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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 November 2005 (10.11.2005)

PCT

(10) International Publication Number
WO 2005/107214 A1

(51) International Patent Classification[7]: H04L 29/06, 12/56

(21) International Application Number: PCT/IB2005/001704

(22) International Filing Date: 28 April 2005 (28.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0409704.4 30 April 2004 (30.04.2004) GB

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

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **LAITINEN, Pekka** [FI/FI]; Hiihtomäentie 44 A 2, FIN-00800 Helsinki (FI).

(74) Agents: **STYLE, Kelda, Camilla, Karen** et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

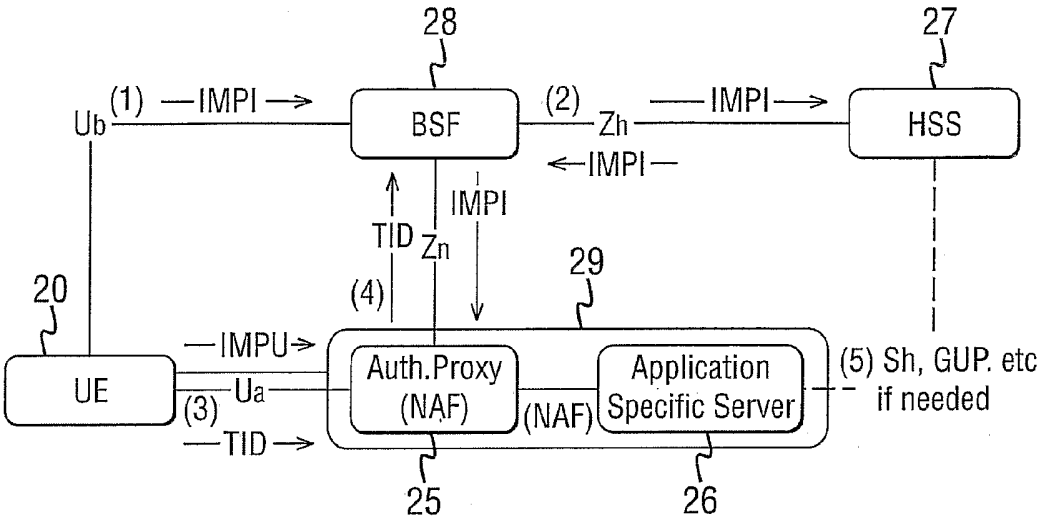
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

(54) Title: A METHOD FOR VERIFYING A FIRST IDENTITY AND A SECOND IDENTITY OF AN ENTITY



(57) Abstract: A method for verifying a first identity and a second identity of an entity, said method comprising: receiving first identity information at a checking entity; sending second identity information from the entity to said checking entity; verifying that the first and second identities both belong to said entity; and generating a key using one of said first and second identity information.

WO 2005/107214 A1

A method for verifying a first identity and a second identity of an entity

Field of the Invention

The present invention relates to verifying the identities of a network entity.

Background of the Invention

The current development towards truly mobile computing and networking has brought on the evolution of various access technologies, which also provide the users with access to the Internet when they are outside their own home network. The first public communication network that provides a truly ubiquitous World Wide Web (WWW) access is the GSM-based mobile telephone network.

So far, the use of the Internet has been dominated by person-to-machine communications, i.e. information services. The evolution towards the so-called third generation (3G) wireless networks brings along mobile multimedia communications, which will also change the way IP-based services are utilized in public mobile networks. The IP Multimedia Subsystem (IMS), as specified by the by the 3rd Generation Partnership Project (3GPP), integrates mobile voice communications with Internet technologies, allowing IP-based multimedia services to be utilized in mobile networks.

The inventors have identified an important problem with mobile multimedia communications in third generation wireless networks, namely that of identity coherence checking in the so-called third generation Generic Authentication Architecture GAA. This is for example described in the Technical specification TS 33.220v6.

The new multimedia capable mobile terminals (multimedia phones) provide an open development platform for application developers, allowing independent application developers to design new services and applications for the multimedia environment. The users may, in turn, download the new applications/services to their mobile terminals and use them therein.

GAA is to be used as a security procedure for a plurality of future applications and services. However, the inventors have identified a flaw in GAA.

In particular, in GAA there is a need for a bootstrapping server function (BSF) to be able to verify a binding between a public identifier of a network application function (NAF) and the GAA internal identifier of the NAF. The public identifier of the NAF is the public host name of the NAF that the user equipment (UE) uses in the Ua interface. The internal NAF identifier is the network address that is used in the corresponding DIAMETER messages in the Zn interface. The public NAF identifier is needed in the boot strapping function because the bootstrapping server function uses it during the derivation of the NAF specific key (Ks_NAF).

This problem is more pronounced if the NAF is doing virtual name based hosting, that is having multiple host names mapped on to a single IP (internet protocol) address. Thus, there may be one-to-many mapping between the internal NAF address and the public NAF addresses. The domain name server is not able to verify that a certain NAF address identified by a certain internal NAF address in the bootstrapping server function is authorised to use a certain public NAF address.

Embodiments of the present invention seek to address the above-described problems.

Summary of the Invention

According to an embodiment of the present invention there is provided a method for verifying a first identity and a second identity of an entity, said method comprising: receiving first identity information at a checking entity; sending second identity information from the entity to said checking entity; verifying that the first and second identities both belong to said entity; and generating a key using one of said first and second identity information.

According to another embodiment of the present invention there is provided a method for verifying an external interface address and an internal interface address of a network application function, comprising the steps of: receiving the internal interface address at a boot strapping function from user equipment; receiving the external interface address at the boot strapping function from the

network application function; and verifying that the external interface address and the internal interface address belong to the same network application function.

According to another embodiment of the present invention there is provided a system comprising a checking entity arranged to receive a first identity of an entity at a checking entity; said entity arranged to send a second identity of the entity from the entity to said checking entity, said checking entity being arranged to verify that the first and second identities both belong to said entity and to generating a key from one of said first and second identities.

According to another embodiment of the present invention there is provided a checking entity arranged to receive a first identity of an entity and a second identity of the entity, said second entity identity being received from the entity, said checking entity being arranged to verify that the first and second identities both belong to said entity and to generating a key from one of said first and second identities.

According to an embodiment of the present invention there is provided an entity comprising a first and second identity, said entity arranged to send the second identity to a checking entity and to receive a key generated from said second identity from the checking entity.

Brief Description of the Drawings

For a better understanding of the present invention and as to how the same may be carried into effect, reference will now be made by way of example to the accompanying drawings in which:

Figure 1 shows an overview of GAA applications;

Figure 2 shows a first signal flow in one embodiments of the invention; and

Figure 2 shows a second signal flow in another embodiment of the invention.

Detailed description of preferred embodiments of the invention

Reference is made to Figure 1 which shows a GAA architecture in which embodiments of the present invention may be incorporated.

User equipment UE 20 is provided. The user equipment can take any suitable form and may for example be a mobile telephone, personal organiser, computer or any other suitable equipment. The user equipment 20 is arranged to communicate with a bootstrapping server function BSF 28 via a Ub interface. The user equipment 20 is also arranged to communicate with a network application function NAF 29 via a Ua interface.

The network application function 29 may be divided to an authorisation proxy function 25 and an application specific server 26. The network application function 29 is connected to the bootstrapping server function 28 via a Zn interface.

The bootstrapping server function 28 is connected to a home subscriber system HSS 27 via a Zh interface. The bootstrapping server function and the user equipment are arranged to mutually authenticate using the AKA (authentication and key agreement) protocol and agree on session keys that afterwards are applied between the user equipment and network application function. Once the bootstrapping procedure has been completed, the user equipment and the NAF can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between the user equipment and bootstrapping server function using the Ub interface. Generally, there will be no previous security association between the user equipment and the NAF. The NAF shall be able to locate and communicate securely with a subscriber's bootstrapping server function. The NAF shall be able to acquire shared key material or NAF specific key material derived from this shared key material that is established between the user equipment and the BSF during the bootstrapping procedure over Ub interface. The NAF is arranged to check the lifetime of the shared key material.

In addition to its normal function, the HSS stores parameters in the subscriber profile relating to the bootstrapping server function. Optionally, parameters relating to the usage of some NAF's are stored in the HSS.

The interfaces will be described in more detail. The Ua interface carries the application protocol which is secured using the key material or derived key material agreed

between the user equipment and the base station function as a result of the run of HTTP digest AKA over the Ub interface.

The Ub interface provides mutual authentication between the user equipment and the bootstrapping server function. It allows the user equipment to bootstrap the session keys based on the 3GPP AKA infrastructure.

The Zh interface protocol used between the BSF and HSS allows the BSF to fetch the required authentication information and subscriber profile information from the HSS. The interface to the 3G authentication centre is HSS internal.

The Zn interface is used by the NAF to fetch the key material or derived key material agreed during a previous HTTP digest AKA protocol run over the Ub interface from the BSF. It can also be used to fetch NAF specific subscriber profile information from the BSF.

In summary, in embodiments of the present invention, the NAF 29 sends the public identifier of the NAF to the bootstrapping server function 28. The bootstrapping server function shall verify the binding between the public and internal NAF identities. The public NAF identifier is used by the BSF to derive the NAF specific key (Ks_NAF) from master key material (Ks) established during bootstrapping procedure in the Ub interface. In particular, embodiments are the present invention are applicable where the network element that is hosting a NAF has one or more network

interfaces used for serving incoming connections from the user equipment. This is the public (or external) network interface and is via the Ua interface. One network interface is for connecting to operator services such as the BSF, that is the internal network interface which is via the Zn interface between the NAF 29 and BSF 28.

The address of the internal network interface in the Zn interface is added for example to the "origin-host" field by the NAF in the DIAMETER message. Embodiments of the present invention convey the external network interface address of the NAF, that is the public address to the BSF from the NAF. This can be done using an AVP (attribute value pair) to transport the information from the NAF 29 to the BSF. As mentioned previously, the external or public address is used by the BSF because the BSF derives the NAF specific key (Ks_NAF) from the fully qualified domain name (FQDN) of the NAF which the user equipment uses, that is the public address of the NAF. The BSF checks that the NAF identified by the internal address used in the Zn interface (NAF_id_Zn) is authorised to use the external address used in the Ua interface (NAF_id_Ua).

In embodiments of the invention, the NAF sends the NAF_Id_Ua in the first message, and receives confirmation (or error) message as response. The UID may or may not be transferred at the same time. The corresponding responses may thus only relate to the mapping of the public and internal NAF identifiers. In embodiments of the invention, both the public and internal NAF identifiers are sent to the BSF, the

BSF checks the mapping between them, and derives the NAF specific key using the public NAF identifier.

Reference is now made to figure 2 which shows a first signal flow in one embodiment of the present invention. Figure 2 shows messaging details between the NAF 29 and BSF 28 via the Zn interface. Before the Zn interface messaging takes place, the user equipment has requested a service from the NAF over the Ua interface. With this request, the user equipment has given a TID (transaction identifier) and possibly a user identifier UID. The user identifier can be transported from the user equipment to the NAF in later messages. Figure 2 describes the case where the TID and UID have been sent from the user equipment to the NAF in the same message.

In step 1a, the NAF 29 sends the TID, the NAF_id_UA and UID to the BSF 28. The BSF verifies the TID to UID mapping and the NAF_id_Zn to NAF_id_Ua mapping. The NAF_id_Ua can be obtained for example from the origin-host AVP. In other words, the BSF checks that the NAF identified by the internal address is authorised to use the external address. If these verifications are successful, the BSF derives the Ks_NAF using the NAF_id_UA.

In step 2a, the BSF sends the Ks_NAF and NAF specific user security settings "USS" to the NAF 29. In some embodiments of the present invention, the NAF may not have any USS and thus the USS AVP is optional. After receiving the Ks_NAF, the NAF can complete the authentication procedure and assume that the UID is correct. If the TID can not be found and

either the TID-to-UID or NAF_id_UA validation fails, the BSF shall return an error message to the NAF.

In the case where the NAF is authorised to verify multiple TID-to-UID mappings, it may send an additional request to the BSF in step 3a which contains the TID and another UID. Upon receiving the TID and UID, the BSF 28 shall verify the TID-to-UID mapping and return the result to the NAF 29. This takes place in step 4a. The BSF shall only do this if the NAF is authorised to verify multiple TID-to-UID mappings. In this case, the NAF may repeat steps 3a and 4a multiple times.

Reference is now to figure 3 which shows the case where the TID and UID have been received in different messages. For example, the TID is sent to the NAF for the UID.

In step 1b, the NAF 29 sends the TID and NAF_ID_Ua to the BSF. The BSF shall verify the NAF_id_Zn to NAF_id_Ua mapping. If this verification succeeds, the BSF derives the Ks_NAF using the NAF_id_Ua.

In step 2b, the BSF sends the Ks_NAF and the NAF specific USS to the NAF. Again, the NAF may not have USS and thus the USS AVP is optional. After receiving the Ks_NAF, the NAF 29 can complete the authentication procedure. If a TID can not be found or the NAF_id_Ua validation fails, the BSF 28 returns an error message to the NAF.

Before step 3b, the NAF has received a UID from the user equipment. In step 3b, the NAF sends a TID and UID for

verification. The BSF provides the result of this verification in step 4b. This procedure is the same as in messages 3a and 4a of Figure 2. In this case, the NAF is allowed to verify the TID-to-UID mapping in a separate message. During steps 1b and 2b no UID was verified. In the case where the NAF is authorised to verify multiple TID-to-UID mapping, it can send another request to the BSF in step 5b and get the results of the verification in step 6b. These steps correspond to steps 4a and 4b of figure 2. Steps 5b and 6b may be repeated a plurality of times.

An error message is sent from the BSF to the NAF if the TID is not found in the BSF database, if mapping of the NAF_id_Ua and NAF_id_Zn could not be verified or if mapping of TID and UID could not be verified.

Thus embodiments of the present invention allow the NAF to send the NAF identifier used by the user equipment over the UA interface to the BSF so that the BSF is able to derive the Ks_NAF.

Claims

1. A method for verifying a first identity and a second identity of an entity, said method comprising:

receiving first identity information at a checking entity;

sending second identity information from the entity to said checking entity;

verifying that the first and second identities both belong to said entity; and

generating a key using one of said first and second identity information.

2. A method as claimed in claim 1, wherein said generating step comprises generating a key from said second identity.

3. A method as claimed in any preceding claim, wherein one of said first and second identities comprises a public identity.

4. A method as claimed in any preceding claim, wherein one of said first and second identities comprises a private identity.

5. A method as claimed in any preceding claim, wherein said receiving step comprises receiving said first identity from user equipment.

6. A method as claimed in any preceding claim, wherein said receiving step comprises receiving a transaction identifier in a same message as the first identity.

7. A method as claimed in any of claims 1 to 5, wherein said receiving step comprises receiving a transaction identifier in a different message as the first identity.

8. A method as claimed in any preceding claim, wherein said key comprises an authentication key.

9. A method as claimed in any preceding claim, comprising the step of sending said key to said entity.

10. A method as claimed in any preceding claim, wherein said generating step is only performed if said verification step is successful.

11. A method as claimed in any preceding claim, wherein if said verification step is unsuccessful the step of sending an error message to the entity is performed.

12. A method as claimed in any preceding claim, comprising the step of verifying a transaction identity to user identifier mapping.

13. A method as claimed in claim 12, wherein a plurality of transaction identifiers are mapped to a user identifier and said verifying step is performed in turn for each transaction identifier to user identifier mapping.

14. A method as claimed in any preceding claim, wherein said entity comprises a network application function.

15. A method as claimed in any preceding claim, wherein said checking entity comprises a boot strapping function.

16. A method for verifying an external interface address and an internal interface address of a network application function, comprising the steps of:

receiving the internal interface address at a boot strapping function from user equipment;

receiving the external interface address at the boot strapping function from the network application function; and

verifying that the external interface address and the internal interface address belong to the same network application function.

17. A system comprising a checking entity arranged to receive a first identity of an entity at a checking entity; said entity arranged to send a second identity of the entity from the entity to said checking entity, said checking entity being arranged to verify that the first and second identities both belong to said entity and to generating a key from one of said first and second identities.

18. A checking entity arranged to receive a first identity of an entity and a second identity of the entity, said second entity identity being received from the entity, said checking entity being arranged to verify that the first and second identities both belong to said entity and to generating a key from one of said first and second identities.

19. An entity comprising a first and second identity, said entity arranged to send the second identity to a checking entity and to receive a key generated from said second identity from the checking entity.

FIG. 1

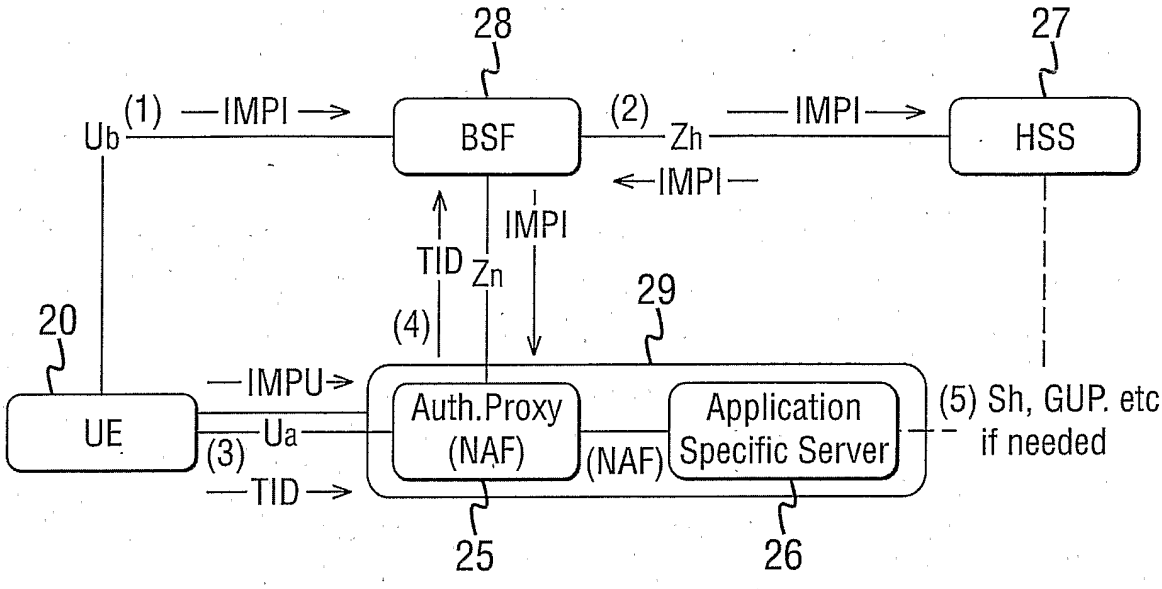


FIG. 2

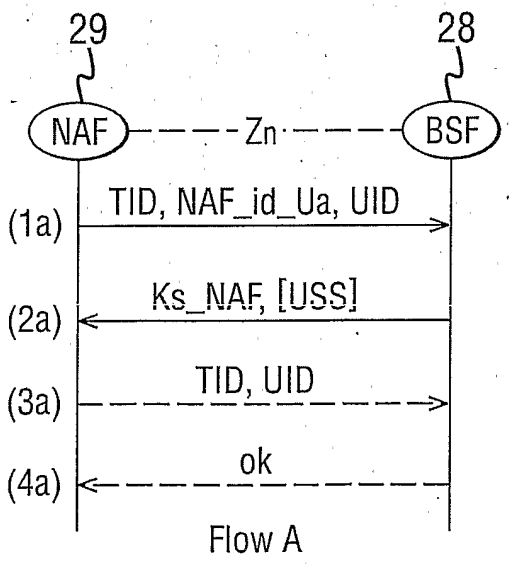
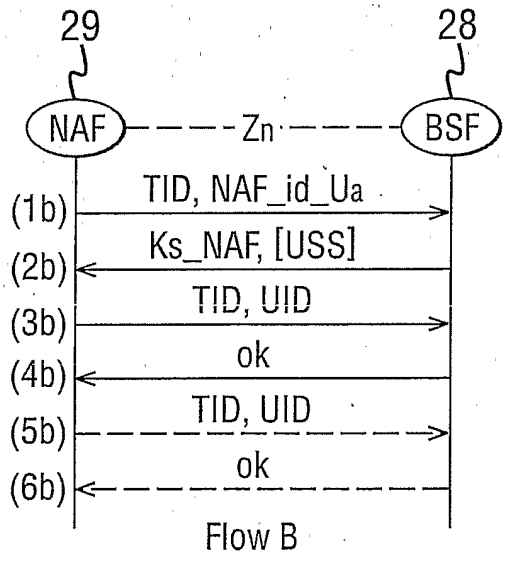


FIG. 3



INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/001704

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/56

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 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, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 365 620 A (SIEMENS AKTIENGESELLSCHAFT) 26 November 2003 (2003-11-26)	1-15, 17-19
A	paragraphs '0024! - '0031!	16
A	WO 03/081431 A (NOKIA CORPORATION; NOKIA INC) 2 October 2003 (2003-10-02) paragraphs '0003! - '0027!	1-19
A	WO 03/005669 A (TELEFONAKTIEBOLAGET LM ERICSSON ; SANCHEZ HERRERO, JUAN, ANTONIO; WALK) 16 January 2003 (2003-01-16) paragraphs '0037! - '0039! paragraph '0047! paragraphs '0050!, '0051!	1-19

-/--

[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
9 September 2005	15/09/2005

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	Olaechea, F

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/001704

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GARCIA D MILLS / NOKIA G MAYER F DEROME H SHIEH / MOTOROLA / BT / LUCENT J BHARATIA / NORTEL / HUTCHISON D WILLIS / DYNAMICSOFT M: "3GPP requirements on SIP" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 1, November 2001 (2001-11), XP015013488 ISSN: 0000-0004 the whole document	1-19
A	"3GPP TS 33.220 - 3RD GENERATION PARTNERSHIP PROJECT; TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS; GENERIC AUTHENTICATION ARCHITECTURE (GAA); GENERIC BOOTSTRAPPING ARCHITECTURE (RELEASE 6)" 3GPP TS 33.220 V6.0.0, XX, XX, March 2004 (2004-03), pages 1-18, XP002334596 the whole document	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2005/001704

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1365620	A	26-11-2003	DE	10223248 A1	04-12-2003
			EP	1365620 A1	26-11-2003
			US	2004153667 A1	05-08-2004
WO 03081431	A	02-10-2003	US	2003229787 A1	11-12-2003
			AU	2003209541 A1	08-10-2003
			WO	03081431 A1	02-10-2003
WO 03005669	A	16-01-2003	AT	286641 T	15-01-2005
			DE	60202527 D1	10-02-2005
			WO	03005669 A1	16-01-2003
			EP	1402705 A1	31-03-2004
			ES	2235065 T3	01-07-2005
			US	2005009520 A1	13-01-2005