



Patent Application

【Application Classification】 patent application

【Applicant】

【Name】 Samsung Electronics Corporation

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Agent】

【Name】 KWON HYUK ROK

【Agent's Code】 9 -1 99 8- 000 11 5 -1

【Registration number of general power of attorney】 200 2-0 60 5 19-2

【Agent】

【Name】 Lee Jeong Soon

【Agent's Code】 9 -1 99 8- 000 40 4 -2

【Registration number of general power of attorney】 200 5-00 5 29 7-6

【Title of Invention】 METHOD AND SYSTEM FOR AUTHENTICATING IN COMMUNICATION SYSTEM

【English Title of Invention】 M E T H O D A N D S Y S T E M F O R A U T H E N T I C A T I N G I N C O M M U N I C A T I O N S Y S T E M

【Inventor】

【Name】 Lee Ji Cheol

Samsung v. Four Batons
IPR2025-00495
Exhibit 1031





【Name in English】 Le e J i C heol
【Individual id number】 Secure Information
【Postal code or zip code】 Secure Information
【Address】 Secure Information
【Nationality】 K R

【Inventor】

【Name】 Alper Yegin
【Name in English】 Al per Y e g in
【Address】 Secure Information
【English Address】 Secure Information
【Nationality】 TR

【Purport】

It is submitted to the head of the Korean Intellectual Property Office as above.
Dae-ri In Kwon Hyuk Rock (Sing or In) Dae-ri In is Jeong-soon (Sing or In).

【Official Fee】

【Application Fee】 0 side 38,000 won
【Additional Application Fee】 39 page 0 won
【Priority Fee】 0 case 0 won
【Examination Fee】 0 claim 0 won
【Total】 38,000 won

【Abstract】

【Summary】

The present invention relates to a method and a system for authenticating a terminal in a communication system. The method for authenticating a terminal in a communication system comprises the steps of: requesting, by a first authentication server, a second authentication server to change an authentication server to enter a link layer of a terminal connected to a physical layer; transmitting, by the second authentication server, a hash value for an authentication variable to the first authentication server when the second authentication server includes the authentication variable of the terminal; transmitting, by the first authentication server, the hash value for the authentication variable provided from the second authentication server to a AAA server; determining, by the AAA server, validity of the hash value for the authentication variable provided from the first authentication server; and transmitting, by the AAA server, the authentication variable used when authenticating the terminal to the first authentication server when it is determined that the hash value for the authentication variable is valid.

【Representative Drawing】

Drawing5

【Index Term】

Authentication , E AP (E x t appreciable A use h entication Protocol),
CertificationAut h ent ic actuator, MS K (M ast er Se ssion K eye)

【Description of the Invention】

【Title of Invention】

Methods and systems for authentication in communication systems {M E T H O D A N D S Y S T E M F O R A U T H E N T I C A T I N G I N C O M M U N I C A T I O N S Y S T E M}

【The Detailed Description of the Invention】

【Technical Field】

【0001】 The present invention relates to a method and a system for authenticating a terminal in a communication system, and more particularly, to a method and a system for changing an authentication server of a terminal without performing a re-authentication procedure of the terminal in a communication system.

【Background Technique】

【0002】 In a communication system, a service provider performs an authentication procedure for a user to determine whether to subscribe to a user who intends to use a network service and whether to provide a service. For example, when an Extended Authentication Protocol (E AP) is used, the terminal and the AAA server perform an authentication procedure as illustrated in FIG. 1 through a serving network of the terminal. E AP is a real protocol such as MD 5 (Message Digest number 5), TLS (Transport Layer Security), SRP (Secure Remote Password), etc. A protocol for encapsulating and transmitting an authentication method (method) for authentication is shown.

【0003】 FIG. 1 illustrates an authentication procedure of a terminal in a wireless communication system according to the prior art.

【0004】 Referring to FIG. 1, when the terminal (Mobile Terminal (MT)) 100 has completed physical layer access (physical layer attachment)

with the authentication server (Authenticator) 110 (step 131), the terminal 100 and the authentication server 110 start a link layer entry procedure of the terminal 100. In this case, the authentication server 110 transmits an EAP request message (EAP Request/Link-layer) for requesting identification information for authentication of the terminal 100 to the terminal 100 (step 133). In this case, the terminal 100 and the authentication server 110 exchange signals through a base station located between the terminal 100 and the authentication server 110. Here, the EAP request message is defined as IEEE (Institute of Electrical and Electronics Engineers) 802.16 In the standard, PKMv2 PKM-REQ/EAP-Transfer.

【0005】 The terminal 100 transmits an EAP response message (EAP Response/Link-layer) including its own identification information to the authentication server 110 in response to the EAP request message (step 135). Here, the EAP response message is defined as PKM-RSP/EAP-Transfer in the IEEE 802.16 standard.

【0006】 The authentication server 110 includes the information included in the EAP response message in the AAA request message (EAP Response/AAA Request) and transmits the information to the AAA server 120 (step 137).

【0007】 The AAA server 120 determines an EAP authentication method (method) using the identification information of the terminal 100 confirmed through the AAA request message. Thereafter, the AAA server(120)The determined EAP authentication method information is transmitted to the terminal 100 through the authentication server 110 (13 steps 9 and 14 1).

【0008】 The terminal 100 checks the EAP authentication method determined by the AAA server 120 through the EAP request message provided from the authentication server 110. Thereafter, the terminal 100 transmits information necessary for the EAP authentication method to the AAA server

120 through the authentication server 110 (steps 143 and 145). In this case, the AAA server 120, the authentication server 110, and the terminal 100 repeatedly perform transmission and reception of EAP authentication method information and information necessary for the EAP authentication method (steps 13 to 145) several times in preparation for packet loss.

【0009】 The AAA server 120 determines whether the terminal 100 is authenticated using the information of the terminal 100 required for the EAP authentication method included in the AAA request message provided from the authentication server 110.

【0010】 If the terminal 100 can be authenticated, the AAA server 120 transmits an authentication success message to the terminal 100 through the authentication server 110 (steps 147 and 149).

【0011】 Accordingly, the terminal 100 completes the link layer connection with the authentication server 110 (step 151). In addition, when the link layer access between the terminal 100 and the authentication server 110 is completed, the AAA server 120 starts excessive gold for the authentication server 110 (AAA Accounting Start 15 step 3).

【0012】 The terminal that has been authenticated by the AAA server through the above-described authentication procedure and has succeeded in entering the link layer is provided with a network service.

【0013】 However, when the above-described authentication procedure is performed, the terminal may fail to enter the network due to a delay due to message transmission/reception between the authentication server and the AAA server. For example, when the terminal authenticated by the AAA server moves to a service area of another network or the authentication server is changed, the terminal needs to perform the authentication procedure as illustrated in FIG. 1 again. However, due to the delay due to the message transmission/reception between the authentication server and the AAA

server, the terminal may fail to enter the network.

【Content of Invention】

【Problem to solve】

【0014】 Accordingly, an object of the present invention is to provide a method and system for reducing a time delay according to authentication of a terminal in a communication system.

【0015】 Another object of the present invention is to provide a method and system for reducing a time delay due to authentication of a terminal when an authentication server (Authentic actuator) of the terminal is changed (relocation) in a communication system.

【0016】 Another object of the present invention is to provide a method and system for authenticating a terminal by using an authentication variable (Authentication parameter) used by another authentication server to authenticate the terminal in an authentication server of a communication system.

【Solution to the Problem】

【0017】 According to a first aspect of the present invention, there is provided a method for authenticating a terminal in a communication system, the method including: requesting, by a first authentication server, an authentication server change to a second authentication server to enter a link layer of a terminal accessing a physical layer; transmitting, by the second authentication server, a hash value for an authentication variable to the first authentication server when the second authentication server includes the authentication variable of the terminal; transmitting, by the first authentication server, the hash value for the authentication variable provided from the second authentication server to an AAA server; and transmitting, by the AAA server, the hash value for the



authentication variable provided from the first authentication server to the first authentication server. The method comprises the steps of: determining validity of a hash value for a received authentication variable; and transmitting, by the AAA server, an authentication variable used when authenticating the terminal to the first authentication server when the hash value for the authentication variable is determined to be valid.

【0018】 According to a second aspect of the present invention, there is provided a communication system for authenticating a terminal, the system including: a first authentication server (Authentication generator) configured to request a second authentication server to change an authentication server to enter a link layer of a terminal connected to a physical layer and transmit a hash value for an authentication variable of the terminal provided from the second authentication server to an AAA server; a second authentication server configured to transmit the hash value for the authentication variable of the terminal to the first authentication server according to an authentication server change request of the first authentication server when the terminal is authenticated by the AAA server before the terminal is connected to the physical layer; and the AAA server configured to transmit the authentication variable used when the terminal is authenticated to the first authentication server when the hash value for the authentication variable of the terminal provided from the first authentication server is determined to be valid.

【Effect】

【0019】 As described above, the authentication server of the communication system performs the authentication procedure of the terminal by using the authentication variable (Authentication parameter) used by another authentication server to authenticate the terminal, thereby reducing the time delay due to the EAP authentication.

【Detailed Description for the Implementation of the Invention】

【0020】 Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to the accompanying drawings. In addition, in the following description of the present invention, when it is determined that a detailed description of a related known function or configuration may unnecessarily obscure the gist of the present invention, the detailed description will be omitted. In addition, the terms described below are terms defined in consideration of functions in the present invention, which may vary depending on the intention of a user or an operator or customs. Therefore, the definition should be made based on the contents throughout the present specification.

【0021】 Hereinafter, the present invention describes a technology for reducing a delay due to Extension Authentication Protocol (E AP) authentication when a terminal is changed to an authentication server (Authentic actuator) in a communication system.

【0022】 In the following description, an authentication server requested to enter a link layer performs a data link entry procedure with a terminal using an authentication variable (Auth entry Parameter) used by another authentication server to authenticate the terminal requesting to enter the link layer. In this case, it is assumed that the other authentication server does not discard the authentication variable of the terminal. Here, the authentication variables include MS K (Master Session Key) and the effective time of MS K (lifetime).

【0023】 In the following description, another authentication server that has not discarded the authentication variable used for authentication of the terminal is referred to as a previous authentication server (Previous Authentic actuator: hereinafter referred to as PA). That is, the terminal and the AAA server performed the authentication procedure via the PA during

the previous time. The terminal is authenticated from the AAA server and PA comprises the authentication variable of the terminal.

【0024】 In the case of performing authentication between the AAA server, the authentication server, and the terminal, the wireless communication system is configured as shown in FIG. 2.

【0025】 2 shows the configuration of a wireless communication system according to the present invention.

【0026】 As illustrated in FIG. 2, the wireless communication system includes a AAA (Aut h entication, Aut h orization, Ac co mounting) server 200, an access gateway (Access Gate way) 210, 220, a base station 212, 222, and a terminal 230. Here, each of the access gateways includes an authentication server.

【0027】 When the terminal 230 accesses the base station 1 212, the terminal 230 performs an authentication procedure with the AAA server 200 through the access gateway 1 210. That is, the terminal 230 and the AAA server 200 perform an authentication procedure through the authentication server 1 included in the access gateway 1 210. For example, when the terminal 230 is initially connected, the terminal 230 and the AAA server 200 perform E AP authentication as illustrated in FIG. 1 through the authentication server 1.

【0028】 When the terminal 230 authenticated by the AAA server 200 moves to the service area of the base station 2 222, the access gateway providing the service to the terminal 230 is changed to the access gateway 2 220.

Accordingly, the authentication server 2 included in the access gateway 2 220 performs an authentication procedure for the terminal 230 using the authentication variable of the terminal 230 obtained from the authentication server 1. For example, the authenticationThe server 2 performs an authentication procedure for the terminal 230 as shown in FIG. 3 below. In this case, the authentication server 1 transmits a hash value (H hash value) for the authentication variable of the terminal 230 to the authentication

server 2.

【0029】 3 illustrates a procedure for authenticating a terminal in an authentication server according to an embodiment of the present invention.

【0030】 Referring to FIG. 3, first, the authentication server determines whether to perform a link layer entry procedure of the terminal in step 301. That is, the authentication server checks whether a link layer entry request signal is received from a terminal in which physical layer access (physical layer attachment) is completed.

【0031】 If the terminal performs the link layer entry procedure, the authentication server proceeds to step 302 to check the PA that passed when the terminal was authenticated from the AAA server before requesting the terminal to enter the link layer. For example, the authentication server may identify the PA through the link layer entry request signal or the handover request signal provided from the terminal. For another example, the authentication server may identify the PA through the location update request signal provided from the terminal. As another example, the authentication server may receive PA information of the terminal from a base station to which the terminal is newly accessed.

【0032】 After checking the PA, the authentication server proceeds to step 303 and requests the PA to change the authentication server of the terminal. For example, the authentication server includes a MAC layer address of a terminal attempting to enter a link layer and identifier information of the terminal. The blue signal is transmitted with PA.

【0033】 Thereafter, the authentication server proceeds to step 304 to check whether an authentication server change response signal is received from the PA.

【0034】 When the authentication server change response signal is received from the PA, the authentication server proceeds to step 305 to check

authentication information for the terminal in the authentication server change response signal. Here, the authentication information for the terminal includes a random variable 1 for authentication of the authentication server and the AAA server, a random variable 2 for authentication of the authentication server and the PA, a hash value for the authentication variable of the terminal, and identifier information of the terminal.

【0035】 After confirming the authentication information for the terminal, the authentication server proceeds to step 3 11 and transmits a hash value for the authentication variable of the terminal provided from the PA to the AAA server. For example, the authentication server transmits an authentication request signal including a hash value of an authentication variable of the terminal, a random variable 1, identifier information of the terminal, and identifier information of the terminal to the AAA server.

【0036】 Thereafter, the authentication server proceeds to step 3 13 to check whether the AAA server has accepted its authentication request through the AAA response signal provided from the AAA server.

【0037】 If the AAA server does not accept the authentication request, the authentication server recognizes that the authentication for the terminal has failed. Accordingly, the authentication server terminates this algorithm. For example, when the AAA server does not accept the authentication request, the authentication server performs E AP authentication on the terminal as shown in FIG. 1.

【0038】 On the other hand, when the AAA server accepts the authentication request, the authentication server proceeds to step 3 15 to generate a hash value for the authentication variable included in the AAA response signal. For example, the authentication server generates a hash value for an authentication variable included in the AAA response signal using a hash function considering the random variable 2 provided from the PA in step

309. For another example, the authentication server generates a key for generating a hash value using an authentication variable included in the AAA response signal. Thereafter, the authentication server may generate a hash value for the key using a hash function considering the random variable 2. **【0039】** After generating the hash value for the authentication variable, the authentication server proceeds to step 3 17 and transmits the generated hash value to the PA. For example, the authentication server transmits an authentication server change confirmation request signal including the generated hash value to the PA.

【0040】 Thereafter, the authentication server proceeds to step 3 19 to check whether an authentication server change confirmation response signal is received from the PA.

【0041】 If an authentication server change confirmation response signal is not received from the PA for a predetermined time or an authentication server change confirmation failure signal is received, the authentication server recognizes that the authentication server change for the terminal has failed. Accordingly, the authentication server terminates this algorithm. For example, when an authentication success response signal is not received from the PA for a predetermined time or an authentication server change failure signal is received, the authentication server performs E AP authentication for the terminal as shown in FIG. 1It.

【0042】 On the other hand, when an authentication server change confirmation response signal is received from the PA, the authentication server recognizes that data link entry of the terminal is successful.

【0043】 Thereafter, the authentication server terminates this algorithm.

【0044】 As described above, the authentication server performs authentication on the terminal using the authentication variable used by the PA for authentication of the terminal requesting entry into the link layer. In

this case, the AAA server performs authentication on the terminal as shown in FIG. 4 below.

【0045】 4 illustrates a procedure for changing an authentication server of a terminal in an AAA server according to an embodiment of the present invention.

【0046】 Referring to FIG. 4, the AAA server checks whether an authentication request signal is received from the authentication server in step 401.

【0047】 If the authentication request signal is received, the AAA server proceeds to step 40 and includes authentication information for the terminal included in the authentication request signal. Here, the authentication information for the terminal includes a hash value for an authentication variable of the terminal, a random variable 1, identifier information of the terminal, and identifier information of an authentication server transmitting an authentication request signal.

【0048】 Thereafter, the AAA server proceeds to step 405 to determine whether to accept the authentication request of the authentication server by using the hash value for the authentication variable of the terminal. For example, the AAA server checks an authentication variable used when authenticating the terminal through the identifier information of the terminal. Thereafter, the AAA server uses the random variable 1. The hash-value used when certifying the terminal about the authentication variable is produced. Thereafter, the AAA server compares the hash value provided from the authentication server with the generated hash value to determine whether to accept the authentication request for the authentication server.

【0049】 If the hash value provided from the authentication server is not the same as the generated hash value, the AAA server determines that the authentication request of the authentication server cannot be accepted because the hash value provided from the authentication server is not

valid. Accordingly, the AAA server proceeds to step 4 13 and transmits authentication failure information to the authentication server.

【0050】 On the other hand, in this case, when the hash value provided from the authentication server is the same as the generated hash value, the AAA server determines that the hash value provided from the authentication server is valid and accepts the authentication request of the authentication server. Accordingly, the AAA server proceeds to step 40 7 and transmits authentication success information to the authentication server. In this case, the authentication success information includes the number of authentication variables used when authenticating the terminal and address information of the AAA server.

【0051】 When the authentication request of the authentication server is accepted, the AAA server proceeds to step 40 9 to end the penalty for the PA of the terminal.

【0052】 In addition, when the terminal and the authentication server are completely entered into the link layer, the AAA server proceeds to step 411 and starts charging the authentication server requesting authentication in step 401.

【0053】 Thereafter, the AAA server terminates this algorithm.

【0054】 In the above-described embodiment, the AAA server generated a hash value for the authentication variable used when authenticating the terminal using the random variable 1.

【0055】 In another embodiment, the AAA server generates a key for generating a hash value using an authentication variable used when authenticating the terminal. Thereafter, the AAA server generates a hash value for the key using a random variable 1. Thereafter, the AAA server may compare the hash value provided from the authentication server with the generated hash value to determine whether to accept the authentication

request for the authentication server.

【0056】 Hereinafter, a procedure for changing an authentication server of a terminal in a wireless communication system will be described.

【0057】 5 illustrates a procedure for changing an authentication server of a terminal in a wireless communication system according to an embodiment of the present invention. Although not shown, each of the base stations is located between the terminal 500 and the authentication servers 510 and 520.

【0058】 Referring to FIG. 5, the terminal (M object T er minor (MT)) 500 and the AAA server 530 perform an authentication procedure through the first authentication server 510. In this case, it is assumed that the terminal 500 has succeeded in the authentication procedure with the AAA server 530 (step 541).

【0059】 If the terminal 500 authenticated by the AAA server 530 moves to perform physical layer access with the second authentication server 520 (step 543), the second authentication server 520 transmits an authentication server change request message (Aut h R el oc 1 nt i Re q) to the first authentication server 520 (step 545). Here, the authentication server change request message includes the MAC layer address of the terminal 500 and its own identifier information. At this time, The second authentication server 520 may identify the first authentication server 510 through a link layer entry request signal or a handover request signal provided from the terminal 500. For another example, the second authentication server 520 may identify the first authentication server 510 through the location update request signal provided from the terminal 500. For another example, the second authentication server 520 may receive the first authentication server 510 information from a base station to which the terminal 500 newly accesses.

【0060】 When the authentication server change request message is received, the first authentication server 510 generates a hash value for

an authentication variable of the terminal 500. For example, the first authentication server 510 generates a hash value for an authentication variable of the terminal 500 by using a hash function in consideration of random variable 1. For another example, the first authentication server 510 generates a key for generating a hash value by using an authentication variable of the terminal 500. Thereafter, the first authentication server 510 may generate a hash value for the key by using a hash function considering the random variable 1. Here, the authentication variable of the terminal 500 represents an authentication variable used when the first authentication server 510 authenticates the terminal 500.

【0061】 After generating the hash value, the first authentication server 510 transmits an authentication server change response message (Auth R el oc 1 nt iR sp) including the generated hash value to the second authentication server 520 (step 57). In this case, the authentication server change response message is a random variable 1 for authentication of the second authentication server 520 and the AAA server 530, a random variable 2 for authentication of the first authentication server 510 and the second authentication server 520, and a terminal 500. The authentication information about the terminal(500) including the identifier information of the hash value about the increase variable and terminal etc. is included.

【0062】 The second authentication server 520 checks authentication information for the terminal 500 in the authentication server change response message. Here, the authentication information for the terminal 500 includes the random variable 1, the random variable 2, the hash value for the authentication variable of the terminal 500, and the identifier information of the terminal, which are included in the authentication server change response message.

【0063】 Thereafter, the second authentication server 520 transmits an AAA

request message (AAA Request) including a hash value for the authentication variable of the terminal 500 to the AAA server 530 (step 54 9). In this case, the AAA request message includes a hash value for the authentication variable of the terminal 500, the random variable 1, the identifier information of the terminal 500, and the identifier information of the second authentication server 520.

【0064】 The AAA server 530 determines whether the hash value for the authentication variable of the terminal 500 provided from the second authentication server 520 is valid. For example, the AAA server 530 confirms an authentication variable used when authenticating the terminal 500 through the identifier information of the terminal 500 included in the AAA request message. Thereafter, the AAA server 530 generates a hash value for an authentication variable used when the terminal 500 is authenticated using the random variable 1 included in the AAA request message. Thereafter, the AAA server 530 compares the hash value provided from the second authentication server 520 with the generated hash value to determine whether the hash value provided from the second authentication server 520 is valid.

【0065】 If so, the hash value provided from the second authentication server (520) and the generated solution. When the hash values are the same, the AAA server 530 determines that the hash value provided from the second authentication server 520 is valid. Accordingly, the AAA server 530 transmits an AAA response message (AAA Re son sequence) including the authentication variable of the terminal 500 to the second authentication server 520 (step 55 1). In this case, the AAA response message includes the number of authentication variables of the terminal 500 and address information of the AAA server 530.

【0066】 On the other hand, when the hash value received from the second

authentication server 520 is not the same as the generated hash value, the AAA server 530 determines that the hash value received from the second authentication server 520 is not valid. Accordingly, the AAA server 530 transmits an AAA response message (AAA Re son sequence) including authentication failure information to the second authentication server 520.

【0067】 The second authentication server 520 checks whether the AAA server 530 has accepted authentication through the AAA response message provided from the AAA server 530.

【0068】 If the AAA server 530 accepts authentication, the second authentication server 520 generates a hash value for an authentication variable of the terminal 500 included in the AAA response message. For example, the second authentication server 520 generates a hash value for the authentication variable provided from the AAA server 530 using a hash function considering the random variable 2 provided from the first authentication server 510. For another example, the second authentication server 520 generates a key for generating a hash value using an authentication variable of the terminal 500 included in the AAA response message. Thereafter, the second authentication server 520 has a hash function considering the random variable 2 provided from the first authentication server 510. A hash value for the key may be generated by using the key.

【0069】 Thereafter, the second authentication server 520 transmits an authentication server change confirmation request message (Aut h R el oc F in Re q) including a hash value for the authentication variable of the terminal 500 to the first authentication server 510 (step 55 3).

【0070】 The first authentication server 510 determines whether the hash value for the authentication variable of the terminal 500 provided from the second authentication server 520 is valid. For example, the first authentication

server 510 generates a hash value for an authentication variable of the terminal 500 stored therein by using a hash function using the random variable 2 transmitted to the second authentication server 520. Thereafter, the first authentication server 510 compares the hash value provided from the second authentication server 520 with the generated hash value to determine the validity of the hash value for the authentication variable of the terminal 500 provided from the second authentication server 520.

【0071】 If the hash value provided from the second authentication server 520 is the same as the generated hash value, the first authentication server 510 determines that the hash value for the authentication variable of the terminal 500 provided from the second authentication server 520 is valid. Accordingly, the first authentication server 510 transmits an authentication server change acknowledgement message (Auth Reloc Fin Rsp) to the second authentication server 520 (step 555).

【0072】 When the first authentication server 510 determines that the hash value for the authentication variable of the terminal 500 provided from the second authentication server 520 is valid, the first authentication server 510 recognizes that the second authentication server 520 has been authenticated by the AAA server 530. Accordingly, the first authentication server 510 and the AAA server 530 terminate the billing processor (557-step).System).

【0073】 When the second authentication server 520 receives the authentication server change confirmation response message from the first authentication server 510, the second authentication server 520 recognizes that the data link entry of the terminal 500 is successful (step 559). Accordingly, the second authentication server 520 and the AAA server 530 start a charging processor (step 561).

【0074】 In the above-described embodiment, it is assumed that the PA does not discard the authentication variable of the terminal. However, when the



PA discards the authentication variable of the terminal, the PA may transmit the authentication server change failure signal to the authentication server requesting the change of the authentication server.

【0075】 Meanwhile, in the detailed description of the present invention, specific embodiments have been described, but various modifications are possible without departing from the scope of the present invention. Therefore, the scope of the present invention should not be limited to the described embodiments, but should be determined not only by the scope of the claims to be described below, but also by equivalents of the scope of the claims.

【Claims】

【Claim 1】

as to the method for certifying the terminal in the communications system

A process of requesting the first certificate server (Authentic actuator) is the certificate server change to the second certificate server for the link layer entry of the terminal connecting to the physical layer

a step of transmitting a hash value for the authentication variable to the first authentication server when the second authentication server includes the authentication variable of the terminal

a step in which the first authentication server transmits a hash value for an authentication variable provided from the second authentication server to an AAA (Authentication, Authorization, Accounting) server

A process of determining the AAA server is the validity of the hash value about the authentication variable which it is provided from the first certificate server

When it is determined that the hash value for the authentication variable is valid, the AAA server transmits the authentication variable used when authenticating the terminal to the first authentication server.

【Claim 2】

The method of claim 1,

The second certificate server is phase before the , terminal connects to the physical layer

A method characterized in that the terminal and the AAA server include an authentication server that has passed through for authentication when authentication has been received from the AAA server.

【Claim 3】

The method of claim 1,

The process of requesting the certificate server change to the second certificate server is ,

and transmitting, by the first authentication server, an authentication server change request message including at least one of a media access control (MAC) address of the terminal and an identifier address of the first authentication server to the second authentication server.

【Claim 4】

The method of claim 1,

A process of transmitting to the first certificate server is ,

The second authentication server transmits an authentication server change response message including at least one of a random variable 1, a random variable 2, a hash value for an authentication variable of a terminal, and identifier information of the terminal to the first authentication server.

【Claim 5】

The method of claim 1,

A process of transmitting to the first certificate server is ,

a step of generating a hash value for the authentication variable of the terminal by using a hash function considering random variable 1 when the second authentication server includes the authentication variable of the terminal

and transmitting the generated hash value to the first authentication server.

【Claim 6】

The method of claim 1,

A process of transmitting to the AAA server is ,

and transmitting, by the first authentication server, an AAA request message including at least one of the identifier information of the first authentication server, a hash value of an authentication variable of the terminal provided from the second authentication server, a random variable 1, and the identifier information of the terminal to the AAA server.



【Claim 7】

The method of claim 1,

A process of deciding the validity of the Hash value about the authentication variable is ,

The terminal corresponding to the terminal identifier which the AAA server is provided from the first certificate server

A process of confirming the authentication information which it used in the authentication of the word

The process , of being created the hash value about the authentication

information which the terminal used when authenticating by using the hash

function considering the random variable 1 provided from the first certificate server

and comparing the hash value for the authentication variable provided from

the first authentication server with the generated hash value to determine the

validity of the hash value for the authentication variable provided from the

first authentication server.

【Claim 8】

The method of claim 7,

A process of deciding the validity of the Hash value is ,

a step of determining that the hash value for the authentication variable

provided from the first authentication server is valid when the hash value for

the authentication variable provided from the first authentication server is the

same as the generated hash value

and determining that the hash value of the authentication variable received

from the first authentication server is not valid when the hash value of the

authentication variable received from the first authentication server is not the

same as the generated hash value.

【Claim 9】



The method of claim 1,
transmitting a hash value for an authentication variable used when the AAA server authenticates the terminal to the second authentication server when the first authentication server receives the authentication variable used when the AAA server authenticates the terminal from the AAA server
A process of determining the validity about the hash-value which the second certificate server is provided from the first certificate server
When it is determined that the hash value provided from the first authentication server is valid, the method further includes transmitting, by the second authentication server, authentication server change success information to the first authentication server.

【Claim 10】

The method of claim 9,
A process of transmitting to the second certificate server is ,
The first certificate server is a process of producing the hash value about the authentication variable which it used when the AAA server authenticates the terminal by using the hash function considering the random variable 2 provided from the second certificate server
and transmitting the generated hash value to the second authentication server.

【Claim 11】

The method of claim 9,
A process of determining the validity about the hash-value is ,
The second certificate server is a process of producing the hash value toward the authentication variable of the terminal it uses the hash function considering the random variable 2 transmitted from the first certificate server and comparing the hash value received from the first authentication server with the generated hash value to determine the validity of the hash value

received from the first authentication server.

【Claim 12】

The method of claim 11,

A process of deciding the validity of the Hash value is ,

a step of determining that the hash value received from the first authentication server is valid when the hash value received from the first authentication server is the same as the hash value generated from the first authentication server

and determining that the hash value received from the first authentication server is not valid when the hash value received from the first authentication server is not the same as the generated hash value.

【Claim 13】

The method of claim 1,

The method according to claim 1, wherein the authentication variable comprises M aster Se ssion K ey (MS K) and lif et time (MS K).

【Claim 14】

in the communications system for certifying the terminal ,

a first authentication server which requests an authentication server change to a second authentication server to enter a link layer of a terminal connected to a physical layer, and transmits a hash value for an authentication variable of the terminal provided from the second authentication server to an AAA (Aut h entication, Aut h orization, Ac counting) server

a second authentication server for transmitting a hash value for an authentication variable of the terminal to the first authentication server according to an authentication server change request of the first authentication server to an authentication server which the terminal and the AAA server pass through for authentication when the terminal is authenticated



from the AAA server before accessing the physical layer and an AAA server for transmitting an authentication variable used when authenticating the terminal to the first authentication server when it is determined that the hash value for the authentication variable of the terminal provided from the first authentication server is valid.

【Claim 15】

The method of claim 14,

The first authentication server transmits an authentication server change request message including at least one of a media access control (MAC) address of the terminal and an identifier address of the first authentication server to the second authentication server to request a change of the authentication server.

【Claim 16】

The method of claim 14,

The first authentication server transmits an AAA request message including at least one of identifier information of the first authentication server, a hash value of an authentication variable of a terminal provided from the second authentication server, a random variable 1, and identifier information of a terminal to the AAA server.

【Claim 17】

The method of claim 14,

The second authentication server transmits an authentication server change response message including at least one of a random variable 1, a random variable 2, a hash value of an authentication variable of a terminal, and identifier information of the terminal to the first authentication server according to an authentication server change request of the first authentication server.

【Claim 18】

The method of claim 14,

The second authentication server generates a hash value for an authentication variable of a terminal by using a hash function considering a random variable 1 according to an authentication server change request of the first authentication server.

【Claim 19】

The method of claim 14,

The AAA server generates a hash value for authentication information used when authenticating a terminal corresponding to a terminal identifier provided from the first authentication server using a hash function considering random variable 1 provided from the first authentication server, and compares the hash value for the authentication variable provided from the first authentication server with the generated hash value to determine validity of the hash value for the authentication variable provided from the first authentication server.

【Claim 20】

The method of claim 19,

When the hash value for the authentication variable provided from the first authentication server and the generated hash value are the same, the AAA server determines that the hash value for the authentication variable provided from the first authentication server is valid

When the hash value of the authentication variable provided from the first authentication server is not the same as the generated hash value, the communication system determines that the hash value of the authentication variable provided from the first authentication server is not valid.

【Claim 21】

The method of claim 14,

The first authentication server transmits a hash value for an authentication variable used when the AAA server authenticates the terminal to the second authentication server when the AAA server receives the authentication variable used when the AAA server authenticates the terminal from the AAA server

When it is determined that the hash value provided from the first authentication server is valid, the second authentication server transmits authentication server change success information to the first authentication server.

【Claim 22】

The method of claim 21,

The first authentication server generates a hash value for an authentication variable used when the AAA server authenticates the terminal by using a hash function considering random variable 2 provided from the second authentication server.

【Claim 23】

The method of claim 21,

The second authentication server generates a hash value for an authentication variable of the terminal using a hash function considering random variable 2 transmitted from the first authentication server, and compares the hash value provided from the first authentication server with the generated hash value to determine validity of the hash value provided from the first authentication server.

【Claim 24】

The method of claim 23,

When the hash value provided from the first authentication server is the same



as the generated hash value, the second authentication server determines that the hash value provided from the first authentication server is valid

When the hash value received from the first authentication server is not the same as the generated hash value, the communication system determines that the hash value received from the first authentication server is not valid.

【Claim 25】

The method of claim 14,

The authentication variable is the effective time (lifetime) of the MS K and , MS K (Master Session Key)A communication system characterized by comprising.



【Description of Drawings】

【0076】 1 is a diagram illustrating an authentication procedure of a terminal in a wireless communication system according to the prior art

【0077】 2 is a diagram showing the configuration of a wireless communication system according to the present invention

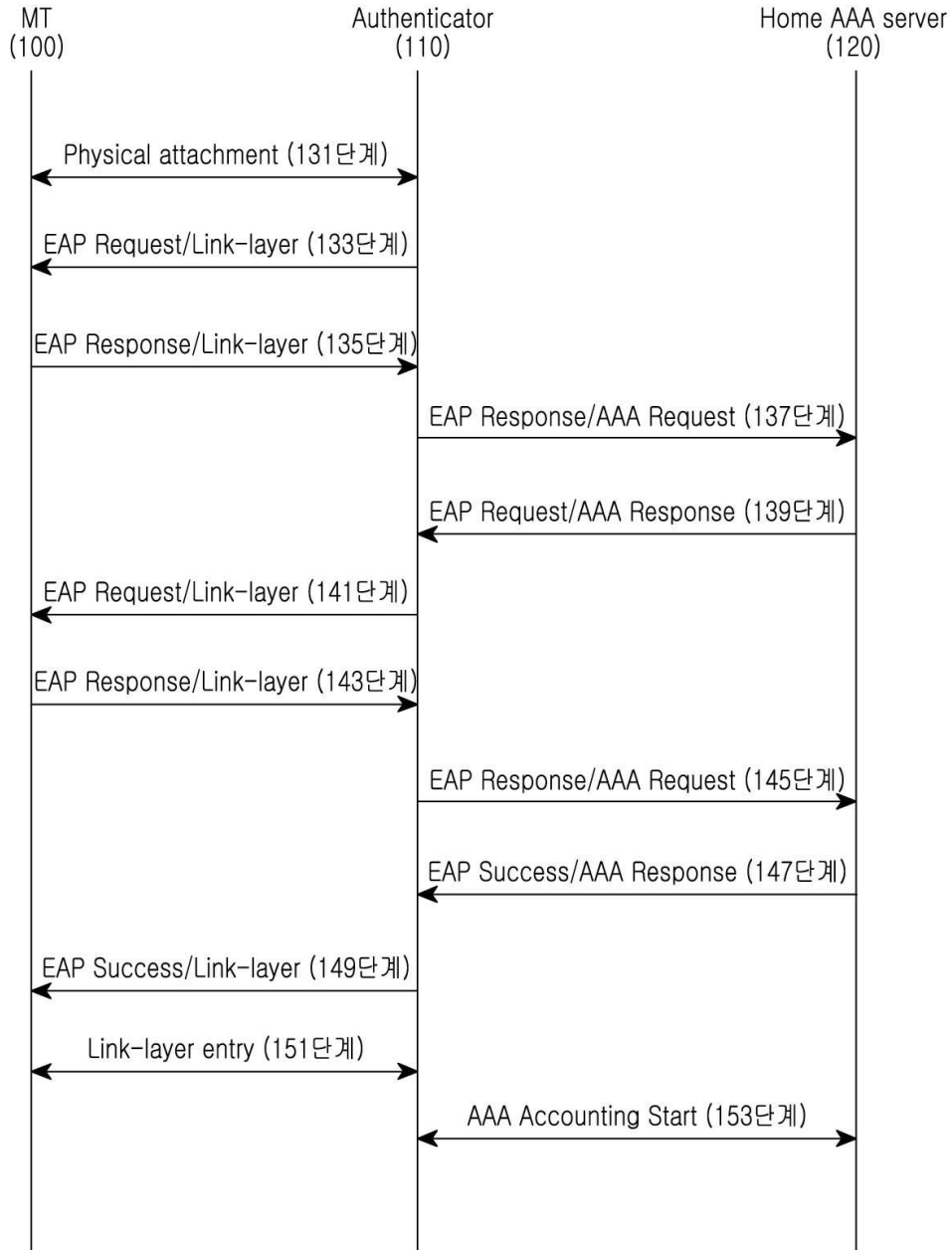
【0078】 3 is a diagram illustrating a procedure for authenticating a terminal in an authentication server according to an embodiment of the present invention

【0079】 4 is a diagram showing a procedure for changing an authentication server of a terminal in an AAA server according to an embodiment of the present invention

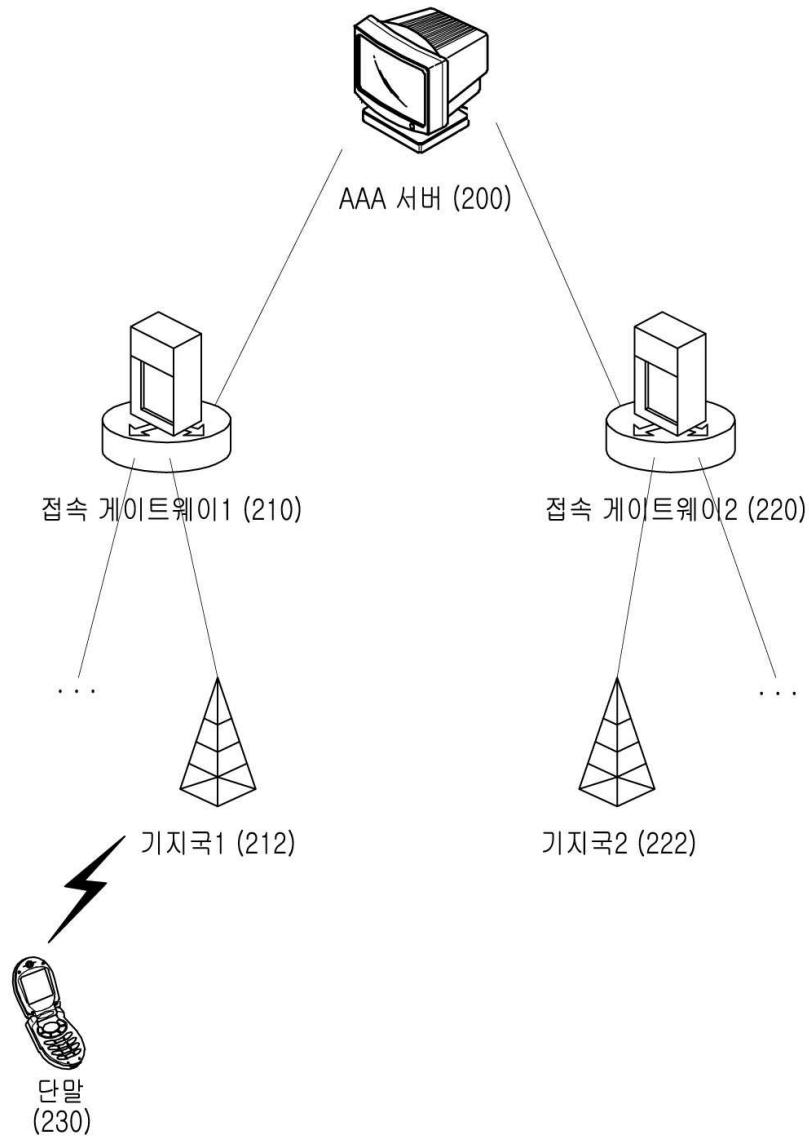
【0080】 5 is a diagram illustrating a procedure for changing an authentication server of a terminal in a wireless communication system according to an embodiment of the present invention.

【Drawings】

【Drawing 1】

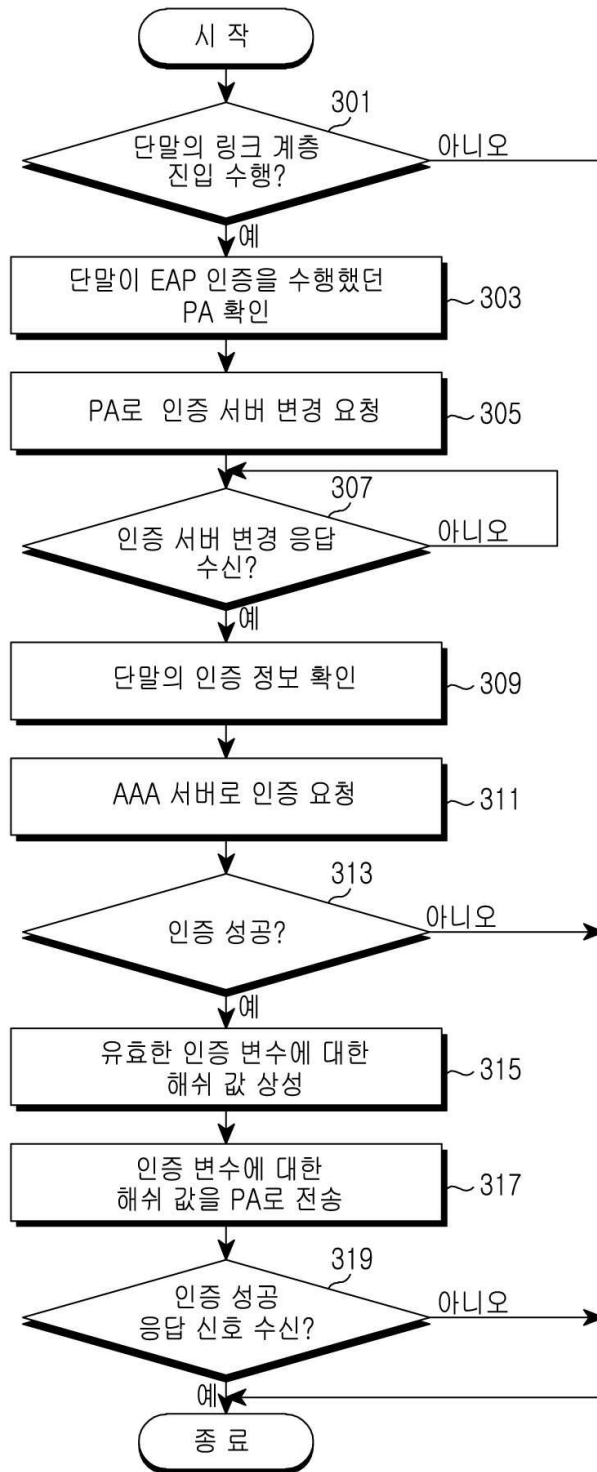


【Drawing 2】



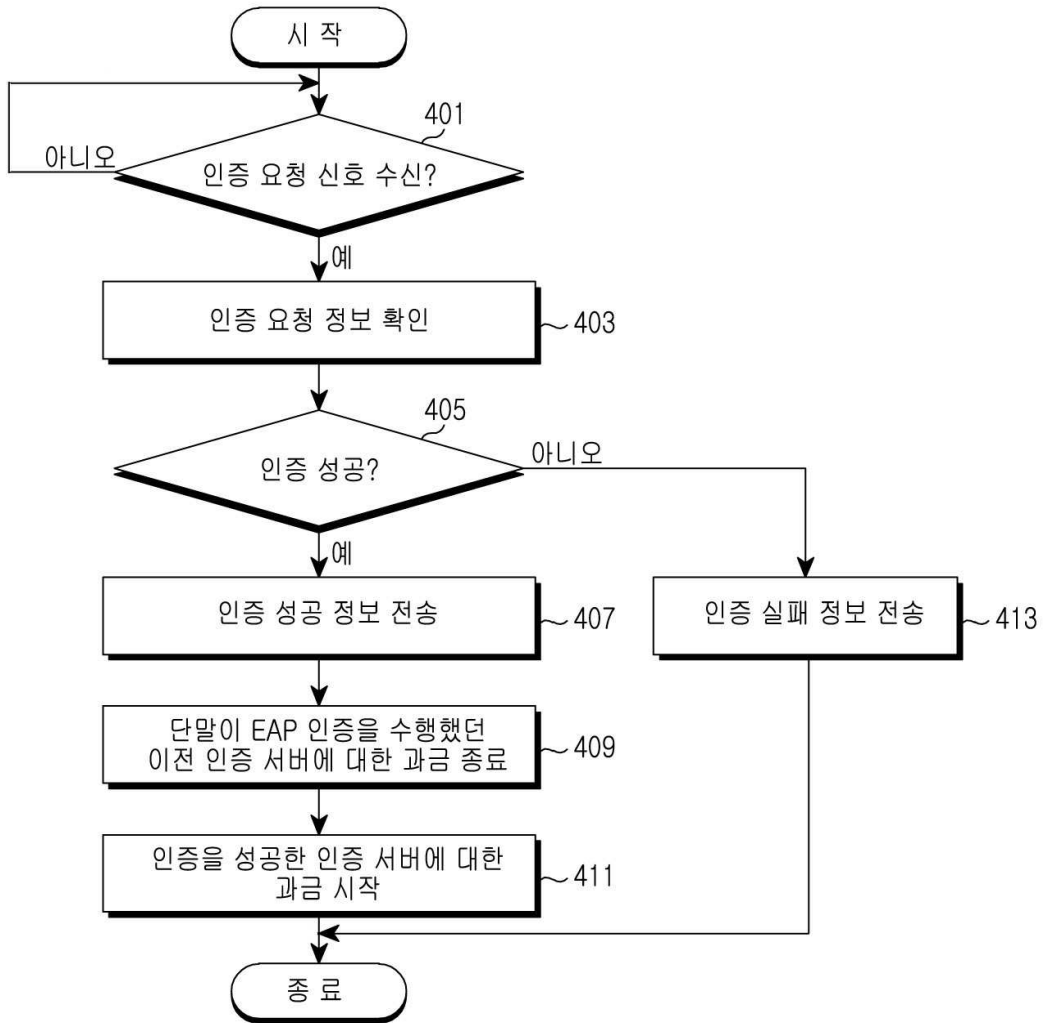


【Drawing 3】

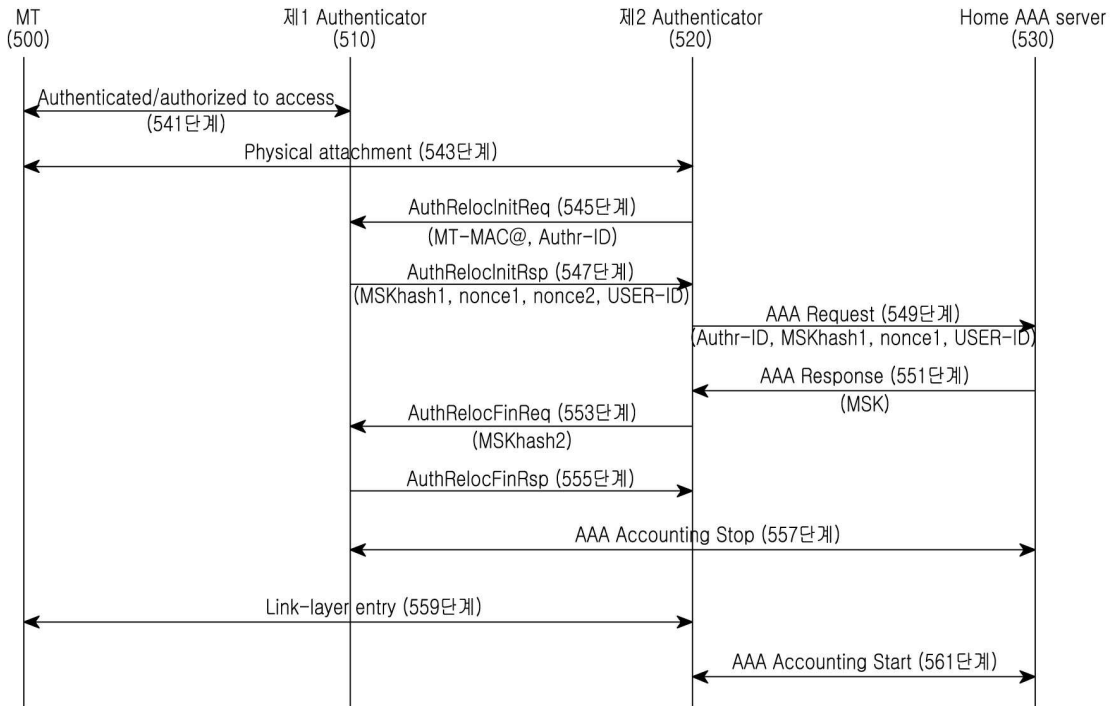




【Drawing 4】



【Drawing 5】





Request for Examination

【Classification】 examination request

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Agent】

【Name】 KWON HYUK ROK

【Agent's Code】 9 -1 99 8- 000 11 5 -1

【Registration number of general power of attorney】 200 2-0 60 5 19-2

【Agent】

【Name】 Lee Jeong Soon

【Agent's Code】 9 -1 99 8- 000 40 4 -2

【Registration number of general power of attorney】 200 5-00 5 29 7-6

【Mark of events】

【Application Number】 10 -200 9- 00 20 3 18

【Title of Invention】 METHOD AND SYSTEM FOR AUTHENTICATING IN COMMUNICATION SYSTEM



【Official Fee】

【Examination Fee】 25 clauses 1, 1 30 thousand won

【Purport】

It is submitted to the head of the Korean Intellectual Property Office as above.

Dae-ri In Kwon Hyuk Rock (Sing or In) Dae-ri In is Jeong-soon (Sing or In).

Sending
 number : 9-5-2015-039722915
Dispatche
 d date : 2015.06.15.
Submissio
 n due 2015.08.15.
 date :

YOUR INVENTION PARTNER

Intellectual Property Office



Request for the Submission of an Opinion

A p p l i c a n t N a m e SAMSUNG ELECTRONICS CO., LTD.(Applicant Code:
 119981042713)

Address

A g e n t N a m e a person besides KWON HYUK ROK

Address

I n v e n t o r N a m e Lee Ji Cheol

Address

I n v e n t o r N a m e Alper Yegin

Address

A p p l i c a t i o n N o 10-2009-0020318

A p p l i c a t i o n d a t e 2009.03.10.

T i t l e o f I n v e n t i o n METHOD AND SYSTEM FOR AUTHENTICATING IN COMMUNICATION
 SYSTEM

1. Because of having the reason for refusal like the examination result next about this application and notifying of this according to the article 63 of Patent Act in case it has the opinion or the correction is needed or it wants opinion (the reply, and the Written Reply) to submit the Amendment [form of attached document No.9 of Enforcement Regulation of Patent Act].

2. In the case to extend the submission due date (2015.08.15.), the due date of submission of the can be extended through the request for an extension of designated period to 4 month. In this case, request for the extension has to do by unit of 1 month and 2 month or greater is summed up in the need in the range that does not exceed 4 month and it can request the extension. The Written Substantiation describing the proprietary is additionally attached in the time for to postponing the designated period to the generation (the guideline reference of the lower part) of the inevitable proprietary in excess of 4 month and request for the extension has to be applied.

[Examination result]

Subject of Claim 1-25
examination claim:

The law articles in connection with the part in which it has the reason for refusal of this application

Sequence number	The part in which it has the reason for refusal	Related law articles
1	Claim preceding clause	The article 29(2) of Patent Act

[The detailed reason for refusal]

The invention described in claim preceding clause of the patent claim of this application cannot receive patent like the lower part according to the article 29(2) of Patent Act since a person having ordinary skill in the art to which the invention pertains easily can invent before the application.

- Follows -

Cited invention 1:KR10-2008-0050971 A(2008.06.10.)

Cited invention 2 : 3GPP TS 23.401 v8.4.1 (2008.12)

Cited invention 3:US2003/0028763 A(2003.02.06.)

a. The application and cited invention

This application is the invention about the terminal certification method at the communication system.

In the cited invention 1 is the heterogeneous wireless network interworking Sisson, it is the invention about the authentication method required for the roaming.

The cited invention 2 is 3GPP TS 23.401 (v8.4.1) standard document.

The cited invention 3 is the invention about the authentication of being modulated for the internet protocol and authentication design.

The application and the method in which the cited invention 1 reduces the time delay according to the authentication of the terminal are provided but the method have the common-point of the effect and purpose.

b. The comparison of the configuration

1) Claim 1 invention

In claim 1 invention is the communication system, case, the case where as to the process, of transmitting the hash value about the authorization parameter with the first certificate server the authenticated user terminal moves from the cited invention 1 to the second wireless-network from the first wireless-network, IMSI,

reserved authentication vectors, CK, IK, the KSI (Key Set Identifier), the IdType showing the kind of the user identifier used for the MK calculation, and the Counter final value as the necessary information in the rapid reapproval and NxReAuthID in MSK and EAP-AKA in which the first certificate server (Authenticator) includes the process of requesting the certificate server change as the second certificate server for the link layer entry of the terminal connecting to the physical layer, and the second certificate server is the authorization parameter (Authentication Parameter) of the terminal are included in the invention about the method for authenticating the terminal. (figure 5.3.2.1-1, Figure 5.3.3.1-1, Figure 5.3.3.2-1 etc) new MME (the first certificate server of the application) requests the context in the cited invention 2 as the old MME (the second certificate server of the application). As to IMSI, the second verification apparatus of the second wireless-network obtains authentication data from the first verification apparatus of the first wireless-network using the user identifier and which is the permanent identifier of the user in authentication data. CK is the busy. The KSI (Key Set Identifier) is the connected key index value. The kinds calculates the final key value of the user terminal which the authentication subject of the second verification apparatus including the AAA server the transmission the hash value about the authorization parameter, and the process of transmitting the authorization parameter uses in the first wireless-network using authentication data the difference of more or less in the explicit material side the response about the corresponding context can be easily drawn from the point that it obtains. It delivers to the HSS (the corresponding in the AAA server of the application) based on the context which (figure 5.3.2.1-1, Figure 5.3.3.1-1, Figure 5.3.3.2-1 etc) new MME receives in point, and the cited invention 2 from the old MME it is the matter which is obvious to the normal technical engineer to verify validity and the authorization parameter which it used when HSS authenticated UE if the context was effective is transmitted with the new MME. The cited invention 3 transmits the authorization parameter (the MAC SRES value etc) calculated by the hash function in ([0080] - [0187]) AAA server (AGW/AAA Home Server). The AAA server the transmission the hash value about the authorization parameter the first certificate server receives from the second certificate server. The process of transmitting the authorization parameter used when it judged validity and the AAA server authenticated the terminal if it was effective with the first certificate server is the AAA function in the cited invention 1. The normal technical engineer easily can draw from the etc. that if the hash value is effective, the AAA server includes and returns the authentication parameter.

2) Claim 2-5 invention

As to claim 2-5 invention. In the configuration, added from the point that it includes transmitting the context response message in which the configuration added from the point that it transmits the context request message in which the

configuration added in claim 2 invention includes the case where the authenticated user terminal moves from the cited invention 1 to the second wireless-network from the first wireless-network, the configuration, and the MME Address etc with the old MME in claim 4-5 invention includes the identifier of the terminal in the cited invention 2, authorization parameter ***, and the random variable etc with the new MME in claim 5 invention the old MME IMSI, the ME Identity (if available), MSISDN, unused EPS Authentication Vectors, KSIASME, KASME, EPS Bearer Context (s), serving GW signalling Address and TEID (s), ISR Supported, UE Core Network Capability in the cited invention 2. As to the configuration, the second verification apparatus of the second wireless-network obtains authentication data from the first verification apparatus of the first wireless-network using the user identifier and which is added from the point that UE was authenticated from the HSS server (AAA server) in the cited invention 2 through the old MME (second certificate server) in claim 3 invention. The new MME (first certificate server) is the old GUTI in the cited invention 2. The normal technical engineer easily can draw from the point that it transmits the Context Response message including the UE Specific DRX Parameters etc. with the new MME.

3) Claim 6-8 invention

The message in which the configuration added in claim 6-8 invention includes the new MME is the identifier of the terminal in the cited invention 2, and authorization parameter is transmitted with the HSS server (AAA server). The HSS server verifies the validity about the authorization parameter. The cited invention 3 transmits the authorization parameter (the MAC SPRES value etc) calculated by the hash function in ([0080] - [0187]) AAA server (AGW/AAA Home Server) and the normal technical engineer can draw from the etc. that if the hash value is effective, the AAA server includes and returns the authentication parameter.

4) Claim 9-12 invention

With it corresponds to the substitution of the technique means of the extent in which generally the configuration added in claim 9-12 invention can be employed by the normal technical engineer from the cited invention 1, and 2 as the specificity means for the object of the invention achievement or the addition the special difference is not generated in the object of the invention and effect with the change.

5) Claim 13 invention

The normal technical engineer as to the configuration, added in claim 13 invention easily can draw in the cited invention 2 from the etc. to include the master key information in the authorization parameter.

6) Claim 14-25 A invention

The reason for refusal of the same purpose is applied since claim 1, and 3, 6, 4, 5, 7-13 invention and technical mapping as to claim 14, 15, 16, 17, 18, 19-25 A invention, are substantially the same.

c. Sintering lawn

Therefore, the normal technical engineer this application easily can draw from the cited invention 1, 2, and the combination of 3.

[Appendix]

Appendix 1 10-2008-0050971 A (2008.06.10.) one copy.

Appendix 2 3GPP TS 23.401 (v8.4.1) (2008.12.) one copy.

Appendix 3 US2003/0028763 A (2003.02.06.) one copy. end.



Amendment to Bibliographic Information

【Classification】 specification etc. correction

【Submitter】 patent office field

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Agent】

【Name】 KWON HYUK ROK

【Agent's Code】 9 -1 99 8- 000 11 5 -1

【Registration number of general power of attorney】 200 2-0 60 5 19-2

【Agent】

【Name】 Lee Jeong Soon

【Agent's Code】 9 -1 99 8- 000 40 4 -2

【Registration number of general power of attorney】 200 5-00 5 29 7-6

【Mark of events】

【Application Number】 10 -200 9- 00 20 3 18



【Dispatch number that caused the submission】 9-5-20 15-0 39 7 22 9-15

【Documents to be corrected】 specification etc

【What to correct】

【Items to be corrected】 like a star

【Correction method】 like a star

【Correction contents】 like a star

【Number of additional claims】 13

【Purport】

As described above, it is submitted to the head of the Korean Intellectual Property Office (the head of the Patent Tribunal, the head of the Tribunal).

【Official Fee】

【Amendment Fee】 4,000,000 won

【Additional fees for examination requests】 5 20,000 won

【Other fees】 0 won

【Total】 524,000 won

Amendment

【Correction item】 Identification number 17

【Correction method】 Change

【Correction content】

【0017】 According to a first aspect of the present invention, there is provided a method for authenticating a terminal in a communication system, the method including: transmitting a first message from a first authentication server to a second authentication server, the first message including identification information of the first authentication server; transmitting a second message from the second authentication server to the first authentication server in response to the first message, the second message including a first hash value, a first random variable, and a second random variable, the first hash value being generated based on a hash function using the first random variable; transmitting a third message from the first authentication server to an AAA server, the AAA server including the first hash value, the first random variable, and the identification information of the first authentication device; determining validity of the first hash value; transmitting a fourth message from the AAA server to the first authentication server in response to the third message when it is determined that the first hash value is valid; transmitting a fifth message from the first authentication server to the second authentication server, the fourth message including an authentication variable of the terminal; determining validity of the second hash value in the second authentication device; and transmitting a sixth message from the second authentication server to the first authentication server in response to the fifth message when it is determined that the

【Correction item】 Identification number 18

【Correction method】 Change

【Correction content】

【0018】 According to a second aspect of the present invention, a communication system for authenticating a terminal includes a first authentication server, a second authentication server, and an AAA server, wherein the first authentication server transmits a first message to the second authentication server, the first message includes identification information of the first authentication server, the second authentication server transmits a second message to the first authentication server in response to the first message, the second message includes a first hash value, a first random variable number, and a second random variable, the first hash value is generated based on a hash function using the first random variable, the first authentication server transmits a third message to the AAA server, the third message includes the first hash value, the first random variable number, and the identification information of the first authentication server, the AAA server determines validity of the first hash value, and transmits a fourth message to the first authentication server when it is determined that the first hash value is valid, the fourth message includes an authentication variable of the terminal, the first authentication server transmits a fifth message to the second authentication server, the fifth message includes a second hash value, the second hash value is generated based on a hash function using the second random variable, the second authentication server determines validity of the second hash value, and transmits a sixth

According to a third aspect of the present invention, there is provided a method of authenticating a terminal in an authentication server, the method including: transmitting a first message to a second authentication server, wherein the first message includes identification information of the first authentication server; identifying a first hash value, a first random variable number, and a second random variable in the second message when the

second message is received from the second authentication server, wherein the first hash value is generated based on a hash function using the first random variable; and transmitting a third message to a AAA server, wherein the third message includes the first hash value, the first random variable number, and the identification information of the first authentication server, and when a fourth message is received from the AAA server, identifying an authentication variable of the terminal in the fourth message; and transmitting a fifth message to the second authentication server, wherein the fifth message includes a second hash value, wherein the second hash value is generated based on a hash function using the second random variable, and receiving a sixth message from the second authentication server in response to the fifth message, wherein when the first hash value included in the third message is determined to be valid, the fourth message is received, and when the second hash value included in the fifth message is determined to be

【Correction item】 Claim 1

【Correction method】 Change

【Correction content】

【Claim 1】

as to the method for certifying the terminal in the communications system a step of transmitting a first message from a first authentication server to a second authentication server, wherein the first message includes identification information of the first authentication server a step of transmitting a second message from the second authentication server to the first authentication server in response to the first message, wherein the second message includes a first hash value, a first random variable, and a second random variable, and the first hash value is generated based on a hash function using the first random variable

a step of transmitting a third message from the first authentication server to an AAA server, wherein the third message includes a first hash value, a first random variable number, and the identification information of the first authentication device

a step of determining the validity of the first hash value in the AAA server

a step of transmitting a fourth message from the AAA server to the first authentication server in response to the third message when the first hash value is determined to be valid, wherein the fourth message includes an authentication variable of a terminal

transmitting a fifth message from the first authentication server to the second authentication server, wherein the fifth message includes a second hash value, and the second hash value is generated based on a hash function using the second random variable

A process of deciding the validity of the , second hash-value in the second verification apparatus

and transmitting a sixth message from the second authentication server to the first authentication server in response to the fifth message when the second hash value is determined to be valid.

【Correction item】 Claim 2

【Correction method】 Change

【Correction content】

【Claim 2】

The method of claim 1,

When the second authentication server is authenticated by the AAA server before the terminal accesses the physical layer, the second authentication server includes an authentication server that the terminal and the AAA server have passed for authentication.



【Correction item】 Claim 3

【Correction method】 Delete

【Correction item】 Claim 4

【Correction method】 Delete

【Correction item】 Claim 5

【Correction method】 Delete

【Correction item】 Claim 6

【Correction method】 Change

【Correction content】

【Claim 6】

The method of claim 1,

The first random variable includes CM AC K E Y CO U N T E R.

【Correction item】 Claim 7

【Correction method】 Change

【Correction content】

【Claim 7】

The method of claim 1,

A process of deciding the validity of the first hash-value is ,

The process of confirming the authentication information which it used when authenticating the , terminal in the AAA server

a step of generating a third hash value based on a hash function using the verified authentication information and the first random variable received from the first authentication server in the AAA server

and comparing, by the AAA server, the first hash value with the third hash

value, and determining the validity of the first hash value based on a result of



the comparison.

【Correction item】 Claim 8

【Correction method】 Delete

【Correction item】 Claim 9

【Correction method】 Delete

【Correction item】 Claim 10

【Correction method】 Delete

【Correction item】 Claim 11

【Correction method】 Change

【Correction content】

【Claim 11】

The method of claim 1,

A process of deciding the validity of the second hash-value is ,

a step of generating a fourth hash value based on a hash function using the second random variable in the second authentication server

The second authentication server compares the second hash value with the fourth hash value, and determines the validity of the second hash value based on the comparison result.

【Correction item】 Claim 12

【Correction method】 Delete

【Correction item】 Claim 13

【Correction method】 Delete

【Correction item】 Claim 14

【Correction method】 Change

【Correction content】**【Claim 14】**

in the communications system for certifying the terminal ,

First authentication server;

Second authentication server; and

AAA (Aut h entication , Aut h orization , Ac counting) server is included

The first authentication server transmits a first message to the second authentication server, wherein the first message includes identification information of the first authentication server

The second authentication server transmits a second message to the first authentication server in response to the first message, wherein the second message includes a first hash value, a first random variable number, and a second random variable, wherein the first hash value is generated based on a hash function using the first random variable

The first authentication server transmits a third message to the AAA server, wherein the third message includes the first hash value, the first random variable number, and the identification information of the first authentication server

The AAA server determines validity of the first hash value, and transmits a fourth message to the first authentication server when the first hash value is determined to be valid, wherein the fourth message includes an authentication variable of a terminal

The first authentication server transmits a fifth message to the second authentication server, wherein the fifth message includes a second hash value, wherein the second hash value is generated based on a hash function using the second random variable

The second authentication server determines validity of the second hash value, and transmits a sixth message to the first authentication server in

response to the fifth message.

【Correction item】 Claim 15

【Correction method】 Delete

【Correction item】 Claim 16

【Correction method】 Delete

【Correction item】 Claim 17

【Correction method】 Change

【Correction content】

【Claim 17】

The method of claim 14,

The second authentication server includes an authentication server through which the terminal and the AAA server pass for authentication when the terminal is authenticated by the AAA server before connecting to the physical layer.

【Correction item】 Claim 18

【Correction method】 Change

【Correction content】

【Claim 18】

The method of claim 14,

The first random variable is a communication system including C M A C K E Y C O U N T E R.

【Correction item】 Claim 19

【Correction method】 Change

【Correction content】

【Claim 19】

The method of claim 14,

When determining that the first hash value is valid, the AAA server generates a third hash value for authentication information used when the terminal authenticates based on a hash function using the first random variable received from the first authentication server, compares the third hash value with the first hash value, and determines the validity of the first hash value based on the comparison result.

【Correction item】 Claim 20

【Correction method】 Delete

【Correction item】 Claim 21

【Correction method】 Delete

【Correction item】 Claim 22

【Correction method】 Delete

【Correction item】 Claim 23

【Correction method】 Change

【Correction content】

【Claim 23】

The method of claim 14,

The second authentication server generates a fourth hash value based on a hash function using the second random variable, compares the second hash value with the fourth hash value, and determines the validity of the second hash value based on the comparison result.

【Correction item】 Claim 24

【Correction method】 Delete



【Correction item】 Claim 25

【Correction method】 Delete

【Correction item】 Claim 26

【Correction method】 Add

【Correction content】

【Claim 26】

as to the method for certifying the terminal in the certificate server

The process , first message transmitting the first message with the second certificate server comprises the identifying information of the , first certificate server

a step of confirming a first hash value, a first random variable number, and a second random variable in the second message when the second message is received from the second authentication server, wherein the first hash value is generated based on a hash function using the first random variable transmitting a third message to an Authentication (AAA) server, wherein the third message includes a first hash value, a first random variable number, and the identification information of the first authentication server

a step of checking an authentication variable of the terminal in the fourth message when the fourth message is received from the AAA server

The process , fifth message transmitting the fifth message with the second certificate server comprises the , second hash value. And the second hash value is generated based on the hash function using the , second random variable

A process of receiving a message the sixth message from the response about the fifth message from the second certificate server is included

When it is determined that the first hash value included in the third message is valid, the fourth message is received, and when it is determined that the

second hash value included in the fifth message is valid, the sixth message is received.

【Correction item】 Claim 27

【Correction method】 Add

【Correction content】

【Claim 27】

The method of claim 26

The method of claim 1, further comprising identifying the second authentication server before receiving the first message.

【Correction item】 Claim 28

【Correction method】 Add

【Correction content】

【Claim 28】

The method of claim 26

The method wherein the first random variable comprises CM A C K E Y C O U N T E R.

【Correction item】 Claim 29

【Correction method】 Add

【Correction content】

【Claim 29】

The method of claim 26

The method further comprising: after receiving the fifth message, when the sixth message is received from the second authentication server, recognizing that the terminal succeeds in accessing the data link layer.

【Correction item】 Claim 30



【Correction method】 Add

【Correction content】

【Claim 30】

The method of claim 26

The first message may further include identification information of the terminal.

【Correction item】 Claim 31

【Correction method】 Add

【Correction content】

【Claim 31】

The method of claim 26

The method further comprising: successfully authenticating, by the terminal, the second authentication server before the first message is transmitted; and performing physical layer entry with the first authentication server.

【Correction item】 Claim 32

【Correction method】 Add

【Correction content】

【Claim 32】

The method of claim 26

The method further comprising: storing, by the first authentication server, the received second random variable.

【Correction item】 Claim 33

【Correction method】 Add

【Correction content】

【Claim 33】

The method of claim 1,

The first message may further include identification information of the terminal.

【Correction item】 Claim 34

【Correction method】 Add

【Correction content】**【Claim 34】**

The method of claim 1,

Before the first message is transmitted, the method further includes successfully authenticating, by the terminal, the second authentication server, and performing physical layer entry with the first authentication server.

【Correction item】 Claim 35

【Correction method】 Add

【Correction content】**【Claim 35】**

The method of claim 1,

The method further comprising: storing, by the first authentication server, the received second random variable.

【Correction item】 Claim 36

【Correction method】 Add

【Correction content】**【Claim 36】**

The method of claim 14,

The communication system wherein the first message further includes identification information of the terminal.

【Correction item】 Claim 37

【Correction method】 Add

【Correction content】

【Claim 37】

The method of claim 14,

The terminal successfully authenticates the second authentication server before the first message is transmitted, and performs physical layer entry with the first authentication server.

【Correction item】 Claim 38

【Correction method】 Add

【Correction content】

【Claim 38】

The method of claim 14,

The communication system in which the first certificate server stores the received second random variable as described above.



Written Opinion

【Classification】 Opinions according to notice of grounds for rejection, etc.

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Agent】

【Name】 KWON HYUK ROK

【Agent's Code】 9 -1 99 8- 000 11 5 -1

【Registration number of general power of attorney】 200 2-0 60 5 19-2

【Agent】

【Name】 Lee Jeong Soon

【Agent's Code】 9 -1 99 8- 000 40 4 -2

【Registration number of general power of attorney】 200 5-00 5 29 7-6

【Mark of events】

【Application Number】 10 -200 9- 00 20 3 18

【Dispatch number that caused the submission】 9-5-20 15-0 39 7 22 9-15



【Opinion Contents】 like a star

【Purport】

As described above, it is submitted to the head of the Korean Intellectual Property Office (the head of the Patent Tribunal, the head of the Tribunal).

Opinion Contents

The applicant intends to express the following opinion on the notification of the submission of opinion on June 15, 2015 on Patent Application No. 20 3 18 of 2009 (hereinafter referred to as 'the present invention').

- all negative -

I. notice of submission of opinion

As a result of the review of this application to the examiner in the notice of submission of opinions dated June 15, 2015, the following reasons for rejection were issued.

[Examination results]

claims subject to examination: claims 1-25.

The part with grounds for rejection of this application and the provisions of the relevant law

seq uen ce n um ber	part with reason for rejection	related law article
1	claim	Patent Act Article 29 Article 2

[Specific grounds for rejection]

1. The invention described in the preceding claim of the claims of the present application is unpatentable in accordance with the Patent Act Article 29(2) because it can be readily derived by a person having ordinary skill in the art before the application as follows.

- Ara -

Cited invention 1: Published Patent Publication No. 10-200 8-00 50 9 71 (200 8.0 6.1 0.)

Cited prior art reference 2: 3 G PP TS 23. 40 1 v 8 4. 1 (200 8. 12)

Cited invention 3: U.S. Patent Application Publication No. US 2003/00 28 7 63 (2003 2.0 6.)

A. The present invention and the cited invention relate to a terminal authentication method in a communication system.

The cited invention 1 relates to an authentication method required for roaming at a son-temp when interworking with a heterogeneous wireless network.

Prior art reference 2 is 3 G PP TS 23. 40 1 (v 8 .4.1) standard document .

The cited invention 3 relates to modularized authentication and authentication design for Internet protocols.

The present invention and cited invention 1 have the same purpose and effect in providing a method for reducing a time delay according to authentication of a terminal.

I . configuration contrast

1) The invention as in claim 1

The invention as in claim 1 pertains to a method for authenticating a terminal in a communication system, the method comprising the steps of: requesting, by a first authentication server, a second authentication server to change the authentication server so as to allow a terminal accessing a physical layer to enter a link layer; and transmitting, by the second authentication server, a hash value for an authentication variable to the first authentication server when the terminal includes the authentication variable (Aut h ent authentication P ar ameter) in the cited invention 1, wherein a second authentication device of a second wireless network uses a user identifier so as to transmit a first authentication field of the first wireless network when a user terminal authenticated from a first wireless network is moved to the second wireless network. The features could be readily derived by a person skilled in the art from the features wherein: authentication data is obtained from a value; the authentication data includes I M S I which is a permanent identifier of a user,

unused authentication vectors, C_K and I_K which are in use, K_{SI} which is an associated key index value, Id_T type which indicates the type of user identifier used in M_K calculation, MS_K and $E_{AP} - A_{KA}$, and Co unter final value and $N_x Re Aut h ID$ as information necessary for fast re-authentication; the features in the cited invention 2 wherein: (Fig figure 5.3.2.1-1, Figure 5.3.1-1, Figure 5.3.3-1, Figure 5.3.2-1, etc.) $n e w M M E$ (a first authentication server of the present invention) requests $con tex t$ to an old $M M E$ (a second authentication server of the present invention) and obtains a response to the corresponding $con tex t$; and a process in which a first authentication server having a slight difference in terms of explicit description transmits, to an AAA server, a hash value for an authentication variable provided from the second authentication server, and the AAA server determines validity, and transmits, No.

2) The claim 2 to the claim 5

The additional features in the invention as in claims 2-5 and 2 could be readily derived by a person skilled in the art from the features in the cited invention 1 wherein: when a user terminal authenticated from a first wireless network is moved to a second wireless network, a second authentication device of the second wireless network obtains authentication data from a first authentication device of the first wireless network by using a user identifier; the feature in the cited invention 2 wherein a UE has been authenticated from an HSS server (AAA server) through an old $M M E$ (second authentication server); the additional feature in the invention as in claim 3 could be readily derived by a person skilled in the art from the feature in the cited invention 2 wherein an $n e w M M E$ (first authentication server) transmits a $con tex t$ request message including an old G_{UTI} , an $M M E$ Address, and the like to an old $M M E$; the additional feature in the invention as in claims 4-5 could be readily derived by a person skilled in the art from the feature in the cited invention 2 wherein an old $M M E$ transmits a con

text response message including an identifier of a terminal, an authentication variable hash value, a random variable, and the like to a new MME; and the

3) The invention as in the claims 6-8

With respect to the additional features in the invention as in the claims 6 to 8, the cited invention 2 indicates that the new MME transmits a message including the identifier of the terminal and the number of authentication variables to the HSS server (AAA server), and the HSS serverThe feature of verifying the validity of the number of authentication variables could be readily derived by a person skilled in the art from the features, in the cited invention 3, of: transmitting an authentication variable (MAC_SECURE value, etc.) calculated by a hash function to an AAA server (AGW/AAA Home Server) ([0080]-[0187]); and allowing the AAA server to return by including an authentication parameter if a hash value is valid.

4) The invention as in the claims 9 to 12

The additional features of the invention as in the claims 9-12 correspond to the substitution or addition of a technical means which could be generally adopted by a person with ordinary skills in the art as a specific means for achieving the purpose of the invention from the cited inventions 1 and 2, and there is no particular difference in the purpose and effect of the invention by the change.

5) The invention of the claim 13

The additional feature of the invention as in the claim 13 can be readily derived by a person having ordinary skill in the art from the feature, in the cited invention 2, of including master key information in an authentication variable.

6) The invention as in the claims 14-25

The invention as in the claims 14, 15, 16, 17, 18, and 19-25 has substantially the same technical idea as the invention as in the claims 1, 3, 6, 4, 5, and 7-13, and thus the same reason for rejection is applied thereto.

All. sintering theory

Therefore, the present invention can be easily derived by a person with ordinary skills in the art from the combination of the cited inventions 1, 2 and 3.

[Appendix]

Attachment 1 Published Patent Publication No. 10-200 8-00 50 9 71 (200 8.0 6.1 0.) 1 part.

Attachment 2 3 G PP TS 23. 40 1 (v 8.4.1) (200 8. 12.) 1 part.

Attached 3 U.S. Patent Application Publication No. US 2003/00 28 7 63 (2 003 2.0 6.) 1 part. End .

II. corrections

The present applicant has revised the claims as follows in order to overcome the reason for rejection described in the notice of submission of opinion.

1. The independent claims 1 and 14 were amended in order to overcome the reason for rejection of point I 1.

This correction is supported by paragraphs [0057] to [0073] of the present invention.

2. In order to make the invention clearer, claims 2, 6, 7, 11, 17 to 19 and 23 are amended.

3. Claims 3 to 5, 8 to 10, 12, 13, 15, 16 and 20 to 22 have been deleted.

4. Claims 26-38 are newly established.

III. contrast between the present invention and the cited invention

1. In the examiner, in point I 1, you have said that a person with ordinary skills in the art can readily invent the invention described in claims 1 to 25.

In order to resolve the reason for the rejection of the examiner, the independent claims 1 and 14 were amended. as a result of examining the cited invention 1 face-to-face by the applicant, the corrected independent claimIt is considered that the invention described in claims 1 and 14 cannot be easily derived by a person having ordinary skills in the art for the following reasons.

firstIndependent claim 1, which is corrected, discloses “a step of transmitting a second message from the second authentication server to the first authentication server in response to the first message, wherein the second message comprises a first hash value, a first random variable number, and a second random variable, and the first hash value is generated on the basis of a hash function using the first random variable”.

On the other hand, in paragraph [10 7] of the cited invention 1, “the AAA server or the VLR o/SG SN o (84) searches for the user information from the reception information, and transmits, to the UAGS (83), the IMSI of the user, the unused authentication vectors, the CK and IK in use and the KSI associated therewith, the Id Type, which is the type of the user identifier used in the MK calculation, the MSK, and the counter (Counter) final value required for fast re-authentication, and the NxReAuthId which is the user identifier for re-authentication (S 106)”.

In addition, in paragraph [110] of cited prior art reference 1, the VLR n/SG SN n or AAA n server (82) calculates MSK, Ken cr, and K aut by using CK, IK, and user Id, which are information received from the VLR o/SG SN o (84), according to the method as shown in figure 7 described above (S 108). Here, the VLR n/SG SN n or the AAA n server (82) replaces the received MSK value because it is a case where the received MSK is different from the calculated value and fast re-authentication is performed.

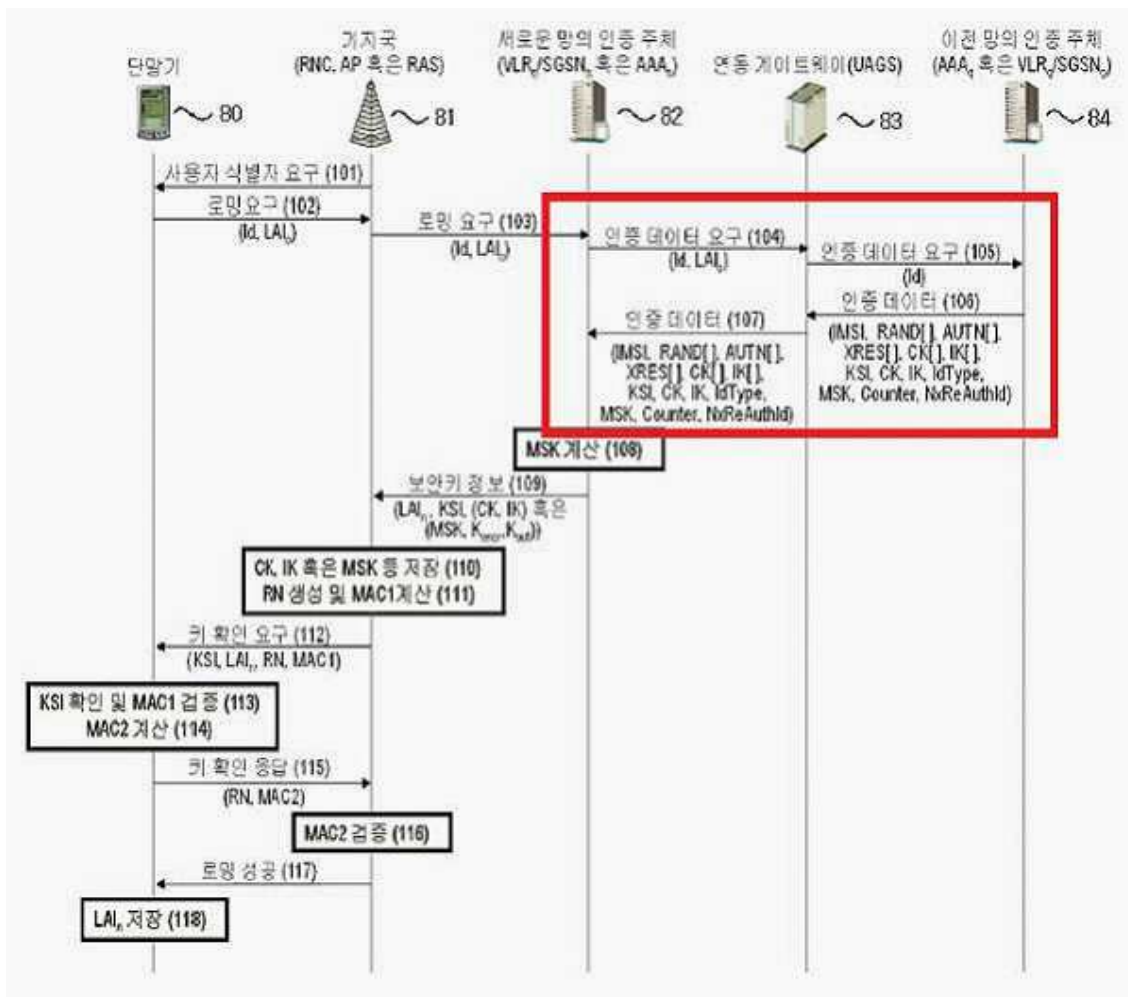
That is, cited prior art reference 1 discloses generating MSK on the basis of CK (Cipher Key), IK (integrity Key), and user ID, and discloses CK or IK use hash function based MSK generation. Since it is not disclosed, it is not disclosed that “the first hash value is generated based on a hash function using the first random variable” of independent claim 1, and it is considered that it cannot be inferred.”

In addition, the cited invention 1 discloses “including a first hash value, a first random variable number, and a second random variable” set forth in independent claim 1. secondthe message itself and abovesecondConfiguration for transmitting a messageIt is considered that this is not disclosed.

And this configuration is not disclosed in cited prior art reference 2 or 3, and it is considered that it cannot be inferred.

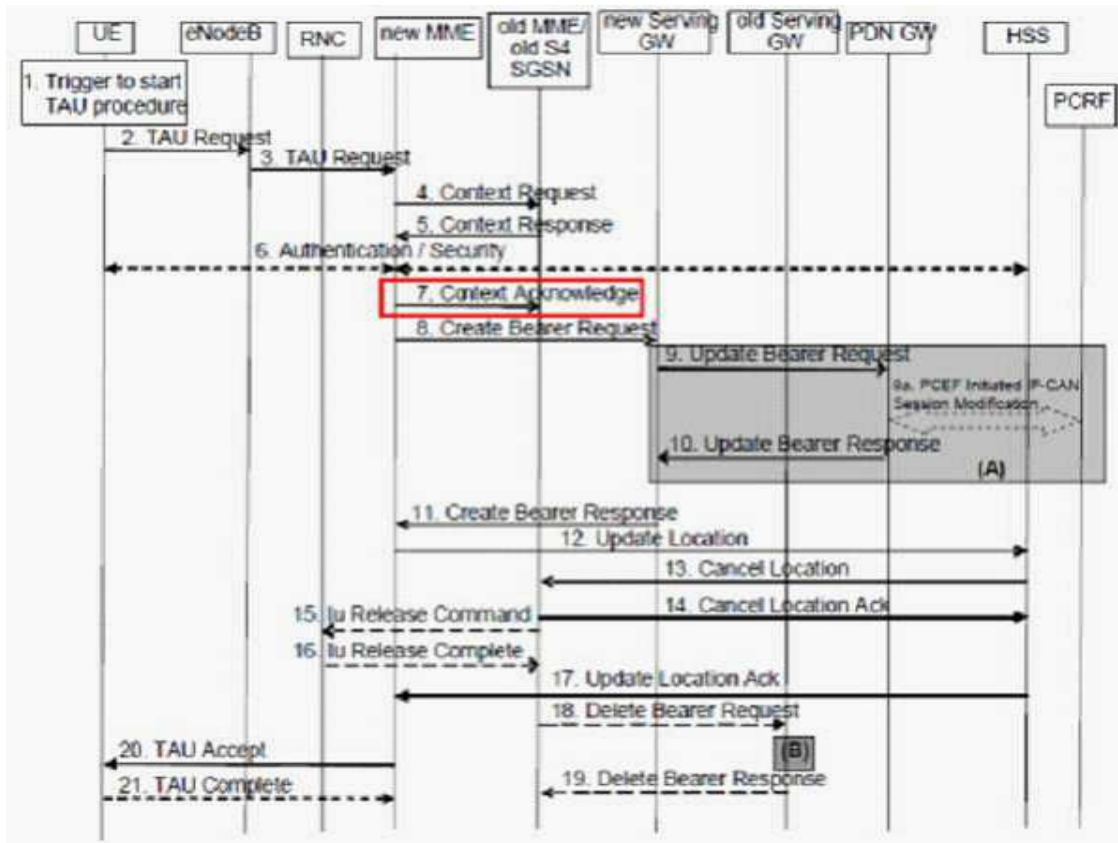
secondIndependent claim 1 discloses “a step of transmitting a fifth message from the first authentication server to the second authentication server, wherein the fifth message includes a second hash value, and the second hash value is generated on the basis of a hash function using the second random variable”.

Meanwhile, figure 10 of the cited invention 1 is as follows.



That is, as the authentication subject (84) of the previous network in the cited invention 1 after the authentication subject (82) of the new network receives the authentication data (107) not sending any message This is illustrated.

And FIG of cited invention 2 .5. 3. 3. 2-1 is as follows.



That is, the cited invention 2 discloses that a new MME transmits Context Acknowledge to Old MME. Here, Context Acknowledge is a message indicating that a new serving gateway has been selected. (see page 62, page 7 of the cited invention 2)

Therefore, as described in independent claim 1, the cited invention 1 or 2 does not disclose a fifth message transmitted from the first authentication server to the second authentication server after the second message, and it is considered that it cannot be inferred.

In addition, as set forth in independent claim 1, the cited invention 1 or 2 includes “the second hash value generated on the basis of a hash function using

the second LAN-DUNN variable. The above fifth message is not disclosed, and it is considered that it cannot be inferred.

And this configuration is not disclosed in cited invention 3, and it is considered that it is not possible to infer it.

third, independent claim 1 describes the feature of 'determining the validity of the second hash value in the second authentication device'.

As discussed above, since the cited inventions 1-3 do not disclose an element corresponding to the second hash value of the independent claim 1, the feature of "determining the validity of the second hash value in the second authentication device" set forth in the independent claim 1 is not disclosed, and it is considered that the feature could not be inferred.

fourth Independent claim 1 discloses 'transmitting a sixth message from the second authentication server to the first authentication server in response to the fifth message when it is determined that the second hash value is valid'.

As discussed above, since the cited inventions 1-3 do not disclose the feature, set forth in independent claim 1, of determining validity of the second hash value, "when it is determined that the second hash value is valid, transfer a sixth message from the second authentication server to the first authentication server in response to the fifth message" set forth in independent claim 1 is not disclosed, and it is considered that it cannot be inferred.

For this reason, since the invention described in independent claim 1 cannot be easily derived by a person having ordinary skill in the art, it is considered that the corrected independent claim 1 does not satisfy claim 29 of the Patent Act.

In addition, it is considered that the independent claim 14, which includes the same configuration as the independent claim 1, does not satisfy the claim 29 of the Patent Act.



In addition, it is considered that the dependent claims 2, 6, 7, 11, 17-19 and 23 of each of the independent claims 1 and 14 do not satisfy the claim 29 of the Patent Act.

IV.texture word

With the above amendment, the applicant hopes that the reason for rejection presented by the examiner will be withdrawn. Please reexamine the present invention and make a patent decision.

Sending
 number : 9-5-2015-085634783
 Dispatch
 d date : 2015.12.08.
 Submissio
 n due 2016.02.08.
 date :

YOUR INVENTION PARTNER



Last
 notified
 tion

Intellectual Property Office

Request for the Submission of an Opinion

Applicant Name SAMSUNG ELECTRONICS CO., LTD.

Address

Agent Name a person besides KWON HYUK ROK

Address

Inventor Name Lee Ji Cheol

Address

Inventor Name Alper Yegin

Address

Application No 10-2009-0020318

Application date 2009.03.10.

Title of Invention METHOD AND SYSTEM FOR AUTHENTICATING IN COMMUNICATION
SYSTEM

1. Because of having the following reason for refusal generated with the correction according to the examination result Patent Act the 47 preparation 1 claim first call about this application and notifying of this according to the article 63 of Patent Act it has the opinion or if necessary, or, the correction hopes in their heart to the submission due date (2016.02.08.) opinion (the reply, and the Written Reply) to submit the Amendment [form of attached document No.9 of Enforcement Regulation of Patent Act].

2. In the case to extend the submission due date (2016.02.08.), the due date of submission of the can be extended through the request for an extension of designated period to 4 month. In this case, request for the extension has to do by unit of 1 month and 2 month or greater is summed up in the need in the range that does not exceed 4 month and it can request the extension. The Written Substantiation describing the proprietary is additionally attached in the time for to postponing the designated period to the generation (the guideline reference of the lower part) of the inevitable proprietary in excess of 4 month and request for the extension has to be applied.

[Examination result]

- Subject of First and second, 6, 7, 11, 14, 17, 18, 19, 23, 26, 27, 28, examination claim: 29, 30, 31, 32, 33, 34, 35, 36, 37, 38 claim
- The law articles in connection with the part in which it has the reason for refusal of this application

Sequence number	The part in which it has the reason for refusal	Related law articles
1	Claim 6, claim 18, and claim 28	Patent Act article 42(4)(1)
2	Claim 2, claim 17, claim 35, claim 38	The article 42(4)(2) of Patent Act

[The detailed reason for refusal]

1. The application cannot be granted since it does not satisfy requirements of the Patent Act article 42(4)(1) due to deficiency in the description of claim 6, claim 18, and claim 28 as pointed out below.

- Follows -

Claim 6 invention limits '... ellipsis ... first random variable, is the inclusion ... ellipsis ... the CMAC KEY COUNTER'. But the matter corresponding to claim is written in the detailed description of the invention and it is guaranteed by the detailed explanation although the content of the attached view is taken into consideration.

The reason for refusal of the purpose of claim 18 , and claim 28 being identical is applied.

2. The application cannot be granted since it does not satisfy requirements of the article 42(4)(2) of Patent Act due to deficiency in the description of claim 2, claim 17, claim 35, claim 38 as pointed out below.

- Follows -

In claim 2, and '... ellipsis ellipsis ... terminal connects to the physical layer' of 17 invention, it is vague because the above indicates.

In claim 35, and 'the process ... ellipsis ... storing the above-mentioned received second random variable in ... ellipsis ... first certificate server' of 38 invention, it is vague because the above indicates.

[The list of reference about the correction]

※ Claim 2, and 17 invention are claim 35 it amends to '... ellipsis ellipsis ... terminal connects to the physical layer', and 38 invention are the method when it amends to 'the process ... ellipsis ... storing the second random variable received in ... ellipsis ... first certificate server' for more specifically doing the meaning.

<<The guideline about 'the list of reference about the correction'>>

1. It was prepared the aid was given in the correction of the applicant including the advanced technology document etc. the examiner confirms until the list of reference about the correction which the examiner presents forwards the Notification of Reason for Refusal.
2. The legal constraint which the applicant follows the list of reference does does not have and the applicant freely can amend the list of reference about the correction. But the applicant correction reflection acceptance and rejection of the list of reference which the examiner presents advisedly has to judge since it has all responsibility about the corrections to the applicant.
3. The Patent decision is not guaranteed to follow the list of reference about the correction which the examiner presents and it can be changed according to the discovery of the prior art in which this list of reference is new etc.



의견(답변, 소명)서

【구분】 거절이유 등 통지에 따른 의견

【제출인】

【명칭】 삼성전자주식회사

【특허고객번호】 1-1998-104271-3

【사건과의 관계】 출원인

【대리인】

【성명】 권혁록

【대리인번호】 9-1998-000115-1

【포괄위임등록번호】 2002-060519-2

【대리인】

【성명】 이정순

【대리인번호】 9-1998-000404-2

【포괄위임등록번호】 2005-005297-6

【사건의 표시】

【출원번호】 10-2009-0020318

【제출원인이 된 서류의 발송번호】 9-5-2015-0856347-83
호】

【의견내용】 별지와 같음

【취지】

위와 같이 특허청장(특허심판원장, 심판장)에게 제출합니다.

대리인 권혁록 (서명 또는 인)

대리인 이정순 (서명 또는 인)





의견내용

2009년 특허출원 제0020318호(이하, "본원발명"이라 합니다)에 대한 2015년 12월 08일자 거절이유에 대하여 본원 출원인의 의견을 다음과 같이 개진합니다.

- 다 음 -

I. 거절이유

1. 특허법 제42조제4항제1호 거절

심사관님께서서는 본원발명의 청구항 제6항, 제18항, 및 제28항의 기재가 상세한 설명에 의해 뒷받침되지 않기 때문에, 특허법 제42조제4항제1호에 따라 특허를 받을 수 없다고 지적하셨습니다.

2. 특허법 제42조제4항제2호 거절

심사관님께서서는 본원 발명의 청구항 제2항, 제17항, 제35항, 제38항항의 발명들의 기재가 불명료하기 때문에, 특허법 제42조제4항제2호에 따라 특허를 받을 수 없다고 지적하셨습니다.

II. 거절이유에 대한 출원인의 의견

1. 특허법 제42조제4항제1호 거절에 대해,

출원인은 심사관님께서 지적하신 제6항, 제18항, 및 제28항을 삭제하였습니다.

2. 특허법 제42조제4항제2호 거절에 대해,

출원인은 청구항 제2항, 및 제17항에서 "상기 단말이 상기 물리 계층에 접속하기 이전에"를 "상기 단말이 물리 계층에 접속하기 이전에"로 정정하였습니다.

출원인은 청구항 제35항, 및 제38항에서 "상기 제1 인증서버에서, 상기 수신된 제2 랜덤 변수를 저장하는 과정"을 "상기 제1인증서버에서 수신된 상기 제2 랜덤 변수를 저장하는 과정"으로 정정하였습니다.

추가로, 출원인은 청구항 제1항에서, 오기재된 "상기 제1 인증 장치"를 "상기 제1 인증 서버"로 정정하였습니다.

III. 결론

심사관님께서서는 위 의견내용을 참고하시고 의견제출통지서상의 거절이유를 해소하기 위하여 제출되는 보정서를 재심사하시어 부디 본원발명에 대한 특허결정을 하여 주시기 바랍니다.





Amendment to Bibliographic Information

【Classification】 specification etc. correction

【Submitter】 patent office field

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Agent】

【Name】 KWON HYUK ROK

【Agent's Code】 9 -1 99 8- 000 11 5 -1

【Registration number of general power of attorney】 200 2-0 60 5 19-2

【Agent】

【Name】 Lee Jeong Soon

【Agent's Code】 9 -1 99 8- 000 40 4 -2

【Registration number of general power of attorney】 200 5-00 5 29 7-6

【Mark of events】

【Application Number】 10 -200 9- 00 20 3 18

【Dispatch number that caused the submission】 9 -5- 20 15 -0 85 6 34 7 -8 3

【Documents to be corrected】 specification etc

【What to correct】

【Items to be corrected】 like a star

【Correction method】 like a star

【Correction contents】 like a star

【Purport】

As above, it is submitted to the head of the Korean Intellectual Property Office (the head of the Patent Tribunal, the head of the Tribunal).

【Official Fee】

【Amendment Fee】 4,000,000 won

【Additional fees for examination requests】 0 won

【Other fees】 0 won

【Total】 4,000,000 won

Amendment

【Correction item】 Claim 1

【Correction method】 Change

【Correction content】

【Claim 1】

as to the method for certifying the terminal in the communications system

a step of transmitting a first message from a first authentication server to a second authentication server, wherein the first message includes identification information of the first authentication server

a step of transmitting a second message from the second authentication server to the first authentication server in response to the first message, wherein the second message includes a first hash value, a first random variable, and a second random variable, and the first hash value is generated based on a hash function using the first random variable

a step of transmitting a third message from the first authentication server to an AAA server, wherein the third message includes a first hash value, a first random variable, and identification information of the first authentication server

a step of determining the validity of the first hash value in the AAA server

a step of transmitting a fourth message from the AAA server to the first authentication server in response to the third message when the first hash value is determined to be valid, wherein the fourth message includes an authentication variable of a terminal

transmitting a fifth message from the first authentication server to the second authentication server, wherein the fifth message includes a second hash value, and the second hash value is generated based on a hash function using the second random variable

A process of deciding the validity of the , second hash-value in the second certificate server

and transmitting a sixth message from the second authentication server to the first authentication server in response to the fifth message when the second hash value is determined to be valid.

【Correction item】 Claim 2

【Correction method】 Change

【Correction content】

【Claim 2】

The method of claim 1,

When the second authentication server is authenticated by the AAA server before the terminal accesses the physical layer, the terminal and the AAA server include an authentication server for authentication.

【Correction item】 Claim 6

【Correction method】 Delete

【Correction item】 Claim 17

【Correction method】 Change

【Correction content】

【Claim 17】

The method of claim 14,

The second authentication server, when the terminal is authenticated by the AAA server before accessing the physical layer, includes an authentication server that the terminal and the AAA server have passed for authentication.

【Correction item】 Claim 18

【Correction method】 Delete



【Correction item】 Claim 28

【Correction method】 Delete

【Correction item】 Claim 35

【Correction method】 Change

【Correction content】

【Claim 35】

The method of claim 1,

The method further comprising storing the second random variable received from the first authentication server.

【Correction item】 Claim 38

【Correction method】 Change

【Correction content】

【Claim 38】

The method of claim 14,

The communications system in which the first certificate server stores the received second random variable.

Sending 9-5-2016-041219246
number :
Dispatche 2016.06.07.
d date :



YOUR INVENTION PARTNER



Intellectual Property Office

Written Decision on Registration

Applicant Name SAMSUNG ELECTRONICS CO., LTD.(Applicant Code:
119981042713)

Address

Agent Name a person besides KWON HYUK ROK

Address

Inventor Name Lee Ji Cheol

Address

Inventor Name Alper Yegin

Address

Application No 10-2009-0020318

Title of Invention METHOD AND SYSTEM FOR AUTHENTICATING IN COMMUNICATION
SYSTEM

Number of claims 20

This is to certify that the application was granted for a patent under Article 66 of Patent Act.

(By the patent right paying the patent fee and receiving the registration according to the article 87 of Patent Act it is generated) End.

[Reference]

1. KR1020080050971 A
2. 3GPP TS 23.401 v8.4.1(2008.12)
3. US20030028763 A1

