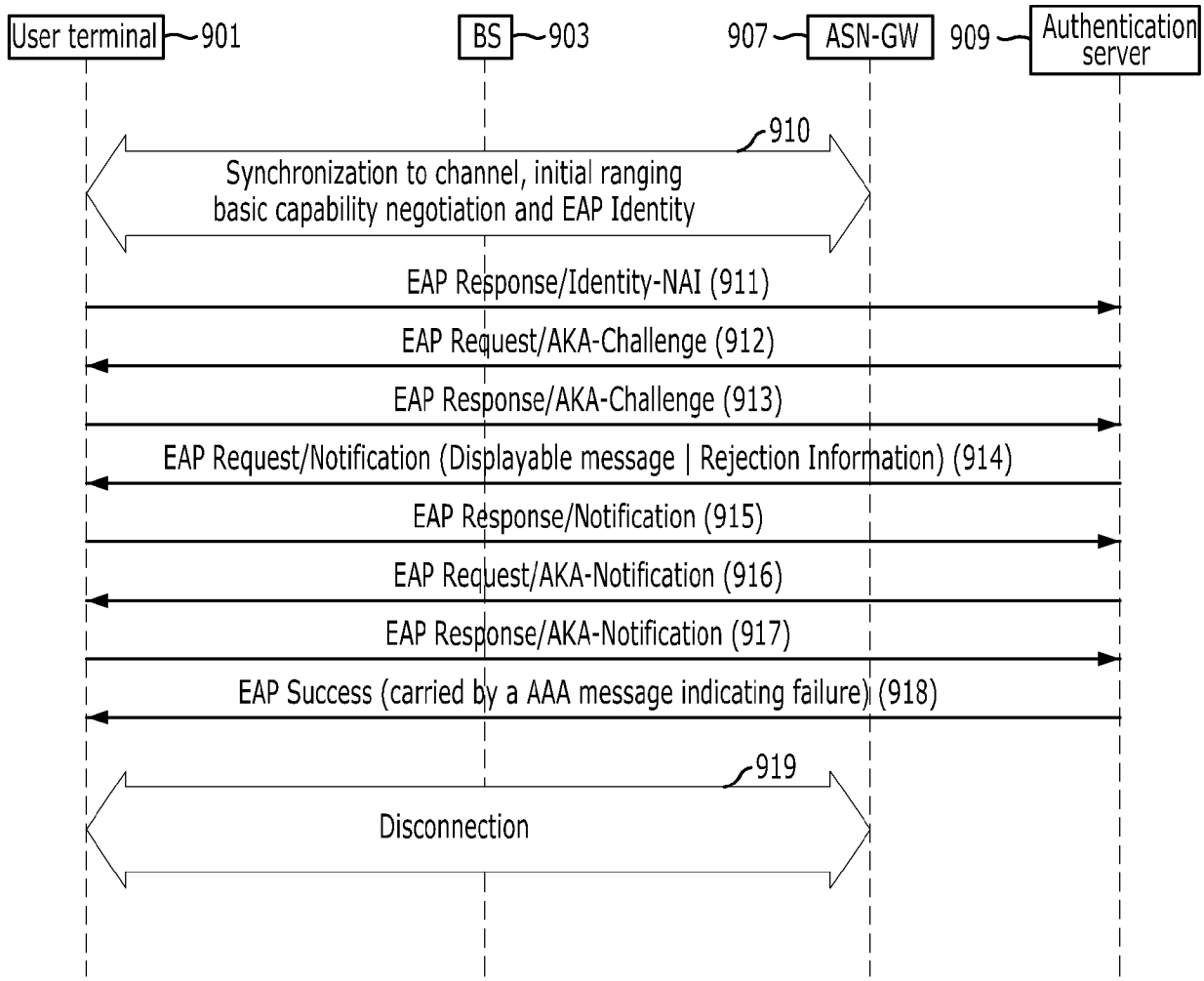
[Fig. 7]


User terminal
701
BS
703
705
ASN-GW
707
Authentication server
710
Synchronization to channel, initial ranging
basic capability negotiation and EAP Identity
EAP Response/Identity-NAI (711)
EAP Request/TLS-Start (712)
EAP Response/TLS(client_hello)-NAI (713)
EAP Request/TLS
(server_hello, certificate,[server_kye_exchange],
[certificate_request],server_hello_done (714)
EAP Response/TLS
(certificate,client_kye_exchange,[certificate_verify],change_cipher_spec,finished) (715)
EAP Request/TLS (change_cipher_spec,finished) (716)
EAP Response/TLS (No data) (717)
EAP Request/Notification (Displayable message | Rejection Information) (718)
EAP Response/Notification (719)
EAP Success (carried by a AAA message indicating failure) (720)
721
Disconnection

[Fig. 8]


User terminal
801
BS
803
805
ASN-GW
807
Authentication server
811
Synchronization to channel, initial ranging basic capability negotiation and EAP Identity
EAP Response/Identity-NAI (812)
EAP Request/TLS-Start (813)
814
TLS Handshake
EAP Response/EAP-TTLS (User-Name, MS-CHAP-Challenge,MS-CHAP2-Response) (815)
EAP Request/EAP-TTLS (MS-CHAP2-Success) (816)
EAP Response/RAP-TTLS (No data) (817)
EAP Request/Notification (Displayable message | Rejection Information) (818)
EAP Response/Notification (819)
EAP Success (carried by a AAA message indicating failure) (820)
821
Disconnection

[Fig. 9]


User terminal
901
BS
903
907
ASN-GW
909
Authentication server
910
Synchronization to channel, initial ranging
basic capability negotiation and EAP Identity
EAP Response/Identity-NAI (911)
EAP Request/AKA-Challenge (912)
EAP Response/AKA-Challenge (913)
EAP Request/Notification (Displayable message | Rejection Information) (914)
EAP Response/Notification (915)
EAP Request/AKA-Notification (916)
EAP Response/AKA-Notification (917)
EAP Success (carried by a AAA message indicating failure) (918)
919
Disconnection