IMS Release 10 Tutorial

Silvia Scalisi
University of Trento

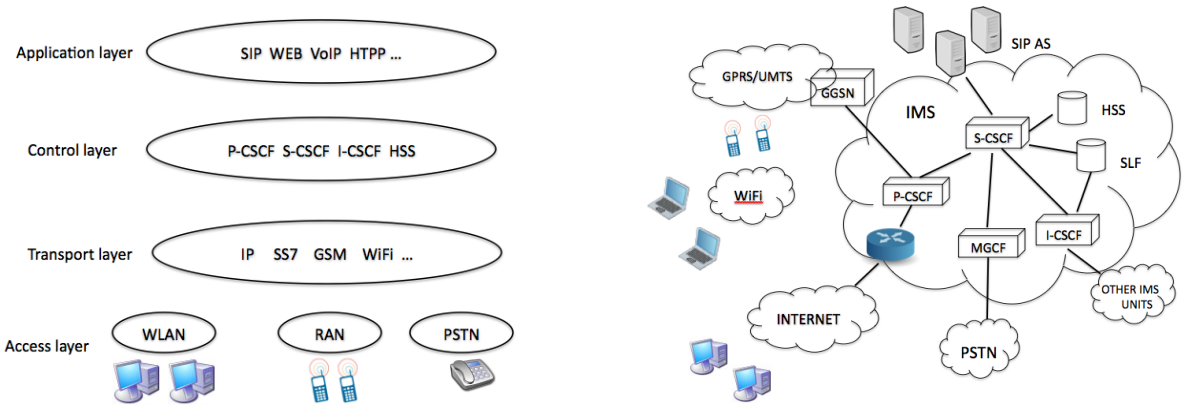
1 Introduction

The IP Multimedia Subsystem (IMS) is a network architecture that delivers services based upon the Internet protocols to mobile users.The idea behind IMS is to bring multiple media, multiple point of access and multiple modes of communication into a single network, enabling end-user experiencing simultaneous voice, data, and multimedia sessions.
Potentially, all the 3G users through the packet switched domain can experience all the power of Internet, so it seems that IMS is an unnecessary technology. Then, why IMS is a promising technology? The packet switched domain provides a best effort service to the users, with no guarantee about the amount of bandwidth a user get for a connection and the delay experienced by the packets: this results in a unstable quality of the conversation or videoconference that can lead, in the worst case, to the frustration of the user in using real-time multimedia service. Moreover, IMS is not only about providing new services but all the services, the ones currently provided by Internet and the future ones.

IMS is an end-to-end architecture that is intended to be "access independent", which means that the services delivery is implemented regardless of the device (mobile phone, cable,..) and the access medium (WiFi, land-line,...). Furthermore, the services are reachable by the user even if they are roaming and when they are far away by their home network.
The Session Initiation Protocol (SIP) has been chosen as a signaling mechanism to control all the traffic in the network, allowing all network entities to communicate with one another regarding service delivery network-wide. Important tasks are performed by the SIP protocol, like enabling two users to communicate, establishing and negotiating a multimedia session between the two.
The tutorial is divided in these sections: the section 2 gives an overview about the architecture of the IMS introducing the main entities and their functionalities; section 3 introduces the IETF protocol SIP and how this is handled by the IMS entities. Section 4 instead refers to the work items of the IMS Release 10 and it is subdivided in three subsections: the first on refers to the enhancement of IMS, the second is the alignment of the IMS to the SIP protocol, and finally study about the future evolution of the IMS.

2 IMS Architecture

The IMS is a three-layered architecture comprised of the *transport layer*, *application layer* and *control layer*, in which the *transport layer* works as an entry/exit point for IMS network and it consists of routers and switches; the *control layer* contains all the CSCF entities to support the call session control; finally, the *application layer* includes the application and media servers which process and store data and generate services for the subscribers (see Fig. 1a).
The main entities of the IMS architecture are depicted in Fig. 1b. The core of the IMS architecture is the *Call Session Control Function* or CSCF. The CSCF performs all the signaling operations, manages SIP sessions and coordinates with other network entities for session control, service control and resource allocation. It consists of three different entities: the *Proxy-CSCF* (P-CSCF),



(a) Three-layered Structure

(b) IMS Architecture

Figure 1: *IP Multimedia Subsystem*

the *Interrogating-CSCF* (I-CSCF) and the *Serving-CSCF* (S-CSCF).

The access point to IMS is the P-CSCF and, as the name suggests, it acts as a SIP proxy server for all the user equipments. Through the P-CSCF doesn't pass bearers of traffic but all the SIP signaling from a user. P-CSCF is only a point of access to IMS and does not authenticate within the IMS. The S-CSCF is responsible for confronting devices that try to establish session without being registered in the network.The P-CSCF has knowledge of all the sessions created through it: if an user loses the connection to the IP network, the P-CSCF is notified and it sends a CANCEL message to all the devices engaged in the session with the user.

While the P-CSCF is the first contact for the user, the I-CSCF acts as a gateway for the IMS network, and it is located at the edge of each administrative domain. It grants or not the access to the operator network by external network forwarding SIP messages, protecting in this way entities like the S-CSCF and the HSS. The I-CSCF has in charge the location of the user, possibly by using a *Subscriber Location Function, (LSF)*: locating a user means to determine the S-CSCF that serves that user as well as the HSS in which his data are stored. The most important role for the I-CSCF is the assignment of a S-CSCF for a user, according to the service that must be supported or based on the geography, that is based on the closeness to the I-CSCF; the S-CSCF assignment is then stored in the HSS for further reference.

The S-CSCF is the core of the IMS, providing the point of control within the network that enables operators to control all service delivery and all sessions. The S-CSCF is a SIP server having in charge of handling all the aspects of the services for a subscriber, maintaining the status of the sessions the user has initiated and controlling and delivering of the content. The S-CSCF has knowledge of all the services subscribed by the users, by downloading from the HSS the user's service profile, and it has the responsibility of enabling such services by contacting the appropriate Application Server.

The *Home Subscriber Server, HSS* is a database that contains all subscribers' data, like the services that is allowed to access, the network in which he is granted to roam and the information about the location of the subscriber. Once information about the subscriber has changed, the entire profile is sent to the S-CSCF making it always synchronized with the HSS.

An important function of the HSS is to provide the encryption and authentication keys of the user: when a user registers himself in the network, he must provide the credentials to the S-CSCF and these are checked against the one stored in the HSS.

Another part not properly belonging to the IMS is the *Media Gateway Control Function, MGCF* that connects the Public Switched Telephone Network (PSTN) domain with the IP/SIP domain, creating in this way a bridge between the SS7 signaling with the SIP signaling in IMS. All the messages arriving from SS7 first passes through the MGCF that maps these messages into SIP

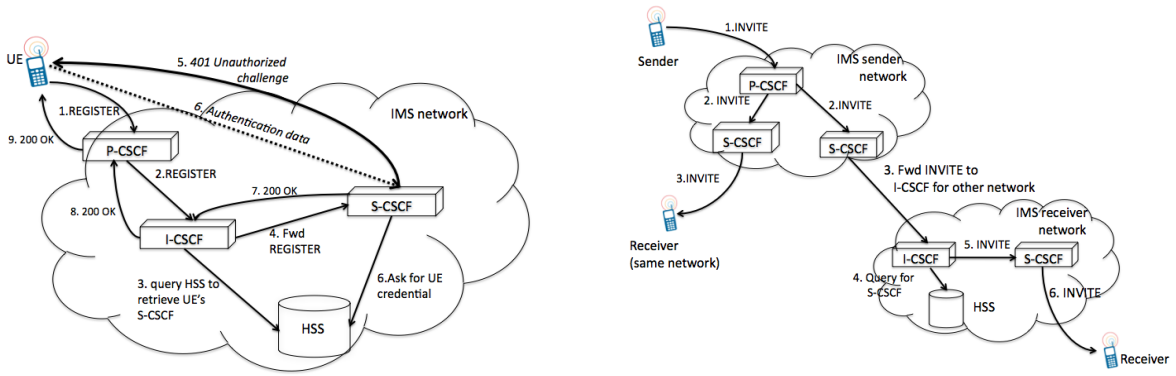
request and then they reach the P-CSCF.

3 SIP within IMS

The *Session Initiation Protocol* (SIP) is the basis of the IMS. It has been chosen by the 3GPP group for the flexibility, simplicity of the request-response interaction model, extensibility, interoperability with existing telephony system, like PSTN. IMS SIP enables all the communications in the network and it controls all the actions performed by the users.
Among the several functionalities of SIP in the IMS architecture, the most important are the location of the user, the spotting of the media involved in the session and their parameters, the creation of a session both in the caller and the receiver side and the management of the parameters for a session.

3.1 SIP Procedures: User registration and Session Initialitation

In order for the IMS architecture to route calls for a UE, it must first know where the UE is actually located: that's why the network requires that all the UEs register to the network when they are activated. Once the UE changes its location, it must re-register itself to the network to provide the updated location information. The registration of an UE in the IMS system is depicted in Fig. 2a. SIP registration allows the UE to use the IMS service and to bind his *public URI* to a URI that contains the IP address of the terminal where the user is logged in. During the registration phase, the UE sends a SIP REGISTER message to the point of access for the IMS network, the P-CSCF; this one must locate the I-CSCF for the subscriber's home network. The I-CSCF now queries the HSS in order to retrieve, if present, the S-CSCF for that UE or in the other case a new one is assigned. Once the REGISTER message arrives to the S-CSCF, it challenges the UE with a *401 Unauthorized* response to obtain from UE the authentication data that are checked against the data stored in the HSS. If the credential are verified, the *200 OK* response is returned back to the UE.
Fig. 2b depicts all the step involved in the establishment of a session for a user that wants to start a communication with another one. As usual, the P-CSCF is the first point of contact for the SIP INVITE message forwarding. After receiving the SIP INVITE, the P-CSCF determines whether the called party resides in the same network or not: if they both are in the same network, the P-CSCF will contact the assigned S-CSCF for called user and forwards the INVITE to that S-CSCF; now, it is in charge of the S-CSCF to send the INVITE to the final receiver. If the called party is in other IMS network, the P-CSCF should locate the I-CSCF for accessing the external network, that will have in charge the location of the user and the routing of INVITE message. Upon receiving the INVITE message, I-CSCF queries the HSS to gather the name of the S-CSCF for the user. The response of the HSS contains the actual location of the user or a *480 temporary unavailable* if the user belongs to that network and has not registered; it can also contain no information because the user is not belonging to that network and the I-CSCF returns a *404 Not Found* to the originator.
In the case in which the user is registered, the INVITE is forwarded to the S-CSCF and finally delivered to the receiver. The receiver sends back to the caller a *200 OK* message to the caller and the last sends an *ACK* to the other party: at this point the *SIP dialog* is successfully established. During these steps, the two parties negotiate the resources: the receiver examines the SDP content of the INVITE messages and determines whether it is able to support the media type and the requested parameters.
Any established session might need to change parameters while it is in progress: this is done by the sending to the participants or a subset of them a new INVITE or an UPDATE message that brings the current description of the session and the change to be made.



(a) IMS Registration

(b) IMS Session Establishment

Figure 2: *IP Multimedia Subsystem*

The termination of a session is done by sending a BYE message to all the participants of the session. Each of the participants send back a 200 OK message.

4 IMS Release 10

4.1 IMS Enhancements

In this section, there will be presented some improvements on the architecture to support and enhance IMS services. In particular, the interworking between the CS and the IMS domain at Home NodeB (HNB), the maintenance of service continuity even if all media streams or part of them are transferred between different UE's terminals, the enhancements of emergency services and the deployment of PSS and MBMS services as IMS services.

3GPP TS 23.832 [8] describes an IMS enabled HNB SubSystem (the Home NodeB and the Home NodeB Gateway) as an extension to the HNB capabilities, such as the possibility to offload the traffic from the CS Domain to IMS: to achieve the cooperation between IMS and CS, for example, the HNB should be able to translate the service in the CS domain in an IMS equivalent service. Possible alternatives for IMS capable HNB are presented, the first one is depicted in Fig. 3: The

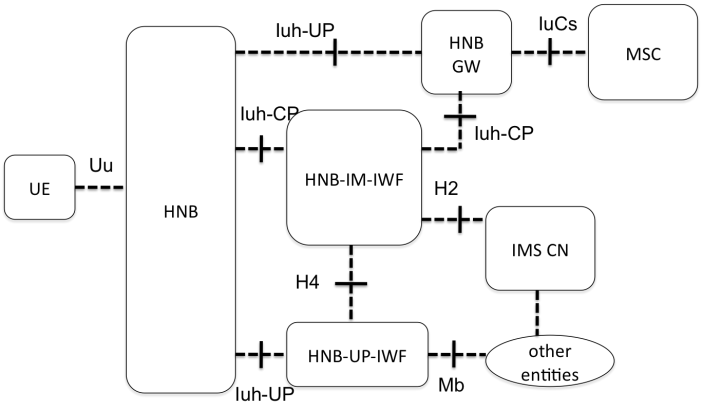


Figure 3: *Home NodeB architecture*

functional entities described in Fig. 3 are:

- HNB-IM-IWF: it is a logical entity that terminates the NAS (Non Access Stratum, i.e. the layer between the Core Network and the UE) control plane for the UE. It decides if the chosen domain is IMS or CS for a particular service: if it is CS, the service request is forwarded to the interface towards the MSC; it interworks NAS signaling with SIP (NAS/SIP-IWF) if the chosen domain is IMS; it acts as HNB-UP-IWF controller to setup and teardown on UP bearers over Iuh interface and IMS bearers towards IMS.
- HNB-UP-IWF: it interworks Iu-h user plane to Mb. HNB-UP-IWF gets bearer set up, interworking and teardown commands from HNB-IM-IWF over H4 reference point.

In this architecture, an example of procedure is the attach procedure by a UE done by sending a message to the HNB-IM-IWF. This one, based on the IMSI and LAI, retrieves the VLR to update the location; it will be the MSC to update the location information on the HSS. After the location update, the HNB-IM-IWF registers the UE towards IMS: at the end of this procedure the UE is registered in the IMS and CS domain.
Fig. 4 depicts the logical architecture for the second alternative:

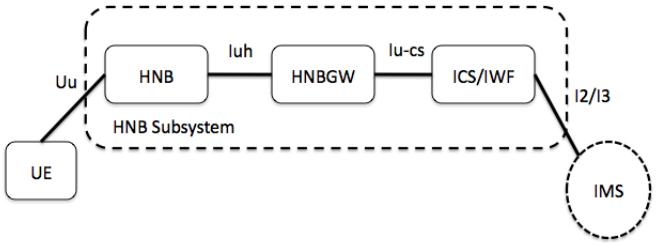


Figure 4: *IMS capable HNB Subsystem using IMS centralised services IWF*

The ICS/IWF controls all the signaling between the user and the network through the Iu-cs reference point and allows the interworking with IMS: in particular, the IMS functionality (SIP UA) is performed by the IWF and contains functions equivalent to MSC server. The only IMS enhanced entity is the ICS/IWF, neither UE, or the HNB or the HNB GW need to be enhanced by IMS specific functions.
Another proposed alternative is the one depicted in Fig. 5:

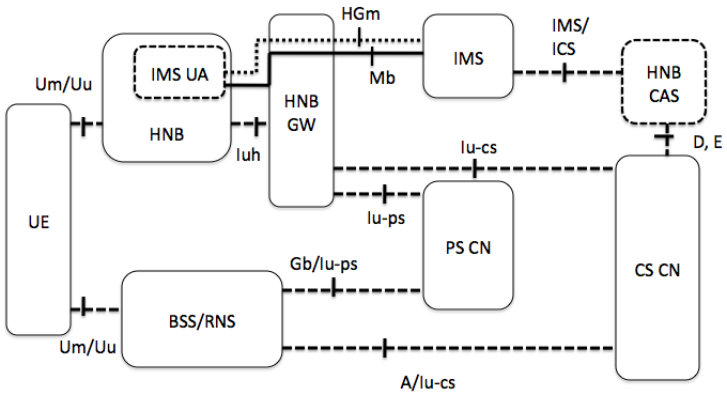


Figure 5: *IMS HNB Reference Architecture with HNB-CAS*

CS-to-IMS interworking is done at the HNB level. In particular, HNB is enhanced with a IMS

User Agent that performs IMS registration in behalf of the HNB and encapsulates information from the radio interface, arrived form Uu/Um, into SIP header and payload destined to the IMS core.
As can be seen in Fig. 5, a new entity is the HNB CAS. The HNB CAS (HNB Convergence Application Server) acts as an Application Server in the IMS network and provides interworking between the IMS UA inside the HNB, the IMS Core and the CS Core Network. The HNB CAS provides CS Domain service to UE utilizing the IMS core by simulating most of the Visited MSC functions. Among its functions, the voice and message convergence, i.e. the routing of calls/messages to/from UE, handover between HNB and a neighbouring macrocell.
Two reference points are depicted in Fig. 5: the *Mb*, used for RTP bearer traffic between the HNB and IMS P-CSCF and *HGm* for the SIP signaling between the same entities as before.
In the same TS other architecture alternatives are listed but they are not covered on this tutorial. Not all the alternatives listed in the TS are recommended for standardization, the effort for the 3GPP standardization are put on the second alternative.

IMS enablest the deployment of IP multimedia applications. The 3GPP TS 26.237 [9] describes how IMS enablers and features make operators and subscribers experience PSS and MBMS services. The 3GPP Packet Switch Streaming (PSS) is a framework that provides IP based streaming application by specifying protocols and codecs within the 3GPP system. 3GPP Multimedia Broadcast and Multicast Service (MBMS) provides a framework for broadcast and Multicast streaming and download applications in 3GPP networks supporting the MBMS bearer service. IMS allows to start and control PSS and MBMS services. The reference architecture can be seen in Fig. 6:

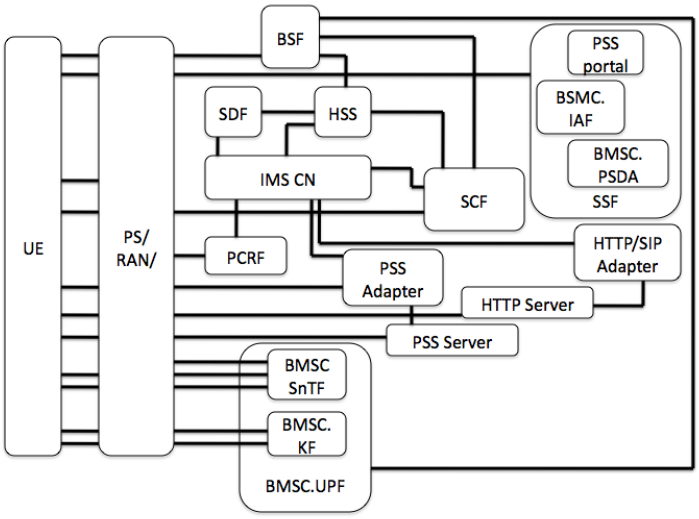


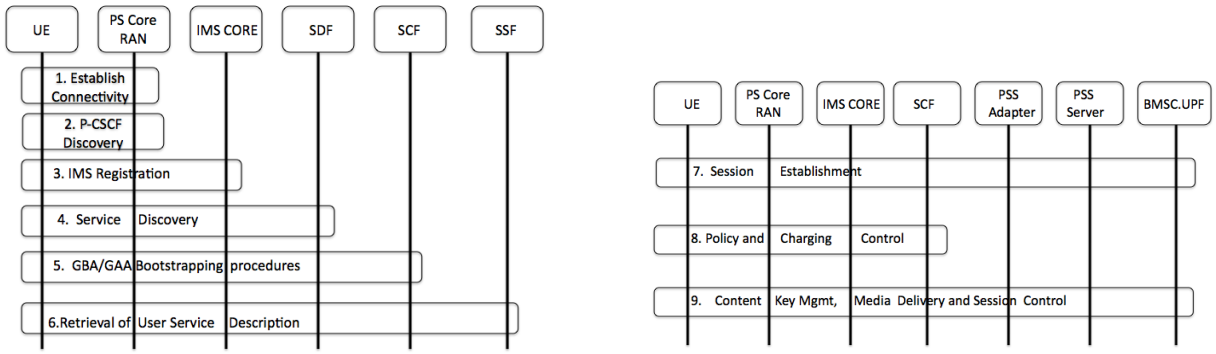
Figure 6: *IMS based PSS and MBMS architecture*

Relevant entities in the architecture in Fig. 6 are the following:

- SDF, *Service Discovery Function*:it is an entry point to the client to attach to the service provide by the service provider.
- SSF, *Service Selection Function*: it provides the service selection information, i.e. a list of available PSS and MBMS services that the UE can browse and select.
- SCF, *Service Control Function*: it performs service authorization during session initialization and its modification, which includes checking PSS and MBMS user's service subscription in order to allow or deny access to the service

- BSF, *Bootstrapping Server Function*: it provides application independent functions for mutual authentication of UE and servers unknown to each other and for bootstrapping the exchange of secret session keys afterwards.
- PSS Adapter: this entity performs bi-directional protocol translation between SIP and RTSP to offer control of PSS servers; it proxies RTSP messaging from the UE and SIP/RTSP translation towards the PSS server.
- PCRF, *Policy and Charging Rules Function*: this function controls the charging and the establishment of resources in the RAN and PS core network.
- PSS Server: It contains media control and media delivery functions.
- BMSC.UPF: it contains all BMSC (Broadcast-Multicast - Service Centre) User Plane sub-functions.

Fig. 7 depicts the procedures from the connection establishment to the User Service Description Retrieval in IMS based PSS and MBMS:



(a) Procedure Overview- Part 1

(b) Procedure Overview- Paert 2

Figure 7: *IMS based PSS and MBMS US procedures overview*

The steps in Fig. 7a are the following: the first 3 steps are the procedure described in the previous sections, the 4th step is the service discover, allowing the client to be informed of the available Service Providers. GBA/GAA bootstrapping procedures authenticate the User for signalling outside IMS and generates the Long Term Key that will be used during content key management procedures; step 6 allows the client to obtain the services session information for the select provider. In Fig. 7b the session allows the client to initiate PSS or MBMS session to retrieve content; the last step, instead, is necessary to generate and distribute the keys to provide secure delivery of content of User. At this point, the delivery session is established and the user receives content.
More details about some of the steps mentioned above:

- Service Provider Discovery: discovery of SDFs, by sending a DNS SRV request to a DNS Server. The output of the DNS SRV lookup is a list of domain name, each pointing to a SDF server available within the specific domain.
- User Service Discovery: discovery the addresses of SSF, and this list is provided to the UE based on the UE capabilities and user's service profile, exposed in a SIP SUBSCRIBE sent to IMS CN subsystem. The NOTIFY message sent by the SDF contains the SSF(s) address(es).

- User Service Description: for HTPP-based retrieval , when sending HTPP request to SSF, the UE may provide personalized information to enable a personalized answer; in general, the UE uses the specifications given from the SSF for session initiation but for any personalization, the SSF should authenticate the user to authorize or deny authorization depending on the authenticated identity.

The PSS Streaming session is established with UE sending a SIP INVITE with a SDP offer, containing to media capabilities, parameters sent by the SSFs, media description for RTSP content control channel and one for content channel. The SSF, upon receiving the SIP INVITE, examines the Request-URI and SDP parameters to determine that it is a PSS session initiation for Live Streaming or Content-on-Demand. The SSF check the *Request URI* and the SDP offer to determine if it is a PSS session request for Live-Streaming or Content-On-Demand. In each case, the SSF selects a PSS adapter and forwards the SIP INVITE to it or forward to a different one if the chosen PSS Adapter answers with 301 or 302. For Live Streaming, the SSF includes a list of Live content channels for the user in the SIP INVITE. Based on the Request-URI and SDP parameters, the SCF selects a suitable PSS Adapter and forwards the SIP INVITE to the selected one. Once receiving a SIP 200 OK response from PSS Adapter, the SCF shall forward the response to UE.
The PSS Adapter is aware of each session between the UE and the adapter itself, and the adapter and the PSS Server. Upon receiving a SIP INVITE, the adapter constructs a RTSP SETUP message for the PSS Server based on the SIP INVITE message to setup the relevant media streams and sends back to the UE the SDP answer in a SIP 200 OK response. The UE, upon receiving the answer from the adapter, starts a TCP connection carrying RTSP to establish the session and exchange RTSP messages. The session parameters can be changed by sending a re-INVITE message and its termination can be done by the UE or the SCF or the PSS Adapter by sending a SIP BYE message.
Regarding MBMS Streaming session initiation, the UE sends a SIP INVITE to SCF through the IMS CN subsystem; SCF responds UE with a SIP 200 OK message when the SIP INVITE is successfully handled. The SIP 200 OK contains an SDP files containing the Multicast address of the service. The UE then activates the MBMS bearers: at this point, the UE can start receiving the MBMS Streaming session data transmitted by the BMSC.UPF. These steps assume that a MBMS USD containing the SDP has already been received.
Once the session is established, the UE can perform the content switching, that is the tuning into a new multicast channel by sending a SIP INFO message to SCF with the content switching information.As usual, a SIP BYE message is used for session teardown. Moreover, the UE can switch from PSS and MBMS streaming and vice versa: the switching is done by sending SIP Re-INVITe message to the SCF that will teardown at the PSS the connection for PSS-to-MBMS switching or will send a SIP INVITE to the PSS adapter.

3GPP TS 23.167 [10] describes the emergency service in the IMS Core Network and the entities to support such services. The emergency services are independent from the IP-CAN (IP Connectivity Access Network), they must be prioritized over non-emergency sessions and must be available to all the barred public user identity. The use of emergency service is allowed to all the user that have enough credentials to authenticate with IMS, that is registered or not. In case, that the user is not registered, he must perform an *emergency registration*. Even if the user does not have credentials, an insecure association between the UE and the P-CSCF, including an equipment identifier to establish the emergency session; it is possible to have the request rejected if no sufficient credentials are available. Location of the user for emergency service is relevant to determine the PSAP (*Public Safety Access Point*) serving the area where the UE is actually located.
The reference architecture is the one depicted in Fig. 8. In this figure, new entities are present:

- *E-CSCF, Emergency -CSCF*: it is the IMS functional element responsible for routing emer-

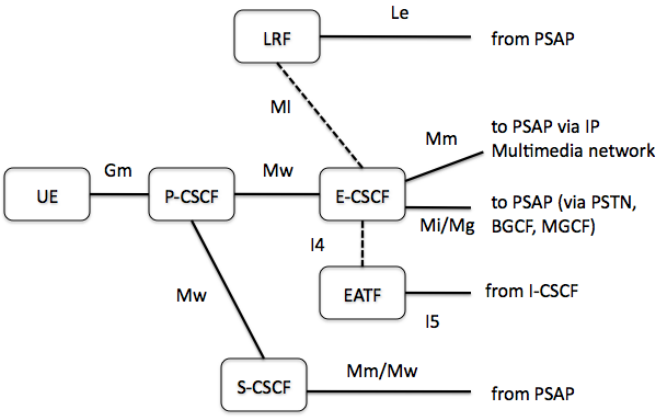


Figure 8: *E-CSCF in the reference architecture*

gency call requests to the nearest PSAP based on the callers location information, as well as other information, such as the type of emergency service being requested. E-CSCF receives from the P-CSCF request for emergency session establishment, and, if required, contacts the LRF to validate the location information given by the UE and routes the request to the appropriate destination.

- *EATF, Emergency Access Transfer Function*: it provides IMS-based mechanisms for enabling service continuity of IMS emergency sessions. It is a function in the serving IMS network, providing the procedures for IMS emergency session anchoring and PS to CS Access Transfer.
- *LRF, Location retrieval Function*: it is responsible for retrieving the local information of the UE starting an emergency session. LRF uses RDF (Routing Determination Function) to provide information to E-CSCF. Provided information are the ESQK (Emergency Service Query Key, that is a 10-digit used to identify a particular emergency call istance), PSAP SIP URI or TEL URI.

An example of procedure related to IMS emergency service is the session establishment: the user capabilities and resource reservation to establish the session are validated and, if required, bearer registration is performed. After these steps, the UE performs the P-CSCF discovery procedure and after the IMS registration: at this point the UE starts an IMS session establishment containing an emergency session indication and any registered public user identity.

The work item "IMS Service Continuity Inter Device Transfer enhancements" is the composition of three different TS, in particular the 3GPP TS 23.237 [11] , 3GPP TS 23.292 [12], 3GPP TS 23.831 [13].
3GPP TS 23.237 [11] presents the architectural requirements and procedures to deliver IMS service continuity for both PS and CS bearers of media. IMS Service Continuity is a home network based IMS application which provides intra-UE transfers of one or more components of IMS multi media sessions across different Access Networks. In addition, Service Continuity enables adding, deleting, and transferring media flows of IMS multimedia sessions or transferring whole IMS multimedia sessions across multiple UEs having IMS subscriptions under the same operator.
The information needed for service continuity consist on details about the media flows being transferred/kept/deleted, which active session is required to be updated or replaced and whether o merge sessions. This information are carried in SIP/SDP or in CS call control message.

The principal functional entity is the SCC AS which implements the access transfer, the inter-UE transfer, terminating access domain selection (T-ADS) and the handling of multiple media flows. The UE must be able to perform actions for the different task: in particular, for access transfer functions, it shall be able to apply operator-specific policy, and to provide all the necessary detail for conducting the task at the SCC AS; for inetr-UE Transfer, it shall be able to discover the target UE(s) and to take the role of Controller in a *Collaborative Session*. A Collaborative Session is a et of two or more Access Leg and related media on two or more UEs and to a remote party are presented as one by the SCC AS. In a Collaborative Session, two roles are identified: the Controller, which is the one in charge of addition, deletion or modification of media flow in the Collaborative Session it controls and it is aware of the state of media flow; for the Controllee role, instead, the UE can modify or release media flow which terminates on it, accept or refuse modification/addition by the Controller or remote party.
In Fig. 9 is depicted the Collaborative Session for inter-UE Transfer:

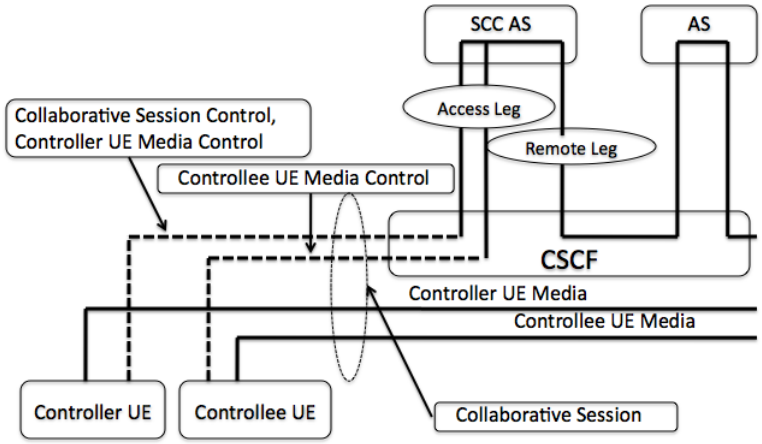


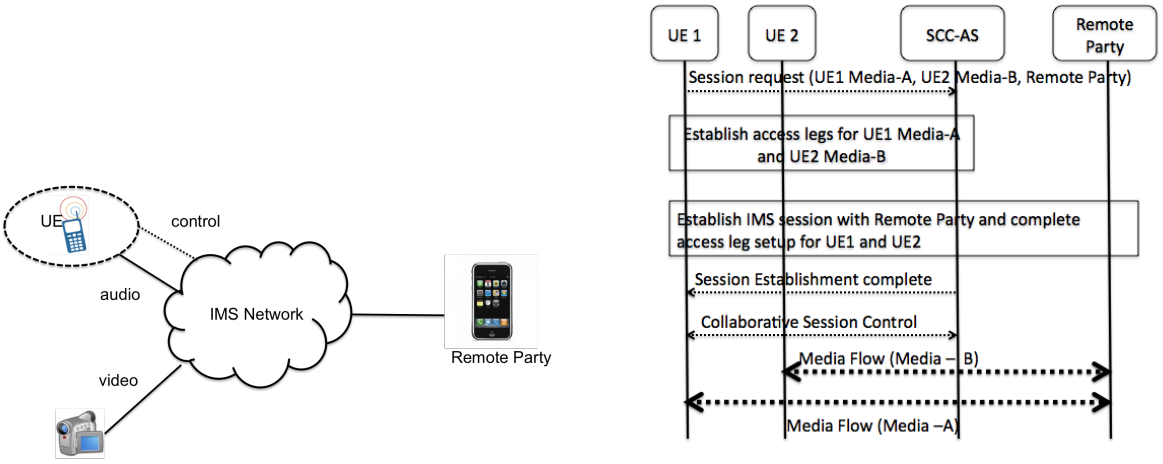
Figure 9: Collaborative Session Signalling and Bearer architecture

The Controller provides the control of the Collaborative Session using IMS signaling on the *Access Leg*, i.e. call control leg between the UE and the SCC AS, and transfer one or more media flow to one or more target UE by using the same Collaborative Session. Controllee provides control for the media using IMS signaling on the *Access Leg*; the SCC AS combines media description and presents one *Remote Leg*, i.e. call control leg between the SCC AS and the remote party from the subscriber's perspective, to the remote party.
As said before, Service Continuity is about transferring media among UEs and different Access Network. Access Transfer procedures enable service continuity between Access Networks. All Access Transfer procedures associated with a session, including initial and subsequent transfers, are executed and controlled in the user's home IMS network by the SCC AS upon the UE's request. When the UE determines that Access Transfer is desirable and possible, a registration in IMS is performed by the UE via the transferring-in Access Network if the user is not already registered via that network. Based on UE and Access Network capabilities, the UE may also maintain some of the media flows in the transferring-out Access Network while transferring the other media flows to the transferring-in Access Network. Upon detection of conditions requiring Access Transfer, the UE establishes a Target Access Leg with the SCC AS via the transferred-in Access Network to request Access Transfer to the transferred-in Access Network. The SCC AS executes the Access Transfer procedure by replacing the Source Access Leg currently communicating to the Remote Leg with the Target Access Leg. If no media flow is retained in the transferred-out access, the Source Access Leg is released. If the UE chooses to retain some media flow(s) in the transferred-

out access, the Source Access Leg is updated to indicate which media flow(s) is retained in the transferred-out access. Upon receiving a request for execution of Access Transfer, the SCC AS performs the Remote Leg Update by switching the Access Leg communicating with the Remote Leg from Source Access Leg to Target Access Leg by communicating the SDP of the Target Access Leg established to the remote end via the user's S-CSCF.
Inter-UE Transfer can be performed:

- while there is an ongoing session in which media flows are transferred from two different UEs : in this case, the request is sent to the SCC AS that removes the media flow from one UE, establishes an Access Leg with the other UE and updates the remote legs. At this point, a Collaborative Session is established with the UEs taking the roles of Controller and Controllee and the media flow is going between the Controllee and the remote party.
- while there is an ongoing session and new media is added from another UE: as usual, the request is processed by the SCC AS that informs the other UE of a new media creation. A response is sent back to the request originator, a Collaborative Session is established and the media flows proceed from all the parties involved.
- at IMS session setup: before setting up a session with the remote party, the originating UE request to the SCC AS a Collaborative Session that will establish a Access Leg with the Controllee; after, the SCC AS sends a session request to the remote party which answers with an SDP offer that will be forwarded to the UEs.
- at IMS terminating setup: the remote party sends a session setup to SCC AS to set up Media-Flow A and Media-Flow B with two UEs, UE-1 and UE-2; the request is sent to UE-1that starts a Collaborative Session, an Access Leg is created at UE-2, an answer is given to the remote party and the media can flow among the parties.

The media can be transferred, for example the from the Controllee to the Controller or between two different Controllee; moreover, media can be added or deleted in the Collaborative Session.
Service continuity is supported when CS is used for transporting the media: in this case, the Gm interface (signaling interface between UE and IMS) can be used for SIP signaling and a change of network may result in the inability to use Gm interface for IMS traffic: in this situation, the service continuity is ensured by switching the signaling in the CS domain. In standard handover, the network allocate a new CS bearer for the signaling and a circuit in the target access network. After the handover, the UE notifies the SCC AS that I1 interface is used for signaling in the termination network. The SCC AS may not detect the UE in the signaling path, with the result that all held session for the user are deleted and the status is updated at the S-CSCF. (Refer to 3GPP TS 24.294 [14] for details on I1 interface between ICS UE and SCC AS and 3GPP TS 23.292 [12]).
3GPP TS 23.831 [13] is a development of the service-continuity in 3GPP TS 23.237, specifically in the area of inter-UE transfer. From 3GPP TS 23.237, each IMS session, in CS or PS domain, is anchored to a SCC AS (Service Centralization and Continuity Application Server) in the home network to provide service continuity for a user. When a inter-UE transfer is about to be establish, the UE who has initiated it, create a Collaborative Session and it will be called Controller UE, instead, the other UEs involved in the Collaborative Session are called Controllee UE: the coordination of the Collaborative Session is done by the SCC AS.
In 3GPP TS 23.831 are described examples of flows between the different entities involved in different procedures like the establishment of Collaborative Session upon originating/termiantion a IMS session. An example can be seen in Fig. 10. In this scenario, the UE 1 establishes a session with a remote party and establishes a Collaborative Session with UE 2 belonging to the same IMS subscription and an IMS session with the remote party; the SCC AS creates two access legs, i.e. the call control leg, for the media flows, sends a IMS session establishment request to



(a) Reference Scenario (b) Sequence Diagram

Figure 10: *Establishment of Collaborative Session at IMS session origination*

the remote party and informs UE1 that the Collaborative and IMS Session are established and media can flow between the parties.

4.2 IMS - IETF SIP Protocol Alignment

This work item is about maintaining alignment of the development of the SIP used in IMS with the one currently defined by IETF. Three Technical Specifications (TS) describe an IP multimedia call control protocol based on SIP and SDP, the multimedia session handling and some examples of signaling flows for session setup in the IM CN subsystem based on SIP and SDP.

The 3GPP TS 23.218 [7], describes the IP Multimedia Call model for handling IP multimedia session origination and termination for a subscriber. The architecture required for service provisioning comprises the S-CSCF talking to the Application Server (AS) through the IP Multimedia service control (ISC) interface: on this interface, the ASs act like a SIP Application Server. The relationship between the network entities are depicted in Fig. 11. The right Application Servers

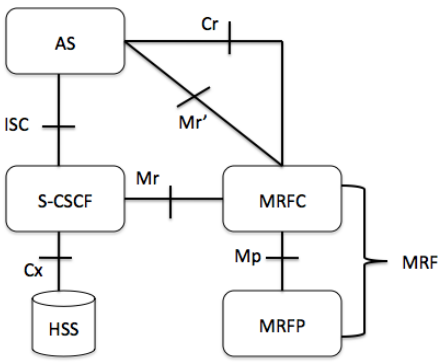


Figure 11: *Functional architecture for support of service provision for IP multimedia subsystem.*

for a service is triggered by using an IMS communication service identifier, called *ICSI*. In the

terminal, the ICSI means dispatching SIP messages to the correct application; in the network, it means the correct Application Server over ISC.
The main goal of this TS is the description of the functional requirements for the S-CSCF, HSS and AS when handling IMS session. Specifically, the most concern is on the S-CSCF that has in charge the handling of different requests from the UE, like handling SIP registration, UE originating/teminating requests, session release and subscription and notification request. For each of this task are listed all the steps performed by the S-CSCF. As an example, in handling the SIP registration, the S-CSCF shall authenticate the served user by obtaining the credentials from the UE and checking against the data in the HSS; after a successfully authenticated registration, the S-CSCF shall download from the HSS all the implicitly registered public user identities associated with the registered public user identity. For each service profile in the implicit registration set, the S-CSCF performs a third party registration to the Application Servers which are interested to be informed about the user registration event of these public user identities. After contacting the Application Server, a 200 OK is sent to the UE from the S-CSCF. All these steps are summarized in Fig. 12.
The HSS, instead, stores all the information about the subscriber needed by the S-CSCF and

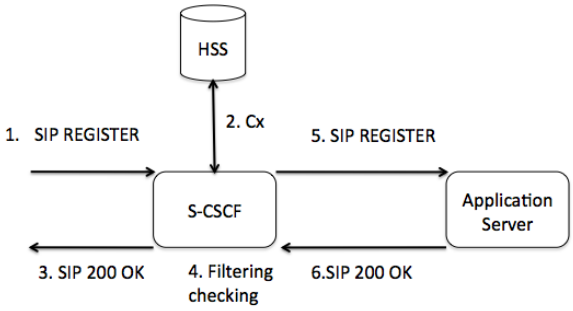


Figure 12: *S-CSCF handling registration*

Application Server and it is involved in the procedures for IP multimedia registration and session. Another important architectural entity in the network is the MRF, the *Media Resource Function* which provides media related functions like media manipulation and playing tones and announcements (see Fig. 11). It is divided in *MRFC, Media Resource Function Controller* and *MRFP, Media Resource Function Processor*. The MRFC acts as a SIP User Agent by interpreting the requests sent by the S-CSCF and the Application Server. MRFC interacts with the Application Server by the interfaces Cr and Mr'. Through these interfaces, the MRFC receives the SIP INVITE requests from the Application Server and translates them to message that control the media resource processing residing in the MRFP.
The functional architecture to support interaction between the S-CSCF and the SIP AS is depicted in Fig. 13. In particular, every UE-originating incoming requests that come from the S-CSCF is handled by the AS-ILCM; this interacts with the application logic to report the call state information. Depending on the service that is being provided, the application logic may instruct the AS-OLCM to modify the request if needed. After processing the request the AS-OLCM may send this request back to the S-CSCF.

The 3GPP TS 24.229 [2] defines the call control protocol based on the Session Initialization Protocol (SIP) and the associated Session Description Protocol (SDP) used in the IM CN subsystem. All the functional requirements for this protocol are taken from the specifications produced by the IETF about SIP and SDP.
SIP defines four types of logical SIP entities, having specific functions and roles in the SIP communication: the User Agent (UA), the Proxy Server, the Redirect Server and the Registrar. In the IMS architecture, these roles are covered by the network entities:

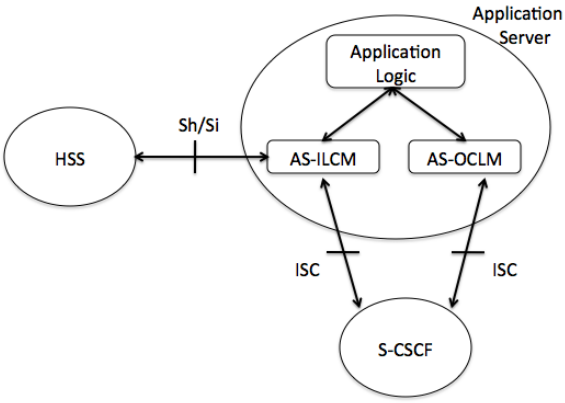


Figure 13: *Application Server functional model*

- the UE acts like the UA;
- the P-CSCF, as well as the I-CSCF, provides the Proxy Server role besides some exceptions;
- The S-CSCF acts like a Proxy Server but under certain circumstances can provide the Registrar role and when it has in charge of executing a third-party registration, it provides the UA role;
- The MRCF shall provide the UA role;
- The AS can act as a UA or as a SIP Proxy.

In order to enable SIP and SDP to operate all the network entities should have an address in the form of a SIP URI and IPv4 or IPv6 addresses. For the subscriber, two types of identities can be identified:

- **private user identity** : it is allocated by the home network operator and it must be available to the SIP application in the UE.
- **public user identities**: one or more public user identities are assigned to the subscriber by the home network operator; at least of one them shall take the form of SIP URI.
  All the public user identities are available to the SIP application within the UE after registration. The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities.

Moreover, for the purpose of indicating the IMS communication service to the network, UE is assigned ICSI values appropriate to the IMS service supported by the UE.

For some of the entities in the IMS network, a list of procedures is presented together with the real usage of SIP:

- **UE**: Before performing any action, the UE should register the public identities with any of the IP address acquired by the UE. All the parameters needed by the UE to perform the registration are stored in the IMS SIM (ISIM), if present: the private user identity, one or more public user identity, the home network domain name used to address the SIP REGISTER request. In case in which the UE does not contain the ISIM, the UE shall generate a private user identity, a temporary public user identity and a home network domain to

address the SIP REGISTER.

The procedures at the UE are:

1. **Registration and Authentication**: the initial registration procedure consists of the UE sending an unprotected or protected, if challenged, REGISTER request to the default port advertised during the P-CSCF discovery procedure. This procedure can be performed only after acquiring the IP address, discovered P-CSCF and established an IP-CAN bearer that can be used for SIP signaling. The *To* and *From* fields of the SIP REGISTER contain the public user identity to be registered; upon receiving the 200 OK, the UE stores the expiration time for the public user identities found in the *To* header, stores as default public user identity the first URI in the *P-Associated-URI* header field (RFC 3455). After the registration, the user can re-register a public user identity or register a new one. The UE can deregister a public user identity previously registered with its contact address at any time. Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs that were using the contact addresses that is going to be deregistered.
   The Authentication is performed during the initial registration or might be done during successive re-registration, de-registration and registration of an additional public user identity. The authentication is required by the S-CSCF who sends to the UE the *401 Unauthorized* response; upon receiving it, the UE extracts from it the RAND (random number) and the AUTN (Authentication Token), checks the validity of the authentication challenge by comparing the locally computed MAC with the one derived from the received AUTN challenge and checks if the parameters required for the setup of security associations are present in the *Security-Server* header field (RFC 3329). If not, the UE abandons the authentication procedure; otherwise, the UE sets up a temporary set of security associations using algorithm specified by the P-CSCF and the parameters in the *Security-Server* header field and sends back the new REGISTER with the *Authorization* header field populated with username, nonce, security algorithm. After receiving a 200 OK, the temporary security associations are replaced with the newly established, eventually used again for registration of new public user identities.
2. **Subscription and Notification**: The UE can subscribe to a specific resource and it receives a SIP NOTIFY message if the state of a resource has changed.
3. **Call Invitation - UE- Originating**: before establishing a SIP session with the receiver, the UE generating the call can reserve network resources based on the application requirements, known as "*precondition mechanism*" (RFC 3312). The other party should be able to reserve local resources, and in order to allow it, the UE originating should specify the precondition in the *Supported* header field. Upon receiving the 200 OK for the local resource reservation and sending the relative ACK, the SIP session can be established.
4. **Call Invitation - UE- Terminating**: the handling of an initial INVITE at the UE receiving it depends on the service requirements for the precondition and the UE's configuration in case the service does not require the precondition mechanism. Upon receiving the INVITE, the UE should check for the presence of the "precondition" option-tag in the *Supported* header field and upon this, it decides to make use or not of the precondition mechanism.

- **P-CSCF**: the P-CSCF is the entry point for the IMS architecture and for this reason it should be prepared to receive the incoming requests on the default ports for unprotected REGISTER or on the ones established during the P-CSCF discovery. The procedures in charge of the P-CSCF are the following:

1. **Registration from the UE**: when the P-CSCF receives a REGISTER request form the UE, it shall insert:
   (a) the SIP URI that identifies the P-CSCF;
   (b) the indication that requests routed from this direction, from the P-CSCF to the UE, are treated as for the UE-terminating case;
   (c) identification of the visited network for the home network;

   in the SIP REGISTER request that will be forwarded to the I-CSCF.
   If the P-CSCF is in the home network, it locates the I-CSCF and, if reachable, forwards the REGISTER request. For a P-CSCF located in the visited network, if the local policy requires the application of IBCF (Interconnection Border Control Function) capabilities in the visited network towards the home network, it forwards the request to an IBCF in the visited network, otherwise the P-CSCF tries to find a point of access for the home network and forwards the request to that entry point. When it receives a 200 OK from the network, as specified in the RFC 3608, it stores the list of service route that will be used to redirect the UE requests to that specific sequence of proxies.
2. **Subscription to user's registration state event package**: upon receiving a 200 OK response to the first initial REGISTER request, the P-CSCF generates a SUBSCRIBE request for the public user identity to which the P-CSCF wants to be subscribed and if the P-CSCF resides in the home network, the request is forwarded to the I-CSCF. When the P-CSCF receives the NOTIFY message, for each of the public user identities still registered, it binds all the public user identities as registered to the contact address; if the state of that public user identity is set to *terminated* in the *Subscription-State* than P-CSCF considers the binding between that identity and the contact address as a de-registrated user. If all public user identities, that were registered by the user using its private user identity, have been deregistered, the PCSCF, will receive from the S-CSCF a NOTIFY request with the *Subscription-State* (RFC 3265) set to "terminated": in this case, the P-CSCF unsubscribe to the state event package for that specific user.
3. **De-Registration**: two kind of de-registration are possibile:
   – user initiated de-registration: if the user wants to de-register a public identity, it sends a SIP REGISTER to the P-CSCF with expiration time set to 0. The REGISTER is then passed through all the entities in order to de-register the user and, as result of the de-registration, a 200 OK is sent back to the P-CSCF from the I-CSCF. Upon receiving this message, the P-CSCF releases all the registrations regarding the user in the *To* header field.
   – network initiated de-registration: as mentioned before, if in the NOTIFY message, the state is set to terminated, the P-CSCF removes all the information for the public user identities.

- **I-CSCF**: the procedures at the I-CSCF are the following:

1. **Registration Procedure**: When the I-CSCF receives a REGISTER request, the I-CSCF shall verify whether or not it has arrived from a trusted domain. If the request has not arrived from a trusted domain, the I-CSCF shall complete the processing of the request by responding with 403 (Forbidden) response. Otherwise, the I-CSCF starts the user registration status query procedure to the HSS. Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity. The HSS answers with a SIP URI and, if it is valid, the I-CSCF forwards the SIP REGISTER to the indicated S-CSCF; if the HSS query returns a list of capabilities, the I-CSCF selects the S-CSCF that fulfils the indicated capabilities, replace the Request-

URI of the received REGISTER request with the URI of the S-CSCF and forwards the REGISTER to the S-CSCF.

2. **Initial Requests**: when the I-CSCF receives an INVITE, it tries to resolve the *Request-URI* to an IP address of the AS hosting the requested service for forwarding the request: in this case, no user location procedure is done because the Request-URI matches one of the PSI (*Public Service Identity*) subdomains configured in the I-CSCF. Otherwise, the I-CSCF starts with the HSS the user location procedure. This procedure can retrieve the URI of the assigned S-CSCF to which is forwarded the request or a list of S-CSCF capabilities: in the last case, the I-CSCF chooses the S-CSCF, puts its SIP URI at the topmost *Route* header field value and forwards the request to the selected S-CSCF.
   Upon an unsuccessful user location query, if the response from the HSS indicates that the user does not exist, and if the Request-URI is a tel-URI containing a public telecommunication number, the I-CSCF may attempt to route the request. If the routeing is attempted, the I-CSCF forwards the request to the transit functionality for subsequent routeing, invokes the part of this transit functionality in charge of translating the number in a routable SIP URI: if translation fails, the I-CSCF sends a *404 Not Found* or *604 Does not exists anywhere* response, otherwise it determines the destination address and the request is processed.

- **S-CSCF**: The S-CSCF acts as the SIP registrar for all UEs belonging to the IM CN subsystem. The procedures at the S-CSCF are the following:

  1. **Registration and Authentication**: an initial registration is defined as an unprotected SIP REGISTER with no authentication information. Upon receiving this initial registration, for the public user identity that has not been registered yet, the S-CSCF recovers the private user identity, the visited network in the *P-Visited-Network* field (RFC 3455) and selects an Authentication Vector (AV) containing the RAND and AUTN to challenge the user. Before performing the challenge, S-CSCF chooses which HSS to query possibly through the use of SLF and informs the HSS that the particular user is served by the S-CSCF. The user is then challenged to provide its credential by receiving a *401 Unauthorized* response.
     For a protected REGISTER, no authentication is done if the *Authentication Header* is set to "auth-done". If the registration expiration interval is set to 0 in the REGISTER, the S-CSCF performs the de-registration procedure. Otherwise, the S-CSCF checks if the public user identity is registered: if not, a new public user identity is going to be registered. If the identity in the *To* header field was already registered, the S-CSCF updates registration bindings, like the *Path* header and the expiration time.
     The success message, the 200 OK, contains the list of received Path headers, a *P-Associated-URI* header field (RFC 3455) containing the list of registered public user identity and its associated set of implicitly registered public user identities, a *Service-Route* header field (RFC 3608) containing the SIP URI of the S-CSCF.
  2. **Subscription to S-CSCF events and Notification**: all the incoming SUBSCRIBE message at the S-CSCF are checked against the local policy in order to verify that the subscriber is authorized to subscribe to the registration state for that user. The subscriber must include all the not-barred public user identities for the user. As usual, a 200 OK message is sent if the subscription was successful. The SIP NOTIFY message containing the full state information for the user is sent once an event occurs; if all the public user identities for the user have been de-registered, the S-CSCF considers the subscription cancelled.
  3. **Call Initiation and Release**: upon receiving a SIP INVITE from/to a served user, the S-CSCF may require the periodic refreshment of the session by one of the two

UEs involved. The SDP offer may or may not examine by the S-CSCF to check if the contained IP address is valid for the IM CN subsystem. In case the IP address is not valid, the S-CSCF returns to the I-CSCF a *305 Use Proxy* response to I-CSCF and the SIP URI of the IBCF to be contacted.
The S-CSCF can release with a CANCEL message a session that is currently being established if notified by the network. If the session was already established, the release is performed by sending to the served user a BYE message based on the information on the related dialog to both the endpoints. Upon receipt of 2xx response for the BYE, the S-CSCF deletes all the dialog information and releases the multimedia session. Moreover, the session can be released when the session timer expires: at this event, the S-CSCF deletes all the information related to that session.

- **AS**: The procedures at the AS are the following:

  1. **Common Application Server (AS) procedures**: in this item, several tasks can be found. Among these:
     (a) Notification about registration status: the AS may support the REGISTER method in order to discover the registration status of the user. For each REGISTER request received, the AS stores the expiration time and sends back a *200 OK* or an appropriate failure message. If the received REGISTER is a third-party REGISTER request, the AS subscribes to the reg event package (RFC 3680) for the public user identity registered at the user's registrar (S-CSCF).
     (b) User identify verification at the AS: when the AS receives a standalone request, the AS checks if the "Privacy" header (RFC 3323) is present: in this case, the request is anonymous and no more actions are required; in the other case, the AS looks for the *P-Asserted-Identity* header (RFC 3325) to retrieve the identity of the user. If no *P-Asserted-Identity* header in the request but the request carries the credentials of the user, the AS checks the correctness of such credentials: upon a success, the AS is aware of the user identity otherwise it challenges the user with a *401 Unauthorized* response.
     (c) Request authorization: once the user identity has been verified or the user is anonymous, the AS checks the authorization policy whether granting or not the requested functionality to the user.
     (d) Carrier Selection: an AS can support the carrier selection for interworking with different networks; it may receive a request with a Request-URI in the form of a tel-URI. If so, it validates the Carrier Identification Code "cic" parameter and insert the Dial Around Indicator "dia". In case the request should end in the ISDN network, the AS translates the SIP URI in a tel-URI and processes the request as if it had arrived from the UE containing this tel-URI in the Request-URI.

     The Application Server may act as:

     (a) **terminating UA or redirect server**: for an AS acting like a terminating UA, the terminating-UE procedures apply. Some exceptions may apply, like the impossibility to send initial registration of its addresses. As a terminating UE, the AS for any initial request or response for dialog stores the "orig-ioi" field value for charging purposes. Furthermore, as a redirect server, it shall propagate any received IM CN subsystem XML message body in the redirected message.
     (b) **originating UA**: in order to act as an originating UE, the AS should be located in the same trusted domain as the S-CSCF to which the request will be sent. As mentioned in the above item, the same procedure for a originating-UE apply. Exceptions apply. In generating a new request, an identity should be provided for the S-CSCF: this identity can be the actual final user included in the *P-Asserted-Identity* header field (RFC 3325) or if not this value is included in the

P-Served-User header field(RFC 5502). These requests are done on behalf of a public user identity of a user and sent to the S-CSCF which proxies them towards their destination.

(c) **SIP proxy**: when acting as a SIP proxy, before forwarding any request received by the S-CSCF, the AS removed its own URI from the message and may modify, delete or add header contents in the SIP request. Again, this message is sent back to the S-CSCF until its final destination.

(d) **performs 3rd party call control**: there are 2 kinds of 'third-party call control": the first one in which the AS receives the requests and generates a new request based on the received one (Routeing B2BUA), in the second way, the AS initiates two requests, which are locally connected at the AS.

The same TS specifies the usage of the Session Description Protocol (SDP) in the IMS architecture. As done for the usage of SIP, for SDP several procedures can be identified for the different IMS entities.

- **UE**: In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. During the session establishment or during session modification procedures, SIP messages shall only contain SDP payload if that is intended to describe the session. The UE includes values for the media involved in the session, like audio packetization rate, bandwidth for each media stream and so on. Once the UE has enough information about the resources by inspecting the SDP contained in every SIP response from the network, the local resource reservation can start. Moreover, if QoS constraints are present, the UE can reuse previously reserved resources.
  In the INVITE request, the originating UE specifies the SDP offer with at least one media description. The UE can try to establish different session through different networks by sending multiple INVITE requests: these networks may reply with a *488 Not Acceptable Here* responses that forces the UE to create a new INVITE request with a subset of media types codec and other parameters of the one contained in the 488 response. Upon a successful reservation of the resources, UE specifies that the preconditions are met, and for all the previously sent INVITE with no preconditions met and related media stream set to inactive, the media stream are set to active.
  At the terminating UE, if desired QoS resources have been reserved, the answer to the SDP offer lists as active all the media that were not listed as inactive in the SDP offer and for each of them a set of codecs are selected.

- **P-CSCF**: All the SIP messages with an SDP offer are examined by the P-CSCF to detect if some media parameters are not allowed by network policy. In case they are not allowed a *488 Not Acceptable Here* message is sent back to the UE containing a SDP payload with SDP parameters that are acceptable by the local policy. The examination is done for all the SIP responses that come at the P-CSCF. The policy is maintained throughout the complete session.

- **S-CSCF**: As the P-CSCF, the S-CSCF examines the SIP messages that carry SDP offer if SDP parameters are not compliant with the local policy. As usual, a *488 Not Acceptable Here* message is generated with SDP parameters allowed according to the local policy and user subscription. If the SDP offer is not compliant with the policy, the S-CSCF terminates the session.

- **MGCF**: MGCF is the connecting point between the circuit-switched domain and the packet one. For a call originating in the circuit-switched domain, the MGCF generates a SIP INVITE and populates the SDP payload with the codecs supported by the Media Gateway (MGW), i.e. the component in charge of media conversion, bearer control and payload

processing. When a call originating in the packet-switched domain ends in the circuit-switched one, MGCF checks for the codecs that matches the requested SDP.

- **AS**: Since AS supports several services, SDP procedures for an AS are dependent on the services provided to the UE. There are no particular requirements for the usage of SDP at the AS, except that each SIP INVITE generated with SDP payload should reflect its capabilities, desired QoS and precondition requirements for the session in the SDP payload. Additionally, if the AS sends a *183 (Session Progress)* response with SDP payload including media types, it has the possibility of requesting confirmation of the resource reservation at the originating endpoint.

Moreover, the same TS specifies some extensions for the SIP headers, SIP compression issues, media control by the AS and the MRFC and other procedure like the discovery of the P-CSCF by the UE.

The 3GPP TS 24. 930 [1] gives real examples of signaling flows for the session setup in the IM CN subsystem based on SIP and SDP. In every of these examples, all the SIP fields are filled with the addresses of the entity sending it, receiving it, routing information, optional tags and so on. The message body contains the description of the session that is about to be initiated: in particular, for a voice call the codecs that are used to convert the voice transmission to digital must be specified so that the receiving UE knows how to decode the voice.

4.3 Study on IMS Evolution

In this section, there will be explained the future evolution of IMS as expected by the Release 10. The future evolution of IMS is wrapped in three Technical Specifications.
The purpose of the 3GPP TS 23.894 [3] is to describe possible optimizations of IMS services in local breakout and of the path taken by the media traffic while traversing different IMS networks. The TS indicates scenarios and solution for both Local Breakout (LBO) and for Optimal Media Routeing (OMR) and finally the evaluation of such solutions.

- **Local Breakout**: an user has subscribed through a home network and it is currently roaming and served by a visited network. Different scenarios are presented. In the first one, the UE can use two different IP addresses: one assigned by the home network for IMS signaling and the other by the visited one for media. The last IP address will be announced in a SDP offer if a session is about to be established and it will be used to deliver media. After the session is established, all the media traffic will not traverse the home network but it will be handled by the IP gateway in the visited network (see Fig. 14). In another

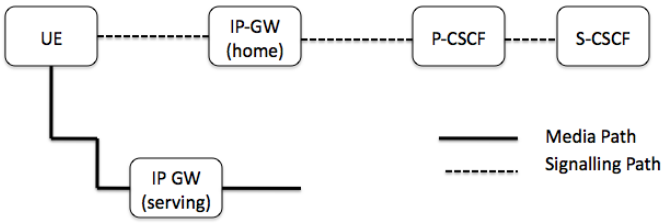


Figure 14: *P-CSCF located in home network – dual IP address*

scenario, the UE has only one IP address for signaling and for media, allocated by the IP gateway of the visited network. Session establishment and sending of data are done as

before. The last two cases apply when the P-CSCF is in the home network: if not, the IP address is assigned by the IP gateway of the visited network and all the data sent to this address will not traverse the home network but it will all be handled by the IP gateway in the serving operator's network.

- **Optimal Media Routeing**: this clause identifies some scenario where the selection of an alternative path provides benefits to IMS by reducing the number of networks entities in the media path. In order to fulfill this requirement, IMS is capable to deploy TrGWs (*Transition Gateway*)between IP realms of each network. The media path for a multimedia stream may traverse an arbitrary number of IP realms between endpoints: if the TrGWs in the media path only have connections to its directly connected IP realms, then the media path cannot be optimized using the allocated TrGW resources. However, if either of the endpoints, or any TrGW on the path, has direct access to one IP realms on the path then a shorter media path can be found. In charge of finding this least path in terms of TrGWs is the IMS-ALG (*IMS Application Gateway*) and the solution for this is obtained by adding information to SDP answer/offer messages and extending IMS-ALG functionalities. The algorithm works in the following way: the media path for each multimedia stream between the UEs is established via an end-to-end SDP offer/answer exchange where each IMS-ALG may choose to modify the connection and port information associated with each media line in the SDP to insert its TrGW in the media path according to normal IMS-ALG procedures. Each IMS-ALG may also identify when one or more TrGWs can be bypassed and modify the forwarded SDP messages to implement the corresponding changes in the media path. As a mentioned, an SDP extension, the 'visited-realm' line, provides connection information on the IP realms on the signaling path: in particular, a realm identifier, connection/port data, and cryptographic signature computed by each IP realm to ensure the data integrity. The use of secondary TrGWs can optimize the path (see Fig. 15): the IMS-ALGs controls the TrGWs in the path toward the UE2 and additionally some other TrGWs on defaul path. The IMS-ALG can advertise its ability to access additional IP realms in the forwarded SDP message. The secondary TrGWs are advertised by an SDP extension, the 'secondary-realm', containing the same information as before. The IMS-ALGs can read this secondary-realm advertisement and if it discovers that it has a direct connection to an IP realm accessible from a TrGW controlled by a previous IMS-ALG in the path then the IMS-ALG may choose to use this alternative media path if it appears to be an improvement over the initial path.

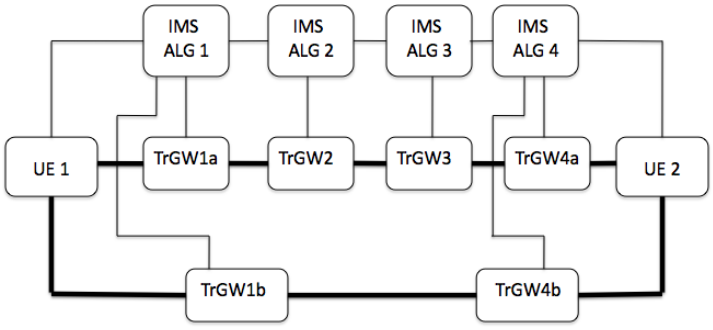


Figure 15: *Configuration using secondary TrGWs*

The use of IMS-ALGs and TrGWs in the home network raises the concern that the media path for a session using local breakout may be anchored in the home network if an OMR algorithm cannot remove the TrGWs allocated in the home network, thus limiting the potential for media path optimization. Nevertheless, the home network may have legitimate security concerns requiring

the use of IMS-ALGs and TrGWs at its border to protect internal network resources. Any TrGW allocated at the home network border serves the purpose of protecting the internal network resources and cannot be subject to bypass.
When the user is roaming and is currently served by a different operator, scenario with "P-CSCF located in home network dual IP address" and scenario with "P-CSCF located in home network single IP address" limit the ability of network elements on the signalling path to control QoS and charging for the media path; on the contrary scenario with "P-CSCF located in serving network single IP address" enables the best control of QoS and charging for the media path.

The 3GPP 23.812 [4]has the scope to study the feasibility of enhancing the IMS architecture, among these investigating improvements on the architecture to reduce the complexity of signalling procedures by reducing the signaling hops; improvements of the system-level load balancing and reliability.
All the procedures in the IMS architecture involve complex steps with the network entities and sometimes not efficient, so a review of these might lead to some optimization. Most of these procedures rely on central entities, i.e. the S-CSCF. If these entities fail, service availability may be impacted. Additionally, the architectural entities are not fully utilized because the load of traffic is not well balanced: some entities might be overload due to an increase of the traffic and other might be under loaded.
Load Balancing at the different network entities is met in different way: the P-CSCF may not accept IMS registration request if it is overloaded, leading to a inefficient distribution of the load; the S-CSCF for a UE is associated by the I-CSCF with no knowledge about the load on the S-CSCF and the optimal choice for better balancing may be done after some time; at HSS, the load balancing depends on the capabilities of the HSS and the data storing planning making not easy to guarantee optimal distribution of traffic among HSSs.
Network Scalability is a main point for maintenance of the users IMS network: when the number of UEs increase, the operator distributes geographically several HSSs. The SLF (Subscriber Location Function) should be able to select the right HSS to query and this task may get worse for distributed SLFs requiring synchronization amongst the entities.
Architectural alternatives are taken into accounts to load balancing-related problem. The P-CSCF, if overloaded, may suggest to the UE registering a redirection to another P-CSCF or sends to UE a *Server Temporary Unavailable* response, that triggers the UE to use DNS to select another P-CSCF.
A *Load Detection Function, LDF* monitors and stores the information of all P-CSCFs and S-CSCFs, i.e. CPU usage, memory used, number of supported user. The DNS is informed about the load information and returns to a requesting UE the address of a low-load P-CSCF to which forward the request. For the initial registration, the LDF can be used to choose the right S-CSCF to which the actual registration will be performed: the DNS is always informed about the load for some relevant S-CSCFs and for each request arriving from I-CSCF, it suggests the S-CSCF to which forward the request. For a re-registration, instead, the choice of a new S-CSCF based on LDF information must be done maintaining service continuity, making this a procedure applicable to UE with no ongoing services.
The availability of better S-CSCFs triggers a re-selection for the UE of the Serving CSCF during the re-registration procedures. Some mechanisms are defined:

1. Mechanism 1: the I-CSCF knows the current S-CSCF assigned to the UE by querying the HSS and checks whether it is the best suited based on capabilities with another query to the HSS; otherwise, a better suited S-CSCF is determined at I-CSCF and assigned to the UE if available, i.e. not overloaded.

2. Mechanism 2: another way to perform S-CSCF re-selection is by adding functionalities to the I-CSCF and HSS: the re-selection, as before, is based on capabilities of the S-CSCF but unlike the previous case, the information about the capabilities are requested to the HSS in a single message and then determined if the S-CSCF is the best one or not.

3. Mechanism 3: during the initial registration, when the I-CSCF select a S-CSCF not preferred, it indicates to the selected S-CSCF that a better S-CSCF may become available later; this second choice is stored in the HSS (*preparation step*); while re-registering, the I-CSCF obtains from the HSS the S-CSCF associated plus the information about the best suited S-CSCF and if the latter is available, the S-CSCF switch may take place.

The purpose of 3GPP TS 23.848 [5] is to find enhancements needed in the current IMS interconnection architecture based on new business model and service delivery scenarios. Since Release 8, the IMS interconnection architecture comprises the IBCF and the TrGW logical entities (see Fig. 16). The IBCF provides application specific functions at the SIP/SDP protocol layer in order to perform interconnection between IM CN subsystem networks by using Ici reference point. The TrGW is located at the network borders within the media path and is controlled by the IBCF and provides functions like network address/port translation and IPv4/IPv6 protocol translation. The functionalities that may be needed at IMS operator border:

- Control Plane: the list of new functions comprise the service level interoperability, i.e. the selection of signaling transport protocol (TCP, UDP, ..) and signaling inspection; interworking between SIP and other protocol; ability for border control plane nodes to exchange VQE (*Voice Quality Enhancement*) capabilities; e2e QoS management and load balancing and routing related features; security and protection, like the DoS (Denial of Service) prevention; access control features, i.e. management of ACL (Access Control List) to ;
- User Plane: the list of new functions comprise the detection of inactive bearer connections; the transrating, i.e. the change of codec packetization time; e2e Qos management; routing and security features; system redundancy features, i.e. backup functionality to maintain service to the end user when the system drops for some reason (natural or artificial).

The Access Control can be configured at the IBCF or stored in a repository (ARP, ACL Profile Repository) managed by the operator and pushed to the IBCF. The Access Control Lists are assigned to a public SIP URI or a group of them, and the associated ACLs profile policy are used during IMS session establishment. Each rule in the ACL is composed by an action (permit, deny,..), filter criteria (all session, IP address of a IMS border peer,...), and a type that specifies if the rules are applied to inbound or outbound session.

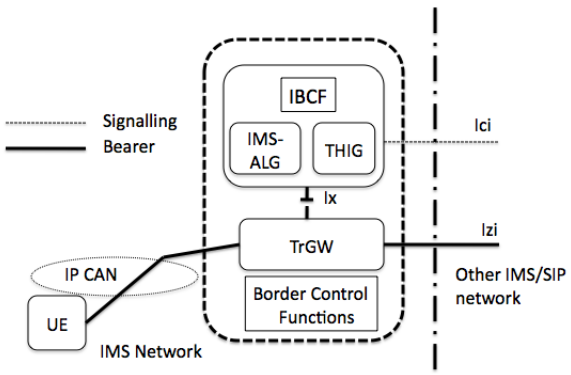
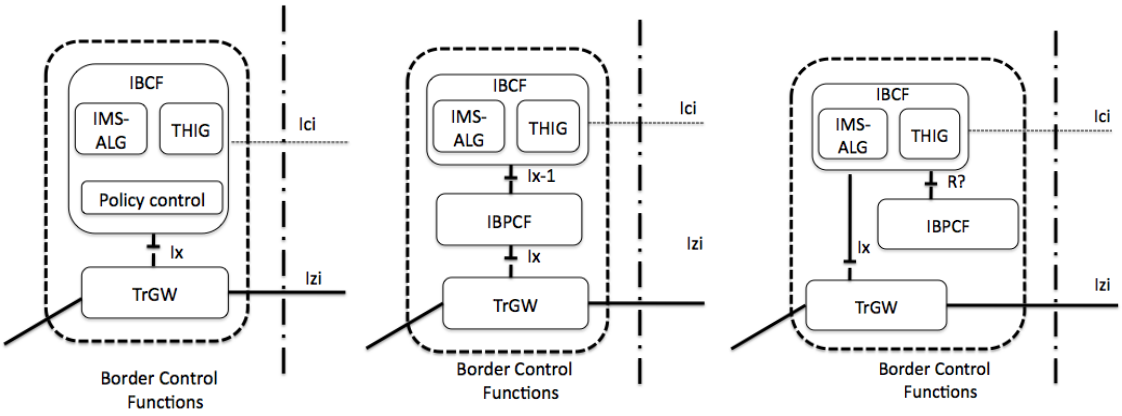


Figure 16: *3GPP IMS Interconnection Architecture, Release 8*

Regard the control policy, three alternatives are proposed: the first one, the policy control functions is an entity in the IBCF (see Fig. 17a) ; in the second, instead, a new entity called *Interconnection Border Policy Control Function,IBPCF* is placed between the IBCF and the TrGw (see Fig. 17b). The IBPCF is responsible for the mapping of requests coming from the IBCF into



(a) Alternative 1 (b) Alternative 2 (c) Alternative 3

Figure 17: *3GPP IMS interconnection architecture*

configuration for the TrGW, taking into account operator-specific policy rules and inter-operator service level agreement (SLA) data. Alternative 3 insert the IBPCF entity as well as a new reference point (whose name has not been established, called in the meantime R?) between the IBCF and the IBPCF. The IBPCF acts on policy requests received over the R? reference point and returns policy decisions over the same reference point to the requestor. (see Fig.17c). Alternative 1 cannot be applied to support non-IMS and IMS traffic at the same time; Alternative 2, instead, supports the possibility to use the same interconnection for IMS traffic and non-IMS traffic, with policy control applied by IBPCF.

Alternative 3 supports the use of the same interconnection for IMS and non-IMS traffic by extending the new reference point R? to the appropriate non-IMS node (see Fig. 18). This allows a consistent use of media QoS and other policies and a common resource allocation view for the IP-interconnects, while still not requiring any other changes to the control and user plane architectures for non-IMS.

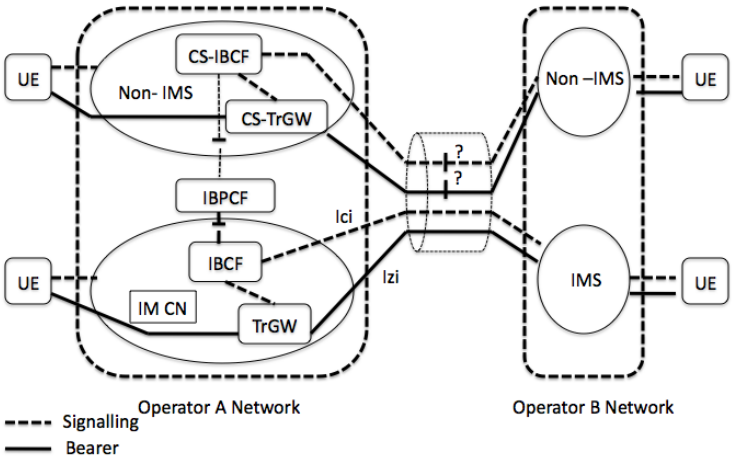


Figure 18: *Common IP interconnection for IMS and non-IMS traffic under Alternative 3*

5 Conclusion - Moving Forward

The aim of this tutorial was to give a (possibly) simple overview of the entire 3GPP Release 10 of IMS by focusing on the relevant parts of the technical specifications in order to give a flavour of the procedures, changing in the architecture and evolution of IMS itself. For sake of clarity, the new aspects for IMS have been grouped together to provide a better understanding of the direction of the evolution of IMS. The most important part covered by this tutorial is the compliance of IMS to the SIP signaling protocol, by describing procedures performed at each network entities, with particular care to the information with which the SIP header fields are filled and their reference to IETF RFCs.
Architectural aspects have been covered to add more capabilities to CS users by providing access to IMS services. Moreover, some enhancements to IMS have been introduced to allow a more satisfying experience of IMS services for the user, like fruition of IP-based streaming service and maintenance of service continuity in case of transferring media among UEs.

Currently, the 3GPP has started working on the IMS Release 11: among the working items, there can be found the study of content distribution in a Peer-to-Peer fashion based on IMS, identifying the potential service requirements and Peer-to-Peer Application Server and an IMS Multimedia Telephony Service that will allow multimedia conversational between two or more users, providing real time bidirectional transfer of speech, video or optionally other type of data, like text.

IMS opens up new perspectives for network operators by allowing them to deploy new services in a fast way, to implement fixed-and-mobile convergence and to guarantee to users all the type of services because IP will support all services (voice, data, video, and so on). From the user perspective, IMS can have multimedia experiences (more than just voice), they can customize their communication and a have a single identity for multiple communication purpose.
IMS was widely hyped in 2006-2007, but as of today has not been as widely implemented as once predicted. Though its reputation has been tarnished, IMS still has favor within the industry, with lots of work and releases coming out. Some critics have expressed opinions about IMS, reducing it to a single protocol, SIP, and for this is doomed to fail because SIP will not conquer Internet; some others refer to SIP as "SS7 over IP", because SIP is as complex as SS7. Opposite opinions can be found as well. So, where the truth lies? It's true that IMS is a complex technology which involves a lots of steps, several entities to pass through and several forwarding of SIP messages but this complexity has a value, because it provides support to application keeping hidden its complexity to them.
The most vendors concern today is on developing IP-based application rather than the core network, as all the 3GPP specification do. IMS in this way is challenged even if some benefits are given to users and operators. Maybe, the only things to do is letting things taking their course.

References

[1] Peter Leis, "3GPP TR 24.930: Signalling flows for the session setup in the IP Multimedia core network Subsystem (IMS) based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, ver. 9.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 15-12-2009, http://www.3gpp.org/ftp/Specs/html-info/24930.htm

[2] Keith Drage, "3GPP TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, ver. 10.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 15-06-2010, http://www.3gpp.org/ftp/Specs/html-info/24229.htm

[3] Mario Madella, "3GPP TS 23.894: System enhancements for the use of IP Multimedia Subsystem (IMS) services in local breakout and optimal routeing of media, ver. 10.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 15-10-2009, http://www.3gpp.org/ftp/Specs/html-info/23894.htm

[4] Gang Li, "3GPP TS 23.812: Feasibility Study on IMS Evolution, ver. 1.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 09-03-2010, http://www.3gpp.org/ftp/Specs/html-info/23812.htm

[5] Rajat Ghai, "3GPP TS 23.848: Study on enhancements to IP Multimedia Subsystem (IMS) border functions for interconnection of IMS based services, ver. 0.9.1", The 3rd Generation Partnership Project (3GPP), ETSI, 30-04-2010, http://www.3gpp.org/ftp/Specs/html-info/23848.htm

[6] Thomas Towle, "3GPP TS 23.228: IP Multimedia Subsystem (IMS); Stage 2, ver. 10.1.0", The 3rd Generation Partnership Project (3GPP), ETSI, 14-06-2010, http://www.3gpp.org/ftp/Specs/html-info/23228.htm

[7] Keith Drage, "3GPP TS 23.218: IP Multimedia (IM) session handling; IM call model; Stage 2, ver. 9.2.0", The 3rd Generation Partnership Project (3GPP), ETSI, 15-06-2010, http://www.3gpp.org/ftp/Specs/html-info/23218.htm

[8] Nicolas Devron, "3GPP TS 23.832: IP Multimedia Subsystem (IMS) aspects of architecture for Home Node B (HNB); Stage 2, ver. 10.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 26-03-2010, http://www.3gpp.org/ftp/Specs/html-info/23832.htm

[9] Frederic Gabin, "3GPP TS 26.237: IP Multimedia Subsystem (IMS) based Packet Switch Streaming (PSS) and Multimedia Broadcast/Multicast Service (MBMS) User Service; Protocols, ver. 9.3.0", The 3rd Generation Partnership Project (3GPP), ETSI, 18-06-2010, http://www.3gpp.org/ftp/Specs/html-info/26237.htm

[10] Curt Wong, "3GPP TS 23.167: IP Multimedia Subsystem (IMS) emergency sessions, ver. 10.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 14-06-2010, http://www.3gpp.org/ftp/Specs/html-info/23167.htm

[11] Jae seung Song, "3GPP TS 23.237: IP Multimedia Subsystem (IMS) Service Continuity; Stage 2, ver. 10.2.0", The 3rd Generation Partnership Project (3GPP), ETSI, 14-06-2010, http://www.3gpp.org/ftp/Specs/html-info/23237.htm

[12] Andy Bennet, "3GPP TS 23.292: IP Multimedia Sybsystem (IMS) centralized services; Stage 2, ver. 10.1.0", The 3rd Generation Partnership Project (3GPP), ETSI, 14-06-2010, http://www.3gpp.com/ftp/Specs/html-info/23292.htm

[13] Heng liang ZHANG, "3GPP TS 23.831: IP Multimedia Subsystem (IMS) Inter-UE transfer enhancements, ver. 1.0.0", The 3rd Generation Partnership Project (3GPP), ETSI, 14-06-2010, http://www.3gpp.com/ftp/Specs/html-info/23831.htm

[14] Heng liang ZHANG, "3GPP TS 24.294: IP Multimedia Subsystem (IMS) Centralized Services (ICS) protocol via I1 interface, ver. 9.2.0", The 3rd Generation Partnership Project (3GPP), ETSI, 15-06-2010, http://www.3gpp.org/ftp/Specs/html-info/24294.htm

[15] Travis Russel, "The IP Multimedia Subsystem (IMS) Session Control and Other Network Operations", McGraw Hill communication, 2007

[16] Gonzalo Camarillo, Miguel A. Garca-Martin, "The 3G IP Multimedia subsystem (IMS): merging the internet and the cellular worlds", John Willey and Sons, June 2004