IMS Roaming and Interworking Guidelines

Version 18.0

08 January 2016

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

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 signalling between the terminal and the IMS as well as between the components within the IMS. SIP is used to establish and tear down multimedia sessions in the IMS. SIP is 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 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 and interworking are seen as major issues. This document aims to increase the IMS interworking & roaming related knowledge level of operators, and to prevent non-interoperable and/or inefficient IMS services and networks. These aims concern especially roaming and interworking cases, because these issues could potentially hinder the deployment of IMS if not handled properly.

Please note that the document does not aim to give an elementary level introduction to IMS, even though Chapter three (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 and interworking, therefore higher level issues like service interconnection are not discussed in detail; see for example GSMA PRD SE.35 [12] for service related documentation. 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 and interworking are out of scope; these are managed by BARG (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 Abbreviations

Term	Description
APN	Access Point Name
AS	Application Server
BGCF	Breakout Gateway Control Function
CDR	Charging Data Record
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
GRX	GPRS Roaming eXchange.
GSM	Global System for Mobile telecommunications
HDVC	High Definition Video Conference
H-PCRF	Home Network- Policy and Charging Rules Function
HPLMN/HPMN	Home Public (Land) Mobile Network
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
ICSI	IMS Communication Service Identifier
IBCF	Interconnection Border Control Function
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
LTE	Long Term Evolution (of RAN)
MGCF	Media Gateway Control Function

Term	Description
MGW	Media Gateway
MRF	Multimedia Resource Function
NAPTR	Naming Authority Pointer DNS Resource Record
NAT	Network Address Translation
NAT–PT	Network Address Translation – Protocol Translation
OAM	Operation, Administration and Maintenance
OMR	Optimal Media Routing
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
SMTP	Simple Mail Transfer Protocol
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
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UTRAN	UMTS Terrestrial Radio Access Network
VoHSPA	Voice over HSPA

Term	Description
VoIMS	Voice & video over IMS (includes IR.58, IR.92 and IR.94)
VoLTE	Voice over LTE
V-PCRF	Visited Network- Policy and Charging Rules Function
VPLMN/VPMN	Visited Public (Land) Mobile Network

1.4 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	UMTS Release 5 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]	GSMA PRD SE.35	IMS Services and Applications
[13]	GSMA PRD SE.36	PoC Roaming and Inter-working Service Requirements
[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/ENUM 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]	GSMA PRD IR.58	IMS Profile for Voice over HSPA
[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

2 Roaming Guidelines

2.1 Introduction

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

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 service provider network. 3GPP architecture specification defines 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 Service Provider's network and the Visited Service Provider's Proxy-Call Session Control Function (P-CSCF) is used to connect the UE to the home IMS.

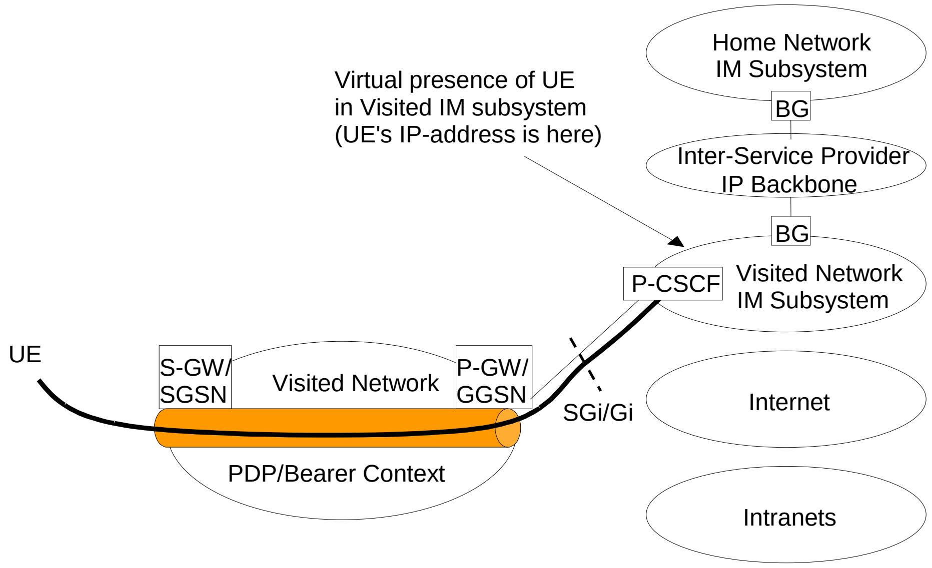

Figure 2-1: UE Accessing IM Subsystem Services with P-GW/GGSN in the Visited network via Visited Network IM subsystem

Figure 2-2 depicts a model where the UE has obtained IP connectivity from the Visited Service Provider's network and the Home Service Provider provides the IMS functionality.

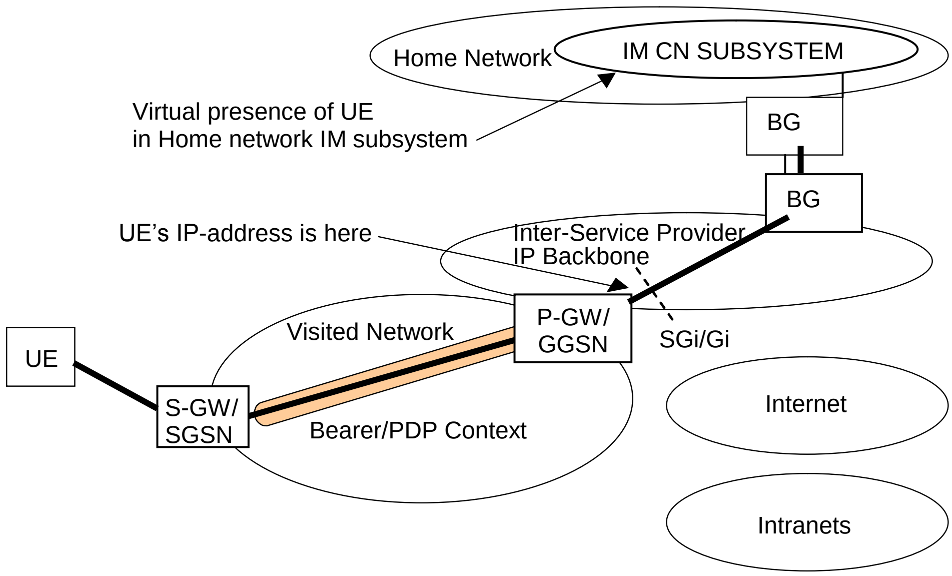

Figure 2-2: Accessing IM Subsystem Services with P-GW/GGSN in the Visited network

Figure 2-3 depicts a model where the UE has obtained IP connectivity from the Home Service Provider's network and the Home Service Provider provides the IMS functionality.

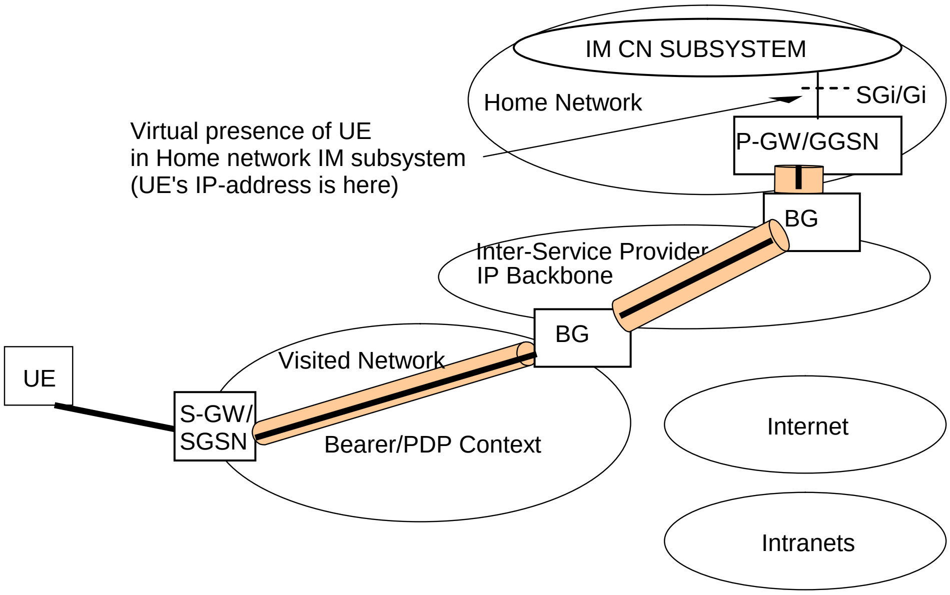

Figure 2-3: UE Accessing IM CN subsystem Services with P-GW/GGSN in the Home network

Figures 2-2 and 2-3 show configuration options that do not require IMS interworking between the Visited and Home IMS networks as the Visited Service Provider's IMS is not used. When roaming is provided utilizing architecture shown in the Figure 2-1 the service providers need to deploy IMS interworking between the Visited and Home IMS Networks as defined in Chapter 3.

2.3 Operational Requirements for IMS Voice and Conversational Services based on Local Breakout and P-CSCF in VPLMN

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.58 [35], IR.92 [28] and IR.94 [36]) when call originator is Roaming should be at least as optimal as that of current 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.

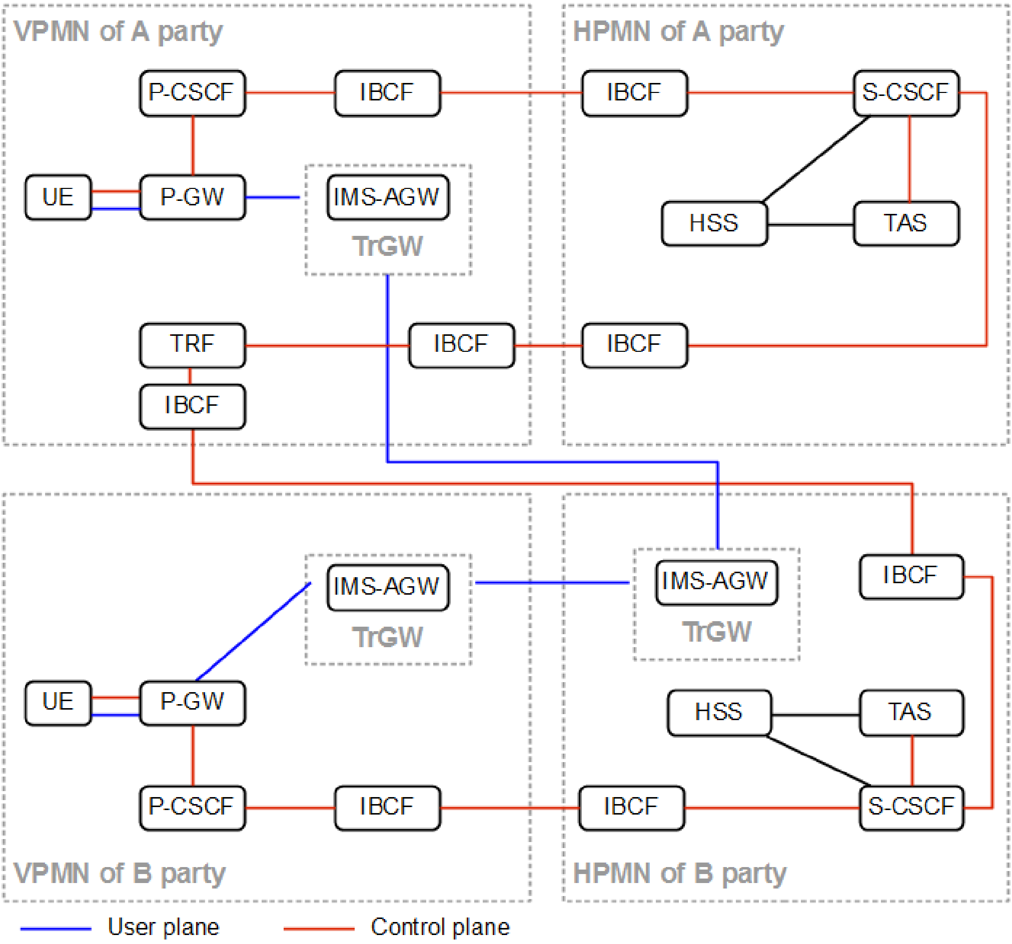

Figure 2-4: Control and User Plane Routing – LBO-VR

Note: Although illustrated as a stand-alone element in the diagram above, the TRF has been defined as a functional element rather than a new network node.
Note: The figure does not depict the interface between UE and the network (Ut reference point).

The second requirement is met by the deployment of P-CSCF (Proxy-Call Session Control Function) functionality in the VPMN and use of Transit and Roaming Function (TRF) which receives the originated call related signalling after it has been processed by the A party HPMN (VPMN Routing). This allows the A party VPMN to send both control and user plane towards the destination and therefore replicate the current CS voice roaming model. By applying Optimal Media Routing (OMR) along the signalling loop from VPMN A to HPMN A and back to VPMN A the media path of originated calls is optimized and not routed to HPMN A. 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) in Figure 2-5 where the media path of originated calls is not optimized and is routed through HPMN A (Home Routing).

The above use of LBO-VR requires to apply OMR along the signalling from VPMN A to HPMN A, and then the HPMN A can decide, e.g. based on the destination:

- To send the signalling back to the VPMN – and then, as described above, OMR is applied from HPMN A to VPMN A as well (Figure 2-4) or
- To bring media to the HPMN A and send both the control and user plane from the HPMN A to the destination – in this case OMR is terminated in HPMN A

The routing decision is performed by the HPMN A in the S-CSCF (or the BGCF).

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

Terminated calls are routed from HPMN to VPMN in the same way in both LBO-HR and LBO-VR architecture.

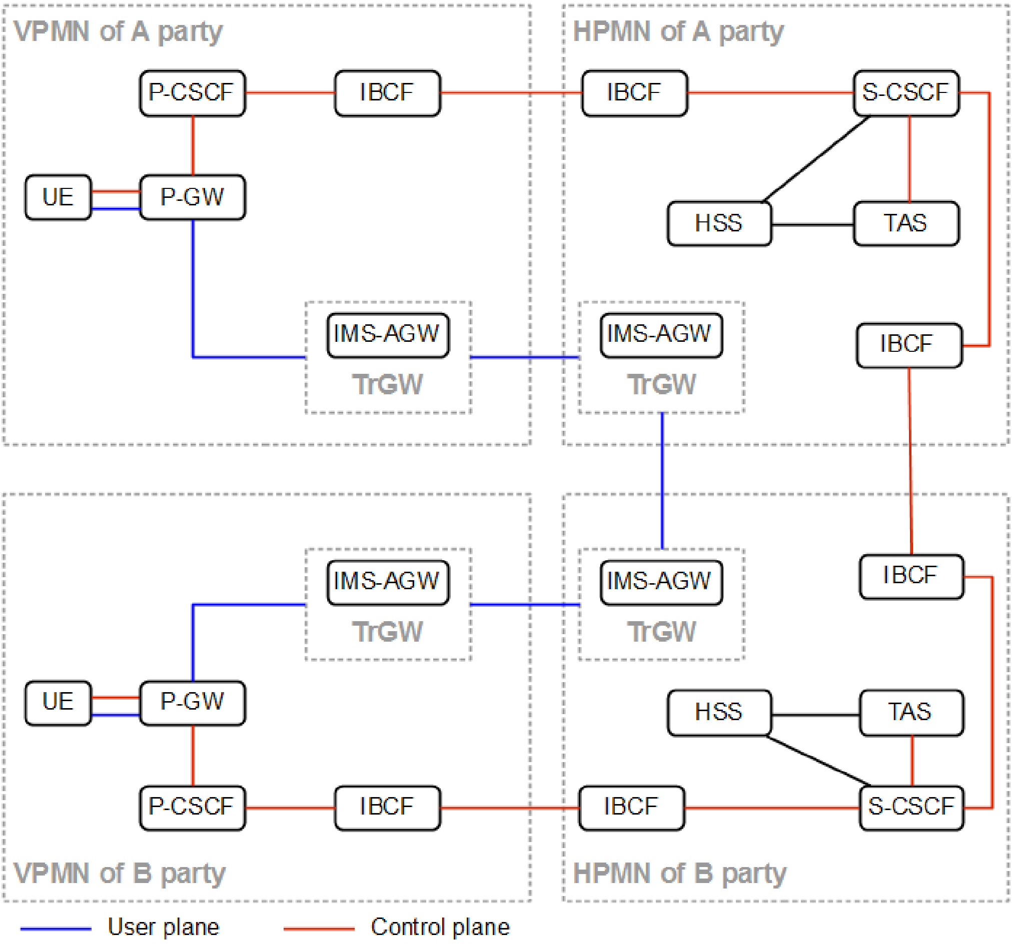

Figure 2-5: Control and User Plane Routing – LBO-HR

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 / video calls based on IR.92, IR.58 and IR.94 can be routed as depicted in Figure 2-4. Even in this case, the user plane of RCS services other than IR.92, IR.58 and IR.94 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 signalling requests will be routed from P-CSCF to S-CSCF which invokes an IP-SM-GW to interwork the SIP signalling to legacy SMS system if needed; see 3GPP TS 23.204 [X] for further details. For the terminating case the legacy SMS signalling is interworked to SIP signaling, if needed, by an IP-SM-GWof the B-Party's HPMN, and the needed stand-alone SIP signalling request is sent from the IP-SM-GW to the B-Party S-CSCF which routes the SIP signalling via the P-CSCF in the VPMN to the B-Party UE.

2.4 VoLTE Roaming Architecture

2.4.1 General

There are three VoLTE 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 VoLTE roaming architecture alternatives in more detail.

2.4.2 VoLTE Roaming Architecture using LBO

The target IMS Voice Roaming Architecture is shown below in Figure 2-6 for EPC (see also IR.88 [26]) and in Figure 2-7 for GPRS (see also IR.33 [34]). For IMS Voice Roaming, the S9 interface between V-PCRF and H-PCRF is optional (see also IR.88 [26]). For routing of media when roaming, see Section 2.3.

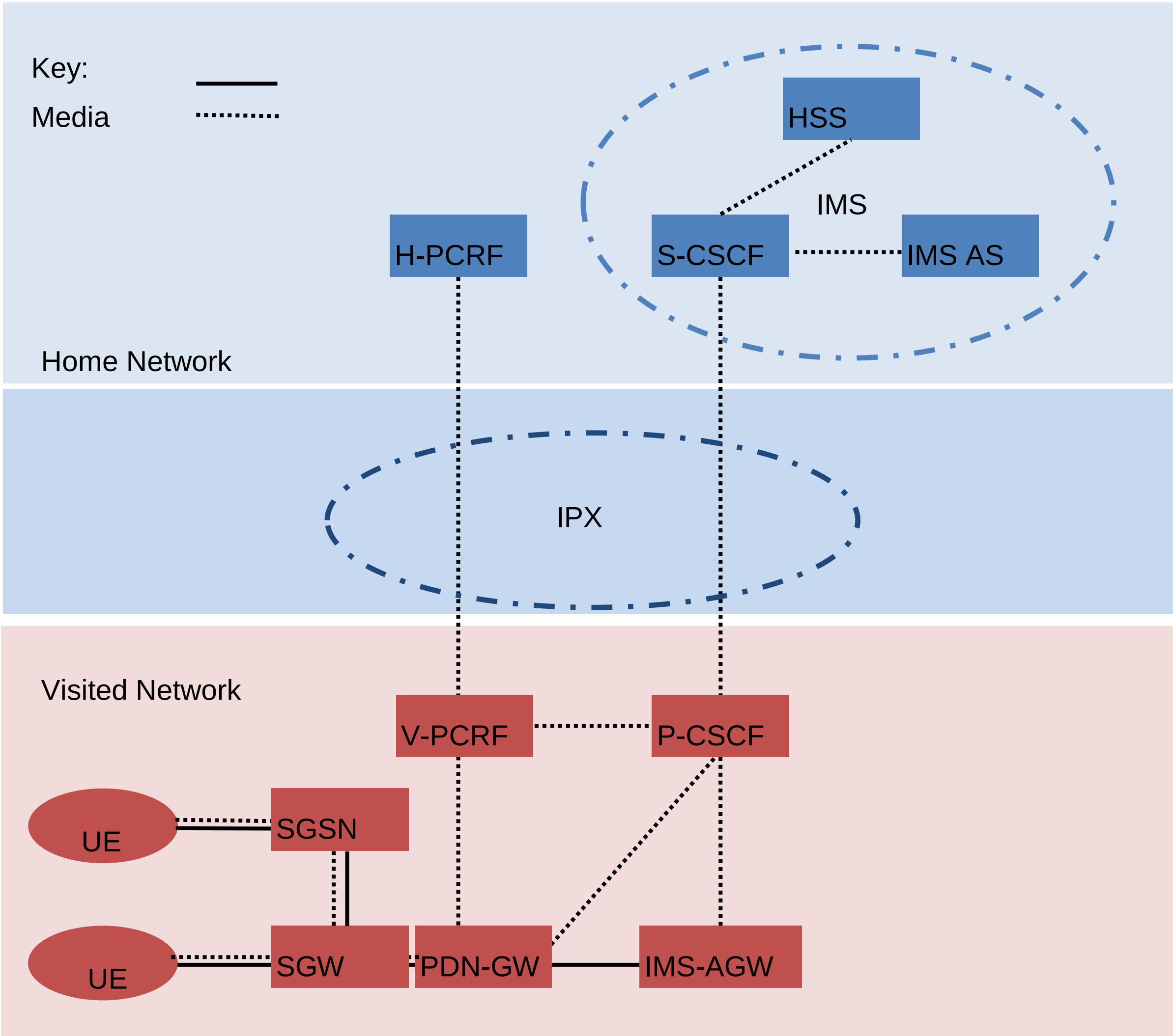

Figure 2-6: Target Voice Roaming Architecture – EPC

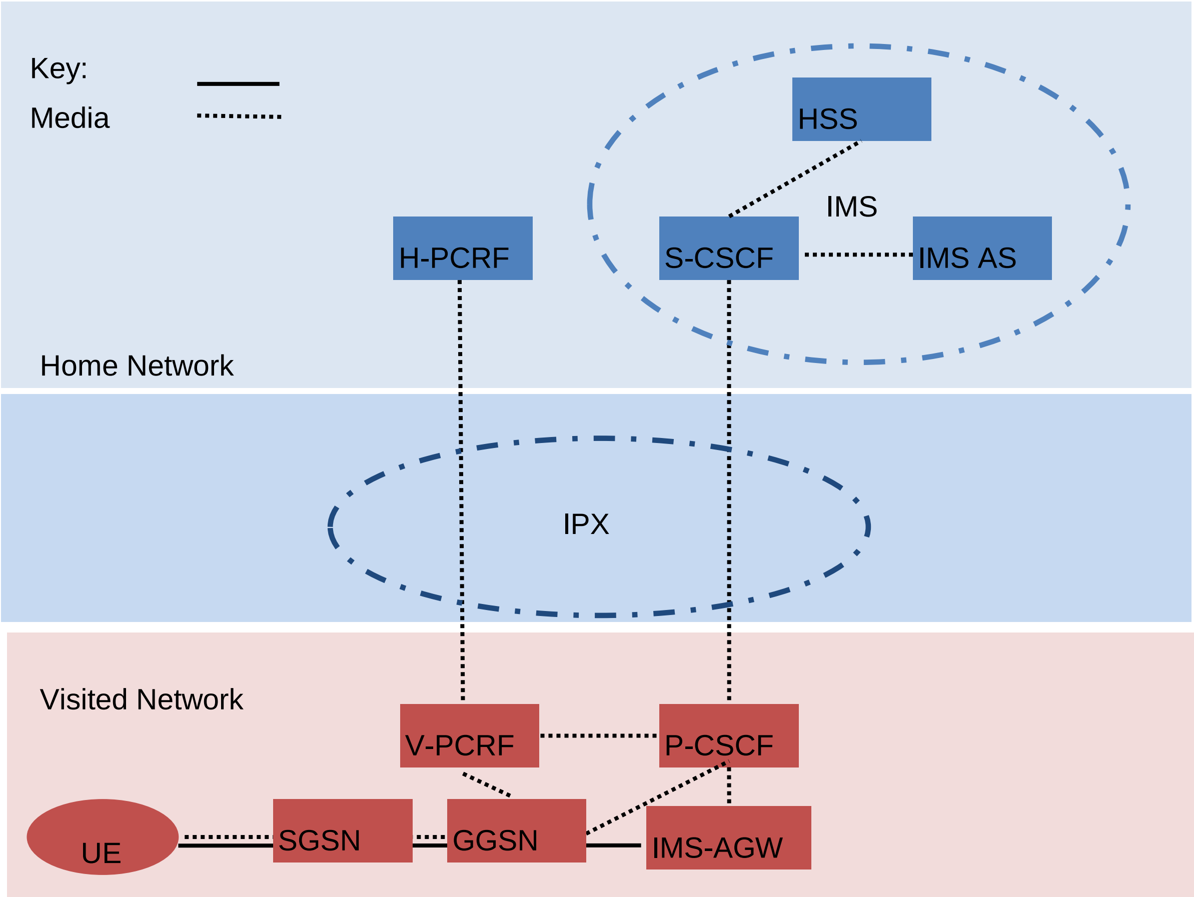

Figure 2-7: Target Voice Roaming Architecture - GPRS

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 session setup by P-CSCF to route 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 SIP route header to route originating stand-alone SIP signalling requests to the S-CSCF and similarily the S-CSCF adds the recorded P-CSCF URI as a SIP route header to route terminating stand-alone SIP signalling requests to the P-CSCF.

The IPX Provider/Carrier performs routing based exclusively upon the topmost SIP Route header that must contain the address of the destination network e.g., for the INVITE the home network of the calling party when in roaming or the visited network of the called party when in roaming.

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

2.4.3 VoLTE Roaming Architecture using S8HR

With S8HR VoLTE 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 (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 Voice is supported by both the VPLMN and the HPLMN.

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

The HPMN must ensure that IMS layer signalling 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 and IMS Roaming agreement type, this protection may have to be deactivated in the HPMN.

> Note: This behaviour that retrieves a subscriber's location is currently not supported by 3GPP (i.e. it is implementation specific) and may require additional network capabilities in order to retrieve a subscriber's location for all calls (both roaming and non-roaming cases).

This is currently under discussion in 3GPP TR 23.749 [42].

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

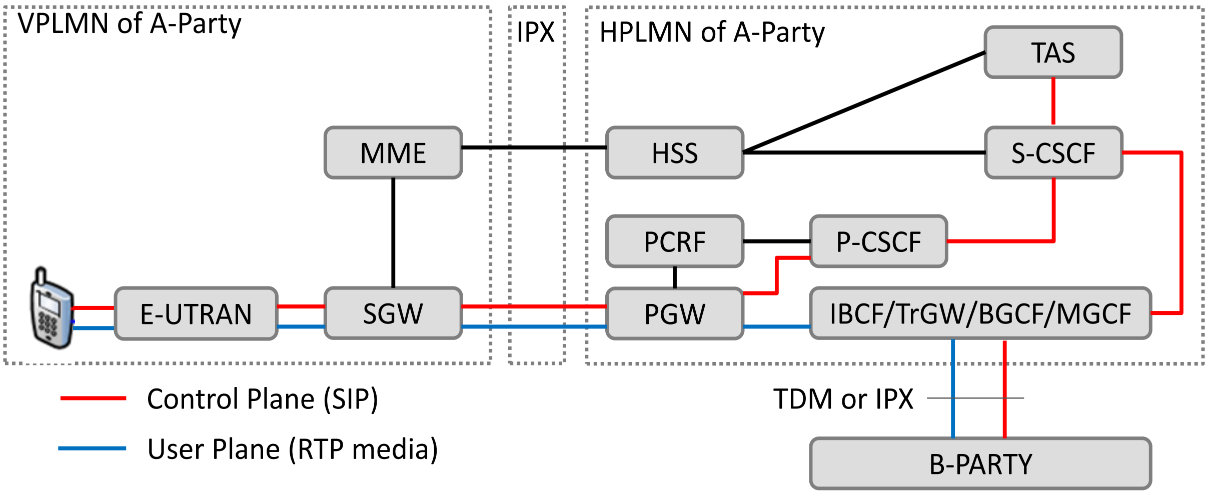

Figure 2-8: S8HR VoLTE Roaming Architecture

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

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

2.5 Transitional Architecture

Figure 2-4 depicts the LBO-VR voice roaming architecture and Figure 2-5 depicts the LBO-HR voice roaming architecture which both fully support IMS emergency calls, SR-VCC, operational requirements and efficiently managed QoS over the GRX/IPX.

Prior the VPLMN providing IMS voice support, it is possible to provide non voice IMS service utilising the 3GPP architecture shown in Figure 2-3. Once the target optimal roaming architecture as shown in Figure 2-6 is in place it must be used for all IMS services.

2.6 VoLTE Roaming Guidelines

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

S8HR for IMS voice roaming can be seen as an IMS Voice 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 IMS interconnection services for terminating calls between HPMNs) and it does not require inter-operator testing of operator terminals with P-CSCF. It is suitable for operators that wish to have VoLTE roaming services without, or before, deploying IMS interconnect services. However, operators also must accept the limitations (no service aware VPMN, no SRVCC support, no geo-local services in VPMN, no media path optimization possible for originated calls, no authenticated IMS emergency call, no decoded IMS Voice Call and SMS Lawful Interception or data retention in the VPMN) and new functionalities (e.g. QoS bearer charging, see GSMA PRD BA.27 [17], and network protection mechanisms) based on their local regulatory requirements. In addition, it requires the IPX providers that are connecting to those operators to support QoS bearer charging.

LBO-HR for IMS roaming requires an IMS interconnect for roaming flows and inter-operator testing of 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 possible 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 possible for originated calls. Media path optimization relies on OMR support by HPMN, VPMN and connecting 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, thereby fulfilling specific roaming needs.

Operators that have to support more than one IMS voice 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 voice roaming architecture.

2.7 Support of SIGCOMP

According to section 8.2 of 3GPP TS 24.229 [6], the P-CSCF is mandated to support SIGCOMP for all subscribers. However, deployments of SIGCOMP in UEs are particularly rare, as is also the support in current operator P-CSCF deployments. In addition, the use of higher-bandwidth networks, such as E-UTRAN, negates 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 telephone numbers given in local format, the TAS must determine whether

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

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

If the number is determined as home-local number, the TAS or S-CSCF must translate the local number to international format to route the call (see Section **Error! Reference source not found.**).

If the number is determined as geo-local number, and in case the signalling can be send back to the VPMN (see Section 2.3), the TAS or S-CSCF must either translate the local number to international format, or the number must be sent 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 local number is received at the TRF in the VPMN and the phone-context includes the “geo-local” string, the number can be treated as if the phone-context was set to the home domain name of the VPMN.

Note: See section 2.2.3 of 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 the number is determined as home-local number, the TAS or S-CSCF in HPLMN must translate the local number to international format (as specified in 3GPP TS23.228[5]).

If the number is determined as geo-local number, the TAS or S-CSCF must translate the numbers to international format to route the call, as specified in 3GPP TS23.228 [5]. When the HPMN translates the geo-local numbers to international format, the home network 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 VPLMN is using a special numbering plan, the HPLMN can be provisioned according to the roaming agreement between HPLMN and VPLMN (and updated if needed) with all local numbers or regional code mappings from the VPLMN(s) and these mappings depend on the UE location.

2.9 Support of Emergency Calls with S8HR architecture

When applying the S8HR VoLTE 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 1: Trying an “anonymous” Emergency Call when Emergency Registration fails is currently not mandatory for IR.92 UE and is FFS.

Note 2: 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.

For options when the UE is not able to use CS technology for Emergency Calls (e.g. VoLTE only UE, UE not supporting VPMN CS technology, lack of CS coverage), see Section 2.9.1 below.

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

2.9.1 Impact on the VPMN using IMS EC

If there is no roaming IMS-NNI between the HPMN and VPMN, the Emergency Registration of inbound roamers will fail.

Note 1: The functionality to avoid failure (e.g. ensuring the success of Emergency Registration or accepting “anonymous” Emergency calls) is under investigation at 3GPP TR 23.749 [43].

Note 2: Trying an “anonymous” Emergency Call when Emergency Registration fails is currently not mandatory for IR.92 UE and is FFS.

2.9.2 Impact on the HPMN for non UE detectable emergency calls

The HPMN should 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 should be able to distinguish non UE detectable emergency calls and treat those emergency calls according to the roaming agreement.

Note 1: Collection of location information at P-CSCF during registration procedure and handling of non UE detectable emergency sessions at P-CSCF are currently not described by 3GPP (i.e. it is implementation specific) and may require additional network capabilities in order to retrieve customer location for all calls (domestic and roaming). It is currently under discussion in 3GPP TR 23.749 [43].

Note 2: How HPMN collects and maintains all emergency numbers and how to recognize them for each roaming partner (potentially all regions in the world) is not described here and will be for future study.

3 Interworking Guidelines

3.1 Introduction

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

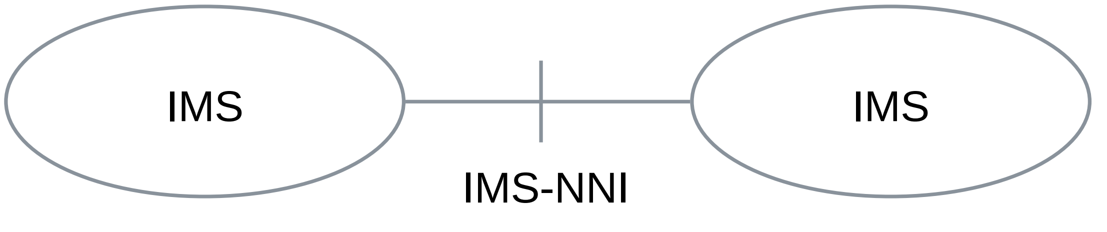

Figure 3-1: High-level view of the interworking model for IMS

There are two architectural variants of how the IMS-NNI can be deployed. These are depicted in Clause 3.2, where an Interconnection Border Control Function (IBCF) is used at the border of each Service Provider, and Clause 3.3, 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 IMS-NNI is independent of these architectural variants.

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]. Ici interface is used to transport SIP signalling, while Izi interface handles media traffic.

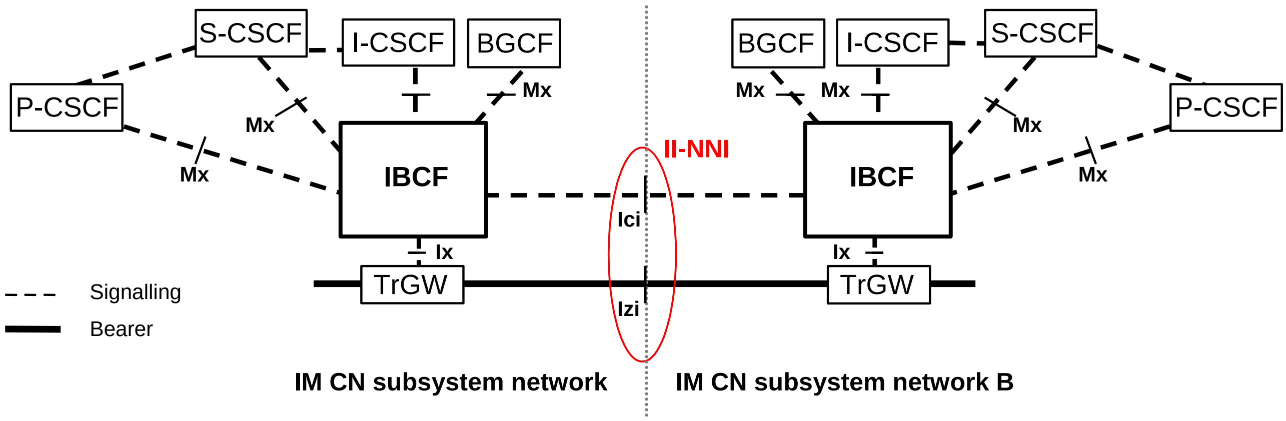

Figure 3-2: IMS interworking using Ici & Izi Interfaces (from 3GPP TS 23.228)

Figure 3-2 shows this model where IBCF (Interconnection Border Control Function) is a node handling control plane for the purpose of for example Topology Hiding Inter-network Gateway (THIG), Application Layer Gateway (ALG), screening of SIP signalling information and generation of Charging Data Records (CDRs). 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/Gi/Sgi Interfaces

Figure 3-3 presents IMS interworking between originated and terminated networks as specified in 3GPP's IMS NNI. SIP signalling is delivered via Mw interface and user plane is transported via Gi/Sgi 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 signalling always flows via IMS core networks.

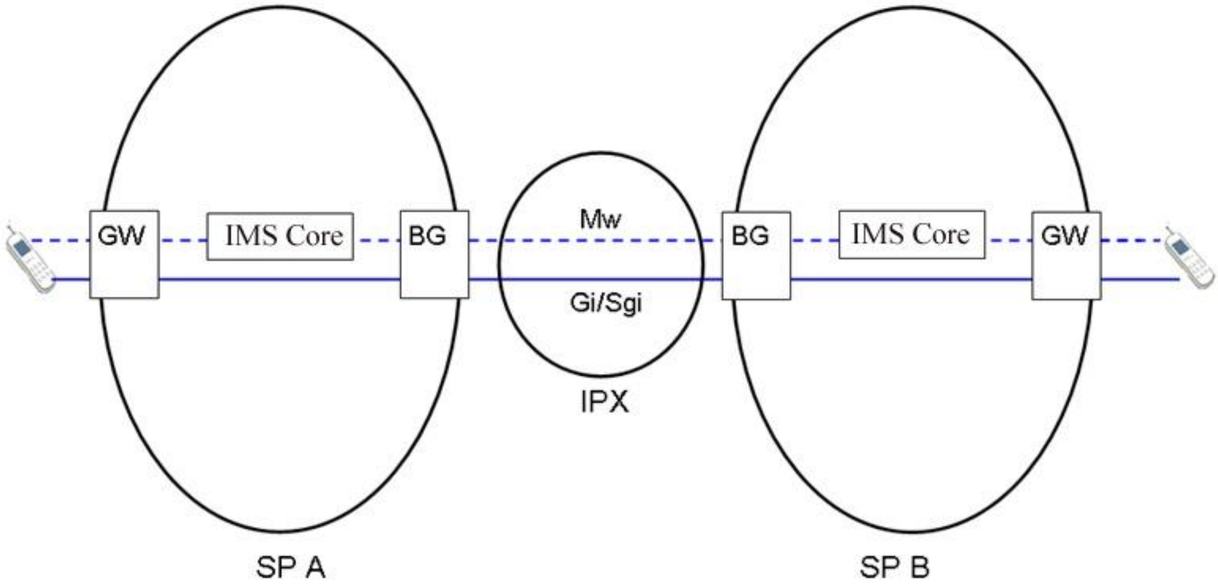

Figure 3-3: IMS interworking using Mw & Gi/Sgi Interfaces (simplified example not showing e.g. FW nodes)

Border Gateway (BG) shown in the figure above is a non-SIP aware element taking care of controlling incoming traffic from the Inter-Service Provider IP Backbone into the operator core system for example by performing filtering on IP layer. In addition to the BG there can be other nodes relevant for the IMS NNI, such as a SIP aware Firewall (FW) located between BG and Serving/ Interrogating (S/I)-CSCF. I-CSCF itself natively takes care of the being the point of contact to IMS.

3.4 Overview

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

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. For example, traffic filtering at the border of operator core network concerning PS roaming using GPRS Tunnelling Protocol (GTP) must be taken care by some other node, somehow.

Therefore, it should be noted that both the option of using Mw/Gi/Sgi interfaces as well as the option of using Ici/Izi interfaces are possible in IMS interworking. 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 interworking scenarios, further details are described in Chapter 6.

Interworking with Internet and corporate intranets is not deal with in detail, although Chapter 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 operator and non-IMS operator. 3GPP specification TS 29.163 [7] covers interfaces and signalling in these cases.

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].

From a technical perspective the required IP network between different operators might be for example public Internet (with Virtual Private Network (VPN)) or direct leased line such as Frame relay or Asynchronous Transfer Mode (ATM). Another solution, which in many cases could be considered to be the preferred choice, is to utilize an existing, proven and reliable Inter-Service Provider IP Backbone, in other words GPRS eXchange/IP eXchange (GRX/IPX), as specified in 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 Interworking (IW) 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 carriers) a leased line or IP-VPN may be more cost effective. As the IP routing is separate from the physical topology, multiple physical connections may co-exist. In practice, operators may have several physical interconnection links: leased line for national traffic, IP-VPN for medium volume or non-Service Provider and IPX for all others. The DNS system will resolve the destination domain to an IP address that will be routed over the appropriate link.

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

Consequently, the preferred Inter-Service Provider IP Backbone in the IMS case is IPX, as it is already the preferred network in the case of, for example, GPRS roaming, Multimedia Messaging Service (MMS) interworking and Wireless LAN (WLAN) Roaming

4.2 IP Addressing

As documented in 3GPP TS 29.165 [19], interworking 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 interworking routing. This separate intermediate Proxy functionality allows operator 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 interworking 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.

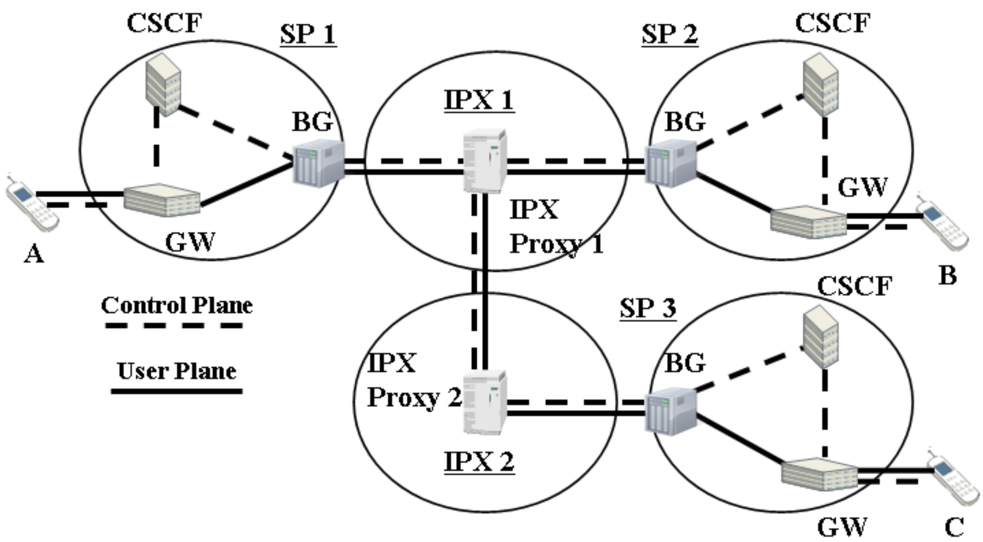

Figure 4-1: Overall Architecture of IMS Interworking using the Proxy Model

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 routed back to the HPLMN of roaming users as described in Section 2.3.

Service Related Guidelines

5.1 Introduction

5 Different end-user services used in IMS have different requirements. As IMS allows any kind of IP based service to be used, issues regarding those have to considered when assessing inter-Service Provider IMS connections. For example routing the Push to Talk over Cellular (PoC) user plane and control plane 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 and interworking environment should be built in a way that it supports multiple different types of IMS based service & applications. Thus, NNI cannot be become the limiting factor when Service Providers are launching new services, including also the deployment of connectivity between the Service Providers.

The actual IMS based services and their requirements are listed in other documents, see for example GSMA PRD SE.35 [12]. This document handles only the specific inter-Service Provider aspects of these different services. The following chapters illustrate the NNI details of some important IMS services.

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 session 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 Telephony

5.2.1 Overview

Generally speaking “IMS Telephony” means IP based basic communication utilizing IMS as the enabling platform which can be used for example to replace the CS based voice & video service with IMS based voice & video. Figure 5-1 below gives a high-level illustration of the architecture where two clients using IMS voice & video UNI are connected together via IMS voice & video NNI, transporting IP based voice & video end-to-end enabled by the IMS core systems of each Service Provider.

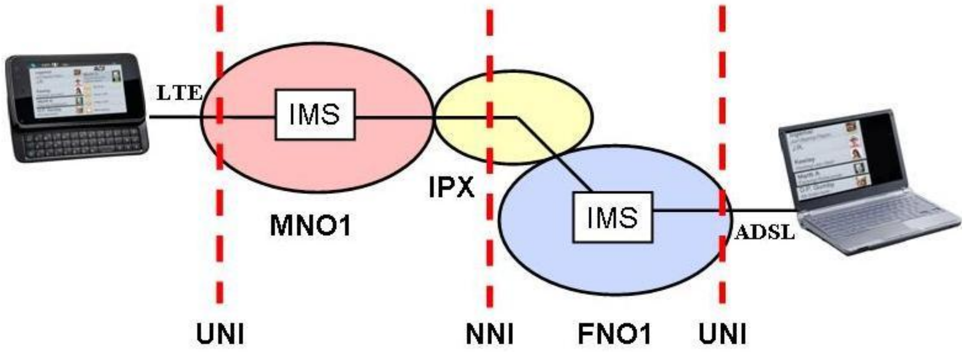

Figure 5-1: High-Level Example of IMS Telephony Connection

Technical solution for IMS Telephony NNI is the VoIMS service as specified in GSMA PRD IR.92 [28], IR.58 [35] and IR.94 [36], based on the IMS MMTel (Multimedia Telephony) standard defined by 3GPP. Generally, the technical details of VoIMS UNI are applicable also for the purpose of VoIMS NNI, for example, the Supplementary Services supported over the interworking interface follow the set defined in GSMA PRD IR.92 [28], IR.58 [35] and IR.94 [36].

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 voice interworking agreement and connection to use IP with Service Provider B, but still have the old TDM based voice interworking in place with Service Provider C. Therefore, Service Provider A must have a mechanism to deal with both PS and CS based voice interworking interfaces. In addition there may be more than one voice NNI option within the PS category, for example SIP and SIP-I.

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

1. The first preference is likely to be a direct IMS-to-IMS call because this requires no 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, also use the same IP based interface (see GSMA PRD IR.90 [27])
2. Fallback to MSC-S and MGW nodes, with the call originating from the IMS core system 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 to MSC, with the call originating from the IMS core system it is converted into a CS call and routed to the receiving Service Provider via CS based voice NNI. Normal ISUP Signalling and TDM mechanisms apply in this scenario (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 such as the requirements the originator needs to fulfill to its subscribers, IMS Telephony NNI knowledge, technical capabilities available to it 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 IMS Telephony NNI as described in Chapter 7.2.3
- The originator may also rely on the IPX provider services to determine if the destination is IMS capable or not.

IMS NNI knowledge can be obtained through look up services. GSMA recommends the use of Carrier ENUM for this purpose as defined in [IR.67]. Carrier ENUM provides information on a per international public telecommunications number basis and can indicate that routing via the IMS Telephony 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 PS/CS interworking. PS/CS interworking technical capabilities available to the originator may include:

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

If the originator does not have or is not willing to provide PS/CS interworking technical capabilities it can make agreements with different carriers to perform PS/CS interworking as depicted in the Figure 7-1.

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 an IMS Telephony NNI exists to that operator, the originating operator may still decide to route the call over the IMS Telephony NNI.

The capabilities that the originator arranges are influenced by cost. Investment in PS/CS conversion technology is normally a CAPEX decision, while agreements with others to perform conversions are OPEX decisions. Where the originator has access to more than one option for any particular call, again, cost may influence the mechanism or 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 to call on.

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

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

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

5.2.3 IMS Voice & Video NNI

In the case of full end-to-end IP based interworking for example between two Service Providers offering VoIMS based service to their customers, connected to each other via IP based NNI transporting SIP signalling and RTP media between IMS core systems including IMS Telephony AS, 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. For the avoidance of doubt, this does not exclude usage of other alternatives, such as a bilateral leased line, for IMS Telephony NNI purposes when seen fit by the participating Service Providers.

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

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

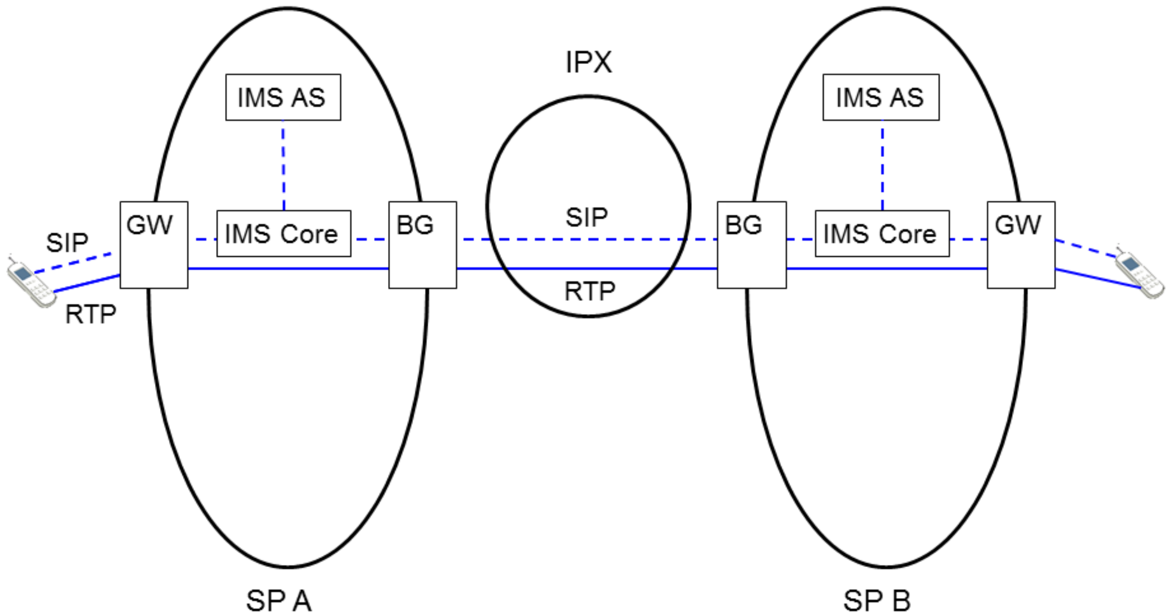

Figure 5-2: IMS-to-IMS Telephony NNI

Figure 5-2 above shows the native IMS Telephony NNI, using IPX in the bilateral Transport Only connectivity option.

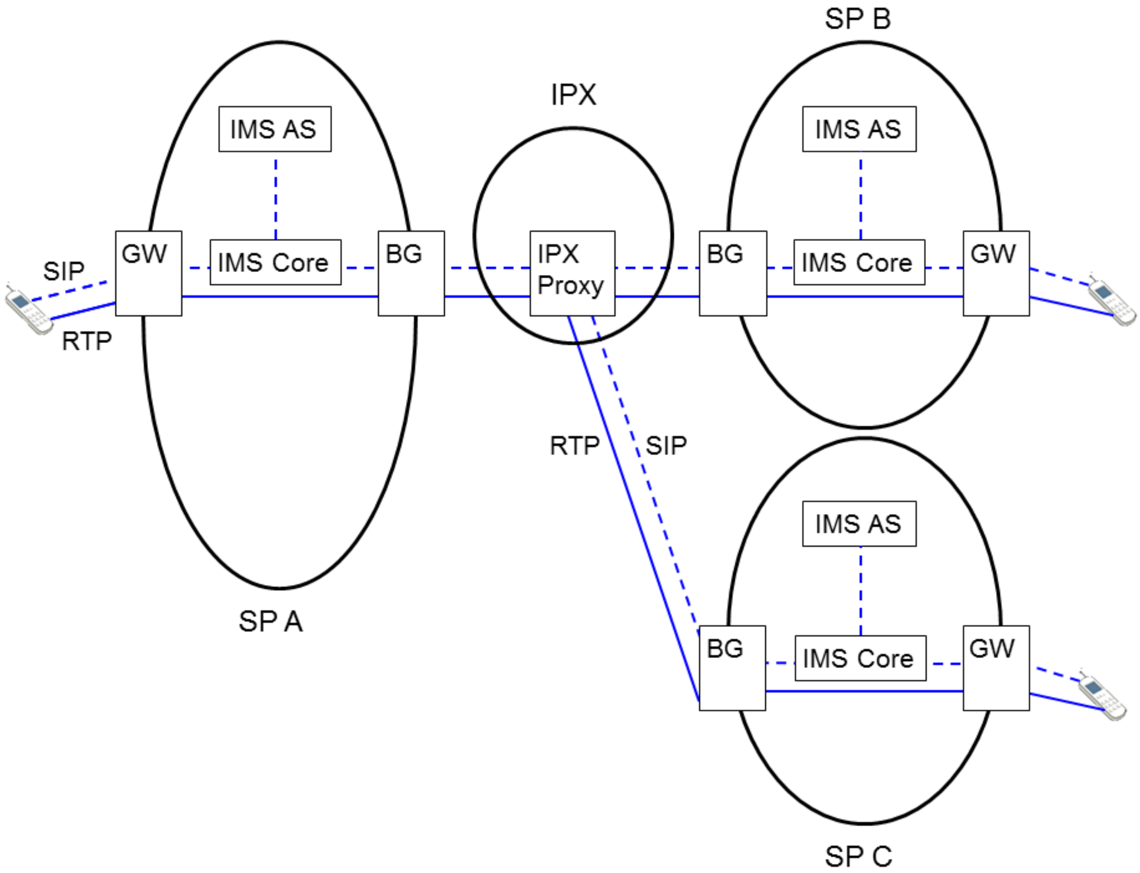

Figure 5-3: IMS-to-IMS Telephony NNI (Hubbing Model)

Figure 5-3 above shows the native IMS Telephony NNI, using IPX in the multilateral Service Hub connectivity option. IPX Proxy is used to forward SIP signalling and RTP media between Service Provider A and Service Providers B and C. Annex C provides further details of IPX Proxy.

5.2.4 PS/CS Interworking

When the native IMS voice NNI (as illustrated in the Chapter 5.2.3) cannot be used the originating IMS network may utilize 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 but further details are out of scope for the present document.

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 IR.67 [24]. Call breakout to CS occurs when the session cannot be routed further via the IMS Telephony NNI. CS breakout can be done either in the originating network, IPX or terminating network, depending on the agreement between Service Providers. In the CS breakout scenario, the BGCF selects the terminating network according to the defined rules. A session is forwarded either to local MGCF (via Mj interface) or to BGCF of terminating network (via Mk interface). MGCF routes call establishment towards terminating network and handles the needed protocol interworking between 3GPP SIP, BICC/SIP-I and ISUP for controlling. IMS-MGW handles the user plane transporting between IP (Mb interface) and PSTN interface.

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

Further information on PS/CS interworking (different scenarios including figures) can be found in Annex A.

5.2.5 General Issues

As documented in Chapter 3, there are two alternative models for IMS interworking. Both of them are valid also for the IMS Telephony NNI purposes. A Service Provider may independently deploy either option defined above mutually exclusive of what an interconnected Service Provider chooses to deploy. For example. Ici/Izi and Mw/Gi/Sgi can interoperate without Service Provider configuration or a dependency on an interworking function.

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

As illustrated in Chapter 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].

The addition of new media streams to an ongoing IMS telephony session (in other words the modification of the session through re-INVITE) is out of the current scope of this specification.

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.

5.3 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, routing of interworking traffic over the Inter-Service Provider interface is simpler than in services that lack this kind of interface. This is due to the fact a server can have an address that belongs to IPX address block (in other words is routable within IPX), while a terminal likely 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)) is routed via POC-4 interface between PoC servers, while control plane

(SIP signalling) is routed via IP-1 interface between IMS core networks. Both of these interfaces are IP based. It is envisioned that both POC-4 and IP-1 will be routed over the Inter-Service Provider IP Backbone, as any other IMS interworking 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 interworking 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 signalling always goes via the Service Provider IMS core.

When P2P service is used user plane is routed directly between terminals implying that terminal IP addresses are utilized in user plane. However, as discussed above typically terminal IP addresses are not routable in the Inter-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] Chapter 6.5.6.

Routing of P2P traffic between Service Providers is handled via using 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 kind of service, since IMS user is always connected to home network.

5.5 RCS

RCS (Rich Communication Suite) 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 IR.92 and IR.58
- Video call based on IR.94

Standard inter-Service Provider interfaces for these particular services are applicable both in the stand-alone case and when used as a part of RCS, thus there's no need to specify anything special for RCS as such.

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

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.

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] 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 TS 23.228 [5] and TS 24.229 [6].

For Public User Identities assigned to a user for receiving inbound calls/sessions, it is recommended to assign at least one E.164 number (MSISDN) to a user in order to enable CS interworking (for both break-in and breakout including SR-VCC). A SIP URI may also be assigned as a Public User Identity for receiving 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 6.3.3 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] compliant UE will use an IPv6 address. However, a IR.92 [28] 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 allow for 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 that of the UE. Such interworking can be taken care of 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 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), and the P-CSCF will establish a new transport leg to the next hop (e.g. I-CSCF), which can be the same or a different version of IP as the one used on the Gm interface if the P-CSCF is dual-stack, or else, be routed via an IBCF (acting as IPv4 to IPv6 proxy) that is dual stack.

6.2 Node Addressing

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

See section 4.2 for more information on the addressing used for IMS nodes connected to the Inter-Service Provider IP Backbone network.

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. 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*Where MNC and MCC are those of the visited network where the P-CSCF is located.

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 negotiating 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 signaling load between the UE and P-CSCF. Therefore it is recommended that where the operator owns the IP network serving the IMS UE and 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 use of Keep-Alive messaging may be unavoidable.

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 of distinguishing whether DNS queries need to be sent towards the Inter-Service Provider IP Backbone DNS or internal/public Internet DNS, due to the two Domain Name Systems being separate.

Chapter 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. GMSA PRD IR.67 [24] specifies the domain names used on the Inter-Service Provider IP Backbone network.

6.4.2 Roaming

When utilizing IMS roaming where the P-CSCF is located in the visited service provider's network, the P-CSCF discovers the home network entry point of the home service provider by resolving the home network domain name as given in the Request-URI of SIP REGISTER request. It is recommended to use only domain names specified in GSMA PRD IR.67 [24] Chapter 2.3.3 in the Request-URI, in order to enable DNS resolution and routing 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 IP Multimedia System Node names specified in GSMA PRD IR.67 [24] Chapter 2.6.

NOTE: When the URI of the finally address IMS node is accompanied by the URI of an entry node of the same network for the purpose of providing topology hiding, the URI of the finally addressed Node may be encrypted. In such a situation, the network entry node URI needs to meet the above requirements.

6.4.3 Interworking

Routing of SIP signalling over the IMS 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 precedence over the Request URI. See below for 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 IR.67 [24] Chapter 5 for more information). Section 5 of this document specifies 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 put in the User part, the domain name of the next network (Carrier or Terminating operator) is put 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 that the domain names used therein are provisioned in the IP backbone network providing the IMS NNI and

are agreed between interconnecting Service Providers in order to guarantee uniqueness .

NOTE: 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 have presence), 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 Chapter 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 are of significance:

A Service Provider may add a Route header entry pointing to the entry node of the selected IPX Provider/Carrier. 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: 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 directly after the possibly present Route header entry for the entry node of the IPX Provider´s network and otherwise as topmost route header entries. After the removal of the possibly present 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 67 [24] Chapter 2.3, or otherwise a domain name that is bilaterally agreed.

NOTE: Route header entries for the destination network are required when Interworking is applied for 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 interworking. For example possible intermediate IPX nodes (such as IPX Proxy) and also terminating networks with regards to securing interworking agreements and potential termination fees, etc. need this service identification. To facilitate that the same NNI can be used for multiple services, it is therefore essential that clear and unambiguous information of the requested service is included in SIP signalling, to ensure that the interconnected parties are in agreement of the service that is requested.

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 services, which 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 for example the Accept-Contact header. This additional information, which the originating Service Provider should ensure to be 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 interworking 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 NNI

When the NNI is used for an originating service request from a roaming user sent towards that users home network, 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 home network 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 home network receives an initial SIP request from one of its outbound roamers and the SIP request does not contain a P-Preferred-Service header, and the SIP request is progressed towards the requested destination, then the home network 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 outbound roamer.

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 above are valid also 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 cached by a specific filter.

6.5.4 ICSI-Values and Alternative Methods to Identify a Service

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

Annex A PS/CS Voice Interworking

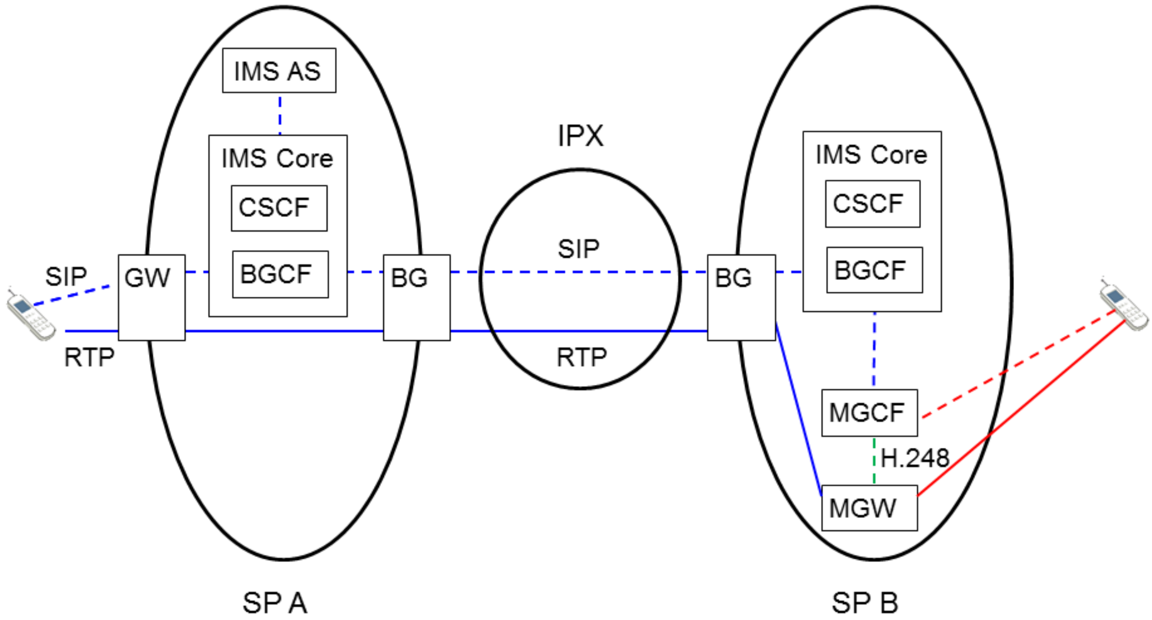

Figure A-1: IMS-to-IMS Voice NNI with receiver using CS UNI

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

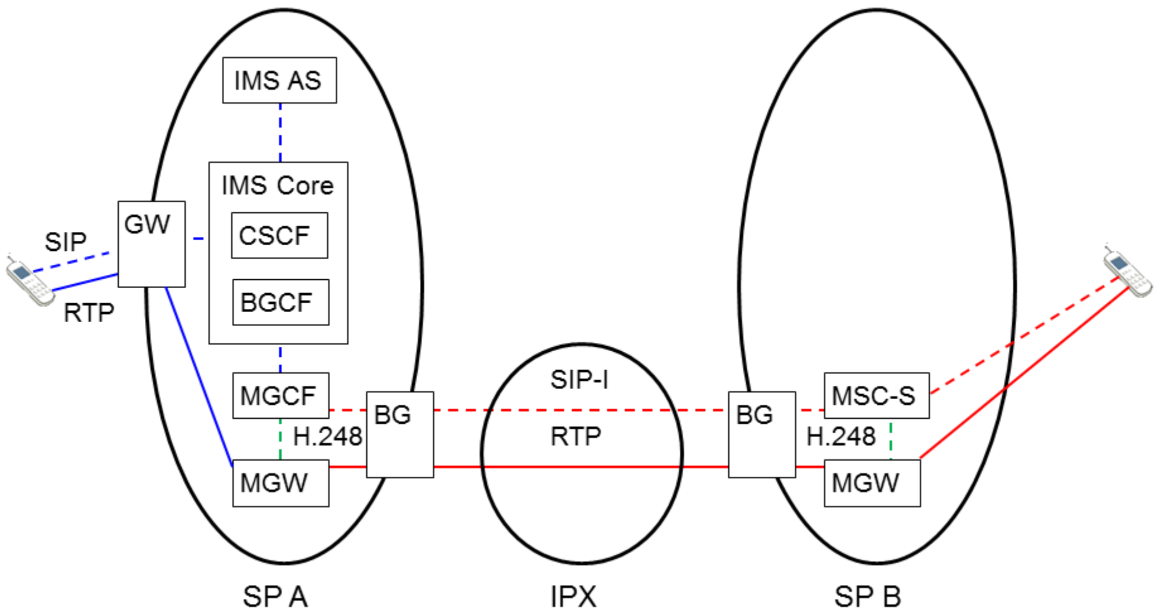

Figure A-2: IMS-to-MSC-S Voice NNI

Figure A-2 above shows an illustrative example of Client A using IP 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.

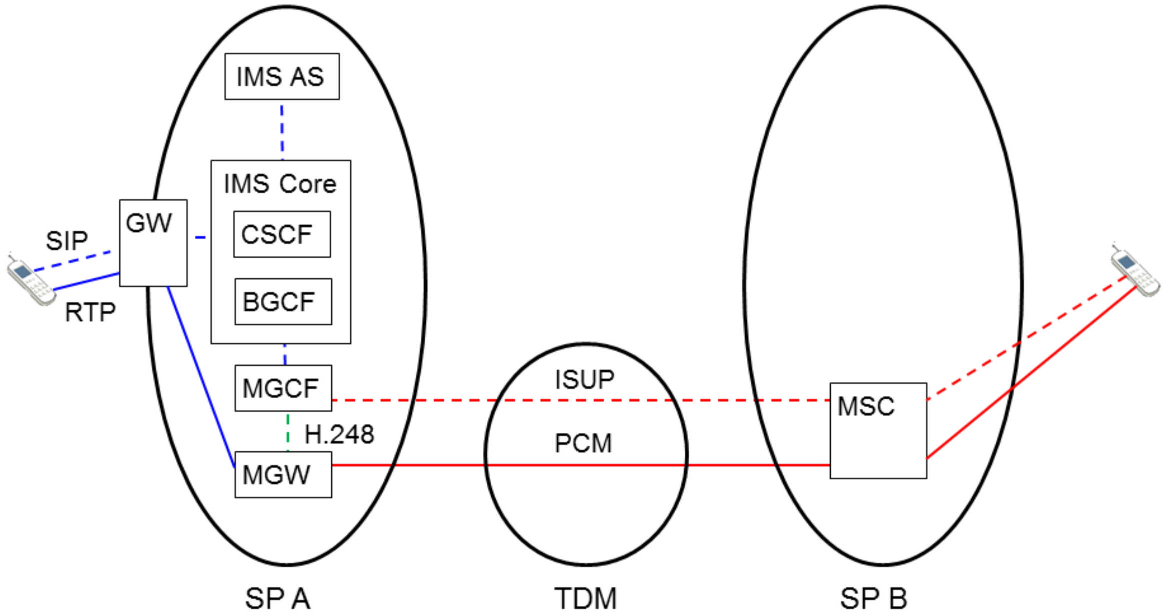

Figure A-3: IMS-to-MSC Voice NNI

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

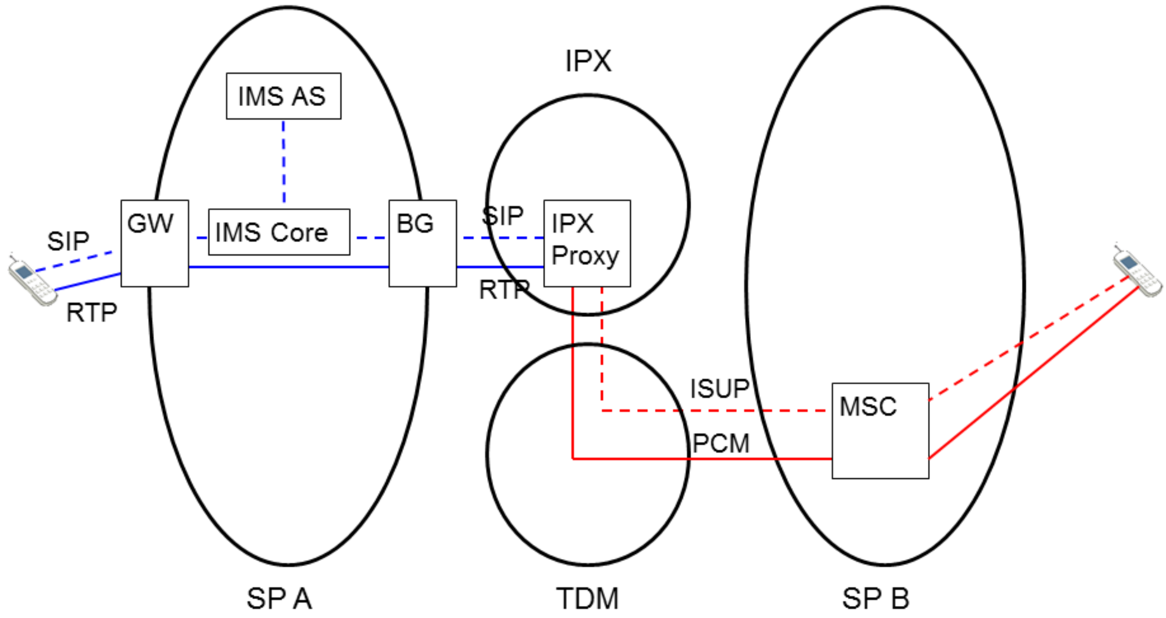

Figure A-4: IMS-to-MSC Voice NNI with IPX performing the TDM breakout

Figure A-4 above shows an illustrative example of Client A using IP based UNI connecting with Client B using CS based UNI for the exchange of voice traffic. The necessary CS/PS conversion is performed by the IPX Proxy in this example, that is the voice NNI is converted from PS 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 (NOTE 1)	Proxy role (NOTE 2)	
	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 (NOTE 1)	Proxy role (NOTE 2)	
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 (NOTE 1)	Proxy role (NOTE 2)	
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 for narrowband voice interworking and AMR-WB codec for wideband voice interworking:
  - An NNI that is not supporting the AMR codec must support G.711 speech codec.
  - An NNI that is not supporting the AMR wideband codec must support G.722 speech codec.
- If a service provider uses high definition codec in its network, it must offer at NNI the G.719 codec.

- A service provider using high definition codec in its network and not offering at NNI the G.719 codec must offer the AAC-LD codec.

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)
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

In 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 that relate to the operation of IMS interworking and roaming, such as protocol interworking and transcoding.

In this Annex, it is intended to identify requirements on the IPX Proxy for IMS interworking 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 interworking 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 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 described 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 protocol in layer 5 and above. 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.

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 B.2.2.2 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 dedicated 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 IR.40 [27] and 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 from Service Providers and other IPX Proxies traffic that originates from and terminates to servers (server-to-server traffic) either within a tunnel or un-tunnelled.

RI27. IPX Proxy shall accept from Service Providers and other IPX Proxies traffic that originates from and terminates to end users (user-to-user traffic) and traffic that originates from end users and terminates to servers or 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 as defined in 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 networked 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 are operated on their behalf by the IPX Provider will be made bilaterally between an individual Service Provider and their IPX Provider, on a service by service basis.

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 at Layer 3, 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 IR.40 [27] and 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 signalling 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 Document Management

D.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	First draft of PRD for IREG Packet		

	28th, 2003	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) and mCR020 (IMS roaming figure)	EMC	Tero Jalkanen / TeliaSonera
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-activation with S8HR) and 1018 (Emergency calls in S8HR)	PSMC	Tero Jalkanen / TeliaSonera

Other Information

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

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.