

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 September 2002 (06.09.2002)

PCT

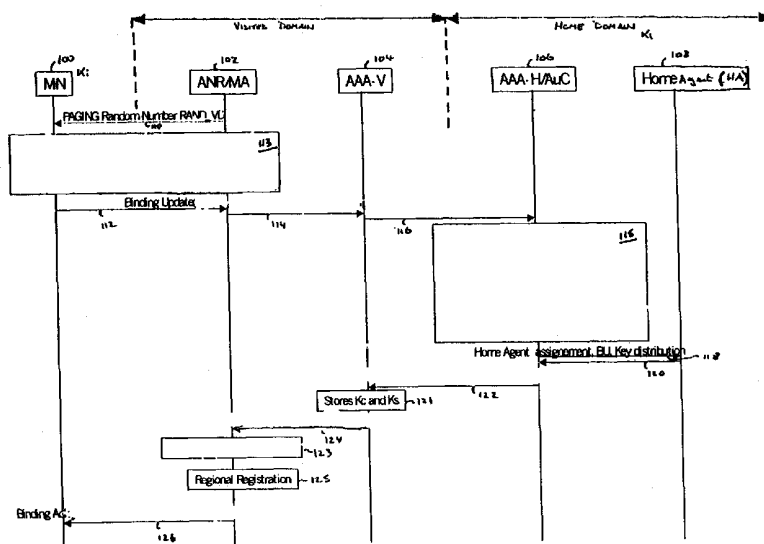
(10) International Publication Number
WO 02/068418 A2

- (51) International Patent Classification⁷: C07D 453/00
- (21) International Application Number: PCT/IB02/01658
- (22) International Filing Date: 25 February 2002 (25.02.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/792,682 23 February 2001 (23.02.2001) US
- (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): FACCIN, Stefano [IT/US]; 3421 Dartmoor, Dallas, TX 75229-2622 (US). LE, Franck [FR/US]; 2715 West Royal Lane #212, Irving, TX 75063 (US).
- (74) Agents: WILLIAMS, David, John et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, 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, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: AUTHENTICATION AND DISTRIBUTION OF KEYS IN MOBILE IP NETWORK



(57) Abstract: There is disclosed a method of establishing a connection between a mobile station and a serving domain, in which a first security association exists between the mobile node and an associated home domain, and a second security association exists between the serving domain and the home domain, the method comprising: transmitting a first message from the mobile node to the serving domain, the first message being encrypted in accordance with the first security association; transmitting the first message from the serving domain to the home domain; decrypting the first message in the home domain in accordance with the first security association; transmitting a second message from the home domain to the serving domain, the second message being encrypted according to the first security association; transmitting the second message from the serving domain to the mobile node; decrypting the second message in the mobile node in accordance with the first security association.

WO 02/068418 A2



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.

AUTHENTICATION AND DISTRIBUTION OF KEYS IN MOBILE IP NETWORKField of the invention

This invention is related to Mobile IP (Internet Protocol) based network architecture and more particularly Mobile IP based cellular networks.

5 Background to the Invention

Many developing network architectures are based on Mobile IP. However, using the Mobile IP protocol for mobility, the mobile node (MN) needs to share a security association with its Home Agent (HA) in its home domain or home network. In addition if hierarchical mobility mechanisms (such as MIPv6RR-regional registration or HMIPv6-
10 Hierarchical Mobile IPv6) are used to optimise signalling in the network, at least one other security association needs to be set up between the mobile node and the Mobility Agent in the visited or serving domain.

If the mobile node is also accessing the network through an access network with a link layer connection that requires ciphering of the data transmitted over the access link in
15 order to protect the data from eavesdropping, another security association must be agreed upon between the MN and some entity in the access network to cipher the data carried over the access link.

Therefore three set of keys need to be distributed for a MN in a Mobile IP network:

- i) The Mobile IP key set to be shared between the MN and its Home Agent, termed **K_m**.
- 20 ii) The key for the hierarchical mobility mechanism set to be shared between the MN and the Mobility Agent in the visited domain, termed **K_s**.
- iii) The Ciphering key to encrypt data over the access link if the MN is accessing the network through an access network with a link layer connection that requires ciphering of the data, termed **K_c**.

25 Today many key distribution protocols exist such as Internet Key Exchange [RFC 2409], Kerberos, etc. to distribute the keys. However these protocols require many messages to be exchanged. As in radio access networks radio resources are limited, such current solutions which rely on many message are not appropriate. When the access network uses

a wireless access link (e.g. in cellular networks), it is highly desirable to reduce the number of messages to be sent over the air interface.

For authentication of the MN and for key distribution some generic mechanisms such as IKE, Kerberos, etc. exist, but they also require many messages to be exchanged, and are
5 thus not suitable for networks using a wireless access link such as cellular networks. In addition many of these solutions distribute the keys by sending them encrypted. However this must be avoided in networks using a wireless access link such as cellular networks, since the wireless link is easily subject to eavesdropping and thus there is the danger of having the keys intercepted. Even if the keys are distributed over the access link by
10 encrypting them, the danger of having the keys intercepted is still too large and this type of solution has traditionally been avoided for networks using a wireless access link such as cellular networks.

One internet draft, 'AAA Registration Keys for Mobile IP (draft-ietf-mobileip-aaa-key-01.txt)', suggests a way to derive the Mobile IP security associations. However the Mobile
15 IP key is sent over the air interface (encrypted), and this must be avoided in cellular networks. In addition this Internet Draft just suggests how to derive the Mobile IP keys. It is an object of the present invention to provide an improved technique for the authentication of the mobile nodes and distribution of keys in a network, and particularly a mobile IP network.

20 Summary of the Invention

This invention describes two methods to distribute the necessary keys in an optimised way. An authentication method is also provided. The authentication procedure provides both user authentication and network authentication.

This invention introduces an optimised authentication and key distribution mechanisms for
25 a mobile node in a Mobile IP based cellular network.

The authentication mechanism provides mutual authentication and is based on challenge-response mechanism. The key distribution procedure requires a minimal number of messages. The key distribution procedure does not require any key, even encrypted, to be sent over the air interface.

Two specific key distribution methods are described in two embodiments. A first method is based on random values, and a second is based on Diffie Hellman values.

This invention enables a network to authenticate a mobile node and a mobile node to authenticate the network. The required security associations in a Mobile IP network architecture are set up without sending an excess of messages over the air interface, and
5 without sending any keys (even encrypted) over the air interface.

The present invention describes a way to authenticate the keys as well as derive them. The authentication and key distribution are advantageously combined in order to reduce the number of messages, but these two procedures may also be performed separately.

10 The technique of the present invention has a number of significant advantages. The procedure does not require many messages to be sent over the air interface. The key distribution mechanisms do not require the key to be sent over the air interface. The key distribution method based on Diffie Hellman is more flexible for a future evolution towards Public Key Infrastructure (PKI).

15 Brief description of the Drawings

The invention will now be described with regard to illustrative examples by way of reference to the accompanying drawings, in which:

Figure 1 illustrates a first embodiment of the present invention;

Figure 2 illustrates a second embodiment of the present invention;

20 Figure 3 illustrates a first modification to the first embodiment of the present invention;

Figure 4 illustrates a second modification to the first embodiment of the present invention;
and

Figure 5 illustrates a third modification to the first embodiment of the present invention.

Description of Preferred Embodiments

25 The present invention is described herein with reference to particular, non-limiting examples. One skilled in the art will appreciate the applicability of the present invention in applications other than those specifically disclosed herein.

The process of initial registration, that may occur when a mobile node (MN) powers on or when a MN enters a new visited network, is described in the following. The user is identified by a Network Address Identifier (NAI) and is authenticated by the network.

At the initial registration, the MN may not have any home agent (HA) assigned to serve it, and may not have the appropriate security keys for communication. In such case, home agent assignment and key distribution happen upon user request during the initial registration.

The mobile node actually requires three sets of key:

- i) A Mobile IP key set to be shared between the mobile and its home network including the associated home agent, termed **K_m**.
- ii) A key for the hierarchical mobility mechanism set to be shared between the MN and the visited or serving domain, termed **K_s**.
- iii) A Ciphering key to encrypt the data over the access link if the MN is accessing the network through an access network with a link layer connection that requires ciphering of the data, termed **K_c**.

Notations: $K(\text{data1}, \text{data2})$: (data1, data2) are sent encrypted with the key K.

Notations: $CK, IK(\text{data1}, \text{data2})$: (data1, data2) are sent encrypted with the key CK and integrity protected with the key IK.

The first embodiment of the invention, described hereinbelow with reference to Figure 1, is based on random numbers. The second embodiment, discussed hereinafter with reference to Figure 2, is based on DH exchange.

In describing the first embodiment with reference to Figure 1, it is assumed that: the MN and the home network have a long term secret K_i defining a security association therebetween; the home and visited networks share a security association allowing data to be sent between these two networks securely; and the AAA-H and home agent also share a security association.

In this embodiment the key distribution is combined with the authentication procedure: before giving keys to any entity, the entity distributing the keys authenticates the parties first. However, the authentication procedure may also be performed separately.

The first embodiment of the present invention is described with reference to the various network elements shown in Figure 1. The network elements comprise a mobile node (MN) 100, an access network router (ANR)/ mobile agent (MA) 102, an AAA-V 104, a AAA-H/AuC 106, and a home agent (HA) 108.

5 In a first step, the access network router (ANR)/mobile agent (MA) 102 of the visited domain generates a first random number, RAND_VD, and pages it over the air interface as represented by arrow 110. The mobile node 100 powers on (or moves to a new visited network) and listens to the router advertisements, and the paged random numbers from the network. The MN also receives a current care-of-address (CoA), and a regional care-of-
10 address (RCoA), from the network.

From the received random number, RAND_VD, and the secret key K_i common to the mobile node and the home network, the mobile node 100 computes a master key K_{c1} which is a function of these two numbers, i.e. $K_{c1} = F_n(K_i, RAND_VD)$. The mobile node then derives the access network specific ciphering key (CK1) and the the access
15 network specific integrity protection key (IK1) from K_{c1} using functions L and M, i.e. $L(K_{c1})=CK1$ and $M(K_{c1})=IK1$. The ciphering and integrity protection keys are used to encrypt the data transmitted over the access link.

The mobile node then generates a second random number for network authorisation being a mobile node random value RAND_MN for use in authenticating the network, and
20 computes authentication data. The authentication data is computed from the value RAND_VD by using the key K_i and an authentication algorithm. Thus the authentication data can be identified as MN_AuthData.

All these computations are carried out in step 113.

The mobile node then sends a binding update (BU) to the ANR/MA as indicated by the
25 arrow 112. The binding update includes the MN regional care-of-address MN_RCoA, the ciphered and integrity protected random number and authentication data MN_AuthData, i.e. CK1,IK1 (RAND_MN, MN_AuthData), the key request, a MAC value, and the visited domain random number RAND_VD.

The ANR/MA 102 receives the BU from the MN, and forwards it to the visited domain
30 AAA server 104. Since this message carries a user authentication extension and a key

request extension, the visited domain AAA server 104 forwards the request to the home AAA server 106 associated with the mobile node 100.

From the user identity, i.e. the identity of the mobile node, the server 106 retrieves K_i . The server 106 uses the $RAND_VD$ value and computes the key K_{c1} using K_i . The server 106
 5 derives the keys $CK1$ and $IK1$ from K_{c1} using the functions L and M , i.e. $L(K_{c1})=CK1$ and $M(K_{c1})=IK1$. The server 106 applies $CK1$ and $IK1$ to decipher and verify the integrity of the $RAND_MN$ and $MN_AuthData...$ The server 106 computes a $MN_AuthData$ based on $RAND_MN$ and K_i . The server 106 computes a
 10 computes NW -Auth Data based on K_i and $RAND$ - MN . Based on K_i , AuC computes three sets of keys:

- i) MIP Key: $K_m, Rand_KM$
- ii) Key for hierarchical mobility model: $K_s, RAND_KS$
- iii) Cipjering Key: $K_{c2}, RAND_Kc2$

15 These computations are carried out in step 115.

The server 106 then verifies the MAC value to make sure the message has not been modified, and generates three further random values: $RAND_K_m$, $RAND_K_s$, and $RAND_K_{c2}$. From these two values, it computes three sets of keys using functions G , H and J :

- 20 i) $G(RAND_K_m, K_i) = K_m$;
- ii) $H(RAND_K_s, K_i) = K_s$; and
- iii) $J(RAND_K_{c2}, K_i) = KC2$.

The AA-H/AuC 106 then chooses a home agent for the mobile node 100, and sends to the chosen home agent 108, as represented by arrow 118, the Mobile IP Key K_m to share with
 25 the MN to authenticate subsequent Binding Updates (MN-HA authentication extensions), and requests the HA to make a binding between the Home address and the Regional Care of Address MN_RCoA of the MN. The Home Agent confirms the reception of the key K_m and the Binding Updtae as represented by arrow 120.

The AAA-H/AuC 106 then sends all the keying material to the visited domain in a second message as represented by arrow 122. The second message comprises the network authentication data NW_AuthData, and the random values RAND_km, RAND_Kc2 and RAND_Ks ciphered and integrity protected by CK1 and IK1, i.e. CK1, IK1 (RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData). Message 122 comprises also the keys Ks and Kc2, and the MAC value. The AAA-H/AuC 106 includes the RAND_MN used to compute the NW_AuthData to allow the MN to verify the network authentication data correctly in case the MN has sent multiple RAND_MN to the home network for different authentication procedures. The AAA-V 104 keeps a copy of the master key Kc2 and the key Ks for the hierarchical mobility mechanism in step 121.

The AAA-V 104, after storing the values Kc2 and Ks, then transmits all the received information to the ANR/MA 102 as represented by arrow 124, which also stores the keys Kc2 and Ks in step 123. The content of the message represented by arrow 124 corresponds to that represented by arrow 122.

Kc2 is used in steps 123 to derive the access network specific ciphering key CK2 and integrity protection key IK2, which are used to cipher and protect data over the air interface, using the functions L and M, i.e. $L(Kc2)=CK2$ and $M(Kc2)=IK2$.

Ks is used to authenticate the binding updates for the hierarchical mobility model from the MN (MN-MA authentication extensions).

The ANR/MA 102 knows from the message received from the mobile node's home network that the user is a valid one, and as such the mobile node has been authenticated. The ANR/MA 102 therefore performs a Binding Update for the hierarchical mobility model as represented by block 125.

The ANR/MA 102 then sends a binding acknowledgement to the mobile node, as represented by arrow 126, to inform it of the success of the binding updates. The ANR/MA 102 also sends to the MN the network authentication data NW_AuthData, and the random values RAND_km, RAND_Kc2 and RAND_Ks ciphered and integrity protected by CK1 and IK1, i.e. CK1, IK1 (RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData). Message 126 comprises also a MAC value.

MN verifies thanks to the MAC that the message has not been altered. MN decipheres and verify for integrity the RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData. MN authenticates the network based on NW_AuthData and Ki. MN uses Ki, F, H and J functions (see above) to compute Ks, Km and Kc2 . The MN derives CK2 and IK2 from Kc2 using the functions L and M, i.e. $L(Kc2)=CK2$ and $M(Kc2)=IK2$, and can then use CK2 and IK2 to cipher and protect data sent over the access link to the ANR/MA.

If the registration for the hierarchical mobility mechanism fails, the mobile node must send a binding update to its home agent informing the regional CoA MN_RCoA is not valid, and requesting the home agent to use its current CoA.

A number of alternatives to the technique described with reference to Figure 1 are described hereinbelow with reference to Figures 3 to 5.

In a second embodiment, it is proposed that the keys may also be computed using the well known Diffie Hellman (DH) algorithm. The mobile node and the other entity with which it is communicating only need to exchange their DH public values in an authenticated way. An example embodiment utilising this technique is described hereinbelow with reference to Figure 2.

In the following, a key establishment between the mobile node and the serving or visited domain is described, (i.e. establishment of Ks).

It is assumed that the MN and the Home Domain share a security association based on Ki, and that the visited domain and home domain share a security association based on K1.

In a first step, the access network router (ANR)/mobile agent (MA) 202 of the visited domain generates a first random number, RAND_VD, and pages it over the air interface as represented by arrow 206. The mobile node 200 powers on (or moves to a new visited network) and listens to the router advertisements, and the paged random RAND_VD from the network.

The mobile node 200 then generates its Diffie Hellman value DH using the Diffie Hellman algorithm. The MN 200 also computes a key Kc from Ki and RAND_VD using function J as indicated above, i.e. $J(RAND_Kc, Ki)=Kc$. The MN 200 derives the keys CK and IK from Kc using the functions L and M, i.e. $L(Kc)=CK$ and $M(Kc)=IK$. As represented by

arrow 208, the MN 200 sends its DH value, encrypted with CK and integrity protected with IK, i.e. CK, IK (DH_MN). Message 208 comprises also of RAND_VD. The Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204 as represented by arrow 210. Before
5 transmitting it to the home domain, the visited domain adds its own DH value encrypted with K1, i.e. the security association shared between the visited domain 202 and the home domain 204. At this point it should be noted that the visited domain may also be referred to as the serving domain.

The Home Domain 204 derives Kc from Ki and RAND_VD, and derives the keys CK and
10 IK from Kc using the functions L and M, i.e. $L(Kc)=CK$ and $M(Kc)=IK$. The Home Domain 204 can then decrypt both CK, IK (DH_MN) and K1 (DH_VD) to recover the mobile node DH value MN_DH, and the visited domain DH value VD_DH. The home domain then encrypts mobile node DH value, DH_MN, using K1, and the visited domain DH value, DH_VD, using CK and IK. The thus encrypted DH values are transmitted to
15 the visited domain 202 as represented by arrow 212.

The visited domain receives DH_MN encrypted with K1. Since the visited domain has an established relationship with the home domain and trusts the home domain, it can decrypt the mobile node DH value encrypted with key K1 to recover the mobile node DH value. It knows DH_MN is the DH public value of the mobile node.

20 The visited domain forwards a message 214 comprising the visited domain DH value encrypted with key CK and integrity protected by IK, compiled by the home domain 201, to the mobile node 200.

In the same way as the visited domain, when the MN receives CK, IK (DH_VD), it can decrypt using CK and IK. Since it trusts its home domain, it knows DH_VD is the DH
25 public value of the visited domain.

The mobile node and the visited domain have at this point exchange the respective DH public values in an authenticated way and can both compute the DH key Ks by using DH_MN and DH-VD. The keys Kc2 and Km may be established in the same way, using the DH mechanism and different DH values, one for each of the three keys to be
30 established. This procedure has the advantage to set up keys at points in the network

(namely MN 200 and Visited Domain 202) without having to send any key over the network.

In the described embodiments, the home domain is used to authenticate the DH public value of the different network entities. In the future, when PKI is implemented, the PKI
5 infrastructure may be used to substitute the home domain role and authenticate the DH public values. This scheme therefore allows easy evolution towards PKI.

In addition, in the above-described embodiments, user authentication is based on symmetric key mechanisms (Ki). However if the mobile node and the home domain have Public Keys, Public Key authentication mechanisms can also be used.

10 The solution may be implemented in existing networks by adding: new extensions in Diameter; or new extensions in Mobile IP.

In the embodiment illustrated in Figure 1, the random number is generated by the visited network. Compared to generation by the home network, this saves one round trip between the visited and the home networks. However, if the network operators prefers, the home
15 network may generate the random value. The random value may still be paged over the air, but as an alternative the mobile node may first send a challenge request to the visited domain and the visited domain forwards it to the home network, and receive the random number responsive thereto.

In the embodiment illustrated in Figure 1, the random value generated by the serving
20 system is used for user authentication and ciphering key computation. In an alternative, this random value may be used for user authentication only, and the home domain may generate the ciphering key Kc in the same way that it computes the keys Km and Ks.

There are three possibilities for sending the keying material to the mobile node over the air interface, as detailed hereafter.

25 "In cleartext": Any user which captures RAND_Km, Kc_mat and RAND_Ks, does not know Ki and therefore can not compute Km, Kc nor Ks. For that reason, the keying material can be sent in "cleartext"

Encrypted with a temporal Key shared between the MN and the Home Domain: A temporal key Kt may be derived from Ki and used to encrypt RAND_Km, RAND_Ks and

for the hierarchical mobility mechanism, it can initiate the registration procedure for the hierarchical mobility mechanism thus saving one round trip over the air interface.

The third BU (arrows 424, 426) is a BU with the MN's Home Agent: the AR cannot perform this BU because it does not have the Mobile IP Key.

- 5 In the example of Figure 4, the number of messages sent over the air interface is reduced to six.

An alternative embodiment is shown in Figure 4. Reference is now made to Figure 5. A first BU 516 requests the Challenge. A second BU 518 carries the authentication data and the keying material.

- 10 A third BU 521 includes two BUs: one 520 for the hierarchical mobility mechanism and one 522 for the HA BU (this latter one will be computed with MN Mobile IP key). The AR will first perform the registration for the hierarchical mobility mechanism; if it fails then the AR informs the MN without executing the HA BU. In the case of success, it transmits the HA BU to the MN's Home Agent.

Kc_mat. This adds another level of protection: to know Km, Ks and Kc, two levels of security must be broken: Kt and Ki. But Kt needs to be re-freshed.

Encrypted with the session key. The mobile node and the visited domain must first share the session key Kc. This can be realized as indicated in the case above (generation of the challenge number by the visited domain). Then RAND_Km and RAND_Ks can be sent
5 encrypted over the air interface

For Integrity protection, a MAC can be computed over every message or if preferred, a MAC can be computed over RAND_Km, another over RAND_Ks, and eventually one over Kc_mat.

10 Computing different MACs, the user may know which one is corrupted, and request a new value for this specific set. However, this results in more MACs being sent over the air interface.

Depending on the access link technology, the access link may have a limited ability to carry information and may not be able to carry all the parameters such as the key request,
15 the random value generated by the MN to authenticate the network, etc.

Therefore the procedure may be split into different parts. After receiving the challenge, the user only sends back the user authentication data; and then once the user is authenticated and a dedicated channel assigned, the mobile node can request key distribution and network authentication.

20 The operators may not let the user send too much information over the air before authentication.

In the embodiments described hereinabove, there is described the combination of the authentication procedure, the key distribution, the mobile IP hierarchical mobility mechanism and the mobile IP home registration. However, one skilled in the art will
25 appreciate that all these procedures can be performed separately or ordered differently. Various possibilities will be presented and described with reference to Figure 3 to 5. However, further modifications may exist and the variations described below are in no way limiting. It should be noted that in Figures 3 to 5 a number of operations are shown which correspond directly to those described hereinabove with reference to Figures 1 and

2. For conciseness, only those message exchanges necessary for an understanding of the modifications presented are described in detail.

Reference is now made to Figure 3. The MN 300 powers on or moves to a new visited domain and listens to the router advertisements. The MN 300 creates and sends (arrow 5 316) a Binding update (BU) request: the destination address is the Mobility Agent (AR) 302 whose address has been provided during the router advertisement. The BU includes the identity of the user, which is the user's NAI, and also include a Challenge Request to indicate to the home network the need to register and be authenticated.

The AR receives the BU from the MN and since this message carries a Challenge Request, 10 it forwards the request (arrow 318) to the local AAA server 310, which transfers it to the Home Network of the user (arrow 320). The AAA-H/AuC 312 generates a random number RAND_HD and sends it to the MN (arrows 322, 324, 326).

This random number provides a strong authentication mechanism, and also serves for anti replay attacks. Timestamp is a possible alternative: it requires fewer messages but requests 15 secured synchronized clocks between the MN 300 and the AAA-H/AuC 312.

From the received random number, RAND_HD, and the secret key K_i common to the mobile node and the home network, the mobile node 300 computes a master key K_{c1} which is a function of these two numbers, i.e. $K_c = F_n(K_i, RAND_HD)$. The mobile node then derives the access network specific ciphering key (CK1) and the the access network 20 specific integrity protection key (IK1) from K_{c1} using the functions L and M, i.e. $L(K_{c1})=CK1$ and $M(K_{c1})=IK1$. The ciphering and integrity protection keys are used to encrypt the data transmitted over the access link.

The mobile node then generates a second random number being a mobile node random value RAND_MN for use in authenticating the network, and computes authentication data 25 MN_AuthData. The authentication data is computed from the value RAND_HD by using the key K_i and an authentication algorithm.

The MN then sends a BU including the authentication data MN_AuthData, computed with K_i , and a Key Request (arrow 328). The binding update includes the ciphered and integrity protected random number and authentication data MN_AuthData, i.e. CK1,IK1

(RAND_MN, MN_AuthData), the key request, a MAC value, and the home domain random number RAND_HD.

The BU is forwarded to the AAA-H (arrows 330, 332). The AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified. From the user identity, i.e.
 5 the identity of the mobile node, the server AAA-H/AuC 312 retrieves K_i . The AAA-H/AuC 312 derives K_{c1} from K_i and RAND_HD, and derives CK1 and IK1 from K_{c1} . The AAA-H/AuC 312 will then decipher and verify the integrity of RAND_MN and MN_AuthData, and authenticates the user by using MN_AuthData and K_i . The AAA-H/AuC 312 computes NW_AuthData based on K_i and RAND_MN. Finally, the AAA-
 10 H/AuC 312 generates three further random values: RAND_Km, RAND_Ks, and RAND_Kc2. From these three values, the AAA-H/AuC 312 computes three sets of keys using functions G, H and J:

- i) $G(\text{RAND_Km}, K_i) = K_m$;
- ii) $H(\text{RAND_Ks}, K_i) = K_s$; and
- 15 iii) $J(\text{RAND_Kc2}, K_i) = K_{c2}$.

Thus in box 331 the AAA-H/AuC derives K_{c1} from K_i and Rand-HD, derives CK1 and IK 1 from K_{c1} , authenticates the MN based on MN_AuthData and K_i . Further NW_AuthData is computed based on K_i and RAND_MN. Based on K_i , AuC computes three sets of keys:

- 20 i) MIP Key: $K_m, \text{RAND_Km}$
- ii) Key for hierarchical mobility model: $K_s, \text{RAND_Ks}$
- iii) Cipherring Key: $K_{c2}, \text{RAND_Kc2}$

The AAA-H/AuC 312 then chooses a Home Agent and sends the Mobile IP key K_m to the selected HA.

25 The AAA-H then sends the keying material to the AAA-V (arrow 334) in a message containing the ciphered and integrity protected RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData, i.e. CK1, IK1 (RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData). Message 334 comprises also the keys K_s and K_{c2} , and a MAC. The AAA-v 310 stores the keys K_{c2} and K_s (step 336). A security association

between the home and visited domains enables the AAA-H and the AAA-V servers to exchange data in a secure way.

The AAA-V 310 transfers the keying material to the AR which will enable the MN to compute the required keys, including the network authentication data the MN will use to
5 authenticate the network (arrow 338). Message 338 contains the ciphered and integrity protected RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData, i.e. CK1, IK1 (RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData). Message 338 comprises also the keys Ks and Kc2, and a MAC.

The AR 302 stores the key Ks (step 340) and the key Kc2, and derives CK2 and IK2 from
10 Kc2 using the functions L and M, i.e. $L(Kc2)=CK2$ and $M(Kc2)=IK2$. The AR 302 forwards the the ciphered and integrity protected RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData, i.e. CK1, IK1 (RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData), the MAC to the MN (arrow 342).

MN (steps 344) verifies thanks to the MAC that the message has not been altered. MN
15 decipheres and verify for integrity the RAND_Km, RAND_Ks, RAND_KC2, RAND_MN, NW_AuthData. MN authenticates the network based on NW_AuthData and Ki. MN uses Ki, F, H and J functions (see above) to compute Ks, Km and Kc2 . The MN derives CK2 and IK2 from Kc2 using the functions L and M, i.e. $L(Kc2)=CK2$ and $M(Kc2)=IK2$, and can then use CK2 and IK2 to cipher and protect data sent over the access link to the
20 ANR/MA.

The MN then performs a BU for the hierarchical mobility mechanism with the Visited Network (arrow 346).

Once the registration for the hierarchical mobility mechanism (step 348) has succeeded, as indicated by arrow 350, the MN executes a BU with its HA (arrows 352, 354).

25 An alternative embodiment is shown in Figure 4. Reference is now made to Figure 4, which illustrates a modification in which the key request and the registration for the hierarchical mobility mechanism are combined.

The first BU (arrow 416, 418) requests the Challenge. The second BU (arrows 420, 422) carries the authentication data and the key request. After the Home network has
30 authenticated the user, the AR knows that the MN is a valid one and since it has the key

Claims

1. A method of establishing a connection between a mobile station and a serving network for serving the mobile station, wherein the mobile station is associated with a home network, a first security association being established between the mobile station and the home network, and a second security association being established between the home network and the supporting network, the method comprising using the first security association to authenticate a communication from the mobile node at the home network, and confirming such authentication to the visited network using the second security association, whereby there is authenticated a connection between the mobile station and the serving network.
2. A method according to claim 1 wherein the mobile node receives a first random number from the visited network, and generates mobile node authentication data in dependence on an authentication algorithm applied to the first random number and the first security association.
3. A method according to claim 2 wherein the mobile node authentication data and the first random number is transmitted from the mobile node to the home network via the visited network.
4. A method according to claim 3 wherein responsive to receipt of the mobile node authentication data and the first random number, the home network authenticates the mobile node.
5. A method according to any one of claims 2 to 4 wherein the mobile node further generates a second random number for use in network authentication.
6. A method according to claim 5 wherein the second random number is transmitted from the mobile node to the home network via the visited network.
7. A method according to claim 6 wherein the home network generates network authentication data in dependence on an authentication algorithm applied to the second random number and the second security association.
8. A method according to claim 7 wherein the home network transmits the network authentication data and the second random number to the visited network.
9. A method according to claim 4 wherein responsive to the network authentication data and the second random number the mobile node authenticates the network.

10. A method according to any one of claims 1 to 9 wherein the mobile node determines a master security key derived from the first security association and the first random number.
11. A method according to claim 10, wherein in dependence on the master security key
5 the mobile node derives an access network specific ciphering key and an access network specific integrity protection key using respective predetermined functions.
12. A method according to claim 11 when dependent upon claim 3 wherein the mobile node authorisation data is encrypted using said cipher and integrity keys.
13. A method according to claim 12 wherein the first random number is not encrypted.
- 10 14. A method according to claim 12 or 13 wherein the home network derives the master key based on the first security association and the first random number.
15. A method according to claim 14 wherein in dependence on the master security key the mobile node derives an access network specific ciphering key and an access network specific integrity protection key using respective predetermined functions.
- 15 16. A method according to claim 1 wherein the step of using the first security association to authenticate a communication from the mobile node at the home network includes transmitting at least one Diffie Hellman value of the mobile node to the visited network using the first security association, wherein the visited network forwards such to the home network.
- 20 17. A method according to claim 16 further including transmitting at least one Diffie Hellman value associated with the visited network to the home network using the second security association.
18. A method according to claim 16 or claim 17, further including transmitting the at least one Diffie Hellman value associated with the mobile node from the home network to
25 the visited network using the second security association.
19. A method according to claim 18 further including transmitting the at least one Diffie Hellman value associated with the visited network from the visited network to the mobile node.
20. A method according to any one of claims 16 to 19, wherein said at least one Diffie
30 Hellman value is used for distribution of Mobile IP key and/or Hierarchical key and/or Master key.

21. A method according to any one of claims 16 to 19, wherein the mobile node receives a first random number from the visited network, and the mobile node computes a master key in dependence on a function of the first random number and the first security association.
- 5 22. A method according to claim 21 wherein the mobile node computes a ciphering key and an integrity key as functions of the master key.
23. A method according to claim 21 wherein the at least one mobile node Diffie Hellman value is encrypted with the ciphering key and the integrity key.
24. A method according to claim 23 wherein the at least one visited domain Diffie Hellman
10 value is encrypted in accordance with the second security association.
25. A method according to any one of claims 21 to 24 wherein the home domain derives the master key from the first random value and the first security association.
26. A method according any preceding claim, wherein the home network further generates at least one random number for distribution of Mobile IP key and/or
15 Hierarchical key and/or Master key.
27. A method according any preceding claim wherein the home network provides the Mobile IP key (or Diffie Hellman value for Mobile IP key) to the Home Agent.
28. A method according any preceding claim wherein hierarchical key is delivered to Mobility Agent in the serving network.
- 20 29. A method according any preceding claim wherein the Master key is stored in the serving network.
30. A method according to claim 20, wherein the mobile node derives from said at least one Diffie Hellman value the Mobile IP key and/or the Hierarchical key and/or the Master key.
- 25 31. A method according any preceding claim wherein public key infrastructure instead of home network is used for authentication of the subscriber.
32. A method according to claim 2, wherein said first random number is generated by the home network.
- 30 33. A method of establishing a connection between a mobile station and a serving domain, in which a first security association exists between the mobile node and an

associated home domain, and a second security association exists between the serving domain and the home domain, the method comprising

- 5 transmitting a first message proxied security association negotiation request from the mobile node to a serving domain, the first message being encrypted in accordance with the first security association
- transmitting such first message request for proxied security association negotiation from the serving domain to said home domain;
- transmitting a second message from the home domain to the serving domain
- transmitting the second message from the serving domain to the mobile node.

- 10 34. A mobile communication system in which a connection is established between a mobile station and a serving network for serving the mobile station, wherein the mobile station is associated with a home network, a first security association being established between the mobile station and the home network, and a second security association being established between the home network and the supporting network,
- 15 the method comprising using the first security association to authenticate a communication from the mobile node at the home network, and confirming such authentication to the visited network using the second security association, whereby there is authenticated a connection between the mobile station and the serving network.

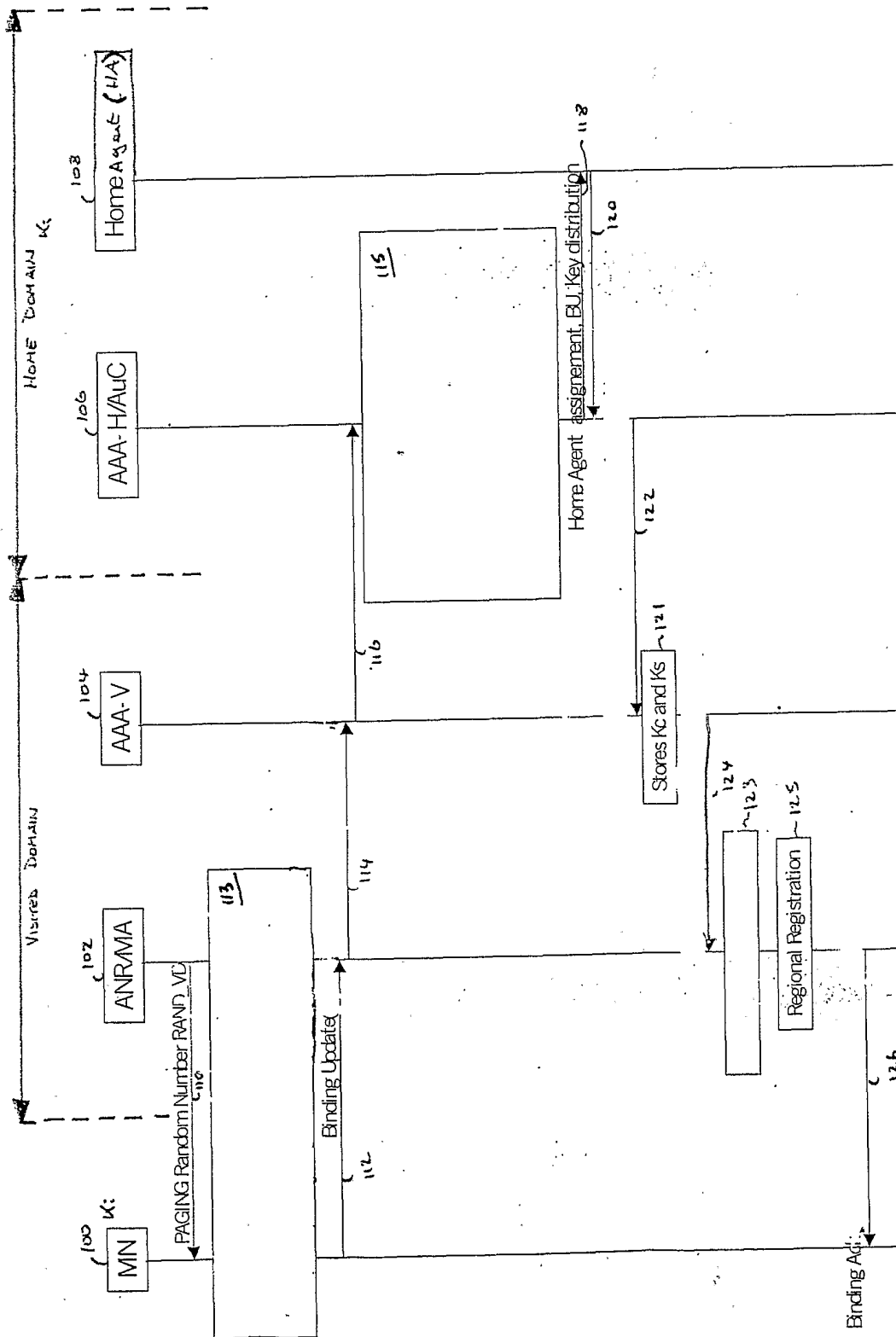


Figure 1

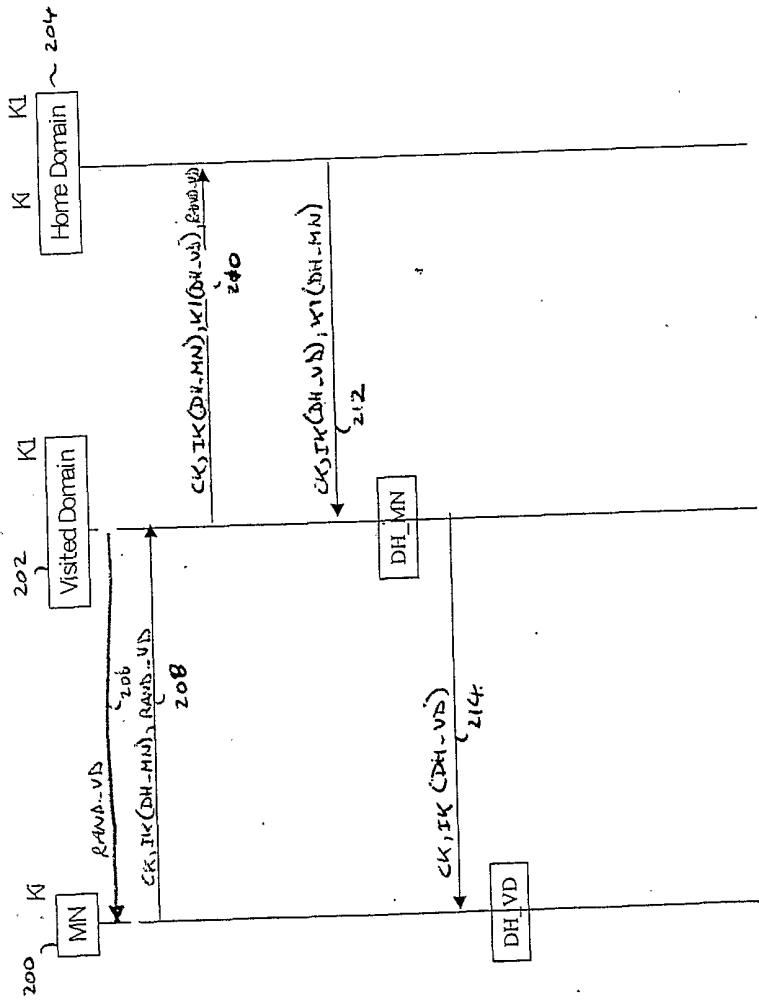


Figure 2

2

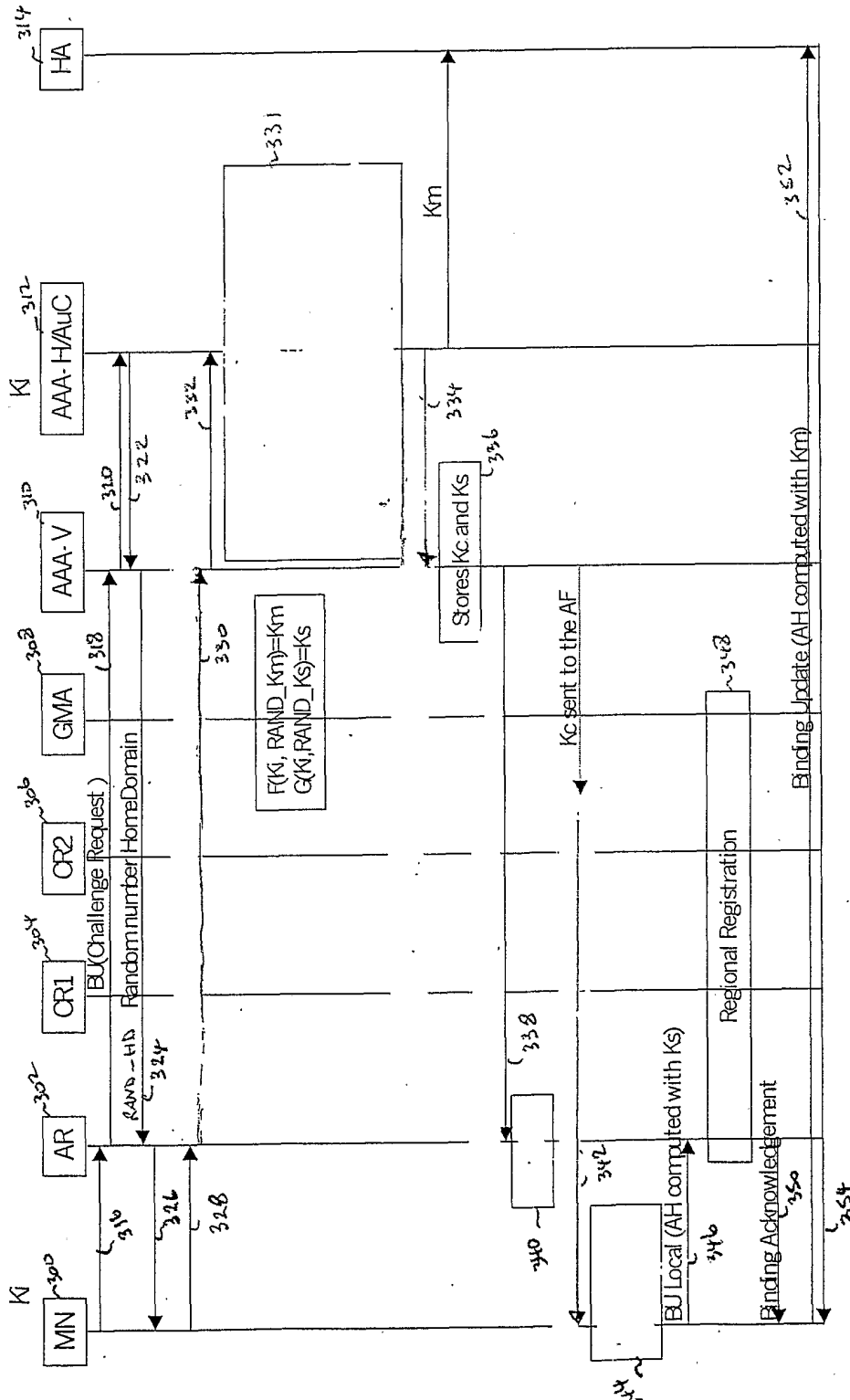


Figure 3

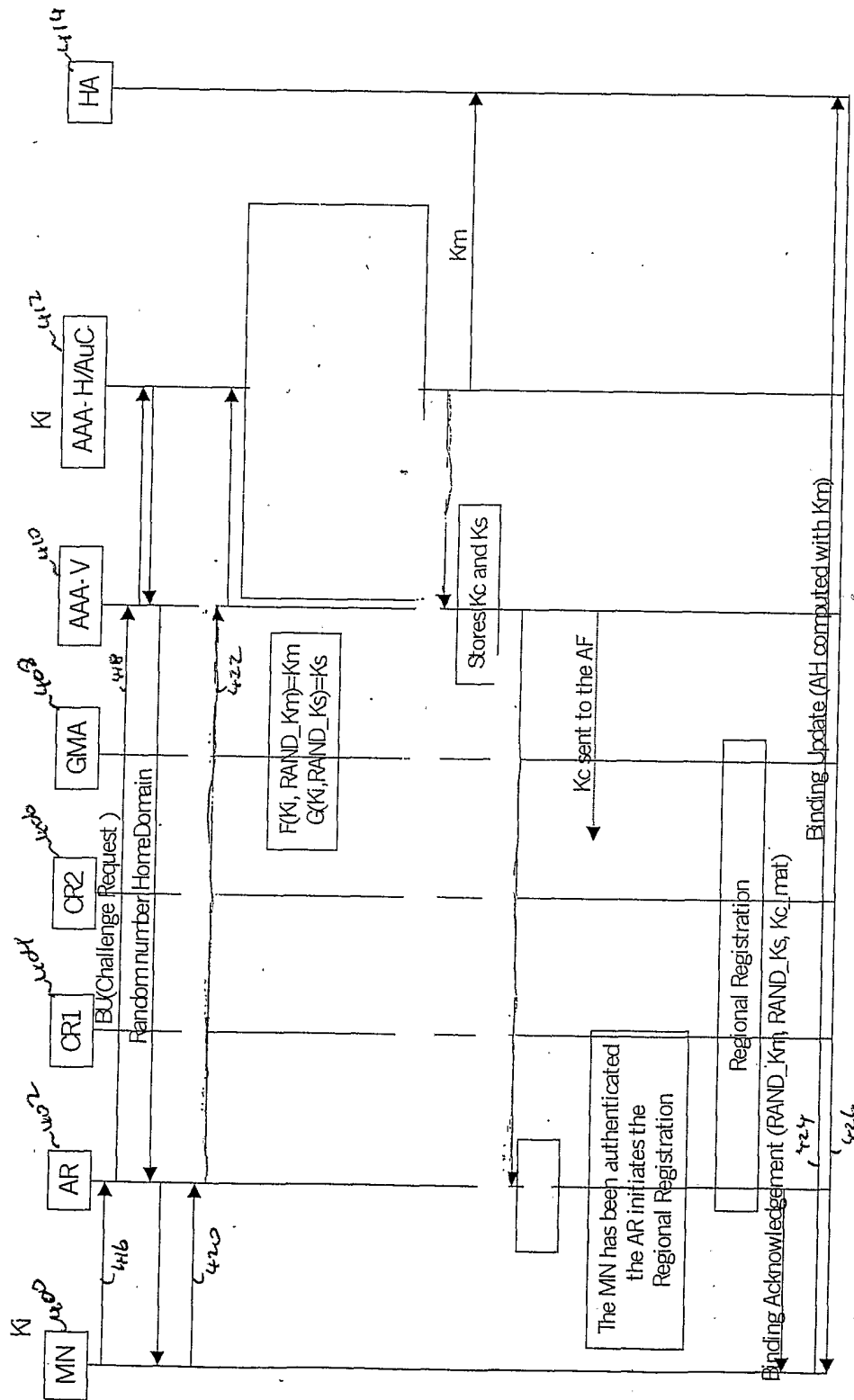


Figure 4

A

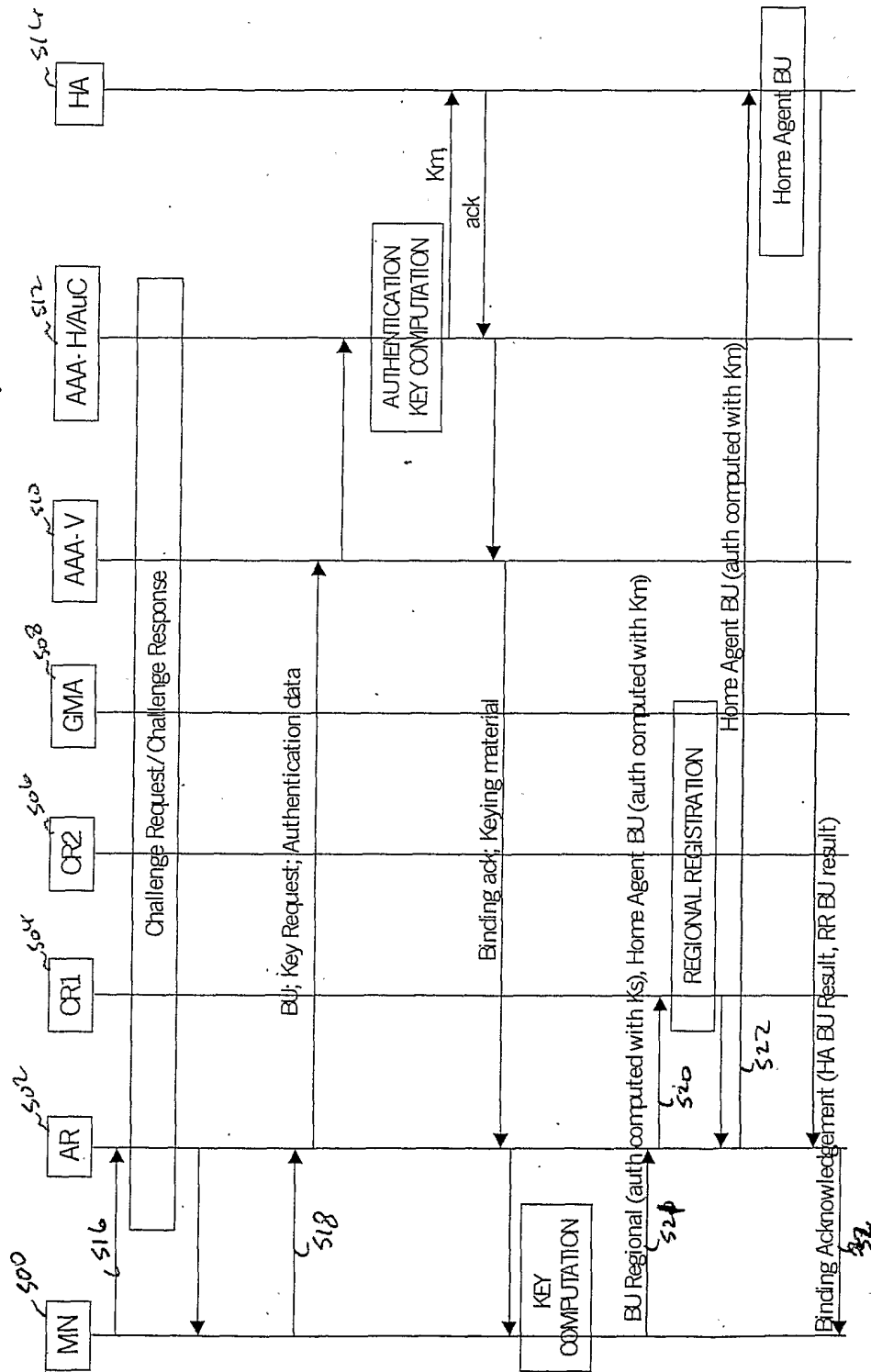


Figure 5

5