



IMS Roaming & Interworking Guidelines

3.6

21 November 2006

This is a non-binding permanent reference document of the GSM Association.

Security Classification Category (see next page)	
Unrestricted - Public	

Security Classification: Unrestricted – Public

This document is subject to copyright protection. The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association

Copyright Notice

© GSM Association 2006

GSM and the GSM Logo are registered and owned by the GSM Association.

Document History

Revision	Date	Brief Description
0.0.1	August 5th, 2003	Input paper IREG Doc 104/03 "IMS Roaming & Interworking Guidelines Proposal" for IREG Portland meeting
0.0.2	October 28th, 2003	First draft of PRD for IREG Packet WP London meeting
0.0.3	January 28th, 2004	Second draft of PRD for IREG IMS Ad Hoc
0.0.4	February 18th, 2004	Third draft of PRD for IREG Amsterdam meeting
0.0.5	April 23rd, 2004	Forth draft of PRD for IREG IMS Ad Hoc
0.0.6	May 18th, 2004	Fifth draft of PRD for IREG Packet WP Madrid meeting
3.0.0	July 30th, 2004	First approved version
3.0.1	December 23rd, 2004	Incorporated IREG Doc 48_025 (NSCR 001 to IR.65 3.0.0)
3.3	November 7 th , 2005	Incorporated Minor CRs 003 and 004
3.4	February 7 th , 2006	Incorporated Minor CR 005
3.5	August 14 th , 2006	Incorporated Minor CR 006
3.6	November 21 st , 2006	Incorporated Minor CRs 007 and 008

Table of Contents

1	GLOSSARY	4
2	SCOPE	5
3	BACKGROUND	6
3.1	INTRODUCTION	6
3.2	ARCHITECTURE & DEFINITIONS	7
4	ROAMING	9
5	INTERWORKING	11
6	REQUIREMENTS FOR THE INTER-PLMN NETWORK	13
6.1	GENERAL ISSUES	13
6.2	IP VERSION ISSUES	13
6.3	SECURITY ISSUES	14
6.4	PROXY	15
7	REQUIREMENTS FOR THE PLMN NETWORK	17
7.1	IP VERSION ISSUES	17
7.2	SECURITY ISSUES	19
8	SERVICE RELATED ISSUES	20
8.1	PoC	20
8.2	PRESENCE & INSTANT MESSAGING	22
8.3	PEER-TO-PEER SERVICES	23
8.3.1.	<i>Video Share</i>	24
9	ADDRESSING AND ROUTING	25
9.1	USER ADDRESSING	25
9.2	GENERAL ISSUES	25
9.3	ROAMING SPECIFIC ISSUES	27
9.4	INTERWORKING SPECIFIC ISSUES	27
10	CONCLUSIONS	30
11	REFERENCES	32

1 GLOSSARY

Terms	Definitions
APN	Access Point Name
AS	Application Server
BGCF	Breakout Gateway Control Function
CDR	Charging Data Record
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENUM	E.164 number and DNS
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
IM-MGW	IP Multimedia – Media Gateway
IM-SSF	IP Multimedia – Service Switching Functionality
IMSI	International Mobile Subscriber Identity
IMS	IP Multimedia Subsystem
ISIM	IMS SIM
MGCF	Media Gateway Control Function
MGW	Media Gateway
MRF	Multimedia Resource Function
NAPTR	Naming Authority Pointer DNS Resource Record
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translation
OAM	Operation, Administration and Maintenance
OSA	Open Service Access
P-CSCF	Proxy CSCF
PCF	Policy Control Function
PDP	Packet Data Protocol
PDP	Policy Decision Point
PDU	Protocol Data Unit
PoC	Push-to-talk over Cellular
QoS	Quality of Service
RAN	Radio Access Network
R-SGW	Roaming Signalling Gateway
S-CSCF	Serving CSCF
SGW	Signalling Gateway
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMTP	Simple Mail Transfer Protocol
THIG	Topology Hiding Inter-network Gateway
T-SGW	Transport Signalling Gateway
UE	User Equipment
URI	Uniform Resource Identifier
URL	Universal Resource Locator
VPLMN	Visited Public Land Mobile Network

2 SCOPE

The goal of this document is to ensure that crucial issues for operators such as interworking and roaming are handled correctly also with IMS.

Document concentrates on the first phase of IMS, i.e. what can be done with IMS by operators within a short timeframe. In other words, non-conversational services like presence and instant messaging form the main area of interest. More advanced IMS features are also handled at some level. Goal of the document is not to describe each and every aspect of IMS in detail, but rather concentrate on the most important issues the first implementations of 3GPP Release 5 based IMS roaming & interworking will face.

Document introduces guidelines for usage of inter-PLMN connections in IMS environment and requirements IMS has for inter-PLMN backbone network. Other issues discussed here are e.g. addressing and routing implications of IMS.

In order to get IMS services successfully started, roaming and interworking are seen as major issues. This document aims to increase the IMS interworking & roaming related knowledge level of operators and to prevent non-interoperable and/or inefficient IMS services & networks. This concerns especially roaming and interworking cases, since these issues could potentially significantly hinder the implementation of IMS if not handled properly.

Some of these issues are already covered in existing IMS specifications, but only vaguely. This leaves too much room for individual implementations, thus increasing the risk of non-interoperable solution for transferring IMS traffic between operators. Especially, it is unlikely that all operators will cover every single possible variation and available option. However, it is not the aim of this document to cover implementation issues as such. There are also IMS interworking and roaming issues that have not been discussed in any specification.

Please note that the document does not aim to give an elementary level introduction to IMS, even though Chapter 3 has a short introduction. (See 3GPP TS 22.228 [3] document for that purpose)

This PRD concentrates on network level roaming & interworking, therefore higher level issues like service interconnection are not discussed in detail, see e.g. SE.35 [13] for service related documentation. Also issues such as radio interface, QoS details, GPRS backbone, interworking with PSTN as well as connections between IMS network elements and terminals/applications are not within the scope of this document. Connections to private networks such as corporate network are also out of scope. Charging and billing related issues regarding IMS roaming and interworking are handled by BARG; see e.g. PRD BA.27 [18].

3 BACKGROUND

Background issues are limited here in the interest of clarity and brevity; readers needing further introduction to IMS should refer for example to the original IMS Roaming & Interworking Guidelines Proposal document (IREG Doc 104/03). Additionally, 3GPP specifications relevant to IMS can be found under References.

3.1 Introduction

The 3GPP Release 5 architecture introduces the addition of a new subsystem known as the IP Multimedia Subsystem (IMS) to the Packet-Switched (PS) domain. IMS supports new IP-based multimedia services as well as interoperability with traditional telephony services. IMS is not a service per se, but a framework for enabling advanced IP services & applications on top of packet bearer.

3GPP has chosen the Session Initiation Protocol (SIP) [2] for control plane signalling between the terminal and the IMS as well as between the components within the IMS. SIP is used to establish and tear down multimedia sessions in the IMS. SIP is text-based request-response application level protocol developed by IETF. Although 3GPP has adopted SIP from IETF, many extensions have been made to core SIP protocol (e.g. new headers, see TS 24.229 [7]) for management, security and billing reasons, for instance. Therefore SIP servers and proxies are more complex in 3GPP system (i.e. in IMS) than they normally are in Internet. However, all 3GPP extensions were specified by the IETF, as a result of collaboration between the IETF and 3GPP, so the SIP protocol as used in the IMS is completely interoperable with the SIP protocol as used on the Internet or any other network based on IETF specs.

IMS is specified to use IPv6. IP traffic between operators is likely going to increase dramatically with the introduction of IMS, since IMS introduces peer-to-peer IP traffic. This means more traffic also for inter-PLMN networks.

IMS is not meant to replace anything; rather it brings new service possibilities to mobile environment. First IMS implementations will support few non-conversational services, like presence and instant messaging, along with near real-time service such as PoC. For more information about IMS based services, see e.g. SE.35 [13]. Gradually IMS will offer more services, but due to problems related to conversational services' delivery, IMS will be a long time only a subset of the 'All-IP' dream.

3.2 Architecture & Definitions

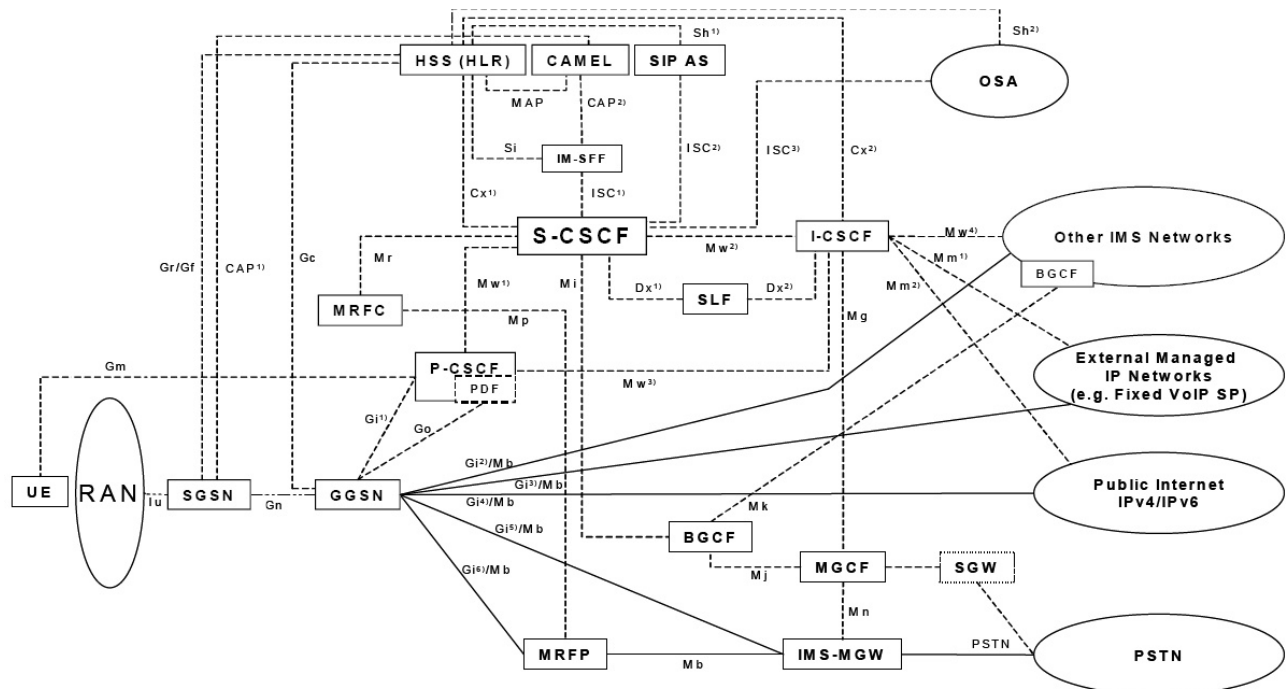


Figure 1: Logical Overview of Rel-5 IMS System Architecture

Proxy-CSCF (P-CSCF) is the first contact point for UE within the IMS. The Policy Control Function (PCF) is a logical entity of the P-CSCF, which manages resource reservation from the GGSN. The main function performed by the P-CSCF is forwarding of the SIP messages from UE to other CSCFs and vice versa. P-CSCF is situated in the same network as GGSN.

Serving-CSCF (S-CSCF) performs the session control services for the end point. The main functions performed by S-CSCF are registration, session control for registered end points and interaction with service platforms. S-CSCF is always situated in the home network, even in the roaming situation and when the services of the visited network are used. Thus the subscriber is always registered into S-CSCF of the home network for purpose of charging and needed interface to HSS.

Interrogating-CSCF (I-CSCF) is the contact point with external networks. Also during registration or session establishment I-CSCF is used to find out the correct S-CSCF from HSS. SIP Register is always routed from P-CSCF (whether Home or Visited Network) to I-CSCF in Home Network. A session establishment (e.g. SIP Invite) is routed directly from P-CSCF to S-CSCF in Home Network and further more towards I-CSCF to find out S-CSCF in terminating network. A THIG (Topology Hiding Inter-network Gateway) function within I-CSCF may be optionally utilized to hide the internal structure of operator's IMS network. An IMS operator may use the THIG functionality when interacting with other IMS or external IP based networks.

Domain Name System (DNS) is used to resolve the IP addresses of IMS entities; E.164 numbers (ENUM DNS) and fully qualified domain names.

MRF (Multimedia Resource Function) performs multiparty call and multi-media conferencing functions. MRF is responsible for bearer control with GGSN and IMS-MGW. MRF consists of two parts MRFC (Multimedia Resource Function Controller) and MRFP (Multimedia Resource Function Processor).

BGCF (Breakout Gateway Control Function) selects the network in which PSTN breakout is to occur.

MGCF (Media Gateway Control Function) is used to control **IMS-MGW (IP Multimedia – Media Gateway)**. IMS-MGW is used for PSTN or CS-domain interconnection. MGCF converts application layer protocols (e.g. ISUP) to SIP.

SGW (Signalling Gateway) is used for e.g. ISUP-over-IP/ISUP-over-SS7 transport layer conversion between IMS and PSTN.

HSS (Home Subscriber Server) is responsible for holding following user-related information: user identification, numbering, addressing, security, location management and user profile information. HSS includes all legacy HLR interfaces and functions.

SLF (Subscription Locator Function) is used to find out the correct HSS. The SLF is not required in a single-HSS environment. SLF is queried during the Registration and Session Setup to get the address of the HSS containing the required subscriber specific data.

It should be noted that in IMS the signalling, i.e. SIP based session control, is separated from the actual user plane, i.e. application payload.

4 ROAMING

It is very important to notice and understand the difference between IMS roaming and interworking. This chapter handles roaming issues; for interworking please see the following chapter.

In principle IMS roaming means that VPLMN packet network resources are used in order to connect to IMS core network, which resides in HPLMN (typical case) or in VPLMN. Even in the latter case only P-CSCF can be in visited network (i.e. P-CSCF and GGSN are always located in the same network), all other IMS core elements are always located at the home network. Thus, the subscriber is always registered with S-CSCF of the home network for the purpose of charging and interfaces to HSS, which is used for e.g. service provisioning needs.

Roaming in IMS case doesn't necessarily differ from normal GPRS roaming from inter-PLMN network point of view because IMS traffic is transferred on top of GTP tunnel, as any other data.

When an IMS subscriber is located at his/her home GPRS/IMS networks he/she will normally access IMS services through a home network Access Point (GGSN). In a roaming scenario, the subscriber either uses a visited network Access Point or a home network Access Point. The home network can restrict use of visited network Access Point.

Figure 2 shows the usual scenario where the user has chosen to use a home network AP to access IMS services. This is a normal GPRS roaming situation where GGSN is in the home network and GTP tunnelling is used across the inter-operator backbone network (e.g. GRX). The visited network doesn't even have to have an IMS domain in this case.

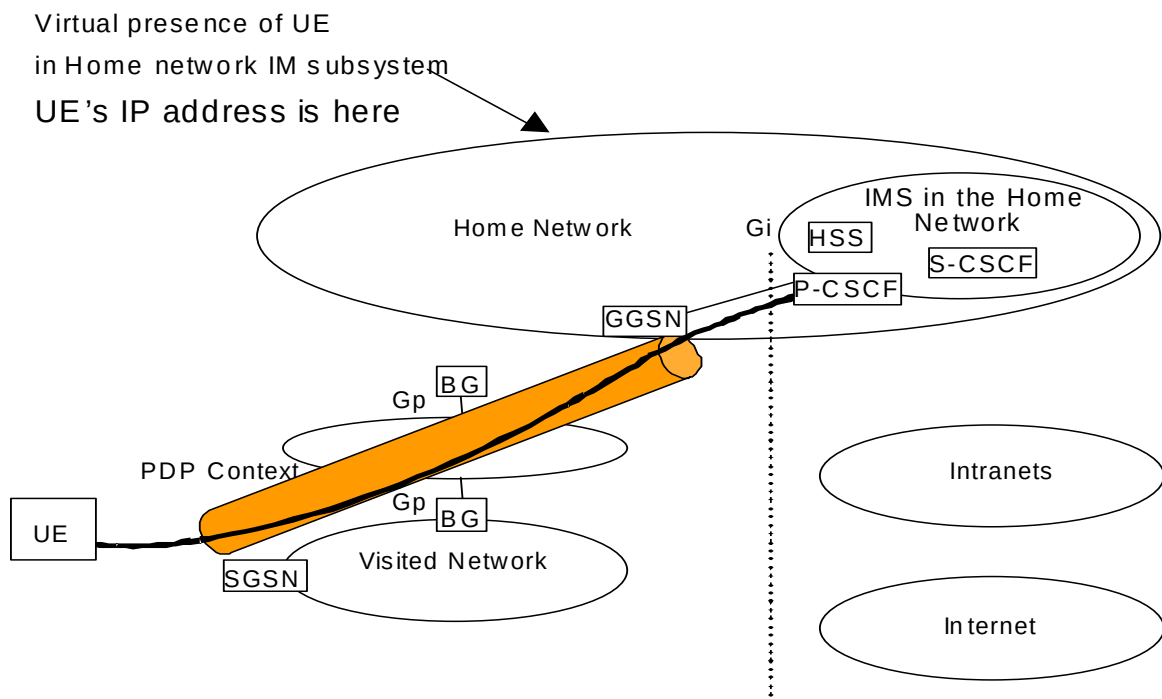


Figure 2: UE Accessing IM CN subsystem Services with GGSN in HPLMN

In the first phase IMS services are likely always used from home network. Consequently IMS roaming is almost similar as GPRS roaming – both from technical and business point of view – since all IMS traffic (SIP, RTP, etc.) is transparent to roaming network and visited network.

Figure 3 presents the scenario where the roaming subscriber uses the visited IMS network. In this case the IPv6 address assigned to the IMS terminal is from the visited network-addressing domain. I-CSCF is a contact point between visited and home networks. In the figure, I-CSCF is only used in home network. Thus, P-CSCF of visited network discusses directly with I-CSCF of home network. Deployment of the I-CSCF functionality provides additional benefits as described in chapters 3.2 and 7.2.

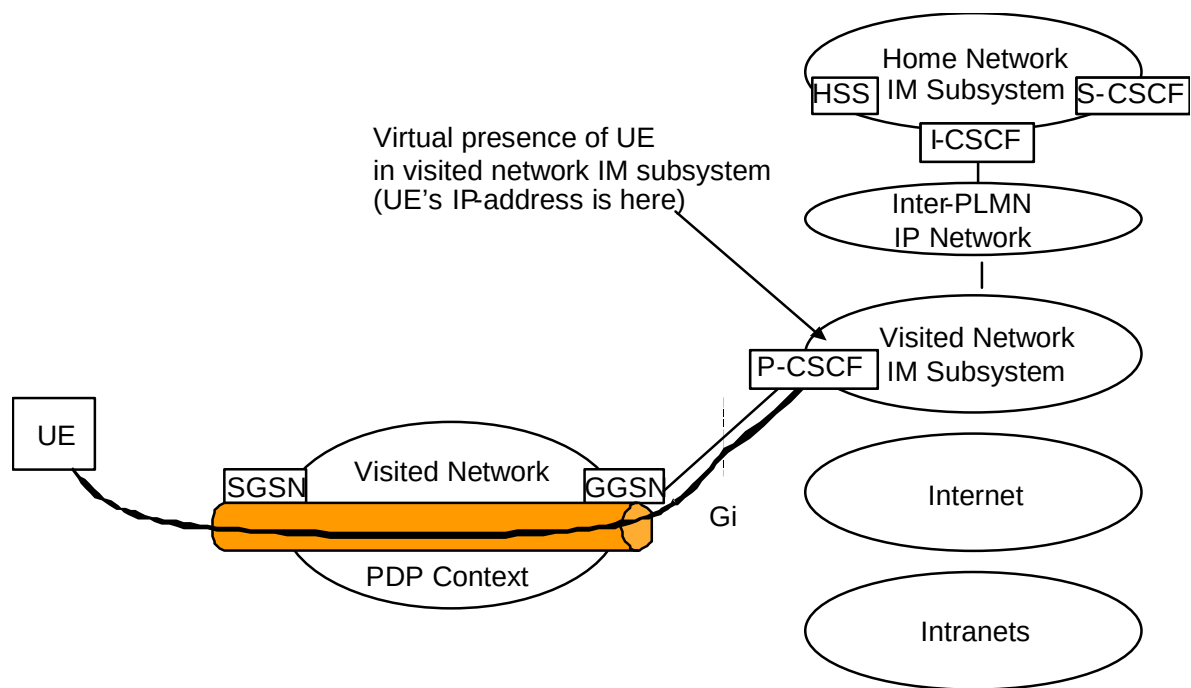


Figure 3: UE Accessing IM Subsystem Services with GGSN in VPLMN

It is likely that the scenario where GGSN is in the home network is the preferred model also for IMS roaming, at least in the first phase. Therefore it should be beneficial for operators to concentrate on this scenario, for now. Using the visited IMS network can offer some benefits, but implementing it is likely feasible later, when the level of real-time traffic increases and therefore issues such as improved QoS control & optimizing routing will become more important.

5 INTERWORKING

In this context the meaning of term IMS interworking is that home network packet resources are used in order to connect to home network IMS core resources and utilize these to set up a session with a customer or a service of another IMS capable network, independently of whether the customer is roaming or not. In another words, IMS interworking means that two different IMS networks are connected through inter-PLMN IP network to enable SIP control and transport of user plane.

Figure 4 shows the usual scenario for IMS interworking between two different IMS networks. This figure presents interworking between IMS originated and IMS terminated network. SIP controlling is delivered via Mw interface and user plane is transported via Gi interface. The actual IMS user traffic is routed directly between the involved GGSNs, while SIP controlling always flows via IMS core networks.

I-CSCF is used as a contact point between operator networks. S-CSCF of originating network discusses either directly or via I-CSCF with I-CSCF of terminating network. Use of I-CSCF in originating network is optional, but may provide additional benefits as described in chapters 3.2 and 6.3.

The inter-PLMN IP network must provide reliable transmission as in case of IMS roaming. Usage of DNS has special importance in interworking scenarios, further details are described in chapter 9.

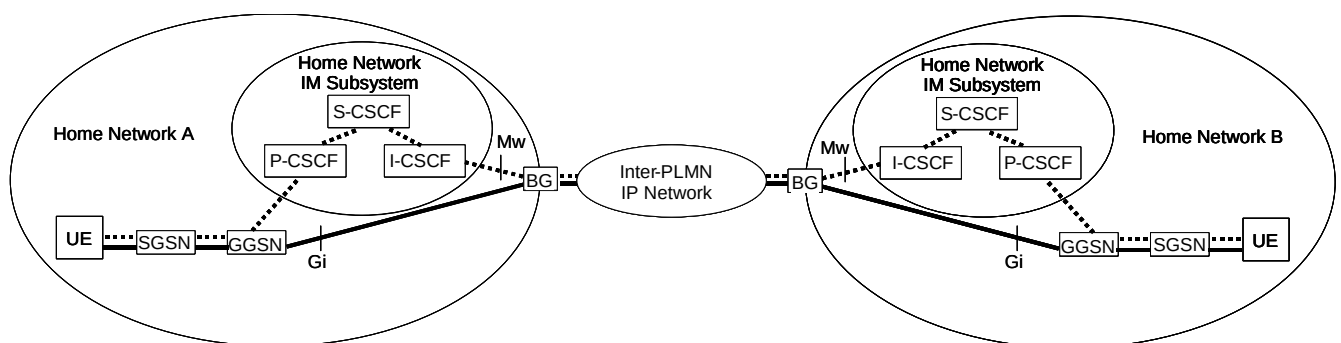


Figure 4: Interworking between two different IMS operators

Interworking with Internet and corporate intranets is not handled in detail, although Chapter 7 considers some issues that are valid also when connecting to these networks.

Interworking with CS networks (CS-domain and PSTN) is needed for call routing between IMS operator and non-IMS operator. 3GPP specifications TS 29.163 [8] and TS 24.228 [6] cover interfaces and signalling in these cases.

Routing from IMS network to CS network associates to PSTN breakout functionality, which means that an IMS call session is established towards CS networks. The PSTN breakout occurs if the type of B-party address is "TEL" (e.g. E.164) instead of SIP URI and there is no IMS subscription available in HSS. In the PSTN breakout BGCF selects the terminating network according to the defined rules. A session is forwarded either to local MGCF (via Mj interface) or to BGCF of terminating network (via Mk interface). MGCF routes call establishment towards

terminating network and handles the needed protocol interworking between 3GPP SIP, BICC/SIP-I and ISUP for controlling. IMS-MGW handles the user plane transporting between IP (Mb interface) and PSTN interface. Thus, call breakout to PSTN can be done either in originating or terminating network, depending on the agreement between operators.

CS originated calls routed towards IMS are handled as any other CS call. If the CS call is to be terminated in IMS, the signalling is terminated in MGCF, which forwards the session to CSCF via Mg interface (3GPP SIP).

6 REQUIREMENTS FOR THE INTER-PLMN NETWORK

6.1 General Issues

General requirements for the inter-PLMN backbone shall be applied from IR.34 "Inter-PLMN backbone guidelines" [1].

From a technical point of view the required IP network between different operators might be e.g. public Internet (with VPN) or direct leased line such as Frame relay or ATM. Another solution, which in many cases could be considered to be the advisable one, is to utilize an existing, proven and reliable inter-operator IP network, i.e. GRX, as specified in IR.34 [1]. This requires some modifications to GRX specifications, but as a result transferring IMS related traffic between different operators is as simple as GPRS roaming traffic. Given these modifications are done, IMS traffic can be routed as IP based traffic on top of GRX.

Using GRX networks to carry IMS traffic is less onerous than building direct connections between each and every IMS network in the world. Operators should evaluate the physical connect for IMS roaming & IW and choose the most appropriate. One suggestion would be to use GRX as the default routing choice but where traffic is high (typically between national carriers) a leased line or IP-VPN may be more cost effective. As the IP routing is separate from the physical topology, multiple physical connections may co-exist. In practice operators may have several physical interconnection links: leased line for national traffic, IP-VPN for medium volume or non-PLMN and GRX for all others. The DNS system will resolve the destination domain to an IP address that will be routed over the appropriate link.

There is no need to build any kind of separate "IMS Roaming & Interworking Exchange network" only for IMS traffic. Issues such as QoS, security, control of interworking networks, overall reliability and issuing of new network features such as support for ENUM are easier handled inside GRX than when using public internet to relay IMS traffic between operators. This is due to the fact that GRX can be considered to be a closed operator controlled network unlike public Internet, which is totally open for everyone.

Consequently, preferred inter-PLMN network also in IMS case is GRX, as it is already preferred network in e.g. GPRS roaming, MMS interworking and WLAN roaming. Existing networks can be reused as much as possible instead of building separate networks for each and every new service. There is no need for new separate VPNs inside GRX for IMS traffic, since IMS traffic can co-exist with current GRX protocols, such as GTP and SMTP.

6.2 IP Version Issues

Originally, 3GPP specifications defined IMS as IPv6 only. However, that decision has been changed and IMS core systems & terminals can be either IPv6 or IPv4 based. General usage of IPv4 and IPv6 regarding IMS is detailed in 3GPP Technical Report 23.981 [19].

IPv6 sets following requirements for roaming and interworking scenarios:

- IMS roaming using home network GGSN (typical scenario)
- IPv6 PDP context type must be supported in visited network SGSN
- IPv6 packets are tunnelled transparently within GTPv1. Thus, it requires no specific IPv6 support from GRX network

IMS roaming using visited network GGSN

- IPv6 PDP context type must be supported in visited network SGSN

- IPv6 connectivity via inter-PLMN network (GRX) must be supported. Native IPv6 support (preferred) or configured tunnelling should be used.
- IPv6 support in inter-operator DNS (see chapter 9)

IMS interworking

- IPv6 connectivity via inter-PLMN network (GRX) must be supported. Native IPv6 support (preferred) or configured tunnelling should be used.
- IPv6 support in inter-operator DNS (see chapter 9)

One alternative for roaming could be use IPv6-over-IPv4 tunnelling in terminal, thus this way it could be possible to use IPv6 while roaming even if VPLMN SGSN does not support IPv6. If Home GGSN model is used, no additional support is required from VPLMN, i.e. traffic is routed within a normal GTP tunnel to the HPLMN. E.g. ISATAP as defined by IETF could be utilized for this tunnelling method.

Native IPv6 support in GRX is the preferred solution. During transition period, while native IPv6 support is not available yet, IPv6-over-IPv4 tunnelling can be used. IETF has specified several flavours of IPv6 tunnelling, for example “Configured Tunnelling” (RFC2893). Also GRE tunnel (RFC 2784) could be utilized. However, from a mobile operator's point of view it is more or less transparent whether GRX providers support IPv6 natively or via tunnelling.

IPv6 transition in inter-PLMN networks is for further study, for example issues such as performance, QoS, availability and costs will be investigated in co-operation with GRX providers.

Peering is an important issue to be considered, since obviously also IPv6 based traffic needs to flow between different operators and different GRX providers in a same fashion than IPv4 based traffic. Thus, mobile operators connecting to each other with IPv6 need to check whether inter-PLMN connection supports IPv6 (all related GRX networks natively or via tunnelling, as well as IPv6 support in necessary peering points).

6.3 Security Issues

In order to maintain proper level of security within the inter-PLMN backbone certain requirements for GPRS operators and Inter-PLMN backbone providers should be taken into account. Same security aspects shall be applied as described in IR.34 [1].

It is strongly recommended that operators should implement firewalls adjacent to Border Gateways. Generally operators should allow only routing information (BGP), GTP traffic, signalling, DNS, SMTP and SIP traffic. However, also traffic related to IMS user plane (such as RTP and HTTP) should be allowed due to IMS interworking. Therefore, due to potentially numerous new protocols introduced by IMS interworking, there should not be any kind of restrictions on the used protocols or port numbers in the GRX anymore. This means that any security mechanisms based on restricting protocols inside the actual GRX network must be replaced by another method. It is important to note that also firewalls must support IPv6 when IPv6 is used.

Security gateways (SEGs) should be used at the border of an operator network, as specified in TS 33.210 [10], if used inter-PLMN network does not offer security by itself. Using SEGs with GRX can be questioned, since IPSec connections are mandatory between SEGs. IPSec tunnels between CSCFs are not needed, if GRX is used, since GRX network by itself provides comparable level of security as IPSec tunnel. SEG is responsible for enforcing security policies for the inter-network traffic; all incoming & outgoing IP traffic shall pass through it.

Usage of IPSec is mandatory if public Internet is used as an inter-PLMN network, i.e. IMS connection must always be secured at some level. If IPSec is used in inter-PLMN IMS connections, it is recommend using the common IPSec parameter set as specified in IR.61 [12] in order to reduce the number of options.

Above all, operators should realize that the actual security level of the whole IMS system depends on much more than just securing the transportation between CSCFs. This is done on an operational service level, where it is decided how these services are deployed and used. GRX itself is nothing else than just IP bearer network, which does not provide any kind of actual security features besides the fact that no outsider should be able to access the GRX network.

Security issues related to IMS services, such as Peer-to-Peer traffic, are for further study.

6.4 Proxy

Optionally Inter-PLMN IP network may deploy an additional element for IMS interworking routing. This separate intermediate Proxy functionality allows operator to make just a single connection from its own IMS core system to the Proxy in the inter-PLMN network regardless of the number of IMS interworking partners. The Proxy is responsible for routing traffic towards correct recipient network.

Within the GSMA SIP Trial activities a number of Proxies have been deployed by different GRX carriers using term “IPX Proxy”. Basically IPX Proxy is a SIP proxy with additional functionality to meet the operator requirements for IMS interworking interface.

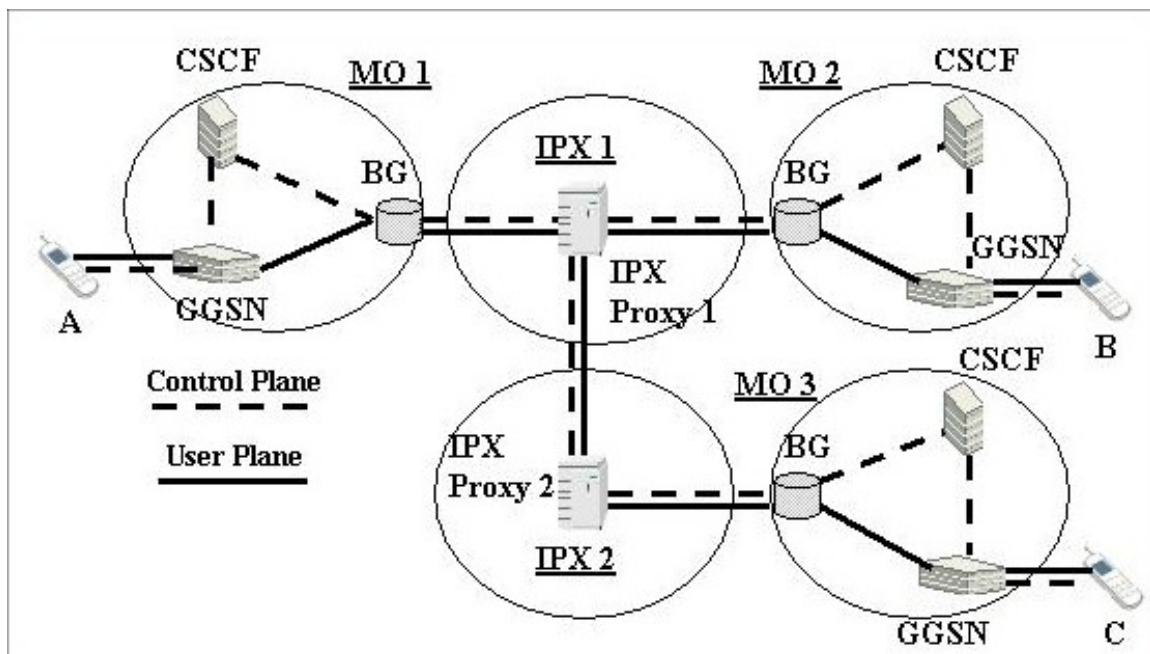


Figure 5: Overall Architecture of IMS Interworking using the Proxy Model

In addition to solving the many-to-many routing problem as described above, following type of functions could be offered by Proxy for IMS interworking purposes:

- Proxy is a logical place for inter-operator charging data creation, since traffic is routed through it
- Proxy is able to route traffic between overlapping IP addresses (such as private IPv4 addresses widely used for terminals)

- Proxy can take care of IP version conversion in case this is not handled by operators themselves
- Proxy has capability for traffic control/policing
- Proxy is able to perform control plane modifications, such as map between different SIP profiles
- Proxy can perform user plane modifications, e.g. transcoding between different voice codecs
- Proxy can perform also ENUM queries on behalf of operator
- Optionally Proxy provider could also possibly function as a commercial broker, meaning that one agreement between operator and Proxy could offer a number of interworking partners

For further detailed information about this kind of additional Proxy functionality offered by inter-PLMN IP network, please see Annex B of GSMA PRD *IR.34 Inter-PLMN Backbone Guidelines*.

7 REQUIREMENTS FOR THE PLMN NETWORK

7.1 IP Version Issues

General usage of IPv4 and IPv6 regarding IMS is detailed in 3GPP Technical Report 23.981 [19].

As shown in the Figure 5, it is possible to use IPv6 on “user IP layer” between terminal and IMS core system/application server regardless of what IP version “network IP layer” uses. Thus as long as IPv6 context type is supported in SGSN and GGSN elements, IPv6 can be used on IMS application layer even though network layer supports only IPv4. I.e. there is not necessarily a need to upgrade network IP layer due to introduction of IPv6.

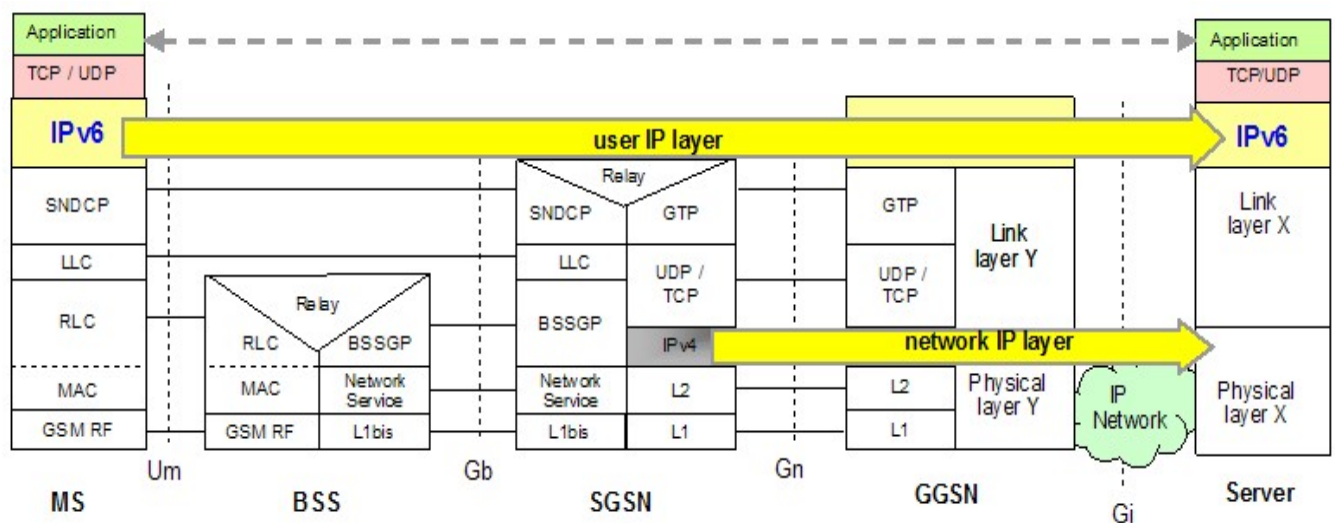


Figure 6: User & Network IP Layers in MS-to-Server Connection

As earlier mentioned, there will be IMS core systems supporting different IP versions (only IPv4, only IPv6 or dual-stack). In any case, optimal solution would be to use only IPv6 based IMS interworking because of following problems:

- A mixture of two versions of IP in IMS interworking would increase the complexity of the solution leading to additional operational efforts and costs
- Connectivity between IMS core systems using different IP versions would require IPv4/IPv6 protocol translation, i.e. deployment of NAT-PT & ALG devices, which involves e.g. scalability problems.

Due to lack of available addresses it is likely that all operators cannot use public IPv4 addresses, even though this would enable more feasible implementation of IPv4 IMS interworking. Therefore, the following difficulties concerning inter-PLMN connectivity with private IPv4 addresses must be taken into account:

1. Direct IPv4 terminal-to-terminal connection (IMS interworking using a peer-to-peer service):
 - o Private IPv4 addresses could be handled also with NATs in both ends, but this requires SIP-ALG for translating IP addresses in SIP messages and setting-up the NAT tables accordingly for the media. Intermediate network element such as SBC (Session Border Controller) deployed within the operator network can be utilized for this purpose
 - o Another way would be agreeing private terminal addresses among operators, but this co-ordination of these address spaces is practically impossible as there are already large amount of operator internal private address spaces deployed
 - o Usage of Proxy in the inter-operator IP network (see Chapter 6.4) helps to address the problem of possible overlapping private IPv4 addresses used by terminals (and potentially also by servers), since Proxy would be responsible for making sure that in case where overlapping happens it can be successfully handled by the Proxy. Thus operators themselves would not need to co-ordinate address ranges or deploy additional network nodes such as SBC in case inter-operator traffic is routed via Proxy
2. IPv4 terminal-to-terminal via server connection (IMS interworking using a client-server service):
 - o If private addresses are used for mobile terminals, there has to be server-to-server protocol between operators' servers. Server-to-server interface must use inter-PLMN routable addresses, i.e. public IPv4 or IPv6. If server does not use IP address that is routable in the inter-operator IP network, it is possible to use e.g. SBC or IPX Proxy also for server-to-server traffic like illustrated above in the case of peer-to-peer traffic

Additionally, IP version issues affect also UEs, since if GRX is used as an inter-PLMN IP backbone, allowed IPv4 addresses should belong only to GRX address block. Other IPv4 address ranges are not routed according to IR.34 [1]. Thus, currently GRX does not support peer-to-peer connectivity between UEs with IPv4 addresses without using GRE to tunnel end-user traffic in order to mask UE IP addresses from GRX.

Intermediate network elements, such as NAT/NAPT/ALG device (e.g. Session Border Controller) in operator network or a gateway/proxy (e.g. IPX Proxy) residing in GRX network, can be used to handle IP version conversions. Necessary functionality could be also integrated as a part of IMS core system, depending on implementation.

Using e.g. IPX Proxy it is possible to automatically handle IP version conversion in such a way that mobile operators themselves would not necessarily need to modify anything, since all IP conversion could be "outsourced" to proxy operator. I.e. then IPv4 based Mobile Operator A would not need to purchase new equipment or modify settings while introducing interworking with IPv6 based Mobile Operator X.

As a general note, end-to-end IPv6 based connectivity would be optimal and would reduce the number of options, but it is quite obvious that there is need for IP address conversions in many cases of IMS inter-operator connections.

As a conclusion using IPv6 for IMS interworking would be the optimal solution, due to requirements posed by P2P services, for instance. However, also IPv4 can be supported, but this

can mean either some restrictions to the used services or deployment of tunnelling and/or intermediate network elements such as NAT/ALG or a proxy in GRX.

In roaming scenarios either IP version can be used, as long as VPLMN supports this (e.g. IPv6 PDP context type supported in SGSN).

7.2 Security Issues

One way to somewhat improve the security level of IMS interworking is to deploy a separate I-CSCF node, which is used as a SIP proxy. With I-CSCF the actual operator core can be hidden, since only the I-CSCF is utilized as a connection point with partners and must be visible. This may help to reduce the vulnerability of the overall system to external attacks (e.g. denial of service attacks). Additionally this can help simplify the problems of how to actually connect IMS core to inter-PLMN network, since it is likely that some sort of proxy/gateway is needed between those. IP address of this kind of component (e.g. I-CSCF) should be listed in PRD IR.21 for informing the roaming/interworking partners.

Another advantage of deploying separate I-CSCF is that you can easily rearrange IMS core elements, e.g. add a duplicate S-CSCF or change its IP address, without having to inform these changes to your roaming/IW partners, since only the I-CSCF IP address is known outside your own network. This is highly desirable from a network management perspective. THIG function of I-CSCF can also hide e.g. exact number and capabilities of S-CSCFs as well as the capacity of the network. However, using THIG could cause interoperability problems, because THIG modifies SIP headers in a non-standard way.

Due to reasons listed above it is recommended that operators deploy I-CSCF elements into their networks.

8 Service Related Issues

Different end-user services used in IMS have different requirements. As IMS allows basically any kind of IP based service to be used, issues regarding those have to be taken into account when thinking about inter-operator IMS connections. For example routing the PoC user plane & control plane between two operator PoC servers has quite different requirements than routing traffic between two users playing a peer-to-peer IMS game.

Typically these issues are more related to interworking rather than roaming, since in normal roaming scenario user always connects to home operator anyway, at least in the first phase. Later, when Visited GGSN roaming model can be used, it will probably mean some changes also to this basic concept.

The actual IMS based services and their requirements are listed in other documents, see e.g. PRD SE.35 - IMS Services & Applications [13]. This document handles only the specific inter-operator aspects of these different services.

8.1 PoC

One of the lead services for IMS deployment is PoC (Push-to-talk over Cellular). Key issues in PoC are that user plane always goes through PoC server and users are registered in their home network PoC server, therefore in interworking scenario user traffic traverses two PoC servers. Additional information about this half-duplex VoIP service can be found for example in PRD SE.36 - PoC Roaming and Inter-working Service Requirements [14].

In order to reduce the number of different options, this document concentrates on the only standardized version of PoC, i.e. PoC specified by OMA (Open Mobile Alliance), see e.g. [15]. OMA PoC servers may connect also to non-OMA compliant PoC servers, but the details of this are not within the scope of this document. Note that OMA PoC server can be deployed on top of IMS, but it can also be deployed on top of any general "SIP/IP core". As this document handles only the standardized IMS, other kinds of possible SIP/IP core implementations are out of scope.

It is assumed that the PoC architecture makes use of IMS capabilities in the 3GPP system. Reason for it is that the PoC server itself does not need to handle issues such as registration, address resolution, charging and AAA support as well as SIP compression, since those are supported by IMS core anyway. Detailed analysis of the requirements caused by PoC deployment for 3GPP based systems (such as IMS) is available in TR 23.979 - 3GPP enablers for OMA PoC Services [16].

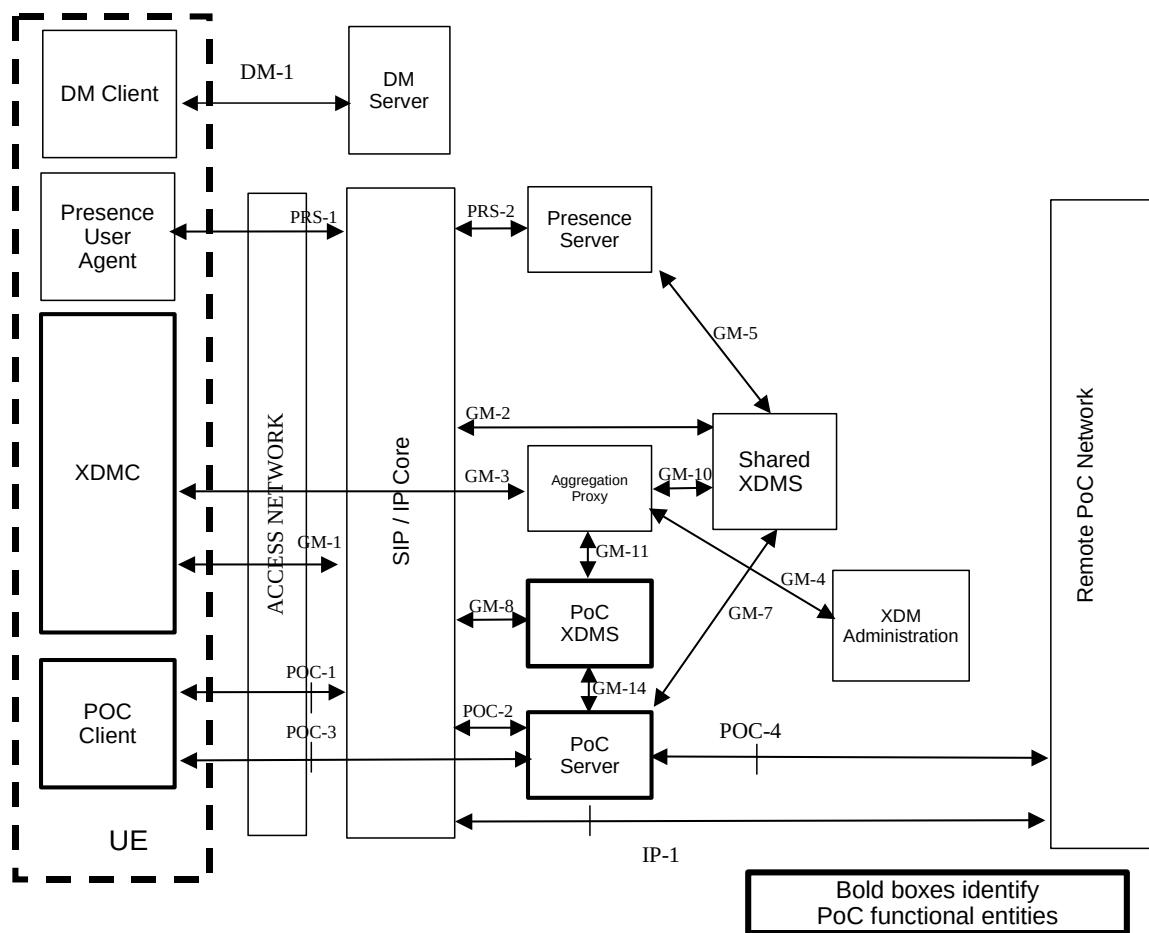


Figure 7: General OMA PoC Architecture [15]

PoC server implementing the application level network functionality for the PoC service is essentially seen as a general Application Server from the IMS perspective. Therefore the communication between the IMS core and the PoC server utilize the ISC interface (see TS 23.228). Note that presence support is optional in OMA PoC, i.e. operator might or might not have deployed the presence server.

For inter-operator PoC connection there are two interfaces: user plane (media + talk burst control, i.e. RTP + RTCP) is routed via POC-4 interface between PoC servers, while control plane (SIP signalling) is routed via IP-1 interface between IMS core networks. Both of these interfaces are IP based. It is envisioned that both POC-4 and IP-1 will be routed over GRX, as any other IMS interworking traffic. Anyway also the PoC user traffic needs to be protected from outsiders, either by using GRX network or by using VPN tunnels.

Deploying two separate network connections between operators needs somewhat more consideration than just a single connection, for example regarding the dual configuration of firewalls/border gateways towards inter-PLMN network. However, the IP-1 interface between IMS core networks is the same as for any other IMS based service, i.e. normal Mw interface is utilized. Thus deploying PoC interworking means that only the PoC server-to-PoC server interface (POC-4) will have to be implemented in the network layer, if these operators already have general IMS interworking in place.

Since PoC has a dedicated server-to-server interface, routing of interworking traffic over inter-PLMN interface is simpler than in services that lack this kind of interface. This is due to the fact a

server can have an address that belongs to GRX address block (i.e. is routable within GRX), while a terminal likely can not have this kind of address.

It is possible for IPv4 based PoC terminal to talk with IPv6 based PoC terminal, since PoC server can act as a translator. As PoC server can “hide” private IP addresses, it is possible to have interworking between different operators even if terminals in both ends are using operator own private IP addressing schemes, since the actual terminal addresses are invisible to the other operator.

PoC interworking traffic on GRX use either IPv4 or IPv6, depending on the implementation and commercial agreements. It should be possible to connect IPv6 based Terminal1 from Operator A to IPv6 based Terminal2 from Operator B using IPv4 based GRX connection, if both PoC servers are dual-stack capable.

As long as IP level connectivity is in order, there should not be any kind of major difficulty in configuring PoC interworking. PoC server connects directly to another PoC server for media transport and IMS core connects directly to another IMS core for control transport. For both roaming and interworking scenarios it is important to consider QoS related issues such as QoS offered by inter-PLMN network, since PoC is a near real time service.

8.2 Presence & Instant Messaging

Some IMS services are based on SIP signalling only, i.e. they do not use a separate user plane at all. For example Presence service as specified by 3GPP [17] is this kind of service. From routing perspective this can be quite easily handled, since only the IMS control plane is used, but there are still some challenges regarding Presence & IM interworking.

There will be a number of different Presence & IM implementations in the market; some natively use IMS, while most don't. In this document non-IMS based Presence & IM systems (such as Wireless Village) are not handled in detail, since they basically have nothing to do with the actual IMS system. IMS based Presence & IM systems may interwork with non-IMS based systems through GW, which handles necessary protocol conversions for example between SIP and Wireless Village protocols along with re-mapping of presence attributes.

3GPP has defined two modes for IM: immediate messaging (pager-mode in IETF) and session-based messaging. The main difference between these two modes is that immediate messaging uses SIP via control plane, while session-based messaging uses MSRP (Message Session Relay Protocol) via user plane. Therefore immediate messaging can use the SIP based control plane interworking interface Mw to send instant messages (using normal SIP MESSAGE method) between terminals, while session-based messaging requires a separate user plane. For session-based messaging transport there are two options: a direct terminal-to-terminal connection (without network support, similar to other peer-to-peer services) or connection via intermediate network components (such as messaging AS and/or MRFC/MRFP).

While immediate messaging can be supported by IMS core itself, a dedicated Presence & IM server is needed in order to have more advanced Presence & IM support in the operator network. From the IMS core point of view this is a general SIP Application Server, which is handled via ISC interface. This means that it is located using SIP URIs and IMS supports normal SIP routing, HSS query, ISC filtering etc. also for Presence & IMS server. Interworking of 3GPP compliant Presence service uses general IP based IMS core-to-IMS core signalling connection, i.e. Mw interface.

Since 3GPP Presence uses only the SIP signalling, it does not contain any IP addresses which would directly require deployment of SIP-ALG. Dual-stack IMS core provides necessary

conversion between IP versions, therefore the service can be provided without any additional NAT in the network.

3GPP compliant Presence should be successfully handled via normal IMS core-to-IMS core control plane connection, which utilizes SIP and can be routed over GRX network. Thus there is no need to deploy a separate interface or make any kind of modifications to normal inter-operator Mw interface for supporting this kind of service. 3GPP compliant IM interworking might need additional support, depending on the used mode.

8.3 Peer-to-Peer Services

The main difference between P2P (Peer-to-Peer) service and client-to-server service is that P2P does not need any kind of application related support from the network, while client-to-server requires some kind of server, such as MMSC or PoC server. Typical P2P services envisioned for IMS are different multi-player games (such as chess, battleship or Reversi), media sharing, imaging and multimedia streaming.

It is possible to deploy P2P services that totally bypass the operator, but this chapter concentrates on "IMS P2P services". Those are services that use the capabilities offered by IMS in order to execute e.g. authentication, registration, service discovery, address resolution and inviting the recipients instead of handling those issues by the P2P application itself. So, even if the media can go directly from one terminal to another terminal via GGSN without any intermediate server or proxy, these services require IMS to support setting up that service, i.e. signalling always goes via operator IMS core.

Different IMS based P2P services itself are typically not standardized; only the session set-up support offered by IMS is standardized. Operator, regardless of how the actual service is deployed, must always offer this session support.

Basically, IMS P2P services use control plane (SIP) to find the recipient, connect to it and send an invite (e.g. to multi-player game) via IMS core elements. After that a direct user plane connection (any kind of application dependent protocol on top of UDP or TCP) is opened between participating terminals via GGSN. Terminals in this scenario have a SIP stack and the required P2P application. Basically, operators just need to support set-up of P2P services with SIP signalling via IMS core, user plane does not necessarily need any kind of operator support.

One major issue to consider in P2P is security, since terminals have to be secured somehow even if direct terminal-to-terminal connections must be allowed. The main aim is to prevent users from attacking others. Standardized method for controlling these connections is GGSN Gating, i.e. use of Go interface. A possible solution for that is routing all traffic through "security gateway", which resides in the operator network, instead of opening a direct connection through GGSN between terminals. This kind of GW would allow some control over the terminal connections also in case P2P services are used.

When P2P service is used user plane is routed directly between terminals implying that terminal IP addresses are utilized in user plane. However, as discussed above typically terminal IP addresses are not routable in the inter-PLMN network, thus user plane needs to be put inside a tunnel in order to be routed over the inter-PLMN network, such as GRX. GRE tunnels are used for this purpose, see Chapter 7.1 for more information about IP address issues. Usage of tunnels also helps to increase the level of security by making sure that end-user traffic cannot be used to attack inter-operator IP network and operator backbone elements since the end-user traffic stays within the GRE tunnel.

Routing of P2P traffic between operators is handled via using normal Mw control plane interface to set-up the service and then routing the user plane over GRX between participating operators. Roaming scenario does not pose any additional requirements for this kind of service, since IMS user is always connected to home network.

8.3.1. Video Share

Video Share is an example of non-standardized IMS based peer-to-peer service. The terminal interoperable Real-Time Live Video Share service allows users to share live video between them over PS connection in real time simultaneously with an ongoing CS voice call. Video Share is a one-to-one unidirectional combinational (CSI) service utilizing 3GPP compliant IMS core systems. Sessions are set up using SIP and video is transferred using RTP. Inter-PLMN network such as GRX is used to route both signaling and media related to the Video Share service between operators. Handling of control plane in Video Share is similar to any other IMS service, i.e. Mw interface is used.

Basic requirements are the same as for other P2P services. Additionally Video Share service requires the inter-PLMN network to support the transport of SIP, RTP and RTCP protocols. As Video Share is a real-time service it has strict QoS requirements for media transport. It is important to notice that Video Share requires the support for terminal IP addresses used in user plane, within the inter-PLMN network this can be organized by using tunneling as discussed in Chapter 8.3.

It should be noted that Video Share is not standardized anywhere, but terminal vendors have implemented an interoperable service based on a technical definition document produced for GSMA SIP Trial purposes. For further details of the Video Share service, please see GSMA document *Video Share Definition*.

9 ADDRESSING and ROUTING

9.1 User Addressing

Every IMS user has at least one private user identity. Private user identity is assigned by the home operator, and used, for example, for Registration, Authorisation, Administration, and Accounting purposes. Private user identity is in the form of a Network Access Identifier (NAI) (RFC 2486), for example *joe.doe@carrier.com*. However, if UE has no ISIM application, private user identity is not known. Therefore it must be derived from the IMSI using the following form: *imsi@mnc<MNC>.mcc<MCC>.3gppnetwork.org*.

Private user identity is not used for actual routing of SIP messages, but it is contained in all registration requests when S-CSCF stores the private user identity. Private user identity is permanently allocated to a user in order to identify the subscription and it is stored in home operator HSS.

In addition to private user identity, every IMS user has one or more public user identities. The public user identity is used in e.g. user-to-user communication. For example, it might be included on a business card. Public user identity is not authenticated by the network during registration, but it must be registered before the identity can be used in IMS activities. Public user identities can be used to identify the user's information within the HSS. Format of public user identity is either SIP URI (RFC 3261& RFC 2396) or the "tel:"-URI format (RFC 2806), for example *sip:clint.eastwood@acme.org* or *tel: +358405344455*. If UE has no ISIM application to host the public user identity, a temporary public user identity must be derived from the IMSI: *sip:imsi@mnc<MNC>.mcc<MCC>.3gppnetwork.org*. However, this temporary identity is not visible for end-users and it is replaced by the actual public user identity fetched from HSS.

Routing of SIP signalling within the IMS uses SIP URIs. E.164 format public user identities are not used for direct routing within the IMS and session requests based upon E.164 format public user identities will require conversion into SIP URI format for internal IMS usage. This conversion is done using ENUM. In all roaming cases, visited network just forwards all requests to home network S-CSCF, which is then responsible for making ENUM query, if necessary. In case of interworking it is up to originating operator's S-CSCF to support this conversion mechanism. Details of conversion mechanism are for further study. However, MNP (Mobile Number Portability) is needed also for IMS.

CSCF, BGCF and MGCF nodes are identifiable using a valid SIP URI (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol. SIP URIs are used when identifying these nodes in header fields of SIP messages.

9.2 General Issues

DNS has an important role in IMS. During the session establishment an originating S-CSCF obtains the address of the I-CSCF for the network operator serving the destination user. Similarly during a registration a visited P-CSCF needs to resolve a home domain name to an address of I-CSCF in order to route SIP messages. DNS infrastructure is used for resolving an address of IMS contact point I-CSCF located in the home network

IMS typically uses multiple DNS queries, for example registration procedure requires at least 6 DNS queries, mobile originated call with E.164 numbers requires at least 3 DNS queries, and receiving a notification (SIP NOTIFY) from the AS requires approximately 4 DNS queries. Actual amount of queries is implementation dependent, but anyway the number of DNS queries

increases significantly in IMS compared to the current level of queries used in GPRS. Usage of cache, however, means that majority of these queries are transmitted only between resolver and the first configured/found DNS server.

3GPP has specified in TS 23.003 [11] that the home network domain name for IMS is *mnc<MNC>.mcc<MCC>.3gppnetwork.org*, if UE does not have an ISIM application. With ISIM operator can use whatever home network domain. At least in the first phase it is likely that all UEs do not have an ISIM application. Therefore this specified home network domain must be taken into consideration. All new services, including IMS, should use this domain name “.3gppnetwork.org” in GRX network. Existing network elements, such APNs, will continue to be addressed with .gprs domain.

There are actually two levels of DNS services regarding IMS framework. Firstly IMS core nodes (like CSCFs) need DNS services. Secondly GPRS core network nodes also use DNS services. The latter has importance especially in a roaming case and is related to inter-operator infrastructure. Level of integration between these two layers is somewhat difficult issue, as is the question of separation of IMS DNS hierarchy from Internet DNS hierarchy. If IMS related DNS was integrated to GRX, that would bring more industry steered freedom for example to DNS name delegation as well as easier and faster integration of new DNS functionality.

There are basically two major alternatives for IMS DNS deployment:

1. IMS domains are resolved using internet DNS infrastructure (e.g., .com)
2. IMS domains are resolved using GRX DNS infrastructure, with three possible implementation models:
 - o IMS Public User Identity (SIP URI) ends with .3gppnetwork.org
 - o Subset of operator's global DNS infrastructure is duplicated in GRX. Thus DNS server related to e.g. *ims.sonera.com* can be found using the DNS service offered by GRX
 - o A mixture of GRX DNS and operator internal mapping schemes is used

Solving IMS roaming & interworking in a reasonable manner with the currently existing GRX infrastructure is a somewhat challenging issue. Biggest requirements regarding this are:

- GRX domains & IP addresses should not be visible to public internet
- .3gppnetwork.org domain is usable only inside GRX network
- User identification cannot be fully controlled, each operator might use whatever naming scheme they wish

In the very first phase IMS roaming & interworking does not necessarily need DNS support, i.e. making inter-PLMN connections can be handled without DNS queries. For example the required IP address of I-CSCF can be found based on used home network domain using static lists by P-CSCF of visited network. However, later when the number of roaming & interworking partners starts to rise, this method likely becomes unmanageable due to amount of manual work needed. Note that IMS service itself relies on DNS right from the start.

Basically network node naming is not necessarily a major problem, since operators can make agreements to deal with it. However, user addressing is a more difficult issue to agree on.

IPv4 and IPv6 DNS information can coexist in the same name server. The smoothness of operation is an implementation issue. Basically operator just needs to make sure that DNS server software is capable of supporting resource records required by IPv6 (such as AAAA resource record). A name server serving both IPv6 and IPv4 resolvers also needs to be reachable using both IP versions.

Coexistence of separate networks means that there is requirement for certain IMS core elements to be reachable & routable from operator internal IP network as well as from inter-PLMN IP network, since they are used both in operator internal connections and inter-operator connections. Thus those IMS elements should be multi-homed or otherwise be capable of supporting two or more network addresses.

Also, IMS core should be capable of distinguishing whether DNS queries should be sent towards inter-PLMN DNS services or internal/public internet DNS services, due to separate DNS hierarchies. This issue is further discussed in chapter 9.4.

9.3 Roaming Specific Issues

Home-GGSN IMS roaming is transparent to GRX, it does not require any additional support from DNS, i.e. no new domains are needed in GRX DNS due to it. Visited-GGSN IMS roaming (i.e. GGSN and P-CSCF are located in visited network) however, needs to be supported by GRX DNS. This is due to the fact that visited network's P-CSCF must find the corresponding home network's I-CSCF based on the home network domain, which is part of Registration request send by UE.

This means that the home network domain is the only domain that needs support from GRX DNS in order to route Registration request in Visited-GGSN roaming case. Domain of private user identity is not used in actual routing, thus it is not necessary to include it into GRX DNS.

Consequently, in the first phase of IMS roaming there is no need for modifications to GRX DNS, since it is likely that IMS roaming will start with Home-GGSN model, which is transparent to GRX.

9.4 Interworking Specific Issues

IMS interworking needs additional support regarding used domains, since recipient belonging to another operator is addressed with user-friendly public user identity such as *mickey.mouse@sonera.fi* instead of *mickey.mouse@mnc123.mcc456.3gppnetwork.org*. Originating operator needs to be able to route INVITE SIP request towards recipient's I-CSCF based on only this *sonera.fi* domain. Therefore there has to some method mapping *sonera.fi* domain and the corresponding I-CSCF IP address. Logically this method would be DNS, but this is a bit problematic. Public DNS likely cannot be used in this, since I-CSCF IP addresses should not be available in public Internet. GRX DNS can neither be used, since GRX DNS should not be used to resolve public domains such as *sonera.fi*.

Figure 5 shows an example of services needed in IMS interworking during session establishment.

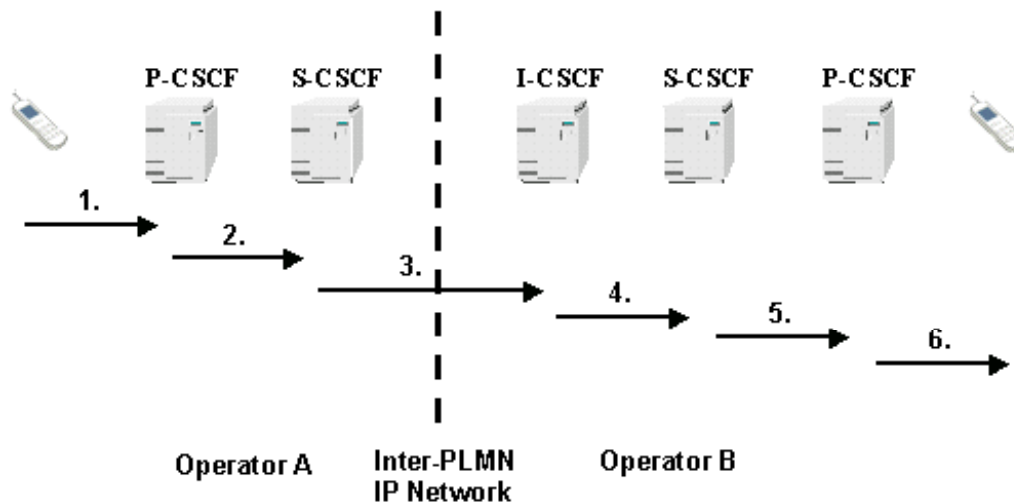


Figure 8: IMS Session Establishment Involving Interworking (Logical Model)

1. Calling User A sends a SIP INVITE containing the addressing information of the recipient User B (SIP URI: *mickey.mouse@sonera.fi*) to P-CSCF
2. P-CSCF forwards SIP INVITE to S-CSCF. DNS can be used to solve S-CSCF IP address by P-CSCF, if needed
3. S-CSCF checks destination domain from the URI of SIP INVITE ("*sonera.fi*") and uses DNS or other operator internal means to obtain IP address of I-CSCF for *sonera.fi*. SIP INVITE is then forwarded to I-CSCF via inter-PLMN IP network
4. CSCF of *sonera.fi* obtains IP address of S-CSCF for User B by utilizing DNS and then forwards SIP INVITE to it
5. After service analysis the S-CSCF of *sonera.fi* forwards SIP INVITE to P-CSCF, which was obtained during the registration procedures
6. P-CSCF forwards SIP INVITE to User B terminal based on the information obtained during the registration procedure

There are some ways to solve this DNS usage issue; all of these require the originating operator maintaining some kind of system by itself to support IMS interworking. This kind of distributed functionality is needed, since GRX DNS itself should not handle *.com* type of domain names. Main issue is to route all IMS inter-operator related queries to stay within the operator community (i.e. use only inter-operator DNS hierarchy), thus Internet DNS should be queried only in the case of traffic destined to external networks. Three ways to solve this issue:

- Use operator's internal DNS (or other database) to store statically configured information mapping domain to I-CSCF IP address (not recommended due to amount of manual labour needed in configuring this static information)
- Better solution would be to use a dynamic query, where each operator would deploy a "private operator DNS server", that replies with correct I-CSCF IP address when another "private operator DNS server" queries it. Addresses of these operator DNS servers itself would be stored in e.g. IR.21 database

Implementing this does not necessarily require additional equipment, for example the existing operator DNS server that is needed anyway due to e.g. GPRS roaming, can be reused for this purpose. Benefit of using this is reducing the number of static mappings to just one thus reducing management efforts and also handling of domain names becomes easier

- Third possible solution uses domain name rewriting by adding "*mncXXX.mccYYY.gprs*" to the domains that need to be resolved (e.g. *operator.com* => *operator.com.mnc123.mcc456.gprs*), therefore making these public domains resolvable for the GRX DNS. Rewriting can be done by the CSCF using internal rewrite lists mapping used public domain name and the corresponding MNC & MCC. But a better solution is to utilize NAPTR (Naming Authority Pointer Resource Record of DNS, RFC 3401-4) domain rewrite rules in the local operator DNS

If DNS solution is used, then CSCF sends a query for DNS concerning the public domain to be resolved. DNS reply contains the rewritten domain name, fetched from the domain specific NAPTR field. Supporting this kind of functionality means that each operator would maintain a list of its IMS partners in its local DNS

Note: The operator should register the domain used in public user identity in order to prevent any problems.

Also, it might be beneficial if operators could agree on the used domain model for IMS public user addressing, e.g. *ims.operator.com*. However, various different domains can be handled, as long as everybody is aware of which domain belongs to which operator. For example, these domains could be listed in IR.21 database.

Since *operator.com* type of domains can exist also in public Internet, care is needed with domain queries in order to avoid mixing these two separate issues. For example it might be possible for IMS user to connect also to fixed line SIP clients, therefore this fixed line recipient (such as *elvis.presley@graceland.com*) needs to be discovered by utilizing normal public internet DNS queries. One solution could be to first check every outgoing domain with internal mapping mechanism and if no I-CSCF is found, then query this domain from public internet DNS and route it there.

Regardless of used solution, it is quite clear that connections between IMS network and public internet can cause several problems, related to e.g. security issues and DNS usage. It is likely desirable to offer IP based communication between IMS users and internet SIP clients, but it must be understood that this requirement adds complexity to IMS deployment model. Especially incoming connections originating from internet are problematic. Operators could e.g. deploy one dedicated I-CSCF just for internet access.

10 CONCLUSIONS

The new paradigm of peer-to-peer IP communications (such as creating a multimedia session including a video stream between mobile terminals) reaches far beyond the capabilities of the good old telephony. It also requires substantially more sophisticated network infrastructure than just plain GPRS connectivity to general Internet services. SIP based session management complemented with the critical mobile network capabilities i.e. authentication, charging, roaming and interworking provided by IMS can offer the required service infrastructure.

Above all, it should be understood that there is no equal standardized system designed for mobile networks, which could be used instead of IMS. IMS allows operators to benefit from a unified infrastructure for new, advanced IP based mobile services. All relevant vendors will implement IMS. Furthermore, the most significant operators have shown great interest to IMS. Thus, IMS market will clearly emerge during the next couple of years.

Successful roaming & interworking is crucial for the success of IMS. Hence it must be handled as soon as possible. Preferred way is to follow common GSM Association guidelines right from the start rather than try to implement a number of different solutions and later see what solution becomes the de facto standard.

A summary of the main conclusions and recommendations concerning IMS roaming and interworking:

- There is no need to build any kind of separate "IMS Roaming & Interworking Exchange network" only for IMS traffic
- The preferred inter-PLMN IP network also in case of IMS roaming and interworking is GRX, since IMS traffic can be routed on top of GRX as any other IP traffic
- It is recommended to minimize the deployment of IPv4 based IMS interworking
- During transition period, while native IPv6 support is not available yet, IPv6-over-IPv4 tunnelling can be used. The most preferable tunnelling mechanism for GRX environment is 'configured tunnelling' (RFC2893)
- Security mechanisms based on restricting protocols inside the actual GRX network must be replaced by another method
- Operators are recommended to deploy I-CSCF elements into their networks
- Home-GGSN IMS roaming is transparent to GRX, it does not require any additional support from DNS
- Some IMS core elements need to be multi-homed (or otherwise configured in similar fashion) in order to be reachable & routable from inter-PLMN network as well as from public networks
- Public user identity in IMS will use various domains such as *operator.com*. Operators should register these domains
- DNS queries regarding IMS interworking need to stay within the operator community, i.e. use only inter-operator DNS hierarchy instead of public internet DNS
- Deploying connection between IMS and internet (e.g. SIP client in PC) require special care, due to security issues and handling of DNS queries

Preferred actions needed in order to successfully handle the technical aspects of IMS interworking & roaming:

- Explore what is the best operator controlled DNS deployment model for IMS look-up
- Check whether the current DNS systems are capable of handling the increased number of queries that IMS will introduce

- Study how address resolution issues (including MNP support) are solved in IMS, for example could operator ENUM be deployed in a feasible timeframe
- Make sure that the need for IPv6 support is well investigated, including IPv4 to IPv6 transition issues
- Modify GRX specification in order to support IMS roaming & interworking
- Study the IMS addressing issues, for IMS components as well as users
- Investigate whether IMS system should be opened for users outside the IMS domain, e.g. SIP clients in public internet, and how this could be successfully handled
- Study how IR.21 should be updated to support also IMS roaming & interworking
Investigate the IMS backwards compatibility issue

11 REFERENCES

1. PRD IR.34 Inter-PLMN Backbone Guidelines
2. IETF RFC 3261 Session Initiation Protocol (SIP)
3. TS 22.228 IP Multimedia Subsystem, Stage 1
4. TS 23.002 UMTS Release 5 Network Architecture
5. TS 23.228 IP Multimedia Subsystem, Stage 2
6. TS 24.228 Signalling flows for the IP multimedia call control based on SIP and SDP
7. TS 24.229 IP Multimedia Call Control Protocol based on SIP and SDP
8. TS 29.163 Interworking between the IMS and CS networks
9. TS 29.162 Interworking between the IMS and IP networks
10. TS 33.210 IP network level security
11. TS 23.003 Numbering, addressing and identification
12. PRD IR.61 WLAN Roaming Guidelines
13. PRD SE.35 IMS Services and Applications
14. PRD SE.36 PoC Roaming and Inter-working Service Requirements
15. OMA Push to talk over Cellular (PoC) - Architecture
16. TR 23.979 3GPP enablers for OMA PoC Services
17. TS 23.141 Presence Service, Architecture and functional description
18. PRD BA.27 Charging and Accounting Principles
19. TR 23.981 Interworking aspects and migration scenarios for IPv4 based IMS Implementations