

(43) International Publication Date
26 November 2009 (26.11.2009)(10) International Publication Number
WO 2009/141919 A1(51) International Patent Classification:
G06F 13/00 (2006.01)(21) International Application Number:
PCT/JP2008/059951(22) International Filing Date:
23 May 2008 (23.05.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **Telefon-aktiebolaget LM Ericsson (publ)** [SE/SE]; SE-164 83, Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MURAKAMI, Shingo** [JP/JP]; 1-22-5-201, Shinsaku, Takatsu-ku, Kawasaki-shi, Kanagawa, 2130014 (JP). **BARRIGA, Luis** [SE/SE]; Glidflyktsgatan 4BV, 128 33, SKARP-NÄCK (SE). **ODA, Toshikane** [JP/JP]; 3-8-19, Hiroo, Shibuya-ku, Tokyo, 1500012 (JP).(74) Agent: **OHTSUKA, Yasunori**; 7th FL., KIOICHO PARK BLDG., 3-6, KIOICHO, CHIYODA-KU, Tokyo, 1020094 (JP).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

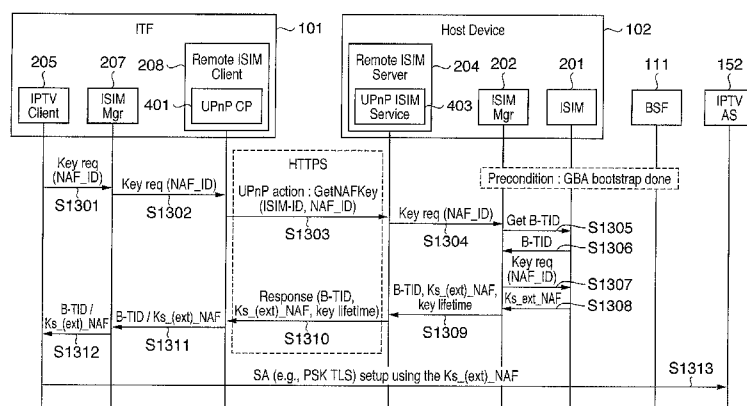
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report (Art. 21(3))

(54) Title: IMS USER EQUIPMENT, CONTROL METHOD THEREOF, HOST DEVICE, AND CONTROL METHOD THEREOF

FIG. 13



(57) Abstract: An IMS User Equipment (UE) is provided. The IMS UE comprises: searching means for searching, based on UPnP technology, a UPnP network for a host device that has IMS subscription information, establishing means for establishing a session with the host device discovered by the searching means, subscription retrieving means for retrieving, from the host device via the session, the IMS subscription information, registering means for registering with the IMS network using the IMS subscription information, key retrieving means for retrieving, from the host device via the session, a first encryption key shared with an IMS application server (AS) in an IMS network by sending identity of the IMS AS to the host device via the session, and communicating means for performing encrypted communication with the IMS AS using the first encryption key.

DESCRIPTION

IMS USER EQUIPMENT, CONTROL METHOD THEREOF, HOST
DEVICE, AND CONTROL METHOD THEREOF

TECHNICAL FIELD

[0001] The present invention generally relates to an IP Multimedia Subsystem (IMS) User Equipment (UE), a method for controlling the IMS UE, a host device, and a method for controlling the host device. The present invention particularly relates, but is not limited to, a technology that enables the IMS UE to utilize IMS subscription information managed by another device such as the host device.

BACKGROUND

[0002] A network architecture called "IP Multimedia Subsystem" (IMS) has been developed by the 3rd Generation Partnership Project (3GPP) as an open standard for handling multimedia services and sessions in the packet domain.

[0003] An IMS Subscriber Identity Module (ISIM) application, or alternatively a Universal Subscriber Identity Module (USIM), stored in a Universal Integrated Circuit Card (UICC) is indispensable to an IMS UE because it contains subscription information that is necessary for the IMS UE to access an IMS

network and receive various IMS-based services. The subscription information includes, for example, user identity information such as an IMS Private User Identity (IMPI) and an IMS Public User Identity (IMPU), credentials, and so on.

[0004] Taking an IPTV system as an example, any IPTV Terminal Function (ITF), such as a Set Top Box (STB) or TV-set, is required to be authenticated by the IMS network and IPTV system with an ISIM in order to receive IPTV services.

[0005] However, not all IMS UEs are necessarily equipped with a UICC. An IMS UE without a UICC must obtain subscription information by some other means in order to access the IMS network. Moreover, it is sometimes desirable even for an IMS UE with a UICC to externally obtain subscription information because the user of the IMS UE may be different from the owner of its UICC. Therefore, a technology for remote ISIM access, that is, a technology that enables the IMS UE to utilize the ISIM of another device, is required.

[0006] As of today, several prior art references are known which provide mechanisms, use cases, or service requirements for remote SIM/ISIM access technology as follows:

[0007] - The 3rd Generation Partnership Project (3GPP) TSG SA WG3 discussed several different models and scenarios where IMS access capabilities are split

into two entities, a device like a PC connected to a fixed IP network and a UMTS UE with a UICC. For example, IMS functionality on a PC and ISIM (or USIM) stored in the UICC of the UMTS UE are linked through some interface so that the PC and the UMTS UE can cooperatively act as an IMS UE with the UICC.

[0008] - A feasibility study was conducted in 3GPP TR 33.817 that presents issues, security threats, potential requirements and the like in an environment where a SIM application is re-used by peripheral devices such as laptop computers or PDAs to be authenticated to mobile operators so that the peripheral devices can access 3GPP and WLAN networks that the mobile operators provide.

[0009] - The Fixed Mobile Convergence Alliance (FMCA) gives the service requirements for a SIM Access and Authentication service where a SIM in a mobile handset is being used as an authentication token on other user devices for the fixed-mobile convergence environment defined by the FMCA.

[0010] - A Bluetooth SIM Access Profile provides a means to allow devices such as car phones with built in GSM transceivers to connect to a SIM card in a phone with Bluetooth, so the car phone itself doesn't require a separate SIM card.

[0011] <Problems with existing solutions>

In order to realize remote ISIM access, some

mechanism in the local environment is eventually required to dynamically discover an available ISIM (or USIM) application and to pair up the discovered ISIM application with the IMS UE. However, none of the prior art references offer a complete and detailed solution for providing such mechanisms.

[0012] The Bluetooth SIM Access Profile could be one solution for realizing remote ISIM access; however, it is difficult to mandate that all home user devices be equipped with Bluetooth adapters given the lack of availability of Bluetooth-equipped user devices in the present market relative to Ethernet or WLAN.

[0013] Moreover, none of the prior art references provide a specific technology to efficiently realize encrypted communication between the IMS UE and an IMS AS when the IMS UE utilizes subscription information maintained by another device.

SUMMARY

[0014] The present invention is intended to address the above-described problem, and it is a feature thereof to introduce a new technology that enables an IMS UE to utilize subscription information maintained by another device. This is achieved by the equipment, methods, and device according to the appended independent claims, and by the embodiments according to the dependent claims.

[0015] According to a first aspect of the present invention there is provided an IMS User Equipment (UE). The IMS UE comprises: searching means for searching, based on UPnP technology, a UPnP network for a host device that has IMS subscription information, establishing means for establishing a session with the host device discovered by the searching means, subscription retrieving means for retrieving, from the host device via the session, the IMS subscription information, registering means for registering with the IMS network using the IMS subscription information, key retrieving means for retrieving, from the host device via the session, a first encryption key shared with an IMS application server (AS) in an IMS network by sending identity of the IMS AS to the host device via the session, and communicating means for performing encrypted communication with the IMS AS using the first encryption key.

[0016] In some embodiments, the communicating means receives, from the IMS AS, content encrypted by use of a second encryption key and the second encryption key encrypted by use of the first encryption key, and the IMS UE further comprises: key decrypting means for decrypting the encrypted second encryption key by use of the first encryption key, and content decrypting means for decrypting the encrypted content by use of the second encryption key. The second

encryption key may be MBMS Traffic Key (MTK).

[0017] In some embodiments, the establishing means receives identity of a key server from the host device, receives a third encryption key shared with the host device from the key server, and encrypts the session by use of the third encryption key. The third key may be `Ks_local_device`.

[0018] According to a second aspect of the present invention there is provided a method for controlling an IMS User Equipment (UE). The method comprises: searching, based on UPnP technology, a UPnP network for a host device that has IMS subscription information, establishing a session with the host device discovered in the step of searching, retrieving, from the host device via the session, the IMS subscription information, registering with the IMS network using the IMS subscription information, retrieving, from the host device via the session, a first encryption key shared with an IMS application server (AS) in an IMS network by sending identity of the IMS AS to the host device via the session, and performing encrypted communication with the IMS AS using the first encryption key.

[0019] In some embodiments, the step of performing receives, from the IMS AS, content encrypted by use of a second encryption key and the second encryption key encrypted by use of the first encryption key, and the method further comprises: decrypting the encrypted

second encryption key by use of the first encryption key, and decrypting the encrypted content by use of the second encryption key. The second encryption key may be MBMS Traffic Key (MTK).

[0020] In some embodiments, the step of establishing receives identity of a key server from the host device, receives a third encryption key shared with the host device from the key server, and encrypts the session by use of the third encryption key. The third key may be Ks_local_device.

[0021] According to a third aspect of the present invention there is provided a host device. The host device comprises: establishing means for establishing a session with an IMS User Equipment (UE) based on UPnP technology, subscription retrieving means for retrieving IMS subscription information from a memory, subscription sending means for sending the IMS subscription information to the IMS UE via the session, key retrieving means for retrieving a first encryption key shared with an IMS application server (AS) in an IMS network based on identity of the IMS AS received from the IMS UE via the session, and key sending means for sending the first encryption key to the IMS UE via the session.

[0022] In some embodiments, the key retrieving means comprises: bootstrapping means for creating a master key shared with a Bootstrapping Server Function

(BSF), and calculating means for calculating the first encryption key based on the master key and the identity of the IMS AS. The master key may be Ks.

[0023] In some embodiments, the establishing means sends identity of a key server to the IMS UE, calculates a second encryption key shared with the IMS UE based on the identity of the key server, and encrypts the session by use of the second encryption key. The second key may be Ks_local_device.

[0024] According to a fourth aspect of the present invention there is provided a method for controlling a host device. The method comprises: establishing a session with an IMS User Equipment (UE) based on UPnP technology, retrieving IMS subscription information from a memory, sending the IMS subscription information to the IMS UE via the session, retrieving a first encryption key shared with an IMS application server (AS) in an IMS network based on identity of the IMS AS received from the IMS UE via the session, and sending the first encryption key to the IMS UE via the session.

[0025] In some embodiments, the step of retrieving the first encryption key comprises: creating a master key shared with a Bootstrapping Server Function (BSF), and calculating the first encryption key based on the master key and the identity of the IMS AS. The master key may be Ks.

[0026] In some embodiments, the step of

establishing sends identity of a key server to the IMS UE, calculates a second encryption key shared with the IMS UE based on the identity of the key server, and encrypts the session by use of the second encryption key. The second key may be Ks_local_device.

[0027] The main advantage of the present invention is as follows. The user is relieved from the burden of inserting their own UICC into the IMS UE because the IMS UE can dynamically discover an available host device that has IMS subscription information (in other words, an available host device that has an ISIM or USIM application) in the UPnP network, and receive IMS-based services by use of the IMS subscription information managed by the host device. Moreover, the present invention is useful in that the IMS UE can efficiently obtain the encryption key used for encrypted communication in connection with the IMS-based services.

[0028] Further features of the present invention will become apparent from the following description of exemplary embodiments with reference to the attached drawings, in which like reference characters designate the same or similar parts throughout the figures thereof.

BRIEF DESCRIPTION OF DRAWINGS

[0029] Fig. 1 shows an overview of the present

invention;

[0030] Fig. 2 is a schematic block diagram illustrating configurations of the IPTV Terminal Function (ITF) and the host device according to the embodiments of the present invention;

[0031] Fig. 3 schematically shows a Universal Integrated Circuit Card (UICC) that stores a plurality of IP Multimedia Subsystem (IMS) Subscribe Identity Modules (ISIMs);

[0032] Fig. 4 shows detailed configurations of the remote ISIM client and the remote ISIM server, and the procedures whereby the remote ISIM client discovers the remote ISIM server according to the embodiments of the present invention;

[0033] Fig. 5 shows the procedures whereby the remote ISIM client receives the ISIM lists from the discovered remote ISIM servers according to the embodiments of the present invention;

[0034] Fig. 6 shows an example of the ISIM list and a screen for ISIM selection;

[0035] Fig. 7 shows the flow of the HTTP Digest-based authentication between the UPnP Control Point (CP) and the UPnP ISIM service according to the embodiments of the present invention;

[0036] Fig. 8 shows an overview of the device authentication and the key establishment according to the embodiments of the present invention;

[0037] Fig. 9 schematically shows the device authentication and key establishment mechanisms between the remote ISIM client and the remote ISIM server according to the embodiments of the present invention;

[0038] Fig. 10 shows the procedures whereby the remote ISIM client establishes a secure association (SA) with the remote ISIM server according to the embodiments of the present invention;

[0039] Fig. 11 shows a selection screen with which the user selects the user ISIM profile according to the embodiments of the present invention;

[0040] Fig. 12 shows the procedures whereby the ITF performs an IMS registration with an IMS network according to the embodiments of the present invention;

[0041] Fig. 13 shows the procedures whereby the IPTV client retrieves Ks_(ext)_NAF from the hosting device according to the embodiments of the present invention; and

[0042] Fig. 14 shows the procedures whereby the IPTV client retrieves the encrypted MTK so that it can decrypt the content according to the embodiments of the present invention.

DETAILED DESCRIPTION

[0043] Embodiments of the present invention will now be described with reference to the attached drawings. Each embodiment described below will be

helpful in understanding a variety of concepts from the generic to the more specific.

[0044] It should be noted that the technical scope of the present invention is defined by claims, and is not limited by each embodiment described below. In addition, not all combinations of the features described in the embodiments are necessarily required for realizing the present invention.

[0045] In the following description, an IPTV service, an ITF, and an IPTV AS are employed in an example of an IMS-based service, an IMS UE, and an IMS AS. However, the present invention can be applied for any kind of IMS-based services and corresponding IMS UEs and IMS ASs. Moreover, although an ISIM is described as a source of IMS subscription information, the present invention can be applied for the case where a USIM is used instead of the ISIM.

[0046] Fig. 1 shows an overview of the present invention. A home network 100 is a communication network based on a UPnP technology. The home network 100 comprises an ITF 101 and a host device 102 that is equipped with a UICC 103. Although it is assumed that ISIM (or USIM) is implemented in the UICC 103 that is physically inserted to the host device, such identity modules may be implemented in another form. For example, an ISIM (or USIM) may be realized as a remotely managed software object that is downloadable

via network to a trusted execution environment of the host device 102, or it may be implemented in an embedded chip (also called Industrial Form Factor) within the host device 102, also possibly remotely managed.

[0047] An IMS network 150 comprises a call session control function (CSCF) 151 and an IPTV AS 152 that is a kind of a network application function (NAF). The IMS network 150 also comprises a Home Subscriber Server (HSS) (not shown). There is also a bootstrapping server function (BSF) 111 that can be accessed from the host device.

[0048] Because the ITF 101 is equipped with IMS functionality, it can make direct communication with IMS network 150 via the standard Gm and Ua interfaces as long as it has IMS subscription information such as an IMPI and IMPU. However, in the present embodiment, the ITF 101 does not have a UICC, or it does have a UICC but shall not use its own UICC for some reason. Accordingly, the ITF 101 retrieves the IMS subscription information maintained in the UICC 103 from the host device 102.

[0049] The host device 102 may be any kind of devices as long as it can provide the ITF 101 with IMS subscription information. For example, the host device 102 may be a dedicated server, a mobile phone, a Home IMS Gateway (HIGA) as disclosed in WO 2006/045706, or

the like. The host device 102 may even be an ITF which itself accesses the CSCF 151 and the IPTV AS 152.

[0050] Fig. 2 is a schematic block diagram illustrating configurations of the ITF 101 and the host device 102. Note that each block in the ITF 101 and the host device 102 may be implemented using dedicated hardware, software executed by a processor (not shown) or a combination thereof.

[0051] The host device 102 comprises an ISIM 201, which is stored in the UICC 103 (not shown in Fig. 2). In the present embodiment, it is assumed that the UICC 103 stores a plurality of ISIMs 201 as shown in Fig. 3, and each ISIM 201 includes one IMPI and one or more IMPUs. This is advantageous because each user can possess one's own ISIM and protect it with one's own Personal Identification Number (PIN). Moreover, each user can individually register with the IMS network by use of one's own ISIM. However, it should be noted that all users might share a single ISIM.

[0052] The host device 102 also comprises an ISIM manager 202 that includes a Generic Bootstrapping Architecture (GBA) client 203, and a remote ISIM server 204.

[0053] It should be noted that the present embodiment can be applied for both the case where the ISIM 201 supports GBA_U and the case where the ISIM 201 does not support GBA_U but the GBA client 203 supports

GBA_ME. GBA_U is a GBA with UICC-based enhancement where the GBA-specific functions are split between the Mobile Equipment (ME) and the UICC. In GBA_U, a master key (Ks) remains in the UICC while only Ks_ext_NAF generated in the UICC is delivered to the ME. On the other hand, in GBA_ME, all GBA-specific functions are carried out in the ME. The UICC is GBA-unaware, that is, a master key (Ks) is delivered to the ME and a NAF-specific key (Ks_NAF) is generated from the Ks in the ME. Note that "Ks_(ext)_NAF" represents Ks_ext_NAF in the context of GBA_U, and Ks_NAF in the context of GBA_ME.

[0054] The ITF 101 comprises an IPTV client 205, an IMS middleware 206, an ISIM manager 207 that includes a GBA client 211, and a remote ISIM client 208. Although the ITF 101 may have an ISIM 209, the ITF 101 does not use it in the present embodiment. A display 210, which displays various kinds of information, is connected to the ITF 101.

[0055] One role of the ISIM 201 is to generate IMS Authentication and Key Agreement (AKA) credentials (i.e., RES, Ck, and Ik). The IMS middleware 206 performs an IMS registration with the IMS AKA credentials over a Gm interface.

[0056] Another role of the ISIM 201 is NAF key derivation. The IPTV client 205 communicates with the IPTV AS 152 over a Ua interface which are made secure

with the encryption key "Ks_(ext)_NAF" derived from a master key (i.e., Ks). Ks is shared by the host device 102 and the BSF 111 as a result of the bootstrapping procedures performed by the GBA client 203.

[0057] The Ua interface is actually secured by Ks_(ext)_NAF using HTTP Digest authentication with server-certificate-based TLS or Ks_(ext)_NAF-based TLS (i.e., Pre-Shared Key TLS defined in RFC 4279) and so on.

[0058] The ISIM manager 202 is equipped with an API that enables access to the ISIM 201. It is not necessary for the ISIM 201 to support GBA_U because the ISIM manager 202 includes a GBA client 203 that supports a Ub interface and GBA_ME.

[0059] The remote ISIM server 204 and the remote ISIM client cooperatively allow the ITF 101 to perform remote ISIM access. More specifically, the ISIM manager 207 and the GBA client 211 have similar functionality to that of the ISIM manager 202 and the GBA client 203 respectively. When the ITF 101 is required to access an ISIM, the ISIM manager 207 accesses the ISIM 201 by way of the remote ISIM client 208 and the remote ISIM server 204.

[0060] Since the remote ISIM client 208 is placed behind the ISIM manager 207, it is hidden from all the functions of the ITF 101 including the IPTV client 205 and the IMS middleware 206. This enables transparent

ISIM access from their perspective, that is, the IPTV client 205 and the IMS middleware 206 need not be aware of whether the ITF 101 is accessing a local ISIM 209 or a remote ISIM 201.

[0061] In the present embodiment, for the following reason, the GBA client 203 but not the GBA client 211 performs the bootstrapping procedures over the Ub interface. If the GBA client 211 runs its Ub interface with support from the remote ISIM 201, information exchange between the ITF 101 and the host device 102 gets complicated. On the other hand, if the GBA client 203 runs a Ub interface, no information need be exchanged between the ITF 101 and the host device 102 for the purpose of the bootstrapping procedures. Moreover, if the host device 102 is also an IMS UE such as an ITF, it needs to keep track of Ks/Bootstrap Transaction Identifier (B-TID) updates which should be also available for local Ua applications residing in the host device 102. In this case, if the host device 102 runs a Ub interface and manages Ks/B-TID by itself, the complexity of information exchange is reduced.

[0062] However, it should be noted that the GBA client 211 might perform the bootstrapping procedures over its own Ub interface.

[0063] Referring to Figs. 4-6, procedures (hereinafter referred to as "discovery process") are described where the ITF 101 finds one or more host

devices 102 and selects an ISIM (more precisely, one of the IMPUs of the ISIM) maintained by the discovered host device(s) 102 to receive a specific IMS-based service.

[0064] As shown in Fig. 4, the remote ISIM client 208 comprises a UPnP control point (CP) 401, and the remote ISIM server 204 comprises a UPnP root device 402 that includes a UPnP ISIM service 403, which is a kind of a UPnP service. Since the remote ISIM server 204 has access to the ISIM manager 202, the UPnP ISIM service 403 can indirectly expose the ISIM 201 via UPnP scheme.

[0065] In order to obtain the IMS subscription information, the remote ISIM client 208 of the ITF 101 searches the home network 100, which is the UPnP network, for the remote ISIM server 204 of the host device 102 as follows. Note that there may be more than one host device 102 in the home network 100, and in this case, more than one remote ISIM server 204 may be discovered.

[0066] In steps S401-S406, the UPnP CP 401 performs the standard UPnP discovery procedure. The service type to discover is set to a defined service identifier in the form of Uniform Resource Name (URN) for the UPnP ISIM service 403.

[0067] In the present embodiment, a UPnP action "Get ISIM List ()" is defined and exposed by the UPnP

ISIM service 403 so that the user can see available ISIM applications behind the remote ISIM server 204. As shown in Fig. 5, the UPnP CP 401 sends this action request to all discovered UPnP ISIM services 403 (steps S501 and S503), and, in response, receives a list (ISIM list) of ISIMs maintained by respective host devices 102 (steps S502 and S504).

[0068] An example of the ISIM list is text data encoded by XML as shown in Fig. 6. Each ISIM instance in the ISIM list is identifiable by a persistent identity (ISIM-ID) (e.g., a hash value of IMPI and all IMPUs) assigned by the UPnP ISIM service 403. The ISIM list contains at least one IMPU and its associated service name(s) such as Push to talk over Cellular (PoC), IPTV, and the like. Originally, the ISIM application itself does not contain any information about services associated with each IMPU; however, it is useful to include such service name information in the ISIM list because doing so allows the user to correctly select a specific IMPU associated with the desired service subscription.

[0069] For this purpose, the host device 102 according to the present embodiment supports the following mechanism: the ISIM manager 202 downloads service profiles in advance per ISIM from HSS. This download can be performed via the standard Ut interface. The service profile contains information

regarding which IMPU is associated with which IMS-based service, which allows the ISIM manager 202 to create mapping information per ISIM that maintains which IMPU is associated with which service. Based on this information, the remote ISIM server 204 creates the ISIM list containing a service name associated with each IMPU as shown in Fig. 6.

[0070] The ITF shows the content of the ISIM list on the display 210 as shown in Fig. 6. In this case, the service name associated with the IMPU serves as a hint for the user to select their desired IMPU. The user selects an ISIM from the ISIM list and further selects an IMPU within the selected ISIM (if the ISIM contains more than one IMPU). The ITF 101 registers with the IMS network 150 using the selected IMS subscription information (i.e., the selected IMPU, the IMPI of the selected ISIM, and so on).

[0071] Referring to Figs. 7-10, procedures (hereinafter referred to as "paring process") are described where the remote ISIM client 208 establishes a secure association (SA) with the remote ISIM server 204.

[0072] Once the user selects an ISIM from the ISIM list, the remote ISIM client 208 first verifies if the user can be authenticated to use the selected ISIM. The user authentication is based on PIN as an ISIM supports a built-in PIN-based user authentication.

[0073] In order to implement a protocol to support the PIN-based authentication, a UPnP action request "Paring ()" is defined. This action request is accompanied with an ISIM-ID as an argument, which is obtained from the ISIM list. The action request and response messages carry relevant HTTP Digest header fields so that the PIN-based authentication is performed based on HTTP Digest. HTTP Digest-based authentication can be performed because the UPnP technology is an HTTP-based technology. Fig. 7 shows the flow of the HTTP Digest-based authentication.

[0074] In step S701, the UPnP CP 401 sends the UPnP action request "Paring (ISIM-ID, Device_ID)" to the UPnP ISIM service 403. In the present embodiment, the UPnP action request contains the Device_ID in addition to the ISIM-ID. The Device_ID is used for key establishment (described later in detail with reference to Fig. 10).

[0075] In step S702, the UPnP ISIM service 403 returns a 401 Unauthorized response that includes a challenge to the UPnP CP 401. After receiving the 401 Unauthorized response, the UPnP CP 401 prompts the user to input the PIN of the selected ISIM 201 via, for example, the display 210, and receives the input PIN.

[0076] In step S703, the UPnP CP sends the UPnP action request "Paring (ISIM-ID, Device_ID)" to the UPnP ISIM service 403 again, but this time it includes

a response derived from the PIN.

[0077] In step S704, the UPnP ISIM service 403 verifies the response and returns a 200 OK response, which indicates successful user authentication, to the UPnP CP 401. The 200 OK response includes B-TID and NAF_ID, which are used for key establishment (described later in detail with reference to Fig. 10).

[0078] After successful user authentication, device authentication and key establishment are performed as shown in Fig. 8.

[0079] In step S801, the remote ISIM server 204 verifies that the remote ISIM client 208 is "trusted", and vice versa.

[0080] In step S802, the remote ISIM client 208 and the remote ISIM server 204 establishes an encryption key between them. After that, a secure transmission channel (e.g., a Transport Layer Security (TLS) session) is set up between them using the established key. Therefore, according to the present embodiment, successful pairing results in establishment of a TLS session between the remote ISIM client 208 and the remote ISIM server 204.

[0081] According to the present embodiment, the remote ISIM client 208 and the remote ISIM server 204 perform the device authentication and key establishment based on a mechanism defined by 3GPP. Using this mechanism, a shared secret key (called

"Ks_local_device") is established between the remote ISIM client 208 and the remote ISIM server 204. Then, the remote ISIM client 208 and the remote ISIM server 204 establish the TLS session using the established Ks_local_device.

[0082] Overview of the device authentication and key establishment mechanisms are described with reference to Fig. 9.

[0083] After the PIN-based user authentication using HTTP Digest (see Fig. 7), the remote ISIM client 208 establishes an HTTPS session to a NAF Key Centre 901. In this case, the remote ISIM client 208 is authenticated to the NAF Key Centre 901 with its device certificate. Then, the remote ISIM client 208 receives Ks_local_device, which is shared with the host device 102, from the NAF Key Centre 901. In this sense, the NAF Key Centre 901 is virtually acting as an operator's authentication center to verify that the IMS UE such as the ITF 101 is trusted. This mechanism also brings the following benefits for the operator:

[0084] - Dynamic device authorization is possible. In other words, with the NAF Key Centre 901, the operator can determine which IMS UE is authorized to perform the remote ISIM access to which remote ISIM (i.e., ISIM maintained by the host device) based on its policies.

[0085] - Tracking and logging of all the remote

ISIM access is possible for the operator, which facilitates, for example, charging of the user.

[0086] As described above, the remote ISIM client 208 is authenticated to the NAF Key Centre 901 with its device certificate. On the other hand, the remote ISIM client 208 can authenticate the remote ISIM server 204 during the TLS handshake based on the established `Ks_local_device` because the remote ISIM server 204 can generate that shared secret (i.e., `Ks_local_device`) only when it is legitimate. Accordingly, the remote ISIM server 204 does not need to have a device certificate in order for the remote ISIM client 208 to authenticate the remote ISIM server 204.

[0087] Fig. 10 shows the flow of the pairing process. As described above, the pairing process starts when the UPnP CP 401 sends the UPnP action request "Pairing ()" to the UPnP ISIM service 403. The action request contains the ISIM-ID and a `Device_ID` of the remote ISIM client 208. A `Device_ID` is required by the remote ISIM server 204 in order to derive a `Ks_local_device` as described in connection with step S1009.

[0088] After step S703, in step S1001, the remote ISIM server 204 requests a B-TID from the ISIM manager 202.

[0089] In steps S1002-S1003, the ISIM manager 202 retrieves the B-TID from the ISIM 201. In the case of

GBA_ME, these steps are not necessary because the ISIM manager 202 maintains the B-TID.

[0090] In step S1004, the ISIM manager 202 returns the B-TID to the remote ISIM server 204.

[0091] In step S704, the UPnP ISIM service 403 returns a 200 OK response to the remote ISIM client 208. The response includes the B-TID together with the NAF_ID of the NAF Key Centre 901. Note that the NAF_ID may be configured in the remote ISIM server 204 in advance.

[0092] In steps S1005-S1008, the remote ISIM server 204 retrieves Ks_(ext)_NAF from the ISIM manager 202. Note that in steps S1006-S1007, the ISIM manager 202 retrieves Ks_ext_NAF from the ISIM 201 in the case of GBA_U, whereas the ISIM manager 202 retrieves the Ck and Ik from the ISIM 201 and calculates Ks_NAF in the case of GBA_ME.

[0093] In step S1009, the remote ISIM server 204 derives Ks_local_device based on the B-TID, the NAF_ID, Ks_(ext)_NAF, and Device_ID.

[0094] In steps S1010-S1013, as described with reference to Fig. 8, the remote ISIM client 208 establishes an HTTPS session with the NAF Key Centre 901 using its device certificate, and retrieves Ks_local_device from the NAF Key Centre 901.

[0095] Finally, in step S1014, the remote ISIM client 208 establishes a Pre-Shared Key (PSK) TLS

session with the remote ISIM server 204 using a pre-shared encryption key (i.e., Ks_local_device), and the paring process completes.

[0096] In some embodiments, the ITF 101 may create a "user ISIM profile" after the user authentication (see steps S701-S704 of Fig. 10). With the user ISIM profile, the ITF 101 can omit the discovery process and a part of the paring process the next time it accesses the target remote ISIM. The user ISIM profile may be created and maintained by the remote ISIM client 208 after the procedure of step S704 (not shown).

[0097] The user can name the user ISIM profile a user-friendly name such as "Alice" or "Bob". Using the user-friendly name, the user can easily choose one's user ISIM profile out of many profiles maintained by the remote ISIM client 208.

[0098] The user ISIM profile contains:

- The Control URL of the UPnP ISIM service 403
- The ISIM-ID
- The PIN code

[0099] In the course of the user ISIM profile creation, the remote ISIM client 208 may prompt the user to set a password for the user ISIM profile in order to prevent misuse of the user ISIM profile by another person. Alternatively, a user may select another option whereby the PIN code for the target remote ISIM is not contained within the user ISIM

profile. In this case, the user is required to input the PIN every time the pairing process is performed.

[0100] In the case that the user ISIM profile has been created by the remote ISIM client 208, when the user wishes to access the IMS network 150 by use of the ITF 101, the user selects their ISIM profile via a selection screen such as one shown in Fig. 11.

[0101] Since the PIN is contained in the user ISIM profile, it is not necessary for the user to input the PIN between steps S702 and S703 of Fig. 10. In step S703, the remote ISIM client 208 retrieves the PIN from the user ISIM profile, derives the response based on the extracted PIN, and sends an action request that includes the response to the remote ISIM server 204.

[0102] In some embodiments, a UPnP request action "User Authentication ()" may be implemented in the UPnP CP 401 and the UPnP ISIM service 403. "User Authentication ()" is different from "Pairing ()" in that the UPnP CP 401 and the UPnP ISIM service 403 do not initiate the pairing process; they only perform user authentication for the purpose of the creation of the user ISIM profile. In this case, the remote ISIM server 204 does not perform the procedures of steps S1001-S1004 in Fig. 10. After step S704, the remote ISIM client 208 creates the user ISIM profile, and terminates the flow of Fig. 10.

[0103] Referring to Fig. 12, procedures

(hereinafter referred to as "registration process") are described where the ITF 101 performs an IMS registration with the IMS network 150. The registration process is performed after the successful pairing (see step S1014 of Fig. 10).

[0104] According to the present embodiment, two UPnP action requests named "Get IMS Registration Info ()" and "AKA Request ()" are defined. The action requests and responses are protected by the TLS session established in step S1014.

[0105] In steps S1201-S1203, the UPnP CP 401 sends "Get IMS Registration Info (ISIM-ID)" to the UPnP ISIM service 403. The remote ISIM server retrieves, from the ISIM 201 by way of the ISIM manager 202, IMS subscription information necessary for the ITF 101 to send an initial SIP Register request, which includes IMPPI, IMPU, P-CSCF address, Home Domain URI, and the like. Then, the UPnP ISIM service 403 returns the IMS subscription information to the UPnP CP 401. If more than one IMPU is returned from the UPnP ISIM service 403, the user is required to select one IMPU to be registered before the next step. Alternatively, if one of the IMPUs has already been selected via the screen shown in Fig. 6, the flow may proceed to the next step without user selection.

[0106] In steps S1204-S1205, the IMS middleware 206 sends an initial SIP Register request to the CSCF

151 using the SIP subscription information. It then receives a 401 Unauthorized response including a random challenge (RAND) and a network authentication token (AUTN) from the CSCF 151.

[0107] In steps S1206-S1207, the UPnP CP 401 invokes an "AKA Request ()" action with arguments: the RAND and AUTN. The remote ISIM server 204 inputs the RAND and AUTN to the ISIM 201 via the ISIM manager 202 to obtain RES, Ck, and Ik, which are eventually sent back to the UPnP CP 401.

[0108] In steps S1208-S1209, the IMS middleware 206 establishes an IPsec channel toward the CSCF 151 using the Ck and Ik, and re-sends a SIP Register request containing the RES to the CSCF 151, which results in successful IMS registration.

[0109] According to the present embodiment, before the IPTV client 205 starts receiving content from the IPTV AS 152, it retrieves a Ks_(ext)_NAF from the hosting device 102 in order to perform encrypted communication with the IPTV AS 152.

[0110] Fig. 13 shows procedures whereby the IPTV client 205 retrieves Ks_(ext)_NAF from the hosting device 102. For this purpose, an UPnP action request "Get NAF Key ()" is defined.

[0111] In steps S1301-S1302, the IPTV client 205 sends a key request that includes NAF_ID of the target IMS AS (i.e., the IPTV AS 152) to the remote ISIM

client 208 by way of the ISIM manager 207.

[0112] In step S1303, the UPnP CP 401 sends the action request "Get NAF Key ()" containing the ISIM-ID and the NAF_ID to the UPnP ISIM service 403.

[0113] In steps S1304-S1309, the remote ISIM server 204 retrieves B-TID and Ks_(ext)_NAF from the ISIM manager 202 and the ISIM 201. Note that Fig. 13 depicts the case of GBA_U. In the case of GBA_ME, steps S1305-S1306 are not necessary because the ISIM manager 202 maintains the B-TID. Moreover, in steps S1307-S1308, the ISIM manager 202 retrieves Ck and Ik instead of Ks_ext_NAF from the ISIM 201, and calculates Ks_NAF based on the Ck and Ik.

[0114] In step S1310, the UPnP ISIM service 403 returns the B-TID, Ks_(ext)_NAF, and its lifetime to the UPnP CP 401. Note that the communication in steps S1303 and S1310 is performed via the TLS session established as a result of the paring process (see Fig. 10).

[0115] In steps S1311-S1312, the IPTV client 205 receives the B-TID and Ks_(ext)_NAF from the remote ISIM client 208 by way of the ISIM manager 207 as a response to the request of step S1301.

[0116] In step S1313, the IPTV client 205 sets up a security association (e.g., PSK TLS session) with the IPTV AS 152 using Ks_(ext)_NAF, thereby performing the encrypted communication with the IPTV AS 152. The IPTV

AS 152 obtains the $Ks_(\text{ext})_NAF$ by sending to BSF 111 a key material request containing B-TID received from the IPTV client 205 during negotiating the security association and the NAF_ID . When the BSF 111 receives the key material request, the BSF 111 generates the $Ks_(\text{ext})_NAF$ and returns it to the IPTV AS 152.

[0117] In some embodiments, the IPTV AS 152 may implement a smartcard-based service protection such as one known from 3GPP TS 33.246 V7.2.0. Although the terminology defined in 3GPP MBMS (3GPP TS 33.246 V7.2.0) is used here for explanatory purposes, the embodiments are not limited to 3GPP MBMS.

[0118] More specifically, the IPTV AS 152 first authenticates the IPTV client 205 with the MBMS Request Key (MRK) while the IPTV client 205 registers to the IPTV AS 152. After successful registration, the IPTV AS 152 encrypts content using an MBMS Traffic Key (MTK), encrypts the MTK using an MBMS Service Key (MSK), and encrypts the MSK using $Ks_(\text{ext})_NAF$, which corresponds to an MBMS User Key (MUK). Then, the IPTV AS 152 sends the encrypted content to the IPTV client 205. The IPTV AS 152 distributes the encrypted MTK by embedding it into a Multimedia Internet Keying (MIKEY) message while the encrypted content is sent to the IPTV client 205 and also distributes the encrypted MSK using a MIKEY message to the IPTV client 205 after the IPTV client 205 has requested for the MSK or when the IPTV

AS 152 decides that it is time to update the MSK.

[0119] Fig. 14 shows procedures whereby the IPTV client 205 retrieves the encrypted MTK so that it can decrypt the content. For this purpose, the ISIM manager 207 has an IPTV Key Manager (KM) 1401 as shown in Fig. 14. The IPTV KM 1401 is an entity similar to the MGW-S/F as defined in 3GPP TS 33.246 V7.2.0, thus a person skilled in the art will understand how to implement the IPTV KM 1401 with reference to the description below.

[0120] In steps S1401-S1402, the IPTV client 205 sends a MRK request message to the IPTV KM 1401 by way of the ISIM manager 207.

[0121] In step S1403, the IPTV KM 1401 sends a key request including the NAF_ID of the target IMS AS (i.e., the IPTV AS 152) to the remote ISIM client 208.

[0122] Then, the UPnP CP 401 retrieves the B-TID, Ks_(ext)_NAF, and its lifetime from the UPnP ISIM service 403 in the same manner as described in steps S1303-S1310 of Fig. 13.

[0123] In step S1404, the remote ISIM client 208 returns Ks_(ext)_NAF and its lifetime to the IPTV KM 1401.

[0124] In step S1405, the IPTV KM 1401 regards Ks_(ext)_NAF as the MUK, and derives the MRK from Ks_(ext)_NAF.

[0125] In steps S1406-S1407, the IPTV KM 1401

sends the MRK to the IPTV client 205 by way of the ISIM manager 207.

[0126] In step S1408, the IPTV client 205 registers to the IPTV AS 152 in which the IPTV client 205 is authenticated to the IPTV AS 152 with the MRK.

[0127] After the registration in step S1408, in steps S1409-S1418, the IPTV client 205 periodically receives the MSK update message and the MTK update message. The IPTV client 205 sends the MSK update message and the MTK update message to the IPTV KM 1401. The IPTV KM 1401 obtains the MSK by decrypting the MSK update message using $Ks_{(ext)}_{NAF}$, obtains the MTK by decrypting the MTK update message using the MSK, and sends the MTK to the IPTV client 205.

[0128] Consequently, in step S1419, the IPTV client 205 can decrypt the encrypted content from the IPTV AS 152 using the MTK.

[0129] As described above, according to 3GPP MBMS, various keys are used to enhance the service protection. However, what is important is that the IPTV AS 152 encrypts the content using a given encryption key, which is also encrypted and sent to the IPTV client 205 together with the encrypted content, and the IPTV client 205 can decrypt the given encryption key if the IPTV KM 1401 has $Ks_{(ext)}_{NAF}$. Accordingly, it should be understood that a person skilled in the art should be able to modify (typically,

simplify) the procedures of Fig. 14 without departing from the concept of service protection.

[0130] <Advantages of the Invention>

The present invention is advantageous in that the user is relieved from the burden of inserting their own UICC into the IMS UE because the IMS UE can dynamically discover an available host device that has IMS subscription information (in other words, an available host device that has ISIM or USIM application) in the UPnP network, and receive IMS-based services by use of the IMS subscription information maintained by the host device. Moreover, it is not necessary for the IMS UE to be equipped with a UICC slot, thus the complexity and cost of the IMS UE can be reduced.

[0131] Moreover, the present invention is useful in that the IMS UE can efficiently obtain the encryption key (e.g., $Ks_{(ext)}_{NAF}$) used for encrypted communication in connection with the IMS-based services.

[0132] While the present invention has been described with reference to exemplary embodiments, it is to be understood that the invention is not limited to the disclosed exemplary embodiments. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

CLAIMS

1. An IMS User Equipment (UE) (101), comprising:
 - searching means (401) for searching, based on UPnP technology, a UPnP network for a host device that has IMS subscription information;
 - establishing means (208, 401) for establishing a session with the host device discovered by the searching means;
 - subscription retrieving means (401) for retrieving, from the host device via the session, the IMS subscription information;
 - registering means (206) for registering with the IMS network using the IMS subscription information;
 - key retrieving means (401) for retrieving, from the host device via the session, a first encryption key shared with an IMS application server (AS) in an IMS network by sending identity of the IMS AS to the host device via the session; and
 - communicating means (205) for performing encrypted communication with the IMS AS using the first encryption key.
2. The IMS UE according to claim 1, wherein the communicating means receives, from the IMS AS, content encrypted by use of a second encryption key and the second encryption key encrypted by use of the first

encryption key,

further comprising:

key decrypting means (1401) for decrypting the encrypted second encryption key by use of the first encryption key; and

content decrypting means (205) for decrypting the encrypted content by use of the second encryption key.

3. The IMS UE according to claim 1 or 2, wherein the establishing means:

receives identity of a key server (901) from the host device;

receives a third encryption key shared with the host device from the key server; and

encrypts the session by use of the third encryption key.

4. The IMS UE according to any one of claims 1-3, wherein:

the searching means receives list information that indicates every set of IMS subscription information maintained by the discovered host device; and

the subscription retrieving means retrieves IMS subscription information selected by a user out of the every set of IMS subscription information.

5. The IMS UE according to claim 4, wherein the list information includes a service profile specifying an IMS-based service associated with the IMS subscription information.

6. The IMS UE according to any one of claims 1-5, wherein the IMS subscription information is maintained in a USIM or ISIM application (201) of the host device.

7. The IMS UE according to any one of claims 1-6, wherein the IMS AS is an IPTV AS (152).

8. The IMS UE according to any one of claims 1-7, wherein the first encryption key is $Ks_{(ext)}_{NAF}$.

9. A method for controlling an IMS User Equipment (UE) (101), comprising:

searching (S401-S406), based on UPnP technology, a UPnP network for a host device that has IMS subscription information;

establishing (S1014) a session with the host device discovered in the step of searching;

retrieving (S1201, S1203), from the host device via the session, the IMS subscription information;

registering (S1204, S1208) with the IMS network using the IMS subscription information;

retrieving (S1303, S1310), from the host device

via the session, a first encryption key shared with an IMS application server (AS) in an IMS network by sending identity of the IMS AS to the host device via the session; and

performing (S1313) encrypted communication with the IMS AS using the first encryption key.

10. The method according to claim 9, wherein the step of performing receives, from the IMS AS, content encrypted by use of a second encryption key and the second encryption key encrypted by use of the first encryption key,

further comprising:

decrypting (S1416-S1417) the encrypted second encryption key by use of the first encryption key; and

decrypting (S1419) the encrypted content by use of the second encryption key.

11. The method according to claim 9 or 10, wherein the step of establishing:

receives identity of a key server (901) from the host device;

receives a third encryption key shared with the host device from the key server; and

encrypts the session by use of the third encryption key.

12. The method according to any one of claims 9-11, wherein:

the step of searching receives list information that indicates every set of IMS subscription information maintained by the discovered host device; and

the step of retrieving the IMS subscription information retrieves IMS subscription information selected by a user out of the every set of IMS subscription information.

13. The method according to claim 12, wherein the list information includes a service profile specifying an IMS-based service associated with the IMS subscription information.

14. The method according to any one of claims 9-13, wherein the IMS subscription information is maintained in a USIM or ISIM application (201) of the host device.

15. The method according to any one of claims 9-14, wherein the IMS AS is an IPTV AS (152).

16. The method according to any one of claims 9-15, wherein the first encryption key is $Ks_{(ext)}_{NAF}$.

17. A host device (102), comprising:

establishing means (403) for establishing a session with an IMS User Equipment (UE) based on UPnP technology;

subscription retrieving means (202) for retrieving IMS subscription information from a memory (103);

subscription sending means (403) for sending the IMS subscription information to the IMS UE via the session;

key retrieving means (202) for retrieving a first encryption key shared with an IMS application server (AS) in an IMS network based on identity of the IMS AS received from the IMS UE via the session; and

key sending means (403) for sending the first encryption key to the IMS UE via the session.

18. The host device according to claim 17, wherein the key retrieving means comprises:

bootstrapping means (203) for creating a master key shared with a Bootstrapping Server Function (BSF); and

calculating means (202) for calculating the first encryption key based on the master key and the identity of the IMS AS.

19. The host device according to claim 17, wherein the key retrieving means comprises:

bootstrapping means (203) for creating a master key in the memory, the master key being shared with a Bootstrapping Server Function (BSF); and

obtaining means (202) for obtaining the first encryption key calculated by an application module in the memory based on the master key and the identity of the IMS AS.

20. The host device according to any one of claims 17-19, wherein the establishing means:

sends identity of a key server (901) to the IMS UE;

calculates a second encryption key shared with the IMS UE based on the identity of the key server; and

encrypts the session by use of the second encryption key.

21. The host device according to any one of claims 17-20, further comprising:

creating means (204) for creating list information that indicates every set of IMS subscription information maintained in the memory; and

list sending means (403) for sending the list information to the IMS UE,

wherein the subscription retrieving means retrieves IMS subscription information specified by the IMS UE.

22. The host device according to claim 21, further comprising receiving means (202) for receiving a service profile specifying an IMS-based service associated with the IMS subscription information, wherein the creating means includes the service profile in the list information.

23. The host device according to any one of claims 17-22, wherein the IMS subscription information is maintained in a USIM or ISIM application (201) stored in the memory.

24. The host device according to any one of claims 17-23, wherein the IMS AS is an IPTV AS (152).

25. The host device according to any one of claims 17-24, wherein the first encryption key is $Ks_{(ext)}_{NAF}$.

26. A method for controlling a host device (102), comprising:

 establishing (S1014) a session with an IMS User Equipment (UE) based on UPnP technology;

 retrieving (S1202) IMS subscription information from a memory (103);

 sending (S1203) the IMS subscription information

to the IMS UE via the session;

retrieving (S1304-S1309) a first encryption key shared with an IMS application server (AS) in an IMS network based on identity of the IMS AS received from the IMS UE via the session; and

sending (S1310) the first encryption key to the IMS UE via the session.

27. The method according to claim 26, wherein the step of retrieving the first encryption key comprises:

creating a master key shared with a Bootstrapping Server Function (BSF); and

calculating the first encryption key based on the master key and the identity of the IMS AS.

28. The method according to claim 26, wherein the step of retrieving the first encryption key comprises:

creating a master key in the memory, the master key being shared with a Bootstrapping Server Function (BSF); and

obtaining (S1308) the first encryption key calculated by an application module in the memory based on the master key and the identity of the IMS AS.

29. The method according to any one of claims 26-28, wherein the step of establishing:

sends identity of a key server (901) to the IMS

UE;

calculates a second encryption key shared with the IMS UE based on the identity of the key server; and encrypts the session by use of the second encryption key.

30. The method according to any one of claims 26-29, further comprising:

creating list information that indicates every set of IMS subscription information maintained in the memory; and

sending (S502, S504) the list information to the IMS UE,

wherein the step of retrieving the IMS subscription retrieves IMS subscription information specified by the IMS UE.

31. The method according to claim 30, further comprising receiving a service profile specifying an IMS-based service associated with the IMS subscription information,

wherein the step of creating the list information includes the service profile in the list information.

32. The method according to any one of claims 26-31, wherein the IMS subscription information is maintained in a USIM or ISIM application (201) stored in the

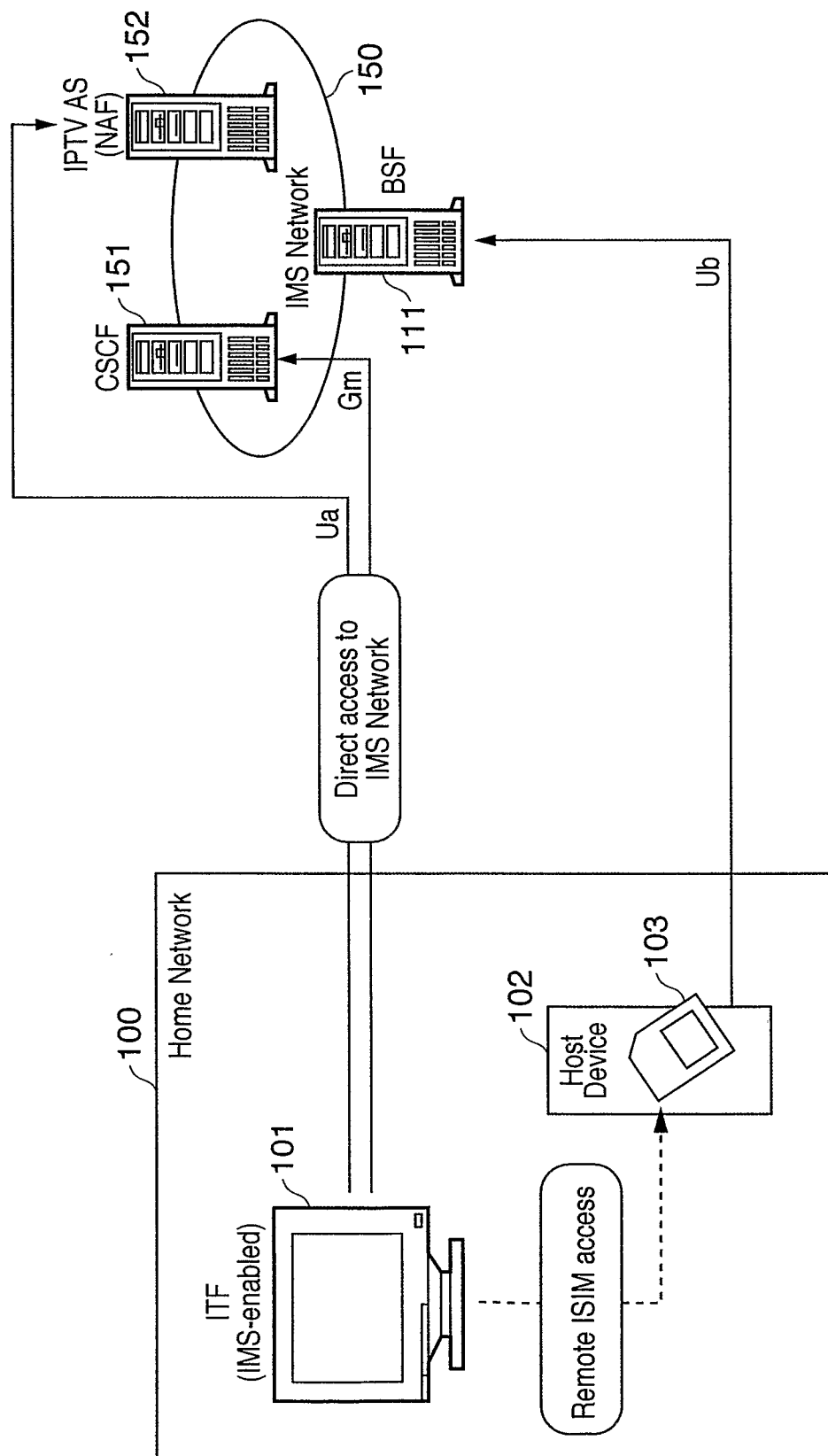
memory.

33. The method according to any one of claims 26-32, wherein the IMS AS is an IPTV AS (152).

34. The method according to any one of claims 26-33, wherein the first encryption key is Ks_(ext)_NAF.

1/14

FIG. 1



2/14

FIG. 2

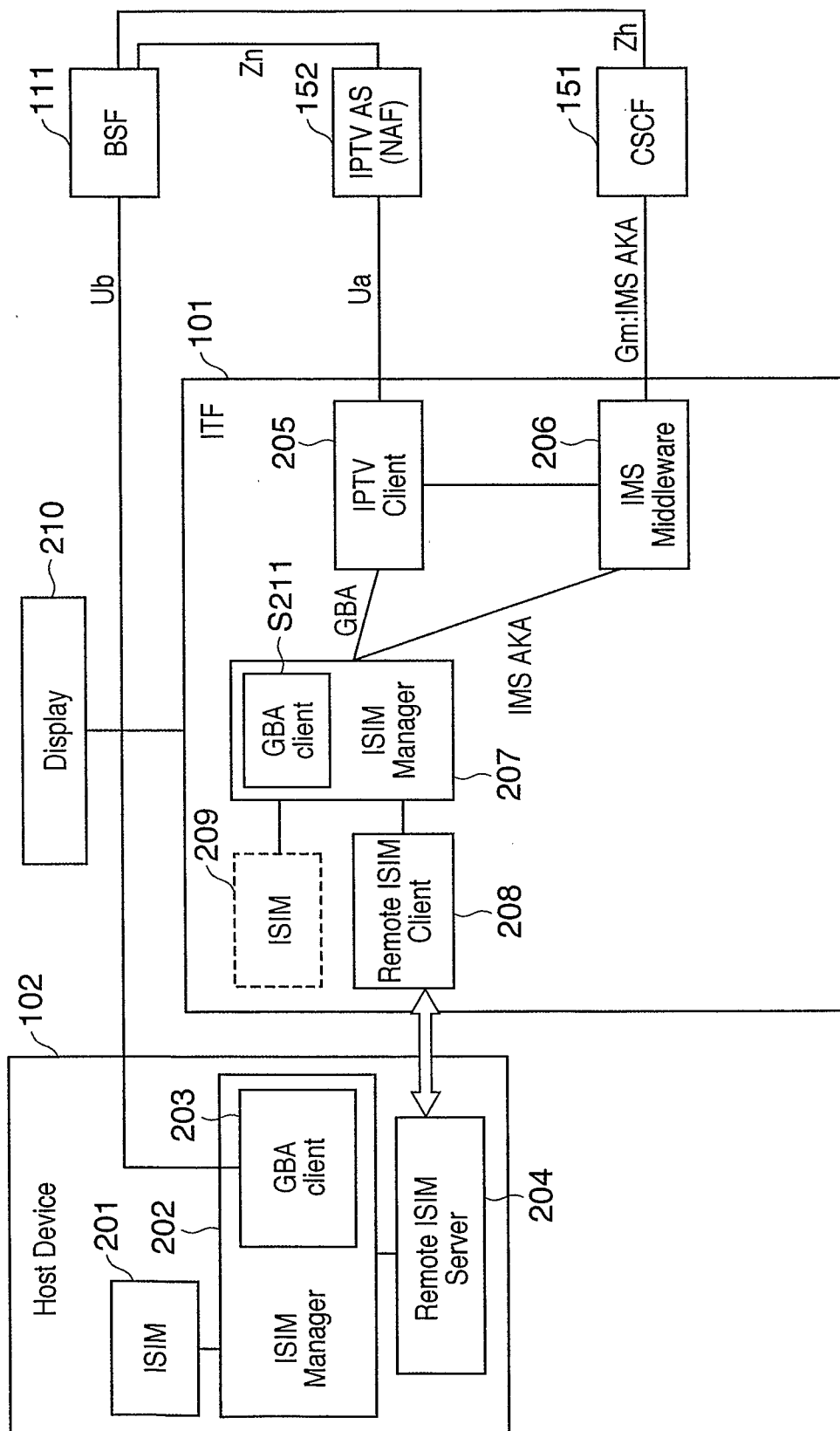


FIG. 3

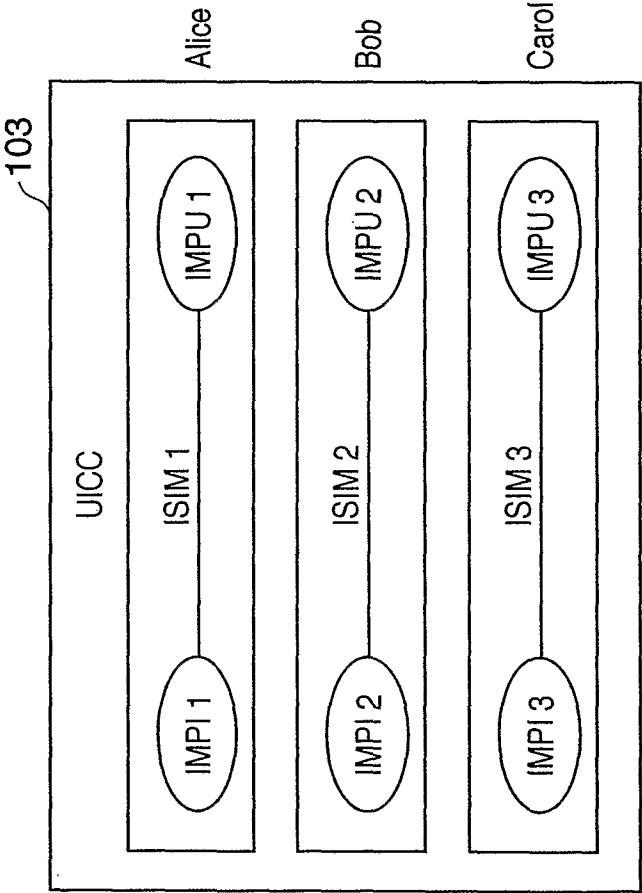


FIG. 4

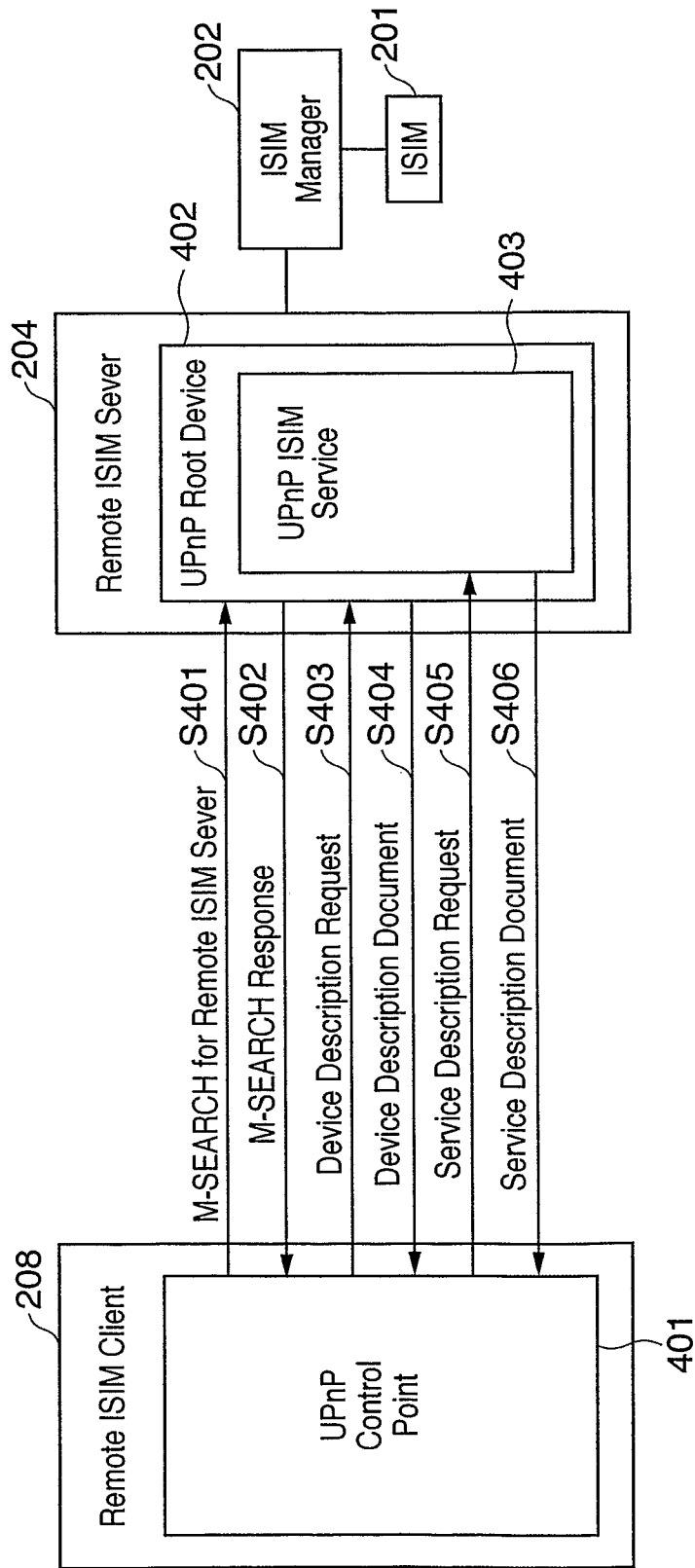
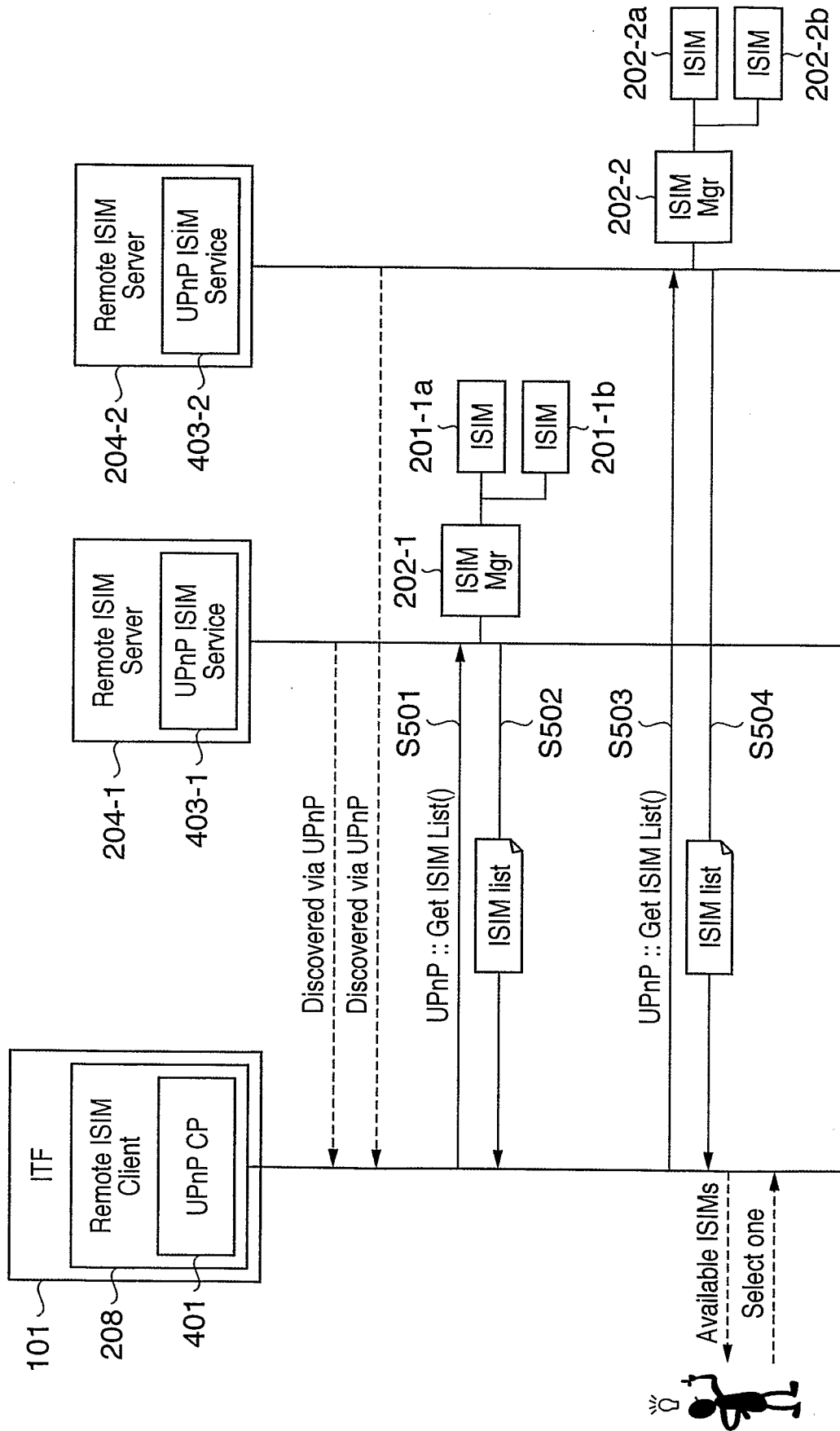


FIG. 5



6/14

FIG. 6

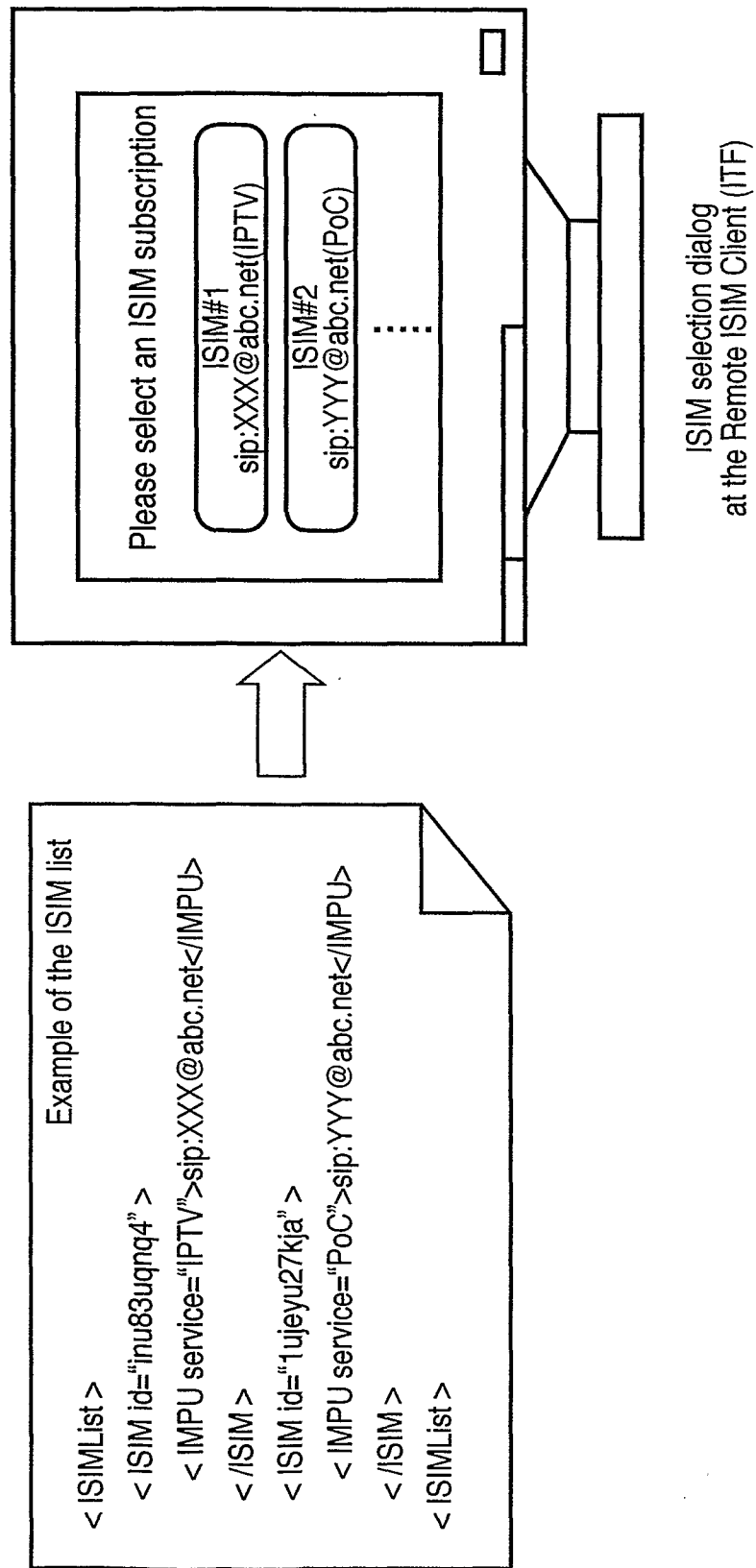
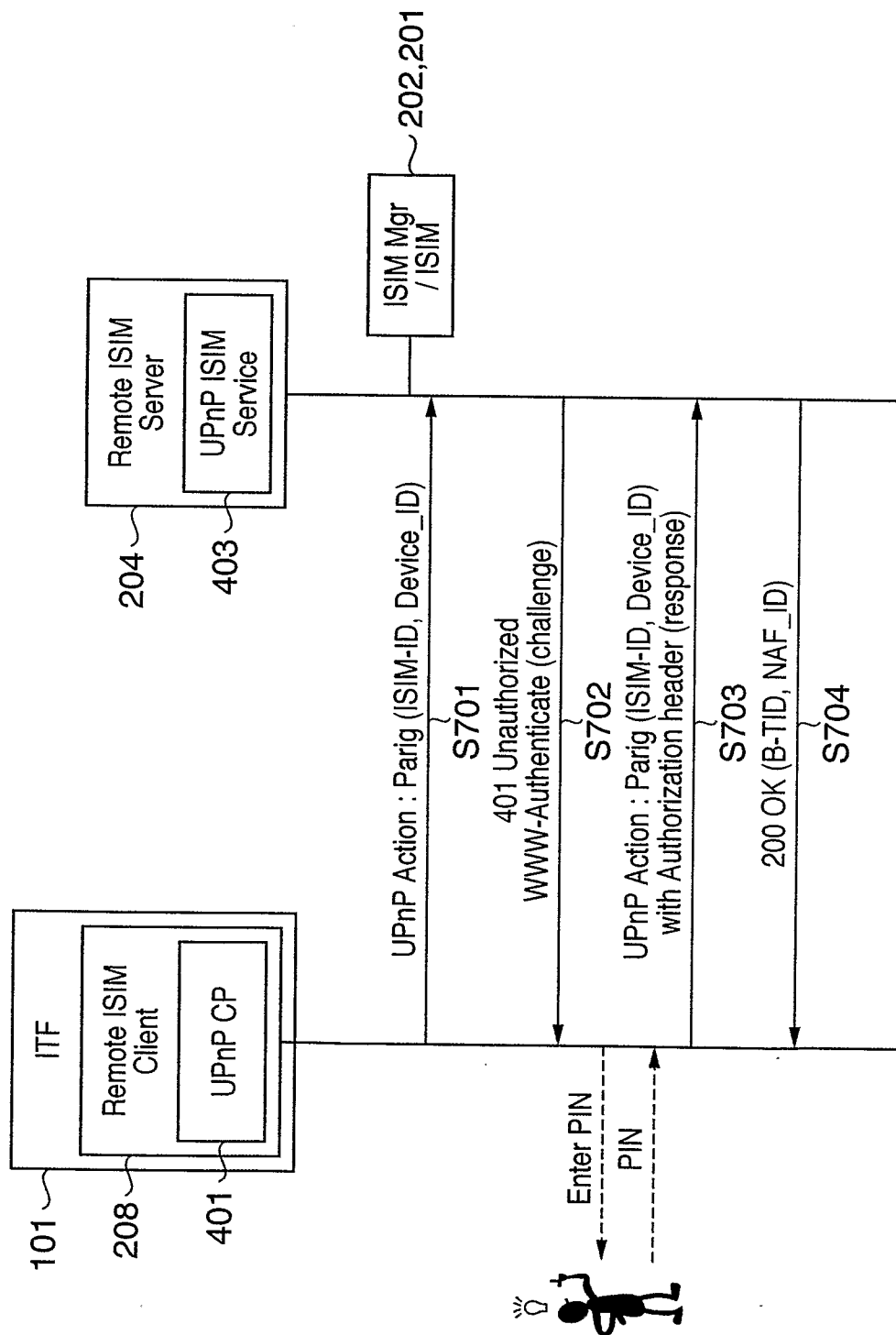
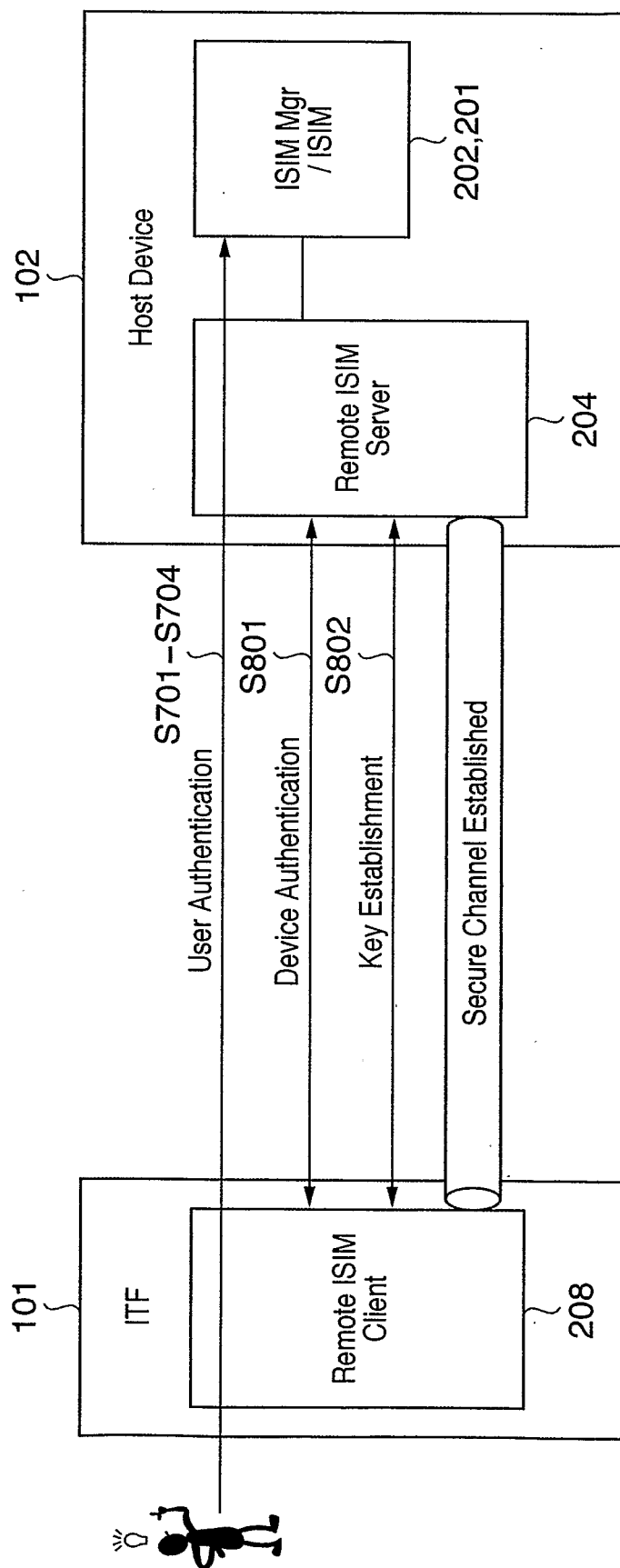


FIG. 7



8/14

FIG. 8



9/14

FIG. 9

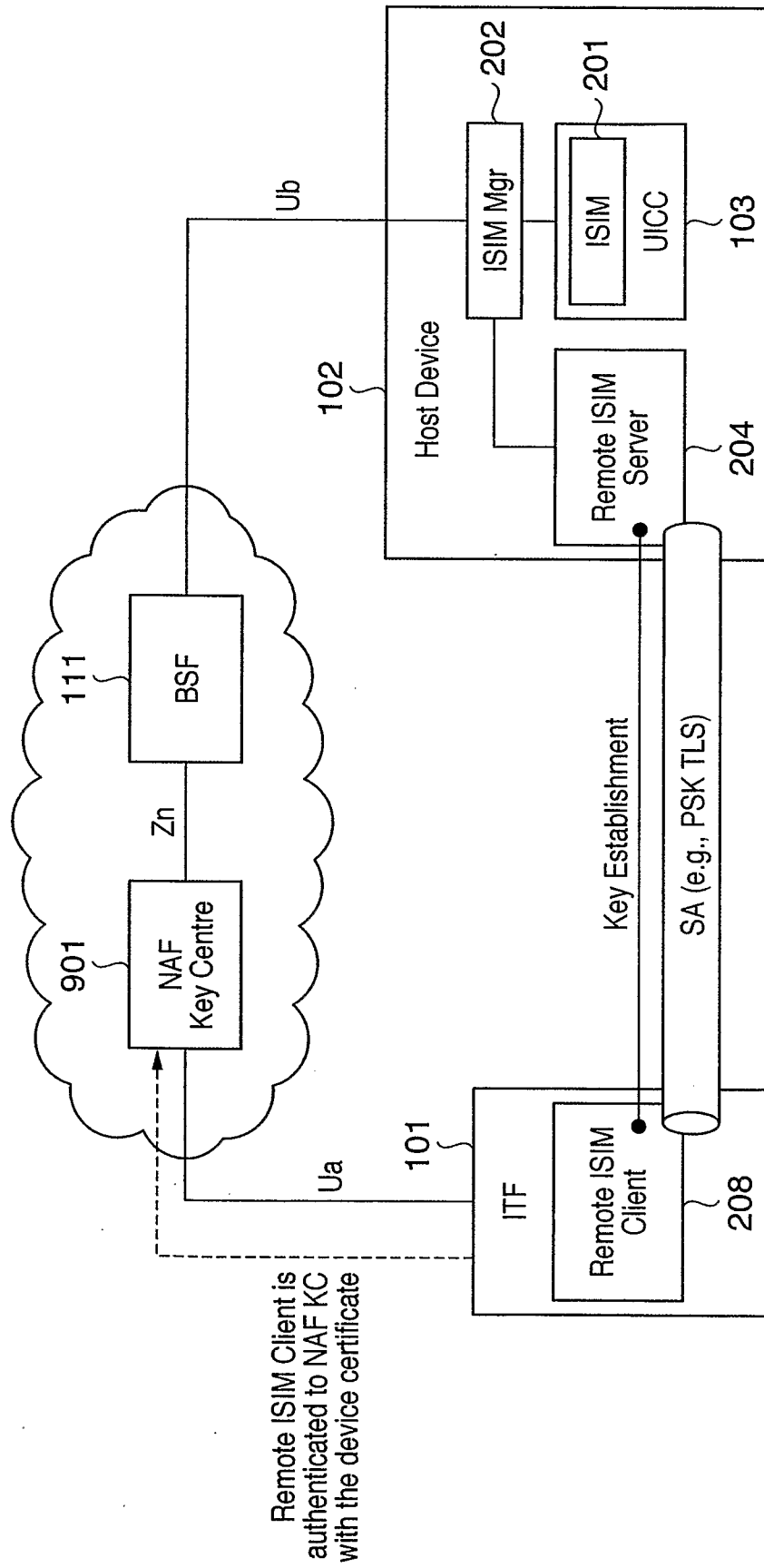
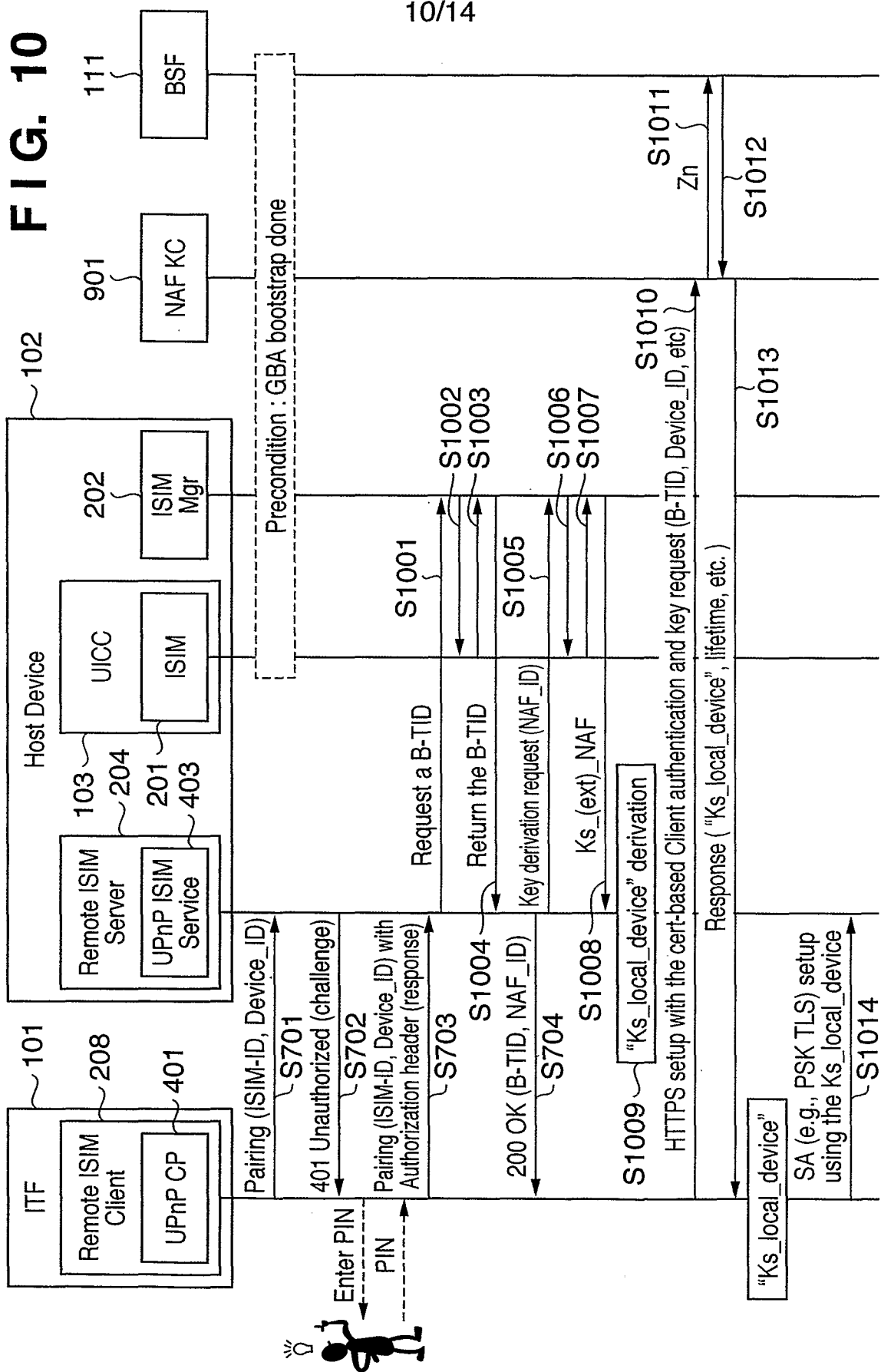


FIG. 10



11/14

FIG. 11

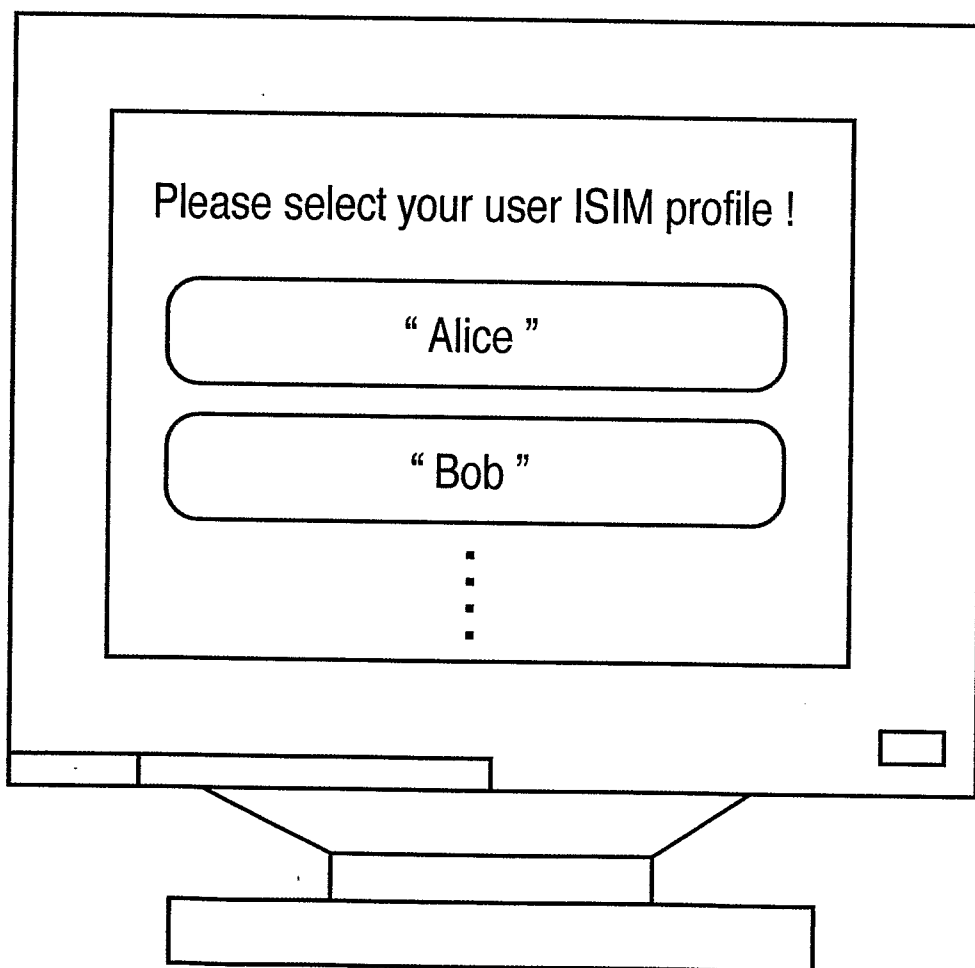


FIG. 12

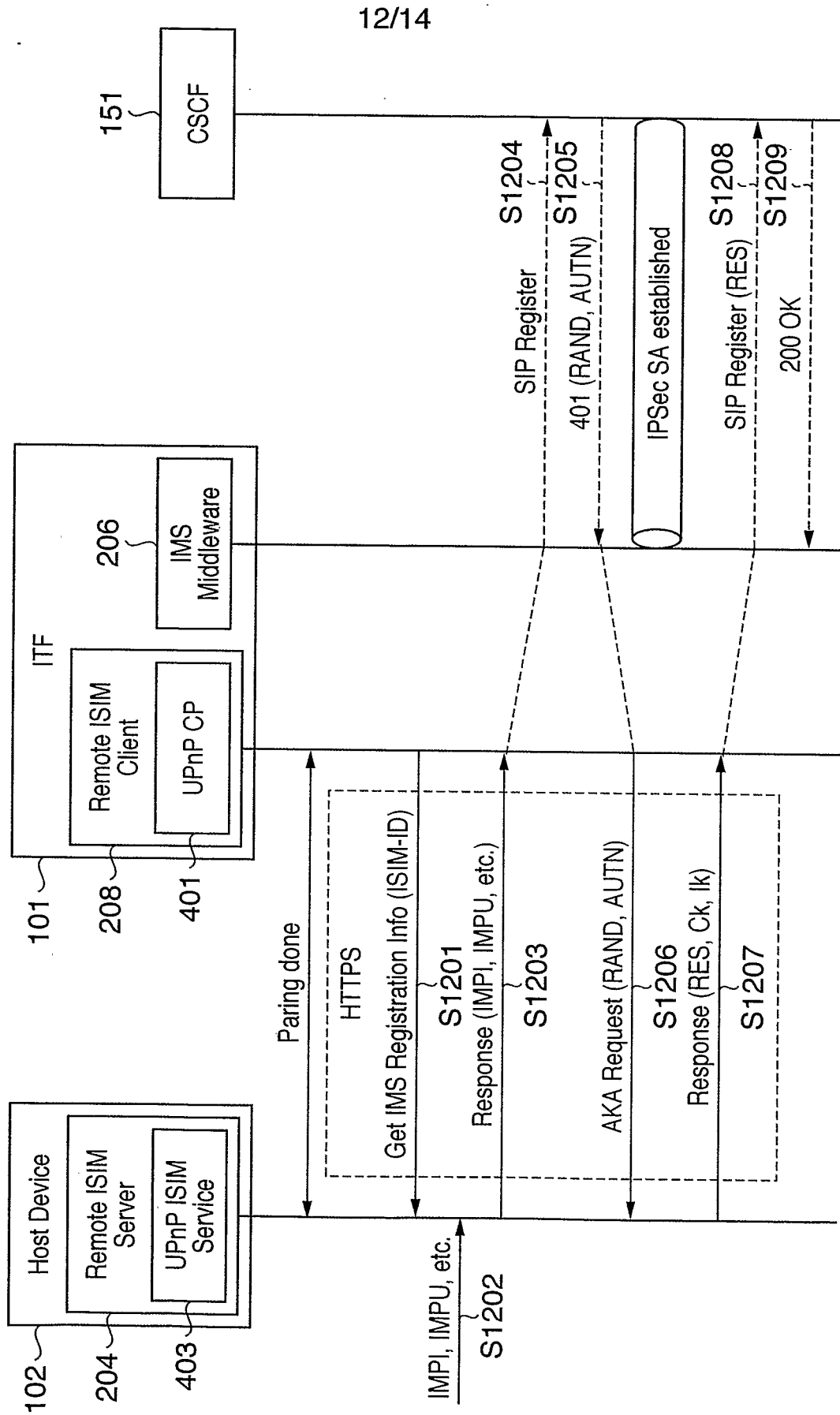
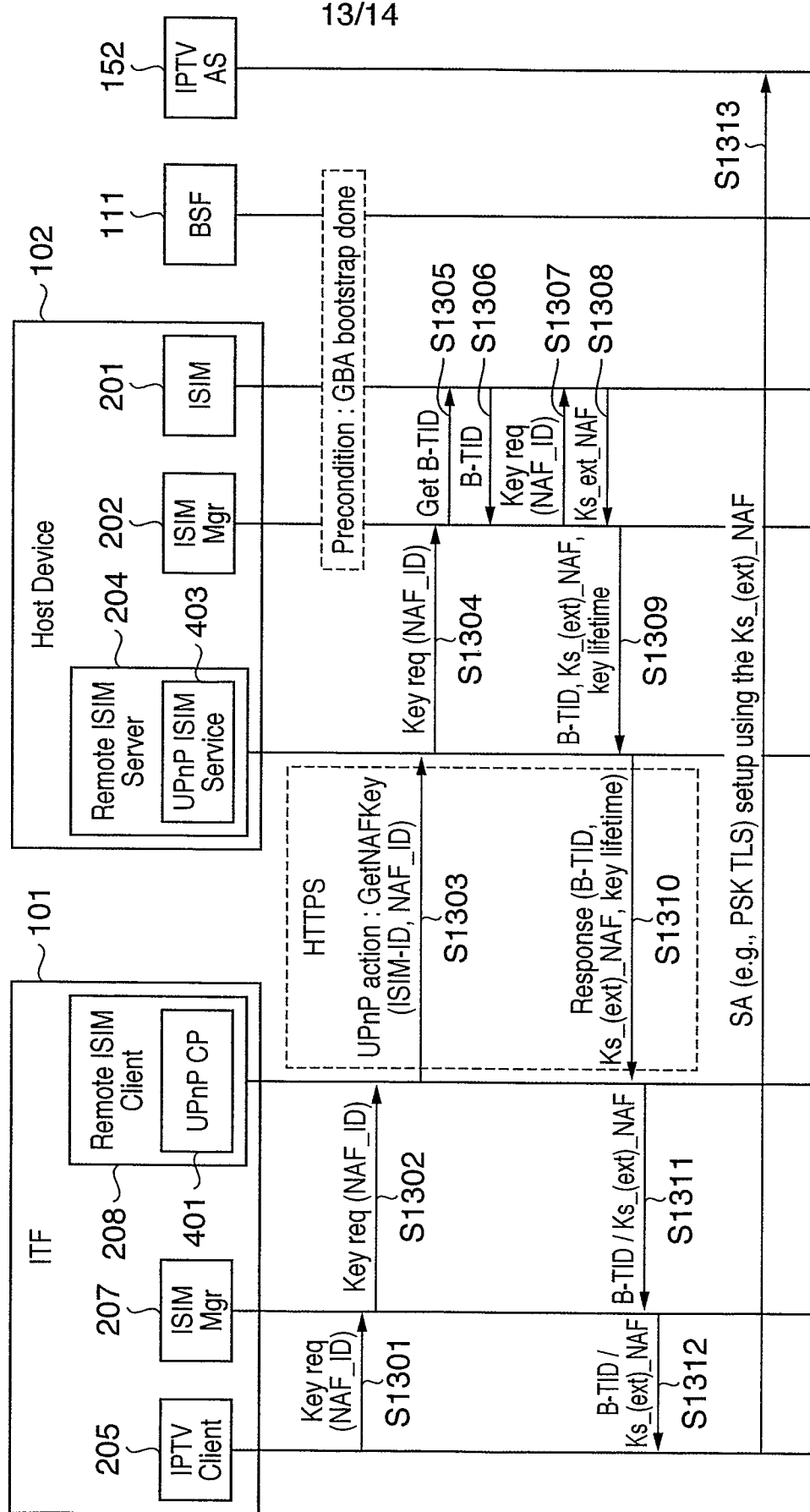


FIG. 13



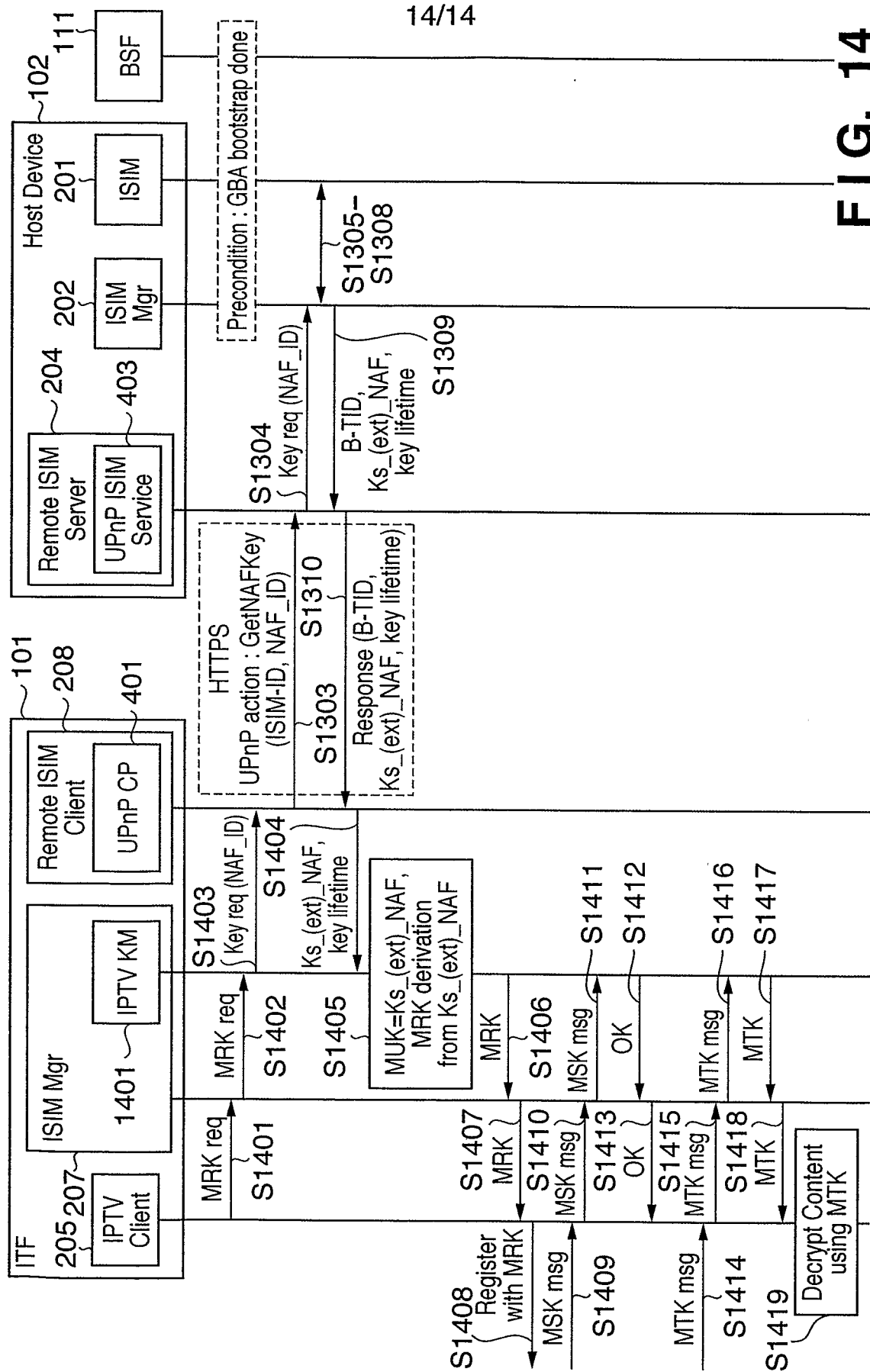


FIG. 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2008/059951

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F13/00 (2006.01) i

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)

Int.Cl. G06F13/00

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

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2008
 Registered utility model specifications of Japan 1996-2008
 Published registered utility model applications of Japan 1994-2008

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006/045706 A1 (TELEFONAKTIEBOLAGET LM ERICSSON) 04 May 2006, pages 6 to 11 & US 2007/0195805 A1 & GB 2419774 A	1-34
Y	Hiroshi DEMPO, Shozo FUJINO, Ippei AKIYOSHI, "Personal Area Network Support in an All-IP Network", PROCEEDINGS OF THE 2005 IEICE COMMUNICATIONS SOCIETY CONFERENCE, THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS, 07 September 2005, pages S-19 to S-20	1-34
Y	JP 2003-324768 A (Sharp Corp.) 14 November 2003, Paragraphs [0006], [0044]-[0048] (No Family)	1-34



Further documents are listed in the continuation of Box C.



See patent family 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 application or patent 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

19.06.2008

Date of mailing of the international search report

01.07.2008

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

Koji TAUCHI

Telephone No. +81-3-3581-1101 Ext. 3565

51

3355

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2008/059951

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-125352 A (Sony Corporation) 25 April 2003, Paragraphs [0047] to [0048] (No Family)	2, 10
A	Peter Howard, "AKA usage in 3GPP", [online] 3GPP TSG SA WG3 Security S3#34, 2004 [retrieved on 19 June 2008], URL: http://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_34_Acapulco/Docs/PDF/S3-040645.pdf	1-34
A	WO 2006/109122 A1 (NOKIA INC.) 19 October 2006, pages 7 to 10 & US 2006/0230436 A1	1-34
A	Rolf Johansson, "Converging Requirements on the Residential Gateway", [online], 2005 [retrieved on 19 June 2008], URL: http://www.iec.org/events/2005/bbwf/pdfs/g2_rolf_johansson_ericsson.pdf	1-34