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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/45452 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/EP01/05832

(22) International Filing Date: 21 May 2001 (21.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/EP00/11889
28 November 2000 (28.11.2000) EP

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FLYKT, Patrik** [FI/FI]; Silmupolku 1 B 43, FIN-00380 Helsinki (FI). **NIEMI, Valtteri** [FI/FI]; Tallberginkatu 3 as 43, FIN-00180 Helsinki (FI). **RAJANIEMI, Jaakko** [FI/FI]; Lapinrinne 2 A 11, FIN-00180 Helsinki (FI). **NIEMI, Aki** [FI/FI]; Otsolahdentie 18 A 26, FIN-02110 Espoo (FI).

(74) Agent: **LESON, Thomas, Johannes, Alois**; Tiedtke-Bühling-Kinne, Bavariaring 4, 80336 Munich (DE).

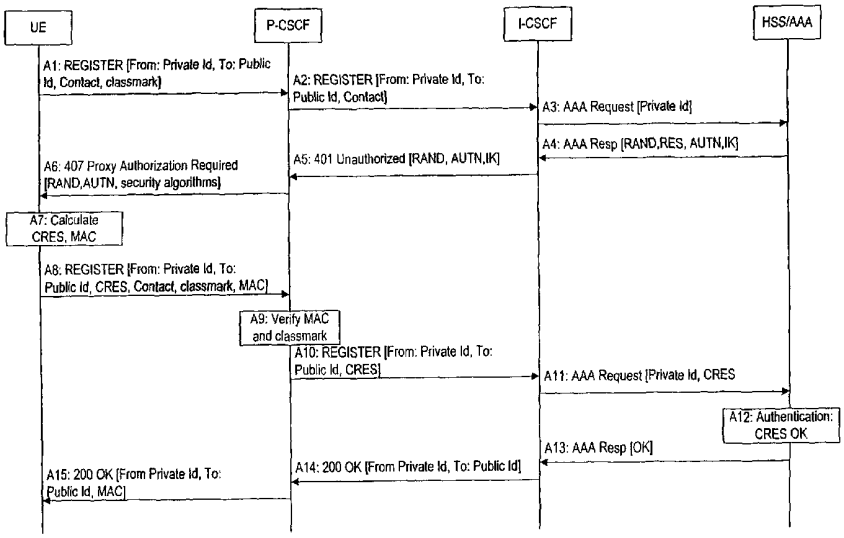
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: INTEGRITY PROTECTION DURING INITIAL REGISTRATION OF A SUBSCRIBER IN A TELECOMMUNICATIONS NETWORK



(57) Abstract: A network system is proposed comprising a network control element and a communication device (UE) associated to a subscriber, wherein the communication device (UE) is adapted to send a registration message (A8) including subscriber information to be protected and an integrity code (MAC), to the network control element, wherein the communication device (UE) is adapted to calculate the integrity code (MAC) by using a part or whole of the registration message (A8) including the subscriber information to be protected, and the network element is adapted to verify the integrity code (MAC) included in the registration message. Also a case is proposed in which the integrity code is calculated in the network control element and verified in the communication device (UE). Furthermore, corresponding methods are proposed.

WO 02/45452 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTEGRITY PROTECTION DURING INITIAL REGISTRATION OF A SUBSCRIBER IN A TELECOMMUNICATIONS NETWORK

Field of the invention

The present invention relates to a method a network system for performing authentication of a subscriber and/or subscriber information and/or security information which like a device related capability information transmitted during the registration.

BACKGROUND OF THE INVENTION

The present invention concerns authentication of a subscriber, and particularly a registration involved in such an authentication.

The general procedure for performing an authentication is described in the following in short. The authentication procedures are similar in GSM and UMTS. Thus, in the following the authentication procedure is described by referring to GSM as an example.

An authentication is usually required when a subscriber registers to the network services. Also an authentication may be required when a connection is established, i.e. when originating or terminating a call. The authentication is performed, for example, in an Authentication Center (AuC) which is usually provided in the Home Location Register (HLR). The VLR to which the MS is currently connected requests a parameter set consisting of a random number RAND (usually, 128 bit) and a scheduled result (RES) from the HLR and sends the RAND

to the MS. In turn, the MS has to calculate a result CRES from the number RAND.

The SIM card of the subscriber comprises a secret subscriber key Ki which is, apart from the SIM, only known to the network operator (HLR/AuC). The SIM card also comprises an algorithm (A3). By using this algorithm, from RAND and Ki a result CRES is calculated (CRES = A3(RAND,Ki)). This result CRES is transmitted to the VLR which in turn checks whether the result is equal to the signed result received from the HLR/AuC, i.e., whether CRES = RES. If this is correct, the authentication is successful.

The above described example is the authentication procedure in GSM. As mentioned above, in UMTS, the authentication of a subscriber is performed similarly. Here, the SGSN (which corresponds to the VLR) requests a parameter set from the HSS (which corresponds to the HLR) comprising a random number RAND, the result RES (which should be the result CRES calculated by User Equipment (UE)), a ciphering key CK, an integrity key IK and an authentication token AUTN. Instead of a SIM card as in GSM, the subscriber uses a so-called USIM (Universal Services Identity Module) which is a logical module implemented e.g. inside a smart card. In comparison to GSM, under UTMS additional functions are provided by the USIM. For example, the USIM checks the authenticity of the network by using the authentication token AUTN.

Nevertheless, authentication of the subscriber is performed similarly to the procedure under GSM. That is, a home network control element (like I-CSCF or the like) sends the parameter to a serving network element (i.e., the SGSN or P-CSCF) which forwards the parameters RAND

and AUTN to the USIM. The USIM calculates a result RES from the random number RAND and a secret subscriber key Ki and sends the result back to the serving network element. Thus, by checking the result, it is possible to decide whether the subscriber is allowed to use the services or not.

However, in the above example the subscriber has to forward critical information to the network. In particular, it has to be assured that the critical fields in the SIP registration, e.g., To From and Contact are not corrupted, manipulated or the like.

This problem also occurs in other cases in which a user has to perform an initial registration.

SUMMARY OF THE INVENTION

Therefore, the object underlying the invention resides in removing the above drawbacks of the prior art and to enable a reliable protection of critical information.

This object is solved by a network system comprising a network control element and a communication device associated to a subscriber, wherein

the communication device is adapted to send a registration message including subscriber information to be protected and an integrity code, to the network control element, wherein

the communication device is adapted to calculate the integrity code by using a part or whole of the registration message including the subscriber information to be protected, and

the network element is adapted to verify the

integrity code included in the registration message.

Alternatively, the object is solved by a network system comprising a network control element and a communication device associated to a subscriber, wherein

the network control element is adapted to receive a registration message from the communication device, to calculate an integrity code by using a part or whole of a message including subscriber information to be protected and to send a message to the communication device, which includes the information to be protected and the integrity code, and

the communication device is adapted to verify the integrity code.

Alternatively, the object is solved by a method for performing registration of a subscriber in a network system, comprising a network control element and a communication device associated to a subscriber, said method comprising the steps of

sending a registration message including subscriber information to be protected and an integrity code to the network control element,

calculating the integrity code by using a part or whole of the registration message including the subscriber information to be protected, and

verifying the integrity code in the network control element.

Alternatively, the object is solved by method for performing registration of a subscriber in a network system, comprising a network control element and a communication device associated to a subscriber, said method comprising the steps of

sending a registration message from the

communication device to the network control element,

calculating an integrity code by using a part or whole of the registration message including subscriber information to be protected,

sending a message to the communication device, which includes the information to be protected and the integrity code and

verifying the integrity code in the communication device.

Thus, according to the invention, an integrity protection for the user performing an initial registration is provided. That is, critical subscriber information can be protected.

According to the invention, there is no public key infrastructure required, since according to the invention an security algorithm based on parts of exchanged messages is used. Hence, the invention can be applied in a so-called shared secret case.

The registration message may be a SIP (Session Initiation Protocol) REGISTER message. The subscriber information to be protected may comprise information regarding the originator of the registration message (e.g., From field in SIP), and/or information regarding the subscriber to be registered (e.g., To field in SIP) and/or a contact field (Contact field in SIP) Also other information or information fields are possible. For example, the subscriber information may comprise the Request-URL (Uniform Resource Locator) field which is the address of the register to which the registration should be sent.

A message including algorithm capability information may be sent from the communication device to the network

control element. Furthermore, the network control element may choose which algorithm is to be used for calculating the integrity code and forward a message including information about the chosen algorithm to the communication device (UE).

That is, a so-called classmark may be included in the message. The classmark refers to the security algorithms capability of the terminal. Hence, this indication (classmark) may be used in case several algorithms are used in the system.

Thus, according to the invention, the problem is solved how the integrity protection is to be setup. This means that the algorithm used is negotiated in a secure way (namely, by using the indication or classmark), and also the starting point of the integrity protection is defined (namely, either in the communication device on sending the registration message or in the network control element on sending the response message to the communication device).

That is, according to the invention, a negotiation of a security algorithm works typically in the following that the terminal tells to the network what it is capable of, i.e. the classmark, the network chooses the security algorithm and tells that to the terminal. Also the network indicates the capability information (i.e. classmark) from which it made the selection for the security algorithm.

The communication device may be adapted to forward the algorithm capability information with the registration message, and the network control element may adapted to verify the algorithm capability information.

That is, the network can check whether the classmark is the same as in the beginning of procedure.

Also, the network control element may be adapted to forward the algorithm capability information with the message including the information to be protected to the communication device, wherein the communication device may be adapted to verify the algorithm capability information.

Thus, also the communication device may check that after the procedure the classmark is the same as in the beginning.

An authentication of the subscriber may be performed. Hence, advantageously the procedure according to the invention is combined with an authentication which requires the registration.

The authentication may be performed by using the integrity code. That is, the network control element can use the integrity code as a result which has to be compared with a scheduled result. By this measure, only one code has to be calculated and forwarded, which reduces operation and signaling load.

The network system may further comprise an additional network control element which is adapted to perform an additional authentication. Hence, two separated authentications may be performed in order to have a more reliable authentication.

The network control element may control a first network, and the additional network control element may control a

second network. Thus, the two authentications may be performed by two different networks individually.

The network system may further comprise an additional network control element for performing an additional authentication, wherein a result is calculated in the communication device from a predetermined number supplied by the additional network control element, and the additional authentication may be performed in the additional network control element by using the result. Thus, the two network elements may perform the authentications independently from each other.

In particular, the invention is advantageously applicable to such a case in which two networks perform authentications independently from each other. Namely, one network may use the predetermined number and the result calculated by the communication device for authentication, and the other network element may use the integrity code for authentication. In this way, the authentication procedure as a whole can be made more reliable, since both network use fully separated codes for their authentications of the subscriber.

The additional authentication may be performed by comparing the result received from the communication device with a scheduled result.

The predetermined number and the scheduled result may be provided by a home subscriber database (HSS), an Authentication Centre (AuC) or an Authentication Authorization and Accounting server (AAA).

The calculation of the integrity code may be performed by using GSM or UMTS algorithms.

The message including information to be protected may be the registration message received from the communication device (UE), or may be a response message (e.g., a 200 OK response) sent from the network in response to the registration message from the communication device.

The invention also proposes a network system comprising a network control element and a communication device associated to a subscriber, wherein

the communication device is adapted to send a registration message including algorithm capability information to the network control element, wherein

the network control element is adapted to choose which algorithm is to be used for calculating an integrity code and to send a corresponding message to the communication device, wherein

the network control element and/or the communication device is adapted to verify the algorithm capability information on a later transmittal of a message including the algorithm capability information.

Furthermore, the invention proposes a method for performing registration of a subscriber in a network system comprising a network control element and a communication device associated to the subscriber, the method comprising the steps of

sending a registration message including algorithm capability information from the communication device to the network control element,

choosing which algorithm is to be used for calculating an integrity code,

sending a corresponding message to the communication device and

verifying the algorithm capability information on a

later transmittal of a message including the algorithm capability information in the network control element and/or the communication device.

In this way, the algorithm used for calculating an integrity code is negotiated in a secure way. Namely, the information regarding the algorithm (classmark as described above) is included in the messages.

The integrity code may be calculated by the communication device by using a part or whole of a registration message, and the registration message and the integrity code may be forwarded to the network control element. In addition, information regarding the used algorithm may be forwarded to the network control element.

Furthermore, the integrity code may be verified by the network control element on receiving the registration message from the communication device by using the information regarding the used algorithm.

The network control element may calculate an integrity code by using a part or whole of a registration message received from the communication device and forward a message and the integrity code to the communication device. Also, information regarding the used algorithm may be forwarded to the communication device.

The communication device may verify the integrity code on receiving the message from the network control element. Moreover, in case also information regarding the used algorithm were forwarded, the communication device may use this information for verifying the integrity code as well.

It is noted that the above-described integrity code may be included in the corresponding messages or may be forwarded in a separate message. Also, the information regarding the chosen algorithm (classmark) may be included in the corresponding message or may be forwarded in a separate message.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings in which:

Fig. 1 shows a network system to which the embodiments are applied,

Fig. 2 shows a UMTS authentication procedure according to a first embodiment,

Fig. 3 shows a UMTS authentication procedure according to a second embodiment, and

Fig. 4 shows a UMTS authentication procedure according to a second embodiment.

DETAILED DESCRIPTION OF EMBODIMENTS

In the following, preferred embodiments of the invention are described in more detail with reference to the accompanying drawings.

In the description of the embodiments, a network system as schematically illustrated in Fig. 1 is taken as an example. In detail, this system consists of two networks

which both are Internet Multimedia Core Network Subsystems (IM CN SS). In the figure, only the main elements are shown.

Both networks contain CSCFs (Call State Control Functions). A User Equipment (UE), which may be a mobile station (MS), is connected to the home network S-CSCF via the P-CSCF if the home network controls the connections. In this case, it is assumed that the subscriber is roaming in a network which is not the home network of the subscriber using the UE. Thus, this network is designated as the visited network.

For an authentication procedure and the like, the P-CSCF contacts the home network of the subscriber. That is, the P-CSCF contacts an Interrogating CSCF (I-CSCF) of the home network which is capable of accessing a Home Subscriber Server (HSS).

It is noted that the connection may be controlled by the visited network. In this case, the connection is not controlled by the S-CSCF in the home network (as shown in Fig. 1) but by a S-CSCF in the visited network.

The procedures performed during authentication of the subscriber are described in the first and second embodiments by referring to Figs. 2 and 3.

According to these embodiments, the authentication is performed by the I-CSCF (or S-CSCF or HSS or a separate network element such as AAA (Authentication Authorization and Accounting server)) and the P-CSCF. Thus, both the serving network (controlled by the P-CSCF) and the home network (controlled by the I-CSCF) are able to verify that the authentication was performed correctly. In the

following, it is assumed that the authentication in the home network is performed by the I-CSCF. Thus, in the signaling diagrams of Figs. 2 to 3, the S-CSCF are omitted.

Fig. 2 shows a signaling flow of an authentication procedure according to the first embodiment.

In case the user registers to the network, the UE sends a registration request to the P-CSCF (step A1). This can be a SIP (Session Initiation Protocol) REGISTER message, for example. In this example, the SIP REGISTER message contains the header fields From, To and Contact. The From field indicates the user address (i.e., Private Identity (Id)), and the To field indicates the destination address (i.e., the Public Identity). Furthermore, the REGISTER message contains a parameter "classmark", which will be described later.

The P-CSCF forwards this request to the home network, i.e., to the I-CSCF (step A2) since in order to perform authentication, the P-CSCF has to obtain the necessary authentication information. The I-CSCF, in turn, sends a GetAuthInfo (Get Authorization Information) message to the HSS or AAA (step A3).

The HSS responds with an Authorization Information Response (AuthInfoResp) (step A4). This response includes a plurality of parameters RAND, RES, AUTN, IK. In particular, a random number RAND is sent. The number RAND is intended for an authentication check performed by the home network. In addition, also a scheduled result (i.e., the result which should be calculated by the UE) is included in the parameters, namely RES.

The I-CSCF forwards a 401 Unauthorized message to the P-CSCF (step A5) including RAND, AUTN and IK. The P-CSCF retrieves RES from the parameters and forwards a 407 Proxy Authorization Required message to the User Equipment (UE) (step A6) including RAND and AUTN. Furthermore, an indication of used security algorithms is also included into this message.

Then, the UE uses the number RAND to calculate a result CRES (step A7). The calculation is performed by using a special predetermined algorithm (e.g. UMTS algorithms) and a secret subscriber key Ki which are stored on the USIM card of the subscriber and which are only known to the HSS.

In addition, the UE may calculate a message authorization code (MAC) by using, e.g., the ciphering key CK or integrity key IK. However, according to the present embodiment, the MAC is calculated from some other part of the SIP message or whole SIP message which is to be sent in step B8. The MAC may be included in a SIP Authorization field or the like (step B7). If the MAC is calculated over the whole REGISTER (B8) message then the subscriber information e.g. From, To and Contact fields information are also authenticated and protected. That is, in order to protect these fields, at least the parts corresponding to the fields should be used for calculating the MAC. It is noted that in this connection the "whole message" refers to the whole REGISTER message without the MAC field.

Thus, after completing the calculations, the UE sends a register message including RES and MAC to the P-CSCF (step A8). In step A8, also the so-called classmark is sent. The classmark refers to the security algorithms

capability of the UE. That is, the classmark indicates which algorithm has actually been used for calculating MAC. The classmark has to be included into the messages only in case several algorithms are used in the systems. This, however, is a most probable case.

In detail, the classmark serves to perform a security negotiation. The terminal (i.e., UE) tells the network (i.e., P-CSCF) of which security algorithms it is capable of. This is performed in step A1, in which the UE includes the classmark into the REGISTER message. Thereafter, the network chooses the security algorithms and indicates this to the terminal. According to the present embodiment, this is performed in step A6 in which the P-CSCF includes the security algorithms information into the 407 message (A6).

In step A9, the P-CSCF verifies the MAC and classmark. That is, the P-CSCF calculates itself a MAC from the corresponding parts of the message, as it is performed in step A7 in the UE. In case both results are the not the same, the authentication fails and the registration request is rejected.

Otherwise, if both results are the same (i.e., MAC calculated by the UE = Mac calculated by P-CSCF), the P-CSCF forwards a register message including CRES and MAC to the I-CSCF (step A10). The I-CSCF verifies the authorization by forwarding an AAA Request to the HSS/AAA (step A11). The AAA performs a check in step A12 by comparing the calculated result CRES with the scheduled result RES. If the two numbers are not the same, the authentication fails and the registration request is rejected.

Otherwise, in step A13 a positive AAA Response is forwarded to the I-CSCF, which in turn forwards a 200 OK message to the UE via the P-CSCF in steps A14 and A15.

The 200 OK messages contain also the original From and To fields such that the UE can check whether these fields have been corrupted.

It is noted that it is also possible to verify MAC in the I-CSCF and to verify CRES in the P-CSCF. Furthermore, the verification of CRES can be performed by the I-CSCF or the P-CSCF alone without referring to the AAA by using the scheduled result RES.

It is noted that the above embodiment is applied to a case in which there is a network system comprising a visited network and a home network. However, the embodiment may also be applied to a case in which the user (UE) is attached only to his home network, i.e., in which the P-CSCF and the I-CSCF are part of his home network.

Thus, according to the first embodiment the UE calculates CRES from RAND and the secret subscriber key Ki by using a predetermined algorithm. In addition, the UE calculates a message authentication code (MAC) which may be calculated from some other part of the SIP message including the subscriber information. Since the MAC is verified in the P-CSCF, according to the first embodiment an early integrity protection is performed.

According to a second embodiment, a late integrity protection is performed. That is, according to the second embodiment the subscriber information (e.g. From, To and Contact fields) of the registration message may also be

authenticated and protected by the user when he receives an acknowledgment (200 OK message) to the registration from the network. The user verifies the subscriber information (e.g., From, To and Contact) fields in the acknowledgment message that they are the same which were included into the registration message sent by the user.

Fig. 3 shows the signaling flow according to the second embodiment.

According to the second embodiment, basically the same situation is assumed as described above by referring to Fig. 1. That is, two networks, a visited network and a home network are involved. In this example, authentication takes place only in the home network.

Steps B1 to B6 are identical to steps A1 to A6 of Fig. 2. In step B7, the UE only calculates CRES, but not the message authentication code MAC. Thus, in step B8, only the subscriber information fields and CRES are included. In step A9, this register message is forwarded from the P-CSCF of the visited network to the I-CSCF of the home network. The I-CSCF performs the authentication in steps B10 to B12 as described above in the steps A11 to A13 of Fig. 2. In step B13, the positive result is forwarded to the P-CSCF.

In step B14, the P-CSCF calculates a message authentication code (MAC) by using the subscriber information, i.e., by using that part of the registration message B8 which comprises these fields.

As the security algorithm for calculating the MAC, the P-CSCF uses the security algorithm(s) which were negotiated in steps B1 and B6.

It is noted that alternatively also the 200 OK response message B13 may be used for calculating the authentication code (integrity code), since also this message contains the subscriber information to be protected.

In step B15, the 200 OK message including MAC and classmark (which indicates the used algorithm) is forwarded to the UE. The UE verifies in step B16 MAC and classmark. That is, the user is able to verify whether the subscriber information is still the same as sent to the network in the registration message B8.

It is noted that also according to the second embodiment, only one network may be present. That is, both P-CSCF and I-CSCF may be located in the home network.

Moreover, also according to the second embodiment an additional authentication may be performed in the visited network. That is, in step B7 another value (e.g., a different MAC calculated form another part of the SIP message) may be used for this authentication.

In the following, a third embodiment of the invention is described by referring to Fig. 4.

The signalling is almost the same as in case of the first embodiment described with reference to Fig. 2. The difference to the first embodiment is that according to the third embodiment the authentication is performed in the S-CSCF (serving CSCF).

Thus, in the following only the differences to the first embodiment are described.

After the I-CSCF has received the REGISTER message (C2), the I-CSCF performs a Cx-Query to the HSS in order to obtain the correct S-CSCF in steps C3 and C4.

It is noted that it is defined in the specifications that the I-CSCF shall send the Cx-Query information flow to the HSS (P-CSCF name, subscriber identity, home domain name, visited network contact name). The P-CSCF name is the contact name that the operator wishes to use for future contact to that P- CSCF. The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that visited network according to the User subscription and operator limitations/restrictions if any. Cx-Query Resp is sent from the HSS to the I-CSCF. If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt. The I-CSCF shall send Cx-Select (serving network indication, subscriber identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function. The HSS shall send Cx-Select Resp (required S-CSCF capabilities) to the I-CSCF."

Thereafter, the REGISTER message is forwarded to the S-CSCF, which in turn basically performs in steps C6 to C9 the same processes as the I-CSCF in Fig. 2 in steps A3 to A6. Also, the calculating and verifying of the MAC in steps C10 C12 corresponds to the steps A7 to A9 in Fig. 2.

After performing a further CxQuery in step C14, the I-CSCF forwards the REGISTER message received in step C13 to the S-CSCF in step C15. The S-CSCF in turn performs

the authentication, i.e., checks whether CRES = RES or not.

After performing a Cx-Put (this informs the S.CSCF name to the HSS) in step C17 and a Cx-Pull (the subscriber profile downloaded to S-CSCF) in step C18, the 200 OK message is forwarded to the UE in steps C19 to C21.

The above description and accompanying drawings only illustrate the present invention by way of example. Thus, the embodiment may vary within the scope of the attached claims.

In particular, the embodiments may be combined such that both an early integrity protection and a late integrity protection may be achieved.

Furthermore, it is noted that in the embodiments described above the IM CN SS (Internet Multimedia Core Network Subsystem) was only mentioned as an example. The invention is by no way limited thereon and can be applied to any kind of network system in an authentication is performed. For example, the invention can also be applied to a GSM and UMTS network systems. It can also be applied in 3rd generation mobile systems where requirements of home control in authentication of the subscriber are strict, as is typically the case in many systems specified in so-called 3GPP2 in North America.

Moreover, it is noted that the authentication described above is only an example in which a protection of subscriber information during an (initial) registration is required. The invention may be applied to other cases in which subscriber information have to be protected during registration or the like.

Claims

1. A network system comprising a network control element and a communication device (UE) associated to a subscriber, wherein

the communication device (UE) is adapted to send a registration message (A8; C11) including subscriber information to be protected and an integrity code (MAC), to the network control element, wherein

the communication device (UE) is adapted to calculate the integrity code (MAC) by using a part or whole of the registration message (A8; C11) including the subscriber information to be protected, and

the network element is adapted to verify the integrity code (MAC) included in the registration message.

2. A network system comprising a network control element and a communication device (UE) associated to a subscriber, wherein

the network control element is adapted to receive a registration message (B8) from the communication device (UE), to calculate an integrity code (MAC) by using a part or whole of a message (B8, B13) including subscriber information to be protected and to send a message (B15) which includes the information to be protected and the integrity code (MAC), to the communication device (UE) and

the communication device (UE) is adapted to verify the integrity code (MAC).

3. The network system according to claim 1 or 2, wherein the subscriber information to be protected comprises information regarding the originator of the

registration message.

4. The network system according to claim 1 or 2, wherein the subscriber information to be protected comprises information regarding the subscriber to be registered.

5. The network system according to claim 1 or 2, wherein the subscriber information to be protected comprises a contact field.

6. The network system according to claim 1 or 2, wherein the communication device (UE) is adapted to send a message (A1; B1; C1) including algorithm capability information to the network control element.

7. The network system according to claim 6, wherein the network control element is adapted to choose which algorithm is to be used for calculating the integrity code (MAC) and to forward a message (A6; B6; C9) including information about the chosen algorithm to the communication device (UE).

8. The network system according to claim 6, wherein

the communication device (UE) is adapted to forward the algorithm capability information with the registration message (A8; C11), and

the network control element is adapted to verify the algorithm capability information.

9. The network system according to claim 6, wherein

the network control element is adapted to forward the algorithm capability information with the message (B15) including the information to be protected to the communication device, and

the communication device (UE) is adapted to verify the algorithm capability information.

10. The network system according to claim 1 or 2, wherein the network element is adapted to perform an authentication of the subscriber.

11. The network system according to claim 10, wherein the network control element performs the authentication by using the integrity code (MAC).

12. The network system according to claim 8, further comprising an additional network control element which is adapted to perform an additional authentication.

13. The network system according to claim 12, wherein the network control element controls a first network, and the additional network control element controls a second network.

14. The network system according to claim 11, further comprising an additional network control element for performing an additional authentication, wherein

the communication device (UE) is adapted to calculate a result (CRES) from a predetermined number (RAND) supplied by the additional network control element, wherein the result (CRES) is used by the additional network control element for performing the additional authentication.

15. The network system according to claim 14, wherein the additional authentication is performed by comparing the result (CRES) received from the communication device (UE) with a scheduled result (RES).

16. The network system according to claim 15, wherein the predetermined number (RAND) and the scheduled result (RES) are provided by a home subscriber database (HSS), an Authentication Centre (AuC) or an Authentication Authorization and Accounting server (AAA).

17. The network system according to claim 1 or 2, wherein the calculation is performed by using GSM or UMTS algorithms.

18. The network system according to claim 2, wherein the message including information to be protected is the registration message (B8) received from the communication device (UE).

19. The network system according to claim 2, wherein the message including information to be protected is a response message (B13) sent from the network in response to the registration message (B8) from the communication device (UE).

20. A method for performing registration of a subscriber in a network system, comprising a network control element and a communication device (UE) associated to a subscriber, said method comprising the steps of

sending a registration message (A8; C11) including subscriber information to be protected and an integrity code (MAC) to the network control element,

calculating the integrity code (MAC)in the communication device by using a part or whole of the registration message (A8; C11) including the subscriber information to be protected, and

verifying the integrity code (MAC) in the network control element.

21. A method for performing registration of a subscriber in a network system, comprising a network control element and a communication device (UE) associated to a subscriber, said method comprising the steps of

sending a registration message (B8) from the communication device (UE) to the network control element,

calculating an integrity code (MAC) in the network control element by using a part or whole of the registration message (B8) including subscriber information to be protected,

sending a message (B15) , which includes the information to be protected and the integrity code (MAC) to the communication device (UE) and

verifying the integrity code (MAC) in the communication device (UE).

22. The method according to claim 20 or 21, wherein the subscriber information to be protected comprises information regarding the originator of the registration message.

23. The method according to claim 20 or 21, wherein the subscriber information to be protected comprises information regarding the subscriber to be registered.

24. The method according to claim 20 or 21, wherein the subscriber information to be protected comprises contact information.

25. The method according to claim 20 or 21, further comprising the step of sending a message (A1; B1; C1) including algorithm capability information from the communication device (UE) to the network control element.

26. The method according to claim 24, further comprising

the steps of

choosing which algorithm is to be used for calculating the integrity code (MAC) and

forwarding a message (A6; B6; C9) including information about the chosen algorithm to the communication device (UE).

27. The method according to claim 25, further comprising the steps of

forwarding the algorithm capability information with the registration message (A8; C11) from the communication device (UE) to the network control element, and

verifying (A9; C12) the algorithm capability information in the network control element.

28. The method according to claim 25, further comprising the steps of

forwarding the algorithm capability information with the message (B15) including the information to be protected from the network control element to the communication device, and

verifying (B16) the algorithm capability information in the communication device (UE).

29. The method according to claim 20 or 21, further comprising a step of performing an authentication of the subscriber.

30. The method according to claim 29, wherein the authentication step is performed by using the integrity code (MAC).

31. The method according to claim 29, wherein the network system further comprises an additional network control element which is adapted to perform an additional

authentication.

32. The method according to claim 31, wherein the network control element controls a first network, and the additional network control element controls a second network.

33. The method according to claim 30, wherein the network system further comprises an additional network control element for performing an additional authentication, further comprising the steps of

calculating a result (CRES) in the communication device (UE) from a predetermined number (RAND) supplied by the additional network control element, and

performing the additional authentication in the additional network control element by using the result (CRES).

34. The method according to claim 33, further comprising the step of performing the additional authentication by comparing the result (CRES) received from the communication device (UE) with a scheduled result (RES).

35. The method according to claim 34, wherein the predetermined number (RAND) and the scheduled result (RES) are provided by a home subscriber database (HSS), an Authentication Centre (AuC) or an Authentication Authorization and Accounting server (AAA).

36. The method according to claim 20 or 21, wherein the calculation is performed by using GSM or UMTS algorithms.

37. The method according to claim 21, wherein the message including information to be protected is the

registration message (B8) received from the communication device (UE).

38. The method according to claim 21, wherein the message including information to be protected is a response message (B13) sent from the network in response to the registration message (B8) from the communication device (UE).

39. A network system comprising a network control element and a communication device (UE) associated to a subscriber, wherein

the communication device (UE) is adapted to send a registration message (A1; B1; C1) including algorithm capability information to the network control element, wherein

the network control element is adapted to choose which algorithm is to be used for calculating an integrity code (MAC) and to send a corresponding message (A6; B6; C9) to the communication device (UE), wherein

the network control element and/or the communication device is adapted to verify the algorithm capability information on a later transmittal of a message (A8; B15; C11) including the algorithm capability information.

40. The network system according to claim 39, wherein the communication device (UE) is adapted to calculate an integrity code (MAC) by using a part or whole of a registration message (A8, C11) and to forward the registration message (A8; C11) and the integrity code (MAC) to the network control element.

41. The network system according to claim 40, wherein the communication device (UE) is adapted to forward also information regarding the used algorithm.

42. The network system according to claim 41, wherein the network control element is adapted to verify the integrity code (MAC) on receiving the registration message (A8; C11) from the communication device (UE) by using the information regarding the used algorithm.

43. The network system according to claim 39, wherein the network control element is adapted to calculate an integrity code (MAC) by using a part or whole of a registration message (B8) received from the communication device (UE) and to forward a message (B15) and the integrity code (MAC) to the communication device (UE).

44. The network system according to claim 43, wherein the network control element is adapted to forward also information regarding the used algorithm.

45. The network system according to claim 44, wherein the communication device (UE) is adapted to verify the integrity code (MAC) on receiving the message (B15) from the network control element by using the information regarding the used algorithm.

46. A method for performing registration of a subscriber in a network system comprising a network control element and a communication device (UE) associated to the subscriber, the method comprising the steps of

sending a registration message (A1) including algorithm capability information from the communication device (UE) to the network control element,

choosing which algorithm is to be used for calculating an integrity code (MAC),

sending a corresponding message (A6) to the communication device (UE) and

verifying the algorithm capability information on a later transmittal of a message (A8; B15; C11) including the algorithm capability information in the network control element and/or the communication device.

47. The method according to claim 46, further comprising the steps of

calculating an integrity code (MAC) by using a part or whole of a registration message (A8; C11) and

forwarding the registration message (A8; C11) and the integrity code (MAC) from the communication device (UE) to the network control element.

48. The method according to claim 47, further comprising the step of forwarding also information regarding the used algorithm to the network control element.

49. The method according to claim 48, further comprising the step of verifying the integrity code (MAC) on receiving the registration message (A8; C11) from the communication device (UE) by using the information regarding the used algorithm.

50. The method according to claim 46, further comprising the steps of

calculating an integrity code (MAC) by using a part or whole of a registration message (B8) received from the communication device (UE) and

forwarding a message (B15) and the integrity code (MAC) to the communication device (UE).

51. The method according to claim 50, further comprising the step of forwarding also information regarding the used algorithm to the communication device.

52. The method according to claim 51, further comprising the step of verifying the integrity code (MAC) on receiving the message (B15) from the network control element by using the information regarding the used algorithm.

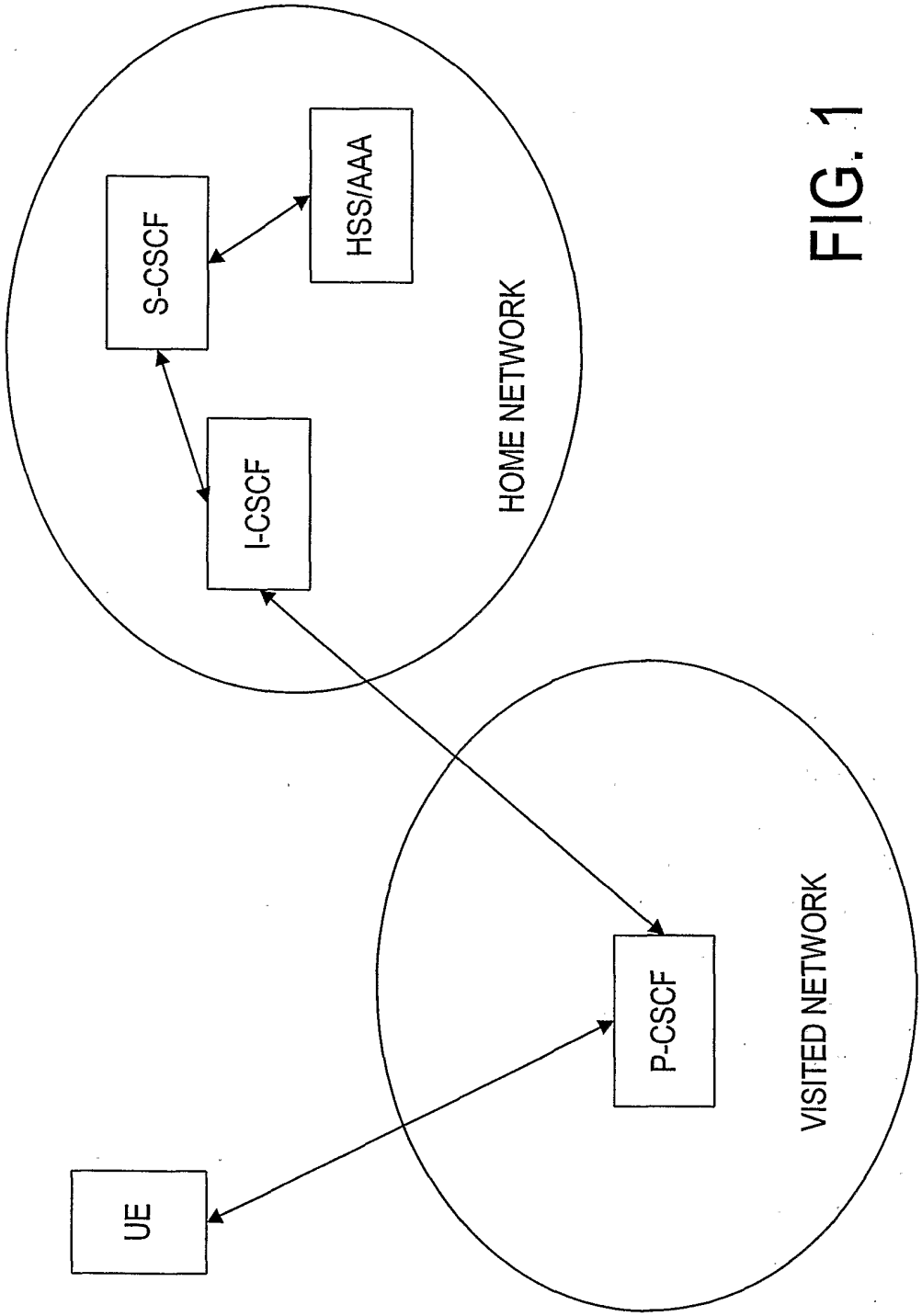


FIG. 1

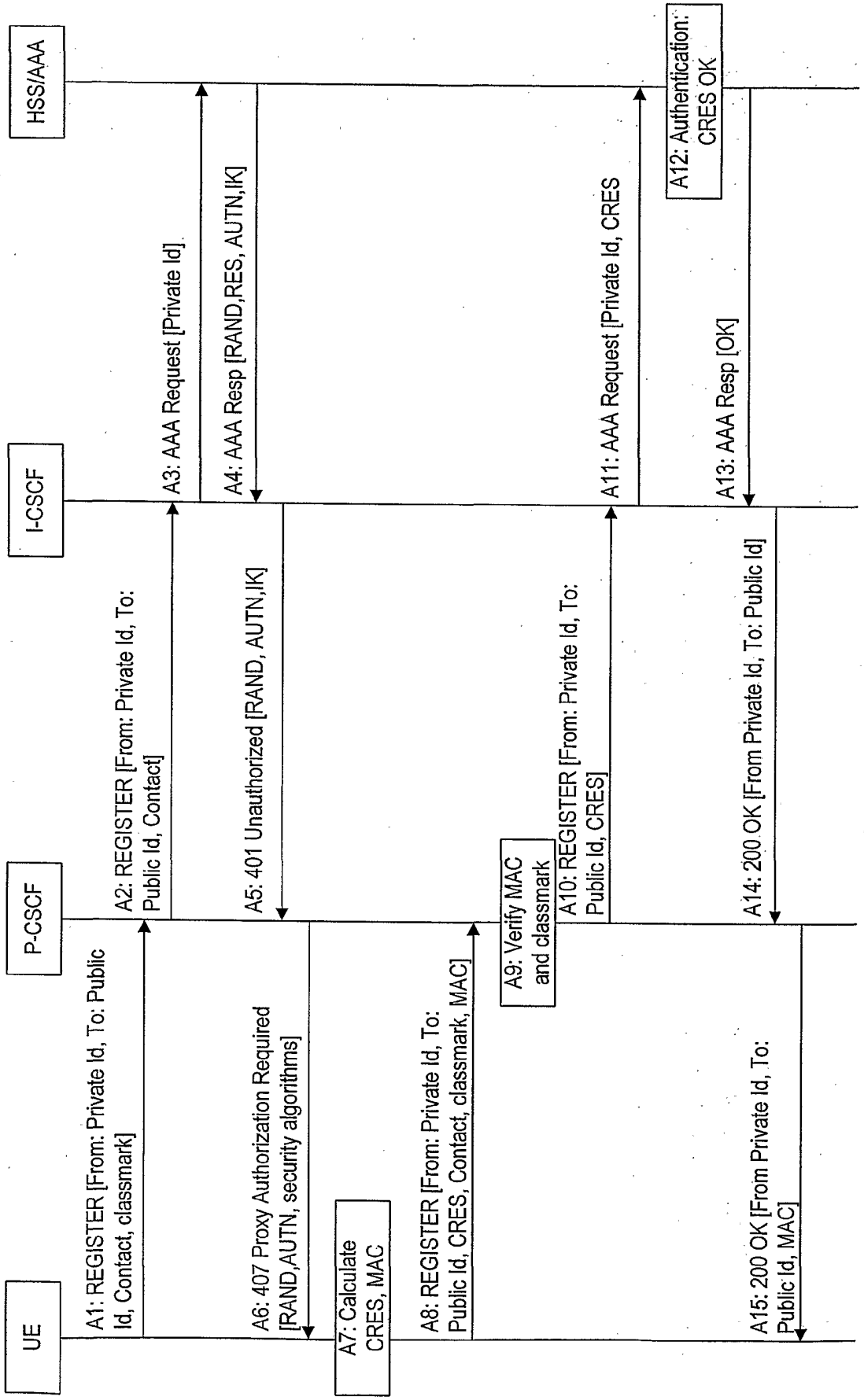

UE
P-CSCF
I-CSCF
HSS/AAA
A1: REGISTER [From: Private Id, To: Public Id, Contact, classmark]
A2: REGISTER [From: Private Id, To: Public Id, Contact]
A3: AAA Request [Private Id]
A4: AAA Resp [RAND,RES, AUTN,IK]
A5: 401 Unauthorized [RAND, AUTN,IK]
A6: 407 Proxy Authorization Required [RAND,AUTN, security algorithms]
A7: Calculate CRES, MAC
A8: REGISTER [From: Private Id, To: Public Id, CRES, Contact, classmark, MAC]
A9: Verify MAC and classmark
A10: REGISTER [From: Private Id, To: Public Id, CRES]
A11: AAA Request [Private Id, CRES
A12: Authentication: CRES OK
A13: AAA Resp [OK]
A14: 200 OK [From Private Id, To: Public Id]
A15: 200 OK [From Private Id, To: Public Id, MAC]

FIG. 2

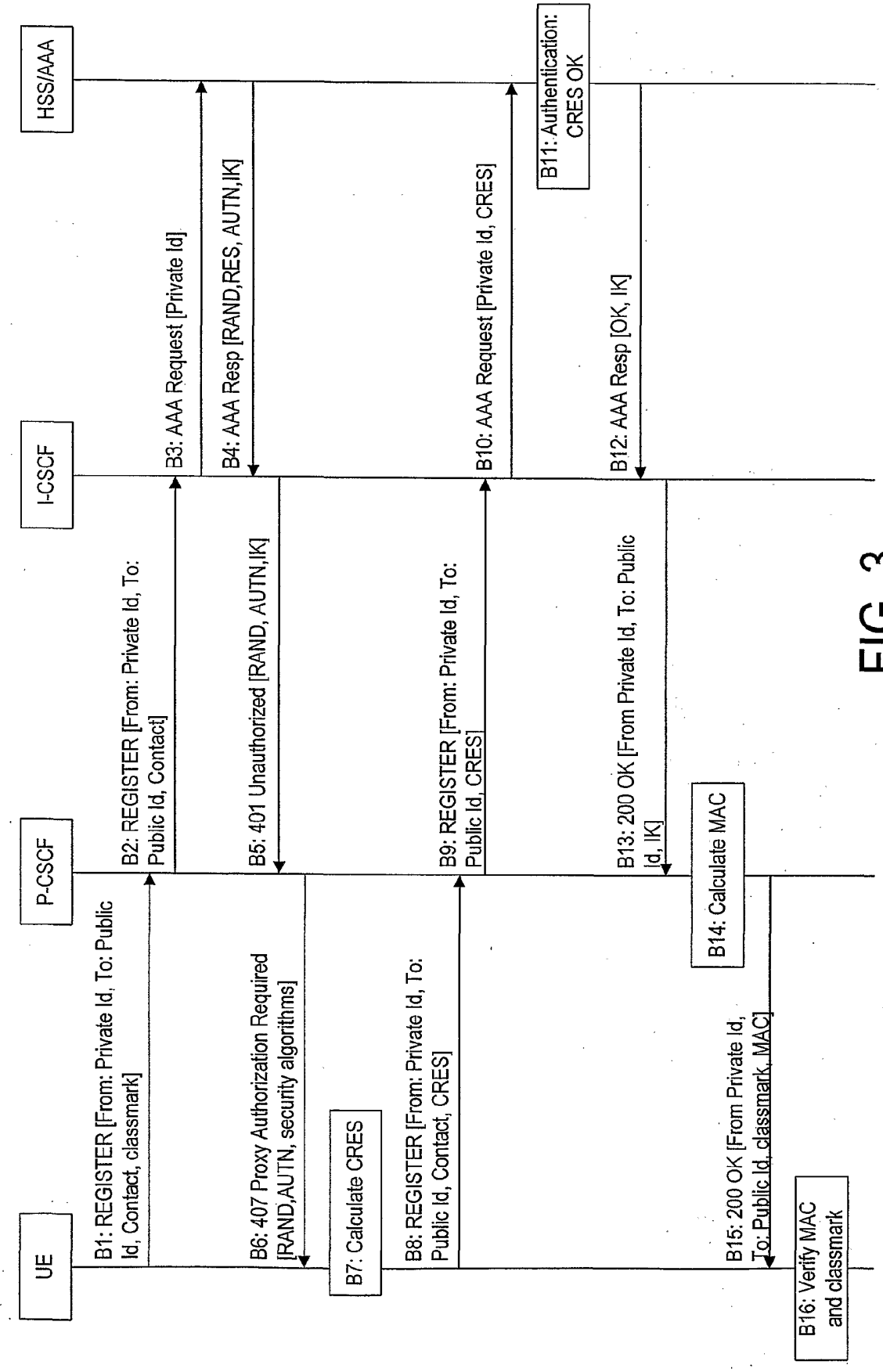

UE
P-CSCF
I-CSCF
HSS/AAA
B1: REGISTER [From: Private Id, To: Public Id, Contact, classmark]
B2: REGISTER [From: Private Id, To: Public Id, Contact]
B3: AAA Request [Private Id]
B4: AAA Resp [RAND,RES, AUTN,IK]
B5: 401 Unauthorized [RAND, AUTN,IK]
B6: 407 Proxy Authorization Required [RAND,AUTN, security algorithms]
B7: Calculate CRES
B8: REGISTER [From: Private Id, To: Public Id, Contact, CRES]
B9: REGISTER [From: Private Id, To: Public Id, CRES]
B10: AAA Request [Private Id, CRES]
B11: Authentication: CRES OK
B12: AAA Resp [OK, IK]
B13: 200 OK [From Private Id, To: Public Id, IK]
B14: Calculate MAC
B15: 200 OK [From Private Id, To: Public Id, classmark, MAC]
B16: Verify MAC and classmark

FIG. 3

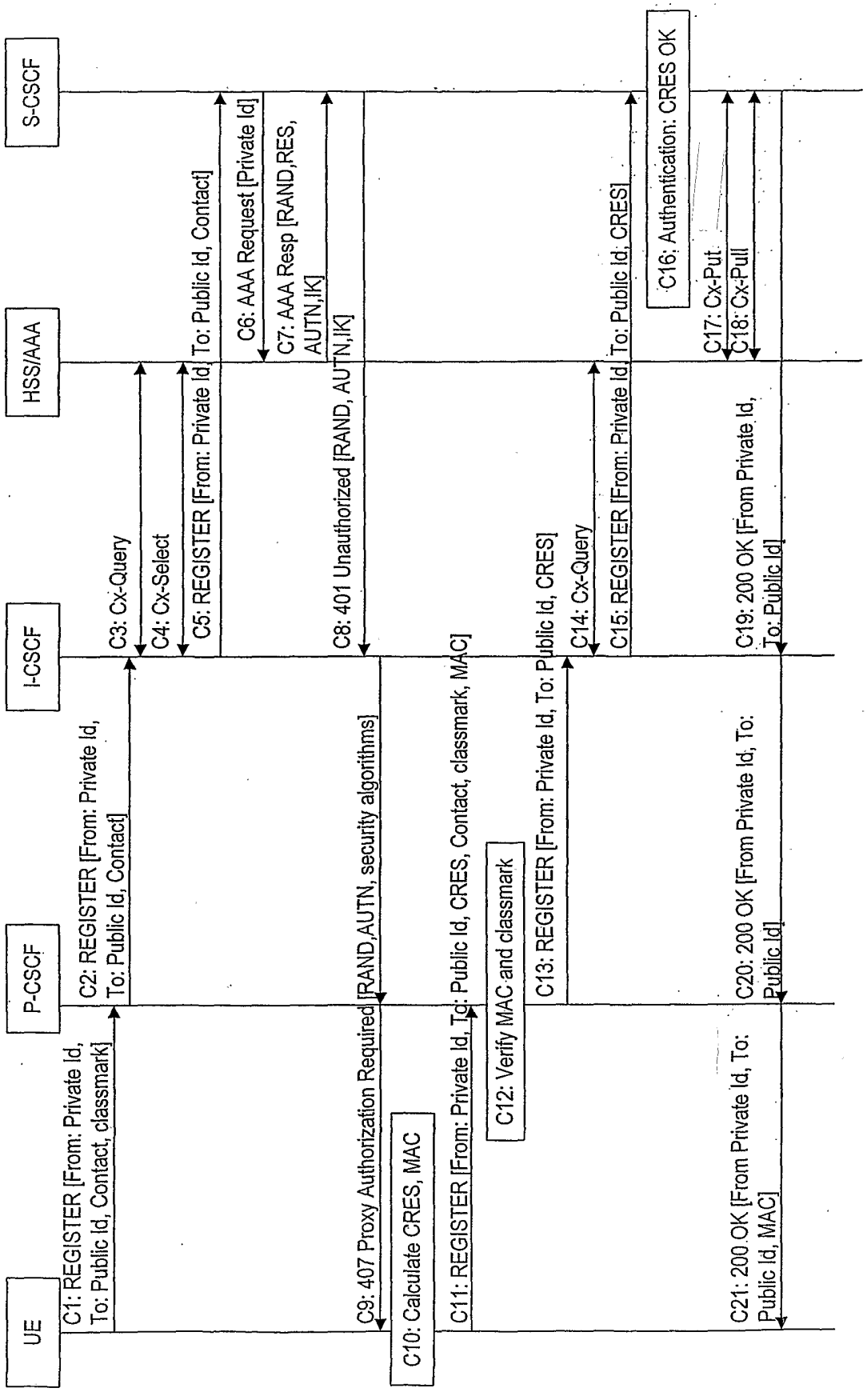

UE
P-CSCF
I-CSCF
HSS/AAA
S-CSCF
C1: REGISTER [From: Private Id, To: Public Id, Contact, classmark]
C2: REGISTER [From: Private Id, To: Public Id, Contact]
C3: Cx-Query
C4: Cx-Select
C5: REGISTER [From: Private Id, To: Public Id, Contact]
C6: AAA Request [Private Id]
C7: AAA Resp [RAND,RES, AUTN,IK]
C8: 401 Unauthorized [RAND, AUTN,IK]
C9: 407 Proxy Authorization Required [RAND,AUTN, security algorithms]
C10: Calculate CRES, MAC
C11: REGISTER [From: Private Id, To: Public Id, CRES, Contact, classmark, MAC]
C12: Verify MAC and classmark
C13: REGISTER [From: Private Id, To: Public Id, CRES]
C14: Cx-Query
C15: REGISTER [From: Private Id, To: Public Id, CRES]
C16: Authentication: CRES OK
C17: Cx-Put
C18: Cx-Pull
C19: 200 OK [From Private Id, To: Public Id]
C20: 200 OK [From Private Id, To: Public Id]
C21: 200 OK [From Private Id, To: Public Id, MAC]

FIG. 4

INTERNATIONAL SEARCH REPORT

Int ɔnal Application No
PCT/EP 01/05832

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 35223 A (CERTICOM CORP ;BLAKE WILSON SIMON (CA); PANJWANI PRAKASH (US)) 15 June 2000 (2000-06-15)	1-5,10, 11, 17-24, 29,30, 36-38
Y	page 3, line 10 - line 20 page 5, line 2 - line 6	6,8,9, 25-28
Y	WO 00 69206 A (NOKIA NETWORKS OY ;MUHONEN AHTI (FI); NIEMI VALTTERI (FI); RAJANIE) 16 November 2000 (2000-11-16) page 8, line 19 -page 9, line 35	6,25,26

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 October 2001	16. 10. 2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schut, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Ir ›nal Application No
PCT/EP 01/05832

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	HANDLEY M ET AL: "SIP: Session Initiation Protocol" NETWORK WORKING GROUP RFC2543, 'Online! 31 March 1999 (1999-03-31), XP002162525 Retrieved from the Internet: <URL:http://www.ietf.org/rfc/rfc2543.txt> 'retrieved on 2001-08-15! page 35, line 17 -page 36, line 2 page 91, line 13 -page 93, line 26 ---	1-5, 18-24, 37,38
Y	EP 1 005 244 A (ICO SERVICES LTD) 31 May 2000 (2000-05-31)	8,9,27, 28
A	abstract ---	39-52
A	US 5 371 794 A (AZIZ ASHAR ET AL) 6 December 1994 (1994-12-06) column 7, line 45 -column 9, line 32 -----	8,9,27, 28,39-52

INTERNATIONAL SEARCH REPORT

ıtional application No.
PCT/EP 01/05832

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/EP 01 /05832

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-7,10-26,29-38

   A network system in which an integrity code is calculated based on subscriber information included in a registration message, the integrity code being sent together with the subscriber information and used for verification at the receiving end.

2. Claims: 8,9,27,28,39-52

   A network system in which algorithm capability information is exchanged between a network control element and a communication device upon registration and is verified on a later transmissal of a message including this information.

INTERNATIONAL SEARCH REPORT

Inf ɔnal Application No
PCT/EP 01/05832

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0035223	A	15-06-2000	AU	1541500 A	26-06-2000
			WO	0035223 A1	15-06-2000
			EP	1135950 A1	26-09-2001
WO 0069206	A	16-11-2000	FI	991088 A	12-11-2000
			AU	4409000 A	21-11-2000
			WO	0069206 A1	16-11-2000
EP 1005244	A	31-05-2000	EP	1005244 A1	31-05-2000
US 5371794	A	06-12-1994	EP	0651533 A2	03-05-1995
			JP	7193569 A	28-07-1995
			US	RE36946 E	07-11-2000