INTERNATIONAL INTERCONNECTION FORUM

FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

Source:

Working Group "IMS-based services and related interconnections"

i3 forum keyword: Voice, IMS, Interoperability

IMS-Based Services: Service Interoperability

(Release 1.2) June 2019

This document provides the i3 forum`s perspective on the interoperability issues related to the international interconnection of multiservice IMS-based platforms focusing on voice and video services originated from fixed as well as mobile networks. The scope covers both the interoperability between a Service Provider and Int. Carrier and between two Int. Carriers.
It does not intend to duplicate other existing specifications or documents on the same issue, but to complement these documents with the perspective of the International Carrier members of i3 forum.

EXECUTIVE SUMMARY

The rise of LTE technology in mobile networks together with the increasing FTTx deployment in the access section of fixed networks have been pushing a strong interest for IMS based services at the international level. These technological developments are paired at the service level by the wide-spread growth of LTE data services and by the deployments in Asia and in the USA, and more recently also in Europe, of Voice over LTE (VoLTE) services with HD voice capabilities.

In the wake of this trend, i3 forum has considered a priority to deliver a set of documents devoted to describing the architectures, the interfaces, the protocols to be adopted for the support of International IMS (*IP MultiMedia Subsystem*) services between two IMS Service Providers or between an IMS Service Provider and non IMS Service Provider adopting, in compliance with previous deliverables, an IPX model at the transport level.

Among the wide set of IMS-based services, in this third release, in addition to a strong focus on voice (fixed Voice over IMS and VoLTE) covering both the basic international call and the roaming cases, the scope is enlarged also to Video over LTE (ViLTE) and Enhanced Messaging Services (RCS).

As a result, focusing on interoperability issues between two Carriers/IPX Providers or between a Service Provider and its IPX Providers, the document addresses:

1) the basic principles for call routing, quality of service control and monitoring as well as network security service at the application layer;
2) an analysis of the impacts on Carriers' / IPX Providers' networks in terms of call types to be supported, physical interconnection, signalling interworking, transcoding and call routing for five major interworking scenarios:

   Case A) from IMS to IMS (with no fixed/mobile interworking);

   Case B) from IMS to IMS (with fixed/mobile interworking);

   Case C) from legacy networks to IMS and vice versa;

   Case D) from IMS to VoIP and vice versa;

   Case E) Interworking with webRTC
3) the discussion on the business and technical impacts of the roaming scenarios recently approved by GSMA;
4) a short analysis of the features and capabilities of the hubbing mode between Service Provder and IPX Provider.

i3 forum companion document "IMS-Based Services: Network - Network Interface definition" is devoted to discuss all the issues related to interface specification.

The ultimate objective of the document, together with a companion i3 forum document devoted to IMS interface definition, is to provide a unique analysis of the impact on Carriers' / IPX Providers' platforms for the provisioning of IMS based services, The focus is given not only to the selection of the proper standard(s) to be adopted within a comprehensive IPX architectural and commercial model, but also to the discussion of the various alternatives to be dealt with and their related results with respect to the end-to-end service.

Table of Contents

1. Scope and objective of the document

Over the last three years, the rise of LTE technology in mobile networks together with the increasing FTTx deployment in the access section of fixed networks have been pushing a strong interest for IMS-based services at the international level.

The mentioned technological development is matched at the service level by the wide-spread growth of LTE data services and by the deployments in Asia and in the USA, and more recently also in Europe, of Voice over LTE (VoLTE)/Video over LTE (ViLTE) services with HD capabilities.

In the wake of this trend, i3 forum has considered a priority to deliver a set of documents devoted to describing the architectures, the interfaces, the protocols to be adopted for the support of International IMS (IP Multimedia Subsystem) services between two IMS Service Providers or between an IMS Service Provider and non IMS Service Provider adopting, in compliance with previous deliverables, an IPX model at the transport level.

Among the wide set of IMS-based services, in this third release, in addition to a strong focus on voice (fixed Voice over IMS and VoLTE) covering both the basic international call and the roaming cases, the scope is enlarged also to Video over LTE (ViLTE) and Enhanced Messaging Services (RCS).

As a result, focusing on interoperability issues between two Carriers/IPX Providers or between a Service Provider and its IPX Providers, the document addresses:

1) the basic principles for call routing (sec. 4), quality of service control and monitoring (sec. 6) as well as security service (sec. 7) at the application layer;
2) an analysis of the impacts on Carriers' / IPX Providers' networks in terms of call types to be supported, physical interconnection, signalling interworking, transcoding and call routing for five major interworking scenarios (sec. 5):
    i. Case A) from IMS to IMS (with no fixed/mobile interworking);
    ii. Case B) from IMS to IMS (with fixed/mobile interworking);
    iii. Case C) from legacy networks to IMS and vice versa;
    iv. Case D) from IMS to VoIP and vice versa;
    v. Case E) Interworking with webRTC
3) The discussion on the business and technical impacts of the roaming scenarios approved by GSMA (sec. 8);

i3 forum companion document "IMS-Based Services: Network - Network Interface definition" is devoted to discuss all the issues related to interface specification.

The final objective of the document, together with a companion i3 forum document devoted to IMS interface definition [1]*, is to provide a unique analysis of the impact on Carriers' / IPX Providers' platforms of the provisioning of IMS-based services. The focus is given not only to the selection of the proper standard(s) to be adopted within a comprehensive IPX architectural and commercial model, but also to the discussion of the various alternatives to be faced and their related results with respect to the end-to-end service.*

In this document, though the interconnection between two IMS-based Service Providers can always be provided by a generic International Carrier, since IPX is the recommended model by i3 forum and GSMA for supporting such interconnection, from Sec. 4 onwards, the terminology IPX Provider is always used for identifying an International Carrier.

2. Symbols and Acronyms

3GPP	3rd Generation Partnership Project
ALOC	Average Length of Call
AMR-NB	Adaptive Multi-Rate Narrow Band
AMR-WB	Adaptive Multi-Rate Wide Band
APN	Access Point Name
ASR	Answer-Seizure Ratio
BGP	Border Gateway Protocol
BSS	Business Support System
CAMEL	Customized Applications for Mobile Enhanced Logic
CLI	Calling Line Identification
CPU	Central Processing Unit
CSCF	Call Session Control Function
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
EF	Expedited Forwarding
ENUM	E.164 NUmber Mapping
ETSI	European Telecommunications Standards Institute
FNO	Fixed Network Operator
FTTx	Fiber To The “x” (n=network, c=curb, b=building, h=home)
GSM	Global System for Mobile Communications
GSMA	GSM Association
HD	High Definition
HPLMN	Home Public Land Mobile Network
HPMN	Home Public Mobile Network
HR	Home Routing
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
IPSec	IP Security
IPX	IP eXchange
IPX P	IPX Provider
ISUP	ISDN User Part
ITU	International Telecommunications Union
KPI	Key Performance Indicator
LBO	Local Break Out
LTE	Long Term Evolution
MNO	Mobile Network Operator
MOS	Mean Opinion Score
MOS_{CQE}	Mean Opinion Score, Communication Quality Estimated
NER	Network Efficiency Ratio
NGN	Next Generation Network
NNI	Network to Network Interface
OBC	Origin Based Charging
OMR	Optimal Media Routing
OSPF	Open Shortes Path First
OSS	Operations Support System

OTT	Over The TOP
PGAD	Post Gateway Answer Delay
PGRD	Post Gateway Ringing Delay
PMN	Public Mobile Network
PoP	Point of Presence
PSTN	Public Switched Telephone Network
QCI	Quality Coded Indicator
QoS	Quality of Service
RAVEL	Roaming Architecture for Voice over IMS with Local Breakout
RCS	Rich Communication Suite
R-Factor	Rating-Factor
RFC	Request For Comments
RTC	Real Time Communication
RTCP	Real Time Control Protocol
RTD	Round Trip Delay
RTP	Real-Time Protocol
S8HR	S8 Home Routing
SBC	Session Border Controller
SD	Standard Definition
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-URI	SIP protocol URI
SLA	Service Level Agreement
SP	Service Provider
SRTP	Secure Real Time Protocol
SS7	Signalling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
Tel-URI	Telephone URI
TLS	Transport Layer Security
URI	Uniform Resource Identifier
ViLTE	Video over LTE
VLAN	Virtual Local Area Network
VoIMS	Voice over IMS
VoIP	Voice over IP
VoLTE	Voice over LTE
VPLMN	Visited Public Land Mobile Network
VPMN	Visited Public Mobile Network
Wifi	Wireless Fidelity

3. References

[1] i3forum, "IMS-Based Services: Network-Network Interface Defintion, Release 1, (May 2017)".

[2] IETF, "RFC 3966; The tel URI for Telephone Numbers".

[3] IETF, "RFC 3986; Uniform Resource Identifier (URI): Generic Syntax".

[4] GSMA, "NG.105; ENUM Guidelines for Service Providers and IPX Providers, Version 1.0, 20 Mar 2017".

[5] R. 3761, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[6] i3forum, "Technical Interconnection Model for International Voice Services, Release 6, (May 2014)".

[7] 3GPP, "TS 29.165; Inter-IMS Network to Network Interface".

[8] i3forum, "Common functionalities and capabilities of an IPX platform, Release 2, May 2014".

[9] IETF, RFC 7118; "WebSocket as a Transport for SIP"..

[10] IETF, RFC7874; Proposed Standard "WebRTC Audio Codec and Processing Requirements".

[11] IETF, RFC 7742; Proposed Standard "WebRTC Video Processing and Codec Requirements".

[12] i3forum, "Technical Interconnection Model for International Voice Services, Release 6, (May 2014)".

[13] ITU-T, "E.437; Comparative metrics for network performance management".

[14] ITU-T, "E.425; Internal automatic observations".

[15] ITU-T, "P.563; Single-sided method for objective speech quality assessment in narrow-band telephony applications".

[16] i3forum, "IMS-Based Services: Technical and Commercial Analysis of International Interconnection and Roaming Services (Release 2.0) May 2016".

[17] ITU-T, "P.1202-2; Parametric non-intrusive bitstream assessment of video media streaming quality - higher resolution application area".

[18] ETSI, "ES 202 667; Audiovisual QoS for communication over IP networks".

[19] GSMA, "IR.34; Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines)".

[20] GSMA, "IR.65; IMS Roaming and Interworking Guidelines".

[21] 3GPP, "TR 23.850; Study on roaming architecture for voice over IP Multimedia Subsystem (IMS) with local breakout".

[22] GSMA, "IR.92; IMS Profile for Voice and SMS".

[23] GSMA, "IR.94; IMS Profile for Conversational Video Service".

[24] 3GPP, "TS 23.228; IP Multimedia Subsystem (IMS); Stage 2".

[25] i3forum, "Voice over IPX Service Schedule".

[26] 3GPP, "TS 24.341; Support of SMS over IP networks; Stage 3".

[27] IETF, "RFC 3261; SIP: Session Initiation Protocol".

[28] 3GPP, "TS 26.114; IP Multimedia Subsystem (IMS) – Multimedia telephony – Media handling and interaction".

[29] 3GPP, "TS 26.441; Codec for Enhanced Voice Services (EVS)".

[30] GSMA, "IR.95; SIP-SDP Inter-IMS NNI Profile".

[31] IETF, "RFC 4733; RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, December 2006".

[32] GSMA, "AA.81; Packet Voice Interconnection Service".

[33] IETF, "RFC 3550; RTP: A Transport Protocol for Real-Time Applications".

[34] IETF, "RFC 4855; Media Type Registration of RTP Payload Formats".

[35] IETF, "RFC 6849; An Extension to the Session Description Protocol (SDP) and Real-time Transport Protocol (RTP) for Media Loopback".

[36] IETF, "RFC 4867; RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs", April 2007".

[37] GSMA, "IR.36; Adaptive Multirate Wide Band".

[38] ITU-T, "P.10/G.100; Telephone Transmission Quality".

[39] ITU-T, "G.107; The E-model: a computational model for use in transmission planning".

[40] ITU-T, "G.107.1; Wideband E-model".

[41] ITU-T, "G.107 Annex B; Quality measures derived from the transmission rating factor R".

[42] ITU-T, "E.411; International network management - Operational guidance".

[43] IETF, "RFC 2328; OSPF Version 2 (April 1998)," .

[44] IETF, "RFC 4271, A Border Gateway Protocol 4 (BGP-4), (January 2006)".

[45] IETF, "RFC 3264; An Offer/Answer Model with the Session Description Protocol (SDP), (June 2002)".

[46] "IETF," RFC 6386; VP8 Data Format and Decoding Guide.

[47] i3forum, "LTE Data Roaming over IPX Service Schedule, Release 1, May 2014".

[48] i3forum, "Enabling HD voice continuity in international calls, Release 1.0, May 2014".

[49] GSMA, "BA.27; Charging Principles".

[50] GSMA, "RCS 5.1; Advance Communications Specification Baseline".

[51] IETF, "RFC 4975; The Message Session Relay Protocol (MSRP), September 2007".

[52] GSMA, "IN.27; Interconnection and Interworking Charging Principles, Version 5.0, 8 February 2016".

[53] i3forum, "Interconnection & Roaming IMS Signaling Profile, Release 3 (May 2016)".

[54] GSMA, "IR.90; RCS Interworking Guidelines, Version 12.0, 2 April 2015".

[55] ITU-T, "H.264 (02/2016); Advanced video coding for generic audiovisual services".

[56] GSMA, "IR.77; Inter-Operator IP Backbone Security Requirements for Service and Inter-operator IP backbone Providers, Version 4.0, 10 November 2015".

[57] GSMA, "IN.25; Proposed national and international RCS-e Interworking Requirements".

[58] ITU-T, "H.265 (04/2015); High efficiency video coding".

[59] ITU-T, "Q.1912.5 (01/2018); Interworking between session initiation protocol (SIP) and bearer independent call control protocol or ISDN user part".

4. Addressing, Routing and ENUM Management

As services migrate away from a circuit switched environment to IP, the user identification number starts to differentiate from the PSTN numbering scheme. This process generates opportunities as well as challenges to manage.
The opportunities lie with the fact that different routing domains can be created, different capabilities can be associated to different services, different codes have to be supported. This variety can generate the need of multiple queries to different database in order to properly identified the destination party of a session (in general for voice, video or messaging). The challenges come from the impact on existing network platforms and related OSS/BSS chain and how to implement this transition phase.

4.1. Addressing

Two basic addressing schemes can be identified:

a) *Tel URI* [2] which endorses the traditional ITU-T E.164 addressing scheme (see [Ref. i3f Tech doc Rel. 6] for additional information);
b) *SIP URI* [3] which links the user identification with his network domain, (*sip:+14085551212@domain.com;user=phone* or *sip:abcdef@domain.com*). For mobile networks GSMA in NG.105 further specified the user identification string as: sip:+14085551212@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org;user=phone

The migration of Tel URI to SIP URI has an important implication on how IPX Providers mediate and terminate calls:

➢ From the technical perspective: routing by domain will increasingly differ from routing by dial code ranges (E.164) in that the addressing scheme becomes decoupled from the PSTN structure. This will impact existing already complex routing engines.

➢ From the operational perspective: traditionally, Service Providers and IPX Providers provide international voice termination pricing by dial code ranges. Pricing by domain will increasingly replace the legacy scheme implying a new way of processing and managing the pricing data.

➢ From the business/commercial standpoint: IPX Providers termination pricing is typically, and in part, a function of the destination network's cost. As costing by domain becomes necessary, so will pricing by domain.

Because of this evolution, the routing, costing and pricing systems will have to be adapted, which implies that IPX Providers will be facing substantial system investments. In the short run however, most of the impact will be on the technical side as it relates to the support of the new addressing scheme.

4.2. Routing

To keep the call path compliant with the service objectives of an IMS-based session (e.g. maintain an AMR-WB codec end-to-end), the routing Carrier / IPX Provider needs advanced knowledge of key information required for the appropriate routing to be applied, e.g. is the number ported, has the called subscriber signed up for IMS-based services, etc..

To cope with these changes in terms of addressing scheme (see sec. 6.1 above) as well as to achieve routing path compliance in the number porting & LTE environment, new tools are needed to:
(i) permanently have available up-to-date ported number & technology information;
(ii) to query (or "dip") such databases real-time.

While ported number & technology resolution solutions are widely available, there are, however, some shortcomings on the availability of ported number databases across countries:

1. Database coverage is limited – e.g. some VoLTE markets do not have any NP database available to carriers.
2. Where there is National NP support, the costs and/or complexity to access the information are often significant

4.3. ENUM-based resolution systems

4.3.1. ENUM Databases

ENUM is the protocol recommended by GSMA (NG.105 [4] corresponding to RFC 3761 [5]) for the ported number & technology resolution, or discovery, as part of routing. Other protocols (e.g. SIP or legacy MAP) can also be used to complement information retrieved by means of ENUM-based resolution..

Databases reachable by ENUM-based query and related access structures are described in much detail in NG.105 [4] and are referred to as ENUM servers, ENUM databases and ENUM proxies.

GSMA NG.105 [4] describes in detail ENUM functionality recommendations for service aware routing, main example being VoLTE termination. Two complementary deployment models have been identified: hierarchical model and ENUM proxy based model.

It should be noted that an ENUM query does not provide a route. It provides another address relevant to the target destination and technology, corrected to solve the NP. Routing entity will use the ENUM information in combination with commercial policies to route traffic towards terminating network.

4.3.1.1. Hierarchical model

ENUM is structured around an authoritative cascading process (NG.105 [4]).
Specifically:

- **Tier 0** authoritative resolution of Tier 1 index. It determines which country Tier 1 database to lookup (number resolution)
- **Tier 1** query returns the national operator Tier 2 database to query (Number resolution)
- **Tier 2** query returns the information on the user device: it confirms whether it is indeed assigned to the network and its service capabilities (e.g. VoLTE enabled) (Technology resolution)

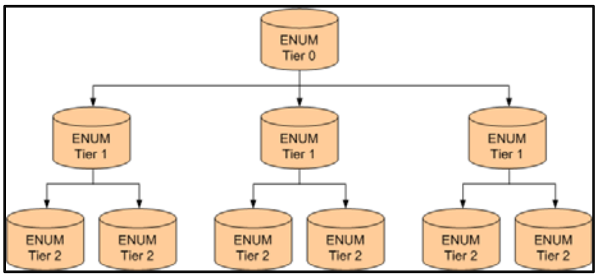

Figure 1 - GSMA ENUM Tiered Architecture

NG.105 [4] differentiates between the traditional repeated or “iterative” querying and more recently the sequential or “recursive” querying.

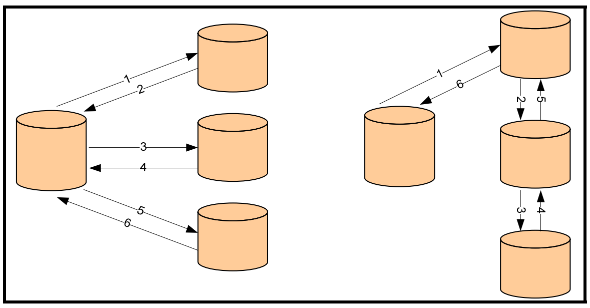

Figure 2 - GSMA “Iterative Querying” (left) and “Recursive Querying” (right)

4.3.1.2. ENUM proxy

Even though hierarchical ENUM has been designed as global solution for service discovery, there are limitations that affect this service resolution model:

- No NP management in the international backbone: ENUM hierarchical model may not be available and/or NP is not applicable within the country. Indeed, for the majority of countries, the handling portability solution is still based on “legacy” solution without ENUM interface. Some countries have also legal constraints which could limit the national NP database access from international entities
- Customer Data Exposure is still a real issue: ENUM Tier-2 (Service Provider level) may not be open to external queries. Some SPs do not intend to open ENUM servers to external queries for security reasons

This complementary ENUM resolution scheme allows SPs and IPX providers to gather B-subscriber info without having all ENUM Tier-0/1/2 available and interconnected. In addition, ENUM Proxy will be able to retrieve routing information from ENUM or non ENUM domains (i.e. legacy environment using other signalling like MAP, Diameter or SIP).

GSMA ENUM proxy interfaces are depicted in Figure 4. The following interfaces have been defined:

- ENUM1 is an ENUM interface used by IMS and/or SIP Proxy to query ENUM Proxy
- ENUM2 is an ENUM interface used by the ENUM Proxy to query ENUM hierarchical model using ENUM FQDN format like 9.8.7.6.5.4.3.2.1.e164enum.net for +123456789” E.164 number
- ENUM3 is an ENUM interface used to exchange information between ENUM Proxy1 and ENUM Proxy2 when they are interconnected
- NENUM1 is a Non ENUM interface used to query external database able to provide the destination SP identity
- NENUM2 is a Non ENUM interface used to query external database able to provide the destination user profile

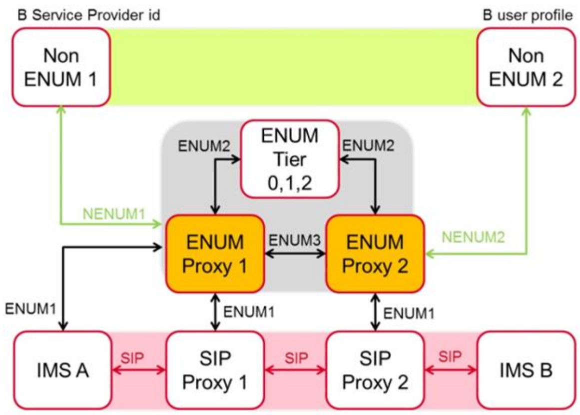

Figure 3 – GSMA ENUM proxy: interfaces definition

Reference model, ENUM use cases and implementation examples are described in NG.105 (section 5).

4.3.2. IPX Providers Management of ENUM Databases

Assuming an IPX Provider offers a full “hubbing” service and adopting the hierarchical mode with I “iterative querying” scheme, the sequence of query is given in the Figure 4 below. Two IPX Ps might be involved in the call path; in this case it is a responsibility of IPX P “B” to perform the resolution process querying the related databases in compliance with the general IPX specification.

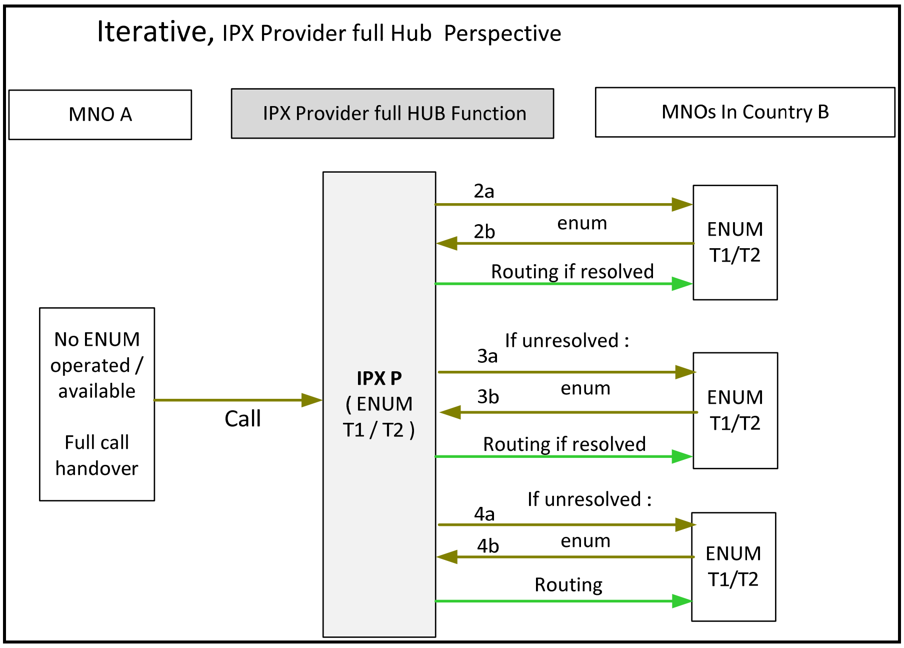

Figure 4 - "Iterative Querying" with hubbing model

Some SPs might want to retain the eventual routing decision. ENUM queries to the IPX Provider are responded with a redirect to MNO B for a valid ENUM response or a negative acknowledgement allowing the originator to use an alternate IPX Provider or an LCR for PSTN termination (see Figure 5 below).

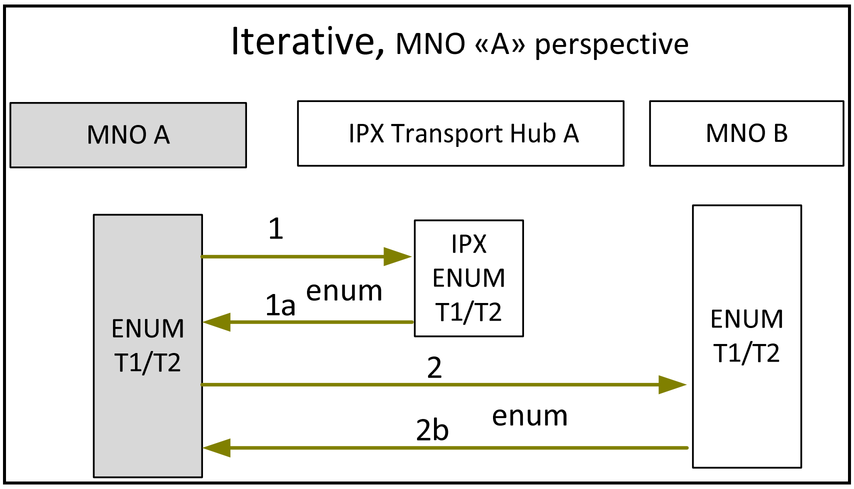

Figure 5 - "Iterative Querying" initiated by MNO.

As far as the "recursive" scheme is concerned, it allows for an IPX Provider to query the termination ENUM database on behalf of the originating Service Provider (or upstream IPX Provider) providing the final response instead of redirecting the originating request.

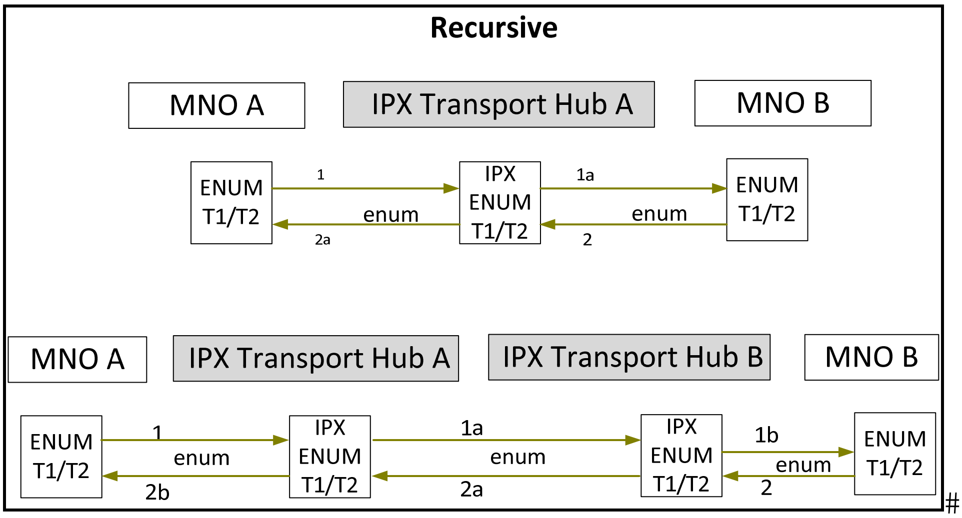

Figure 6 - "Recursive Querying"

The call is handed over to the IPX Provider which performs all the needed forward-queries to the involved ENUM server(s), if necessary several times.

Should IPX providers adopt ENUM proxy model, the possible query sequences apply:

- IPX A determines SP id to select IPX B which will retrieve B user profile
- IPX A retrieves SP id and queries user profile via ENUM3 interface (i.e. ENUM proxy A to ENUM proxy B query)
- IPX A retrieves both SP id and user profile via ENUM3 interface

5. Interoperability Cases for other IMS and Legacy networks

As described above, the technology for voice telephony as well as other services is currently in transition from a TDM-based legacy platform towards IP-based solutions aiming to support both basic VoIP service (today widespread globally) and IMS services (currently limited to small geographical areas).

The traditional voice service is also in the process of being enhanced with features like high quality voice (HD Voice), adding pictures or video to a voice call, and other features that enrich the final customer experience. These features call for a different set of services capabilities and new requirements in terms of signaling, interworking / interoperability, routing and transcoding.

This section is focused on analyzing and discussing the basic functions to be performed by Carriers/IPX Providers in a wide variety of transmission scenarios between IMS networks and legacy networks, and between fixed and mobile IMS networks. In this respect, the following five cases have been identified covering the most relevant voice call scenarios:

Case A): Calls originated from a fixed IMS to be terminated to a fixed IMS and, in an equivalent way, all originated from a mobile IMS 4G to be terminated to a mobile IMS 4G;

Case B): Calls originated from a fixed IMS to be terminated to a mobile IMS 4G and vice versa;

Case C): Calls originated from a non-IMS (fixed TDM or mobile 2G/3G) network to be terminated to an IMS (fixed IMS or mobile IMS 4G) network and vice versa;

Case D): Calls originated from an IMS (fixed IMS or mobile IMS 4G) network to be terminated to a VoIP legacy network (including OTTs) and vice versa;

Case E): Interworking with webRTC.

For all above cases signalling (control plane) and user traffic (media plane) of the same session shall be transported in an associate mode at every NNI interface between Service Provider and IPX Provider and between two IPX Providers.

5.1. Case A) from IMS to IMS (with no fixed/mobile interworking)

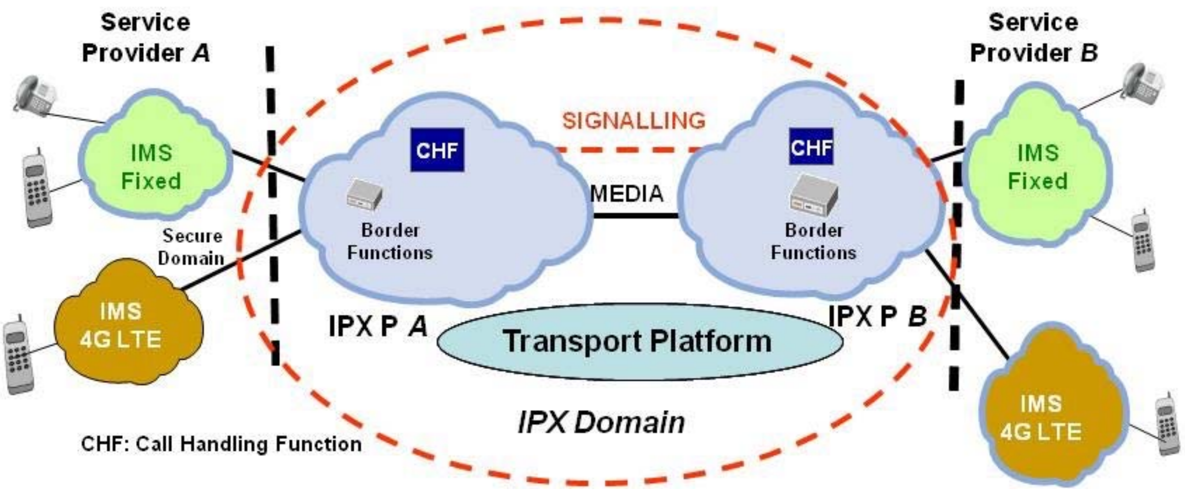

Figure 7 – From IMS to IMS (with no fixed/mobile interworking)

Services: In this use case (see Figure 7), IMS services can be available in all variants, e.g. voice SD and HD calls, video calls, ready to future enhancements. Due to the different characteristics of fixed and mobile devices, additional and supplementary services are limited by the functionalities of these devices and the related network capabilities.

Physical Interconnection: Standard IP interconnection over multiple transmission systems (see *"Technical Interconnection Model for International Voice Services", Rel. 6, May 2014,* [6]*) and "IMS- Based Services: Network-Network Interface Definition", Rel. 1, May 2017,* [1]*).*

Signaling: Support of the standard IMS Signalling as per 3GPP specification TS 29.165 complemented by i3 forum deliverables [7]. No interworking / interoperability is required.

Transcoding: Codec transparency is an issue. In general, for fixed networks no transcoding is needed in this scenario assuming the endpoint devices are HD enabled, whereas for mobile networks because of the diversity of AMR-WB codecs (e.g. bandwidth efficient or octet-aligned) transcoding may be required ensuring in any case the end-to-end HD quality.

Addressing: In addition of the basic Voice over IPX requirement of maximum two IPX Providers end-to-end (see [8]) two addressing schemes can be used:

a) Tel-URI or SIP-URI user=Phone: no impact for the Carrier / IPX Providers networks;
b) SIP-URI Alphanumeric: this option requires important changes in voice service platform and in its relationship with the OSS/BSS systems.

5.2. Case B) from IMS to IMS (with fixed/mobile interworking)

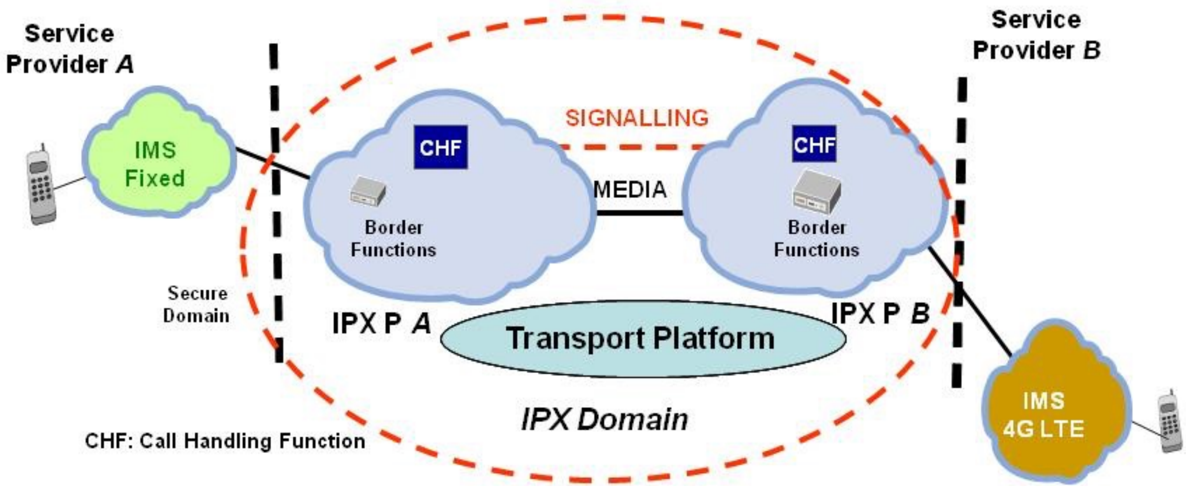

Figure 8 - From IMS to IMS (with fixed/mobile interworking)

Services: In this use case (see Figure 8), IMS services can be available in all variants, e.g. voice SD and HD calls , video calls, ready to future enhancements. Due to the different characteristics of fixed and mobile devices, additional and supplementary services are limited by the functionalities of these devices and the related network capabilities.

Physical Interconnection: standard IP interconnection over multiple transmission systems (see *"Technical Interconnection Model for International Voice Services", Rel. 6, May 2014,* [6]*) and "IMS-Based Services: Network-Network Interface Definition", Rel. 1, May 2017,* [1]*).*

Signaling: Support of the standard IMS Signalling as per 3GPP specification TS 29.165 complemented by i3 forum deliverables [7]. No interworking / interoperability is required.

Transcoding: If the call cannot successfully negotiate a common wideband codec on each side (e.g. for fixed handset G.722 and for mobile handset AMR-WB), then the transcoding between these codecs can be done by one of the two SP on either side or by the IPX Provider in between or in case of multiple IPX Providers, by one of these IPX Providers.

However, it is common practice in the market that the originating SP takes care of transcoding. In any case, there is the certainty to set-up the call using the G.711 codec.

Addressing: In addition of the basic Voice over IPX requirement of maximum two IPX Providers end-to-end (see [8]) two addressing schemes can be used:

a) Tel-URI or SIP-URI user=Phone: no impact for the Carrier / IPX Providers networks;
b) SIP-URI Alphanumeric: this option requires important changes in voice service platform and in its relationship with the OSS/BSS systems.

5.3. Case C) from IMS to legacy networks and vice versa

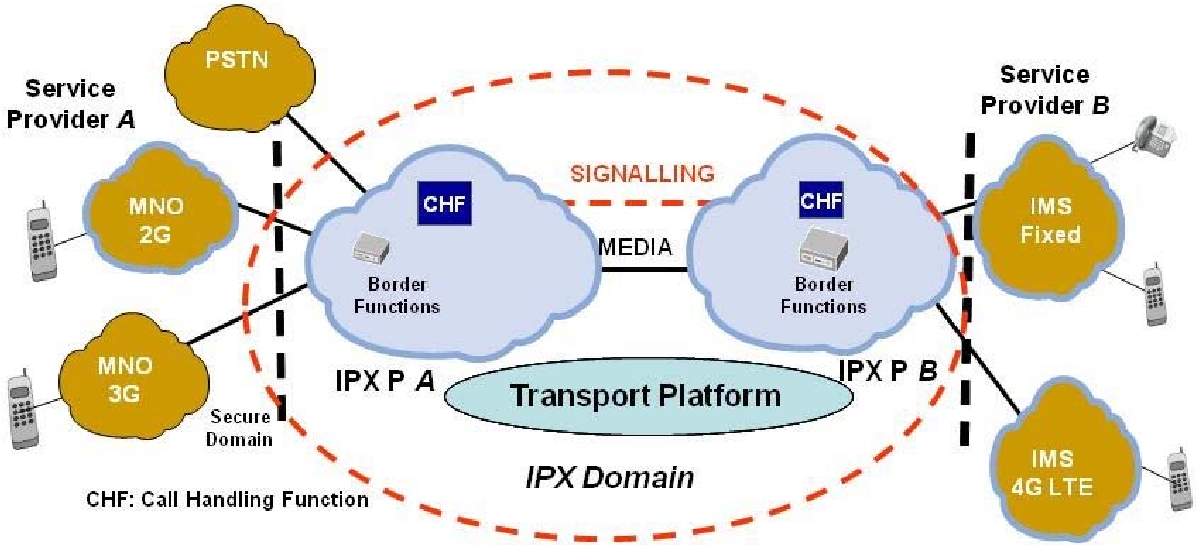

Figure 9 - From legacy networks to IMS

Services: for this use case (see Figure 9), voice is the basic service to be provided. The expansion to additional and supplementary services is limited by the functionalities of both legacy and IMS networks and the interworking capabilities between these two types of networks.

In mobile 3G networks, HD voice can be offered by MNOs provided that they support transcoder free operation (TrFO). If Carriers / IPX Providers can manage HD codecs or better, are TrFO enabled, even in this use case HD voice can be offered end-to-end.

Physical Interconnection: standard IP interconnection over multiple transmission systems (see *"Technical Interconnection Model for International Voice Services", Rel. 6, May 2014,* [6]*) and "IMS-Based Services: Network-Network Interface Definition", Rel. 1, May 2017,* [1]*).*

Signaling (i.e. from ISUP to SIP IMS): The signaling interworking and interoperability is typically performed by the 1st IPX Provider between the calling and called party.

Transcoding: If different codecs are declared from the originating and terminating party, then the transcoding between these codecs can be performed by one of the two Service Providers or by the 1st IPX Provider (i.e. the closest to the originating party) or by the 2nd IPX Provider (i.e. the closest to the terminating party).

However, it is common practice in the market that the originating Service Provider takes care of the transcoding. It is also common practice, that if no better codecs can be selected, then the G.711 codec is selected on both sides as the codec to be used for the call. As a result, in this scenario, the end-to-end communication is mainly implemented by means of the G.711 codec. With regards to the support of HD Voice:

a) for fixed PSTN networks: this service is not available;
b) for mobile 3G networks: this service is possible based on TrFO and IP based backhauling.

Addressing: In addition to the basic Voice over IPX requirement of maximum two IPX Providers end-to-end (see [8]) only the addressing schemes based on E.164 apply (i.e. Tel-URI or SIP-URI user=Phone see section 9.1 of this document).

No specific requirements to the Carrier/IPX Provider apply.

5.4. Case D) from IMS to VoIP and vice versa

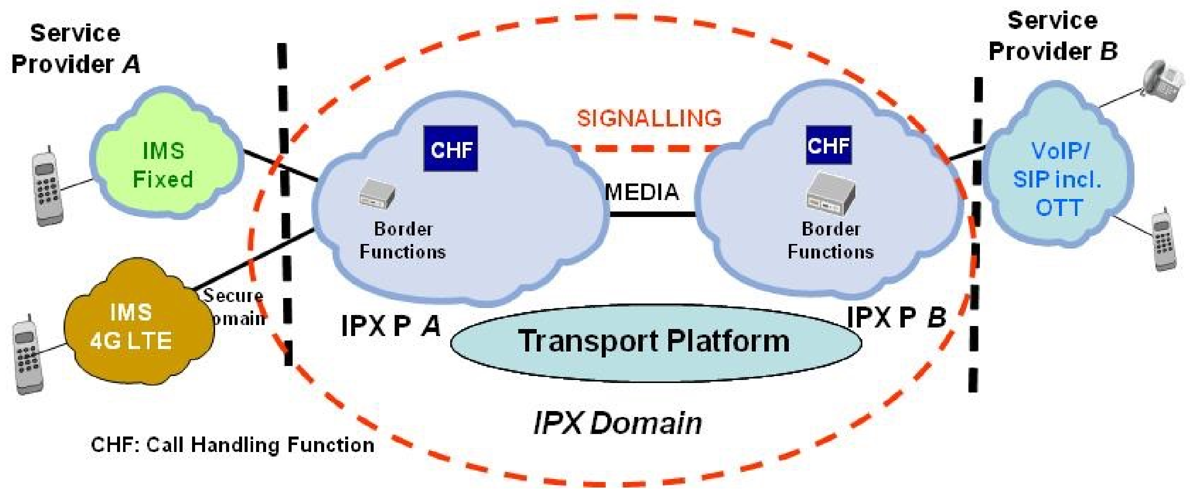

Figure 10 – From IMS to VoIP

Services: In this use case (see Figure 10), the transport layer is fully IP but interoperability between different signaling protocols and codecs (e.g. transcoding an OTT proprietary codec) is needed, resulting in a related impact on quality of service (e.g. part of the call path may be over Public Internet).

The voice service can be offered in the SD and HD variants. Interoperability of supplementary services is not natively ensured and, if needed, may require additional implementations for SPs and IPX Ps.

Physical Interconnection: IP interconnection over multiple transmission systems (see *"Technical Interconnection Model for International Voice Services", Rel. 6, May 2014,* [6]*) and "IMS-Based Services: Network-Network Interface Definition", Rel. 1, May 2017,* [1]*).*

Signaling: The signaling interworking and interoperability is typically performed by the 1st IPX Provider between the calling and called party.

Transcoding: If different codecs are declared from the originated and terminating party, then the transcoding between these codecs can be performed by one of the two Service Providers or by the 1st IPX Provider (i.e. the closest to the originating party) or by the 2nd IPX Provider (i.e. the closest to the terminating party).

In this case, in addition to standard telecom-originated codecs, also codecs typically used by OTT Providers (e.g. Opus) have to be considered. Currently, OTTs, in addition to their proprietary codecs, also support the codecs standardized in the telecom world (e.g. G.711 and G.729).

Addressing: In this case in addition to the two addressing schemes specified in the telecom industry (Tel-URI and SIP-URI) already mentioned in the other cases; the proprietary addressing schemes of the various OTT Providers has to be taken into account. *As of today, it is a widely solid market trend that the mapping from the telco addressing scheme to other addressing scheme is carried out in the OTT Providers domain.*

5.5. Case E) Interworking with webRTC

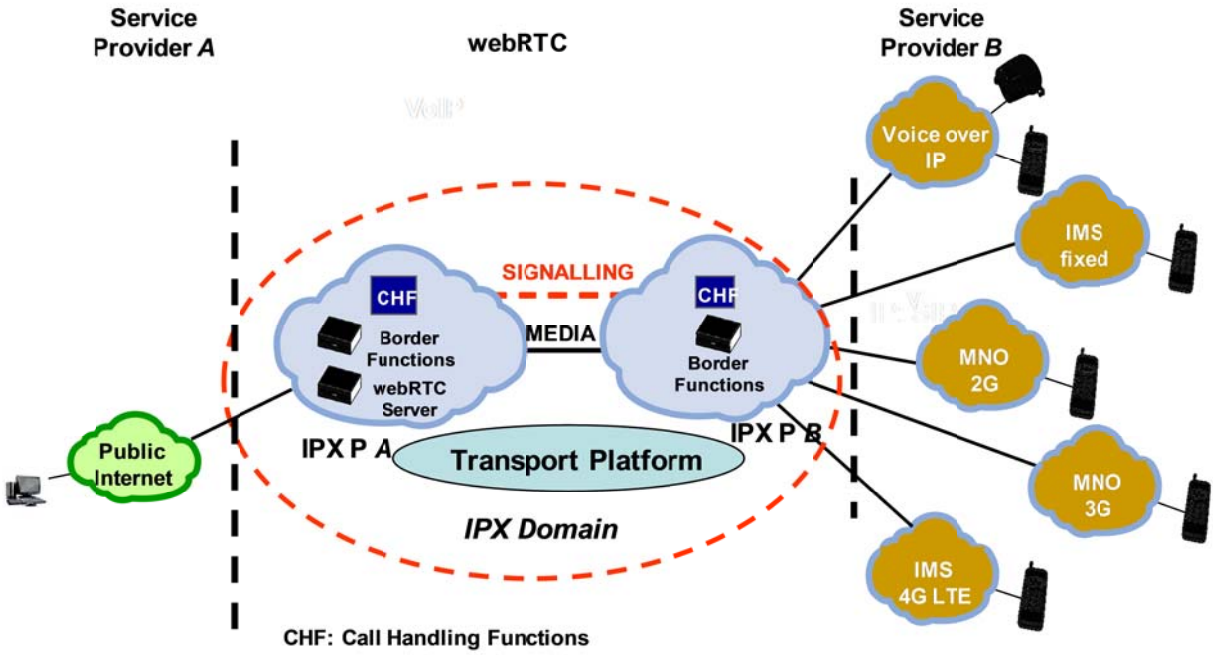

Figure 11 - Interworking with webRTC

Services: for this use case (see Figure 11), voice and video are the basic services to be provided. The expansion to additional and supplementary services is limited by the functionality of the type of network that is being used and by the characteristics of fixed and mobile devices.

Physical Interconnection: IP interconnection over multiple transmission systems (see *"Technical Interconnection Model for International Voice Services", Rel. 6, May 2014,* [6]*) and "IMS-Based Services: Network-Network Interface Definition", Rel. 1, May 2017,* [1]*).*

Signaling: The signaling interworking between html and SIP is typically performed by the first IPX provider between the calling and the called party. For the connectivity to a webRTC server no signaling mechanisms have been specified and therefore the used signaling mechanism can differ between different implementations. Due to the usage of SIP in many communication scenarios often SIP over Websockets [9] is implemented.

Transcoding: In case different codecs are declared from the originating and the terminating party, then the transcoding between these codecs can be performed by one of the two Service Providers or by the first IPX Provider or by the second one. However, it is common practice in the market that the originating Service Provider takes care of transcoding.

Audio codecs: The i3Forum mandates as narrowband codecs G.711, G.729, G.729a, G.729b and G.729ab. Mandatory wideband codecs are G.722 and G.722.2. The IETF mandates for webRTC services the implementation of Opus and G.711 (see [10]).

Video codecs: The i3Forum mandates H.264. The IETF mandates for webRTC services the implementation of VP8 and H.264 (see [11]).

Addressing: In addition to the basic IPX requirement of maximum two IPX providers two different addressing schemes need to be matched. For IMS-based services Tel-URI or SIP-URI are widespread in use whereas for a webRTC application addressing is done via the public IP number and the port number of the device in use. Such an identifier can also be represented by SIP-URI, however, the fact that IP addresses change on a regular basis is an additional aggravating complication.

6. QoS control and monitoring for media services

The control and the monitoring of quality aspects of a service are important activities for the offering of telecommunication services characterized by predefined levels of quality. These activities make us of descriptive parameters that can be measured and controlled in a quantitative way.

These parameters are often classified into two separate classes. One parameter class pertains to the network layer and is able to support the quality of a service in a service-agnostic way. The second parameter class relates to the media-dependent characteristics of a given service. Audio and video are the types of media that are taken into account as well as the processing of these media for the transmission in a given service. The parameters of both classes can influence each other and their combination very likely will have an impact on the user-related experience of an end-to-end service quality.

6.1. Architectural scenario

Packet-switched networks consist of a series of exchange points that are interconnecting the domains and networks of several network and service providers which makes the prediction of a certain quality level for a service more unpredictable than in the case of a network and a service that is run by a single provider.

Taking into account that future-proof services will run in a full IP environment, IMS is the architectural framework for delivering IP-based services. This framework makes use of the IPX model as it is described in section **Errore. L'origine riferimento non è stata trovata.** for guaranteeing pre-defined levels of quality for a given service in the environment of interconnectivity and roaming.

Following these premises, the reference architecture for QoS control and monitoring looks as follows:

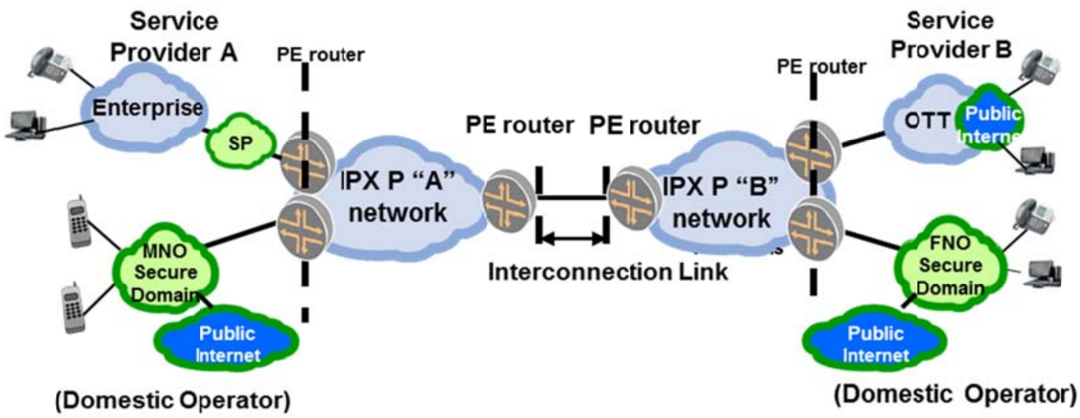

Figure 1 - QoS Reference Model

It depends on the business contracts between providers and also on associated SLAs whether the monitoring of quality parameters is done in a single provider's network or across a chain of successive networks that in the extremum can extend to an end-to-end quality monitoring.

The definition of any specific commercial agreement associated with SLAs and/or QoS reporting is outside the scope of this document.

6.2. Identification of KPI parameters

After having set the requirements for the quality of a service, network and service providers need to define a set of Key Performance Indicators (KPIs) that are used to benchmark and to monitor the quality aspects of a service. KPIs specify what parameter is measured and accompanying assessment techniques detail how and when it will be measured. The description of these assessment techniques is outside the scope of this document but where appropriate references are given. KPIs have to result in quantifiable measurements that reflect the quality of service to be evaluated, however, they almost always require qualitative analysis to support their interpretation. These parameters are thought to support monitoring purposes against pre-set thresholds, for the checking of SLA compliance and for QoS reporting.

The KPI descriptions given in the following two clauses are classified according to the layer they are used for. For this paper transport-related methods are media-agnostic and concentrate on quality parameters related to the IP layer. Service-related methods and their functionalities take into account the media characteristics of a service. Depending on the usage scenario and on the characteristics of a KPI, a method can be used to aim to local significance or to an end-to-end evaluation.

6.3. Transport-related methods

6.3.1. Round-trip delay

The round-trip delay time of a signal is the period it takes for a signal to be sent to a specified destination plus the period to receive some acknowledgement for this signal at the originating site of the signal. Therefore, this delay time describes the propagation times between two points in a network and is very often taken to evaluate the throughput rate in interactive bi-directional communications. In IP-based networks the Ping command, integral part of many operation systems, is very often used to test the ability of a source to reach a specified destination.

6.3.2. Jitter

In IP-based networks data is sent using data packets of equal lengths and these data packets are normally sent out in equal intervals. Due to changes in the network architecture or influenced by the inclusion of new network devices, these intervals can become disrupted and the delay between adjacent data packets can vary. Jitter is defined as the variation in delay of received data packets.

6.3.3. Packet loss

In IP-based networks data packets can be lost in transit, they can be dropped for network congestions reasons or they may be corrupted in such a way that they are no longer available for their intended purpose. Data packets, they may be lost or corrupted, are classified as lost packages. The ratio between the total amount of lost packages and the total amount of sent packages in a given period is called packet loss.

6.4. Service-related methods

Service-related methods take into account the characteristics of the communication media to be transported in IP-based networks. Some of these methods are only applicable to voice services, other ones to audio-visual services consisting of related audio and video data.

6.4.1. Average Length of Conversation (ALOC)

This method is applicable to voice services as well as to audio-visual services. The average length of conversation is measured for completed calls only. Significant variances in values when measured on different routes to the same destination can be a hint for irregularities. A description for setting up the measurement using the SIP- or the SIP-I protocol is given in [12]. A list of factors that can impact this parameter is given in [13].

6.4.2. Answer Seizure Ratio (ASR)

This method is applicable to voice services as well as to audio-visual services. The answer seizure ratio expresses the relationship between the number of seizures that result in an answer signal and the total number of seizures. It is a direct measure of the effectiveness of the service being offered. A definition of this parameter and a list of factors that can impact it are given in [13]. A description for setting-up measurements using the SIP- or the SIP-I protocol is given in [12].

6.4.3. Network Efficiency Ratio (NER)

This method is applicable to voice services as well as to audio-visual services. This method is designed to express the ability of networks to deliver calls to the far-end terminal. This ratio expresses the relationship between the number of seizures and the sum of the number of seizures resulting in either an answer message, or a user busy, or a ring no answer. Its relationship to ASR is specified in [14]. A description for setting-up measurements using the SIP- or the SIP-I protocol is given in [12].

6.4.4. Post Gateway Ringing Delay (PGDR)

This method is applicable to voice services as well as to audio-visual services. It expresses the time between a request for a call setup and the alerting signal for that call. A description for setting-up measurements for calculating the value of this method is given in [12].

Note: PGRD is preferred over PGAD (Post Gateway Answer Delay) because the latter depends on the end-user behavior.

6.4.5. Speech quality assessment in narrow-band telephony application

This method is only applicable to speech services that make use of narrowband speech signals. The algorithm described in [15] works single-sided and does not need a separate reference signal. The speech signal has to be narrow-banded and it has to fulfill the requirements specified in section 6 of ITU-T Rec. P.563 [15] but it can be of any nature. Therefore, also decoded speech is allowed to be evaluated. The algorithm delivers a MOS value on a 1 to 5 scale.

NOTE: An extension of this method to be used for wide-band telephony applications is currently under development in ITU-T SG12.

6.4.6. Parametric non-intrusive bitstream assessment of video media streaming quality

This method is only applicable to video services making use of the H.264 video coding scheme as recommended to be used in [16]. Many assessment methods compare quality-related parameters of an unprocessed video stream to the parameters of the same video stream after its processing. Taking into account that in nowadays' networks an unprocessed video stream is very unlikely to be available, an algorithmic model has been developed which does not need the reference of an unprocessed video stream. This method is described in ITU-T Rec. P.1202-2 [17] and it delivers a MOS value in the range of 1 to 5.

6.4.7. Audiovisual QoS for communication services

This method is applicable to audiovisual services making use of the H.264 video coding scheme as recommended to be used in [16] and taking into account the mutual influence of audio and video. The method as described in ETSI ES 202 667 [18] does not automatically deliver a MOS value but offers several manual calculation possibilities for evaluating the quality of audiovisual communication depending on context and usage scenario. The appropriate model has to be selected by the service provider.

6.5. Technical enablers for QoS Management

6.5.1. CLI Management

For the management of IMS services the Calling Line Identification (CLI) is a key requirement for roaming, charging and operational practices. It is the intention of the CLI to transmit a caller's telephone number to the called party's telephone equipment when the call is being set up. Whether this service can be successfully presented to the callee depends on the service capabilities of the involved operators. If this service is supported in an international IMS environment, it is mandatory that international IPX Providers (see Figure 1Figure 1) will pass on the CLI unaltered. IPX Providers, under normal operational conditions, are not expected to check CLI validity. An IPX Provider cannot guarantee that:

- the CLI will be transmitted by the originating Service Provider;
- the CLI received from the originating Service Provider is a valid value, i.e. a value of a CLI owned or ported to Service Provider, and indeed, is the correct CLI for the calling party;
- the CLI forwarded to an interconnecting IPX Provider will be delivered to the terminating user, or delivered without any error being introduced beyond the interconnecting IPX Provider;

Call should never be rejected with "no-CLI", instead, a surcharge if possible can be applied by the terminating party.

6.5.1.1. CLI Privacy

As a communications provider, International Carriers have privileged access to CLI. The three privacy markings in SIP used to satisfy data protection requirements are:

a. Available – where the CLI can be used for display purposes;

The recommended SIP message in this case will have the below format:

From: <sip: +447584123456@domain; user=phone>
P-Asserted-Identity: <sip: + 447584123456@domain; user=phone>
Or
From: <sip: +447584123456@domain; user=phone>
P-Asserted-Identity: <sip: + 447584123456@domain; user=phone>
Privacy: none

b. **Withheld** – where the caller has exercised the possibility of preventing the display of CLI information, therefore the CLI is present but classified restricted;

The recommended SIP message in this case will have the below format:

From: <sip: + 447584123456@domain; user=phone>
P-Asserted-Identity: <sip: + 447584123456@domain; user=phone>
Privacy: id; user
Or alternatively the following format is permitted:
From: <sip: anonymous@anonymous.invalid>
P-Asserted-Identity: <sip: + 447584123456@domain; user=phone>
Privacy: id

c. Unavailable – where, at any point in the end-to-end conveyance of a communication, it is not possible:

- o to offer End-User privacy choices and ensure that they are respected
- o to display the caller's CLI information that is prevented by Communications Providers in order to preserve the anonymity of a caller's Network Number when a Presentation Number is available.

The recommended SIP message in this case will have the below format:

From: <unavailable@anonymous.invalid>
P-Asserted-Identity: <sip: @domain; user=phone>
Privacy: id

In TDM networks CLIP and CLIR have been standardized with the following meanings: CLIP will represent the CLI is available to be displayed; CLIR will represent the caller ID was restricted from display.

6.5.1.2. CLI Presentation

IPX Providers can ensure that a CLI received is always passed on unmodified across their own domain except in the case to change CLI from national format to international format. A CLI in SIP would normally be in the format specified in section **Errore. L'origine riferimento non è stata trovata.**, so no change of format would be necessary. IPX Providers can also have specific agreements with other interconnecting IPX Providers in order to guarantee CLI transparency.

The same principles apply in case of adoption of SIP-URI addressing format (see section **Errore. L'origine riferimento non è stata trovata.**).

In recent years Origin Based Charging principle has been adopted by wholesale industry in some regions. It follows that correctness of CLI affects also charging between operators and lack of clear definition for valid CLI may lead to disputes between them.

In this regards, a valid CLI is defined as:

- It is transferred through P-Asserted Identity SIP header, according to RFC 3325 [55]
- It is one which complies with the format set out in the ITU-T numbering plan E.164, meaning that "+" and "Country Code" have to be included in CLI and no national significant numbers are considered as valid CLI
- It has been designated as available for use in the Numbering Plan of the country it belongs to
- Should P-Asserted Identity SIP header be unavailable or not compliant to ITU-T numbering plan E.164, From SIP header can be used to determine CLI only for presentation purposes but not for Origin Based Charging

The recommendation for the SIP presentation rule is the following:

> If PAI is present and it is a valid E.164 number, this could be used for presentation by end network; IPX provider handing over traffic to an end network could agree to meet interworking requirements of the end network.

Calls without a CLI, with invalid CLI, with manipulated CLI could be invoiced at the highest rate by the terminating carrier.

6.5.1.3. VoIP to TDM interworking considerations

Reference ITU recommendation for VoIP-TDM interworking is ITU-T Q.1912.5 [59]. This recommendation provides guidelines on SIP to BICC/ISUP interworking and viceversa. In particular, it specifies how incoming SIP signalling has to be mapped to ISUP. For this interworking scenario, there can be two cases affecting CLI definition:

1. The call signalling has a well formed P-Asserted-ID (PAI) header. In this case the ITU recommendation states that SIP PAI header has to be mapped to the ISUP Calling Party Number
2. The call signalling has no well-formed P-Asserted-ID (PAI) header. In this case ITU recommendation leaves room for interpretation since it states that it is a network option to either include a network provided E.164 number or omit the Address Signals of Calling Party Number.

As far as scenario 2 is concerned, recommendation is to omit Address Signals of Calling Party Number regardless of From header content. The rationale behind this recommendation is that for Origin Based Charging P-Asserted-ID is the only SIP header transferring valid CLI information.

6.5.1.4. P-Asserted-ID URI considerations

P-asserted-ID header may contain either Tel URI or SIP URI. For CLI identification pourposes multiple P-Asserted-ID headers should not be used unless there is a P-asserted-ID containing Tel URI and/or a P-asserted-ID containing SIP URI and user=phone. In this case both type of URIs must contain the same phone number. If none of the above exist and contain a valid E.164 number, CLI will not be considered valid and call could be invoiced at the highest rate by terminating carrier.

6.5.1.5. CLI management in case of diverted calls

In case of a diverted call, headers involved in CLI identification are either Diversion header or History info in SIP domain, Redirecting Number in the ISUP domain.

Since Origin Based Charging has been adopted, CLI identification has a meaning not only for presentation but also for applying different rates according to the origin of the call.

In a diverted call, that is A number calling B number with a diversion service to C number, looking into the B to C leg, these are the headers that identify each origin related number:

- A number: From and P-Asserted-ID (SIP), Calling Party Number (ISUP)
- B number: top most Diversion or History-Info Header (SIP), Redirecting Number (ISUP)

So considering the B to C leg an operator needs to decide which is the correct CLI for presentation and for Origin Based Charging purposes.

Recommendation for presentation is to use A number, following the same rules previously described in this document.

Recommendation for Origin Based Charging is to use B number, since in case receiving a diverted call B number represents the actual incoming path.

The impact of this recommendation on Origin Based Charging varies depending of the combination of A and B numbers and the final destination of the call.

6.5.2. Traffic classification

In compliance with GSMA IR.34 Sec. 6.2.5 [20], IPX Providers are committed to managing IMS-based traffic considering traffic classes according to the QCI value received from the service providers.

For voice services as well as for audiovisual services, this implies the management of the packetized traffic as Conversational Service applying the Diff. Serv. PHB code “EF” (Expedite Forwarding) equivalent to the DSCP code “46” (in decimal base).

6.6. Technical implementations of quality requirements

6.6.1. Measurement of QoS parameters

The above described scenario and the accompanying requirements call for the ability to measure the identified transport parameters across two specific network domains (see Figure 1 above). It should also be possible to analyze the call flow in order to locate and isolate faults. As of today, service and IPX providers make use of their own existing methodologies and measurement capabilities within their domain but there is no implementation of any standardized aggregation scheme or report system to send quality reports back to the originating service provider. As a result, there is no applied methodology for assessing values of QoS parameters end-to-end (i.e. from the first piece of equipment in the IPX Provider`s network facing the originating Service Provider, to the last piece of equipment in the Carrier`s network facing the terminating Service Provider).

6.7. KPI computation for SLA / QoS reporting

Whatever the definition of a specific QoS parameter and its measurement process, the KPI of this parameter has to be estimated at the operational level by means of a series of measures that generate statistical samples. These samples, properly computed in accordance to a selected statistical function, give the requested KPI.

The following measurement scheme is proposed. Let:

- T be the reporting period (e.g. T = one month)

- i be the index of the suite of measurements by the Border Function and/or probes and/or Call Handling Function (as applicable)
- KPIi be the measured value of the i-th sample for the considered KPI (e.g. RTD)
- N be the number of measurements over the period T (i=1..N)

The generic KPI is computed as a function of all the measured "N" samples $KPI = f(KPI_1, KPI_2, \ldots, KPI_N)$.over a time period, the length of which is outside the scope of this document.

The following functions are suggested:

- *RTD: 95 / 99 % percentile or average*
- *Packet loss: 95 / 99 % percentile or average*
- *Jitter: 95 / 99 % percentile or average*

As far as the market practices are concerned, it has to be noted that, from a commercial perspective, the statistical function "average" is the preferred option in most of the cases.

Very often QoS measurements will be done independently in concatenated network sections and then the question arises whether the performance levels of these network sections can be used as an estimation for an end-to-end performance. Such an estimation is possible under the condition that the distribution function of the measured values is known which is normally not the case. However, for the estimation of an overall delay it can be assumed that the measurements done in the network sections were done statistically independent from each other and the values measured follow a normal distribution. In this case, the overall delay can be estimated as the sum of the average values calculated for each network segment.

With reference to the equipment and systems to be used for carrying out these measurements, a number of technical options are available on the market, encompassing external probes as well as internal testing routines to be launched by network elements. Additional Business Support Systems are required for the statistical post-processing computation.

6.8. Managing QoS

6.8.1. Managing QoS at the commercial level

As a general principle, each IPX Provider can offer KPIs of QoS parameters according to its own commercial policy. As a result, each IPX Provider is free to select the QoS parameters subject to QoS Control and Monitoring as well as the related configuration parameters of the operational process for collecting data (statistical samples) in order to produce the KPIs.

6.8.2. Managing QoS at the operational level

There are two possible general methods for QoS control and related SLA enforcement:

a) *SLA enforcement through fault management*

A QoS problem is raised upon SP Customer request claiming a QoS degradation by opening a trouble ticket with its serving IPX Provider. The IPX Provider (IPX P_A) and the SP will then work together to verify if there is an end-to-end QoS fault. In such a case, IPX P_A will start troubleshooting within its own network and, in the event that no cause of degradation is detected, it passes downstream (cascading) to the interconnected IPX P (IPX P_B) the task of solving the problem. If the problem is identified, and if the repair duration is above the limits set in the SLAs, then the IPX Ps must pay the penalties negotiated in the contract.

b) *Enforcement through constant monitoring and reporting of KPI values*

In this option, an IPX Provider constantly measures the QoS in its network (e.g. RTD, NER) and reports these values to its customers; for example, on a monthly basis. This last option can be very difficult to manage and not fully scalable for hundreds of routes. This solution is only optional and it is up to each IPX Provider to decide to offer it for one or several routes.

In reality, regarding both operational and commercial QoS, an IPX Provider acts both according to methodology a) and b) above, aiming to maximize QoS performance, while optimizing operational efforts.

An SLA can foresee penalties in case that the agreed QoS levels are not met by the contracted IPX Provider.

7. Security Management in an IMS environment

The engagement between two or more parties in a communication is always a source of risk for the involved parties, and potentially even for other not directly involved parties. Risk is inherent to any activity and should be dealt with through a combination of measures and processes to avoid or, at least reduce, it.

IMS services are the evolution of the core services of FNOs/MNOs platforms; as such their security is critical. As of today they are offered by a very narrow set of Service Providers which expect the interconnection to be performed in a secure and trusted environment, in the same way the legacy services were. IMS Services have associated important money flows; they are therefore prone to suffer attacks and fraud. All parties involved in IMS Services should understand that it is their responsibility to participate in the security of these services.

The discussion that follows separates the topics related to the security at the transport IPX layer from the threats and actions to be carriers out at the service layer.

7.1. Security at the transport layer

Please make reference to the activity and deliverables of i3 forum *"IMS-Based Services: Network-Network Interface Definition"*, Rel. 1, May 2017, [1]).

Many different threats, vulnerabilities, attacks can be carried at the service layer. For the sake of easy presentation the following categories have been identified:

- Volumetric attacks
- Protocol attacks
- Authentication
- Encryption, Integrity and Privacy
- Fraud

7.1.1. Volumetric attacks

Volumetric Distributed Denial of Service (DDoS) attacks are also known as floods. DDoS attackers seek to overwhelm the target with excessive data, often gained through reflection and amplification DDoS techniques. Volumetric attacks seek to make use of as much bandwidth as possible.

These attacks are quite common in the VoIP space, and the most common form of DDoS attack is a crafted DDoS attack. This attack involves bombarding the IBCF (or as commonly known SBC, Session Border Controller) with a large quantity of packets. These packets are expertly crafted to force the SBC to devote a large portion of its resources to processing them. Attacks of this type include SIP packets, which require heavy-duty parsing by the control plane CPUs, and TCP SYN packets intended to exhaust all the TCP listen ports on the SBC.

Volumetric attacks can also be performed in combination with IP spoofing techniques. It follows that IBCF can be bombarded with a large quantity of packets having a "spoofed" source IP address that belongs to an interconnected partner/network and containing "fake" SIP INVITE requests. The attacked IBCF could then manage these SIP INVITE requests as regular session bids, thus leading to IBCF resources overload.

7.1.2. Protocol attacks

Most common form of protocol attacks originate from deliberately manipulated SIP messages. This attack involves the usage of a field name or value in the protocol header that is RFC compliant, but deviates from normal use. Examples of the attacks might include using field values which contains hundreds of characters where less than a dozen is expected. These protocol attacks using SIP messages make SIP applications vulnerable to attacks that flood servers with huge quantities of fraudulent data, eventually overwhelming the server. Protocol attacks can also result in buffer overflow conditions, which may result in arbitrary code execution.

These attacks can be handled by an SBC with a high degree of flexibility in message manipulation, when encountering a “fuzzed” message. Most importantly, the degree of flexibility in inspecting and manipulating the messages should not affect the SBC’s ability to process legitimate flows, in fact the SBC must still be able to achieve its rated load when performing this essential function.

To protect against this type of attack, SBCs need to be able to fix the malformed SIP / SDP. Furthermore, the mechanism to fix the malformed protocol needs to be flexible enough to defend against new attacks, without costly code enhancements.

7.1.3. Authentication

The most common authentication attacks come from not being able to keep up requests from compromised or malicious IP addresses attempting to penetrate your IP/IMS network. As an SBC is typically deployed at the network’s edge, SBCs are usually the first line of network defense. It expects malicious activity to originate on its untrusted interface.

SIP uses a challenge and response mechanism. If a request contains incorrect or no authentication information it will be challenged by a "*401: Unauthorized*" response. The request must then be resent with the correct authentication details.

The IMS architecture uses authentication to police access to the IMS services. The initial SIP REGISTER is authenticated to verify the user’s identity and establish a binding between that identity and the device that the user is using. The nature of that binding can vary depending on the capabilities of the device and the IMS network itself.

7.1.4. Encryption and Integrity

Though it is highly desirable an IPX platform is separated from the Public Internet (see Sec. 4 and Sec. 9.1), it is very well known that some access/interconnection links could exploit Public Internet resources. In addition, IP media packets travelling over the Internet are sent as completely open packet stream. As a result, media conversations are sent as RTP streams of data not encrypted or protected in any way and anyone having access to the underlying network can listen in on those conversations.

On top of being able to spy on voice packets, it’s also possible for a malicious device to inject additional content into the messages, or adjust the message. This could be executable code that is used to gain root access to your system and completely compromise it.

Security experts have tackled these two problems in parallel, with encryption and integrity checks. Encryption ensures that only trusted recipients can read the contents of the message; integrity checks ensure that the recipient can be confident that the message was sent by the expected sender, without tampering.

However encryption and integrity schemes cannot run end to end because the devices in the network core need to be able to inspect and modify the messages. A device is required to interwork between the insecure outside and the secure core of the network. That device is the IBCF functional block using the IMS terminology or SBC using the common network terminology.

There are various schemes available to operators, although none have got widespread adoption:

- *TLS (Transport Layer Security) can be used to encrypt the signaling*
  - It runs over TCP on a per-port basis and is negotiated when the TCP connection is set up.
- *IPsec can be used to encrypt signaling or media*

- It runs at the IP layer, below the transport protocol.
- It can be negotiated in two ways – IKE (Internet Key Exchange) and IMS-AKA (Authentication and Key Agreement).
  - IPsec is negotiated via IKE during system initialization.
  - IMS-AKA negotiates in SIP registration message exchange.

- *SRTP is used to encrypt RTP packets*
  - There are a variety of schemes, but the most common is to exchange keys in the SDP of a session set up using TLS.

The correct scheme to use depends on a couple of factors.

- *Access or interconnect?*
  - Interconnect SBCs have a low number of trunking connections with a high volume of traffic.
  - Access SBCs have a large number of connections to access devices each of which handles a low volume of traffic.
- *Signaling or media?*
  - Signaling is used to set up calls. It consist of variable sized, large messages that can be sent at any time.
  - Media consists of a much larger volume of packets, which are often small. They can only be sent when a call is set up.

In interconnect scenarios it is expected signaling to use TLS or IPsec, and media to use IPsec. The IPsec encryption is often performed by downstream routers from the SBC, to reduce encryption demands on the SBC.

The access scenario is outside the scope of this document.

7.1.5. Fraud

Please make reference to the activity and deliverables of i3 forum *"Fight Against Fraud Working Group"*.

7.2. Incident Response

It has already been discussed that the security of the IPX domain is a task involving the cooperation of all interconnected parties. This applies not only to the prevention of security breaches, but also to the response in case such a breach is detected.

All participants in the IPX domain shall define at least the following:

- Personnel in charge of determining, investigating and solving security breaches;
- Personnel responsible for mitigating security breaches;
- The assignment of contact persons for notification of security breaches;
- A process for handling security incidents.

8. VoLTE roaming scenarios

In existing circuit switching (CS) mobile systems, two basic roaming schemes have been adopted (OMR scheme, though specified, has presently no implementation in the market):

a) *Via Visited PMN routing* (or local break-out): the visited network routes voice calls for inbound roamers directly to the requested destination network. The VPMN is responsible for all wholesale costs associated with the termination charges for routing those calls. The HPMN is then charged per minute for the usage of the VPMN network including the wholesale termination costs when applicable;

b) *Via Home PMN routing*: in this case the visited network has an agreement with HPMN to use CAMEL triggers hence the HPMN has the possibility to retrieve the call (signaling and media) on its own network and then terminate the call.

Since the early beginning of mobile communications, the mobile community has been adopting these roaming schemes for all CS mobile systems and the reasons for this wide adoption are:

- they are service aware: all involved networks (HPMN, VPMN and Int. Carrier(s) know via signalling that a voice call has to be terminated);
- the related signalling protocols (SS7 and CAMEL) are worldwide accepted standards;
- the standard voice business model is retained: the calling party pays with a deterministic charging scheme based on destination and call duration;
- for most call scenarios, the call routing can be optimised to follow the shorter path to the destination network.

It is worth outlining that in the CS environment, from the Int. carrier/IPX Provider perspective; two different and distinct services are offered to MNOs: an international voice service for terminating the call and a signaling service.
In a VoLTE IP-based scenario, the above well-established paradigm has been put under question in the GSMA and two scenarios have been approved:

a) *Service aware option: LBO HR or Ravel* based on SIP IMS signaling being managed by all networks in the call chain and assuming the same business model of the CS scenario; and

b) *Service unaware option: S8HR* based on a data connection, exploiting the data layer of the LTE networks (S8 interface of Evolved Packet Core) from the Visited up to Home network where the IMS Core is located. Some issues are still under discussion and details are given in the section 10.2 below.

The remainder of section 10 shortly discusses the two options as well as offers a statement which aims to present the i3 forum position on this debate.

8.1. Service aware roaming option

This model has been already specified by GSMA in IR.65 “IMS Roaming and Interworking Guidelines Version 15.0” October 2014 [21] and it is based on the SIP IMS signaling for allowing the exchange of information between VPMN, Int. Carrier/IPX Provider, HPMN both on the originating side and the terminating side.

The technical specification has been developed by 3GPP in the document TR 23.850 [22] which has been conceived and designed with the objective of replicating the 2G/3G business model and related charging scheme. Considering that in IMS, the call control is performed by Serving – CSCF and the service policies are located in the Telephony Application Server, 3GPP worked out the LBO model which encompasses two cases:

a) Service aware VoLTE model via HPMN routing (LBO HR according to GSMA terminology)

b) Service aware VoLTE model via VPMN routing (LBO RAVEL according to GSMA terminology)

From the International Carrier/IPX Provider perspective, the support of this VoLTE roaming model implies the need to support the SIP IMS signaling profile (see Sec. 7) and specifically, the support of the SIP Route header and OMR parameters in order to correctly forward the signaling information towards the Home Serving-CSCF according to the RAVEL scenario.

In addition, while in 2G/3G there might be the case where no CAMEL agreement is in place between the two MNOs and all calls are necessarily routed by VPMN, in VoLTE, since in any case the signaling information goes back to HPMN, the Home network can decide <u>on a call-by-call basis, whether to route the call to its destination via its own network or to leave this task to the VPMN</u>. This implies that, in the case that the HPMN of the calling party roamer opts for a VPMN routing, the managed SIP IMS signaling information has no associated media in the segment between the VPLMN and HPLMN. From a commercial standpoint, today's clear distinction between a voice service and a signaling service disappears.

8.1.1. Service aware VoLTE roaming call with HPMN routing

In this case, the Home PMN retains full control of call routing and signaling, and media follows the same path. In terms of latency, in case of calls not terminating in the HPMN or in a PMN of the home country, the delay could be significant especially when intercontinental routes are involved.

Figure 13 depicts the signaling and media paths, showing the main IMS functional blocks involved.

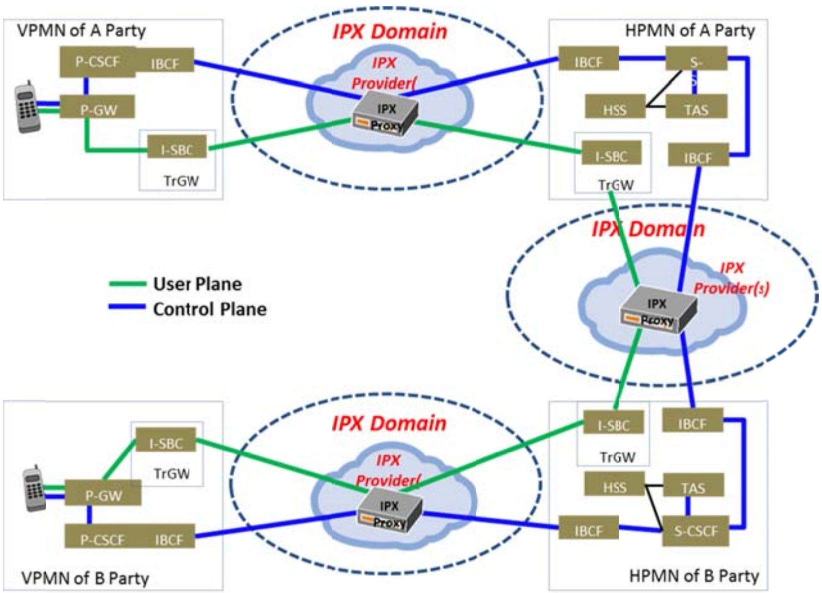

Figure 13 - Service aware roaming model with Home PMN routing

8.1.2. Service aware VoLTE roaming call with VPMN routing

In this case, the Visited PMN, after exchanging information with the HPMN, is responsible for call routing. This scenario is the closest to the present 2G/3G roaming model and requires the support of Int. Carriers / IPX Providers in case the call has to be terminated outside the VPMN or the VPMN's country.

The media path can be optimised, and there is clear distinction of the signalling path.

Figure 14 depicts the signaling and media paths, showing the main IMS functional blocks involved.

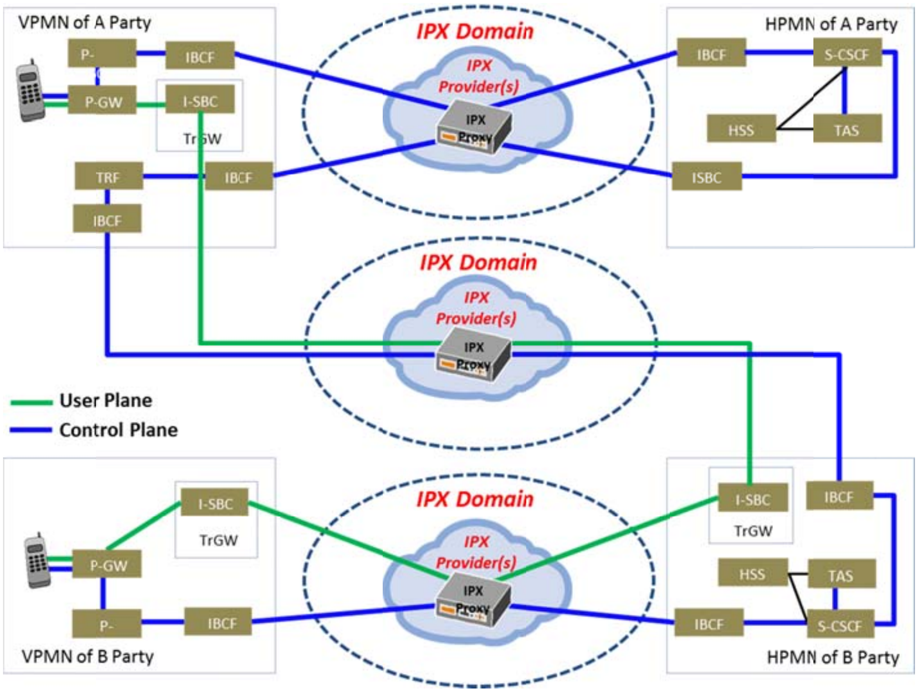

Figure 14 - Service aware roaming model with Visited PMN routing

8.2. Service unaware S8HR (via S8 interface) roaming option

In the Summer of 2014, GSMA launched a task force named Revolver whose aim is to assess the feasibility and suitability of some LTE roaming models. In addition to the service aware models described in the previous section, Revolver recommended to consider a new scheme based on a roaming data connection (service unaware).

This architecture is defined by:

a. VPMN and HPMN are interconnected by a data channel (e.g. IPX Transport) where specific QCIs are provided in the Radio Access network and then mapped to the expected DSCP / Traffic Class in the Core and Transport networks; the S8 interface is used between the two LTE Evolved Packet Cores;
b. this data path encompasses both signaling and media without service awareness on the transport networks;
c. the VPLMN supports all 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;
d. 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 [4], Section 6A and 7, for more details;
e. HPMN of the calling party has the full control over routing to the destination and is responsible for any interconnect fees associated with call delivery;
f. given that the transport between VPMN and HPMN is service unaware, the HPMN IMS provides a UNI interface to the calling party, thus an EPC interworking is needed between VPMN and HPMN; and as a result, the VPMN is not service aware;
g. Both signalling and media use same IMS APN established with the HPLMN, each with specific QCI as defined in GSMA PRD IR.92 [23] and IR.94 [24];
h. once signaling has reached the HPMN, it makes use of standard IMS SIP signaling when routing the call towards the destination network. In case the terminating party is in roaming, a new data path is generated between the terminating HPMN and the terminated VPMN.
i. The PCRF framework of the HPLMN is used. QoS rules are generated in the HPLMN and enforced by the VPLMN as per roaming agreement.

From the technical standpoint, there are still a number of open points on how to guarantee emergency calls and lawful intercept in compliance with the different regulations, and in terms of latency, the same considerations already given in sec. 10.1.1 for the service aware Home routing model apply: it could imply a longer transmission path than a VPMN routing. It is up to HPLMN how to implement Lawful Intercept functions, and 3GPP TS33.107 [10] captures possible LI architecture options. Despite those open points S8HR is strongly pushed by many operators to accelerate VoLTE Roaming deployment and as IPX providers, Carriers will need to support both options.

Figure 15 depicts the signaling and media paths showing the main IMS functional blocks involved.

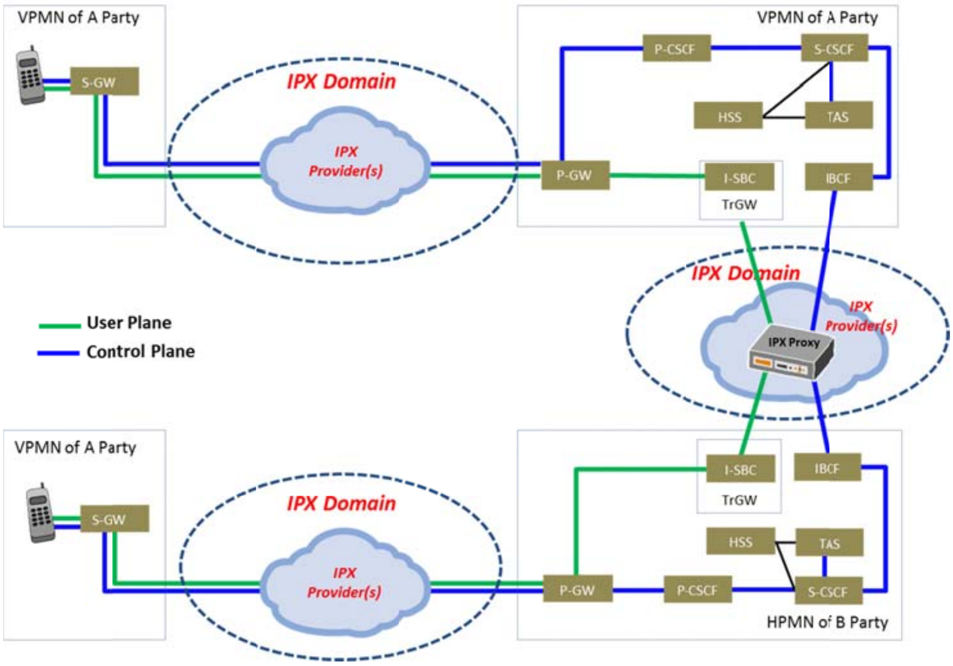

Figure 15 - Service unaware roaming model based on S8 Home Routing

From the commercial perspective this model has been proposed and supported by MNOs who have already launched LTE services and like to offer roaming services to their own subscribers without waiting for an IMS implementation in the visited network.

In terms of the business model, it clearly marks a difference with respect to the existing 2G/3G roaming scheme, moving from voice to a data service, where charging is based on volume (packets) rather than duration (minutes). There is no firm commercial guideline in the market, but technically, it requires that MNOs are capable to properly distinguish this roaming traffic (different APN and different QCI management) as well as necessitating that IPX Providers have the capability to properly charge differentiated quality IPX transport service.