Electronic Communications Committee (ECC)
within the European Conference of Postal and Telecommunications Administrations (CEPT)

NGN AND IMS CALL SETUP

Constanta, July 2007

EXECUTIVE SUMMARY

This report provides an introduction to the NGN architecture and the main functional elements as specified by ETSI TISPAN, and provides a set of diagrams to show the main signal flows for:

- Connection to a network with the establishment of IP-connectivity
- Call set up from mobile to mobile
- Call set up from mobile to fixed PSTN terminal.

The flows are for a terminal connecting to an IMS-based Next Generation Network working according to 3GPP/TISPAN Release 5 standards. It should be noted that early implementations of Next Generation Network will not use IMS but will use ISUP messages encapsulated in SIP.

The purpose of the report is to enable the reader to understand the basic operation.

The intention is to add further information to later versions of the report.

Table of contents

IMS AND NGN CALL SETUP

1 INTRODUCTION

The purpose of this report is to explain the normal operation of registration and call setup for a mobile originated call in IMS and NGN. This report is not meant to be an endorsement of any one technology or release as opposed to any other. Due to the continuing development of standards in this area and the period when this report was prepared, this report is based primarily on 3GPP Release 5.

IMS allows two different configurations depending on whether the P-CSCF is located in the home or in the visited network.

In the **long-term vision** of IMS the P-CSCF (and GGSN) will be located in the visited network (which requires IMS support by the visited network).

In the **short-term vision** of IMS the P-CSCF (and GGSN) is located in the home network (because it cannot be expected that all roaming partners will upgrade their networks at the same time the home network starts with IMS). In this case no IMS support is expected from the visited network (i.e. no 3GPP Release 5 compliant GGSN is provided in the visited network). This configuration has the severe disadvantage that it causes tromboning of media streams, as the media plane traverses the GGSN and thus in most cases takes a longer path to its destination.

When the IP Connectivity Access Network is GPRS, the location of the P-CSCF depends on the location of the GGSN, because the P-CSCF controls the GGSN via the so-called GO interface which is always an network internal interface because otherwise its operation would be complex.

This report is based on the long-term vision of IMS.

This report is based on mobile access and originating calls according to 3GPP Release 5. It is planned to add to later releases of this document:

- Upgrades according to NGN specifications based on 3GPP Releases 6 and 7
- Fixed originating calls including NASS and RACS functionalities, which are specified within TISPAN.

2 ABBREVIATIONS AND EXPLANATION OF TERMS

The meaning of the abbreviations is taken from standards but the explanatory text that follows is not.

3GPP Third generation Partnership Project (for mobile standards)

APN Access Point Name. The logical name for a service or network

AS Application Server, interfacing the S-CSCF and hosting and executing services. The AS can be located either in the home network or in an external third-party network. There are 3 different types of AS:

- SIP AS: A native application server for IP multimedia services based on SIP.
- OAS-SCS: Open Service Access-Service Capability Server. It inherits all the OSA capabilities, e.g. those to access the IMS securely from external networks and therefore, it acts as an interface between the OSA Application Server and the OSA Application Programming Interface as well as an Application Server.
- IM-SSF: IP Multimedia Service Switching Function for the support of CAMEL in the IMS (Customized Application for Mobile networks Enhanced Logic developed for GSM).

ASF Application Server Function. An ASF offers value added services and resides either in the user's home network or in a third party location. The third party could be a network or simply a stand-alone AS.

AUC Authentication Centre. The AuC can be considered a subset of the HSS that holds the following functionality for the CS Domain and PS Domain:

- The AuC is associated with an HLR and stores an identity key for each mobile subscriber registered with the associated HLR. This key is used to generate security data for each mobile subscriber.

- The AuC communicates only with its associated HLR over a non-standardised interface denoted the H-interface. The HLR requests the data needed for authentication and ciphering from the AuC via the H-interface, stores them and delivers them to the VLR and SGSN, which need them to perform the security functions for a mobile station.

BGCF Breakout Gateway Control Function, providing routing based on telephone numbers and only used when calling a subscriber in a circuit switched network. It selects the appropriate network where interworking with the circuit switched domain is to occur or selects an appropriate PSTN gateway.

GGSN Gateway GPRS Support Node, responsible for IP address management and QoS and the provision of external gateway functions.

GPRS General Packet Radio Service. This is a network added later to the GSM for the support of non real time packet switched Internet services. GSM/GPRS is referred to as 2.5 generation network which provides around 64 kbps data rates. Its major components are the SGSN and the GGSN.

GSM Global System for Mobile Communication. The second generation of mobile networks, upcoming in 1990, is designed for circuit switched voice traffic and low rate data service (14,4 – 28,8 kbps).

HLR Home Location Register

HSDPA High Speed Downlink Packet Access. HSDPA is based on techniques such as adaptive modulation and hybrid automatic repeat request to achieve high throughput, reduce delay and achieve high peak rates.

HSS Home Subscriber Server. As an evolution of the HLR of the GSM, it is a database for user related information including location information, security (authentication and authorization) information, user profile, etc.

IBCF Interconnection Border Control Function

I-BGF Interconnection BGF

ID Identity, used to uniquely identify users and services. In the PSTN telephone numbers are used to identify users (or services like e.g. 800 for freephone). In the IMS there is also a deterministic way to identify users and services:

Public User Identities: A home network operator allocates one or more (e.g. to differentiate between private and business) Public User Identities to each IMS-subscriber. In the IMS it is possible to register several Public User Identities by either using one SIP message that carries all the Public User Identities the user wants to register or registering one Public User Identity after the other by sending from the UE to the S-CSCF a REGISTER message per Public User Identity (note: At any time the user can register an additional Public User Identity). A Public User Identity is either a SIP URI (e.g. sip:alois.sommerer@operator.com) or a TEL URI (e.g. tel:+44-4123-4567) or a combination of both (e.g. sip:+44-4123-4567@operator.com; user=phone). TEL URIs are needed for calls to/from the PSTN.

Private User Identities: A home network operator allocates one Private User ID to each subscriber, its format is neither a SIP URI nor a TEL URI but a Network Access Identifier (NAI) and looks like: username@operator.com. Private User IDs are exclusively used for subscription identification and authentication purposes, but not for routing of SIP messages. It is not necessarily known by the subscriber, but stored on the UICC. In 3GPP Release 6 more than one Private User ID is possible per IMS subscriber.

Public Service Identities: In 3GPP Release 6 a Public Service ID is allocated to a service hosted in an Application Server. It has the format of a SIP-URI or a TEL-URI.

IMS IP Multimedia Subsystem: Based on technical specifications of the 3GPP working groups, IMS combines the latest trends in technology, provides a common platform to develop multiple multimedia services, supports QoS, interworking with the internet and circuit-switched networks, and roaming, and supports a multitude of charging rules and principles. Release 5 focuses on mobile networks only (see also UMTS) while Release 6 is the so-called access-independent IMS; i.e. it provides support for different access networks. The interfaces within the IMS use the following protocols:

- SIP (used to control sessions)
- DIAMETER (which an evolution of RADIUS is used for Authentication, Authorization, and Accounting and is e.g. used to interact with the HSS)
- COPS (Common Open Policy Service) is used to transfer policies between PDPs and PEPs
- H.248 (also referred to as MEGACO, say MEdia GAteway COntrol, is used to control the media plane. E.g. it is used by the MGCF to control the MGW)
- RTP (Real Time Protocol) and RTCP (Real Time Control Protocol) transports the real time media streams.

IM SSF IP Multimedia-Service Switching Function.

IP-CAN IP Connectivity Access Network. There are a multiple types eg: Digital Subscriber Line, Local Area Networks, GPRS, WLAN, etc. Note: The IP-CAN may not be owned by a single organisation as the SGSN may be in the visited network and the GGSN in the home network at least in the short term vision of IMS.

ISIM IP multimedia Service Identity Module. It contains parameters used for user-identification and –authentication as well as terminal configuration in the IMS environment. This application can co-exist on the UICC with the SIM and USIM. The IMS-relevant parameters stored in the ISIM are:

- **Private User Identity** (allocated to the user)
- **Public User Identity** (one or more SIP URIs of Public User Identities allocated to the user)
- **Home Network Domain** URI (SIP URI of the home network domain name)
- **Long-term secret** (used for authentication and for calculation of the integrity and cipher keys used between the terminal and the network.

ISUP ISDN Signalling User Part

IWF Interworking Function

I-CSCF Interrogating-Call/Session Control Function. It is logically located at the edge of an administrative domain (usually in the home network) and its address is listed in the DNS. After retrieval of the user location information from the SLF/HSS, SIP requests are routed further to the S-CSCF. A network will include typically a number of I-CSCFs for scalability and redundancy reasons.

LCS LoCation Services. LCS is a service concept in system (e.g. GSM or UMTS) standardization. LCS specifies all the necessary network elements and entities, their functionalities, interfaces, as well as communication messages, due to implement the positioning functionality in a cellular network. Note that LCS does not specify any location based (value added) services except locating of emergency calls.

LI Lawful Interception

MBMS Multimedia Broadcast Multicast Service. A unidirectional point-to-multipoint service in which data is transmitted from a single source entity to a group of users in a specific area. The MBMS has two modes: Broadcast mode and Multicast mode.

MGCF Media Gateway Control Function. Used for protocol conversion (mapping SIP to ISUP over IP and vice versa) and control of resources in the MGW.

MGW Media Gateway, interfacing the media plane of the GSM or PSTN and thus mapping the RTP to PCM time slots and performing transcoding when the IMS terminal does not support the codec used at the PSTN-side (typically: IMS terminal using AMR codec, PSTN using ITU G.711 codec).

MRF Media Resource Function, located in the home network and used to play announcements, mix media streams (e.g. conference bridge), transcode between different codecs, provides specific statistics and media analysis. The function is subdivided into a Media Resource Function Controller (MRFC, which acts as a SIP User Agent and contains the SIP interface to the S-CSCF) and a Media Resource Function Processor (MRFP, which provides the media-related functions).

MRFC Multimedia Resource Function Controller. The MRFC, in conjunction with an MRFP located in the transport layer, provides a set of resources within the core network for supporting services.

MRFP Multi Media Resource Function Processor. The MRFP provides specialized resource processing functions beyond those available in media gateway functions.

MTP Message Transfer Part. The MTP provides the functions that enable User Part significant information passed to the MTP to be transferred across the Signalling System No. 7 network to the required destination. In addition, functions are included in the MTP to enable network and system failures that would affect the transfer of signalling information to be overcome. This constitutes a sequenced connectionless service for the MTP user.

NAPT NAPT is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. NAPT allows mapping of tuples of the type (local IP addresses, local TU port number) to tuples of the type (registered IP address, assigned TU port number). NAPT is defined in the RFC3022 section 2.2.

NASS Network Attachment Subsystem. The NASS provides the following functionalities: Dynamic provision of IP address and other user equipment configuration parameters (e.g. using DHCP), User authentication, prior or during the IP address allocation procedure, Authorization of network access, based on user profile, Access network configuration, based on user profile, and Location management.

P-CSCF Proxy-Call/Session Control Function. Allocated to the IMS terminal during IMS registration, it is an outbound/inbound SIP server passing all the SIP messages to and from the terminal and provides some basic functionality related to security (integrity protection to ensure that the contents of the message have not changed since its creation, user authentication, correctness of SIP request initiated by the IMS terminal). Additionally, it provides compression/decompression of SIP messages, generates charging information towards a charging collection node and may include a PDF (Policy Decision Function, which authorizes media plane resources and manages QoS over the media plane). An IMS network includes a number of P-CSCF for scalability and redundancy reasons (each P-SCSF serves a number of IMS terminals). The P-CSCF is always located in the same network where the GGSN is located. It is expected that the first IMS networks will have GGSN and P-CSCF in the home network.

PDP Policy Decision Point

PEP Policy Enforcement Point

RNC Radio Network Controller

PES PSTN/ISDN Emulation Subsystem. The PES supports the emulation of PSTN/ISDN services for legacy terminals connected to the NGN, through residential gateways or access gateways.

PSTN Public Switched Telephone Network

RACS Resource and Admission Control Subsystem. RACS is the TISPAN NGN subsystem, responsible for elements of policing control including resource reservation and admission control in the access and aggregation networks. The RACS also includes support for a Network Address Translator (NAT) at any place or set of places in the access, aggregation and core networks.

RTSP Real Time Streaming Protocol. The Real Time Streaming Protocol, or RTSP, is an application-level protocol for control over the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video.

SCCP Signalling Connection and Control Part. The SCCP provides additional functions to the Message Transfer Part (MTP) to cater for both connectionless as well as connection-oriented network services to transfer circuit-related

and non-circuit-related signalling information and other types of information between exchanges and specialized centres in telecommunication networks (e.g. for management and maintenance purposes) via a Signalling System No. 7 network.

SCIM Service Capability Interaction Manager. The SCIM functionality is an application which performs the role of interaction management.

SCTP Stream Control Transmission Protocol. It is a reliable transport protocol operating on top of a potentially unreliable connectionless packet service such as IP. It offers acknowledged error-free non-duplicated transfer of messages. Detection of data corruption, loss of data and duplication of data is achieved by using checksums and sequence numbers. A selective retransmission mechanism is applied to correct loss or corruption of data.

SDP Session Description Protocol (a textual format to describe multimedia sessions). It includes e.g. the IP address of the requestor, the port number where the requestor expects to receive audio and video, and the list of audio and video codecs supported.

SGF Signalling Gateway Function. The Signalling Gateway Function (SGF) performs the signalling conversion (both ways) at transport level between the SS7 based transport of signalling and IP based signalling transport.

SGSN Service GPRS Support Node, responsible for mobility management, security and authorization.

SGW Signalling Gateway, interfacing the signalling plane of the PSTN or GSM and performing lower layer protocol conversion (it transforms ISUP over MTP into ISUP over SCTP/IP).

SIM Subscriber Identity Module. An application on the UICC that holds primarily GSM user subscription information.

SIP Session Initiation Protocol (defined in RFC 3261 by the Internet Engineering Task Force in June 2002) is based on HTTP (Hypertext Transfer Protocol, defined in RFC 2617 by the Internet Engineering Task Force in June 1999) and therefore is a textual request-response protocol designed to provide basic call control and application signalling for voice and multimedia calls or sessions in a packet-switched network. It benefits from simplicity, scalability, robustness, flexibility, and extensibility and has the following format:

- Start Line (in case of a SIP Request called Request Line, in case of a SIP response called Status Line)
- Header Fields (there exist mandatory and optional Header Fields)
- empty line
- optional Message Body (a set of Header Fields provide information about the message Body). The Message Body provides e.g. the SDP.

The start line includes always the SIP protocol version used. In case of a Status Line it also includes a status code and a reason phrase (e.g. SIP/2.0 180 Ringing). In case of a Request Line, it also includes a method name and a request URI (e.g. INVITE sip:Joe.Blogs@domain.com SIP/2.0).

Status codes ranges are:

- 100-199 (Provisional or informational),
- 200-299 (Success),
- 300-399 (Redirection),
- 400-499 (Client Error),
- 500-599 (Server Error), and
- 600-699 (Global Failure).

Method names are e.g.

- ACK (acknowledges the establishment of a session),
- BYE (terminates a session),
- INVITE (establishes a session),
- PRACK (acknowledges the reception of a provisional response), etc.

A SIP transaction consists of a request from the client, zero or more provisional responses, and one final response from the server. As SIP is not an efficient protocol regarding message size (because its textual based) users with low-bandwidth access (e.g. radio access) need to minimize the amount of data transmitted via the access network. For this reason signal compression will be applied for SIP messages exchanged between the UE and the P-CSCF.

SIP extension: The SIP core protocol is relatively simple and encourages future extensions, i.e. allows system designers to subsequently add new features. SIP can be extended in at least three ways:

- defining new message body types
- defining new headers
- defining new message types.

Interoperability of extensions: The base protocol includes mechanisms for extension management and rules for how to deal with unknown or unexpected extensions. Extensions are identified by a standardized token that is registered with IANA (Internet Assigned Numbers Authority). Two SIP implementations dynamically assess which extensions are supported and negotiate down to a basic level of operation.

SIP AS SIP Application Server

SLF Subscription Location Function. If a network contains more than one HSS because the number of subscribers is too high to be handled by one single HSS, the SLF maps user addresses to HSSs.

SS7 Signalling System No 7, the signalling used in circuit switched networks.

S-CSCF Serving-Call/Session Control Function. It is a SIP server which performs session control and acts as a SIP registrar (mapping of the IP address of the terminal where the user is logged on and the user's SIP address, i.e. the Public User Identity). Mainly it performs routing functionality and thus, all SIP signals to and from the IMS terminal traverse the S-CSCF. In the case a telephone number is dialed instead of a SIP URI (Uniform Resource Identifier) the S-CSCF provides a translation service based on DNS E.164 Number Translation. The S-CSCF interfaces to the HSS for user authentication and downloading of the user profile as well as asking the HSS for mapping its address with the user for the duration of the registration. Each S-CSCF serves a number of IMS terminals. The S-CSCF is always located in the home network.

T-MGF Trunking Media Gateway Function. The T-MGF provides the media mapping and/or transcoding functions between an IP-transport domain and switched circuit network facilities.

TCAP Transaction Capabilities Application Part. Transaction Capabilities provide functions and protocols to a large variety of applications distributed over switches and specialized centres in telecommunication networks (e.g. databases).

TD-SCDMA TD-SCDMA is an innovative mobile radio standard for the physical layer of a 3G air interface. It has been adopted by ITU and by 3GPP as part of UMTS release 4, becoming in this way a global standard, which covers all radio deployment scenarios: from rural to dense urban areas, from pico to micro and macrocells, from pedestrian to high mobility. TD-SCDMA is equally adept at handling both symmetric and asymmetric traffic, making it perfectly suited for mobile Internet access and multimedia applications.

TDD Time Division Duplex

UE User Equipment.

UICC Universal Integrated Circuit Card: A removable smart card with standardized interface and limited storage capacity used to hold subscription information, authentication keys, phone numbers, messages, etc. It may contain one or several logical applications such as SIM (Subscriber Identity Module), USIM (Universal Subscriber Identity Module) and ISIM (IP multimedia Service Identity Module). The UICC itself refers to the physical card, whereas SIM, USIM and ISIM refer to applications stored on the UICC.

UMTS Universal Mobile Telecommunication System. Standardized by 3GPP, it is referred to as the third generation network, providing data rates of 2 Mb/s and supporting video and audio streaming and location based services.

- Release 99 defines the basic architecture consisting of the UMTS Terrestrial Radio Access Network (UTRAN), the Circuit Switched Core Network (CS-CN), and the Packet Switched Core Network (PS-CN).
- Release 4 adds new services but does not change the Release 99 architecture.
- Release 5 offers both traditional telephony as well as packet switched enhanced multimedia services over a single converged packet based network, using SIP as the basic protocol and IMS as the signalling architecture.

UPSF User Profile Server Function

URI Universal Resource Identifier. Identifies users (similar to email addresses)

USIM Universal Subscriber Identity Module. Used to access UMTS networks, this application stored on the UICC includes information similar to that on a SIM.

UTRAN UMTS Terrestrial Radio Access Network.

3 ESTABLISHMENT OF IP-CONNECTIVITY

This section describes how a mobile IMS User Equipment (UE) establishes connectivity with its home or serving network and registers on that network.

The IP-CAN (IP Connectivity Access Network) has a GPRS architecture and thus, is composed of SGSN and GGSN nodes. Note the IP-CAN may not be owned by a single organisation as the SGSN may be in the visited network and the GGSN in the home network at least in the short-term vision of IMS.

The mobile UE is roaming and is equipped with an UICC (Universal Integrated Circuit Card), which includes an ISIM application (ISIM is IMS specific while USIM is only UMTS specific).

The visited network to which the UE is going to attach provides IMS services and therefore the P-CSCF (as well as the GGSN) of the calling party is located in the visited network.

3.1 Location update and setup of logical connection between UE and SGSN

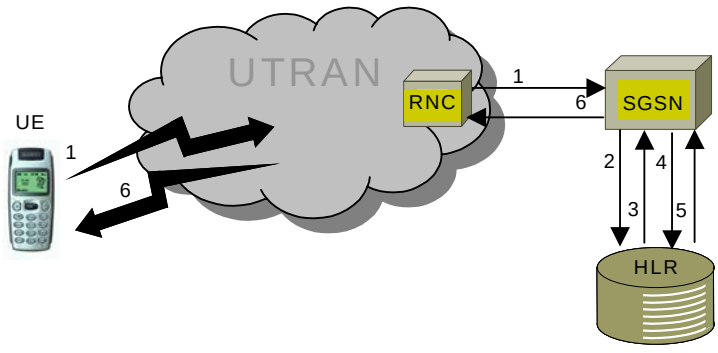


Figure 1: Location update and setup of logical connection between UE and SGSN

1- When the UE is switched on, the ATTACH message is sent via RNC to the SGSN. The RNC and the SGSN have a semi permanent connection to each other.

2 - The SGSN asks the HLR of the UE's home network for authentication by providing the IMSI of the subscriber. This signalling uses the MAP protocol if GPRS or UTRAN are used as the access network.

3 - The HLR provides authentication parameters to the SGSN.

4 - The SGSN asks the HLR for the subscriber profile and informs the HLR about the cell_id in which the UE resides so that the HLR's record of the subscriber's location can be updated.

5 - The HLR responses by sending of the subscriber profile (subscribed services, QoS profile, static IP-address allocated by the network operator, etc.) to the SGSN. (This is equivalent to updating the VLR)

6 - The SGSN sends ATTACH COMPLETE message to the UE, including the UE IP-address for the UE's end of the PDP Context tunnel..

3.2 Activate PDP-Context

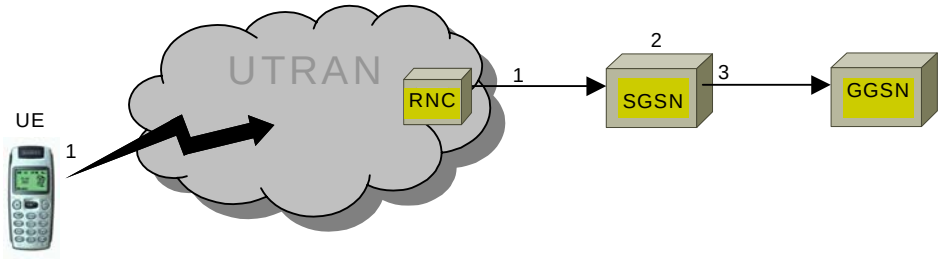


Figure 2: Activate PDP-Context (first part)

1- When ATTACH COMPLETE message is received, the UE automatically sends the ACTIVATE PDP CONTEXT REQUEST message to the SGSN. In case the UE is an IMS terminal the APN requested by the UE indicates the IMS network.

2 - The SGSN provides a crosscheck with the subscriber profile initially received from the HLR and selects the appropriate service node (e.g. the appropriate GGSN).

3 - If the subscriber is NOT roaming, or the subscriber is roaming but the visited network provides IMS services and thus the P-CSCF is located in the visited network, the SGSN sends the CREATE PDP CONTEXT REQUEST to the appropriate GGSN, which is in the same network to which the SGSN belongs. Otherwise the SGSN has to send the message to the GGSN of the home network. The reason is that the GGSN and P-CSCF are always located in the same network, because their interface is always an intra-operator interface to make its operation simpler.

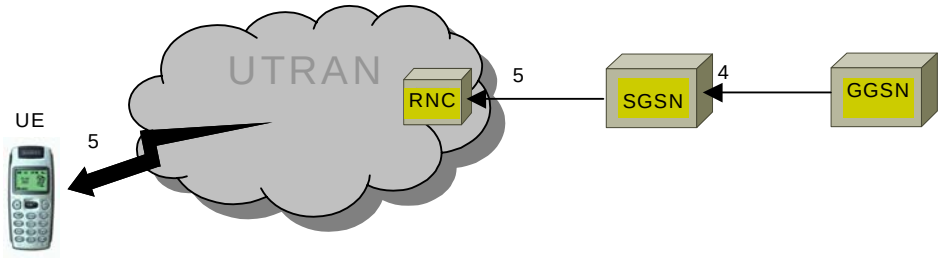


Figure 3: Activate PDP-Context (second part)

4 - The GGSN sends CREATE PDP CONTEXT RESPONSE message to the SGSN. This message includes the IP-address of the P-CSCF (the GGSN stores the P-CSCF addresses).

5 - The SGSN sends ACTIVATE PDP CONTEXT ACCEPT message to UE. It conveys the IP-address of the P-CSCF to be used by the UE to continue with SIP services. A logical tunnel called the PDP Context has now been set up between the UE and the GGSN.

This is the so-called ”integrated procedure”.

In the so-called ”stand alone procedure” the address of the GGSN instead of the address of the P-CSCF is returned to the UE and the UE has to contact the DNS (with the help of a DHCP server) to get the address of the P-CSCF.

From now on the P-CSCF is assigned to the UE. This assignment does not change until the UE is powered off or goes out of coverage.

3.3 IMS Service Registration

The purpose of service registration is to request authorization to use IMS services. This is essential before a session can be established.

During service registration:

- The user binds his public user identity to a contact address
- The home network authenticates the user
- The user authenticates the home network
- The home network authorizes the SIP registration and usage of IMS resources
- The home network verifies that there is a roaming agreement with the visited network
- The UE and P-CSCF negotiate the security mechanism in place for subsequent signalling
- P-CSCF and UE establish a set of security associations for the integrity of SIP messages exchanged
- The UE and P-CSCF upload to each other the algorithms used for SIP message compression (SIP message compression is essential for the air-interface, as SIP is a text based protocol and thus has long messages).

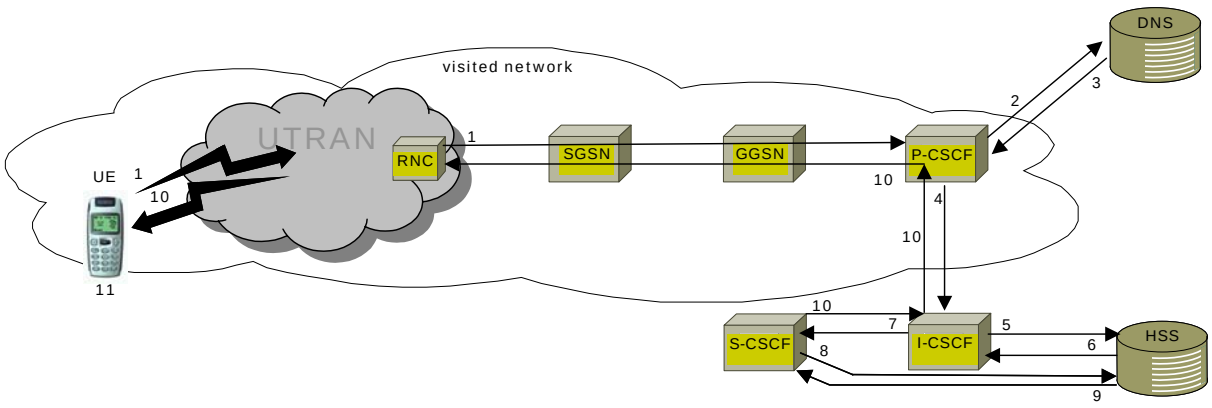


Figure 4: Service registration

1 - The UE sends SIP REGISTER message to P-CSCF. This message includes:

- URI that identifies the home network (e.g. home.net)
- Public User Identity (i.e. the SIP address of the user, which e.g. is on his business card)
- Private User Identity (may not be known to the user, comparable with the IMSI in GSM, and used for authentication only)
- Contact address (IP address of the UE obtained from the GGSN, or the host name where the user is reachable)

The first three IDs are stored in the ISIM of the UE.

2 - The P-CSCF contacts the DNS to locate an entry point into the home network by sending the home domain name.

3 - DNS provides the address (the SIP URI) of the I-CSCF of the home network. (Note: registration always goes via the I-CSCF, whereas session setup may use the S-CSCF directly).

4 - The P-CSCF sends SIP REGISTER message to I-CSCF. This message includes

- SIP URI of the P-CSCF
- Public User Identity
- Private User Identity
- visited network ID (for the check of existence of a roaming agreement).

5 - The I-CSF is not aware of whether or not an S-CSCF is already allocated to the user and what the address of this S-CSCF is. To check this and additionally to carry out a first step authorization, I-CSCF uses the Diameter protocol to send a message called UAR (User-Authentication-Request) via the Cx reference point to the HSS. This message includes the:

- visited network ID
- Private User Identity
- Public User Identity.

6 - The HSS validates the Private User ID and Public User ID. It sends the Diameter message UAA (User-Authentication-Answer) to I-CSCF. This message includes either the SIP URI of the S-CSCF if already allocated previously or a set of S-CSCF capabilities.

If this is the first registration after UE is powered on, HSS usually returns a set of mandatory (e.g. SIP calling) and optional (e.g. charging) S-CSCF capabilities.

Note: The standard does not indicate what these capabilities are and how they are specified. They are network individually defined.

7 - The I-CSCF has a configurable table of S-CSCFs and their capabilities and selects the appropriate S-CSCF. Then it sends the SIP REGISTER message to this S-SCSF, including:

- subscriber ID
- visited network contact name
- home network contact point
- P-CSCF name.

8 - The S-CSCF contacts the HSS by means of the Diameter message MAR (Multimedia-Auth-Request) to get authentication data of the subscriber and to inform the HSS about the S-CSCF URI allocated to that user.

Note: S-CSCF needs user data to authenticate the user (initial registrations are always authenticated by the S-CSCF, other SIP messages like INVITE are never authenticated in the IMS).

9 - The HSS returns the user authentication data, which will be stored in the S-CSCF.

10 - The S-CSCF sends SIP 401 UNAUTHORIZED message back to the UE. This message traverses the I-CSCF, the P-CSCF, and the GPRS-nodes.

11 - Upon receipt of the SIP 401 the UE realizes that there is a challenge included and contacts its ISIM to build up the credentials.

Note: The actual credentials depend on the IMS network and are derived from the UICC. In fact, authentication information is stored in the UICC, which builds up the credentials used for security purposes.

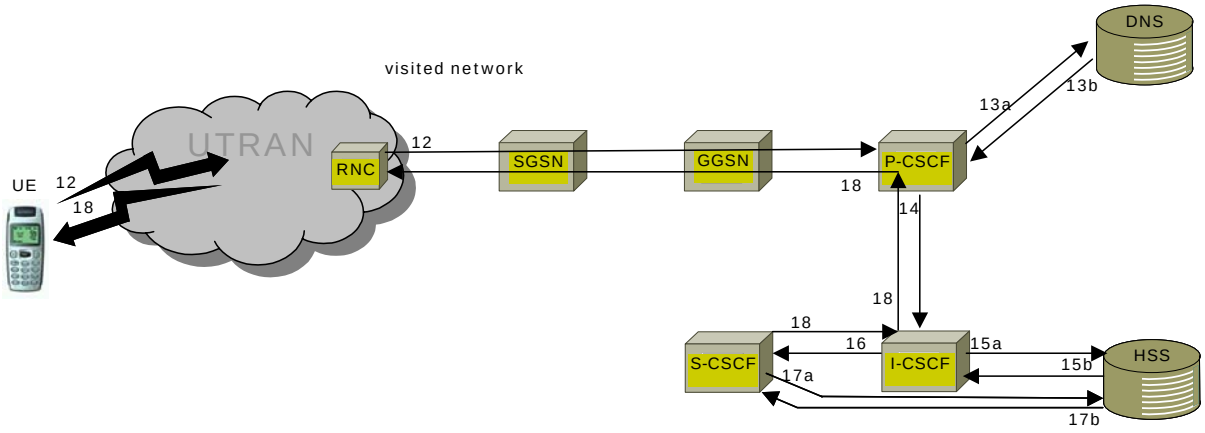


Figure 5: Service registration continued

12 - The UE sends a SIP REGISTER message again to the P-CSCF.

13 - The P-CSCF does the same procedure as already done after reception of the initial SIP REGISTER message: It contacts DNS to get the address of the I-CSCF of the home network.

Note: Due to DNS load balancing mechanisms the address of the I-CSCF in the home network may not be the same as derived upon receipt of the first SIP REGISTER message.

14 - The P-CSCF passes the SIP REGISTER message to the I-CSCF, which now will run the same procedure as already run initially.

15a - As the (eventually new) I-CSCF is not aware of whether or not an S-CSCF is already allocated to the user and what the address of this S-CSCF is and – eventually - to carry out a first step authorization. I-CSCF uses the Diameter protocol to send a message called UAR (User-Authentication-Request) via the Cx reference point to the HSS. This message includes again the visited network ID, the Private User Identity, and the Public User Identity.

15b - The HSS returns the Diameter message UAA (User-Authentication-Answer) to I-CSCF, which includes now the SIP URI of the S-CSCF already allocated to the user.

16 - The I-CSCF passes the SIP REGISTER message to the S-CSCF, which validates the credentials received against the authentication user data already stored.

17 - The S-CSCF sends the Diameter message SAR to inform the HSS that the user is now registered. In response, by means of the Diameter message SAA, the HSS returns the user profile to the S-CSCF, which will be stored locally in the S-CSCF.

Note: The user profile includes all the Public User Identities and indicates which of them are automatically registered in the S-CSCF. It also includes the initial filter criteria, i.e. a collection of triggers used to determine the application server providing the service when a SIP request arrives.

The S-CSCF has stored now the contact URI for the user as well as the list of URIs along the path to the UE. The S-CSCF will route initial SIP request to the UE along this list of URIs.

18 - The S-CSCF sends the SIP 200 OK back to the UE to indicate the successful registering. The S-CSCF, and possibly also the I-CSCF, adds its address to the Record-Route Header (depending on the strategy of the home network operator). The UE is now registered in the IMS for the duration of time indicated in the expires-parameter of the SIP 200 OK.

4 CALL ORIGINATION TO A MOBILE IMS TERMINAL

This chapter describes how the UE sets up a session to another IMS terminal while both IMS terminals are roaming in different visited networks and both IMS terminals belong to different home networks.

Assumptions:

- The networks to which the UEs are attached provide IMS services (long term vision).
- The originating UE is roaming and is equipped with an UICC (Universal Integrated Circuit Card) which includes an ISIM application (ISIM is IMS specific while USIM is only UMTS specific).
- Call origination describes the session set up initiated by UE1 to another IMS terminal (UE2) roaming in another visited network.
- Both UEs have already registered on their home IMS.
- The Home Network of UE1 does not involve an I-CSCF, but the Home Network of UE2 does.
- Neither at the calling side nor at the called side is an IMS Application Server involved.

Figure 6 shows an overview of the involved networks and nodes/functions in the call/session set up.

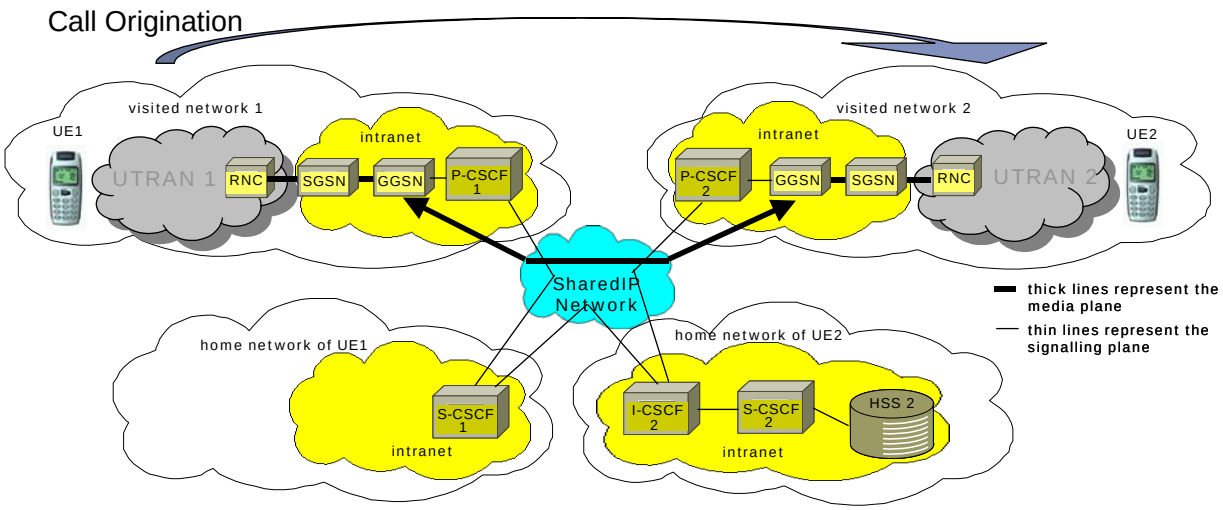


Figure 6: Overview of mobile to mobile call

Figure 7 shows the total signalling flows.

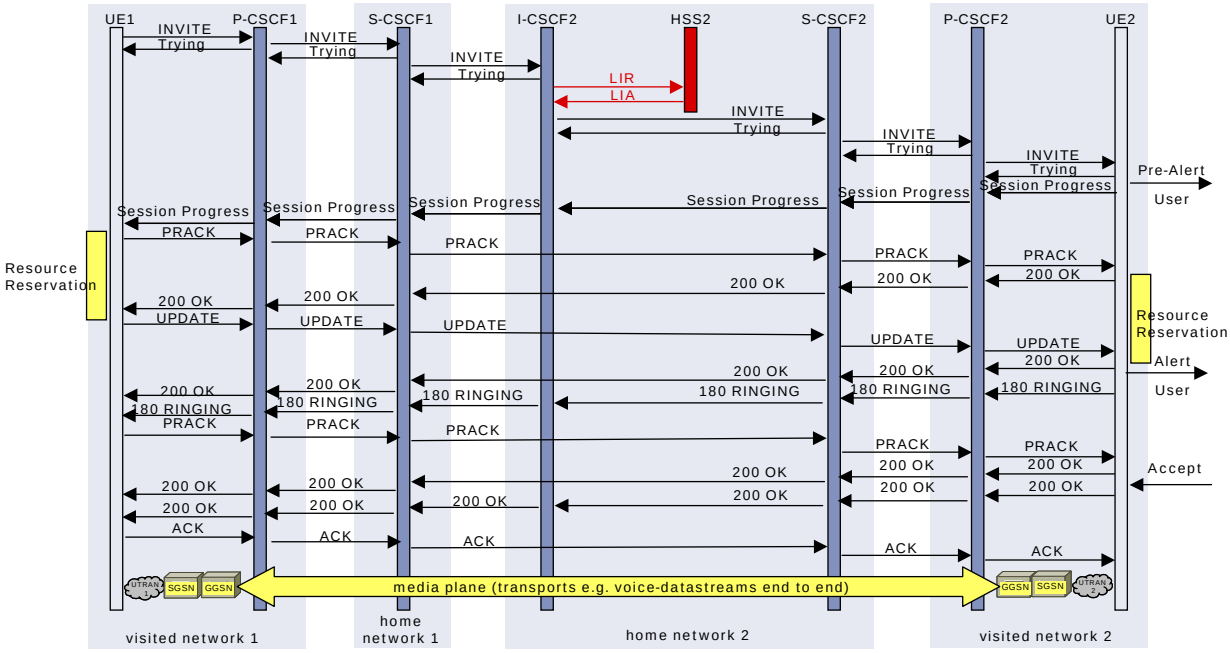


Figure 7: Overview of signalling flows
(SIP messages are black, Diameter messages are red)

The signalling flows are now examined in more detail.

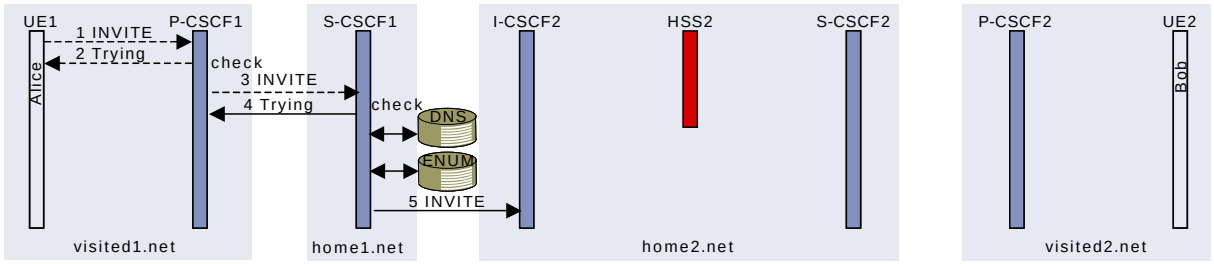


Figure 8: Mobile to mobile call setup

1 - The UE1 sends the SIP INVITE message to its P-CSCF1. It includes:

a) the Public User Identity of the called party (sip: bob@home2.net)

b) the IP address and port number to which the UE1 expects a response as well as the information for signal compression and the transport protocol used to the next hop (e.g UDP, TCP, SCTP). Note: Every node in the chain is free to choose its appropriate transport protocol

c) the IP address and port number to which the UE1 expects subsequent responses after the response to the INVITE message

d) a route list (list of SIP proxies which serve the UE1 and which to be traversed, e.g sip: PCSCF1@visited1.net and sip:SCSCF1@home1.net)

e) the preferred identity of the UE1 user (”Alice Jones” sip: alice@home1.net) if the user has more than one Public User Identity, to indicate which one to be used for this session (to be included in the charging record, to be shown to the called party, to trigger different services)

f) the type of access network used by UE1 (eg UTRAN) for service customization and determination of available

bandwidth as well the radio cell ID, which implicitly contains some location information to be used for local services like e.g. ”list of local dentists”. Note: This information is transferred down to the home network but not further!

g) end-to-end information explaining who is calling (sip: alice@home1.net), who is called (sip: bob@home2.net), and the Call-ID

h) additional information like e.g. SIP-extensions to be used/supported and in the SDP e.g. the audio and/or video codec format supported by the UE1. Note: The complete message content is shown in APPENDIX A of this report

i) SDP containing the list of codecs supported by the UE1.

2 - Upon receipt of the INVITE, the P-CSCF1 returns an acknowledgement (TRYING message) back to the UE1 to inform the sender of the INVITE that his message has been reliably received by the next hop in the chain.

3 - Next, the P-CSCF1 undertakes some internal checks and procedures. It:

- checks if the Route Header is correct and includes the S-CSCF in the home network,
- checks the requested media parameters against the policy of the visited network operator (e.g. G.711 codec not allowed because of 64 kb/s-bandwidth necessity),
- checks the P-Preferred Identity against the list of all the Public User Identities received during the Terminal Registration-Process, and replaces the P-Preferred Identity with the P-Asserted Identity in the INVITE message sent onwards to the S-CSCF1. If there is not a match, the P-CSCF selects one Public User ID out of its list. If there is a match, it puts the received Public User ID into the P-Asserted Identity header. This check provides authentication of the Public User ID,
- removes/modifies some Headers, e.g which relate to security or signal compression) and insert charging headers in the INVITE message,
- records the route together with its own SIP URI.

If all the checks were passed, the P-CSCF1 forwards the modified INVITE to the S-CSCF1 (or to the I-CSCF of the home network operator 1). If all the checks were not passed, the P-CSCF1 would return an error message or 488 NOT ACCEPTABLE HERE message (which includes a list of media types, codecs and other SDP-parameters which are allowed) to UE1.

4 - Upon receipt of the INVITE the S-CSCF1 first of all returns the TRYING message to P-CSCF1.

5 - Next, the S-CSCF1 (it was allocated to the UE1 during Service Registration procedure) identifies the user by means of the value in the P-Asserted-Identity header and retrieves the User Profile which was already downloaded during Terminal Registration. Next the S-CSCF1:

- evaluates the filter criteria stored in the User Profile to find out if and which Application Servers need to be involved,
- checks SDP-parameters against local network policy , e.g. codec format, because user has a cheap subscription which does not allow some media or high speed codecs,
- analyses the called address which can be a SIP URI or a TEL URI. In case of a SIP URI (sip:bob@home2.net) or a SIP URI with mapped telephone number (e.g. sip:+44-4123-4567@home2.net), S-CSCF1 contacts DNS to find the address of a SIP server (usually an I-CSCF) in the network home2.net . In case of a TEL URI, which may belong to a PSTN user or GSM user, the S-CSCF1 contacts ENUM to get a SIP URI. If there is no SIP URI available, the S-CSCF1 will contact the BGCF (Breakout Gateway Control Function)
- adds a TEL URI of the caller to the P-Asserted-Identity header of the INVITE message. This is used in the case the call terminates in the PSTN to enable the PSTN to identify the caller.

The S-CSCF1 sends the modified INVITE message to the I-CSCF2.

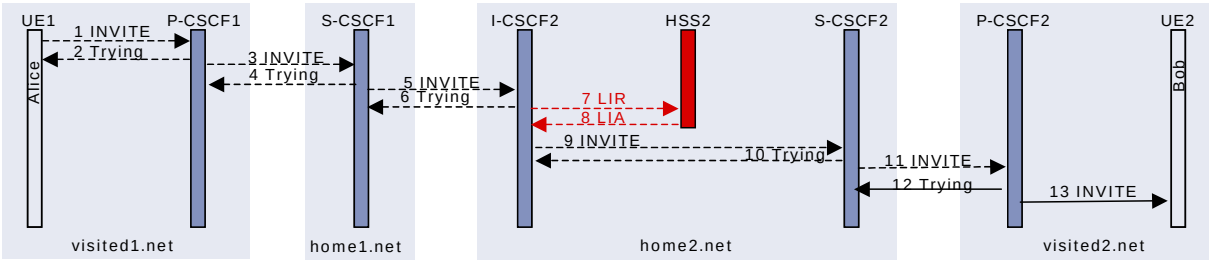


Figure 9: Mobile to mobile call setup (continued)

6 - The I-CSCF2 acknowledges the message reception by sending back the TRYING message to S-CSCF1.

7 - The I-CSCF2 queries the HSS2 about the called SIP URI to get informed, which S-CSCF is already allocated to that user (during the Register Terminal procedure the address of the S-CSCF2 was stored in the HSS). It sends the Diameter message LIR (Location-Information-Request), which includes the value sip: bob@home2.net.

8 - The HSS2 returns the address of the allocated S-CSCF2 to the I-CSCF2 by means of the Diameter message LIA (Location_Information_Answer).

9 - The I-CSCF2 forwards the INVITE message to the S-CSCF2. In this message the address of the I-CSCF2 may or may not be inserted by the I-CSCF2, which is dependent on the configuration made by the network operator (either he wants to hide the address of the S-CSCF2 or not. If it is to be hidden, all SIP signalling is passed via the I-CSCF2 so that the I-CSCF2 can add its address to the Record-Route Header before sending the INVITE message to the S-CSCF2).

10 - S-CSCF2 sends the TRYING message back to the I-CSCF2.

11 - Upon receipt of the INVITE message the S-CSCF2 evaluates the initial filter criteria (same evaluation as the S-CSCF1 has already done) to check if Application Services are to be involved at the called side. As the S-CSCF2 typically remains in the signalling path (in 3GPP R5 always, in 3GPP R6 in some cases) the S-CSCF2 adds its own SIP URI to the Record-Route Header in the INVITE message. Additionally, it inserts the address of the P-CSCF2 (sip:pcscsf2@visited2.net) in the Route Header – this was learned during Terminal Register Procedure when UE2 was powered on. Thus all SIP signalling will now traverse I-CSCF2 as well as P-CSCF2.

Further on, the S-CSCF2 will probably change the Request–URI in the INVITE message to the Contact URI (normally an IP address obtained during registration), which is the current point of contact of the subscriber.

Note: A user can have several Public User Identities and can register subsequently one after the other by sending new REGISTER messages to the S-CSCF (e.g. bob@home2.net and bob-business@home2.net). In these REGISTER messages the Contact Header always includes the Contact URI of the terminal. Depending on the Public User IDs registered by this time, the S-CSCF2 changes the Request-URI to the Contact URI it also adds the initial called party ID as well so that the correct alerting signal can be used if the called party has configured his terminal to alert with different tones depending on the public identity called. Note the choice of field for the initial called party ID in this last stage of the signalling is not yet agreed or stable one possibility is the P-Called-Party-ID.

The S-CSCF forwards the modified INVITE message to the P-CSCF2.

12 - The reception of the INVITE message will be acknowledged by returning the TRYING message.

13 - As the received INVITE message includes already the IP address of the called terminal, the P-CSCF2 identifies the Public User Identity in the P-Called-Party-ID Header to find the proper security association established with the UE2. Then it checks the contents of the Privacy Header: If it includes an ID, then P-CSCF2 removes the P-Asserted-Identity Header so that the called party is then unable to see who the caller is. If the Privacy Header includes ”none” (which means, that there are no privacy requirements from the caller) the P-Asserted-Identity Header remains unchanged. Then the P-CSCF2 carries out a number of functions related to charging, security, control of GGSN, compression of signalling, etc. and adds its own SIP URI to the Record-Route Header in the INVITE message (thus, the P-CSCF2 remains in the path for subsequent signalling). Finally, the modified INVITE message is forwarded to the UE2.
The content of the INVITE message received by the UE2 is shown in APPENDIX B.

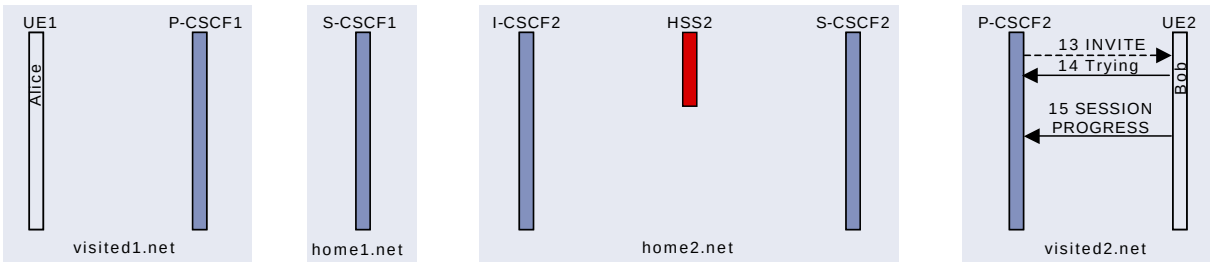


Figure 10: Mobile to mobile call setup (continued)

14 - Upon receipt of the INVITE message the UE2 sends the TRYING message and

15 - follows the call flow model stated in the Require-Header: precondition (i.e. when "precondition" is included in the Require Header, UE2 has to respond with a SESSION PROGRESS message that contains an SDP answer to communicate the media streams and codecs the UE2 is able to handle for this session).
Next, the UE2 inspects

- the P-Asserted-Identity header to extract the identity of the caller and
- the P-Called-Party-ID header to determine to which of the several identities of the user the INVITE is addressed.

The combination of both identities may be used now or in a later stage to play a personalized ringing or display a picture of the caller, etc.

The called terminal is now at the pre-alert stage.

The SESSION PROGRESS message sent by the UE2 back to P-CSCF-2 includes advice for the UE1 to send an updated SDP when terminal resource reservation on calling side has been completed (the calling and the called party will be alerted only when resource reservation has been completed on both sides).

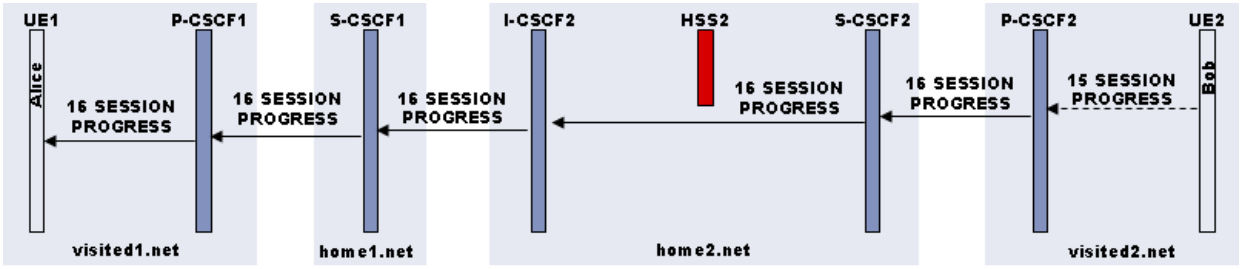


Figure 11: Mobile to mobile call setup (continued)

16 - The SESSION PROGRESS message traverses step by step all the nodes back to the UE1. Except the I-CSCF1, all other nodes provide some checks and functions before sending the message onwards. The SESSION PROGRESS includes SDP containing the list of codecs supported by both UE1 and UE2.

For example, P-CSCF2 inserts a P-Asserted-Identity header whose value is the same as that included in the P-Called-Party-ID header of the former INVITE (by this way the other nodes get the public user identity of the called party being used for this session). Another example is that the S-CSCF-1 removes the P-Asserted-Identity header if privacy requirements indicate so.

Finally, the SESSION PROGRESS message arrives at the UE1.

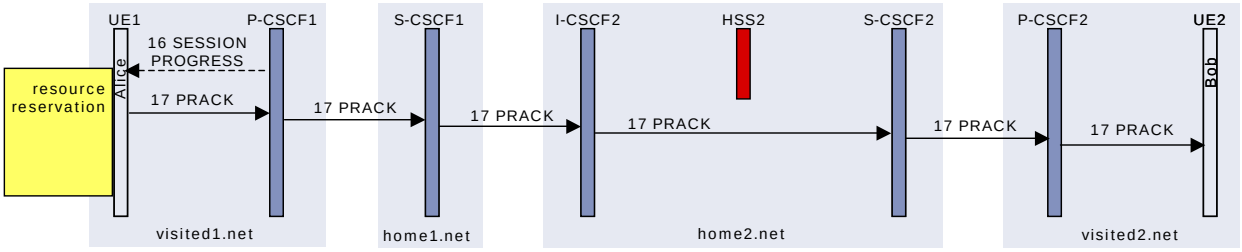


Figure 12: Mobile to mobile call setup (continued)

17 - Upon receipt of the SESSION PROGRESS message (which includes the IP-address of UE2) the UE1 is informed:

- whether or not the UE2 accepts a session with the media streams proposed (or only audio but no video)
- what codecs are supported at both ends.

The UE1 now selects a codec from the list supported at both ends for each media stream.

Then the UE1 starts resource reservation. This is a procedure that is dependent on the underlying IP Connectivity Access Network and will require some dialog with the packet and radio nodes (GGSN, SGSN, RNC).

Finally, the UE1 forwards the PRACK message (including the final SDP identifying the selected codec) to the UE2. Note: At this time the resource reservation of UE1 most probably will not be completed.

This message traverses all the nodes in the chain (the path is derived from the Record-Route header of the SESSION PROGRESS message).

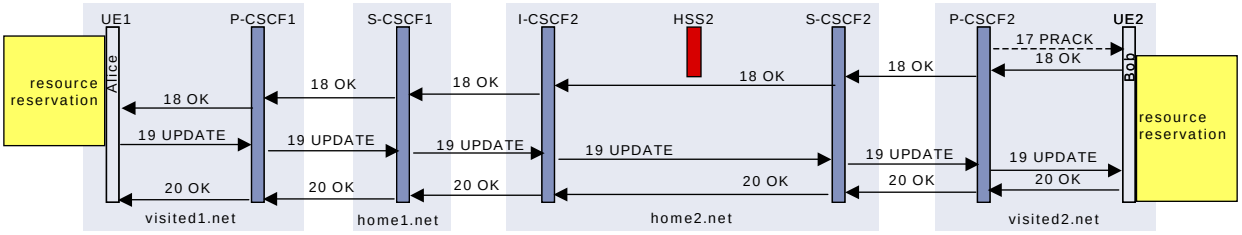


Figure 13: Mobile to mobile call setup (continued)

18 - Upon receipt of the PRACK message the UE2 confirms media streams and codecs by means of the OK message. The OK message traverses all the nodes in the chain back to UE1. When the P-CSCF2 sees the OK message is commences the resource reservation (involving GGSN, SGSN, RNC) at the called side.

19 - When the necessary resources have been reserved at the calling side, UE1 sends the UPDATE message to UE2 (traversing all the nodes in the chain).

20 - As any other message with SDP-content the reception of the UPDATE message will be acknowledged by the UE2 with an OK message (traversing all the nodes in the chain). At this time the UE2 may still be engaged in resource allocation.

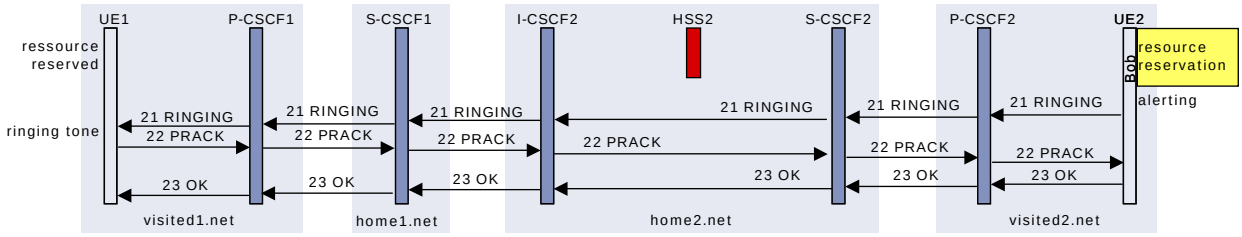


Figure 14: Mobile to mobile call setup (continued)

21 - Once resource reservation has been completed at the called side (as well as at the calling side - these are independent processes which can be completed in any order) the UE2 starts alerting the called party and generates the RINGING message back to UE1.

22 - Upon receipt of the RINGING message the UE1 applies a locally stored ring tone to the caller and sends the PRACK message to UE2.

23 - The PRACK message will be acknowledged by the UE2 by sending the OK message to UE1.

At this stage the called party gets ringing and the calling party hears ring tone.

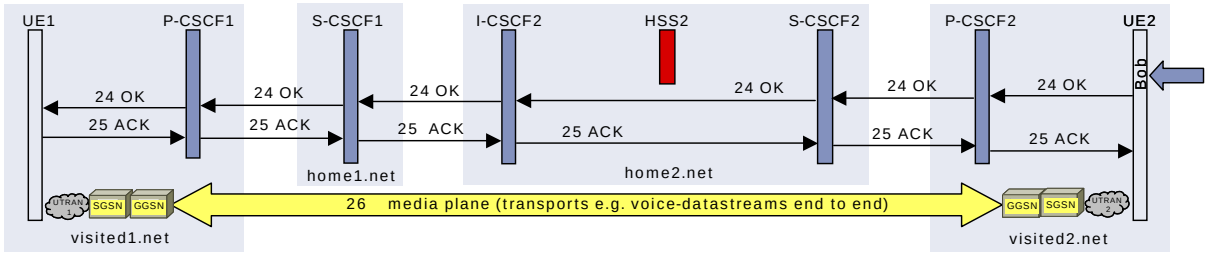


Figure 15: Mobile to mobile call setup (continued)

24 - When the called party answers (i.e. accepts the session) the UE2 sends an OK message, which completes the INVITE-transaction at the called side.

25 - When the OK message has arrived, the UE1 stops ring tone and forwards the ACK message to UE2 to acknowledge the establishment of a session.

26 - The session set up is now completed and both parties can generate their audio and video streams. These media streams are sent end-to-end (UE1<->UE2) via the media plane

5 CALL ORIGINATION TO A PSTN TERMINAL

This chapter describes how the mobile UE sets up a session to a PSTN terminal while the mobile IMS UE is roaming in a visited network.

Assumptions:

- The network to which the mobile UE is attached provides IMS services (long term vision).
- The mobile UE is roaming and is equipped with an UICC (Universal Integrated Circuit Card) which include an ISIM application (ISIM is IMS specific while USIM is only UMTS specific).
- The Home Network of the mobile UE does not involve an I-CSCF.
- Based on the destination address and operator agreements the session is handled by the BGCF of the home network of the mobile UE.
- Based on the home network configuration the BGCF does not remain in the signalling path after MGCF has been selected.
- No IMS Application Server is involved at the calling side.

Figure 16 shows an overview of the involved networks and nodes/functions in the call/session set up.

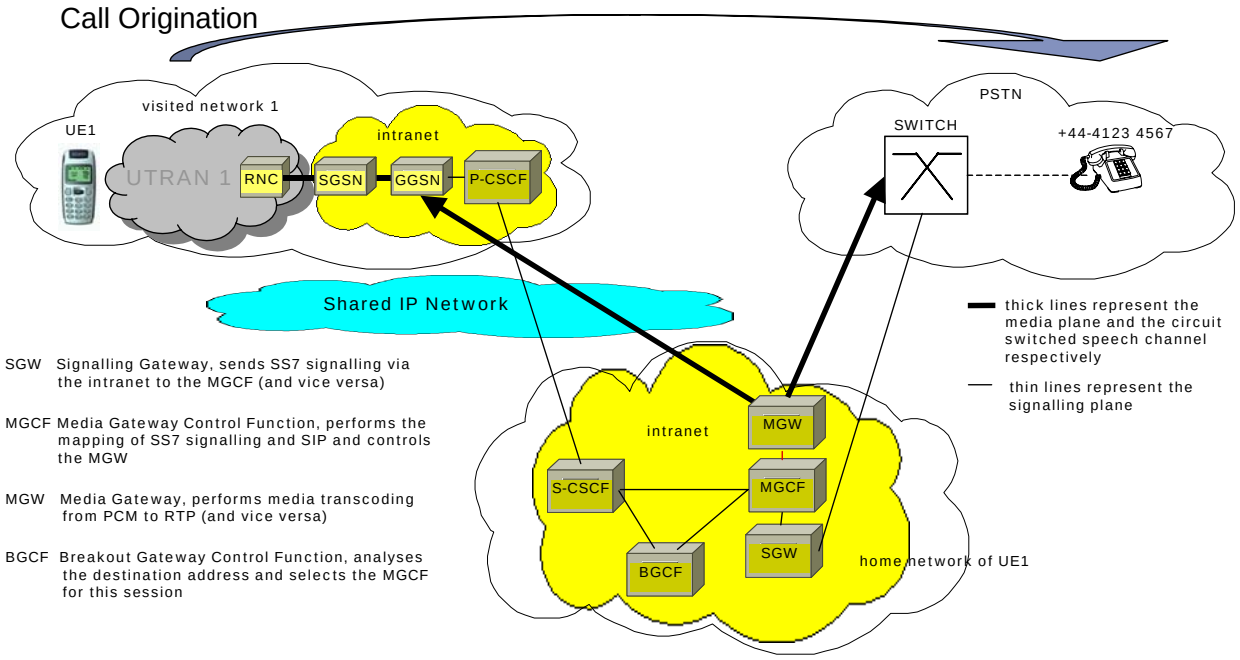


Figure 16: Overview of mobile to PSTN call

Figure 17 shows the total signalling flows.

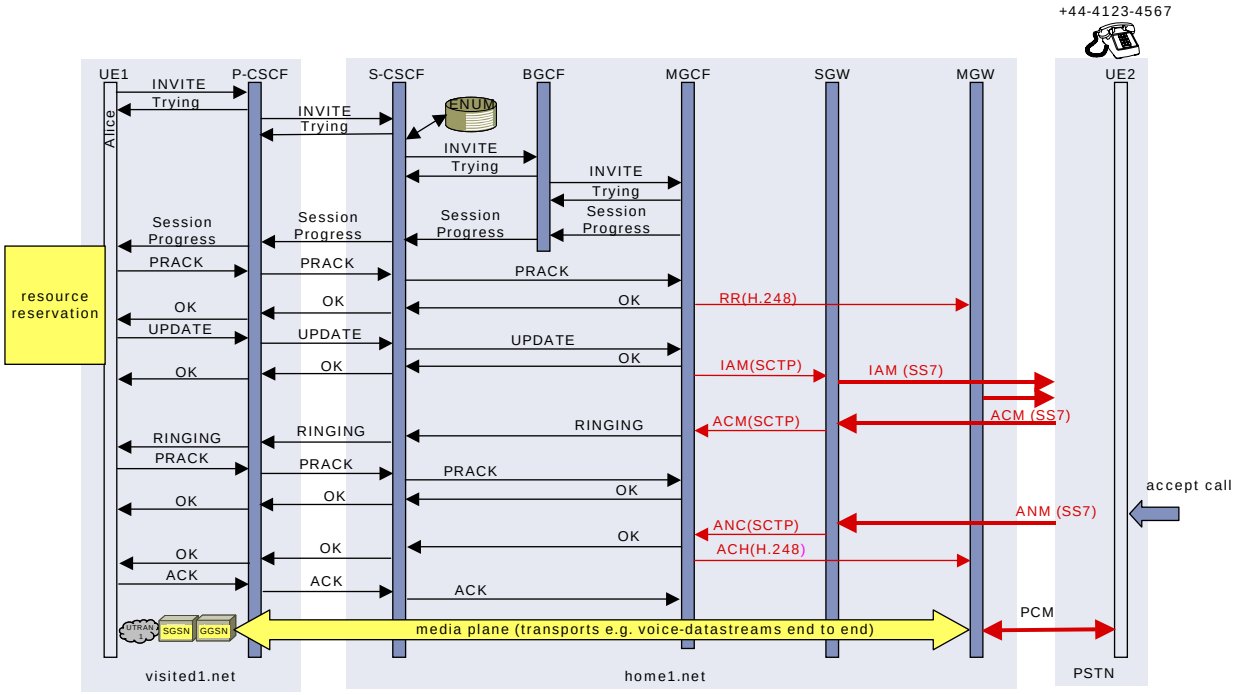


Figure 17: Overview of signalling flows
(SIP messages are black, SS7/MAP messages are red)

The signalling flows are now examined in more detail.

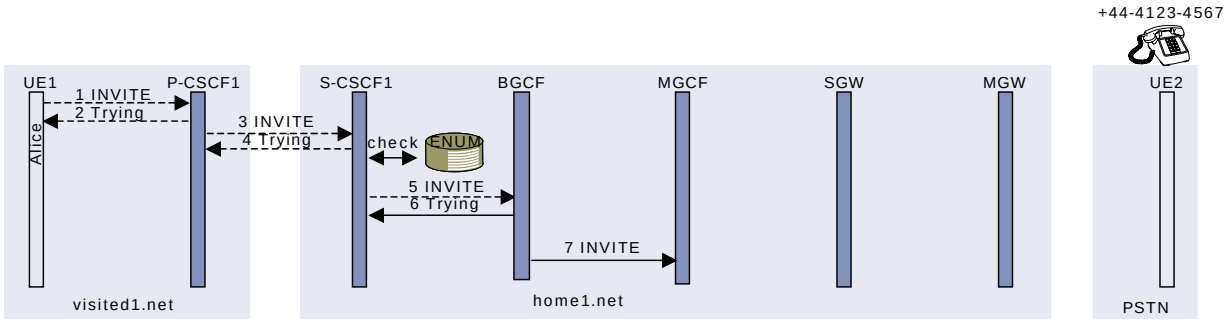


Figure 18: Mobile to PSTN call setup

1 - UE1 sends the SIP INVITE message to its P-CSCF. It includes:

a) the Public User Identity of the called party, which is a TEL-URI (tel: +44-4123-4567)

b) the IP address and port number where the UE1 expects a response as well as the information for signal compression and the transport protocol used to the next hop (e.g UDP, TCP, SCTP). Note: Every node in the chain is free to choose its appropriate transport protocol

c) the IP address and port number to which the UE1 expects subsequent responses after the response to the INVITE message

d) a route list (list of SIP proxies which serve the UE1 and which to be traversed, e.g PCSCF1@visited1.net and SCSCF1@home1.net)

e) the P-Preferred Identity of the UE1 user (”Alice Jones” alice@home1.net) if the user has more than one Public User Identity, to indicate which one is to be used for this session (to be included in the charging record, to be shown to the called party, to trigger different services)

f) the type of access network used by UE1 (eg UTRAN) for service customization and determination of available bandwidth as well the radio cell ID which implicitly contains some location information to be used for local services like e.g. ”list of local dentists”. Note: This information is transferred down to the home network but not further!

g) end-to-end information explaining who is calling (tel: +44-4987-6543), who is called (tel: +44-4123-4567), and the Call-ID

h) additional information like e.g. SIP-extensions to be used/supported and the audio and/or video codec format supported by the UE1.

2 - Upon receipt of the INVITE, by means of sending the TRYING message the P-CSCF1 returns an acknowledgement back to the UE1 (to inform the sender of the INVITE that his message has been reliably received by the next hop in the chain).

3 - Next, the P-CSCF undertakes some internal checks and procedures. It:

- checks if Route Header is correct and includes the S-CSCF in the home network
- checks the requested media parameters against the policy of the visited network operator (e.g. G.711 codec not allowed because of 64 kb/s-bandwidth necessity)
- checks the P-Preferred Identity against the list of all the Public User Identities received during the Terminal Registration-Process, and replaces the P-Preferred Identity with the P-Asserted Identity in the INVITE message sent onwards to the S-CSCF. If the there is not a match, the P-CSCF selects one Public User ID out of its list. If there is a match, it puts the received Public User ID into the P-Asserted Identity header. This check provides authentication of the Public User ID
- removes/modifies some Headers (e.g which relate to security or signal compression) and insert charging headers in the INVITE message)
- puts its identity (SIP URI) into the Record Route Header .

If all the checks were passed, the P-CSCF1 forwards the modified INVITE to the S-CSCF1 (or to the I-CSCF of the home network operator 1).

4 - S-CSCF sends TRYING message back to P-CSCF.

5 - Upon receipt of the INVITE, the S-CSCF allocated to the UE1 identifies the user by means of the value in the P-Asserted-Identity header and retrieves the User Profile which was already downloaded during Terminal Registration. Next the S-CSCF:

- evaluates the filter criteria stored in the User Profile (to find out if and which Application Servers need to be involved,
- checks SDP-parameters against local network policy (e.g. codec format, because user has a cheap subscription which does not allow some media or high speed codecs),
- analyses the called address, which will be a TEL URI. The S-CSCF contacts ENUM. In this case of a call to the PSTN ENUM will not return a SIP URI. It may return a negative response (RCODE =3) or a TEL URI. Both these possibilities trigger the S-CSCF next to contact the BGCF (Breakout Gateway Control Function, specialized in routing SIP requests based on telephone numbers),
- adds the TEL URI of the caller to the P-Asserted-Identity header of the INVITE message. This is used to enable the PSTN to identify the caller. The S-CSCF forwards the modified INVITE message to the BGCF.

6 - Upon receipt of the INVITE the BGCF returns the TRYING message and

7 - analyses the destination address (i.e. the TEL URI). Based on agreements the home network operator may have for call termination in the PSTN, the BGCF decides whether the session should be handled by a local MGCF or by a remote MGCF.

If the session to be handled locally, the BGCF further decides if it wants to stay in the chain of nodes traversing the further message flow or not (i.e. whether or not it should insert its own SIP ID into the Record Route header of the INVITE message). The BGCF then routes the INVITE message to the MGCF (in our example to a local MGCF, and announces that it does not wish to remain in the signalling path for the rest of the session).

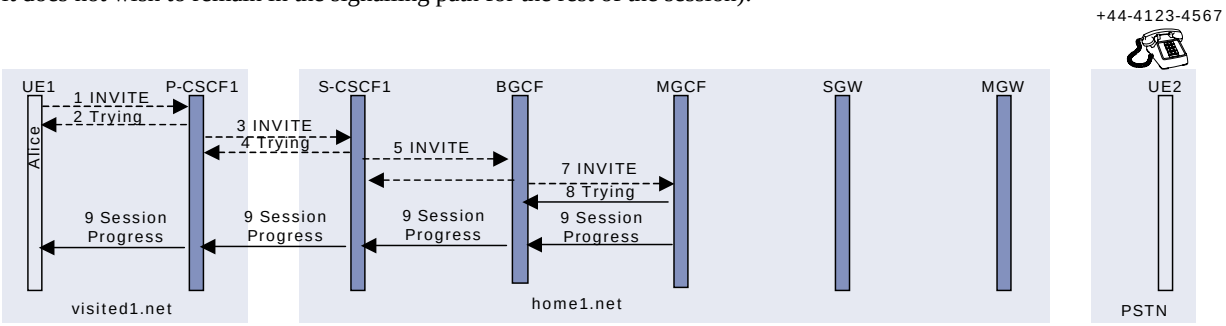


Figure 19: Mobile to PSTN call setup (continued)

8 - Upon receipt of the INVITE message the MGCF returns the TRYING message and

9 - Then the MGCF selects the SGW and MGW to be used for this session to meet the required preconditions (one MGCF can control many SGW and MGW). The MGCF then responds with a SESSION PROGRESS message that contains an SDP answer to communicate the media streams and codecs the MGW is able to handle. The SESSION PROGRESS message sent by the MGCF back to UE1 includes an SDP body as well as advice for the UE1 to send an updated SDP and to communicate when terminal resource reservation on calling side is completed (the calling and the called party will be alerted only when resource reservation has been completed on both sides).

Next, the MGCF inspects the P-Asserted-Identity header to extract the identity of the caller.

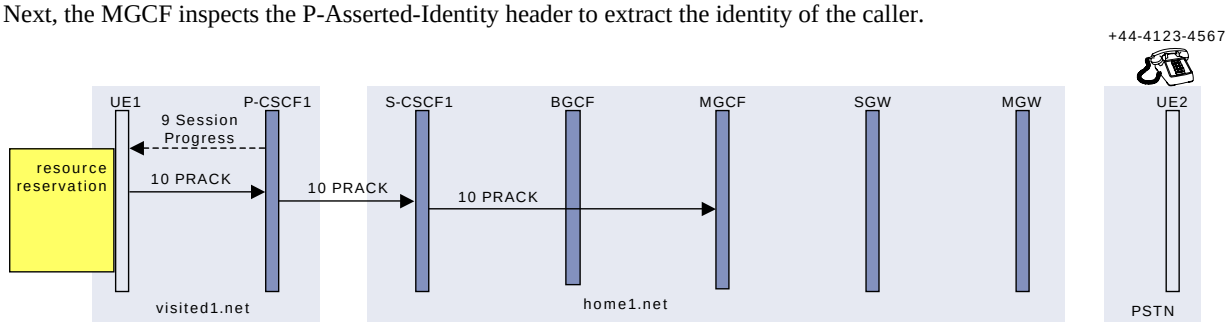


Figure 20: Mobile to PSTN call setup (continued)

10 - Upon receipt of the SESSION PROGRESS message (which includes the IP-address of the reserved PCM channel at the MGW as well as the Route Header field without the address of the BGCF) the UE1 is informed:

- whether or not the UE2 accepts a session with the media streams proposed (for the time being only audio is specified)
- what codecs are supported at the MGW connected to the called PSTN network.

The UE1 now selects a codec that is supported at both ends for the audio stream.

Then the UE1 starts resource reservation. This is a procedure that is dependent on the underlying IP Connectivity Access Network and will require some dialog with the packet and radio nodes (GGSN, SGSN, RNC).

Finally, the UE1 forwards the PRACK message to the MGCF. Note: At this time the resource reservation of UE1 most probably has not been completed.

The PRACK message traverses all the nodes listed in the Record-Route header of the SESSION PROGRESS message.

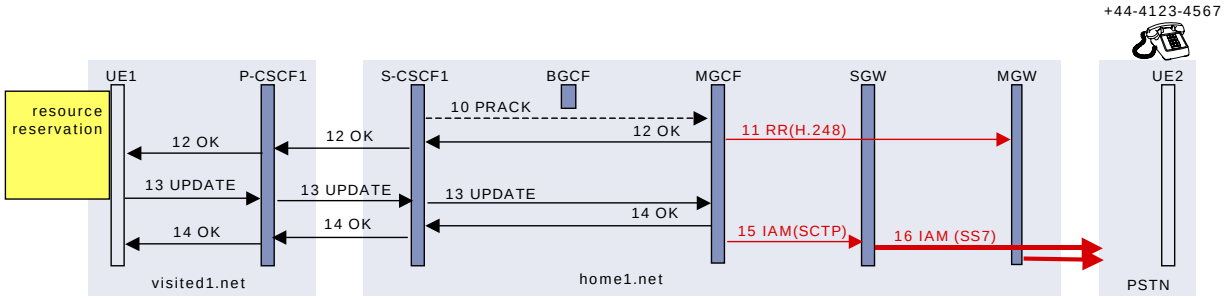


Figure 21: Mobile to PSTN call setup (continued)

11 - Upon receipt of the PRACK message the MGCF starts resource reservation RR in the MGW. The messages between the MGCF and the SGW are typically transported over SCTP, the interaction with the MGW is based on H.248.

12 - Then the MGCF confirms final codec format by means of the OK message. The OK message traverses all the nodes in the chain back to UE1.

13 - When the necessary resources have been reserved at the calling side, UE1 sends the UPDATE message to MGCF (traversing all the nodes in the chain).

14 - As any other message with SDP-content the reception of the UPDATE message will be acknowledged by the MGCF with an OK message (traversing all the nodes in the chain).

15 - The MGCF triggers the SGW to establish a speech path through the PSTN down to the called party.

16 - This request is transcoded by the SGW into SS7 signalling (the Initial Address Message). In parallel the PCM speech channel is set up between MGW and the PSTN.

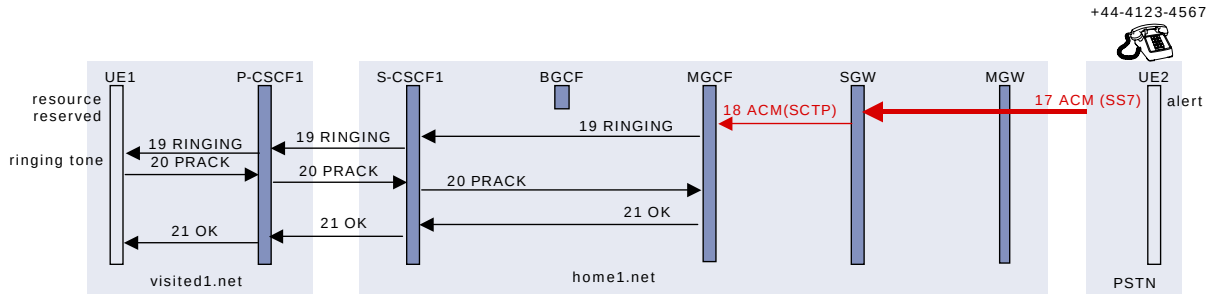


Figure 22: Mobile to PSTN call setup (continued)

17 - When the circuit switched path through the PSTN is set up, the SGW receives on SS7 side the ACM (Address Complete Message) from the PSTN, which indicates that the called party is alerted.

18 - The SGW passes the ACM to the MGCF (packed into SCTP).

19 - The MGCF performs the mapping of SS7 signalling and SIP and thus, sends the RINGING message back to UE1.

20 - Upon receipt of the RINGING message the UE1 applies locally stored ring tone to the caller and sends the PRACK message back to the MGCF.

21 - The PRACK message will be acknowledged by the MGCF by sending the OK message to UE1.

At this stage the called party gets ringing and the calling party hears ring tone.

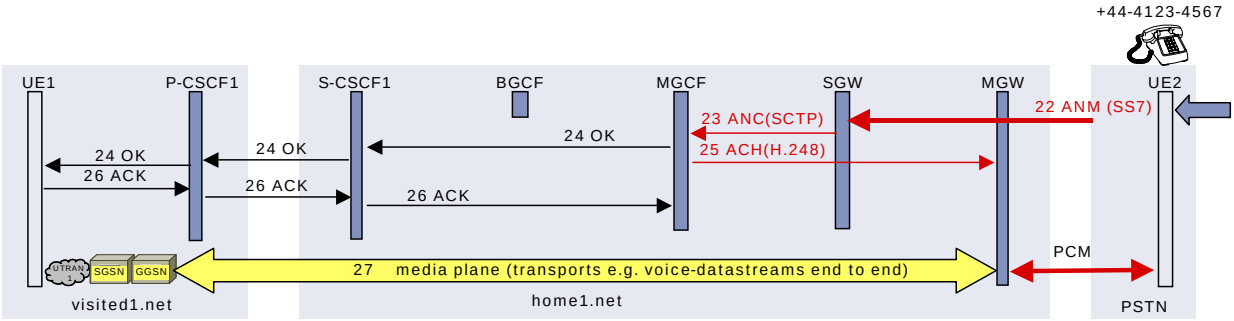


Figure 23: Mobile to PSTN call setup (continued)

22 - When the called party answers the SGW receives the SS7 message ANM (Answer Message).

23 - The reception of the ANM is communicated to the MGCF by means of the ANC (Answer Signal, Charge) over SCTP.

24 - The MGCF sends an OK message to the UE1 which completes the INVITE-transaction at the called side and

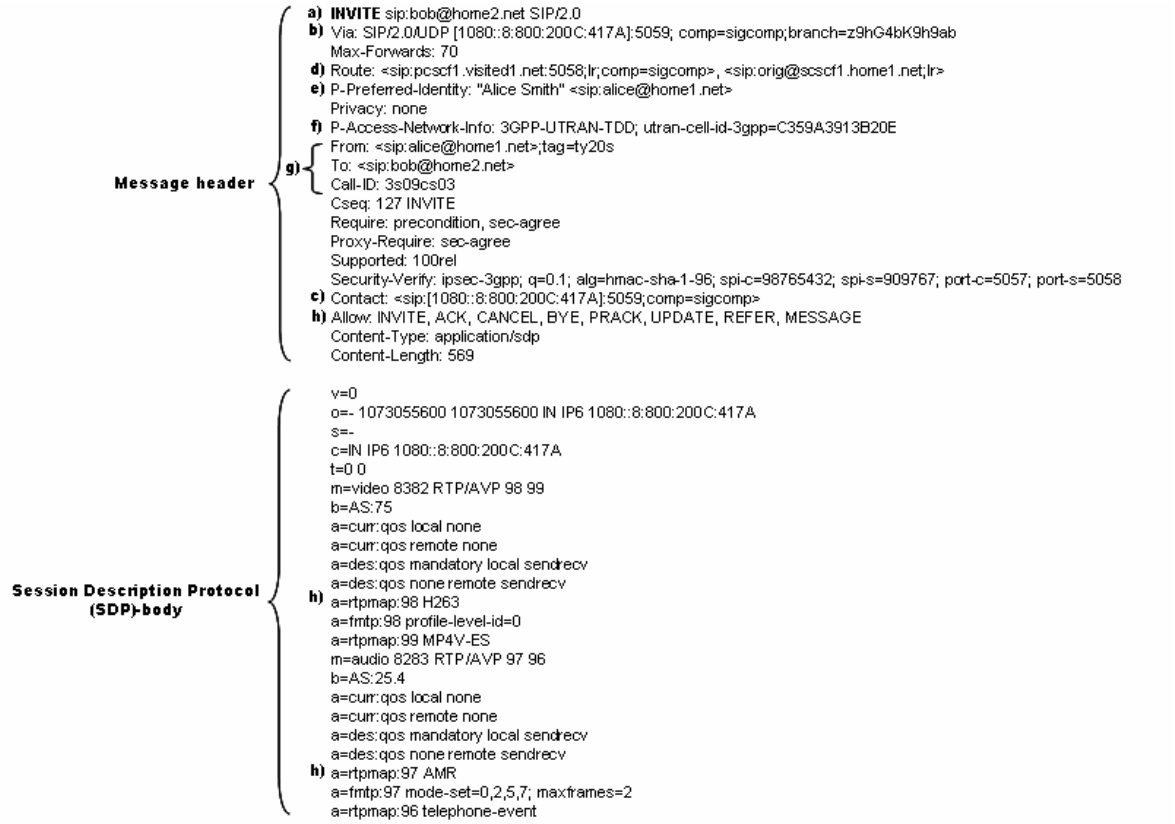
25 - requests the MGW to activate the PCM channel in forward direction (ACH=Activate Channel).

26 - When the OK message has arrived at the UE1 it stops ringing tone and forwards the ACK message to MGCF to acknowledge the establishment of a session.

27 - The session set up is now completed and both parties can generate their audio streams. These media streams are sent end-to-end (UE1<->UE2) via the media plane.

APPENDIX A: EXAMPLES OF SIP MESSAGES

SIP INVITE sent by the calling UE



a) - h) refer to the explanations provided to message 1 in Figure. 8

Note: The information marked with g) is not inspected by any network node. Therefore the user can insert into the FROM Header any value, even a SIP URI not belonging to him!

Example of SIP INVITE received by the called UE

```
INVITE sip:[1081::5:800:200A:B2B2]:5055;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5056;comp=sigcomp;
branch=z9hG4bK2a2qr
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bKvp2yml
Via: SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bKra1ar
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bKs1pp0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bKoh2qrz
Via: SIP/2.0/UDP [1080::8:800:200C:417A]:5059;comp=sigcomp;
branch=z9hG4bK9h9ab
Max-Forwards: 65
Record-Route: <sip:pcscf2.visited2.net:5056;lr;comp=sigcomp>
Record-Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "Alice Smith" <sip:alice@home1.net>,
<tel:+1-212-555-1234>
P-called-Party-ID: <sip:bob@home2.net>
Privacy: none
P-Media-Authorization: 00200001001001017064663l2e686f6d65312e6
e6574000c02013942563330373200
From: <sip:alice@home1.net>;tag=ty20s
To: <sip:bob@home2.net>
Call-ID: 3s09cs03
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[1080::8:800:200C:417A]:5059;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: 569

v=0
o=- 1073055600 1073055600 IN IP6 1080::8:800:200C:417A
s=-
c=IN IP6 1080::8:800:200C:417A
t=0 0
m=video 8382 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 8283 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

APPENDIX B: 3GPP RELEASES

The following table summarises the various 3GPP Releases.

Release	Frozen	Contents
Release 99	December 1999	Defines UTRA and many other initial features. The basis for early 3G deployment.
Release 4	March 2001	Enhancements to Release '99 plus separation of control plane from user plane in core network. First steps towards IP-based operation. Also defines the low chip rate TDD mode (TD-SCDMA)
Release 5	June 2002	Further enhancements. Introduces: IMS – IP-based Multimedia Services HSDPA – High Speed Downlink Packet Access
Release 6	December 2004	Includes 2nd Phase of IMS, High Speed Uplink, MBMS, Presence, AMR-WB extension for high audio quality, plus many other features designed to deliver the full 3G experience
Release 7	Due mid 2007	Many features planned, including: • Various enhancements • IMS, LCS, video and voice services, radio, codecs, security, LI etc) • 7.68 Mcps TDD • 3.84 Mcps TDD Enhanced Uplink • Multiple Input Multiple Output antennas (MIMO) • Rel-7 Improvements of the Radio Interface (UMTS2600, UMTS900, UMTS2600 TDD Option, UMTS1700) • PS domain and IMS impacts for supporting IMS Emergency calls • System enhancements for Fixed Broadband access to IMS (FBI) • Advanced Global Navigation Satellite System (A-GNSS) concept • Multimedia Telephony Capabilities for IMS • Transferring of emergency call data to Public Service Answering Point (eCall) • Development of UEA2 and UIA2 Algorithms (back up for Kasumi)

Table B1: 3GPP Releases