

IMS Roaming, Interconnection and Interworking Guidelines

Version 32.0

14 October 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2020 GSM Association

Disclaimer

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.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Scope 5
1.3 Definitions 6
1.4 Abbreviations 6
1.5 References 9
2 Roaming Guidelines for EPS 11
2.1 Introduction 11
2.2 3GPP Background 11
2.3 Operational Requirements for IMS Voice and Video and other IMS Services based on Local Breakout and P-CSCF in VPMN 13
2.3.1 Operational Requirements for IMS Voice and Video 13
2.3.2 Operational Requirements for RCS Services 15
2.3.3 Operational Requirements for SMSoIP 15
2.4 IMS Roaming Architecture 16
2.4.1 General 16
2.4.2 VoIMS Roaming Architecture using LBO 16
2.4.3 IMS Roaming Architecture using S8HR 17
2.5 Support for Non-Voice IMS Services 18
2.6 IMS Roaming Guidelines 19
2.7 SIGCOMP 19
2.8 Support of Home-Local and Geo-Local Numbers 20
2.8.1 Home-Local and Geo-Local Numbers Overview 20
2.8.2 Home-Local and Geo-Local Numbers when visited network routing is applied (LBO-VR) for VoIMS 20
2.8.3 Home-Local and Geo-Local Numbers when home-routing is applied (S8HR or LBO-HR) 20
2.9 Support of Emergency Calls with S8HR architecture 20
2.9.1 Impact on the VPMN using IMS Emergency Call (void) 21
2.9.2 Impact on the HPMN for non UE detectable emergency calls 21
2.10 Gate Control and Traffic Policing 22
2.11 Support of Originated User Identity in Terminating Requests 22
2.12 Support of Basic SRVCC Procedures with S8HR Architecture 23
2.12.1 General SRVCC requirements 23
2.12.2 SIP-I between Roaming Partners 24
2.12.3 CS NNI between Roaming Partners 25
2.12.4 Handover Time 26
2.13 Support of Enhanced SRVCC Procedures with S8HR Architecture 27
2A Roaming Guidelines for 5GS 27
2A.1 Introduction 27
2A.2 3GPP Background 27
2A.3 Operational Requirements 29
2A.4 IMS Roaming Architecture 30

2A.4.1 General 30
2A.4.2 IMS Roaming Architecture using LBO 30
2A.4.3 IMS Roaming Architecture using N9HR 31
2A.5 Support of Non-Voice IMS services 31
2A.7 SIGCOMP 32
2A.8 Support of Home-Local and Geo-Local Numbers 32
2A.9 Support of Emergency Calls with S9HR architecture 32
2A.10 Gate Control and Traffic Policing 32
2A.11 Support of Originated User Identity in Terminating Requests 32
2A.12 Support of Basic SRVCC Procedures with N9HR Architecture 32
3 Interconnection Guidelines 32
3.1 Introduction 32
3.2 Ici/Izi Interfaces 33
3.3 Mw and Mb Interfaces 34
3.4 Overview 34
4 Inter-Service Provider IP Backbone Guidelines 35
4.1 General 35
4.2 IP Addressing 36
4.3 Security 36
4.4 Proxy 36
4.5 Media Routing 37
5 Service Related Guidelines 37
5.1 Introduction 37
5.2 IMS Based Voice and Video Communication 37
5.2.1 Overview 37
5.2.2 Multiple Voice NNIs 38
5.2.3 VoIMS NNI 41
5.2.4 IMS to CS Interworking 43
5.2.5 General Issues 44
5.2.6 IMS Voice & Video: SDP Offer and Answer 44
5.3 PoC 45
5.4 Peer-to-Peer Services 45
5.5 RCS 46
5.5.1 RCS Functional Architecture 47
5.5.2 Service Providers Identification 49
5.5.3 A2P/P2P Traffic Discrimination 49
5.5.4 Discovery and Routing (Resolving Number Portability) 50
5.6 HDVC 50
5.7 IMS NNI in case of multiple IMS core network deployments 50
6 Addressing and Routing Guidelines 51
6.1 User and UE Addressing 51
6.2 Node Addressing 52
6.2.1 P-CSCF Identifier Coding 52

6.3 Network Address Translation (NAT) / Network Address and Port Translation (NAPT) 53
6.4 Routing 53
6.4.1 General 53
6.4.2 Roaming 53
6.4.3 Interconnection 54
6.5 Identification of Services 55
6.5.1 Overview 55
6.5.2 Service Request over the Originating Roaming II-NNI 56
6.5.3 Special Consideration for Non-INVITE Initial SIP Requests 56
6.5.4 ICSI-Values and Alternative Methods to Identify a Service 57
6.5.5 Service Request Over the Terminating Roaming II-NNI 57
Annex A IMS to CS Voice Interworking 58
Annex B Usage of 3GPP TS 29.165 for HDVC 61
B.1 Control Plane Interconnection 61
B.1.1 SIP Methods Relevant for HDVC 61
B.1.2 Major Capabilities 63
B.1.3 Control Plane Transport 65
B.2 User Plane Interconnection 65
B.2.1 Media & Codecs 65
B.2.2 User Plane Transport 66
B.3 Summary of SIP Header Fields 66
Annex C IPX Proxy Requirements 68
C.1 Introduction 68
C.1.1 General 68
C.1.2 IPX Provider Requirements 68
C.1.3 Operational Requirements 70
Annex D SRVCC Performance with S8HR & CS NNI 71
Annex E Document Management 72
E.1 Document History 72
Other Information 75

1 Introduction

1.1 Overview

The 3rd Generation Partnership Project (3GPP) architecture has introduced a subsystem known as the IP Multimedia Subsystem (IMS) as an addition 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 and applications on top of a packet bearer.

3GPP has chosen the Session Initiation Protocol (SIP) [2] for control plane signaling 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 a text-based request-response application level protocol developed by the Internet Engineering Task Force (IETF). Although 3GPP has adopted SIP from IETF, many extensions have been made to the core SIP protocol (for example new headers, see 3GPP TS 24.229 [6]) for management, security and billing reasons, for instance. Therefore, SIP servers and proxies are more complex in the 3GPP system (that is, in IMS) than they normally are in the Internet. However, all 3GPP extensions were specified by the IETF, as a result of collaboration between the IETF and 3GPP. Therefore, 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 specifications.

1.2 Scope

The goal of this document is to ensure that crucial issues for operators such as interconnection, interworking and roaming are handled correctly following the introduction of IMS (IP Multimedia Subsystem).

This document introduces guidelines for the usage of inter-Service Provider connections in the IMS environment, and requirements that IMS has for the Inter-Service Provider IP Backbone network. Other issues discussed here include the addressing and routing implications of IMS.

In order to introduce successfully IMS services, roaming, interconnection and interworking are seen as major issues. This document aims to increase the IMS interconnection, interworking & roaming related knowledge level of operators, and to prevent non-interoperable and/or inefficient IMS services and networks. These aims concern especially roaming, interconnection and interworking cases, because these issues could potentially hinder the deployment of IMS if not handled properly.

This document describes a number of possible roaming architectures (namely for Local Breakout and Home Routing) for IMS roaming over different generations of 3GPP systems. However, based on past experience (in particular for IMS roaming over EPS), it is recommended that only the Home Routing architecture is deployed to support IMS services except for emergency service.

Please note that the document does not aim to give an introduction to IMS, even though Section 3 has a short introduction. Please see 3GPP TS 22.228 [5] document for this purpose.

This Permanent Reference Document (PRD) concentrates on network level roaming, interconnection and interworking, therefore, higher level issues like service interconnection are not discussed in detail. For protocol details of the interconnect see GSMA PRD IR.95 [50]. Furthermore, issues such as radio interface, Quality of Service (QoS) details, General Packet Radio Service (GPRS) backbone, interworking with Public Switched Telephone Network (PSTN) as well as layer 3 (IP) connections between IMS network elements and terminals/applications are not within the scope of this document. Connections to private networks, such as corporate networks, are also out of scope. Charging and billing related issues regarding IMS roaming, interconnection and interworking are out of scope; these are managed by the GSMA Wholesale Agreements & Solutions Group, WAS (see for example GSMA PRD BA.27 [17]).

Throughout this PRD, the term "GPRS" is used to denote both 2G/GERAN GPRS and 3G/UTRAN Packet Switched (PS) service.

1.3 Definitions

Term	Description
BG	Border Gateway, router with optional firewall functions (Network Address Translation (NAT), Topology Hiding) between intra-Service Provider and Inter-Service Provider IP Backbone networks. Note: BG terminology as defined here may cover following possible equipment depending on the technology and the operator policy: - IP firewall - I-SBC - IBCF - GMSC
Interconnection	The term Interconnection refers to the technical physical and logical connection between networks
Interworking	Is the functionality of two networks to talk to each other enabling services to be delivered across the two networks.

1.4 Abbreviations

Term	Description
5GC(N)	5G Core (Network)
5GS	5G System
APN	Access Point Name
AS	Application Server
BG	Border Gateway
BGCF	Breakout Gateway Control Function
CAPEX	Capital Expenses
CDR	Charging Data Record

Term	Description
CS	Circuit Switch
CSCF	Call / Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDGE	Enhanced Data rates for GSM Evolution
ENUM	E.164 Number Mapping
E-UTRAN	Evolved UTRAN (also known as "LTE")
GERAN	GSM / EDGE Radio Access Network
GRE	Generic Routing Encapsulation
GRX	GPRS Roaming eXchange.
GSM	Global System for Mobile telecommunications
HDVC	High Definition Video Conference
H-PCRF	Home Network- Policy and Charging Rules Function
HPMN	Home Public Mobile Network
HR	Home Routed
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
ICSI	IMS Communication Service Identifier
IBCF	Interconnection Border Control Function
II-NNI	Inter IMS NNI
IM-MGW	IP Multimedia – Media Gateway
IM-SSF	IP Multimedia – Service Switching Functionality
IMSI	International Mobile Subscriber Identity
IMS	IP Multimedia Subsystem
IMS-AGW	IMS Access Gateway
IPX	IP eXchange
ISIM	IMS SIM
LBO	Local BreakOut
LTE	Long Term Evolution (of RAN)
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
NG-RAN	Next Generation RAN
NR	New Radio
OAM	Operation, Administration and Maintenance

Term	Description
OMR	Optimal Media Routing
OPEX	Operational Expenses
OSA	Open Service Access
P-CSCF	Proxy CSCF
P-GW	Packet Gateway
PCF	Policy Control Function
PDN-GW	Packet Data Network Gateway
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
SIGCOMP	SIGnalling COMPression
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMF	Session Management Function
SMTP	Simple Mail Transfer Protocol
SP	Service Provider
SRVCC	Single Radio Voice Call Continuity
TAP3	Transferred Account Procedure version 3
TAS	Telephony Application Server
THIG	Topology Hiding Inter-network Gateway
TRF	Transit and Roaming Function
TrGW	Transition Gateway
T-SGW	Transport Signalling Gateway
UE	User Equipment
UPF	User Plane Function
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UTRAN	UMTS Terrestrial Radio Access Network
VoIMS	Voice & video over IMS (includes IR.92, IR.94 and IR.51 as well as NG.114 and NG.115)
V-PCRF	Visited Network- Policy and Charging Rules Function

Term	Description
VPMN	Visited Public Mobile Network

1.5 References

Ref	Doc Number	Title
[1]	GSMA PRD IR.34	Inter-Service Provider IP Backbone Guidelines
[2]	IETF RFC 3261	Session Initiation Protocol (SIP)
[3]	3GPP TS 22.228	IP Multimedia Subsystem, Stage 1
[4]	3GPP TS 23.002	Network Architecture
[5]	3GPP TS 23.228	IP Multimedia Subsystem, Stage 2
[6]	3GPP TS 24.229	IP Multimedia Call Control Protocol based on SIP and SDP
[7]	3GPP TS 29.163	Interworking between the IMS and CS networks
[8]	3GPP TS 29.162	Interworking between the IMS and IP networks
[9]	3GPP TS 33.210	IP network level security
[10]	3GPP TS 23.003	Numbering, addressing and identification
[11]	GSMA PRD IR.61	WLAN Roaming Guidelines
[12]	3GPP TS 33.107	3G security; Lawful interception architecture and functionsVoid
[13]	GSMA PRD NG.119	Emergency Communication
[14]	OMA	Push to talk over Cellular (PoC) - Architecture
[15]	3GPP TR 23.979	3GPP enablers for OMA PoC Services
[16]	3GPP TS 23.141	Presence Service, Architecture and functional description
[17]	GSMA PRD BA.27	Charging and Accounting Principles
[18]	3GPP TR 23.981	Interworking aspects and migration scenarios for IPv4 based IMS Implementations
[19]	3GPP TS 29.165	Inter-IMS Network to Network Interface (NNI)
[20]	3GPP TS 23.221	Architectural requirements
[21]	3GPP TS 23.003	Numbering, addressing and identification
[22]	GSMA PRD AA.80	Agreement for IP Packet eXchange (IPX) Services
[23]	GSMA PRD IR.40	Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminals
[24]	GSMA PRD IR.67	DNS Guidelines for Service Providers & GRX/IPX Providers
[25]	GSMA PRD IR.77	Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers
[26]	GSMA PRD IR.88	LTE Roaming Guidelines

Ref	Doc Number	Title
[27]	GSMA PRD IR.90	RCS Interworking Guidelines
[28]	GSMA PRD IR.92	IMS Profile for Voice and SMS
[29]	3GPP TS 32.260	Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging
[30]	3GPP TS 32.275	Telecommunication management; Charging management; Multimedia Telephony (MMTel) charging
[31]	3GPP TS 29.214	Policy and charging control over Rx reference point
[32]	3GPP TS 29.212	Policy and charging control over Gx reference point
[33]	GSMA PRD IR.83	SIP-I Interworking Description
[34]	GSMA PRD IR.33	GPRS Roaming Guidelines
[35]	Void	Void
[36]	GSMA PRD IR.94	IMS Profile for Conversational Video Service
[37]	IETF RFC 3455	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
[38]	IETF RFC 1035	Domain names - implementation and specification
[39]	3GPP TS 29.079	Optimal Media routeing within the IP Multimedia Subsystem (IMS); Stage 3
[40]	IETF RFC 6223	Indication of Support for Keep-Alive
[41]	GSMA PRD IR.39	IMS Profile for High Definition Video Conference Service
[42]	3GPP TS 23.167	IP Multimedia Subsystem (IMS) emergency sessions
[43]	3GPP TR 23.749	Study on S8 Home Routing Architecture for VoLTE
[44]	3GPP TS 24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
[45]	3GPP TS 32.251	Telecommunication management; Charging management; Packet Switched (PS) domain charging
[46]	3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[47]	3GPP TS 23.203	Policy and charging control architecture
[48]	IETF RFC 3312	Integration of Resource Management and Session Initiation Protocol
[49]	IETF RFC 4032	Update to the Session Initiation Protocol (SIP) Preconditions Framework
[50]	GSMA PRD IR.95	SIP-SDP Inter-IMS NNI Profile
[51]	GSMA RCC.07	Rich Communication Suite 6.0 Advanced Communications Services and Client Specification

Ref	Doc Number	Title
[52]	3GPP TS 23.204	Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access
[53]	GSMA PRD IR.51	IMS Profile for Voice, Video and SMS over unstrusted Wi-Fi access
[54]	GSMA PRD NG.105	ENUM Guidelines for Service Providers and IPX Providers
[55]	3GPP TS 26.114	IMS Multimedia Telephony - Media handling and interaction
[56]	3GPP TS 23.237	IP Multimedia Subsystem (IMS) Service Continuity
[57]	GSMA PRD NG.114	IMS Profile for Voice, Video & Messaging over 5GS
[58]	GSMA PRD NG.113	5GS Roaming Guidelines
[59]	GSMA PRD NG.115	IMS Profile for Voice, Video & Messaging over Untrusted WLAN connected to 5GC
[60]	3GPP TS 23.501	System architecture for the 5G System (5GS); Stage 2
[61]	3GPP TS 23.503	Procedures for the 5G System (5GS); Stage 2
[62]	3GPP TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3
[63]	GSMA PRD NG.106	IMS Profile for Voice, Video and SMS over trusted Wi-Fi access

2 Roaming Guidelines for EPS

2.1 Introduction

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

2.2 3GPP Background

The roaming capability makes it possible to use IMS services even though the user is not geographically located in the service area of the Home Public Mobile Network (HPMN).. 3GPP architecture specifications define three different deployment configurations. These configurations are shown in Figures 2-1, 2-2 and 2-3 which are extracted from Section 5.4 of 3GPP TS 23.221 [20]. A short introduction is given here. For a more detailed explanation please see 3GPP TS 23.221 [20].

Figure 2-1 depicts a model where the User Equipment (UE) has obtained IP connectivity from the Visited Public Mobile Network (VPMN) and the Proxy-Call Session Control Function (P-CSCF) in the VPMN is used to connect the UE to the HPMN IMS.

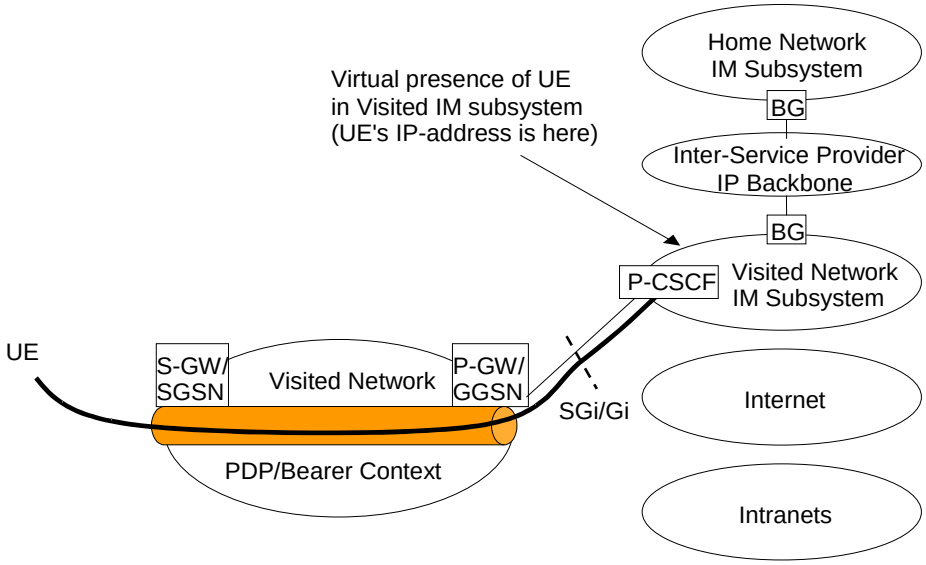


Figure 2-1: UE Accessing IMS Services with P-GW/GGSN in the VPMN via VPMN IMS

Figure 2-3 depicts a model where the UE has obtained IP connectivity from the HPMN and the HPMN provides the IMS functionality, e.g. for S8HR.

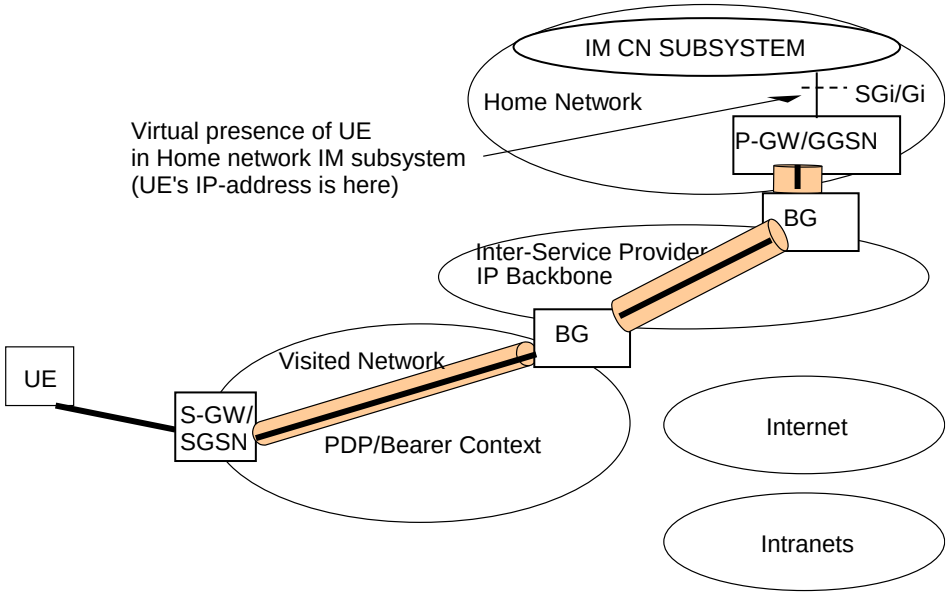


Figure 2-3: UE Accessing IMS Services with P-GW/GGSN in the Home network

Figure 2-3 shows configuration options that do not require IMS interconnection between the VPMN and HPMN IMS as the VPMN IMS is not used. When roaming is provided utilizing the architecture shown in the Figure 2-1 the service providers need to deploy IMS roaming interconnection between the VPMN and HPMN IMS as defined in Section 3.

2.3 Operational Requirements for IMS Voice and Video and other IMS Services based on Local Breakout and P-CSCF in VPMN

2.3.1 Operational Requirements for IMS Voice and Video

Three key operational requirements have been identified:

1. Routing of media for Voice & video over IMS (VoIMS; includes IR.92 [28] and IR.94 [36]) when call originator is Roaming should be at least as optimal as Circuit Switched (CS) domain.
2. The charging model for roaming used in CS domain shall be maintained in VoIMS.
3. Allow the HPMN to decide, based on service and commercial considerations & regulatory obligations, to enforce the routing of the originated traffic to itself (home routing).

A solution to the first requirement necessitates that the user plane is not routed towards the HPMN of the A party (unless so desired by HPMN A). When the GRX/IPX network is used as the interconnect network, the addressing requirements specified in IR.34 [1] and IR.40 [23] need to be followed. With this in mind, Local Breakout VPMN Routing (LBO-VR) architecture is illustrated in Figure 2-4.

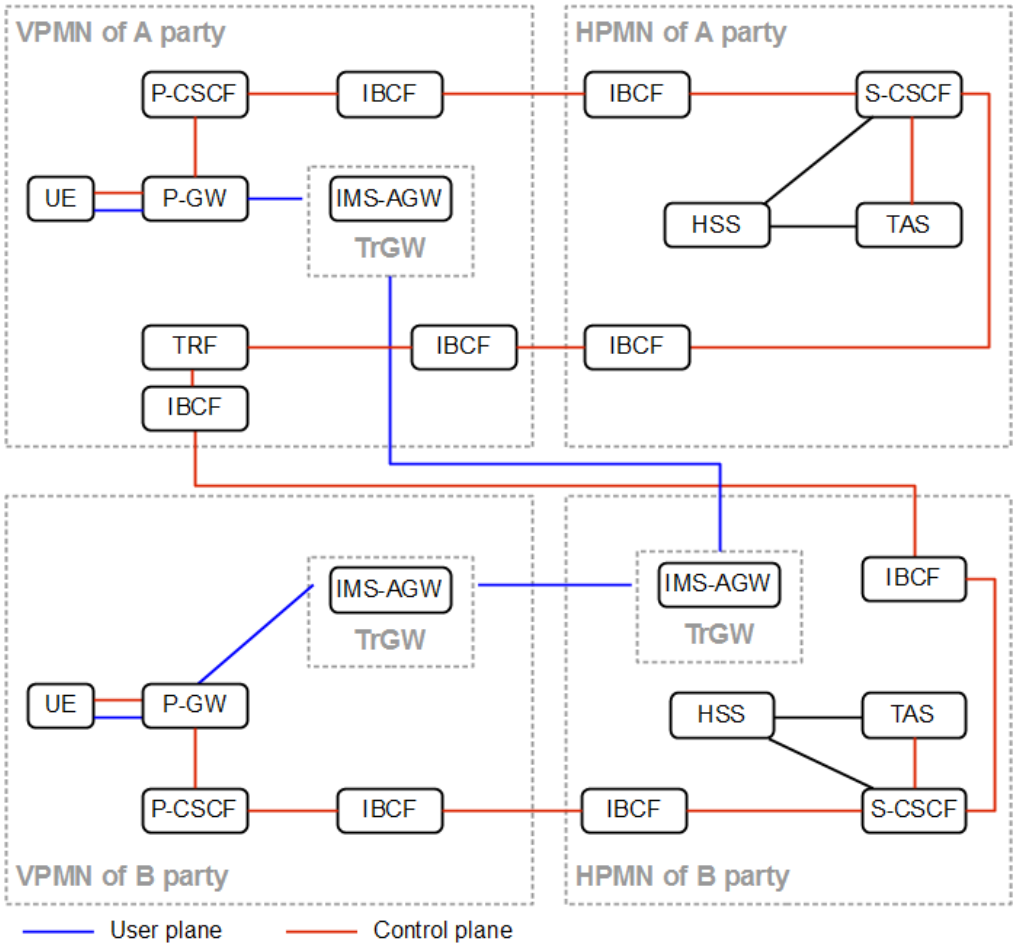


Figure 2-4: Control and User Plane Routing – LBO-VR

The figure does not depict the Ut interface (between UE and the network).

The second requirement is met by deploying P-CSCF (Proxy-Call Session Control Function) and Transit and Roaming Function (TRF) within the VPMN. The TRF receives the originated call related signaling after it has been processed by the A party HPMN allowing the A party VPMN to send both control and user plane towards the destination (VPMN routing) and therefore replicate the current CS voice roaming model. By applying Optimal Media Routing (OMR) along the signaling loop from A party VPMN to A party HPMN and back to A party VPMN the media path of originated calls is optimized and not routed to A party HPMN. The TRF, P-CSCF, together with Packet Data Network Gateway (P-GW) and Billing Mediation, deliver the charging information needed for the VPMN to generate TAP3 records. 3GPP TS 23.228 [5], TS 32.260 [29] and 3GPP TS 32.275 [30] provide further details.

The last requirement is met by supporting home routing according to the LBO Home Routing (LBO-HR) as depicted in Figure 2-5 where the media paths of originated calls are not optimized and are routed through A party HPMN (Home Routing).

The use of LBO-VR requires OMR to be supported along the signaling from A party VPMN to A party HPMN, and then the A party HPMN should decide (e.g. based on the destination):

- To send the signaling back to the A party VPMN – and then, as described above, OMR will be required along the signaling from A party HPMN to A party VPMN (Figure 2-4) or;
- To bring media to the A party HPMN and send both the control and user plane from the A party HPMN A towards the destination in this case OMR is terminated in A party HPMN.

The above decision is performed by SCSCF (or the BGCF) in A party HPMN.

If only supporting LBO-HR and not LBO-VR then the support of OMR is not needed along the signaling from A party VPMN to A party HPMN.

Routing from B party HPMN to B party VPMN is not affected by LBO-HR or LBO-VR.

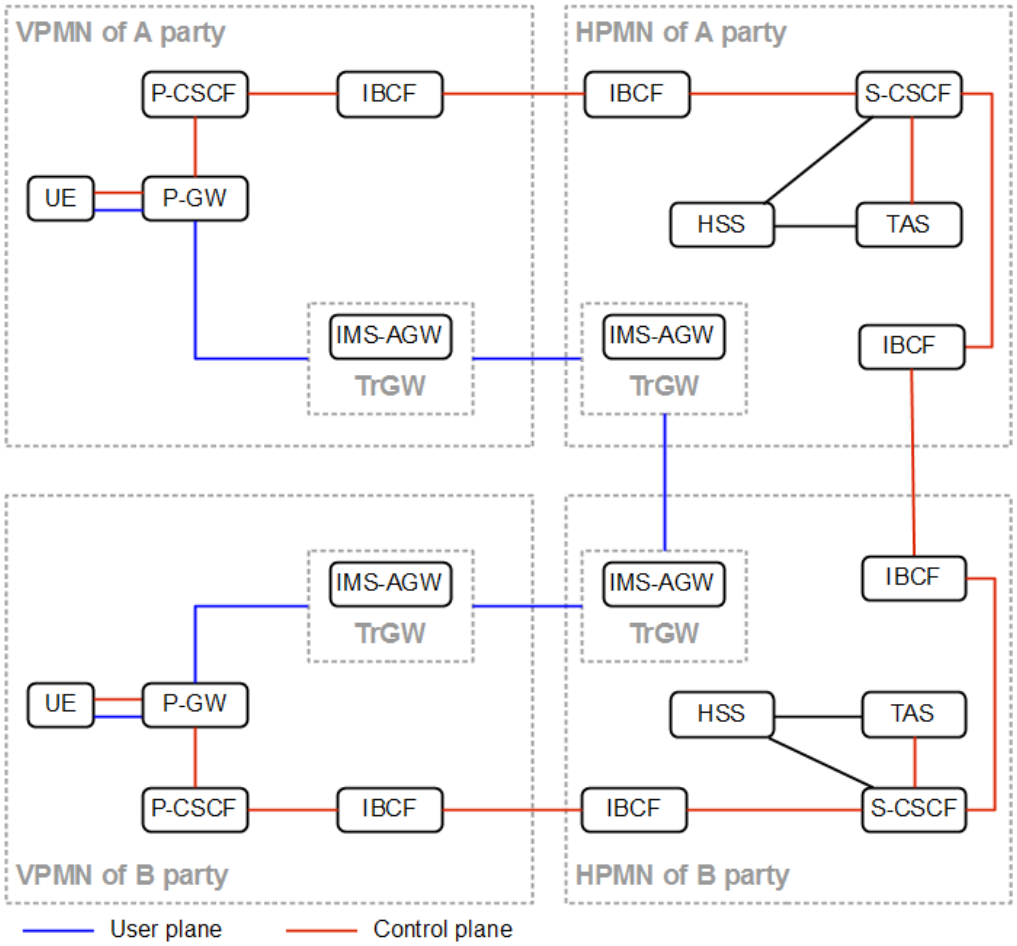


Figure 2-5: Control and User Plane Routing – LBO-HR

2.3.2 Operational Requirements for RCS Services

When using the same P-CSCF in the VPMN also for RCS services (see Section 5.5), then the user plane of voice and video calls based on the GSMA PRDs IR.92 [28], and IR.94 [36] can be routed as depicted in Figure 2-4. Even in this case, the user plane of RCS services other than IR.92 [28] and IR.94 [36] can be routed as depicted in Figure 2-5. An example of such home routed user plane in RCS is Message Session Relay Protocol (MSRP) traffic.

2.3.3 Operational Requirements for SMSoIP

If using SMSoIP, then the same P-CSCFs (in the VPMNs) and S-CSCFs (in the HPMNs) are used as for VoIMS as shown in Figure 2-5. For the originating case the needed stand-alone SIP signaling requests will be routed from P-CSCF to S-CSCF which invokes an IP-SM-GW to interwork the SIP signaling to legacy SMS system if needed; see 3GPP TS 23.204 [52] for further details. For the terminating case the legacy SMS signaling is interworked to SIP signaling, if needed, by an IP-SM-GW of the B party HPMN, and the needed stand-alone SIP signaling request is sent from the IP-SM-GW to the B-Party S-CSCF which routes the SIP signaling via the P-CSCF in the VPMN to the B-Party UE.

2.4 IMS Roaming Architecture

2.4.1 General

There are three IMS roaming architecture alternatives described in this document, namely:

- LBO-VR (Local Breakout VPLMN routing) and LBO-HR (Local Breakout HPLMN routing), as described in Section 2.3 and 2.4.2; and
- S8HR (S8 Home routed), as described in Section 2.4.3

Which of these alternatives is used is decided per roaming agreement. The following Sections describe the IMS roaming architecture alternatives in more detail.

2.4.2 VoIMS Roaming Architecture using LBO

The IMS Roaming Architecture using LBO is shown below in Figure 2-6 for EPC (see also GSMA PRD IR.88 [26]). For IMS Roaming the S9 interface between V-PCRF and H-PCRF is not needed (see also GSMA PRD IR.88 [26]). For routing of media when roaming, see Section 2.3.

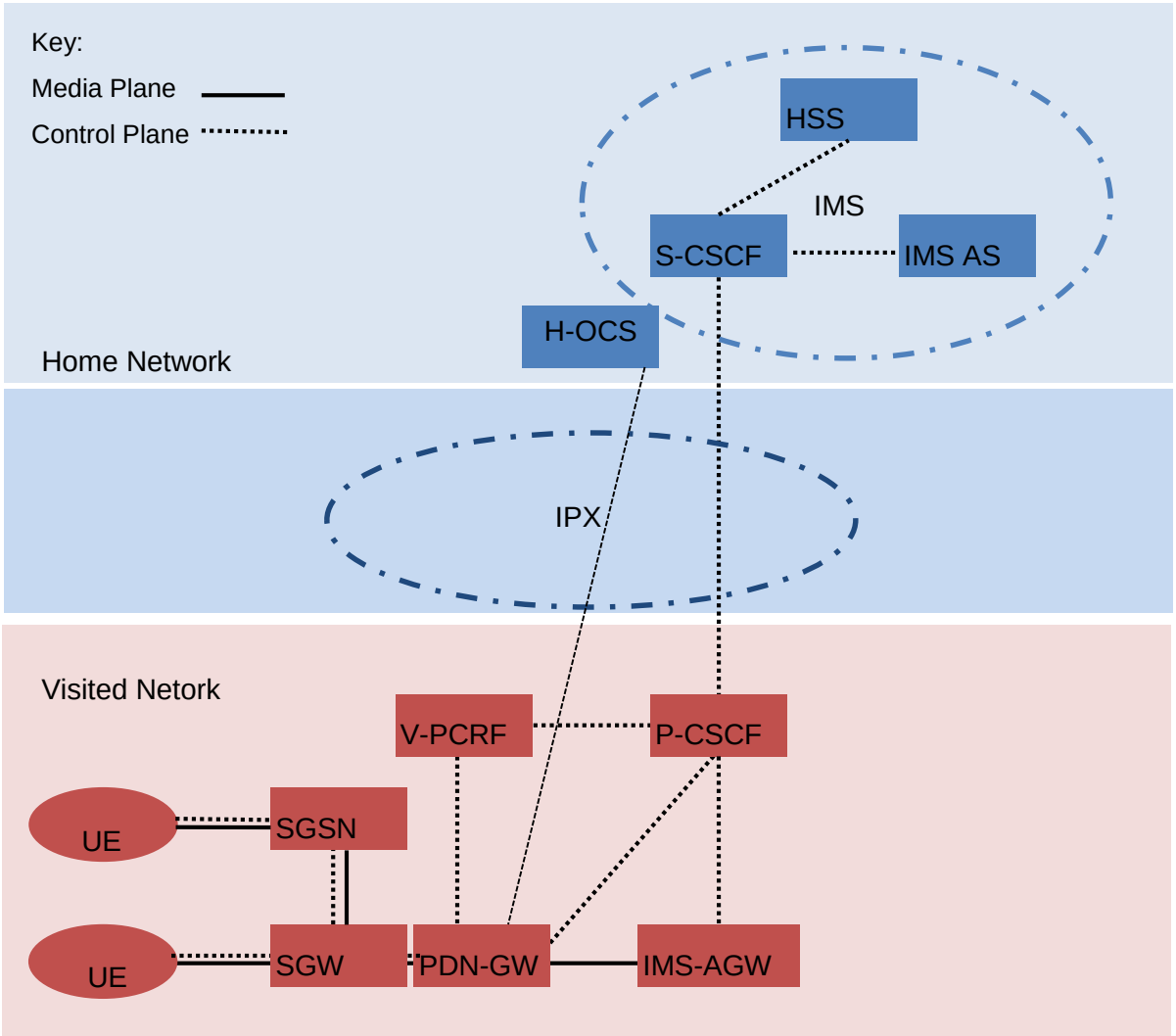


Figure 2-6: Voice Roaming Architecture using LBO – EPC

For IMS roaming to work, the P-CSCF and S-CSCF exchange and record each other's Uniform Resource Identifiers (URIs) during IMS registration as specified in 3GPP TS 24.229 [6]. The recorded S-CSCF URI is added as SIP route header during the session setup by P-CSCF to route the originated sessions to the S-CSCF and similarly the S-CSCF adds the recorded P-CSCF URI as a SIP route header to route terminated sessions to the P-CSCF as specified in 3GPP TS 24.229 [6].

If using SMSoIP, then the recorded S-CSCF URI is added by P-CSCF as a SIP route header to route originating stand-alone SIP signaling requests to the S-CSCF and similarily the S-CSCF adds the recorded P-CSCF URI as a SIP route header to route the terminating stand-alone SIP signaling requests to the P-CSCF.

The IPX network performs routing based exclusively upon the topmost SIP Route header that must contain the address of the destination network e.g. the A party HPMN address roaming or the B party VPMN address when roaming for the SIP invite.

The LTE and EPC roaming guidelines are specified in GSMA PRD IR.88 [26] and the GPRS roaming guidelines are specified in GSMA PRD IR.33 [34]. The transport aspects of the inter-PLMN interfaces are specified in GSMA PRD IR.34 [1]. The V-PCRF to P-CSCF (Rx) and the V-PCRF to PGW (Gx) interfaces are specified in 3GPP TS 29.214 [31] and 3GPP TS 29.212 [32] respectively.

2.4.3 IMS Roaming Architecture using S8HR

With S8HR IMS Roaming, the IMS well-known APN is resolved to the PGW in the HPLMN as shown in Section 2.2 (Figure 2-3) and in addition QoS level roaming support is required to support IMS Voice and Video telephony (VoIMS), i.e. service specific QoS other than the default QoS are supported on the home-routed PDN connection for the IMS well-known APN when roaming. IMS is supported by both the VPMN and the HPMN.

HPMN and VPMN must exchange information and agree, per roaming agreement, to the use of IMS roaming using S8HR taking into account local regulatory requirements in the VPMN.

The HPMN must ensure, based on the roaming agreement, that IMS layer signaling and media confidentiality protection is not activated in order to enable the VPMN to meet the local regulatory requirements.

If the HPMN uses IMS layer signalling and media confidentiality protection on its network (e.g. for the HPMN's own subscribers, for inbound roaming LBO IMS subscribers), then, based on the customer location retrieved through subscription to the PCRF, this protection must be deactivated in the HPMN for its S8HR outbound roamers if required by the VPMN to meet its regulatory requirements. It is a requirement for the operation of S8HR LI that IMS signaling messages and media packets are not encrypted at the S-GW (see 3GPP TS 33.107 [12] section 20.1.1).

A high level architecture diagram is represented in Figure 2-8 below.

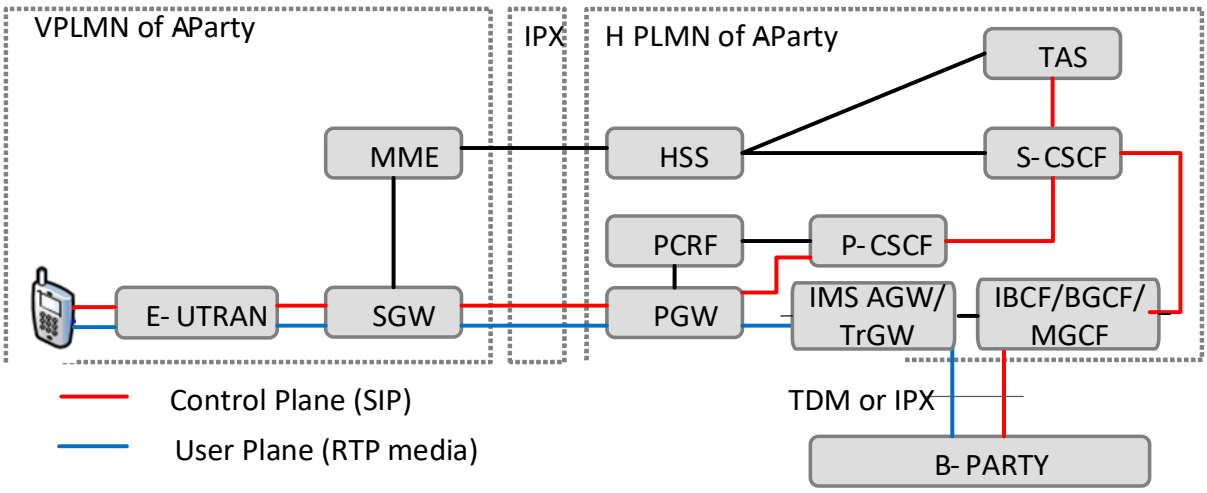


Figure 2-8: S8HR IMS Roaming Architecture (VoIMS service shown)

The salient characteristics of the S8HR architecture for voice roaming (non-emergency services) are:

- VoIMS calls are home routed using IMS well-known APN via S8 interface; i.e. the IMS UNI is provided directly between UE and the HPMN for non-emergency calls.
- The IPX only differentiates the signalling and media traffic based on the requested QoS levels.
- The HPMN has full control over the VoIMS (non-emergency) call routing.
- The VPMN is not service aware, but it is QoS and APN aware.
- The VPMN supports all E-UTRAN and EPC capabilities to serve IMS inbound subscribers, e.g., IMS voice over PS support indication to the UE, QCI=1 bearer for conversational voice; QCI=2 bearer for conversational video, and QCI=5 bearer for IMS signalling in EPC and E-UTRAN.
- The PCC framework of the HPMN is used. QoS rules are generated in the HPMN and enforced by the VPMN as per roaming agreement.
- VPMN has the ability to downgrade requested QoS, or reject the requested bearer, in case QoS values are outside the ranges configured in the MME per roaming agreement. Please refer to GSMA PRD IR.88 [26], Section 7, for more details

Note: S8HR requires support for anonymous emergency calls over IMS.

2.5 Support for Non-Voice IMS Services

It is possible to provide non-voice IMS services (e.g. RCS) using the 3GPP architecture with P-GW / GGSN in the home network (as shown in Figures 2-3) before supporting any of the IMS roaming architectures for VoIMS. Once the selected IMS roaming architecture is in place it can also be used for non–voice IMS services.

2.6 IMS Roaming Guidelines

LBO-VR (Figure 2-4), LBO-HR (Figure 2-5) and S8HR (Figure 2-8) show for IMS roaming support different functionality, regulatory requirements and needs as follows:

- S8HR for IMS roaming used for VoIMS can be seen as an VoIMS and QoS extension of (existing) EPC data roaming. As depicted in Figure 2-8, it does not require the use of IMS interconnect for roaming flows (IMS interconnect may still be required for terminating calls between HPMNs) and it does not require inter-operator testing (P-CSCF with I/S-CSCF or home operator terminals with P-CSCF). It is suitable for operators that wish to have IMS roaming services without, or before, deploying IMS interconnect services. However, operators also must accept the limitations (no service aware in VPMN, no geo-local services in VPMN, no media path optimization possible for originated calls, and new functionalities (e.g. QoS bearer charging, see GSMA PRD BA.27 [17], and network protection mechanisms) based on their local regulatory requirements). SRVCC is supported as described in Section 2.11. In addition, it may require the IPX providers that are connecting to those operators to support QoS bearer charging. Anonymous emergency calls over IMS, as specified in GSMA PRD IR.92 [28] are authenticated using EPC access credentials.
- LBO-HR for IMS roaming requires an IMS interconnect for roaming and inter-operator testing (P-CSCF with I/S-CSCF and home operator terminals with P-CSCF in VPMN). It fully supports voice charging for mobile originated and terminated calls (see GSMA PRD BA.27 [17]), IMS emergency calls, SR-VCC, operational requirements and QoS over the GRX/IPX. It is suitable for operators that need LBO capabilities to meet their local regulatory requirements but can accept limitations such as lack of geo-local service support in VPMN and no media path optimization for originated calls.
- LBO-VR for IMS roaming extends LBO-HR by adding support for geo-local services in the VPMN and media path optimization for originated calls. Media path optimization relies on OMR support by HPMN, VPMN and interconnected IPX providers. LBO-VR is suitable for operators that need all the support provided by LBO-HR for IMS roaming but also require support for geo-local services in VPMN and media optimization for originated calls.

Operators that have to support more than one IMS roaming architecture, i.e., support S8HR in combination with LBO-HR, LBO-VR or both, also have to support the functionality for more than one IMS roaming architecture.

The IMS roaming architecture in use for a specific terminal can be used for all IMS services on the IMS well-known APN.

2.7 SIGCOMP

The use of higher-bandwidth networks, such as E-UTRAN, rejects the need for SIGCOMP.

Note**:** See Section 2.2.7 of IR.92 [28] for more information specific to E-UTRAN access to IMS based services.

2.8 Support of Home-Local and Geo-Local Numbers

2.8.1 Home-Local and Geo-Local Numbers Overview

For VoIMS calls with telephone numbers given in local format, a TAS in HPMN serving the A Party must determine whether

- The number pertains to the HPMN dialling plan when roaming, that is it is a home-local number, or
- The number pertains to the VPMN dialling plan, that is, it is a geo-local number of the VPMN.

2.8.2 Home-Local and Geo-Local Numbers when visited network routing is applied (LBO-VR)

If a TAS determines a number to be a home-local number, the TAS must then translate the number to international format to route the call (see Section 2.3).

If a TAS determines the number to be a geo-local number, it must either translate the number to international format to route the call directly or via VPMN, or the number must be sent back to the VPMN unchanged with phone context set to “geo-local”. For geo-local numbers that correspond to home-local service numbers, see Section 2.8.3.

When a call with a geo-local number is received at the TRF in the VPMN, the number must be treated as if the phone-context was set to the home domain name of the VPMN.

Note: See Section 2.2.3 of GSMA PRD IR.92 [28] for more information on “phone-context” parameter.

2.8.3 Home-Local and Geo-Local Numbers when home-routing is applied (S8HR or LBO-HR)

If a TAS determines the number as home-local number, the TAS must translate the local number to international format (as specified in 3GPP TS 23.228 [5]).

If a TAS determines the number as geo-local number, the TAS must translate the numbers to international format to route the call, as specified in 3GPP TS 23.228 [5]. When the HPMN IMS translates the geo-local numbers to international format, the HPMN can also consider home-local service numbers that correspond to geo-local numbers (as specified in 3GPP TS 24.229 [6]).

For scenarios where the VPMN is using a special numbering plan, the HPMN can be provisioned according to the roaming agreement between the HPMN and the VPMN (and updated if needed) with all local numbers or regional code mappings from the VPMN(s),which may depend on the UE location. If the HPMN is not provisioned accordingly, then the HPMN may not be able to route calls to geo-local numbers.

2.9 Support of Emergency Calls with S8HR architecture

When applying the S8HR IMS Roaming architecture option, the following Emergency Call options are available (as specified in 3GPP TS 23.167 [42]):

- Emergency Call using Circuit-Switched Fallback
- IMS Emergency Call without IMS emergency Registration

  Note**:** Operators should be aware of local regulations for emergency calls. If IMS emergency calling is not required, the VPMN may force the UE to perform a CS Fallback for emergency calls.

A non UE detectable emergency call will be carried via EPC to IMS in the HPMN, see Section 2.9.2 below.

2.9.1 Impact on the VPMN using IMS Emergency Call (void)

For a description of the procedures of the VPMN to control the access to IMS emergency services for inbound roamers refer to section 6.4 of [26].

If local emergency numbers must be supported for roamers in the VPMN, then the VPMN shall send these numbers to the Emergency Number List and/or the Extended Emergency Number List to the UE during the Attach and Tracking Area Updating procedures, as specified in 3GPP TS 24.301 [44]. The VPMN may send numbers to the Emergency Number List and/or to the Extended Emergency Number List depending on the HPMN, e.g. to manage overlaps of national emergency numbers with numbers in the numbering plan of the HPMN, as per roaming agreement. If a local emergency number of the VPMN is not sent to the UE, then calls of a HPMN subscriber to this number will be handled via regular normal session establishment via S8HR.

Note 1: 3GPP does not define rules and procedures for the network on how to provision the Emergency Number List or the Extended Emergency Number List in Attach and Tracking Area Update responses.

Note 2: It is assumed that legislation of local emergency numbers in the VPMN overrules the applicability of the HPMN numbering plan in most cases. However, the management of HPMN specific Emergency Number List is a sensible mechanism for VPMNs to manage overlaps in number plans, e.g. to save their PSAPs from overload due to false routings of calls from inbound roamers.

2.9.2 Impact on the HPMN for non UE detectable emergency calls

The HPMN must be informed by the VPMN about which numbers will be provided as emergency numbers in the VPMN, according to the roaming agreement. If the VPMN has an emergency number that could not be notified to the UE by the Emergency Number List (as specified in 3GPP TS 24.301 [44]), and must be treated as a non UE detectable emergency number in the HPMN, the HPMN must be able to distinguish non UE detectable emergency calls and treat those emergency calls as described in section 5.2.10 of 3GPP TS 24.229 [6] and resulting in the emergency call being completed in the VPMN.

Note 1: Collection of location information at P-CSCF during registration procedure and handling of non UE detectable emergency sessions at P-CSCF require additional network capabilities in order to retrieve customer location for all calls (domestic and roaming). It is addressed in 3GPP TS 24.229 [6] annex L.2.2.6.

Note 2: The HPMN (P-CSCF) is assumed to be provisioned with a list of roaming partners' emergency service identifiers as described in 3GPP TS 24.229 [6] section 5.2.10. A list of emergency service identifiers for all countries can be found in annex F of GSMA PRD NG.119 [13].

Note 3: If the VPMN does not notify the Emergency Number List to the UE, then local service numbers which clash with VPMN emergency codes would be handled as local service numbers at the HPMN. Else, such codes would be treated as UE-detected emergency numbers.

2.10 Gate Control and Traffic Policing

The IMS Application Level Gateway (IMS-ALG) and IMS Access Media Gateway (IMS-AGW) are described in Annex G of 3GPP TS 23.228 [5]. The IMS-ALG and IMS-AGW enable gate control and traffic policing between IP-CAN and IMS domain in all VoIMS roaming architectures (LBO-VR, LBO-HR and S8HR). The IMS-ALG is collocated with the P-CSCF in Figures 2-5, 2-6, 2-7 and 2-8. The IMS-ALG and IMS-AGW allow policing of SIP signaling bearer and of dedicated bearers, e.g. to avoid direct communication between UEs, and unauthorized usage.

Uplink and downlink service level gating control can be performed by the PDN GW as described in 3GPP TS 23.401 [46] and 3GPP TS 23.203 [47] e.g.

- to ensure that all traffic via the PDN connection to the IMS well-known APN is only between the PDN-GW and the P-CSCF / IMS-AGW; and
- to prevent downlink media via the signaling bearer on the PDN connection to the IMS APN.

2.11 Support of Originated User Identity in Terminating Requests

The HPMN of the terminating UE is in charge of ensuring that Originating User Identity trusting policy meets its commitment to its customers. In particular, the HPMN of the terminating UE is responsible for preventing spoofed originating user's identity to the terminating user.

In case of an incoming SIP request coming from a non-trusted domain (e.g. coming from an international IBCF or not coming from an MGCF), and if the HPMN of the terminating UE wants to prevent the presentation of the From header field URI by the terminating UE, the HPMN of the terminating UE must:

- if the P-Asserted-Identity header field is not included in the SIP request, set the From header field of the SIP request to the unavailable URI, i.e. sip: unavailable@unknown.invalid as specified in 3GPP TS 23.003; or

- if the From header field of the SIP request contains a URI that is not anonymous and if this URI is different from the URI(s) included in the P-Asserted-Identity header field(s) of this SIP request, set the From header field URI of the SIP request to the URI of the P-Asserted-Identity header field in the SIP request.

Note 1: By implementation, this control can be done by an ingress IBCF or by an application server.

Note 2: “Trusted domain” definition should be considered from an operator point of view.

2.12 Support of Basic SRVCC Procedures with S8HR Architecture

The basic SRVCC procedure with S8HR architecture can be performed without IMS interconnect between Roaming Partners. There are two potential options defined in this chapter:

- With SIP-I
- With CS NNI

2.12.1 General SRVCC requirements

All the following SRVCC requirements should be fulfilled to execute the procedures in Sections 2.12.2 and 2.12.3:

1. STN-SR range of the HPMN should be allowed on the International GW of the Home and Visited networks.
2. The SRVCC MSS builds ISUP IAM and sends it over the ISUP interconnect
3. The Home MGCF needs to be configured to discriminate between national and international SRVCC, and, in case of international SRVCC, should be able to offer a SIP Invite to the Home ATCF with SDP without mode-set for the offered codec as specified in Table 6.1 of 3GPP TS 26.114 [55].
4. Home ATCF will send the INVITE with the original codec (AMR-WB) to SCC-AS via S-CSCF.
5. An accurate CLI must be delivered over the international ISUP interconnect carriers.

It is recommended that SRVCC be permitted/blocked on the basis of the individual roaming agreements (e.g. due to excessive handover time leading to dropped calls – see section 2.12.4). SRVCC can be blocked in the roaming scenario by: -

- The VPMN via: -
  - Update Location Request (ULR) message from the MME to HSS.
    - If the MME does not send the UE-SRVCC-Capability AVP or sends the UE-SRVCC-Capability AVP with a value of zero, then the HSS is informed that SRVCC is not supported in the VPMN and the HSS will not send the STN-SR AVP in ULA (Update Location Answer) message.
- The HPMN via: _
  - the Update Location Answer (ULA) message from HSS to MME.
    - If SRVCC is supported in the VPMN, the HSS can still block SRVCC by not sending the STN-SR AVP in the ULA message. The absence of the STN-SR AVP informs the MME that SRVCC is not supported by the HPMN.
  - the Insert Subscriber Data Request (IDR) message from HSS to MME.
    - The absence of the STN-SR AVP within the Subscription-Data AVP informs the MME that SRVCC is not supported by the HPMN.

2.12.2 SIP-I between Roaming Partners

This solution for SRVCC implies an IP interconnect between VPLMN and HPLMN. However, services like SRVCC (a/b/midcall) are not supported as the SRVCC related SIP parameters are lost in this scenario.

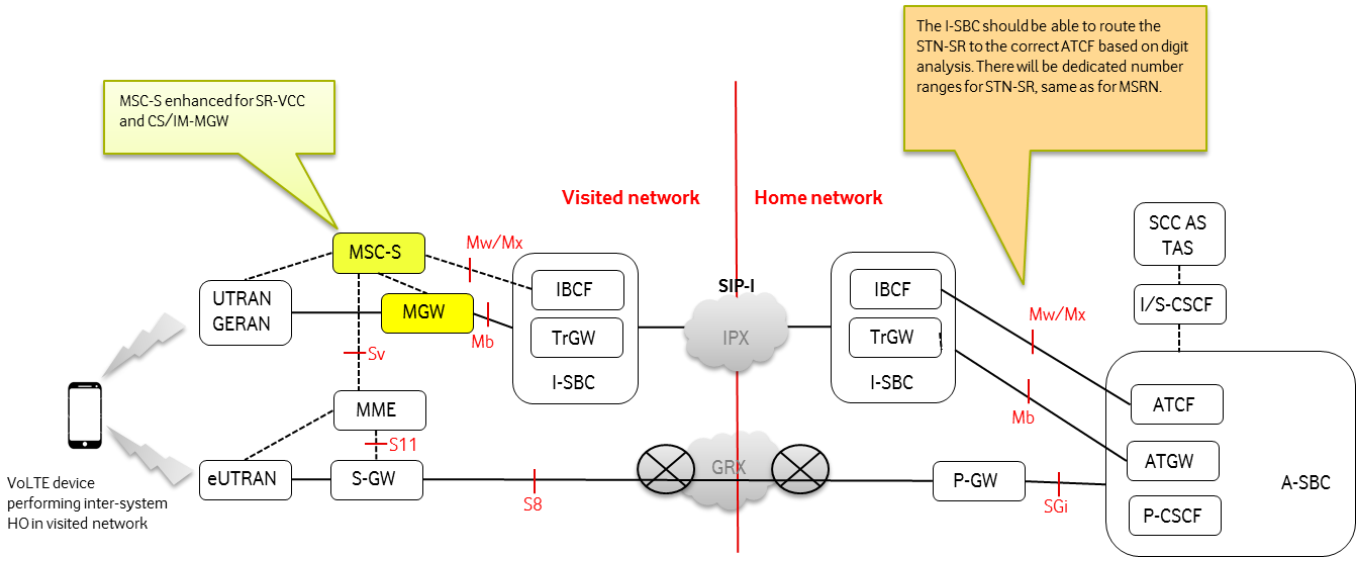


Figure 2-9 - SRVCC with SIP-I Architecture

The summary of the SRVCC procedure for a handover from E-UTRAN to UTRAN/GERAN, with optimized session/media anchoring in the ATCF/ATGW and SIP-I between the Home and Visited network is as follows:

- The SRVCC procedure is performed according to 3GPP TS 23.216 up to the Initiation of Session Transfer.
- Then the eMSC-S initiates the Session Transfer by generating a SIP Invite, carrying the STN-SR in the Request URI field of the SIP header, and the C-MSISDN in the P-Asserted-Identity field.
- According to 3GPP TS 23.003, STN-SR follows the E.164 telecommunications number format, so it includes a CC+NDC belonging to the operator who owns the ATCF that allocated the STN-SR. The eMSC-S will then determine the next hop for SIP signaling by number analysis.
- In case of SIP-I (i.e. realized via IPX with capability to route Tel URI based on number ranges) the I-SBC in the Visited network will be able to route the STN-SR by digit analysis to the I-SBC of the Home network, according to the interconnect agreements.
- The I-SBC in the Home network will forward the SIP Invite to the ATCF that originally allocated the STN-SR.
- Using the info included in the SIP Invite received from the eMSC-S through the SIP-I (STN-SR and C-MSISDN), the ATCF identifies the anchored session that is to be transferred and starts executing the access transfer. The media path is set up and the codec selected.
- Once the access transfer is successfully completed, the eMSC-S sends a SRVCC PS to CS Response message to the source MME that synchronizes the prepared relocations and sends a Handover Command message to the source E UTRAN. Consequently, the UE tunes to the target UTRAN cell. After that, the UE re-establishes the connection with the network and can send/receive voice data.

2.12.3 CS NNI between Roaming Partners

This solution for SRVCC implies MSS/MGCF configuration based on the STN-SR information coming on the international ISUP interconnect. Services like SRVCC (a/b/midcall) are not supported as the SRVCC related SIP parameters are lost in this scenario.

.

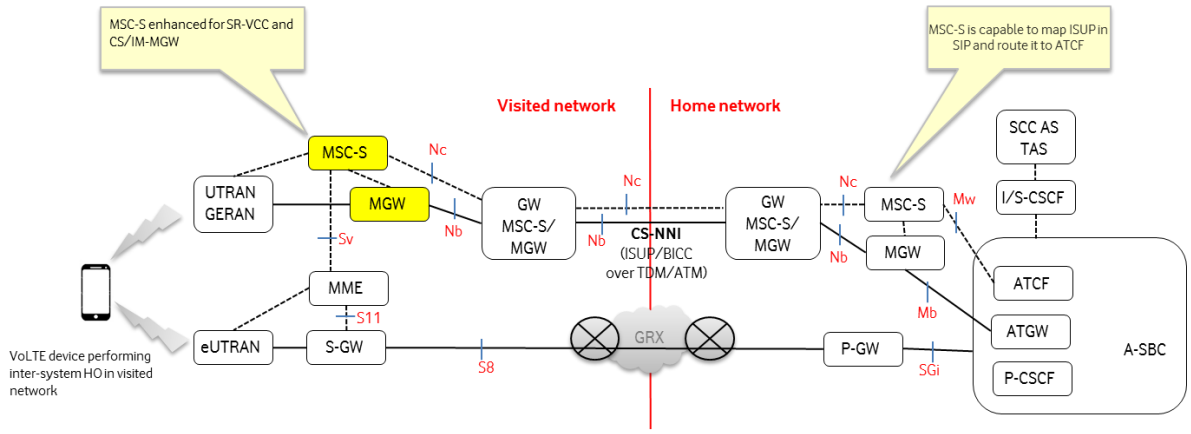


Figure 2-10 – SRVCC with CS-NNI Architecture

Figure 2-10 shows the SRVCC with CS-NNI architecture that allows for ISUP/BICC Signalling exchange between eMSC-S in VPLMN and eMSS (Gateway) in HPLMN for the SRVCC procedure.

Visited eMSS/MGCF creates and sends an IAM message in ISUP signalling through CS-NNI and Home MSS/MGCF converts ISUP in SIP signalling and forwards SIP Invite (with STN-SR and C-MSISDN) to ATCF. Note that C-MSISDN (as per 3GPP TS 24.237) shall reach the Home Network as caller in the IAM message and this shall not be dropped by any carrier.

The summary of the SRVCC procedure for a handover from E-UTRAN to UTRAN/GERAN, with optimized session/media anchoring in the ATCF/ATGW and CS NNI between the Home and Visited network is as follows:

- The SRVCC procedure is performed according to 3GPP TS 23.216 up to the Initiation of Session Transfer.
- Then the eMSC-S initiates the Session Transfer by generating a ISUP IAM, carrying the STN-SR in the Called Party field of the ISUP header, and the C-MSISDN in the Calling Party field. According to 3GPP TS 23.003, STN-SR follows the E.164 telecommunications number format, so it includes the CC+NDC that belongs to the operator who owns the ATCF that allocated the STN-SR. Based on the number analysis, the eMSC-S will then determine the next hop for ISUP signaling being the Gateway MSC-S (GW MSC-S).
- In case of CS-NNI, the GW MSC-S in the Visited network will be able to route the STN-SR by number analysis to the GW MSC-S of the Home network, according to the voice interconnect agreements.
- The GW MSC-S in the Home network will forward the IAM message to a MGCF that performs the ISUP (or BICC) to SIP interworking converting the IAM message into a SIP Invite sent to the ATCF that originally allocated the STN-SR.
- Using the information included in the SIP Invite received from the eMSC-S through the CS-NNI (STN-SR and C-MSISDN), the ATCF identifies the anchored session that is to be transferred and starts executing the access. The media path is set up and the codec selected.
- Once the access transfer is successfully completed, the eMSC-S sends a SRVCC PS to CS Response message to the source MME that synchronizes the prepared relocations and sends a Handover Command message to the source E UTRAN.
- The source E-UTRAN sends a Handover from E-UTRAN Command message to the UE. The UE tunes to the target UTRAN cell. After that, the UE re-establishes the connection with the network and can send/receive voice data.
- Potential codec mismatch issues have been identified in the trials which used the option with CS NNI. This can be overcome with a MSS/MGCF configuration based on the STN-SR information coming on the international ISUP interconnect.

2.12.4 Handover Time

In S8HR voice roaming, if a call is handed off to 3G, the voice call interruption time is depending on the geographic distance between VPLMN and HPMN because the session transfer request is sent from the VPLMN to the anchoring point of the call, in the HPMN.

The duration of the handover is mainly influenced by the geographical distance between Operators and the international voice carriers.. Therefore the distance and the voice carriers are more relevant in the case of SRVCC with CS-NNI between Roaming Partners.

Some of the values measured in the trials with CS-NNI are in Annex D.

2.13 Support of Enhanced SRVCC Procedures with S8HR Architecture

If the network supports enhanced SRVCC for S8HR in deployments without IMS-level roaming agreement, then both the VPMN and HPMN must support Annex C of 3GPP Release 16 TS 23.237 [56].

2A Roaming Guidelines for 5GS

2A.1 Introduction

The following sections provide a brief description of IMS Roaming architectures in the context of 5GS based on 3GPP Release 15 (except otherwise stated).

The description is based on section 2 (pre-5G) and only main differences, if any, are highlighted in the following sections.

The security related functionalities are not shown for simplicity in roaming architectures as the objective is only to describe the “IMS roaming principles”. They have obviously to be supported accordingly for 5GS roaming deployments.

2A.2 3GPP Background

The following architectures are defined by Release 15 of 3GPP TS 23.228 [5] for IMS Roaming over 5GS and are depicted in the following figures for LBO (Local BreakOut) and HR (Home Routed) solutions.

1. LBO Roaming with P-CSCF in VPMN using 5GS to support IMS Services (Figure 2A-1)
2. LBO Roaming with P-CSCF in HPMN using 5GS to support IMS Services (Figure 2A-2)
3. LBO with P-CSCF in VPMN with Loopback possibility using 5GS to support IMS Services (Figure 2A-3)
4. Home Routed Roaming using 5GS to support IMS Services (Figure 2A-4)

Solutions 1, 3 and 4 are elaborated later as potential IMS roaming solutions. Solution 2 is out of scope.

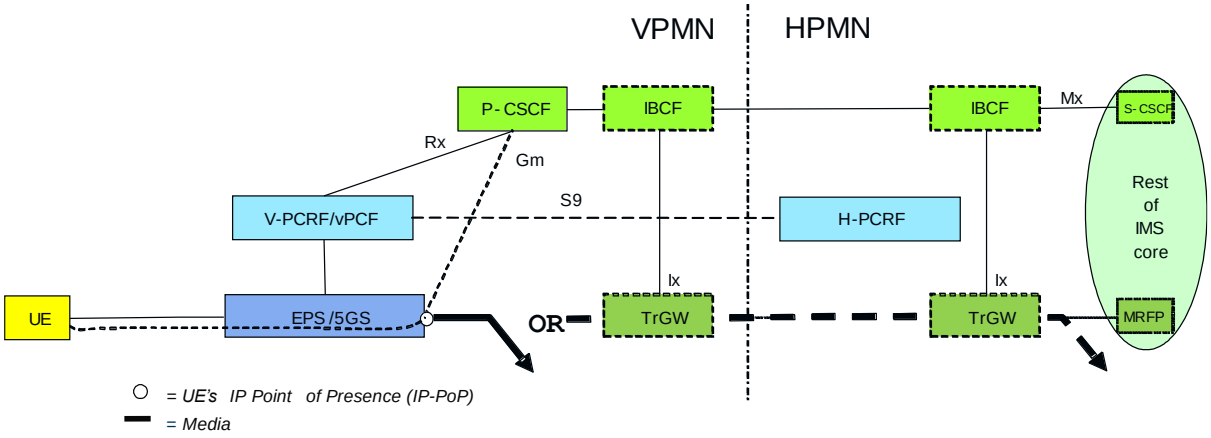


Figure 2A-1: LBO Roaming with P-CSCF in VPMN using 5GS to support IMS Services

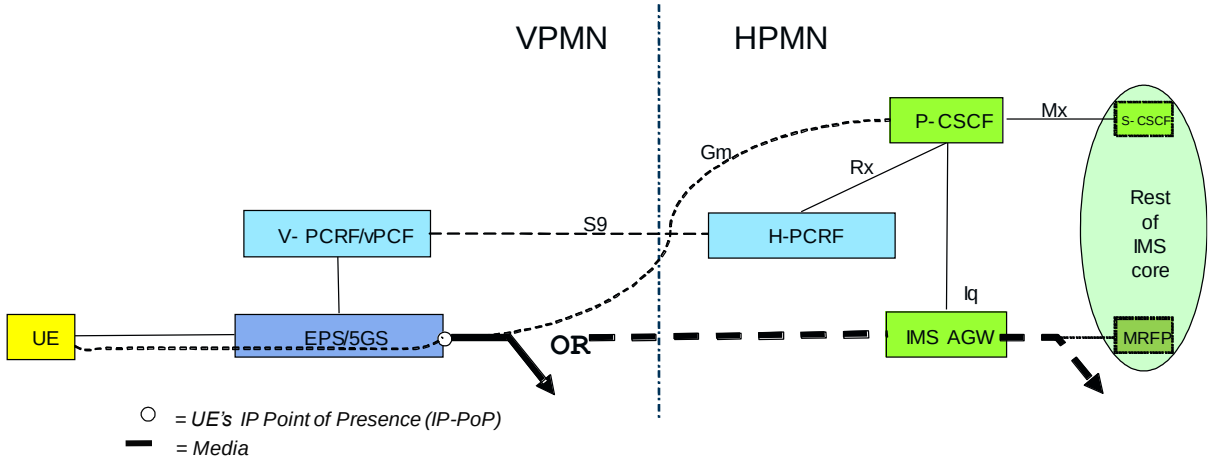
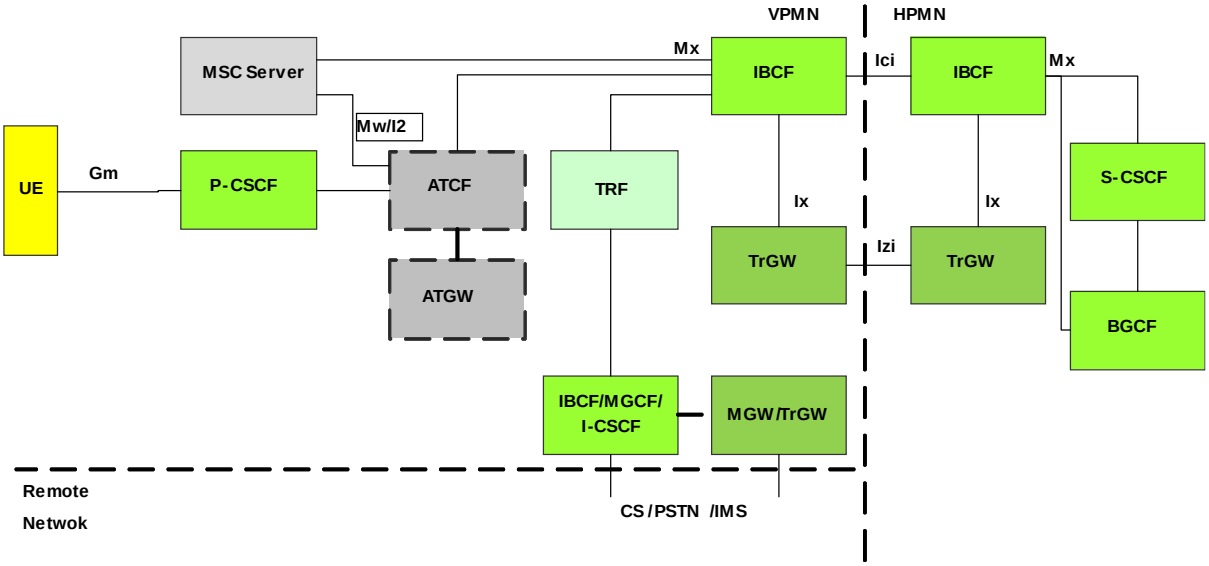


Figure 2A-2: LBO Roaming with P-CSCF in HPMN using 5GS to support IMS Services



Note: This is a generic roaming architecture from an IMS perspective. Some NFs are out of scope (e.g. those related to (e)SRVCC such as ATCG / ATGW).

Figure 2A-3: LBO with P-CSCF in VPMN with Loopback possibility using 5GS to support IMS Services

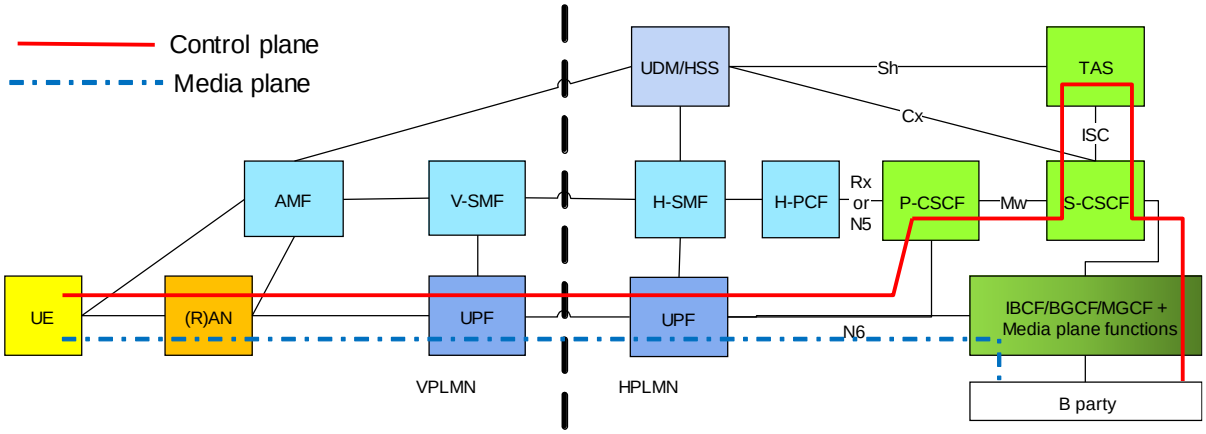


Figure 2A-4: Home Routed Roaming using 5GS to support IMS Services

2A.3 Operational Requirements

The operational requirements for LBO are as specified in section 2.3.1 and are illustrated in Figure 2A-5 (LBO-VR) and Figure 2A-6 (LBO-HR).

The operational required for RCS services are as specified in section 2.3.2 except that the reference IMS profile for voice and video calls is GSMA PRD NG.114 [56] and shown in Figure 2A-5. The operational required for SMSoIP are as specified in section 2.3.3 and shown in Figure 2A-6.

2A.4 IMS Roaming Architecture

2A.4.1 General

There are three IMS roaming architecture alternatives described for 5GS in this document, namely:

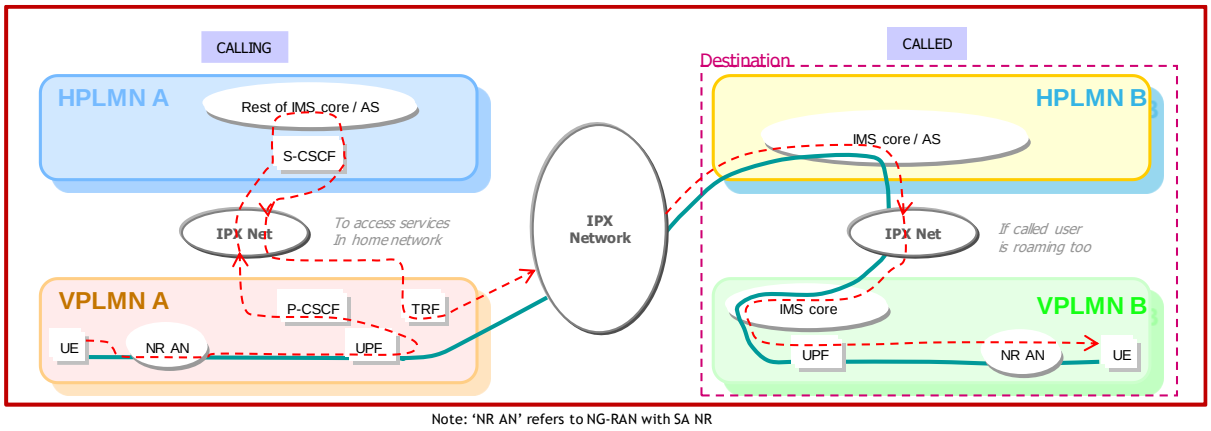
- LBO-VR (Local Breakout VPMN Routing) and LBO-HR (Local Breakout HPMN Routing) as described in sections 2A.3 and 2A.4.2; and
- S9HR (S9 Home routed) as described in section 2A.4.3

Which of these alternatives is used is decided per roaming agreement. The following sections describe the IMS roaming architecture alternatives in more detail.

2A.4.2 IMS Roaming Architecture using LBO

The IMS Roaming Architecture using LBO for 5GC is shown below in Figure 2A-5 (LBO-VR) and Figure 2A-6 (LBO-HR) (see also GSMA PRD NG.113 [57]).

The functionalities required are supported as described in section 2.4.2 but using the 5GC architecture (see 3GPP TS 23.501 [59] and GSMA PRD NG.113 [57]).



Note: 'NR AN' refers to NG-RAN with SA NR

Figure 2A-5: Control and User Plane Routing – LBO-VR

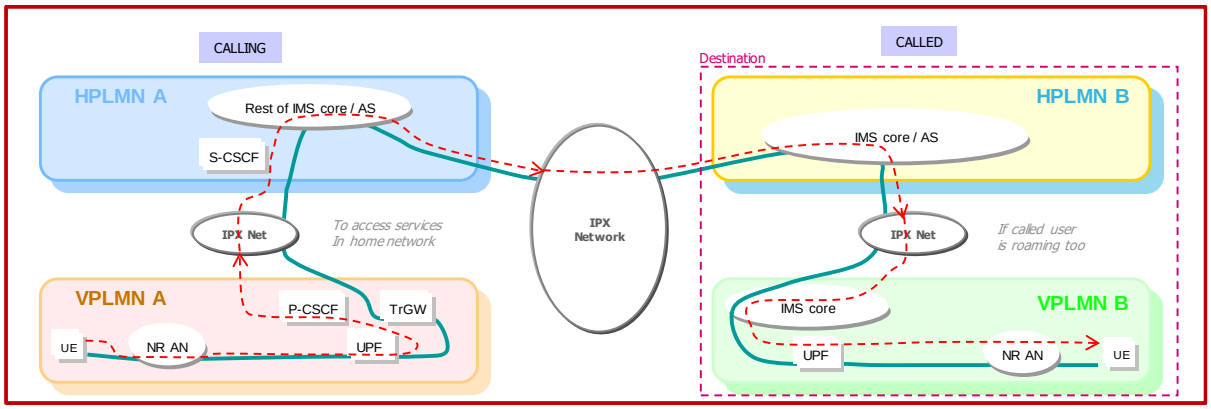


Figure 2A-6: Control and User Plane Routing

2A.4.3 IMS Roaming Architecture using N9HR

The IMS Roaming Architecture using N9HR for 5GC is shown below in Figure 2A-7 (see also GSMA PRD NG.113 [57]).

The functionalities required are supported as described in section 2.4.3 but using the 5GC architecture (see 3GPP TS 23.501 [59] and GSMA PRD NG.113 [57]), namely usage of UPF in the HPMN.

The salient characteristics of the N9HR architecture for VoIMS Roaming (non-emergency services) are like described in section 2.4.3 but with some terminology changes:

- VoIMS calls are home routed using IMS well-known DNN via N9 interface; i.e. the IMS UNI is provided directly between UE and the HPMN for non-emergency calls.
- The IPX only differentiates the signalling and media traffic based on the requested QoS levels.
- The HPMN has full control over the VoIMS (non-emergency) call routing.
- The VPMN is not service aware, but it is QoS and DNN aware.
- The VPMN supports all NG-RAN (with Stand-alone NR) and 5GC capabilities to serve IMS inbound subscribers, e.g., IMS voice over PS support indication to the UE, 5QI=1 bearer for conversational voice; 5QI=2 bearer for conversational video, and 5QI=5 bearer for IMS signalling in NG-RAN (with Stand-alone NR) and 5GC.
- The PCC framework of the HPMN is used. QoS rules are generated in the HPMN and enforced by the VPMN as per roaming agreement.
- VPMN has the ability to downgrade requested QoS, or reject the requested bearer, in case the QoS values are outside the ranges configured in the MME per roaming agreement. Please refer to GSMA PRD NG.113 [57] for more details
- N9HR requires support for anonymous emergency calls over IMS.

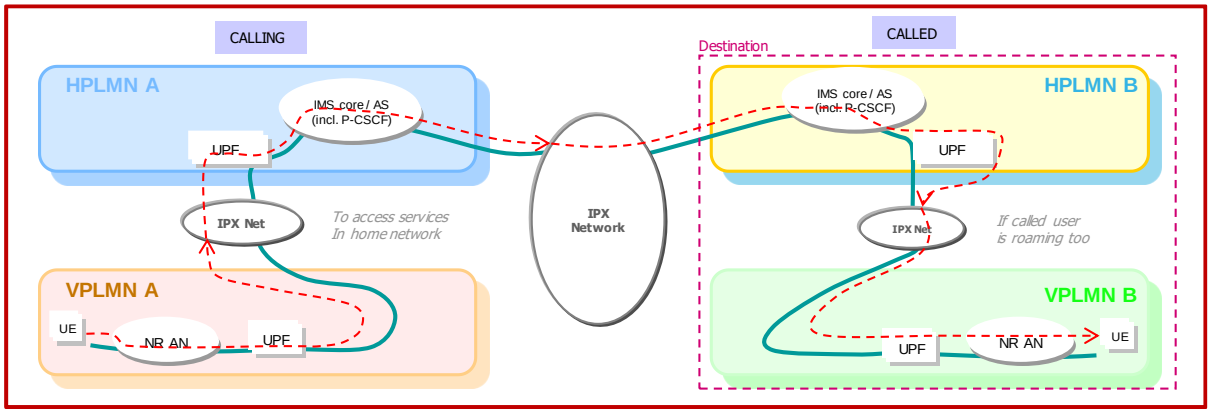


Figure 2A-7: Control and User Plane Routing – S9HR

2A.5 Support of Non-Voice IMS services

This functionality is supported as described in section 2.5 except that a UPF is used in the home network as shown in Figure 2A-4.

2A.6 IMS Roaming GuidelinesThe guidelines for IMS Roaming over 5GS are in line with the description provided in section 2.6 except that they are depicted in Figure 2A-5 (LBO-VR), Figure 2A-6 (LBO-HR) and Figure 2A-7 (N9HR).

The IMS roaming architecture for 5GS to support IMS services implies the use of the IMS well-known DNN.

2A.7 SIGCOMP

The use of higher-bandwidth access networks, such as NG-RAN with Stand-Alone NR, rejects the need for SIGCOMP.

> Note: See section 2.2.8 of GSMA PRD NG.114 [56] for more information specific to NG-RAN (Stand-Alone NR) access to IMS based services.

2A.8 Support of Home-Local and Geo-Local Numbers

This functionality is supported as described in section 2.8.

2A.9 Support of Emergency Calls with S9HR architecture

The support of Emergency Call with N9HR architecture option is supported as described in section 2.9 except that the reference should be made to 5GC and 3GPP TS 24.501 [61].

2A.10 Gate Control and Traffic Policing

This functionality is supported as described in section 2.10 except that the uplink and downlink service level gating control can be performed by the SMF / UPF as described in 3GPP TS 23.501 [59] and 3GPP TS 23.503 [60].

2A.11 Support of Originated User Identity in Terminating Requests

This functionality is supported as described in section 2.10.

2A.12 Support of Basic SRVCC Procedures with N9HR Architecture

This functionality is not applicable to IMS Roaming for 5GS for at least the present version.

3 Interconnection Guidelines

3.1 Introduction

interconnection of two different IMSs shall be guaranteed in order to support end-to-end service interoperability. For this purpose, Inter-IMS- Network to Network Interface (NNI) between two IMS networks is adopted. The general interconnection model is shown in Figure 3-1.

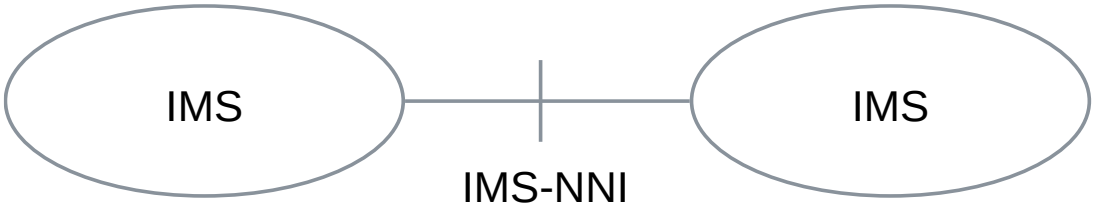


Figure 3-1: High-level view of the interconnection model for IMS

There are two architectural variants of how the Inter-IMS-NNI (II-NNI) can be deployed. These are depicted in Section 3.2, where an Interconnection Border Control Function (IBCF) is used at the border of each Service Provider, and Section 3.3, in where no IBCF is used at the border of each Service Provider. It is also possible that an IBCF is only used at the border of one Service Provider. However, the SIP profile applicable at the II-NNI is independent of these architectural variants. See PRD IR.95 [50] for the protocol details of the II-NNI.

3.2 Ici/Izi Interfaces

3GPP has defined border nodes and interfaces specifically for the purpose of IMS NNI in 3GPP TS 29.165 [19]. The Ici interface is used to transport SIP signaling, while the Izi interface handles media traffic.

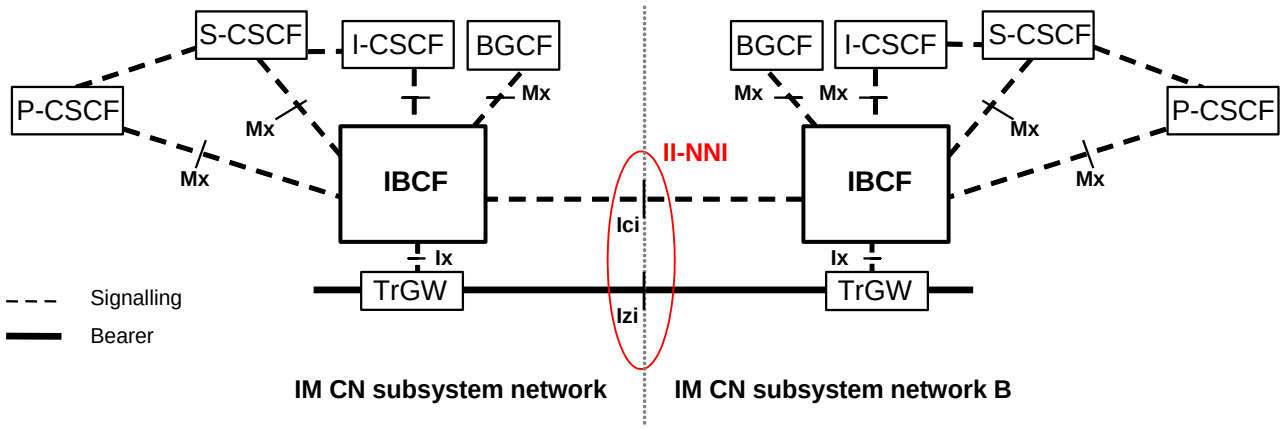


Figure 3-2: IMS interconnection using Ici & Izi Interfaces (from 3GPP TS 23.228)

Figure 3-2 shows this model where IBCF (Interconnection Border Control Function) is a functional entity that handles the control plane for the purpose of topology hiding, application layer gateway, screening of SIP signaling information and generation of Charging Data Records (CDRs) as an example. TrGW (Transition Gateway) is controlled by IBCF and can provide functions such as Network Address Translation – Protocol Translation (NAT-PT) and IPv4/6 conversion for the user plane. The TrGW is the preferred location for NAT/NAPT (Network Address Translation / Network Address and Port Translation) functionality in this deployment architecture.

3.3 Mw and Mb Interfaces

Figure 3-3 presents IMS interconnection between originated and terminated networks as specified in 3GPP's IMS NNI. SIP signaling is delivered via Mw interface and user plane is transported via Mb interface. The actual IMS user traffic (such as Video Share stream) is encapsulated using Generic Routing Encapsulation (GRE) tunnel within the Inter-Service Provider IP Backbone (as illustrated in GSMA PRD IR.34 [1]). SIP signaling always flows via IMS core networks.

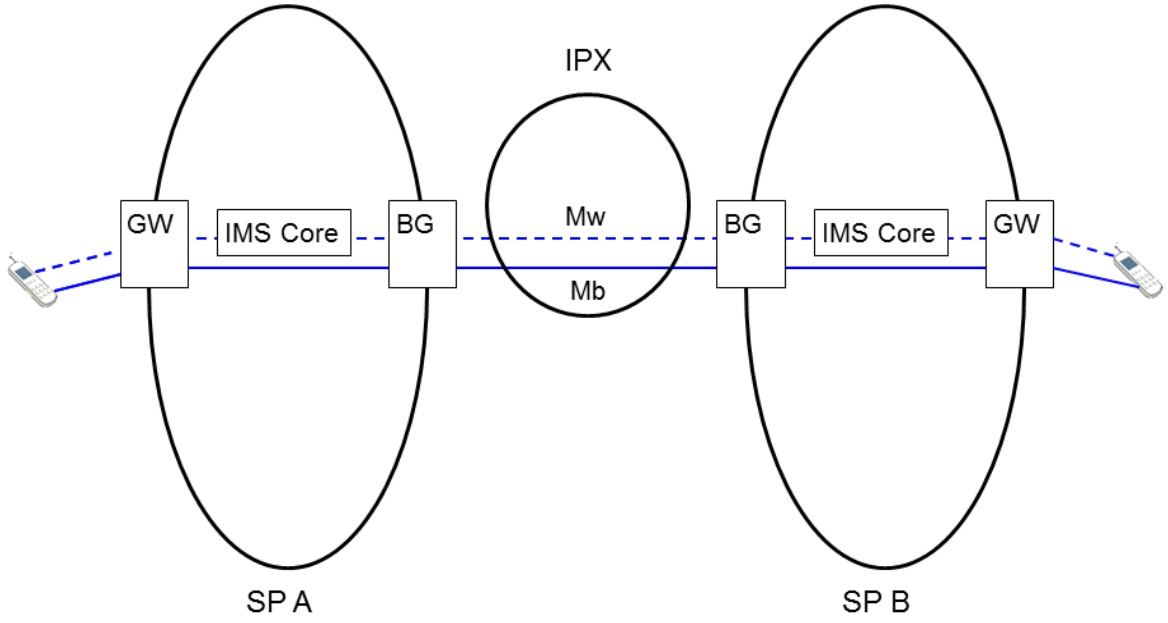


Figure 3-3: IMS interconnection using Mw & Mb Interfaces (simplified example not showing e.g. FW nodes)

Border Gateway (BG) shown in the figure above is a SIP unaware IP level element performing filtering on the IP layer. In addition to the BG there can be other nodes relevant for the II-NNI, such as a SIP aware Firewall (FW) located between BG and I/S-CSCF. I-CSCF is the point of contact to IMS.

3.4 Overview

Whilst 3GPP TS 29.165 [19] illustrates II-NNI using IBCF and Transition Gateway (TrGW) nodes, it actually only shows the interface profile between two operators. In other words, it does not specify any requirements on how the operator core network is implemented as long as the behaviors over Ici and Izi interfaces are as expected.

Note**:** One related issue is that IBCF and TrGW do not solve all the issues related to IP based inter-operator related cases in general since they handle only SIP based traffic and associated user plane traffic.

It should be noted that both the option of using Mw and Mb interfaces as well as the option of using Ici and Izi interfaces are feasible in IMS interconnection. In other words, individual operators can select the most optimal solution suitable.

The Inter-Service Provider IP Backbone must provide reliable transmission as in case of IMS roaming. Usage of Domain Name System (DNS) has special importance in interconnection scenarios, further details are described in Section 6.

Interworking or interconnection with Internet and corporate intranets is not described in detail, although Section 6 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 operators and non-IMS operators. 3GPP specification TS 29.163 [7] covers interfaces and signalling for the case that the interworking is between the 3GPP IM CN subsystem and BICC/ISUP based legacy CS networks. It is also possible that the SIP-I based interworking as specified in GSMA PRD IR.83 [33] is used.

4 Inter-Service Provider IP Backbone Guidelines

4.1 General

General requirements for the Inter-Service Provider IP Backbone shall be applied from GSMA PRD IR.34 [1].

Using the IPX networks to carry IMS traffic is easier than building direct connections between every IMS network in the World. Operators should evaluate the physical connection for IMS roaming and interconnection and choose the most appropriate. One suggestion would be to use the IPX network as the default routing choice.

However where traffic is high (typically between national operators) 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 the national traffic, IP-VPN for the medium volume or non-Service Provider and IPX for all others. The DNS system will resolve the destination domain to an IP address that will be used for routing over the appropriate link.

It is not necessary to build any kind of separate “IMS Roaming & Interconnection Exchange network” only for IMS traffic. Issues such as QoS, security, control of interconnections , overall reliability and issuing of new network features such as support for E.164 number and DNS (ENUM) are easier handled inside the IPX networks than when using public Internet to exchange IMS traffic between operators. This is because IPX networks are considered closed operator controlled network unlike the public Internet, which is open for everyone.

The preferred Inter-Service Provider IP Backbone in the IMS case is IPX, as it is already the preferred network for packet data roaming, Multimedia Messaging Service (MMS) interworking and Wireless LAN (WLAN) Roaming for instance.

4.2 IP Addressing

As documented in 3GPP TS 29.165 [19], interconnection by means of the IMS NNI may support IPv4 only, IPv6 only or both. Support of the different IP versions on the Inter-Service Provider IP Backbone network is specified in GSMA PRD IR.34 [1] and GSMA PRD IR.40 [23].

4.3 Security

In order to maintain proper level of security within the Inter-Service Provider IP Backbone certain requirements for the Service Providers and Inter-Service Provider IP Backbone providers should be taken into account. The same security aspects shall be applied as described in GSMA PRD IR.34 [1] and GSM PRD IR.77 [25].

4.4 Proxy

The Inter-Service Provider IP Backbone may deploy an additional element for IMS routing. This separate intermediate Proxy functionality allows operators to make just a single connection from their own IMS core system to the Proxy in the Inter-Service Provider IP Backbone regardless of the number of IMS interconnection partners. The Proxy is responsible for routing traffic towards the correct recipient network. The proxy is also responsible for the cascading billing model and arbitration on IPX. The proxy is recommended for any multilateral implementation. The proxy shall support routing based on the request URI and SIP route header described in Section 6. More requirements and details on the IPX Proxy are listed in Annex C.

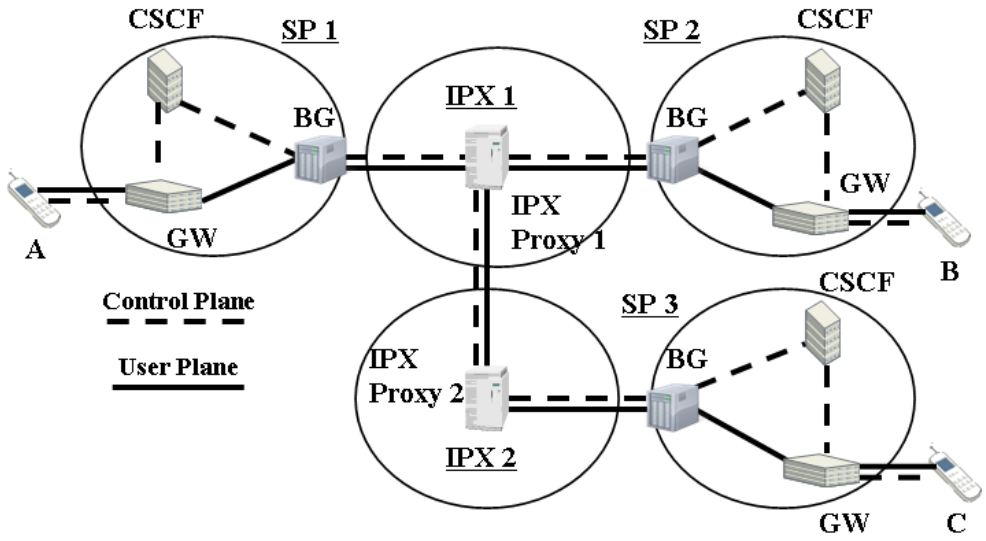


Figure 4-1: Overall Architecture of IMS Interconnection using the Proxy Model

In IPX this Proxy functionality is offered in the Bilateral Service Transit and Multilateral Service Hub connectivity options, as illustrated in the GSMA PRD AA.80 [22].

For further detailed information about this kind of additional Proxy functionality offered by the Inter-Service Provider IP Backbone, please see Annex C.

4.5 Media Routing

The IPX Provider should support OMR functionality as specified in 3GPP TS 29.079 [39], if it is allowed between two operators to prevent the user plane to be through the HPMN of roaming users, as described in Section 2.3.

5 Service Related Guidelines

5.1 Introduction

Different end-user services used in IMS have different requirements. As IMS allows different kind of IP based services to be used, issues have to be considered when assessing inter-Service Provider IMS connections. For example routing the Push to Talk over Cellular (PoC) user and control plane traffic between two Service Provider PoC servers has quite different requirements than routing traffic between two users in a peer to-peer IMS session.

The roaming, interconnection and interworking environment should be built in such a way that it supports multiple different types of IMS based services and applications. Thus, II-NNI cannot be the limiting factor when Service Providers are launching new services.

The actual IMS based services and their requirements are listed in other documents.

It should be noted that according to the GSMA Interconnect Working Group (IWG), only the originator of a multiparty session can add further participants to ongoing sessions such as multiparty chat or conference call. This general limitation applies to all IMS services in order to limit the possibilities for fraud.

5.2 IMS Based Voice and Video Communication

5.2.1 Overview

IMS based Voice and Video communication service (VoIMS) uses IMS as the enabling platform. VoIMS can be used for example to replace the CS based voice and video telecommunication service. Figure 5-1 below gives a high-level illustration of the architecture in which two clients using VoIMS UNI, are connected together via VoIMS NNI, transporting IP based voice and video user data end-to-end enabled by the IMS core systems of each Service Provider.

.

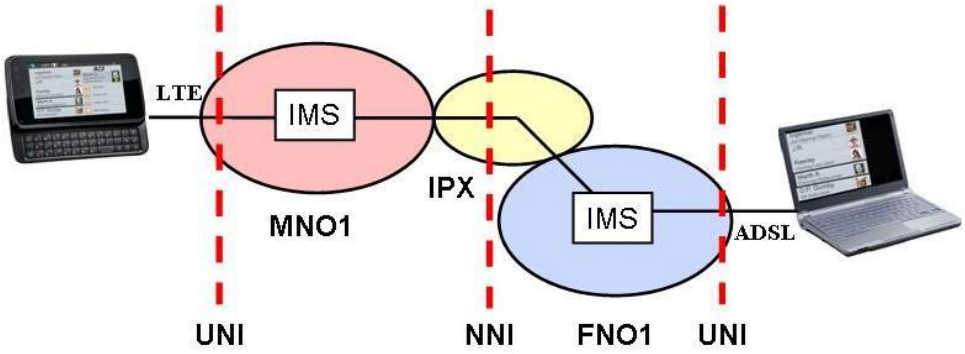


Figure 5-1: High-Level Example of IMS based Voice and Video communication

VoIMS UNI are specified in GSMA PRD IR.92 [28] IR.94 [36], IR.51 [53] and NG.106 [57] which are based on the IMS MMTel (Multimedia Telephony) standard defined by 3GPP. VoIMS NNI is specified in GSMA PRD IR.95 [50].

5.2.2 Multiple Voice NNIs

It is very likely that Service Providers will have to handle more than one voice NNI at the same time for the same service. For example, Service Provider A could have updated its agreement and technology for voice interconnection to use IP with Service Provider B, but still have the old TDM based voice interconnection in place with Service Provider C. Therefore, Service Providers originating VoIMS must have mechanisms to deal with both IMS and CS based voice interconnection . In addition there may be more than one voice NNI option (see also Figure 5-2). IPX Proxy may be used to forward SIP/SIP-I signaling and RTP media between Service Providers. More requirements and details on the IPX Proxy are listed in Annex C.

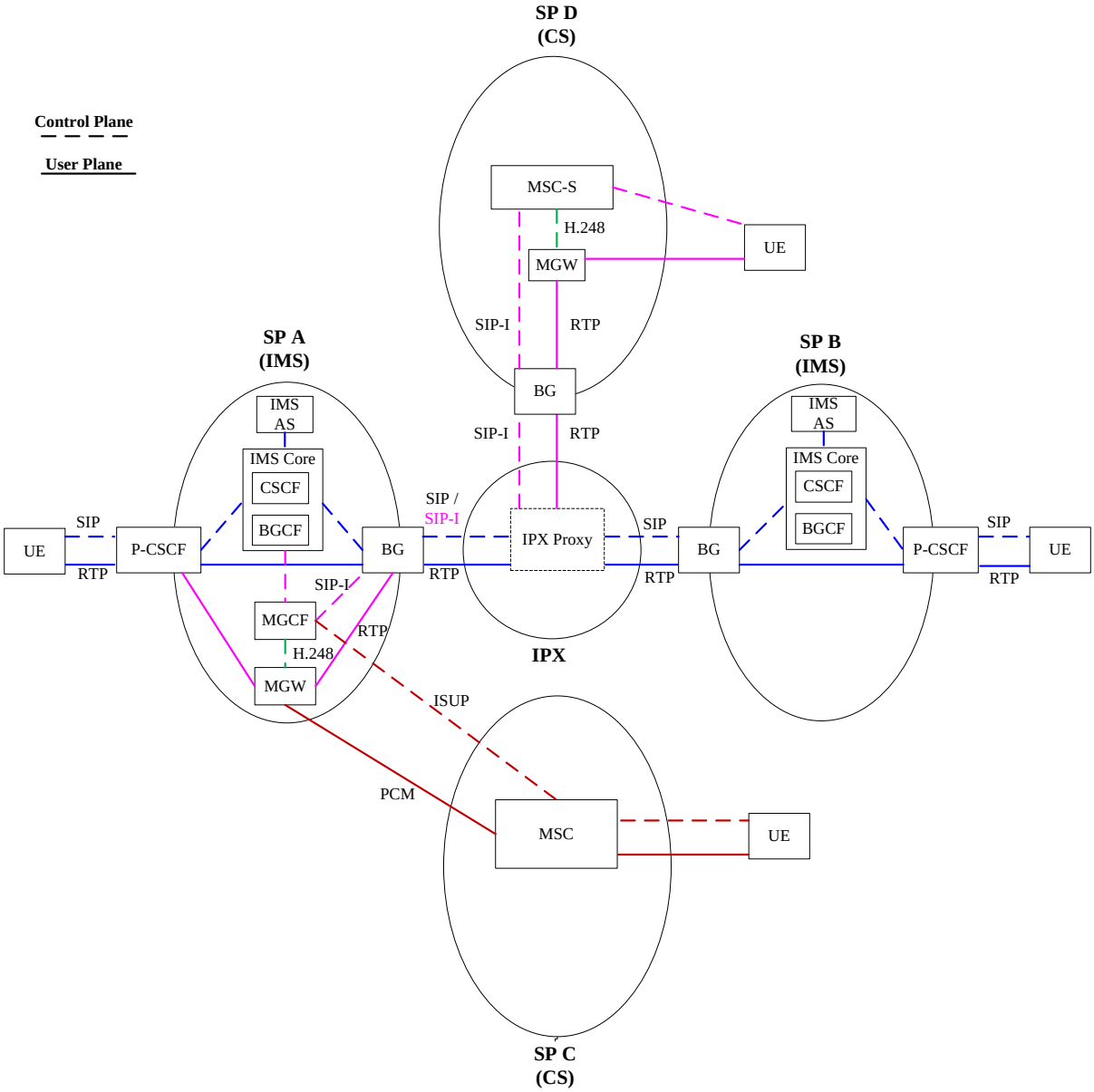


Figure 5-2: Multiple Voice NNIs

The originating Service Provider has a preference list for the outgoing VoIMS calls, for example:

1. Direct IMS-to-IMS call; this does not require the use of conversions or fallback mechanisms, offering the best possible quality. Signalling uses SIP and media RTP/RTCP. Other IMS based services, such as RCS, may also use the same IP based interface (see GSMA PRD IR.90 [27])
2. Fallback to CS domain, where the VoIMS call is converted into a CS call. The voice NNI can be:

    - IP based: SIP-I Signalling and RTP/RTCP media (see GSMA PRD IR.83 [33])
    - IP based: BICC Signalling and RTP/RTCP media with Nb UP Framing (see 3GPP TS 29.163 [7])

- ATM based: BICC Signalling and media with Nb UP Framing (see 3GPP TS 29.163 [7])

3. Fallback CS domain, where the VoIMS call is converted into a CS call using normal ISUP Signaling and TDM mechanisms.(see 3GPP TS 29.163 [7])

The originating Service Provider is responsible to determine which voice NNI to use for any particular call/session according to its local policy, as well as the requirements the originator needs to fulfill to its subscribers, VoIMS NNI knowledge, technical capabilities available, and cost. It is assumed that:

The originator will find a way to deliver traffic and,

- In the case of an IMS to IMS session the preferred solution is to deliver the traffic as IP end to end utilizing VoIMS NNI as described in Section 5.2.3
- The originator may also rely on the IPX provider services to determine if the destination is IMS capable or not.

II-NNI knowledge can be obtained through look up services. GSMA recommends the use of Carrier ENUM for this purpose as defined in NG.105 [54]. Carrier ENUM provides information on an international public telecommunications number basis and can indicate which routing via the II-NNI is possible. IMS routing is possible when a Carrier ENUM translation request provides a globally routable SIP URI. If this translation attempt fails at the originating S-CSCF the call can be delivered via IMS to CS interworking. IMS to CS interworking technical capabilities available to the originator may include:

- Local ability to convert IMS traffic into CS traffic
- Local ability to issue traffic using SIP-I

If the originator does not have, or is not willing to provide IMS to CS interworking, agreements with different carriers to perform IMS to CS interworking could be made.

Note that even if Carrier ENUM does not provide a globally routable SIP URI, the originating Operator may obtain knowledge of the terminating operator by other means, and if a VoIMS NNI exists to that operator, the originating operator may still decide to route the call over that VoIMS NNI.

The capabilities that the originator arranges are influenced by cost. Investment in IMS to CS conversion technology is normally a CAPEX decision, while agreements with others to perform conversions are OPEX decisions. In case the originator has access to more than one option for any particular call, the cost may influence the mechanism of voice NNI chosen.

Policy differs between Service Providers. The result is that the IMS NNI ecosystem will include Service Providers with a wide variety of combinations of the above capabilities and agreements.

It should be noted that in the case where neither VoIMS NNI nor IMS to CS interworking is supported, then the session would fail.

If Service Providers wish to enable the IPX to perform IMS to CS conversions they have to make the subscriber voice NNI information available to the IPX. One method of doing this is to allow the Carrier ENUM to access the IPX.

Today it is possible for the user plane of a call to undergo multiple conversions between TDM and packet transport in the case of a CS to CS call. For IMS telephony it is recommended that IMS to IMS calls/sessions undergo no conversions. For IMS to CS scenarios it is recommended that the conversion takes place only once.

5.2.3 VoIMS NNI

In the case of full end-to-end IMS based interconnection between two Service Providers offering VoIMS to their customers, connected to each other via II-NNI, no conversion or transcoding mechanisms should be needed.

IPX is being used as an example of the inter-Service Provider IP Backbone in the following figures. This does not exclude the use of other alternatives, such as a bilateral leased line, for VoIMS NNI purposes when fitted by the Service Providers.

It is recommended using a Carrier ENUM lookup during session setup to translate the international public telecommunications number into a globally routable SIP URI.

Section 3 depicts two models for generic II-NNI. Those models are fully applicable for the VoIMS NNI. A generic term “IMS Core” in the figures below is used to show that both architecture alternatives presented in Section 3, are equally applicable for the VoIMS NNI. The hubbing model is more convenient to reach a large amount of IMS peers as it can provide interworking and cascade billing, while the direct IMS-to-IMS model is preferred when a large amount of calls is expected between two service providers.

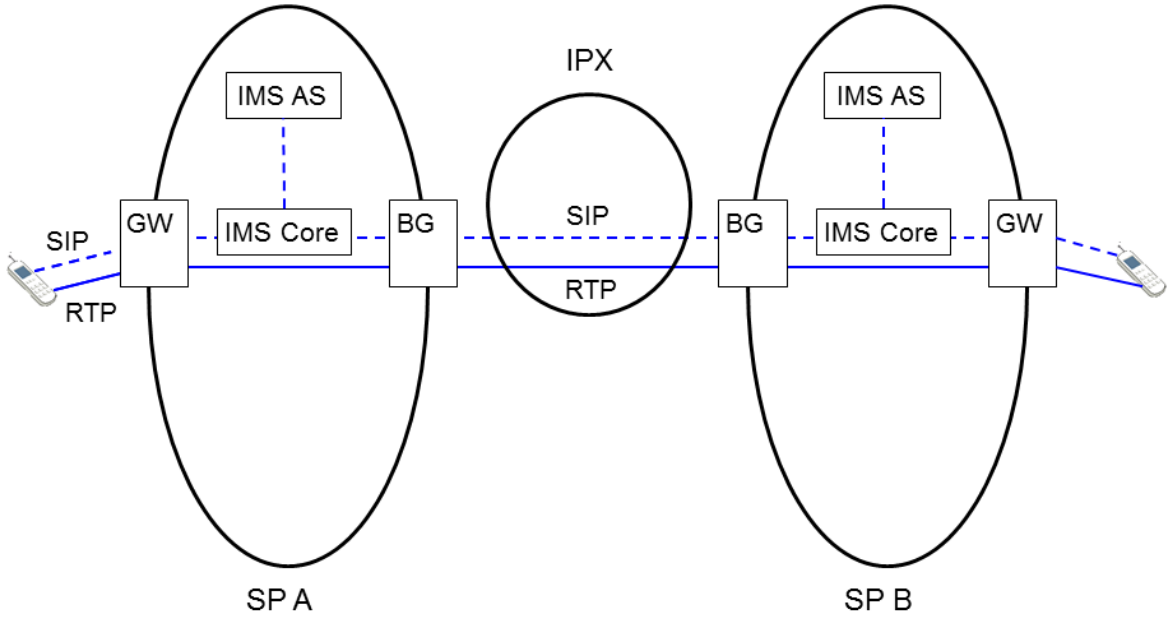


Figure 5-3: VoIMS NNI

Figure 5-3 above shows the VoIMS NNI, using IPX in the bilateral Transport Only connectivity option.

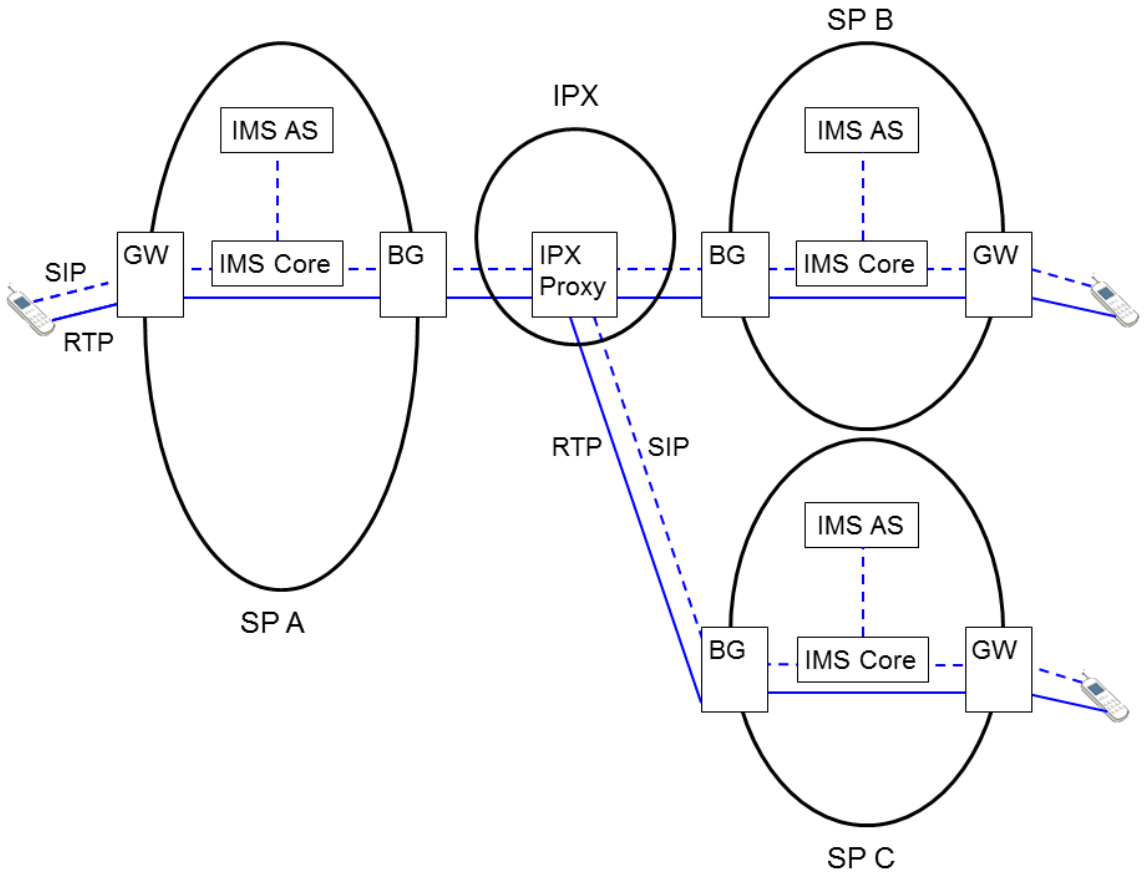


Figure 5-4: VoIMS NNI (Hubbing Model)

Figure 5-4 above shows the VoIMS NNI, using IPX in the multilateral Service Hub connectivity option. IPX Proxy is used to forward SIP signaling and RTP media between Service Provider A and Service Providers B and C. Annex C provides further details of IPX Proxy.

5.2.4 IMS to CS Interworking

When VoIMS NNI (as illustrated in the Section 5.2.3) cannot be used, the originating IMS network may use the capabilities specified in GSMA PRD IR.83 [33] (SIP-I based interworking) and 3GPP TS 29.163 [7] (BICC/ISUP based interworking). This is briefly described below. For further details see Annex A.

A Carrier ENUM lookup may be used during session setup to identify that the terminating user is an IMS subscriber as defined in GSMA PRD NG.105 [54]. Call breakout to CS occurs when the session cannot be routed further via the VoIMS NNI. CS breakout can be done either in the originating network, IPX or terminating network, depending on the agreement between Service Providers. At CS breakout, the originating BGCF selects the terminating network according to the defined rules. A session is forwarded either to local MGCF (via Mj interface) or to a BGCF of the terminating network (via Mk interface). MGCF handles the needed protocol interworking on the control plane between 3GPP SIP and BICC, SIP-I or ISUP. IMS-MGW handles the user plane interworking between RTP/UDP/IP (Mb interface) and PSTN user plane interface.

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

5.2.5 General Issues

5.2.5.1 Interconnection Models

As documented in Section 3, there are two alternative models for IMS interconnections. Both of them are valid for the VoIMS NNI purposes. A Service Provider may independently deploy any option defined above regardless of what an interconnected Service Provider chooses to deploy. Ici/Izi and Mw/MB can interoperate without Service Provider configuration or a dependency of an interworking function.

5.2.5.2 IPX

General QoS related guidance on IPX as documented in GSMA PRD IR34 [1] Section 8 is fully applicable also for the purpose of VoIMS NNI.

5.2.5.3 Adding Participants to a Conference

As illustrated in Section 5.1, only the originator of a conference call can add further participants to ongoing conference call. This is aligned with the similar restrictions placed towards other IMS based multiparty services, for example IMS based Chat service in GSMA PRD IR.90 [27].

5.2.5.4 Addition of New Media Streams

The addition of new media streams to an ongoing VoIMS session (in other words the modification of the session through re-INVITE) is within the current scope of this specification - see GSMA PRD IR.94 [36] section 2.2.2 and GSMA PRD NG.114 [56]..

5.2.5.5 SIP Accept-Contact Header

The Accept-Contact of an initial SIP INVITE request may, besides the MMTel (ICSI) feature tag, optionally also contains the 'audio' feature tag and the 'require' parameter. Said optional parts are set by RCS Broadband Access clients.

5.2.5.6 SIP Preconditions

As stated in GSMA PRD IR.92 [28] and NG.114 [56], the network has the option of disabling SIP preconditions. This means that any network involved in the interconnection or roaming path has that option. In that case, the considered network shall disable SIP preconditions by removing both the “precondition” option-tag from the SIP Supported header and the related SDP media attributes.

Note: The “precondition” SIP option-tag and the related SDP media attributes are defined in IETF RFC 3312 [48] as updated by IETF RFC 4032 [49].

5.2.6 IMS Voice & Video: SDP Offer and Answer

The payload types for AMR and AMR-WB with no mode-set specified in the initial SDP offer (see also GSMA PRD IR.92 [28] and NG.114 [56]) may be modified by the network to set the

mode-set according to the operator's policy before forwarding the SDP offer. Payload types with a specified mode-set cannot be modified by the network without providing RTP and RTCP interworking or transcoding between the unmodified and the modified mode-set.

The payload types for AMR and AMR-WB in the SDP answer (see also GSMA PRD IR.92 [28] and NG.114 [56]) should not be modified by the network. The network cannot modify or add a mode-set for AMR or AMR-WB payload types in the SDP answer without providing RTP and RTCP interworking or transcoding between the unmodified and the modified (or added) mode-set.

Note: Including a mode-set in the initial SDP offer by the network bears the risk of transcoding or even call failures unless the network knows the related capabilities of the network or the network knows the destination where the call is routed to.

5.3 PoC

PoC (Push-to-talk over Cellular) is an example of IMS based service using server-to-server connection between the Service Providers. Since PoC has a dedicated server-to-server interface, traffic routing over the Inter-Service Provider interface is simpler than in those services that lack this kind of interface. This is due to the fact that a server can have an address that belongs to an IPX address block (in other words is routable within IPX), while a handset cannot have this kind of address.

For the Inter-Service Provider PoC connection there are two interfaces: user plane (media + talk burst control, that is Real-time Transport Protocol (RTP) + Real-Time Transport Control Protocol (RTCP)) routed via POC-4 interface between PoC servers, while control plane (SIP signaling) 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 the Inter-Service Provider IP Backbone, as any other IMS routing of traffic. Anyway also the PoC user traffic needs to be protected from outsiders, either by using IPX network or by using VPN tunnels.

Deploying two separate network connections between Service Providers needs more consideration than just a single connection. For example, consideration is needed regarding the dual configuration of firewalls/border gateways towards the Inter-Service Provider IP Backbone. However, the IP-1 interface between IMS core networks is the same as for any other IMS based service, in other words normal Mw or Ici 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 Service Providers already have general IMS interconnection in place.

5.4 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 Multimedia Messaging Service Centre (MMSC) or PoC server. Typical P2P services envisioned for IMS are different multi-player games (such as chess or battleship), media sharing, imaging and multimedia streaming.

Even if the media can go directly from one terminal to another terminal without any intermediate server or proxy, these services require IMS to support setting up that service, in other words signaling always goes via the Service Provider IMS core.

When a P2P service is used, the user plane is routed directly between terminals implying that terminal IP addresses are used in user plane. However, as discussed above typically terminal IP addresses are not routable over the Inter-Service Provider IP Backbone, thus user plane needs to be put inside a tunnel in order to be routed over the Inter-Service Provider IP Backbone, such as IPX. GRE tunnels are used for this purpose as documented in GSMA PRD IR.34 [1] Section 6.5.6.

The routing of P2P traffic between Service Providers is handled via normal Mw/Ici control plane interface to set-up the service and then routing the user plane over the Inter-Service Provider IP Backbone between participating Service Providers. Roaming scenario does not pose any additional requirements for this service, since IMS user is always connected to home network.

5.5 RCS

RCS (Rich Communication Suite) (see GSMA PRD RCC.07 [51]) represents an IMS based service which combines a number existing stand-alone applications into an interoperable package, allowing end-users to for example see the capabilities of other users within the client address book before setting up a call/chat/message session with them.

From the IMS point of view RCS is a bundle of various standardized services, consisting of for example:

- Capability exchange based on OMA SIMPLE Presence and SIP OPTIONS
- Social Presence Information based on OMA SIMPLE Presence and XDM
- Chat based on OMA SIMPLE IM and CPM
- Voice call based on GSMA PRD IR.92
- Video call based on GSMA PRD IR.94
- Voice / video call based on GSMA PRD NG.114

For further details of the inter-operator aspects of RCS service, see GSMA PRD IR.90 [27].

5.5.1 RCS Functional Architecture

Some RCS specificities will be described in this section.

RCS solutions will used various approaches.(compared to other IMS services like voice) and, RCS specificities are related to

- Service: RCS terminals could interact directly like voice, or could interact with applications. Business between Application and Person (named A2P) will be seen as the evolution of A2P SMS and will represent for Service Providers significant wholesale revenues. Therefore, it is really important to define the technical solutions enabling such A2P RCS revenues.
- Architecture: different architectures like operator hubbing, hosting RCS platforms by RCS hub for several Service Providers

RCS traffic is composed of 2 major flows:

- Person-to-Person (P2P): RCS exchanges between 2 RCS users owned by Service Providers (SP).
- Application-to-Person (A2P): RCS exchanges between an application (MaaP, Chatbots, …) and an RCS user (traffic which could be from the application and/or from the user)

RCS platforms, managing A2P and/or P2P traffic, will be based on

- Direct relationship of 2 RCS platforms (deployed by the SP) or RCS group platforms (regrouping several operators in an RCS operator hub)
- Connection of RCS platforms (or RCS operator hubs) via a transit hub

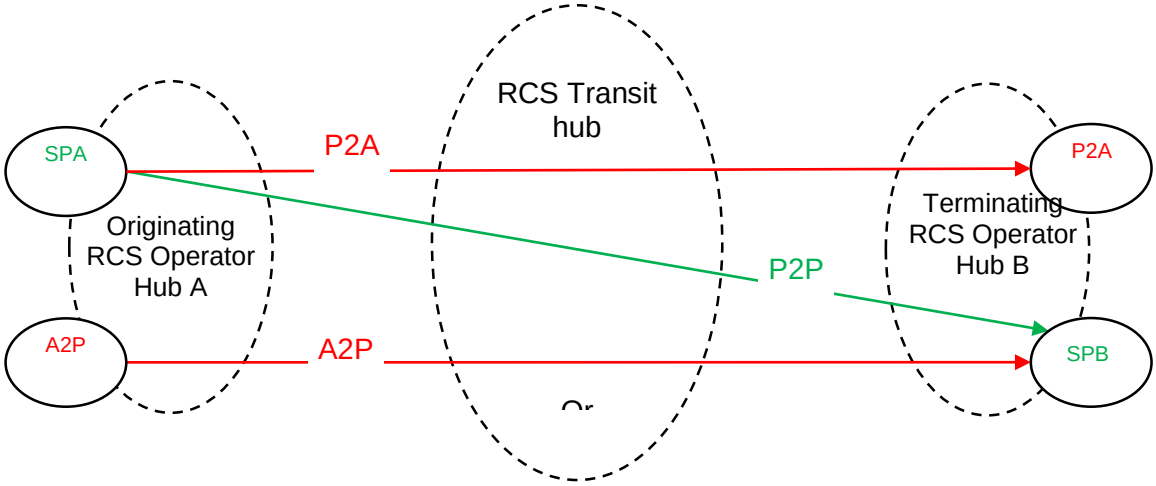


Figure 5-5: RCS Functional Architecture (Hub or not / A2P/P2A or P2P)

RCS operator Hubs (or RCS platform) could be connected

- Directly, or via the IPX transport (for the IP connectivity)
- Via an IPX proxy (for SIP/media connection via a transit hub)

A2P platforms could be connected to the RCS platforms using several approaches

- directly, or via the IPX transport (for the IP connectivity)
- via a SIP aware entity (for SIP or SIP/media connection via a transit hub)
- hosted by an RCS operator hub

From the technical perspective, the RCS operator hub could be composed of

- a Border gateway (example hub A)
- a Border gateway and IMS instance per Service Provider (example hub B)

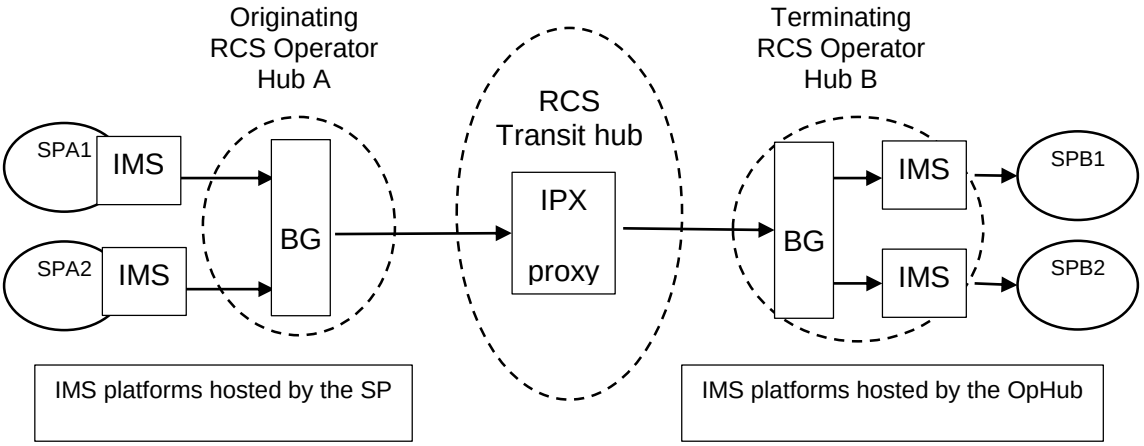


Figure 5-5: RCS Technical Architecture

For all those architecture options, the following requirements will be a common issue for the technical design:

- Identification of the originating and terminating service providers (P2P or A2P), in order to identify clearly the business actors
- Discrimination of A2P (including A2P/P2A) traffic versus P2P
- Discovery & Routing to the terminating service provider via the hub, resolving Number Portability

5.5.2 Service Providers Identification

In order to identify unambiguously the RCS business actors, originating, terminating and transit (in case of transit hub) service providers are associated to the following SIP information:

- Originating SP is associated to “orig-ioi” parameter.
- Terminating SP is associated to “term-ioi” parameter.
- In case of Transit hubs, “transit-ioi” parameter could be used by the transit hub, while “orig-ioi” and “term-ioi” shall not be modified and will be guaranteed between originating and terminating networks. “transit-ioi” parameter shall not be voided.

Notes:

1. “ioi” (Inter operator Identifier) parameters are part of P-Charging-Vector header and usages are clearly defined in reference 3GPP 29.165 [19]
    a. SIP requests containing the type 2 "orig-ioi" with the entry which identifies the home originating network;
    b. SIP responses containing the type 2 "orig-ioi" and type 2 "term-ioi" header field parameters with the entries which identify the home originating network and the home terminating network respectively;
    c. For the II-NNI for the transit scenario, SIP requests and responses containing the "transit-ioi" header field parameter with the entry(ies) which identify the transit network(s);
2. For Group Chat, the ioi parameter reflects the operator of the Group Chat server. In case Group Chat server changes as a result of Group Chat restart after the original focus was terminated, the ioi should reflect the new Group Chat server.

5.5.3 A2P/P2P Traffic Discrimination

In order to implement potentially different business models for A2P and P2P, it could be nice to rely on some information to discriminate the A2P/P2P traffic origin (A2P) or destination (P2A).

All domain names (including “ioi” parameter) related to the originating (A2P) or terminating (P2A) actor used in SIP signaling could be coded with the following policy as described in RCC.07 section 2.5.4 and section 2.6.1.3:

1. Alphanumeric SIP URIs (Example:sip:<bot_service_id_userpart>@botplatform.<botplatformdomain>)
2. Short code like telephone number represented as a Tel URI (Example: tel:555; phone-context=example.com)
3. Contact tag in the SIP message from ChatBot: **“+g.gsma.rcs.isbot”**

All domain names (including “ioi” parameter) associated to Service Providers could be coded using the following URI format:

1. In case of RCS operator being an MNO, SP domain could be used using the URI format as defined by NG.105 [54] including mnc<MNC>.mcc<MCC>.3gppnetwork.org
2. In case of RCS operator being an MVNO hosted by another SP, the ioi of that operator can be created by adding mvno name to the SP domain, in the format: <MVNO>.mnc<MNC>.mcc<MCC>.3gppnetwork.org.

5.5.4 Discovery and Routing (Resolving Number Portability)

In order to route RCS traffic to the destination, Number Portability resolution shall be resolved.

Various technologies could be used:

1. ENUM technology could be used by the originating IMS platform (SPA or RCS operator hub A) in order to discover the destination IMS platform (SPB or RCS operator hub B). As defined in NG.105 [54], ENUM proxy architecture could be used, enabling the interrogation of various Data Base (ENUM, HLR, NP DB, …).
2. Dynamic Discovery of the destination based on the origin of the traffic received. Each customer could be associated to an SPB or RCS hub B, based on the observation of the incoming traffic. A Data Base could be built in real-time, observing incoming traffic. This Dynamic Discovery Data Base shall be used to select the destination.

5.6 HDVC

The HDVC (High Definition Video Conference) service, based on IMS, comprises point to point and (multiparty) video conferences with one full duplex audio stream with tight synchronisation to one main video stream and another video stream aimed for sharing of, for example, presentation slides.

The HDVC service itself (UNI) is defined in GSMA PRD IR.39 [41].

The NNI specificities (as mentioned in Section 3.2) for the HDVC service are based on 3GPP TS 29.165 [19]. The updates of TS.29.165 for HDVC usage are specified in Annex B of the present PRD.

5.7 IMS NNI in case of multiple IMS core network deployments

IMS services as described in the Sections 5.2 and 5.5 may be deployed in

- Single IMS core for all IMS services or
- Dual IMS cores, one IMS core for MMTEL services and one IMS core for RCS services.

There is a need to provide inter-connect between MNOs that have chosen different deployment options (i.e. single IMS core versus dual IMS cores). Such interconnects are subject to bilateral agreements between MNOs.

It is recommended that a single IMS NNI for all IMS services is used, in order to avoid impacts by operators having decided for a dual IMS core deployment on operators having decided for a single IMS core deployment for all IMS services. In this case, the related

ENUM configuration points to a single IMS core network address for a given (MSISDN) number and all SIP messages destined for a given (MSISDN) number are routed to a single entry point. It is then within the responsibility of the operator with dual IMS cores or of its IPX provider to ensure correct routing of SIP messages to the right IMS core.

Based on the bilateral agreement, operators may agree to have a dedicated IMS NNI for RCS services as described in GSMA PRD IR.90 [27] in parallel with the IMS NNI used for IMS Telephony, e.g. if both operators have deployments with dual IMS cores with one for IMS Telephony and one for RCS. In this case, traffic must be sent across the correct NNI dependent on the whether it is related to MMTel or RCS services. In such deployments, the target IMS core network can be selected via ENUM as described in .section 4.2.3 of GSMA PRD NG.105 [54].

As a third option, it is also possible that there is no direct bilateral agreement in place and one operator may elect to advertise a single NNI for all services and another to have two separate NNIs for MMTel and RCS. Such operators must be connected via an intermediate network (e.g.IPX). In this case, it is recommended to use ENUM to resolve the destination telephone number to multiple SIP URIs and identify the correct target IMS Network as described in section 4.2.3 of GSMA PRD NG.105 [54].

For details of the NNI between a single IMS core and dual IMS core, see GSMA PRD IR.95 [50] section 13.

6 Addressing and Routing Guidelines

6.1 User and UE Addressing

IMS user addressing is defined in 3GPP TS 23.228 [5] and its format is defined in 3GPP TS 23.003 [10]. GSMA PRD IR.92 [28] and NG.114 [56] further clarifies that UEs and IMS core network must support Public User Identities in the form of SIP URIs (both alphanumeric and those representing Mobile Subscriber ISDN Numbers (MSISDNs)) and Tel URIs as follows:

Alphanumeric SIP URIs

Example: sip:voicemail@example.com

MSISDN represented as a SIP URI

Example: sip:+447700900123@example.com;user=phone

MSISDN represented as a Tel URI

Example: tel:+447700900123

To support the use of MSISDN as a Public User Identity, the network must associate a Tel URI with an alphanumeric SIP URI using the mechanisms specified in 3GPP TS 23.228 [5] and 3GPP TS 24.229 [6].

For Public User Identities assigned to a user, and in order to receive inbound calls/sessions, it is recommended to assign at least one E.164 number (MSISDN) to this user in order to enable CS interworking (for both break-in and breakout and for SR-VCC). A SIP URI may also be assigned as a Public User Identity to receive inbound calls/sessions, however, it should be noted that domain names used therein need to be agreed between interconnecting Service Providers in order to guarantee uniqueness and routing (see Section 6.4.3 for more information).

The UE and the IMS core network can use either IPv4 or IPv6. If a UE is assigned both an IPv4 and an IPv6 address, then an IR.92 [28] or NG.114 [56] compliant UE will use an IPv6 address. However, a IR.92 [28] or NG.114 [56] non-compliant UE may prefer to use IPv4 and may also use the IMS well-known APN (as defined in IR.88 [26]). Therefore, in order to avoid service outage to the UE, it is recommended that operator networks that allocate both an IPv4 address and IPv6 address to a UE also allow the UE to use either IPv4 or IPv6 addressing in their IMS networks.

Due to UEs being able to use different IP versions, establishing an IMS session with an end point can require IP version interworking for the user plane if that end point is using a different version of IP to the one used in the UE. Such interworking can be taken care by an interconnecting network (for example, the IPX – see IR.34 [1] for more information) or by a function (e.g. TrGW) located in the originating HPMN or in the terminating HPMN. For roaming, the originating VPMN or terminating VPMN may also perform the interworking (subject to the roaming agreement with the HPMN).

Note**:** IP version interworking is not required for the control plane because the control plane from the UE terminates at the P-CSCF (Gm interface). The P-CSCF will then establish a new transport leg to the next hop (e.g. I-CSCF), which can be either the same or different IP version as the one used on the Gm interface in case the P-CSCF is dual-stack, or the new transport leg is routed via an IBCF (acting as IPv4 to IPv6 proxy) that is also dual-stack.

6.2 Node Addressing

6.2.1 P-CSCF Identifier Coding

The P-Visited-Network-ID (see IETF RFC 3455 [37]) is generated by the P-CSCF for the purpose of identification of the location of the P-CSCF (for LBO roaming architecture) and location of the UE (for LBO and S8HR / N9HR roaming architecture). In order to provide ease of charging and billing in the home network, the format of the P-Visited-Network-ID must take the form of an Internet domain name (as per IETF RFC 1035 [38]) and adhere to the following scheme

- *ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org*, for LBO roaming architecture where MNC and MCC are those of the visited network where the P-CSCF and the UE are located; or

- optionally*, s8hr.ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org*, for S8HR roaming architecture (P-CSCF is located in the home network) where MNC and MCC are those of the visited network where the UE is located (received by the P-CSCF from Rx interface as defined in 3GPP Release 14 TS 29.214). Since for S8HR this FQDN will never be exposed to partners it is referenced as optional.
- optionally*, n9hr.ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org*, for N9HR roaming architecture, similar to S8HR case.

6.3 Network Address Translation (NAT) / Network Address and Port Translation (NAPT)

A NAT/NAPT function (known hereafter as just "NAT function") can be deployed on an IP network that is serving an IMS UE for example to enable private IPv4 address ranges to be used for UE Gm interface IP addressing. However, if the NAT function is deployed between the UE and the P-CSCF then this may lead to the UE and P-CSCF to negotiate the use of Keep-Alive messaging (as defined in IETF RFC 6223 [40]) in order to keep address bindings fresh in the NAT function.

Such Keep-Alive messaging can have a negative effect on UE battery life and increases signalling load between the UE and P-CSCF. Therefore it is recommended that where the operator owns the IP network serving the IMS UE and if there is a need to perform NAT, the NAT function should be deployed in a way that is transparent to the UE (as recommended in Annex E.6 of 3GPP TS 23.228 [3]).

> Note**:** There may be cases where the presence of a NAT function between the UE and P-CSCF cannot be avoided, for example Wi-Fi networks, and in such cases the use of Keep-Alive messaging may be unavoidable, see e.g. GSMA PRD IR.51 [53].

6.4 Routing

6.4.1 General

Coexistence of separate networks means that there is a requirement for certain IMS core elements to be reachable and routable from a Service Provider's internal IP network as well as from the Inter-Service Provider IP Backbone network, since they are used both in internal connections and external connections. Thus, those IMS elements should be multi-homed or otherwise be capable of supporting two or more network addresses.

In addition, the IMS core should be capable to distinguish whether DNS queries need to be sent towards the Inter-Service Provider IP Backbone DNS or internal/public Internet DNS, since the two Domain Name Systems are separated.

Section 7 of GSMA PRD IR.34 [1] illustrates the general guidelines for Service Providers, including this issue of handling multiple IP networks from a single IMS core system. GSMA PRD IR.67 [24] specifies the domain names used on the Inter-Service Provider IP Backbone network.

6.4.2 Roaming

In case of IMS roaming where the P-CSCF is located in the VPMN, the P-CSCF discovers the HPMN entry point by resolving the HPMN domain name as given in the Request-URI of SIP

REGISTER request. It is recommended to only use domain names as specified in GSMA PRD IR.67 [24] Section 2.3.3 for the Request-URI, in order to enable DNS resolution and routing when using the Inter-Service Provider IP Backbone network.

Similarly, and for the same purpose, when Node URIs are exchanged in roaming situations for later usage during call setup, (for example when P-CSCF and S-CSCF URIs are exchanged during registration), those URIs shall be based on IMS Node names specified in GSMA PRD IR.67 [24] Section 2.6.

When the URI of the IMS final address node is accompanied by the URI of an entry node of the same network for the purpose of providing topology hiding, the URI of that node's final address may be encrypted. In such a situation, the network entry node URI needs to meet the above requirements.

6.4.3 Interconnection

Routing of SIP signaling over the II-NNI shall normally be based on the use of SIP URIs. Routing is based on the Request URI, unless one or more Route headers are present, in which case they take priority over the Request URI. See below for the use of Route header in case of roaming.

Session requests based upon E.164 format Public User Identities (see clause 6.1) should be converted into an NNI routable SIP URI format. This conversion can be done using ENUM (see GSMA PRD NG.105 [54] for more information).
Section 5 of this document as well as GSMA PRD NG.105 [54] specify a number of cases where an IMS NNI can be used even if the E.164 number conversion using ENUM is not performed or has failed. For such cases the originating operator may either:

- Send the SIP request using the Tel URI format, or
- Prior to sending the SIP request, convert the Tel URI to a SIP URI as follows: The content of the Tel URI is placed in the User part, the domain name of the next network (Carrier or Terminating operator) is placed in the host part and a user parameter set to "Phone" is added, resulting in sip:<E.164>@<next_network>;user=phone

Session requests based upon user entered alphanumeric SIP URIs require either a conversion to an NNI routable SIP URI (see Note below) or the domain names used therein to be provisioned in the IP backbone network providing the IMS NNI to be agreed between interconnecting Service Providers in order to guarantee uniqueness .

Note 1: The 3GPP and other standards bodies are looking into a more structured approach for resolving the issue of routing between IMS networks, particularly for multi-national corporate entities (who may have different Service Providers in different countries where they are present), as part of their work on "IMS Network Independent Public User Identities (INIPUI)".

For IMS interworking, the IMS of the originating Service Provider discovers the IMS point of contact (I-CSCF/IBCF) of the terminating Service Provider based on the recipient domain as documented in the Section 4.5.2 of GSMA PRD IR.67 [24].

A Service Provider may provide a SIP Route header. For an IPX Provider, the topmost Route header entries have significance:

A Service Provider may add a Route header entry pointing to the entry node of the selected IPX Provider. If present, this Route header entry will be the topmost Route header entry received by the IPX Provider´s network, and will be removed by the entry node of the IPX Provider´s network according to RFC 3261 procedures, and not be used for routing within the IPX Provider´s network.

Note 2: A Route header entry pointing to the entry node of the IPX Provider´s network can be used for routing within the Service Provider´s network, for instance in order to help the Service Provider to select a particular interconnection network among multiple serving IPX Providers.

The Service Provider may also include one or more Route header entries identifying particular IMS nodes that must be traversed in the destination Service Provider´s network. When being received by the entry node of the IPX Provider´s network, those Route header entries will appear right after the Route header entry, if present, for the entry node of the IPX Provider´s network and otherwise as topmost route header entries. After the removal of the Route header entry for the entry node of the IPX Provider´s network, the IPX Provider´s network shall route based on the top-most Route header entry. The top most Route header must contain a SIP URI with a domain name that is in accordance with GSMA PRD IR.67 [24] Section 2.3, or otherwise a domain name that is bilaterally agreed.

Note 3: Route header entries for the destination network are required when there is a roaming leg between a VPMN and a HPMN (see Section 2.3). The destination network then is the network that terminates the roaming leg, i.e. for session request, the originating HPMN or the terminating VPMN.

6.5 Identification of Services

6.5.1 Overview

Identification of services is an important aspect of interconnection. For example possible intermediate IPX nodes (such as IPX Proxy) and also terminating networks with regards to securing interconnection agreements and potential termination fees, etc. need this service identification. To facilitate the using of the same NNI for multiple services, it is essential that clear and unambiguous information of the requested service should be included in SIP signalling. This will ensure that the interconnected parties agree the requested service.

According to 3GPP TS 24.229 [6], charging and accounting is based upon the ICSI (IMS Communication Service Identifier) of the P-Asserted-Service header and the actual media related contents of the SIP request. Therefore, the content of the P-Asserted-Service header is the prime source for identifying the requested service and must be included in the initial SIP requests for all services that have an ICSI defined.

However, a well-formed SIP request also contains other headers and fields that can be used to identify the service, e.g. by a terminating UE, such as the Accept-Contact header. This additional information, which the originating Service Provider should ensure to maintain consistent with the service identified in the P-Asserted-Service header, could also be used to identify different variants of the same service or similar services sharing the same ICSI. Also it must be used for the few services, that still do not have an associated ICSI.

To allow a smooth upgrade of existing NNI deployments, and when based on bilateral agreements between the interconnected parties, the information defined as additional to the P-Asserted-Service header can also be used for an “Alternative Method” to identify the service at the NNI.

6.5.2 Service Request over the Originating Roaming II-NNI

When the II-NNI is used for an originating service request from a VPMN towards HPMN, no P-Asserted-Service header can be included in the initial SIP request. Instead the P-Preferred-Service header populated by the UE can be used at the NNI, even if the requested service has not yet been asserted by the home network.

When the HPMN receives an initial SIP request from one of its outbound roamers and the SIP request contains a P-Preferred-Service header, the SIP request must only be progressed if the P-Preferred-Service header is replaced by a P-Asserted-Service header containing an ICSI that corresponds to the ICSI received in the P-Preferred-Service header.

When the HPMN receives an initial SIP request from a VPMN and this SIP request does not contain a P-Preferred-Service header, and the SIP request is progressed towards the requested destination, the HPMN shall include a Feature-Caps header containing information about the asserted service used for the progressed SIP request in the first 1XX and 2XX response (to the initial SIP request) sent back towards the VPMN.

6.5.3 Special Consideration for Non-INVITE Initial SIP Requests

Although most IMS services are using the SIP INVITE to establish a media connection to be used to carry the service content end-to-end, there are some IMS services e.g. SMSoIP and in RCS, for which the service content is delivered as part of the Non-INVITE SIP session or stand-alone SIP signalling requests.

The Procedures described in the Section 6.5.2 are also valid for such Non-INVITE Service requests.

However, non-INVITE SIP session requests and Stand-Alone SIP requests, are also frequently used for basic IMS signalling mechanisms, and do not necessarily pertain to a particular IMS service, e.g. Registration signalling for roaming UEs.

Therefore, the absence of an ICSI in a P-Asserted/Preferred-Service SIP header or the failure to identify the service using the alternative method, must not automatically lead to the conclusion that a non-supported service is requested, and that the SIP request shall be

rejected. In particular a border node such as an IBCF should allow such SIP requests, unless they are caught by a specific filter.

6.5.4 ICSI-Values and Alternative Methods to Identify a Service

The ICSI values associated with a specific service are specified in the corresponding service specification. In addition, for the RCS services, GSMA PRD IR.90 [27] includes information about ICSIs as well as specifying the alternative method for each individual RCS service.

6.5.5 Service Request Over the Terminating Roaming II-NNI

When the II-NNI is used for a terminating service request from an HPMN towards a VPMN in IMS Roaming Architecture using LBO (see Section 2.4.2), the P-Asserted-Service header must be included by the HPMN in the initial SIP request for all services that have an ICSI defined.

Note: urn:urn-7:3gpp-service.ims.icsi.mmtel is the ICSI value used to indicate the IMS Multimedia Telephony.

Based on bilateral agreements between the interconnected parties, the information defined as additional to the P-Asserted-Service header can also be used for an “Alternative Method” to identify the service at the NNI.

Annex A IMS to CS Voice Interworking

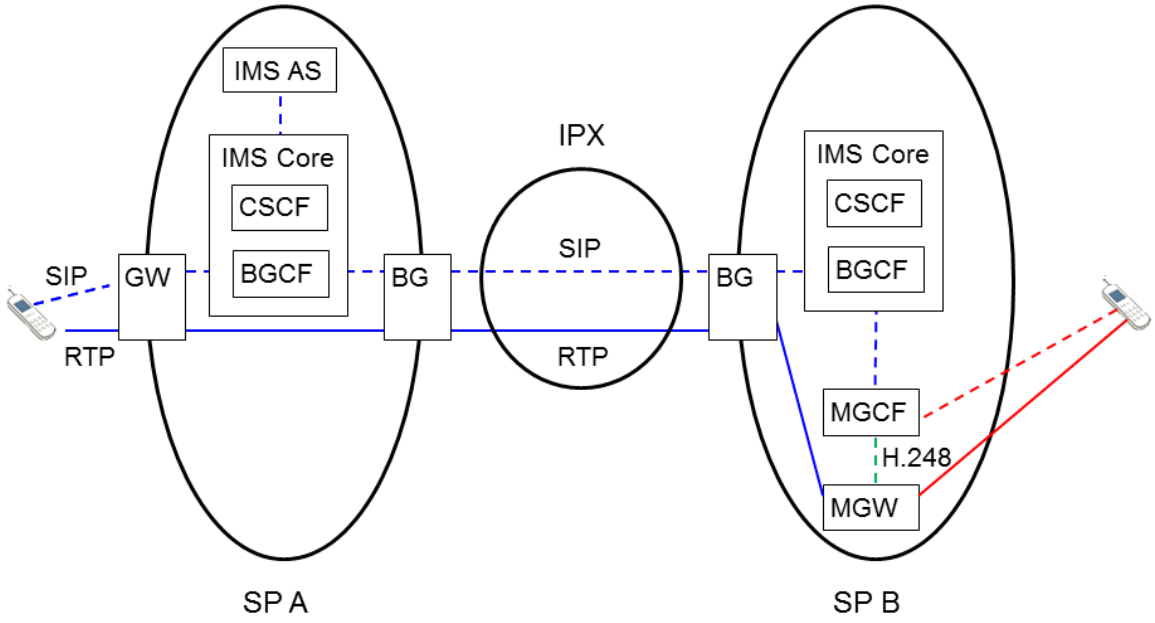


Figure A-1: IMS-to-IMS Voice NNI with receiver using CS UNI

Figure A-1 above shows an illustrative example of Client A using an IMS based UNI connecting with Client B using CS based UNI. In this example, the necessary IMS to CS conversion takes place in Service Provider B premises (as decided by the Service Provider A's BGCF): that is the IMS based voice NNI.

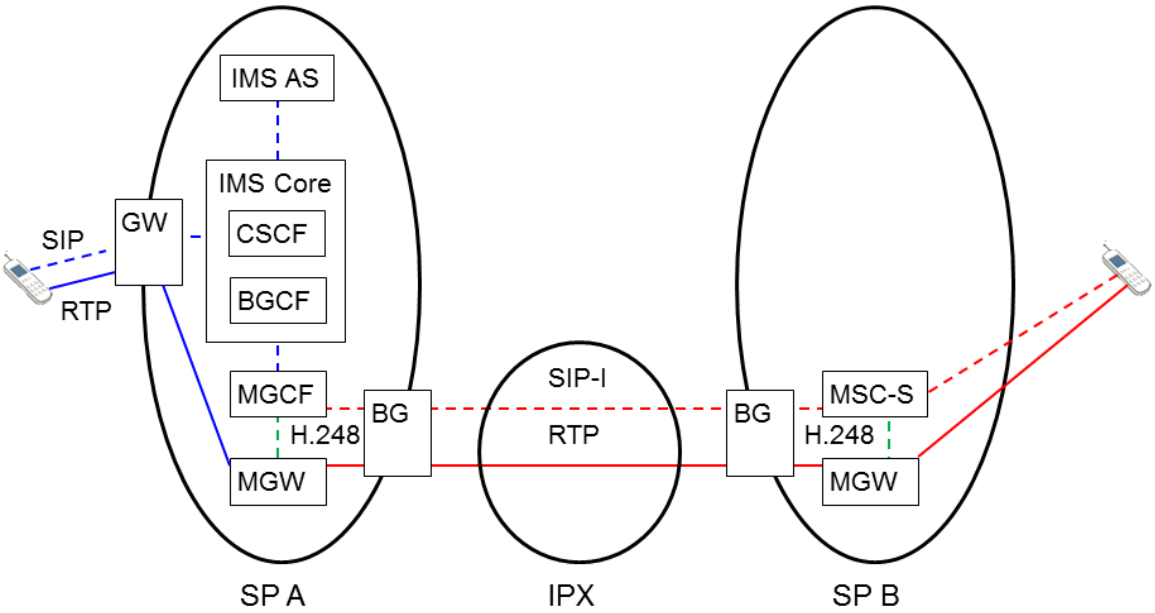


Figure A-2: IMS-to-MSC-S Voice NNI

Figure A-2 above shows an illustrative example of Client A using an IMS based UNI connecting with Client B using CS based UNI. The voice NNI in this scenario is IP based, using SIP-I between MGCF of Service Provider A and MSC-S of Service Provider B.

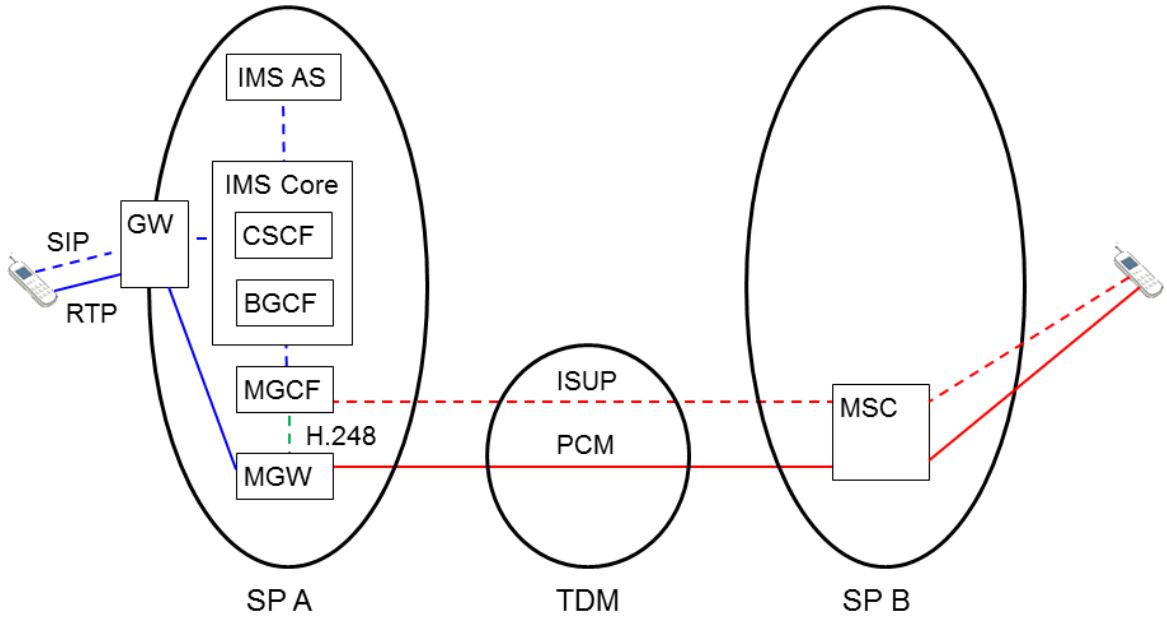


Figure A-3: IMS-to-MSC Voice NNI

Figure A-3 above shows an illustrative example of Client A using an IMS based UNI connecting with Client B using CS based UNI for the exchange of voice traffic. In this example, the necessary IMS to CS conversion takes place in Service Provider A premises , that is the CS based voice NNI.

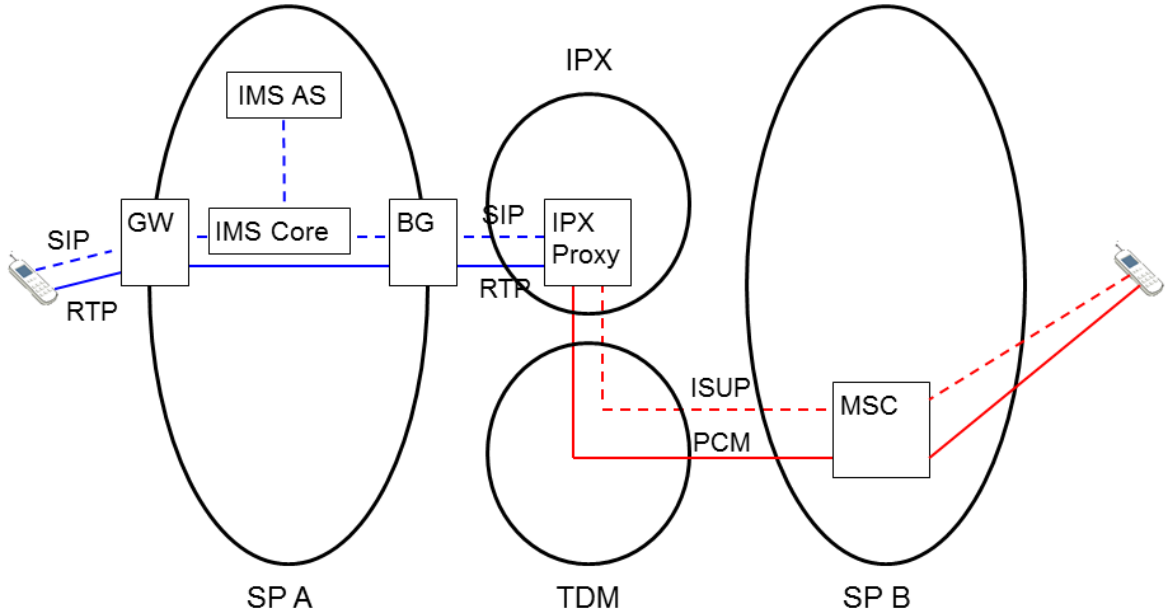


Figure A-4: IMS-to-MSC Voice NNI with IPX performing the TDM breakout

Figure A-4 above shows an illustrative example of Client A using an IMS based UNI connecting with Client B using CS based UNI for the exchange of voice traffic. In this example, the necessary IMS to CS conversion is performed by the IPX Proxy, in which the voice NNI is converted from IMS to CS.

Annex B Usage of 3GPP TS 29.165 for HDVC

This annex highlights the updates required compared to 3GPP TS 29.165 [19] (Release 9) for HDVC / NNI.

Note: The reference numbers of the specifications used in the next Sections are those of 3GPP TS 29.165 [19] except otherwise mentioned.

B.1 Control Plane Interconnection

B.1.1 SIP Methods Relevant for HDVC

The following Table B.1 represents the HDVC related modifications compared to a corresponding table (6.1) in 3GPP TS 29.165.

Item	Method	Ref.	II-NNI	
			Sending	Receiving
5A	INFO request	IETF RFC 6086 [28]	n/a (in place of o) See Note 1	n/a (in place of o). See Note 1
5B	INFO response	IETF RFC 6086 [28]	n/a (in place of o) See Note 1	n/a (in place of o). See Note 1
9A	MESSAGE request	IETF RFC 3428 [19]	n/a (in place of o) See Note 1	n/a (in place of o). See Note 1
9B	MESSAGE response	IETF RFC 3428 [19]	n/a (in place of o) See Note 1	n/a (in place of o). See Note 1
10	NOTIFY request	IETF RFC 3265 [20]	m (in place of c1) See Note 2	m (in place of c1). See Note 2
11	NOTIFY response	IETF RFC 3265 [20]	m (in place of c1) See Note 2	m (in place of c1) See Note 2
15A	PUBLISH request	IETF RFC 3903 [21]	n/a (in place of c1) See Note 3	n/a (in place of c1) See Note 3
15B	PUBLISH response	IETF RFC 3903 [21]	n/a (in place of c1) See Note 3	n/a (in place of c1) See Note 3
16	REFER request	IETF RFC 3515 [22]	o See Note 4	o See Note 4
17	REFER response	IETF RFC 3515 [22]	o See Note 4	o See Note 4
Item	**Method**	**Ref.**	**II-NNI**	
			Sending	**Receiving**
20	SUBSCRIBE request	IETF RFC 3265 [20]	m (in place of c1) See Note 2	m (in place of c1) See Note 2
21	SUBSCRIBE response	IETF RFC 3265 [20]	m (in place of c1) See Note 2	m (in place of c1) See Note 2

Table B.1: Supported SIP methods (changes for HDVC)

Note 1: This method is not used in the current release of HDVC.

Note 2 SIP SUBSCRIBE/NOTIFY must be supported for the “reg-event” package (roaming) and for the “conference-status” package (roaming and inter home) if NNI is between a HDVC visited network and a HDVC home network, for example, when using LTE access and roaming.

Note 3: In TS 29.165, it is defined as Optional in case of NNI roaming interface to cover the interface between the UA and its home presence server. This method is not used for the HDVC service.

Note 4: The REFER method is used in HDVC for multipoint (adding a new participant). The detailed usage for is described in Clause 12.19 of TS 29.165.

B.1.2 Major Capabilities

The following Table B.2 represents the HDVC related modifications compared to a corresponding table (6.1.3.1) in 3GPP TS 29.165.

Item	Capability over the Ici	Reference item in 3GPP TS 24.229 [5] for the profile status		Profile status over HDVC II-NNI
		UA Role	Proxy Role	
	Basic SIP (IETF RFC 3261 [13])			
17	IETF RFC 6086 [39]: SIP INFO method and package framework	13	20	n/a (in place of o) See Note A
17A	draft-ietf-sipcore-info-events-08 [39]: legacy INFO usage	13A	20A	n/a (in place of o) See Note A
19	IETF RFC 3515 [22]: the SIP REFER method	15	22	o See Note D
Item	Capability over the Ici	Reference item in 3GPP TS 24.229 [5] for the profile status		Profile status over HDVC II-NNI
		UA Role	Proxy Role	
23	IETF RFC 3265 [20]: SIP specific event notification (SUBSCRIBE/NOTIFY methods)	20, 21, 22, 23	27, 28	m (in place of c1). See Note B
29	IETF RFC 3428 [19]: a messaging mechanism for the Session Initiation Protocol (SIP) (MESSAGE method)	27	33	n/a (in place of o) See Note A
32	IETF RFC 3455 [24]: private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)	30	35	See following 33-34-35-36-37-38 (in place of o)
44	IETF RFC 3903 [21]: an event state publication extension to the session initiation protocol (PUBLISH method)	41	51	n/a (in place of c1) See Note C
47	IETF RFC 3891 [54]: the Session Initiation Protocol (SIP) "Replaces" header	44	54	m (in place of o)
48	IETF RFC 3911 [55]: the Session Initiation Protocol (SIP) "Join" header	45	55	n/a (in place of o)
49	IETF RFC 3840 [56]: the callee capabilities	46	56	m (in place of o) See Note E
56	IETF RFC 5627 [62]: obtaining and using GRUUs in the Session Initiation Protocol (SIP)	53	63	n/a (in place of c1)
62	IETF RFC 5365 [67]: multiple-recipient MESSAGE requests in the session initiation protocol	59	69	n/a (in place of o if 29, else n/a)

65	IETF RFC 5366 [70]: conference establishment using request-contained lists in the session initiation protocol	62	72	m (in place of o)
66	IETF RFC 5367 [71]: subscriptions to request-contained resource lists in the session initiation protocol	63	73	n/a (in place of o if 23, else n/a)
68	IETF RFC 4964 [73]: the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular	65	75	n/a (in place of o)
77	IETF RFC 6050 [26]: Identification of communication services in the session initiation protocol	74	84, 84A	m (in place of o)
Item	Capability over the Ici	Reference item in 3GPP TS 24.229 [5] for the profile status		Profile status over HDVC II-NNI
		UA Role	Proxy Role	
88	IETF RFC 3862 [92]: common presence and instant messaging (CPIM): message format	85	95	n/a (in place of o) See Note A
89	IETF RFC 5438 [93]: instant message disposition notification	86	96	n/a (in place of o) See Note A

Table B.2: Major capabilities over II-NNI (changes for HDVC)

Note A: This method is not used in the current release of HDVC.

Note B: SIP SUBSCRIBE/NOTIFY must be supported for the “reg-event” package (roaming) and for the “conference-status” package (roaming and inter home) if NNI is between a HDVC visited network and a HDVC home network, for example, when using LTE access and roaming .

Note C: In TS 29.165, it is defined as Optional in case of NNI roaming interface to cover the interface between the UA and its home presence server. This method is not used for the HDVC service.

Note D: The REFER method is used in HDVC for multipoint (adding a new participant). The detailed usage for is described in Clause 12.19 of TS 29.165.

Note E: This capability can appear at the roaming NNI.

B.1.3 Control Plane Transport

Clause 6.2.1 of TS 23.165 applies.

B.2 User Plane Interconnection

B.2.1 Media & Codecs

The codecs described in the HDVC UNI profile applies with the following clarification for Voice:

The NNI must support the AMR codec and the AMR-WB codec for both roaming and interconnection between PMNs
If super-wideband or full band voice interworking is offered then the EVS codec must be supported
In case of interworking with fixed networks, NNI should support in addition the G.711 for narrowband voice interworking, G.722 for wideband voice interworking, and G.719 for super-wideband and full band voice interworking. For super-wideband and full band voice interworking if G.719 is not supported, AAC-LD should be supported

B.2.2 User Plane Transport

The following Table B.3 represents the HDVC related modifications compared to a corresponding table (7.2.1) in 3GPP TS 29.165.

The user plane transport of the II-NNI can use the protocols listed in Table B.3. The used protocols to transport media are negotiated by means of SDP offer/answer.

Item	RFC	Title	Support
5	RFC 4585	Extended RTP Profile for Real-time Transport Control Protocol (RTCP) - Based Feedback (RTP/AVPF)	Mandatory (in place of Optional)
6	RFC 793	Transmission Control Protocol	Mandatory in case BFCP is used. N/A if not (in place of Optional)

Table B.3: Supported transport-level RFCs to be described in SIP/SDP messages (changes for HDVC)

B.3 Summary of SIP Header Fields

The following Table B.4 represent the HDVC related modifications compared to a corresponding table (A.1) in 3GPP TS 29.165 (Annex A).

Item	Header field	Ref.	II-NNI
55a	Refer-Sub	[5]	m in the case the REFER request is supported, else n/a See Note
55b	Refer-To	[5]	m in the case the REFER request is supported, else n/a See Note
57	Replaces	[5]	m (in place of o)

Item	Header field	Ref.	II-NNI
66a	SIP-ETag	[5]	n/a (in place of:" m in the case the PUBLISH request is supported, else n/a")
66b	SIP-If-Match	[5]	n/a (in place of: "m in the case the PUBLISH request is supported, else n/a")

Table B.4: Supported header fields (changes for HDVC)

Note: The REFER method is used in HDVC for multipoint (adding a new participant). The detailed usage for is described in Clause 12.19 of TS 29.165.

Annex C IPX Proxy Requirements

C.1 Introduction

When implementing an IPX network, a number of functional requirements are placed upon an IPX Provider to support the correct operation of the IPX as a whole. As part of the commercial and technical agreement with a Service Provider, an IPX Provider may also be able to provide additional functions related to the operation of IMS interconnection and roaming, such as protocol interworking and transcoding.

In this Annex, it is intended to identify requirements on the IPX Proxy for IMS interconnection and roaming and classify them in to one of two groups:

- **IPX Provider Requirements** (identified as '**RI**' in the requirements Sections below), which are those that IPX Providers are required to support for the correct operation of IMS interconnection and/or roaming.
- **Operational Requirements** (identified as '**RO**' in the requirements Sections below), which are those that may be implemented for specific applications and relate to the support of specific Service Providers.

C.1.1 General

IPX Proxy Operational Requirements applies to Bilateral and Multilateral interconnect models.

C.1.2 IPX Provider Requirements

The set of IPX Provider Requirements in this Section provide functions for the overall support of the IPX. All IPX Provider Requirements shall be supported by all IPX Providers.

RI1. IPX Proxy shall be able to add, modify or remove fields/headers in the SIP/SDP protocol. All additions, modifications or removals shall be agreed with the directly connected Service Providers (SP) and IPX providers who are affected. No modifications to standard interworking/interconnection interfaces need to be done because of IPX Proxy.

RI2. IPX Proxy shall be able to handle inter-Service Provider traffic in a secured and controlled manner. More detailed requirements for the IPX Provider to achieve this are provided in IR.77 [19].

RI3. IPX Proxy shall support the IMS NNI interfaces described in this document and in IR.95 [50].

RI4. It shall be possible to have an IPX Proxy-to-IPX Proxy connection.

RI6. The Control Plane shall always be routed via the IPX Proxy.

RI7. The User Plane may be routed via the IPX Proxy. Routing of the User Plane via the IPX Proxy shall be for the support of Operational Requirements (for example, Transcoder insertion) as defined in Section C.1.3 below.

RI9. IPX Proxy shall verify that the source address of packets received from the Service Providers directly connected to it are associated with and registered to those Service Providers.

RI10. IPX Proxy shall have knowledge of the SIP specific capabilities of the Service Provider that it is serving for a specific session, and ensure media is appropriately handled for that session.

RI11. IPX Proxy shall be able to be used by a Service Provider as the point of connectivity for multiple destination Service Providers, without the need for the Service Provider to modify traffic based on destination Service Provider capabilities and connection options.

RI12. IPX Proxy should be able to verify that the next application level hop is reachable.

RI13. IPX Proxy shall have dedicated interface(s) towards an external management system for O&M purposes.

RI14. IPX Proxy shall have reporting capabilities, regarding IPX Proxy performance, and shall be able to provide reports to the Network Management system.

RI15. IPX Proxy shall support the requirements for availability of services as specified in AA.80 [22] service schedules.

RI16. IPX Proxy shall be able to support single-ended loopback testing, in order to enable a Service Provider to test the IPX Proxy without involving another Service Provider.

RI17. IPX Proxy shall support QoS functions as described in IR.34 of this document.

RI18. IPX Proxy shall be able to support legal interception requirements, in compliance with national laws as well as international rules and obligations.

RI19. IPX Proxy shall be able to support secure interface(s) towards the billing system.

RI20. IPX Proxy shall support SIP error codes as specified by IETF and 3GPP.

RI21. IPX Proxy shall forward unknown SIP methods, headers, and parameters towards the recipient without modification. This is to allow support of new SIP extensions. However, IPX Proxy should log and report when such unknown elements are detected, in case it is used for malicious purposes.

RI22. Addresses used in the underlying IPX network layer for IPX Proxy shall comply with requirements in GSMA IR.40 [27] and GSMA IR.77 [19]. Such addresses include those for tunnel endpoints.

RI25. IPX Proxy shall not modify IPv6-based IP addresses in the user plane (if no IPv4 related conversion is needed).

RI26. IPX Proxy shall accept traffic originated in Service Providers and other IPX Proxies, and terminated in servers (server-to-server traffic) either within a tunnel or un-tunnelled.

RI27. IPX Proxy shall accept traffic originated in Service Providers and other IPX Proxies, and terminated in end users (user-to-user traffic), traffic originated from end users and

terminated into servers and vice versa (user-to-server and server-to-user traffic) only if it is transported within a tunnel.

RI28. IPX Proxy shall not adversely affect QoS key Performance Indicator (KPI) parameters to end-to-end connections compared to when there is no IPX Proxy.

RI29. IPX Proxy shall be able to relay the Type of Service (ToS) field of the IP header from source to destination unmodified. If the IPX Proxy inserts an Interworking function that requires the ToS field of the IP header to be modified, then the IPX Proxy shall modify the ToS field accordingly.

RI30. IPX Proxy shall block user plane traffic not related to on-going control plane sessions.

RI31. IPX Proxy shall be able to apply session admission control based on session capacity and rate, on a per Service Provider basis. IPX Proxy shall generate alarms when the capacity or rate limit for a specific Service Provider is exceeded.

> Note: The black/white lists are provided by the Service Provider to the IPX Provider. How this is done is out of scope of the current PRD.

RI34. IPX Proxy shall be able to generate Inter-Service Provider charging data based on the GSM Association charging principles defined in GSMA IN.27.

RI35. IPX Proxy shall be able to produce Inter-Service Provider charging data based on events detected in the User Plane and Control Plane.

RI36. IPX Proxy shall be able to produce application specific charging data reflecting the occurrence of Chargeable Events identified in Service Schedules for that application.

RI37. IPX Proxy shall support required CDR formats to report Chargeable events to external billing systems.

C.1.3 Operational Requirements

The set of Operational Requirements described in this Section provides functions that could be hosted either by the Service Provider within their own network implementation, or could be effectively ‘outsourced’ to the IPX Provider, for the IPX Provider to operate on behalf of the Service Provider. The decision on whether these functions are kept within the Service Provider's network or if operated on their behalf by the IPX Provider will be taken bilaterally and on a service by service basis between an individual Service Provider and their IPX Provider,

Where such requirements and functions are operated by the IPX Provider, the IPX Provider shall implement these functions in a way that is ‘transparent’ to other Service Providers. In this case, transparent implies that a Service Provider B that is connecting to Service Provider A must be unaware above IP Layer, of whether the functions described in this Section are implemented within Service Provider A’s network or within their IPX Provider’s network, as identified by requirements defined in GSMA IR.40 [27] and GSMA IR.77 [19].

All requirements described in the remainder of this Section shall maintain this concept of transparency in their implementation.

RO1. IPX Proxy shall have DNS and ENUM resolver capability.

RO2. IPX Proxy shall be able to provide transcoding, when needed.

RO3. IPX Providers can offer support of interworking functionality between different control plane protocols to Service Providers. If Service Providers require the support of this functionality, it shall be provided transparently as an IPX Proxy function.

RO4. IPX Providers can offer support of interworking functionality between different user plane protocols to Service Providers. If Service Providers require the support of this functionality, it shall be provided transparently as an IPX Proxy function.

RO5. IPX Proxy shall be able to support 3GPP standards compliant interfaces relevant to interconnect functions for IMS-based services connectivity

RO7. IPX Proxy shall be able to store routing information, regarding the IP address/port pair used for a particular media stream between two Service Providers. This information is required to allow the IPX Proxy to open and close pinholes for the media streams associated with a signaling exchange.

RO8. IPX Proxy shall support all transport protocols required for the services to be interconnected using that IPX Proxy.

RO10. IPX Proxy shall support opening pinholes for user plane traffic traversal based on control plane protocol information.

RO11. IPX Proxy shall support closing pinholes used by user plane traffic based on control plane protocol information.

RO12. IPX Proxy may support the ability to provide maximum admission control limits on a per domain basis.

RO13. IPX Proxy shall be able to apply policy-based functionality on a per application and service provider basis.

RO14. IPX Proxy shall be able to support user plane policing based on the data rate.

Annex D SRVCC Performance with S8HR & CS NNI

Performance testing of SRVCC in the S8HR based roaming scenario with CS NNI has indicated the following values for the audio interruption time:

0.135sec for a distance of ~1400km
0.465sec to 3sec for a distance >8000km

Annex E Document Management

E.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.0.1	August 5th, 2003	Input paper IREG Doc 104/03 "IMS Roaming & Interworking Guidelines Proposal" for IREG Portland meeting	IREG	Tero Jalkanen / TeliaSonera
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 7th, 2005	Incorporated Minor CRs 003 and 004		
3.4	February 7th, 2006	Incorporated Minor CR 005		
3.5	August 14th, 2006	Incorporated Minor CR 006		
3.6	November 21st, 2006	Incorporated Minor CRs 007 and 008		
4.0	July 21st, 2010	Incorporated Major CRs 015 (Updates to Chapters 2-11) and 016 (IMS Telephony NNI)		
5.0	December 22nd, 2010	Incorporated Major CR 017 (Roaming Architecture for IMS)	IREG # 59 EMC # 86	Tero Jalkanen / TeliaSonera
6.0	01 August 2011	Submitted to DAG and EMC final approval date 30 Aug 2011 (Major CR 018 SIGCOMP alignment)	EMC	Tero Jalkanen / TeliaSonera
7.0	December 28th, 2011	Incorporated MCR 019 (IMS roaming details: Use of URIs)	EMC	Tero Jalkanen / TeliaSonera

		and mCR020 (IMS roaming figure)		
8.0	May 9th, 2012	Incorporated MCR 021 (RAVEL)	IREG#62 EMC	Tero Jalkanen / TeliaSonera
9.0	June 28th, 2012	Incorporated MCR 022 (Inclusion of VoHSPA)	PSMC	Tero Jalkanen / TeliaSonera
10.0	July 31st, 2012	Incorporated MCR 024 (RCS 5.0 support)	PSMC	Tero Jalkanen / TeliaSonera
11.0	November 9th, 2012	Incorporated MCR 023 (Correction of Target Voice Roaming Architecture Figure), MCR 025 Clarifying P-Visited Network ID format), MCR 026 (Analysis in the TAS for RAVEL)	PSMC	Tero Jalkanen / TeliaSonera
12.0	February 15th, 2013	Incorporated CR1001 (OMR supporting on Inter-Service Provider IP Backbone), CR1002 (Clarification of NAT-NAPT deployment and Keep-alive messaging), CR1003 (Correcting user addressing description) & CR1004 (Integration of HDVCNNI)	PSMC	Tero Jalkanen / TeliaSonera
13.0	April 4th 22nd, 2014	Incorporated CR1006 (URI Formats at the NNI), CR1008 (Use of the SIP route header for IMS Voice Roaming) & CR1009 (Route Headers and Node URIs)	PSMC	Tero Jalkanen / TeliaSonera
14.0	April 28th, 2014	Incorporated CR T7 (P-CSCF Identier Coding), CR1005 (Details from IPv6 Transition Whitepaper) & CR CR1007 (Roaming Guidelines for RCS when using IMS APN)	PSMC	Tero Jalkanen / TeliaSonera
15.0	October 28th, 2014	Incorporated CR1011 (Updates for Service Identification)	PSMC	Tero Jalkanen / TeliaSonera
16.0	April 1st, 2015	Incorporated CR1010 (Alignment with IPX R3) and CR1012 (SMSoIP when roaming)	PSMC	Tero Jalkanen / TeliaSonera
17.0	November 11th, 2015	Incorporated CRs 1013 (VoLTE Roaming Guidelines), 1014 (LBO HR and LBO VR), 1015 (Changes for VoLTE S8HR Roaming) and 1016 (Geo-local Number Handling Clarification)	PSMC	Tero Jalkanen / TeliaSonera
18.0	January 4th, 2016	Incorporated CRs 1017 (Need for confidentiality protection de-	PSMC	Tero Jalkanen / TeliaSonera

		activation with S8HR) and 1018 (Emergency calls in S8HR)		
19.0	March 30th, 2016	Incorporated CRs 1020 (Gate control and traffic policing), 1021 (Gy and S9 roaming interface clarification), 1022 (Support for Home-Local and Geo-Local Number Translation by TAS only), 1023 (Support for EVS codec) and 1024 (Editorial update)	PSMC	Tero Jalkanen / TeliaSonera
19.1	1st June, 2016	Incorporated CR 1019 (Removal of any reference to SE.35)	PSMC	Tero Jalkanen / Telia Company
20.0	2nd June, 2016	Incorporated CR 1025 (Disabling SIP Preconditions)	PSMC	Tero Jalkanen / Telia Company
21.0	19th September, 2016	Incorporated CRs 1027 (IMS NNI in case of multiple IMS core network deployments) and 1028 (Modified VoLTE interworking routing description)	PSMC	Tero Jalkanen / Telia Company
22.0	11th October, 2016	Incorporated CR 1030 (Updates for alignment, clarification and correction)	PSMC	Tero Jalkanen / Telia Company
23.0	19th December, 2016	Incorporated CRs 1029 (SDP offer and answer) and 1031 (Interconnection and Interworking terminology)	PSMC	Tero Jalkanen / Telia Company
24.0	6th March, 2017	Incorporated CRs 1032 (S8HR Alignment with 3GPP Release 14 additional changes) and 1033 (Updates for alignment and addition of multiple voice NNIs figure for better understanding)	PSMC	Tero Jalkanen / Telia Company
25.0	8th May, 2017	Incorporated CR 1034 (Alignment with 3GPP Release 14)	PSMC	Tero Jalkanen / Telia Company
26.0	2nd June, 2017	Incorporated CRs 1035 (Geo-Local Number Limitations) and 1036 (ENUM Reference Correction)	PSMC	Tero Jalkanen / Telia Company
27.0	10th August, 2017	Incorporated CRs 1037 (PAS Header in Terminating Roaming NNI) and 1038 (IMS Interworking Description)	TG (formerly PSMC)	Tero Jalkanen / Telia Company

28.0	2nd May, 2018	Incorporated CRs 1039 (S8HR Lawful Intercept Alignment with 3GPP Release 14), 1040 (SRVCC options with SIP-I and CS NNI for the S8HR architecture) and 1041 (Support of Emergency Calls with S8HR architecture)	TG	Tero Jalkanen / Telia Company
29.0	20th November, 2018	Inclusion of CR.1043 Change of IMS roaming recommendation regarding LBO and CR 1042 RCS changes	TG	Tero Jalkanen / Telia Company
30.0	8th April, 2019	Inclusion of CR 1044 Support of originated user identity in terminating requests and CR 1045 Clarification of 'Open' Codec	TG	Tero Jalkanen / Telia Company
31.0	9th April, 2020	Inclusion of CR 1046 Alignment with 3GPP for Support fo SRVCC in S8HR	TG	Tero Jalkanen / Telia Company
32.0	13th October, 2020	Inclusion of CR 1048 Recommendation to support Home Routing for IMS Services and CR 1049 Update for support of IMS Roaming for 5GS	TG	Tero Jalkanen / Telia Company

Other Information

Type	Description
Document Owner	NG
Editor / Company	Tero Jalkanen / Telia Company

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.