International Interconnection forum for services over IP (i3 Forum)

(www.i3Forum.org)

Source:
Workstreams “Technical Aspects”, “Service Requirements”
Keywords: Voice over IPX

“Voice over IPX Service Schedule”

(Release 1.0, May 2013)

Revision history

Date	Rel.	Subject/Comment
May 12th 2013	1.0	First release of the Voice over IPX service schedule replacing previous i3 forum Voice over IPX documents

Executive Summary

The IPX model, as defined by the GSMA, is an international, trusted and QoS controlled IP backbone, consisting of a number of competing carriers (IPX Providers) that interconnects Service Providers according to mutually beneficial business models. The objective of this document is to provide a service and technical architecture that allows Service Providers and IPX Providers to enable a productive IPX business model. This document defines how the following requirements can be fulfilled.

- Service Providers (MNO, FNO, ASP, ISP, OTT Provider): Providing guaranteed service quality, reliability and security for IP-based service delivery with other Service Providers in the IPX ecosystem.
- IPX Providers: Allowing for technical and economical efficiencies while providing IPX-based services to Service Providers.

This document addresses specific aspects related to a Voice over IPX (VoIPX) service. Principles and features common to all IPX networks are described in the IPX Core document.

A VoIPX service is a high-quality voice service based on an IPX domain consisting of IPX Providers networks. It confirms IPX concepts such as security, cascading and Service Provider to Service Provider responsibility. VoIPX calls shall remain within the IPX domain unless a break-in / break-out connectivity is agreed with Service Providers in order to achieve a global connectivity. An IPX Provider has to disclose the type of connectivity used to reach each terminating SP (direct, indirect, break-out).

VoIPX service can be offered in transit or hubbing business models.

Table of Contents

1 Scope and Objective of the document

This document is the Service Schedule for the Voice over IPX Service. As such it replaces, jointly with the “Common functionalities and capabilities of an IPX platform” document, the previously published by i3Forum “Technical Specifications for Voice over IPX service”.

The IPX model, as defined by the GSMA is an international, trusted and controlled IP backbone that interconnects Service Providers (SPs) according to mutually beneficial business models. It is designed to offer highly efficient and commercially attractive methods of establishing interworking and roaming interconnection arrangements for IP services.[8] The IPX environment consists of a number of IPX Providers (IPX Ps) in competition, selling interconnect services to SPs. The IPX Ps’ networks are mutually interconnected where there is demand by SPs.

In line with market trends—which call for reliable, trusted, secure and quality controlled international voice service—i3 Forum endorses such a service evolution and releases this document as the third version of the implementation specification for the voice service within the framework of IP Packet Exchange (IPX) model conceived and specified by GSMA [8].

In the above scenario, the following needs/requirements can be recognised for the provision of voice over IPX services:

From Service Providers, as the entity offering services to final users, needing guaranteed quality (reliable and secure) IP-based services towards corresponding (terminating) Service Providers, using modular and transparent interconnection and functions provided by IPX Providers, in a global private network, and

From Carriers (IPX Providers), as the entity offering interconnection services, serving any IPX compliant SP at the proper level of technical and economic efficiency by means of the designing, implementation and operation of multi-service converged platform(s) for all types of IPX services,

with the common objective to implement a service and technical architecture that is business-sustainable for both Service Providers and Carriers.

Consequently, the IPX would result in an evolution of the existing architectural model for voice, implying the transition from present local, mono-service (voice) interconnection model, towards a multi-service, converged, global, functionally-layered interconnection model.

This document, assuming and endorsing the basic GSMA technical / commercial requirements:

- focuses from the business perspective on the Multilateral Hubbing connectivity mode;
- provides a set of specifications which can be implemented achieving the basic requirements of GSMA IPX model for areas such as IP routing, signalling, media, security, quality of service control and service routing;
- differentiates from current GSMA specification on some specific topics which have been matter of analysis and study between MNO representatives and i3 Forum carriers in the past years.

As a result, this implementation specification document should not be considered as an alternative architecture with respect to the GSMA IPX model but as a carriers’ contribution devoted to provide a detailed technical guidance for the implementation of the Voice over IPX service.

Services offered via private interconnection and/or via the Public Internet remain a technical and commercial option outside the IPX environment, as per i3 Forum specifications [2], and Service Providers/Carriers are free to request/offer Internet-based services according their own policies.

The content of this document is based on the latest available version of the GSMA IPX specification. i3 Forum is ready to update the content of the document in next releases following the GSMA specification updates.

2 Acronyms

3GPP	3rd Generation Partnership Project
ACM	Address Complete Message
ALOC	Average Length Of Conversation
AMR	Adaptive Multi-Rate
AMR-NB	Adaptive Multi-Rate Narrow Band
AMR-WB	Adaptive Multi-Rate Wide Band
ANM	Answer Message
AS	Autonomous System
ASR	Answer Seizure Rate
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BSS	Business Support System
CBC	Cipher Block Chaining
CC	Country Code
CDR	Call Detail Record
CHF	Call Handling Function
CIN	Calling Party's Number
CLI	Calling Line Identification
CN	Comfort Noise
CSMA/CD	Carrier Sense Multiple Acces/Collision Detect
CUG	Closed User Group
DES	Data Encryption Standard
Diffserv	Differentiated Services
DNS	Domain Name Service
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
DTX	Discontinuous Transmission
EF	Expedited Forwarding
EG	ETSI Guide
ENUM	E.164 NUmber Mapping
ETSI	European Telecommunications Standards Institute
FNO	Fixed Network Operator
FoIP	Fax over IP
GIC	Group Identification Code
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSM	Groupe Speciale Mobile
GSMA	GSM Association
GSN	Global Subscriber Number
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IC	Identification Code
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFT	Internet Facsimile Transfer
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPIA	IP Interworking Alliance
IPPM	IP Performance Metrics
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	IP eXchange
IPX P	IPX Provider
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunications Union
KPI	Key Performance Indicator
MAP	Mobile Application Part
MIME	Multipurpose Internet Mail Extensions
MNO	Mobile Network Operator
MoIP	Modem over IP

MOS	Mean Opinion Score
MOS_{CQE}	Mean Opinion Score, Communication Quality Estimated
NDC	National Destination Code
NER	Network Efficiency Ratio
NGN	Next Generation Network
NNI	Network to Network Interface
OSS	Operations Support System
PE-router	Provider Edge router
PGAD	Post Gateway Answer Delay
PGRD	Post Gateway Ringing Delay
PHB	Per-Hop Behaviour
PLMN	Public Land Mobile Network
P-router	Provider router
PSTN	Public Switched Telephone Network
PT	Payload Type
QoS	Quality of Service
REL	RELease
R-Factor	Rating-Factor
RFC	Request For Comments
RR	Receiver Report
RTCP	Real Time Control Protocol
RTCP XR	Real Time Control Protocol eXtended Reports
RTD	Round Trip Delay
RTP	Real-Time Protocol
SBC	Session Border Controller
SDES	Source DEScription
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP URI	SIP protocol Uniform Resource Identifier
SIP-I	SIP with encapsulated ISUP
SIP-T	SIP for Telephones
SLA	Service Level Agreement
SMS	Short Message System
SN	Subscriber Number
SONET	Synchronous Optical Network
SP	Service Provider
SR	Sender Report
SRTP	Secure Real Time Protocol
SS7	Signalling System 7
STQ	Speed processing Transmission and Quality aspects
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
tel-URI	Telephone Uniform Resource Identifier
TUP	Telephone User Part
UDP	User Datagram Protocol
UDPTL	facsimile UDP Transport Layer
URI	Uniform Resource Identifier
VAD	Voice Activity Detection
VBD	Voice Band Data
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoIPX	Voice over IPX
WB	Wideband

3 References

[1] I3 Forum “Common functionalities and capabilities of an IPX platform”, Release 1, December 2012

[2] i3 Forum “Technical Interconnection Model for International Voice Services”, Release 5, May 2012

[3] i3 Forum White Paper “Voice Path Engineering in International IP based Voice Networks”, Release 3.0, May 2011

[4] i3 Forum “Routing and Addressing services for International Interconnections over IP”, Release 1.0, May 2010

[5] i3 Forum “ White Paper: Techniques for Carriers’ Advanced Routing and Addressing Schemes”, Release 1.0, May 2010

[6] i3 Forum “Technical White Paper on Security for IP Interconnections”, Release 1, May 2011

[7] i3 Forum “Interconnection IMS Signalling Profile”, Release 1.0, May 2012

[8] GSMA IPXWP “IPX White Paper”, October 2006

[9] GSMA AA.81 “Packet Voice Interconnection Service Schedule to AA.80”, Version 2.1 and subsequent approved change requests.

[10] GSMA IR.36 “GSMA PRD IR.36 “Adaptive Multirate Wide Band version 1.0”, December 2011

[11] IETF RFC 1423: - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, February 1993

[12] IETF RFC 2328 “OSPF Version 2”, April 1998

[13] IETF RFC 2597 “Assured Forwarding PHB Group”, June 1999

[14] IETF RFC 3246 “Expedited Forwarding (Per-Hop Behavior)”, March 2002

[15] IETF RFC 3247 “Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behaviour)”, March 2002

[16] IETF RFC 3261 “SIP: Session Initiation Protocol”, June 2002

[17] IETF RFC 3264, “An Offer/Answer Model with the Session Description Protocol (SDP)”, June 2002

[18] IETF RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, September 2002

[19] IETF RFC 3325 “SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks”, September 2002

[20] IETF RFC 3389 “Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)” September 2002

[21] IETF RFC 3550 “RTP: A Transport Protocol for Real-Time Applications”, July 2003

[22] IETF RFC 3551 “RTP Profile for Audio and Video Conferences with Minimal Control”, July 2003

[23] IETF RFC 3611 “RTP Control Protocol Extended Reports (RTCP XR)”, November 2003

[24] IETF RFC 3966 “The tel URI for Telephone Numbers”, December 2004

[25] IETF RFC 3986 “Uniform Resource Identifier (URI): Generic Syntax”, January 2005

[26] IETF RFC 4028 “Session Timers in the Session Initiation Protocol (SIP)”, April 2005

[27] IETF RFC 4244 “An Extension to the Session Initiation Protocol (SIP) for Request History Information”, November 2005

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

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

[30] IETF RFC 4855 "Media Type Registration of RTP Payload Formats", February 2007

[31] IETF RFC 4867 "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs April 2007

[32] IETF RFC 5806 "Diversion Indication in SIP", March 2010

[33] IETF draft-ietf-mmusic-media-loopback-18 "An Extension to the Session Description Protocol (SDP) for Media Loopback", September 2011, work in progress

[34] IETF draft-wu-xrblock-rtcp-xr-one-way-delay-00 "RTCP XR Report Block for One Way Delay metric Reporting", January 2012, work in progress

[35] ITU-T Recommendation E.164 "The international public telecommunication numbering plan", 1997

[36] ITU-T Recommendation E.411 "International Network Management – Operational guidance", March 2000

[37] ITU-T Recommendation E.425 "Network Management – Checking the quality of the international telephone service. Internal automatic observations", March 2002

[38] ITU-T Recommendation E.437 "Comparative metrics for network performance management", May 1999

[39] ITU-T Recommendation G.107 "The E model, a computational model for use in transmission planning", March 2005

[40] ITU-T Recommendation P.10 "Vocabulary of terms on telephone transmission quality and telephone sets", December 1998

[41] ITU-T Recommendation Q1912.5 "Interworking between Session Initiation Protocol and Bearer Independent Call Control or ISDN User Part", 2004

[42] ITU-T Recommendation T.30 "Procedures for document facsimile transmission in the general switched telephone network", September 2005

[43] ITU-T Recommendation T.38 "Procedures for real-time Group 3 facsimile communication over IP networks", June 1998

[44] ITU-T Recommendation T.38 "Procedures for real-time Group 3 facsimile communication over IP networks", April 2007

[45] ITU-T Recommendation T.38 "Procedures for real-time Group 3 facsimile communication over IP networks", September 2010

[46] ITU-T Recommendation V.152 "Procedures for supporting voice-band data over IP networks", January 2005.

[47] ETSI EG 202 057-2 "Speech processing transmission and quality aspects (STQ); user related QoS parameter definitions and measurements; Part 2: Voice Telephony, Group 3 Fax, modem data services and SMS"; October 2005

[48] ETSI EN 300 175-8 V2.4.0 "Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI)", December 2011

4 Basic Definitions

In this document the following definitions, discussed and agreed upon between GSMA's IPIA and i3 Forum representatives in 2009, apply:

1) **IPX (IP Packet eXchange)**: A private managed backbone providing guaranteed Quality of Service, security and cascading payments. The IPX is a network of networks provided by the whole group of interconnected IPX Providers.

2) **Service Provider (SP)**: A business entity entering into a contractual relationship with IPX Provider(s) which offers services to final users providing termination (origin and destination) for IP services traffic. Thus, "service provider" includes MNOs, FNOs (for example, fixed broadband operators and NGNs), ISPs, ASPs and similar entities.

   The business entity acts as Service Provider for the "numbers/user id's" of its own contracted end users and those contracted through distribution entities with an exclusive commercial contract with the Service Provider and that share the same access network of the SP (ex.: MVNOs).

3) **IPX Provider (IPX P)**: A business entity (such as an IP Carrier) offering IP interconnect capabilities to SPs, possibly through NNI with other IPX Ps for one or many IPX services compliant with the IPX operational criteria and compliant with the defined SLA and interconnect agreement for that end-to-end service.

4) **End-to-End (SP-to-SP)**: End-to-End means from Service Provider premises to Service Provider premises. Thus, Service Provider core and access networks are excluded.

5) **VoIPX**: Identifies a specific logical subset of IPX devoted to manage voice service in terms of interfaces, features and capabilities. VoIPX confirms IPX concepts such as security, cascading and Service Provider to Service Provider responsibility.

6) **VoIPX Functional Architecture**: Identifies the set of VoIPX functions and options/features.

5 IPX Reference Configuration for Voice service

5.1 Reference Business Framework

The reference business framework for the Voice over IPX service is described in detail in chapter 5.1 of "Common functionalities and capabilities of an IPX platform" [1].

- The IPX domain consists of all the IPX Providers' networks and their interconnections. IPX Providers can connect to non-IPX compliant Carriers or Service Providers with the intent to either forward traffic (break-out) to destinations not reachable via the IPX, or to accept traffic destined to an IPX compliant Service Provider (break-in). In both cases, the rules of cascading responsibilities, Quality of Service and security shall be fulfilled.

5.2 Break-in / break-out

The issue of break-in / break-out is very important in the scope of the Voice over IPX service. The transport of voice communications is a long established service that is undergoing a big change now in terms of the technology being used to transport these voice calls. Traditionally transport was done over pure capacity networks in circuits of 56 or 64 kbits/s usually bundled in groups of 24 or 32 (T1, E1) which in turn are bundle over STM-x circuits. The industry is migrating this transport to IP networks including IPX. Both during and after the transition to IP, there is still a need to define and manage break-in / break-out between the IPX and TDM and/or non-IPX IP networks. Allowing break-in/break-out via legacy networks, e.g. TDM and IP, for Voice Service between an IPX Provider and a Non-IPX compliant Service Provider has several advantages:

- Many destinations will remain reachable only via TDM and non IPX compliant IP connections for some considerable time. Not allowing TDM and IP break-in / break-out would exclude many destinations from a direct communication via the IPX domain and SPs would have to keep TDM interconnects operational in parallel to IPX-based interconnects in order to have access to these providers, and to receive calls from those SPs;
- Break-out / break-in NNIs support a faster deployment of IPX services for voice as they break the dependency on all networks migrating to IP at the same time.

5.2.1 Break-out from the IPX Domain (outgoing traffic)

In order to deliver traffic received from participating SPs towards non IPX destinations, the IPX Provider may be interconnected with non IPX Providers and non IPX compliant SPs as far as:

- Those SPs reached through a break-out of the IPX domain are announced as reachable through a non IPX compliant interconnection. In this case all end-to-end (SP-to-SP) IPX capabilities are maintained within the IPX domain and best practice operations are assured outside the IPX domain. This has to be disclosed in the commercial agreement between originating SP and IPX Provider.
- If the termination of the call due to network faults is not possible within the IPX domain, when commercially agreed, the break-out route becomes the only way to terminate the call. In this case the security is given according to best practice operations. The remaining capabilities of the end-to-end (SP-to-SP) connection, as an objective, are compliant with the commercial agreement between originating SP and IPX Provider.

5.2.1.1 Break-in to the IPX Domain (incoming traffic)

If commercially agreed with the receiving part, the IPX Provider may inject traffic from other non IPX-compliant trusted SPs provided that the security of the IPX is not affected.

5.3 Connectivity options

The IPX consists of two layers:

(1) the IPX Core provides connectivity enabling the provisioning of IPX services between IPX Ps and/or SP. This layer provides a guaranteed QoS IP transport function, (2) the Service Layer provides establishment of connections and management of billing and settlements for a service.

The IPX domain supports three interconnect models as detailed in the following sections.

5.3.1 Bilateral – Transport Only (transport without service awareness)

Defined and described in i3 Forum IPX Core document [1].

This connectivity mode, being service agnostic, is considered out of scope for this document. Two Service Providers can set-up a voice interconnection between themselves if they receive the appropriate Transport Only connectivity mode from IPX Provider(s).

5.3.2 Bilateral - Service Transit (transport with service awareness)

Defined and described in i3 Forum IPX Core document [1]. In this connectivity mode the IPX Providers offer service-aware VoIPX transport to the Service Providers whereas accounting and charging of termination fees is settled directly between the Service Providers (reference to chapter 13). In case of multiple IPX Ps, there is a need to ensure that all enable this model.

5.3.3 Multilateral - Hubbing (transport and hubbing with service awareness)

Defined and described in i3 Forum IPX Core document [1]. This connectivity mode is the one in which the IPX Providers, in addition to that described in 5.3.2, also provides settlement of termination fees to the Service Providers . This connectivity mode also offers the capability to provide a global reach (as illustrated in chapter 12).

5.4 Reference Technical Architecture

For a detail reference technical architecture please go to chapter 5.2 of “Common functionalities and capabilities of an IPX platform” [1].

6 Transport Functions

The transport functions for the Voice over IPX service are described in section 6 of ”Common functionalities and capabilities of an IPX platform” [1]. More detailed information related explicitly to the Voice over IPX service is described in the following subsections.

6.1 Dimensioning Requirements at the transport layer

In order to ensure that, at the interconnection, sufficient capacity is present with the highest level of confidence, a dimensioning scheme with an over-provisioning factor is suggested. In the following table, the bandwidth to be allocated per call is given for the most common codecs:

Codec	Packetisation (msec.)	IPv4	IPv6
		BW (kbits/s)	BW (kbits/s)
G.711	20	104,640	114,240
G.729	20	37,440	47,040
G.722 (64kbits/s)	20	104,640	114,240
G.722.2 (12.65)	20	43,020	52,620
G.722.2 (23.85)	20	56,460	66,060

Note: The IPv4 and IPv6 bandwidth values of the above table consider the bandwidth of the codec plus the overhead of the Ethernet, IP (either IPv4 or IPv6), UDP and RTP protocols and assume a value equal to 10% as the over-provisioning factor. The signalling bandwidth is considered in the 10% over-provisioning factor.

6.2 IP Packet Marking

The general IP Marking principles are given in the i3f IPX Core document

The Voice over IPX traffic types are mapped to the GSMA traffic classes as per the following table:

Traffic Type	GSMA Traffic Class
Voice Media	Conversational
Voice Signalling	Conversational or Interactive

As a result for all the interconnection configurations described above the following table applies:

Traffic Type	DSCP Marking	IP Precedence	802.1Q VLAN
Voice Media	DSCP 46/EF (101110).	5	5
Voice Signalling	DSCP 26/AF31 (011010) or DSCP 46/EF (101110)	3 or 5	3 or 5

Note: There is no consensus whether the signalling has to be treated in the Expedited Forwarding ([14][15]) or Assured Forwarding ([13]) Per Hop Behaviours. As a result, due to historical reasons there are two possible values but interactive is the preferred one.

7 Signalling Functions

The interconnection model for VoIPX described in this document supports a basic SIP profile (as described in section 7.1) or an ISUP enabled SIP profile (as described in section 7.2) or a SIP-IMS enabled SIP profile (as described in 7.3).

7.1 Functions for supporting signalling protocol SIP (IETF RFC 3261)

7.1.1 Transport of SIP (IETF RFC 3261) signalling information

UDP is the default transport protocol for SIP. Usage of other transport protocols is discussed in the Interconnection Model [2].

7.1.2 SIP signalling protocol profile

The SIP profile shall comply with RFC 3261 [16] with the addition of the following considerations:

- The compact form of SIP shall not be used.
- The Request-URI shall be set in accordance to section 9.
- The support of IETF RFC 4028 [26], which addresses SIP Timers specification, is optional. The IPX Provider receiving the INVITE message shall comply with IETF RFC 3261 [16] section 16.8 if IETF RFC 4028 [26] is not supported**.**
- The P-Asserted-Identity header defined in RFC 3325 [19] shall be transported transparently if present.
- The Privacy header defined in RFC 3323 [18] shall be supported.
- The Diversion header defined in RFC 5806 [32] shall be supported.
- The History-Info header defined in RFC 4244 [27] shall be supported
- The following body types shall be supported:
    - application/sdp
- The following body types may be supported:
    - application/dtmf
    - application/dtmf-relay
    - multipart/mixed.

Subject to bilateral agreement, the IPX Provider may or may not apply privacy before forwarding SIP messages over the interconnection interface. When applying privacy, it shall be applied as follows:

Originating User Privacy Request	**Originating IPX Provider behaviour**
CIN Known, Presentation not restricted	Forward CIN in From, Contact and P-Asserted-Identity headers
CIN Known, Presentation restricted	Use “anonymous@anonymous.invalid” in From and Contact headers. Make sure that both user and domain name privacy are guaranteed.
CIN not known	Use “Unavailable” in From and Contact headers.

Note: when a SIP message is passed to an untrusted domain, the inclusion or removal of the P-Asserted-Identity header shall be determined by consulting the Privacy header. If a Privacy header is not present it is recommended to include the P-Asserted-Identity header, but in this case bi-lateral agreement should dictate final treatment (IETF RFC 3323 [18], 3325 [19]). When the SIP message is passed to a trusted domain, the P-Asserted-Identity header should not be removed (IETF RFC 3325 [19]).

7.1.3 SIP Message support

SIP methods, as listed in the Interconnection Model [2], section 7.1.3, shall be supported.

7.1.4 SIP Header support

SIP headers, as listed in the Interconnection Model [2], section 7.1.4, shall be supported.

7.1.5 Alignment with 3GPP SIP / ISUP mapping

In late 2010 / early 2011 i3 Forum and 3GPP jointly worked to finalize a unique mapping of SIP Status Codes and ISUP Cause Code Values. The output of this activity is a new version of 3GPP 29.163, dated March 2011, which encompasses releases back to release 7 (i.e. 7.22.0). i3 Forum endorses this document from 3GPP.

7.2 Functions for supporting signalling protocol SIP-I (ITU-T Rec. Q.1912.5)

7.2.1 Transport of SIP-I (ITU – T Q.1912.5) signalling information

UDP is the default transport protocol for SIP. Usage of other transport protocols is discussed in the Interconnection Model [2], section 7.2.1.

7.2.2 SIP-I (ITU – T Q.1912.5) signalling protocol profile

This signalling protocol profile shall be in accordance with ITU-T Recommendation Q.1912.5 [41] Annex C Profile C.

7.3 Functions for supporting signalling protocol IMS SIP

A profile of the IMS SIP signalling devoted to the interconnecting scenario is given in [7].

7.4 End-to-end Signalling Information Transparency

IPX-Ps should act and operate in order to guarantee transparency of the end-to-end signalling information, particularly CLI information. However, the full transparency cannot be guaranteed in all cases and in all signalling scenarios.

8 Media Functions

This section discusses the recommendations for the voice path and fax for VoIPX interconnections. For more information of the voice engineering, please refer to the i3 Forum – “Technical Whitepaper on Voice Path Engineering” [3].

A VoIPX interconnection shall support the following services and service features:

- Voice phone calls using different codecs (see 8.2),
- DTMF support,
- Fax connections.

Both PSTN and VoIP subscribers could originate the above listed services. Media functions in VoIPX interconnections shall ensure the following:

- End-to-end IPX-Core based transport for all the above listed services
- Assurance of the best available VoIPX quality by providing end-to-end codec negotiation transparency unless transcoding is required and optionally supported by the IPX-P

8.1 Voice calls – protocol profiles

For calls between two or more terminals the following protocol stack shall be used:

- RTP protocol for real time media;
- UDP protocol at the transport layer.

8.1.1 Real Time Protocol / Real Time Control Protocol

The Real Time transport Protocol (RTP) and Real Time transport Control Protocol (RTCP) shall be used for international voice services as defined in IETF RFC 3550 [21] and IETF RFC 3611 [23]. According to RFC 3550 for particular applications the following items should be additionally defined:

- Profile definition;
- Payload format specification.

In order to guarantee measurements of QoS parameters, RTP and RTCP flows have to be passed through end-to-end for the voice over IP connection except when media stream conversions such as transcoding or packetisation period transrating occur.

The profile that shall be used for international voice interconnection is defined in IETF RFC 3551 [22]. The list of protocol parameters defined in this RFC [22] that shall be used is given below.

8.1.1.1 Real Time Protocol data header

The RTP data header is defined in Section 2 of RFC 3551 [22]. The content of this section is endorsed.

8.1.1.2 Real Time Protocol Payload types

The following RTP payload types shall be supported:

- G.711 A-law, G.711 µ-law, G.729, G.729a, G.729b, G.729ab, G.722, AMR-WB as defined in Section 6, Table 4 of RFC 3551 [22].
- Detailed definition of the above mentioned and other supported codecs payload types is in Sections 8.3 - 8.4 of this document.
- Comfort Noise is defined in Section 4 of RFC 3389 [20] (static PT 13 (8 kHz) or dynamic).
- Telephone Events (DTMF tones) as defined in the Section 3.3 of IETF RFC 4733 [29](dynamic)
- Telephone tones as defined in the Section 4.4 of IETF RFC 4733 [29] (dynamic).

8.1.1.3 Real Time Protocol data header additions

No RTP header additions will be used.

8.1.1.4 Real Time Protocol data header extensions

Use of RTP data header extensions is not recommended.

8.1.1.5 Real Time Control Protocol report interval

Recommended bandwidth allocation to RTCP reports would be 1.25% of session bandwidth for senders and 3.75% for receivers. Other bandwidth allocations are possible as described in Section 2 of IETF RFC 3551 [22].

8.1.1.6 Sender Report/Receiver Report (SR/RR) extensions

Generally no SR/RR extensions will be used. Optional extensions may be used if agreed bilaterally.

8.1.1.7 Source Description (SDES) use

The SDES use is specified in IETF RFC 3551 [22] Section 2.

8.1.1.8 Security - security services and algorithms

According to RFC 3550 [21] Section 9.1, the default encryption algorithm is the Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode, as described in Section 1.1 of RFC 1423 [11], except that padding to a multiple of 8 octets is indicated as described for the P-bit.

In the scope of this document RTP (media) encryption is not recommended.

8.1.1.9 String-to-key mapping

No string to key will be used.

8.1.1.10 Congestion - the congestion control behaviour

RTP and this profile may be used in different contexts. Some congestion control guidelines can be found in Section 2 of IETF RFC 3551 [22]. Under normal operational conditions congestion should be avoided by network engineering techniques.

8.1.1.11 Transport protocol

The UDP as well as the TCP protocols are defined in RFC 3551 [22] section 2 as the transport layer for RTP. In the scope of this document only the UDP protocol shall be used as the RTP transport layer for voice services.

8.1.1.12 Transport mapping

The standard mapping of RTP and RTCP addresses and ports at the transport layer is used as in RFC 3551 [22] Section 2 with the following recommendations:

- RTP should use an even destination port number and the corresponding RTCP stream should use the next higher (odd) destination port number as described in RFC 3550 [21] Section 11,
- Symmetrical UDP protocol should be used (the same port numbers).

8.1.1.13 Encapsulation of Real Time Protocol packets, multiple Real Time Protocol data packets

Encapsulation of the RTP packets in the UDP protocol shall be used as defined in [21].

8.2 Voice Codecs

Many different coding schemes have been defined, implemented and used for international voice service. In the scope of this document these codecs are divided into 2 categories:

Mandatory codecs: the IPX Provider shall be able to carry all voice media flows encoded as per any of the i3 Forum recommended codecs, to be considered mandatory in this context, and shall allow the negotiation of these codecs between both originating and terminating Service Providers. As a result, an IPX Provider has to support all mandatory codecs listed in Table 1 in Section 8.3. Provided at least one of the mandatory codecs is present in the session description protocol (SDP) offer, and provided at least one of the mandatory codecs is supported by both originating and terminating Service Providers, then codec negotiation is guaranteed to be successful. For destinations where one of the mandatory codecs is not available by the IPX P, these destinations shall be disclosed to the SP. For any transcoding related matters see section 8.5.2.

Optional codecs: other codecs which are recommended due to their significant market relevance.

In future releases of this document, other codecs may be added to the list of mandatory and optional codecs.

8.3 Codecs Supported for Narrow Band Transmission of Voice

Narrow Band codecs reproduce the audio bandwidth of the PSTN and it is expected that they will be used in IP based voice networks for some time. The codecs to be supported for Narrow Band transmission are:

Group 1. Mandatory Narrow band codecs	Group 2. Optional Narrow band codecs
G.711 A-law, μ-law 64 kbit/s	AMR-NB
G.729, G.729a, G.729b, G.729ab 8kbit/s	

Table 1 Mandatory and Optional Narrow Band Codecs for Voice

Note: as far as the conversion between G.711 A-law and G.711 μ-law is concerned, the existing conventions apply (i.e. conversion will be done by the countries using the μ-law).

Note: i3 forum recognises that the G.711 codec needs much higher bandwidth than other codecs like AMR-NB and confirms its willingness to review, in future releases of this document, the content of Table 1 above to align it with market developments.

8.3.1 Guidelines for Engineering

Packetisation period for mandatory Narrow Band codecs:

- for G.711 A-law and μ-law, the packetisation period shall be 20 ms.
- for G.729, G.729a, G.729b, G.729ab, the packetisation period shall be 20 ms.

Payload type definition for mandatory Narrow Band codecs:

G.711 A-law	PT= 8 Static
G.711 μ-law	PT= 0 Static
G.729, G.729a	PT= 18 Static
G.729b, G.729ab	PT= 18 Static. Optional parameter “annexb” may be used according to RFC 4855 [30]

Packetisation period for other (optional) Narrow Band codecs:

- for AMR-NB the packetisation period shall be 20 ms.

Payload type definition for other Narrow Band codecs:

AMR-NB	PT=Dynamic as defined in RFC 4867 [31]

8.4 Codecs supported for Wideband Transmission of Voice

There is a general trend towards the increased use of wideband codecs. They provide superior voice quality and their use may reduce voice quality degradation due to transcoding. Support of wideband codecs by IPX Providers is optional. However, when an IPX Provider supports wideband codecs, this section applies and specifies what needs to be supported. The codecs to be supported for Wideband transmission are:

Group 1. Mandatory Wideband codecs (*)	**Group 2. Optional Wideband codecs**
G.722 (generally used by fixed network operators)	
AMR-WB (generally used by mobile network operators)	

Table 2 Mandatory and Optional Wideband Codecs for Voice

(*) The mandatory status is conditional on the support of wideband voice interconnection: if Wideband voice interconnection is supported, then the Group 1 codecs in Table 2 are mandatory as defined in Section 8.2.

8.4.1 Guidelines for Engineering

Bitrates and Modes for mandatory Wideband codecs

The requirements for AMR-WB are taken from GSMA PRD IR.36 [10] and RFC 4867 [31]. The requirements for G.722 are taken from Dect-ND ETSI EN 300 175-8 [48]

AMR-WB can operate in a 9 modes at source codec bit rate of 23.85 kbit/s, 23.05 kbit/s, 18.25 kbit/s, 15.85 kbit/s, 14.25 kbit/s, 12.65 kbit/s, 8.85 kbit/s and 6.60 kbit/s.

The AMR-WB configurations specified for 2G and 3G are:

WB-Set 0 = {		12.65	8.85	6.60}
WB-Set 2 = {	15.85	12.65	8.85	6.60}
WB-Set 4 = {	23.85	12.65	8.85	6.60}

No other combination of the 9 AMR-WB modes is allowed for voice telephony. The other modes of AMR-WB may be used for other applications.

All these 3 supported configurations are TrFO compatible. However, WB-Set 0 is the guaranteed minimum common denominator mandatory for all configurations and shall be supported. This configuration also includes DTX, i.e. WB-SID frames and no data transmission during inactive speech; support of SID frames in reception is mandatory; generation is optional. All other modes are optional.

G.722 shall be supported at a bit rate of 64 kbit/s.

Packetisation period for mandatory Wideband codecs

- for G.722, the packetisation period shall be 20 ms
- for AMR-WB, the packetisation period shall be 20 ms

Payload type definition for mandatory Wideband codecs

- G.722 PT=9 Static
- AMR-WB PT=Dynamic as defined in RFC 4867 [31]

8.5 Codec/Packetisation period use and transcoding guidelines

Codec and packetisation period selection, and particularly transcoding, have a great impact on end-to-end voice quality in VoIP networks.

Note that if an IPX Provider chooses to either transcode or change the packetisation period it will be necessary for the IPX provider to utilise a Border Function such as an SBC to terminate and re-originate the new media stream. This Border Function would also be required to undertake any required G.711 A-Law/G.711 µ-Law (companding) conversion as in section 8.3.

Note: This is an example of the additional Border Function functionalities referred to in section 10.1

8.5.1 Voice quality estimation

It is necessary to ensure that voice transmission quality is acceptable for all IP interconnection configurations and designs. If a voice path design gives a poor voice quality estimate, the network configuration and/or codec/packetisation period choice should be redesigned.

The detailed rules as well as the method of end to end voice quality estimation for this purpose are given in the i3 Forum white paper “Voice Path Engineering in international IP-based networks” [3].

Generally the design should take into consideration:

- the codec/packetisation period parameters of all involved interconnected networks (e.g. originating SP and domestic network – international IPX providers’ networks – international carriers’ networks (break out case) – terminating SP and domestic network);
- the packetisation period latencies taken in conjunction with both originating and terminating domestic and local access networks latencies;
- the propagation delay;
- De-jitter buffer latency (including de-jitter buffers associated with any intermediate media conversion function, such as transcoding);
  Note: Attention has to be given to the dimensioning of the de-jitter buffer prior to de-packetising [3] for media stream conversion (such as transcoding) and in the terminating SP network.
- the expected packet loss and codec packet loss robustness;
- the transmission bandwidth (cost);
- the voice quality (product) required.

8.5.2 General guidelines

The following general guidelines aim to provide default rules for codec choice and transcoding responsibility:

- Codec transparency shall be maintained when feasible, i.e. transcoding should be avoided whenever possible, if it impacts speech quality;
- the order of codec/packetisation period preference is determined by the originating terminal and should be honoured wherever possible;
- if a G.711 encoded call is to be routed across the borders of either North America or Japan then G.711 A-law/µ-law conversion might be necessary and this companding conversion shall be done by the IPX Provider/international carrier in the countries using the µ-law;
- if the call is to be routed to a TDM network, only one transcoding is recommended. If required, it should be performed during the voice over IP/TDM conversion;
- in case no common codec can be used between both end Service Providers, in the first instance it is the responsibility of Service Providers to support transcoding in order to ensure successful voice interoperability for their services.

An extensive treatment of voice quality impairments generated by codec and/or transcoding functions is given in [3].

8.6 Fax calls – protocol profiles

To enable sending and receiving fax messages from TDM to VoIP or TDM to TDM via VoIP across the IPX domain the following methods can be used:

- Fax relay according to ITU-T T.38 ([43], [44] y [45])
- VBD according to ITU-T V.152 [46]
- Pseudo VBD fax pass through

8.6.1 8.6.1 Fax over IP guidelines

T.38 fax relay ([43], [44] y [45]) shall be supported as the first choice. ITU-T T.38 version 0 (06/1998) [43] is mandatory, latest version 5 (09/2010) [45] is strongly recommended. It is recommended to use T.38 fax relay method for the following reasons: T.38 is the de facto standard in a VoIP network; T.38 provides interworking/conversion between different codecs, e.g. G.711 A/μ-law conversion. The protocol stack should be: IFT protocol for T.30 [42] media, UDPTL (Facsimile UDP Transport Layer) and UDP protocol in transport layer.

It is recommended that Standard G3 Group facsimile shall be supported as mandatory. V.34 Group 3 facsimile support is optional. Recommended target solution, is the implementation of the latest T.38 standard which allows full support of SG3 fax.

It is also possible but not recommended to use VBD FoIP service according to ITU-T V.152 [46] as the second choice and pseudo VBD with G.711 A-law or μ-law codec with the addition that it is also possible to use dynamic payload instead of static in SDP negotiation, VAD disabled and constant jitter buffer as the third choice.

8.7 Handling of early media

In this document the term “*early media*” encompasses ringback tones, announcements, and in general, any type of media different than user–to–user communication (i.e., any media before the sending/receiving of the 200 OK message).

In TDM networks, ring–back tone is rendered by the called side whereas, in IP networks, it is usually rendered by the calling side. However, all scenarios that can be encountered by an IPX Provider interconnecting, upstream and downstream, with ISUP, SIP and SIP-I based networks, need clarification. Handling of Early–Media is governed by the presence of the P-Early-Media header, when this header is supported. This is described in the Interconnection Model [2], section 9.1. When the P-Early-Media header is not supported, the behaviour of the IPX Provider is as described in the Interconnect Model [2], section 9.2.

9 Numbering and Addressing Scheme

This deliverable is E.164-based [35]. The objective of this section is to define the format of numbers and addresses that will be exchanged in signaling messages between operators in international IP interconnection for voice services.

9.1 Numbering and addressing in E.164-based International interconnection

International IP interconnection for voice services will be based on SIP [16] and SIP-I [41]. In the first phase of implementation only E.164 numbers shall be used as destination address. These numbers shall be used in tel-URI and SIP URI as described in sections 9.3 and 9.4 respectively.

9.2 International numbering scheme in TDM network

International number format used in International IP interconnect for voice shall conform to E.164 standard [35]. A telephone number is a string of decimal digits that uniquely identifies the network termination point. The number contains the information necessary to route the call to this point.

According to this standard, a full international number in global format contains a maximum of 15 digits starting from Country Code (E.164 [35] Section 6) and has the following format:

1. For geographical areas:	CC NDC SN	maximum 15 digits.
2. For global services:	CC GSN	maximum 15 digits.
3. For networks:	CC IC SN	maximum 15 digits.
4. For groups of countries:	CC GIC SN	maximum 15 digits.

Where:

- CC Country Code for geographic area 1 – 3 digits
- NDC National Destination Code
- SN Subscriber Number
- GSN Global Subscriber Number
- IC Identification Code 1 – 4 digits
- GICGroup Identification Code 1 digit

Support of ISDN sub addressing as defined in E.164 [35] (Appendix B, Section B. 3.3) in international voice IP interconnect is OPTIONAL as it is very rarely used.

9.3 TEL-URI Addressing scheme

A tel-URI shall conform to IETF RFC 3966 [24]. According to this RFC global unique telephone numbers are identified by a leading “+” character so E.164 based addressing used in SIP INVITE message SHALL be as follows:

1. For geographical areas:	+CC NDC SN	maximum 15 digits.
2. For global services:	+CC GSN	maximum 15 digits.
3. For networks:	+CC IC SN	maximum 15 digits.
4. For groups of countries:	+CC GIC SN	maximum 15 digits.

An example of a tel-URI would be:

```
tel:+14085551212
```

9.4 SIP-URI Addressing scheme

A SIP-URI shall conform to IETF RFC 3986 [25]. In order to setup an international voice call, the telephone number used in the SIP-URI shall be a valid E.164 number preceded with the “+” character and the user parameter value "phone" should be present as described in RFC 3261 [16] section 19.1.1.

An example of a SIP-URI would be:

sip:+14085551212@domain.com;user=phone

9.5 Other Addressing scheme

Other addressing scheme than ITU-T E.164, such as SIP URIs where the user part is a “string”, could be used depending on technical and commercial development and mutual agreement between SP and IPX P.

10 Security Functions

The general requirements for IPX security are defined in section 10 of “Common functionalities and capabilities of an IPX platform” [1]. For more information please refer to the i3forum – Technical White Paper on Security for IP Interconnections [6].

10.1 Network elements for border function

All voice traffic coming into / leaving an IPX Provider’s network shall pass through a Border Function.

As a result, all IP packets (for signaling and media) crossing a voice interconnection are originated and received by a Border Function.

In Section 5 the definitions of Border Function as well as the mapping with the corresponding functions for the control and user (media) plane are given.

A typical example of Border Function is a SBC (Session Border Controller).

The main functions of the SBC are the following:

- Perform control functions by tightly integrating session signalling and media control.
- They are the source and destination for all signalling messages and media streams coming into and leaving the IPX Provider’s network.
- A Session Border Controller breaks down into two logically distinct functions.
    - The Signalling SBC function controls access of SIP signalling messages to the core of the network, and manipulates the contents of these messages.
    - The Media SBC function controls access of media packets to the network, provides differentiated services and QoS for different media streams, and prevents service theft.

Furthermore, additional functionalities could be implemented in the SBC.

The security mechanisms provided by Border Function systems are listed in section 10.2.

10.2 Security features and capabilities

An extensive discussion of security threats is given in i3 Forum White Paper on Security for IP Interconnection reference [6]

10.3 Security Threats

An extensive discussion of security threats is given in i3 Forum White Paper on Security for IP Interconnection reference [6]

10.4 Recommendations Matrixes

These matrixes specify the mechanisms that shall be used to protect VoIP interconnections. The matrixes specify mechanisms by component service interface for Private oriented connections and Public (access only) as detailed in Sections 5 and 6.

There are three levels specified:

- Basic – the basic security mechanisms that reflect the minimum generally accepted industry practices for securing these services. This is not sufficient for a Voice over IPX service.
- i3F Recommended – in addition to basic, mechanisms consistent with the implementation documents of the i3 Forum.
- i3F Optional – in addition to recommended, other mechanisms that can be used to further enhance security for the specified service.

10.4.1 External Service Interfaces Recommendations

In addition to the traditional IP layer security mechanisms (e.g. access control lists, selective BGP announcements, BGP neighbour authentication encryption using MD5, etc.), the following matrix, which applies at the service layer, is a subset of what is recommended in the security whitepaper and it specifies which mechanisms should be deployed for external service interfaces related for VoIP interconnections over the IPX, for the three security levels: basic, recommended and optional.

Configuration	**Basic**	**i3F Recommended** *(additional to Basic)*	**i3F Optional** *(additional to Recommended)*
		SIP/SIP-I interface	
Private Interconnection	Access Control List[1] Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Border Function filtering** **Application Level Relaying** **Topology Hiding** **Traffic policing**	i3F Recommended + Encryption Deep Packet Inspection Intrusion Detection Systems
Public Interconnection for access only	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Border Function filtering** **Application Level Relaying** **Encryption** **Topology Hiding** **Traffic policing**	i3F Recommended + Deep Packet Inspection Intrusion Detection Systems
		RTP Interface	
Private Interconnection	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Dynamic Port opening** **Media Filtering** **Topology Hiding**	i3F Recommended + Encryption SRTP Traffic policing Deep Packet Inspection Intrusion Detection Systems
Public Interconnection for access only	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Dynamic Port opening** **Media Filtering** **Topology Hiding**	i3F Recommended + Encryption SRTP Traffic policing Deep Packet Inspection Intrusion Detection Systems

[1] In this table the Access Control List security mechanism makes reference to the actions performed by Border Functions

11 Quality of Service Measurements

The general principles of Quality of Service measurements in an IPX are defined in section 11 of “Common functionalities and capabilities of an IPX platform” [1]. i3Forum recognises a trend in the wholesale industry which calls for quality monitored and controlled services both from FNOs and MNOs Service Providers. This trend gets its most significant validation from the IPX (IP eXchange) model conceived and designed by GSMA.

GSMA, for the voice service over an IPX platform, identifies in AA.81 [9] the need to measure, in addition to the traditional voice parameters (see section 11.1.2), transport-dependent parameters such as packet loss, delay and jitter. Specifically, GSMA states the need:

1. to measure and report the service dependent KPIs for ASR, ABR, NER, ALOC, PGRD
2. to measure and report transport-dependent parameters KPIs for packet loss, packet delay and packet jitter;
3. to carry out the above measures following the RTP path and not the shortest path driven by OSPF / BGP / other IP routing protocols; [12][28]
4. to perform the measures of the transport-related parameters, the measurement can be (a) for the whole IPX Provider domain, i.e. from the last equipment in the IPX Providers network facing the originating Service Provider, to the first equipment in the Carriers network facing the terminating Service Provider or (b) for the whole IPX Provider domain described above with the addition of one or both of the Service Provider access legs up till their edge router/SBC.

The figure below describes the reference configuration for QoS measurement.

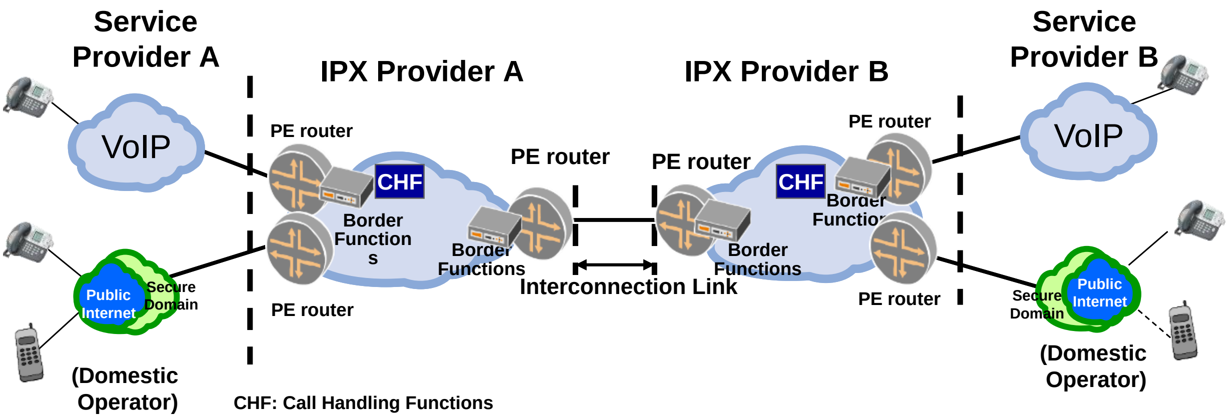

Figure 9 - Reference configuration for QoS measurement

This section describes the QoS parameters definitions, their measurement configurations and KPI calculations pertaining to the international interconnection between IPX Providers and between IPX Providers and their customers (Service Providers).

KPIs are defined for the purpose of:

- Monitoring (supervision) against preset thresholds
- Service Level Agreement (SLA) compliance and Quality of Service reporting IPX Provider with another IPX Provider or IPX Provider with a Service Provider.

Any commercial agreement associated with SLA and/or QoS reporting is outside the scope of this document.

11.1 QoS parameter definitions

The following QoS parameters are considered the most relevant and they are divided in two sets pertaining to the transport layer, and the service layer, as follows:

- Transport parameters

  - round-trip delay
  - jitter
  - packet loss
- Service parameters
  - MOS_{CQE} / R-factor
  - ALOC
  - ASR
  - NER
  - PGRD

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

Other parameters can be measured by IPX Providers for the above listed actions.

No KPI specific to fax quality is defined in the scope of this document since fax quality is measured end-to-end in compliance with ETSI EG 202 057-2 [47].

CLI Management

CLI transparency is not considered a KPI in the scope of this document; however, it is strongly recommended and assumed that international IPX Providers will pass on CLI unaltered.

IPX Providers, under normal operational conditions, are not expected to check CLI validity. They 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 (if received over a TDM link at the originating international gateway). A CLI in SIP would normally be in the format specified in Section 9 of this report, so no change of format would be necessary.

IPX Providers can also have agreements with other interconnecting IPX Providers that will guarantee CLI transparency.

There is no certainty that:

- CLI will be transmitted by Service Provider A;
- the CLI received from Service Provider A 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, even where that IPX Provider has undertaken to guarantee transmission across its network, will be delivered to the terminating user, or delivered without any error being introduced beyond the interconnecting IPX Provider.

In the following subsections the definitions of the QoS parameters listed above are given.

11.1.1 Parameters relevant to the transport layer[2]

Round Trip Delay

Round Trip Delay is defined as the time it takes for a packet to go from one point to another and return

Jitter

Jitter is the absolute value of differences between the delays of consecutive packets

Packet loss

Packet loss is the ratio between the total lost packets and the total sent packets over a given time period

[2] These transport parameters have been defined in [1] but are included here again for the sake of completeness

11.1.2 Parameters relevant to the service layer

The above service layer parameters are defined. (Note: en-bloc signalling, ISUP messages sent in one block, is assumed. The case of overlap signalling is out-of-scope).

MOSCQE / R-factor for voice calls

MOS (Mean Opinion Score) is a subjective parameter defined in ITU-T Rec. P.10 [40] as follows “The mean of opinion scores, i.e., of the values on a predefined scale that subjects assign to their opinion of the performance of the telephone transmission system used either for conversation or for listening to spoken material.”

ITU-T Rec. G.107 [39] defines an objective transmission rating model (the E-model) for representing voice quality as an R-Factor, accounting for transmission impairments including lost packets, delay impairments and codecs. The impairment factors of the E-model are additive, thus impairments from different network segments may be added to obtain an end-to-end value.

The R-Factor may be converted into an estimated MOS which is called MOS Communication Quality Estimated or MOS_{CQE} (as defined in ITU-T Rec. P.10 [40]) using formula in ITU-T Rec G 107 Annex B [39]. As a result, MOS is thus an actual user opinion score, and all measurements done by equipment (including R-Factor and MOS_{CQE}) are estimates, and may differ from what actual customers would perceive.

ALOC

Average Length of Conversation (ALOC) expresses the average time in seconds of conversations for all the calls successfully setup in a given period of time. In a TDM environment ALOC has been defined in ITU-T Recommendation E.437 [38]:

$$\textbf{ALOC} = \frac{\textbf{Time periods between sending answer and release messages}}{\textbf{Total number of answers}}$$

In a Voice over IP environment, and for the purpose of this document, ALOC is defined as follows:

- SIP protocol: ALOC is measured from the time of SIP 200 OK (in response to an INVITE initiating a dialog) to the time of call release (SIP BYE).
- SIP-I protocol: ALOC is measured from the time of a SIP 200 OK with an encapsulated ANM to the time of receiving a BYE message with encapsulated REL.

ALOC depends on user behaviour[3].

ASR

Answer Seizures Ratio (ASR) expresses the ratio of the number of calls effectively answered in a given period of time against the number of call session requests in that time. In a TDM environment, ASR has been defined in ITU-T Rec. E.411 [36] with the following formula:

$$\textbf{ASR} = \frac{\textbf{Seizures resulting in answer signal}}{\textbf{Total Seizures}}$$

In a Voice over IP environment, and for the purpose of this document, ASR is defined as follows:

[3] ALOC indicates a problem may exist when it goes outside of an acceptable range for all customer calls to a particular destination. ALOC is not dependent upon an individual user’s behaviour during one or two calls, but on changes in the behaviour of a majority of users, indicating a widespread problem may now exist.

- SIP protocol: ASR is the ratio between the number of received 200 OK (in response to an INVITE initiating a dialog) and the number of sent INVITE initiating a dialog.
- SIP-I protocol: ASR is the ratio of the number of received 200 OK with an encapsulated ANM (in response to an INVITE with an encapsulated IAM initiating a dialog) to the number of INVITE sent with an encapsulated IAM.

ASR depends on the user behaviour[4].

NER

Network Efficiency Ratio (NER) expresses the ability of a network to deliver a call without taking into account user interferences (measure of network performance) in a given period of time. In a TDM environment, NER has been defined in ITU-T E.425 [37] released in 2002 with the following formula:

$$\mathbf{NER} = \frac{\textbf{Answer message or user failure}}{\textbf{Total Seizures}}$$

Note: user failure includes caller abandonment.

In a VoIP environment, and for the purpose of this document, NER is defined as follows:

- SIP protocol: NER is the ratio of the number of received responses amongst the following responses, with the number of sent INVITE initiating a dialog:
  - a response 200 OK to an initial INVITE or
  - a BYE response or
  - a 3xx response or
  - a 404, 406, 410, 433, 480, 483, 484, 485, 486 or 488 response or Note that 403 is not included because it is categorized as both Network and User events and 403 is not sent to international networks
  - a 600, 603 or 606 response
  - a CANCEL message (in forward direction i.e., from the calling party)
- SIP-I protocol: NER is the ratio of the number of received responses amongst the following responses, to the number of sent INVITE with an encapsulated IAM:
  - a response with an ANM encapsulated or
  - a response with REL encapsulated and cause value 1, 17, 18, 19, 20, 21, 22, 28, 31, 50, 55, 57, 87, 88 or 90, or
  - a CANCEL message (in forward direction i.e., from the calling party)

Note: it is recognised that cause value 53 (outgoing calls barred within CUG) has to be considered as a user failure. Being the scope of this document limited to international interconnection it is assumed that no SIP message related to this cause value 53 will be received.

Note that the NER will be inconsistent with the ITU legacy NER definition if ITU-T Q.1912.5 SIP response codes are used for calculation. To avoid this, the use of MIME encapsulated ISUP Disconnect Cause Value is preferred but, if this is not possible, use of the SIP Response Code as specified in the above SIP protocol NER definition is suggested.

PGRD

[4] ASR indicates a problem may exist when it goes outside of an acceptable range for all customer calls to a particular destination. ASR is not dependent upon an individual user's behaviour during one or two calls, but on changes in the behaviour of a majority of users, indicating a widespread problem may now exist.

Post Gateway Ringing Delay (PGRD) expresses the time elapsed between a request for a call setup and the alerting signal for that call. In a VoIP environment, and for the purpose of this document, PGRD is defined as follows:

The PGRD is the elapsed time after INVITE till media is available to the remote device. It can be calculated with the average time between sending an INVITE initiating a dialog and the first received message of the following SIP Responses:

- 180 resulting in local ringing at the remote device.
- The first 200 OK without preceding 180 or 183, resulting in the call/session being answered.
- 183 with SDP and if there is no 180, resulting in media being available from the far end to the remote device. The media from the far end to the remote device will typically be ringing, but there are scenarios where the media would be either a tone or an announcement.

An exception to the above maybe at a PSTN gateway that receives MIME's ISUP, in which case the receipt of an ACM (with status of subscriber free) or CPG (alerting) in the MIME's ISUP can be used for the PGRD calculation. However, both ACM (Subscriber Free) and CPG (alerting) should be conveyed in a SIP 180 response.

Note: only INVITEs initiating a dialog for which an alerting response is received are taken into account.

11.2 Implementing GSMA quality requirements

11.2.1 Transport and Service Parameters

The above described requirements call for the ability to measure the identified transport parameters for a specific segment reporting the collected data to the Customer / Service Provider. This implies the need to:

- measure the identified parameters for the identified end-to-end domain across downstream network(s) for QoS reporting;
- analyse the call flow in order to locate and isolate faults.

On the basis of the extensive analysis carried out by i3 forum jointly with other bodies and vendors, there is only one protocol (RTP Control Protocol, RTCP) which reports back the quality information of the downstream networks but:

- the RTCP stream is generated by the RTP endpoint and it propagates back across all border functions in the path. Since no information is available in the RTCP reports indicating where the actual RTCP end-point is located in the downstream networks, there is uncertainty on the segment actually being measured;
- transcoding functions generate a new RTP / RTCP stream so making the measurement unreliable;
- the solution assumes the carrier network elements fully support IETF RFC 3550 [24] and IETF RFC 4855 [106] and generate RTCP reports.

As a result, there is currently no means to adequately meet the listed challenges above. More specifically, it is not possible to have a direct, reliable and accurate measure of transport KPIs from the originating Service Provider edge to the terminating Service Provider edge (end-to-end).

This document proposes methodologies and guidelines for practical measurement of transport KPIs based on whether one or more networks are involved in the end-to-end domain is:

- a single network domain
- multiple network domains.

11.2.2 Service parameters

As far as the measurement of the service parameters is concerned, following the consolidated market trend and technological capabilities, the requirements can be satisfied by existing methodologies already implemented by Carriers with the exception of MOSCQE.

The above statement implies that the quality level of the Service parameters of the downstream segment (from the interface between the originating Service Provider /1st IPX Provider to the final user) can be affected by the quality of the terminating Service Provider network.

11.3 Methodologies for QoS Measurements – Single Network Domain

In this case only one IPX Provider connects both the originating and the terminating Service Providers.

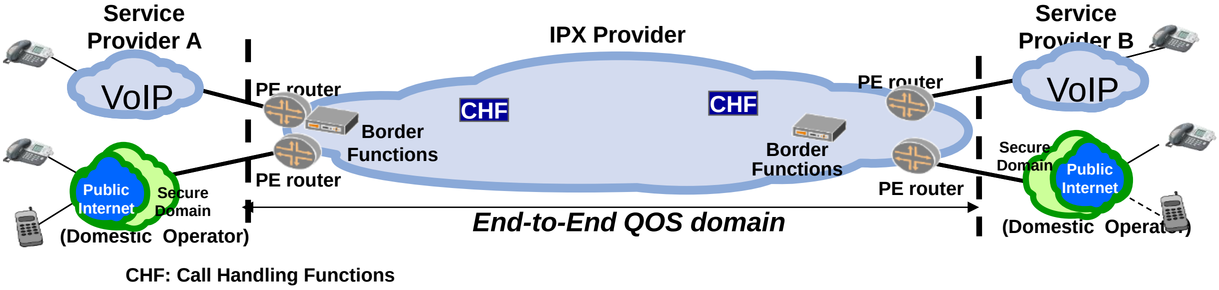

Figure 10 - QoS measurements for single network domain

It is recognised that Border Function, either at network ingress or at network egress, might not be co-located with the PE router so identifying an internal network segment shorter than the real IPX Provider's network domain. On the basis of the following guidelines paragraphs, it is noted that the results in that having Border Functions close to the PE router leads to more accurate measurement and is therefore advisable. However, it is also recognised that it may not be economically viable to have a Border Function co-located with each PE router. Therefore, a trade-off is required between the number of PE routers, the number of Border Function and the relevant economics.

In this scenario the IPX Provider can measure:

Round Trip Delay via RTCP[5]: Being the RTP control protocol uniquely positioned to mimic voice packet behaviour better than any other control protocol, it is suggested this protocol is adopted to measure round trip delay. This is a passive measurement performed on all live traffic and it calls for a full compliance of the RTP end-point to the existing standards, specifically IETF RFC 4855 [30]

It is noted that one way delay, as of today, cannot be measured with RTCP. As a result, with regard to the MOS measurement, since ITU–T G.107 R FACTOR/ G.107 E-model [39] requires one way delay measurement, this is estimated by halving the round-trip delay. This approximation is valid assuming symmetrical IP routing on the underlying IP backbone; in some cases, for various reasons (geography, redundancy, optimisation) this might not be the case.

An IETF draft [34] addresses this subject of one way delay via RTCP. The relevant document is a work in progress and the capabilities defined in it will be available on the Border Functions in the future.

Though the measurement of the Round Trip Delay via RTCP, being an embedded capability of the Border Functions, seems the most common methodology to be used by IPX Providers, it has to be noted that other approaches might be implemented. One alternative candidate solution is to use (non-intrusive) RTP monitoring relying on external probes.

Packet Loss via RTP:

Measuring RTP which is the real voice traffic is the most accurate approach of measuring the performance of the voice application. It is suggested this protocol is adopted to measure packet loss.

Packet Jitter via RTP:

For the same reasons as for the loss measurements, for jitter measurement, RTP is uniquely positioned to measure accurately live traffic.

[5] In the current version of GSMA IR.92, RTCP is turned-off during an active call.

11.4 Methodologies for QoS Measurements – Multiple Networks Domain

In this case, there is more than one IPX Provider between the originating and the terminating Service Providers. Two different approaches are discussed: the first one is related to an immediate implementation whereas the second one is related to a medium term implementation.

11.4.1 Aggregation-based approach

In the figure below two IPX Providers are connected with the objective to produce an end-to-end report for originating Service Provider A across IPX Provider A and B.

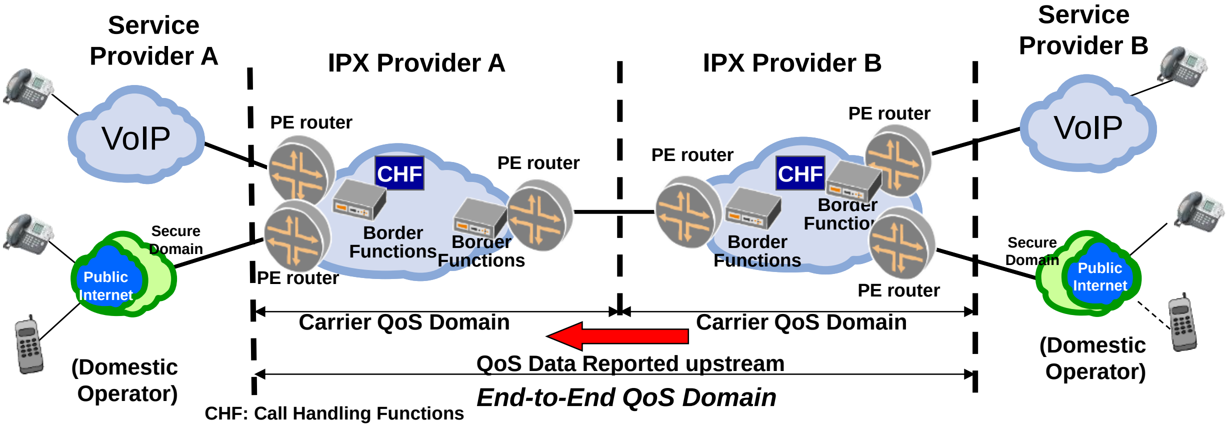

Figure 11- Aggregation based approach

The IPX Provider delay on the NNI between two IPX Providers in this document is assumed to be negligible since IPX Providers, in the vast majority of the cases, interconnect in TeleHouses / Carrier Hotels. If this condition is not met the transmission delay has to be added and considered an offset.

The performance across two domains is estimated by aggregating the performance across each domain. This can be computed as follows:

Delay: each segment is measured as described in the single domain approach. The total delay is estimated by adding up the delay over each domain.

Loss: each segment is measured as described in the single domain approach. The total Packet Loss is estimated by calculating the complement of the joint probability of a successful transmission on both networks:

Packet Loss end-to-end = [1 - (1 - PL1) * (1 - PL2)]
where PL1 is the Placket Loss of the 1st network
and PL2 is the Packet Loss of the 2nd network

Jitter: no aggregation scheme can be applied since there is no mathematical model which can correlate the jitter data measured by each network in the end-to-end domain. Notwithstanding this technical difficulty, it is suggested the jitter measured by the last domain is passed to the originating Service Provider, since this measurement is the closest to the end of the IPX Providers' domain.

Consensus is required from the involved IPX Providers in order to report the requested QoS data to the originating Service Provider. Multiple ways can be adopted (e.g. secure ftp, download and import from web portal) and IPX Providers are free to agree the most suitable way provided that security and integrity of the data is preserved.

11.4.2 Media Loopback approach

An approach to be available on the second half of 2012 is the active measurement methodology based on media loopback which is under specification by IETF in draft-ietf-mmusic-loopback-18 [33].

The establishment of the requested loopback type is initiated by a “loopback source” using new SDP media attributes, thereby providing the capability to monitor the quality of the media in an active session using the offer/answer model [17] to establish a loopback connection. Also, guidelines on handling RTP [21], as well as usage of RTCP [30] and RTCP XR [23] for reporting media related measurements are provided for this solution. This relevant RFC is expected to be published by IETF in the future.

Hence, this methodology is based on dummy calls generated by the ingress Border Functions of the 1st Carrier / Service Provider up to the egress Border Functions of the last Carrier / Service Provider.

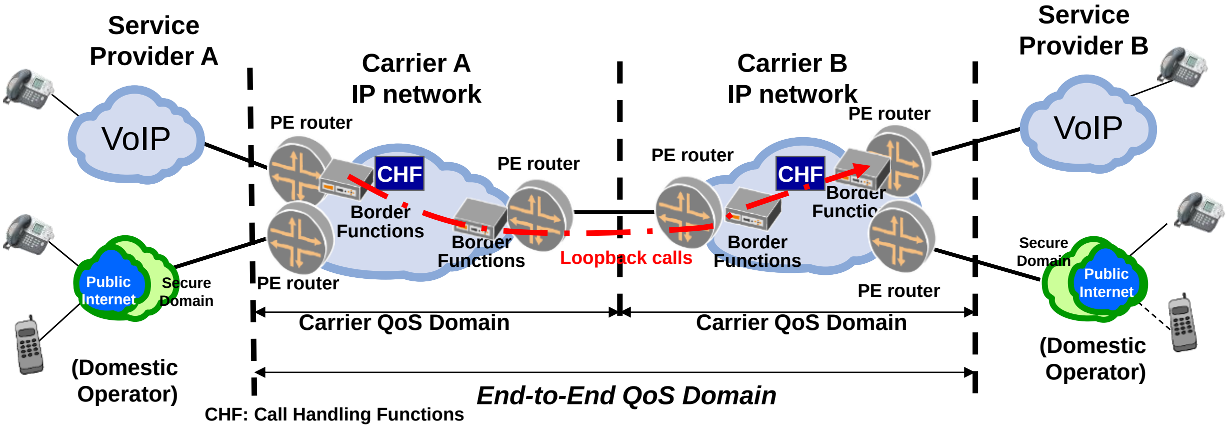

Figure 12- Media Loopback approach

The media loopback methodology identifies three operating modes (use cases), namely “direct loopback”, “encapsulated loopback” and “media loopback.” In the encapsulated packet loopback case, the incoming RTP packet is encapsulated and returned to the loopback source to generate one-way statistics for each direction of travel by examining the sequence numbers and time stamps in the outer header and the encapsulated packet header. The loopback source uses the packet header to generate two-way statistics as a result, it is suggested that this approach is adopted since it allows to measure the transport parameters (delay, loss and jitter) across multiple carriers with one call every sampling period.

It has to be noticed that if both IPX Providers’ Border Functions where the loopback call takes place operate with a stratum 1 Primary Reference Clock then the one way delay can be measured.

The downside of this methodology, to be carefully considered, is the number of required testing calls, which significantly increases when the number of routes to measure increases. For the sake of information, assuming a conservative approach where all IPX Providers are fully meshed and all routes of each Carriers / IPX Providers are used by all other IPX Providers, for a domain with 20 Carriers / IPX Providers, each with 8 POPs generating 2 calls / h , call duration 30 sec, each IPX Provider has to generate nearly 916k calls / month.

Another subject that deserves study and convergence among all involved parties is the type of the number to be called. There are 2 alternatives:

- SIP URI (e.g. Frankfurt@ipxprovidername.com) but presently not all CHF are capable to manage this addressing scheme;
- E.164 based addresses but it requires an ad-hoc testing numbering plan, for example with the definition of a special testing code, (i.e. equivalent to a country code) and a unique IPX Provider identifier (i.e. SPID).

11.5 KPI computation for SLA / QoS reporting

As a general principle each IPX Provider can offer KPIs of QoS parameters according to its own commercial policy.

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)

KPIs are averaged values over a time period, the length of which is outside the scope of this document.

Generally speaking, the reported KPI is obtained as a function of all the measured samples $KPI = f(KPI_0, KPI_1,..., KPI_N)$. The following functions are suggested:

- RTD: 95 / 99 % percentile or average
- LOSS: 95 / 99 % percentile or average
- JITTER: 95 / 99 % percentile or average

Note: as far as the above transport parameters are concerned, it has to be noticed that, from a commercial perspective, the function “*average*” is the preferred option.

- MOS: 95 / 99 % percentile
- ALOC: average (by definition)
- NER: average (by definition)
- ASR: average (by definition)
- PGRD: 95 / 99 % percentile.

12 Routing and Traffic Management

12.1 General Service Routing Principles

In section 5 a graphical example of an IPX domain for voice services has been described in figure 3. In addition to participating SPs, this figure shows IPX-Ps within the IPX domain, as well as Carriers and SPs outside this domain.

In agreement with GSMA White Paper on IPX that, in section 3.2, calls for a closed environment, in this document a routing confined within the IPX domain is always recommended unless:

- the call has to be routed towards a carrier in break-out in agreement with the contract signed between SP and IPX P;
- the call has to be routed towards a carrier in break-out since there are no available network resources which allow the call completion within the IPX domain.

The qualification process of carriers as IPX Provider as well as of Service Provider is outside the scope of this document.

12.2 Number of IPX Providers in the SP-SP communication

The GSMA IPX technical specifications require that not more than 2 IPX–Ps be involved in the SP-SP (end–to–end) communications, unless otherwise addressed by a specific GSMA service schedule. This limit is clarified for the voice service in AA.81 where it is written in section 2: *assume that any two PVI Service Providers are interconnected by at most two IPX networks unless this is not possible in exceptional cases. In the event that more than two IPX providers are needed to provide the connectivity, the QoS requirements shall remain unaltered*.

i3 Forum recognises the need to limit as much as possible the number of IPX Ps in the SP-SP communication to maximize the possibility of meeting quality requirements but, considering:

- the existing architecture of the voice network, very different from the GRX architecture, is based on hundreds of bilateral IP interconnections, and
- the intrinsic need of the wholesale business to route the call according the best price/quality trade-off,

the i3 Forum believes that the quality requirements can be achieved even if in some situations this GSMA IPX model constraint cannot always be met. Intercontinental calls are an example where the limit of 2 IPX–Ps cannot be guaranteed.

i3 Forum recognises that the number of involved IPX–Ps should not modify the quality requirements for a given SP-SP communication.

12.3 Routing Transparency

The minimum set of information that the IPX Provider shall provide to the Service Provider consists of the type of connectivity used to reach each terminating SP. These connections have to be classified into three groups depending if the connectivity is made through:

1) direct connectivity (i.e., there is only 1 IPX Provider from Originating Service Provider to terminating Service Provider),
2) indirect connectivity (i.e., there is more than 1 IPX Provider from Originating Service Provider to terminating Service Provider),
3) break-out connectivity (or gateway connectivity) between the IPX Domain and the Non-IPX Domain.

The above information is provided in the commercial agreement between the IPX provider and the service provider and applies under normal operating conditions (i.e., no network failures and/or no network congestion).

12.4 Opt-in / opt-out scheme

In compliance with GSMA doc AA.81 [9] section 6 no opt-in/opt-out scheme has to be supported for the VoIPX service.

12.5 Break-in / break-out connectivity

12.5.1 Break-in / break-out connectivity options

Break-in and break-out can be implemented via three technology options:

- via TDM interconnection
- via private IP interconnection as defined in section 6 of this document. This option implies that no unidentified third party is able to affect the bilateral voice over IPX service and hence:
    - only voice over IPX service or other IPX services traffic is exchanged across the interconnection;
    - only public IP addresses (provided by IANA) are used and they are not announced onto the Public Internet;
    - all the voice traffic, from the SP's PE router to the IPX P's border functions, shall be secured, either physically or logically, from Internet traffic.
- via public IP access interconnections as specified in section 6.2.4 of this document provided that
    - IPSec encryption is used for signalling information;
    - all the voice traffic, entering the IPX P network, crosses the IPX P's border functions.

12.5.2 Break-in / break-out notification

All SPs interconnected to the IPX domain via Public Internet in compliance with the access configuration described in section 6.3.1 have to be advertised to other SPs as break-in sources / break-out destinations.

All SPs and Carriers interconnected as described in section 9.4.1 have to be advertised to other SPs as break-in sources / break-out destinations.

12.6 Role of DNS and ENUM registry

GSMA IR.67 provides guidelines for DNS and ENUM in the GRX/IPX architecture. As defined in IR.67 DNS on the GRX/IPX backbone is completely separate from DNS on the Internet.

i3 Forum recognises that DNS/ENUM structure and capabilities can be used for addressing and routing purposes, but many different solutions are already in the market for providing routing and addressing capabilities to IPX Providers. Furthermore, these solutions are based on DNS/ENUM technology as well as other technologies (e.g. SS7/MAP protocol, SIP Re-direct protocol, Diameter protocol).

It is envisaged that the spreading of advanced routing and addressing schemes (complementing ITU-T E.164 model or alternative to ITU-T E.164 model) will increase in the future and two i3 Forum deliverables ([4] and [5]) contain the first principles to be considered and the first guidelines to be followed. In any case, regardless the technical and market evolution, an IPX–P has the right to select its own technical and commercial solution in order to successfully route the call to destination.

12.7 Number Portability Resolution

GSMA IPX requirements indicate that the Service Provider to which the IPX Provider terminates a call should not have to transit the call to another provider. Number portability complicates the satisfaction of this requirement. The i3 Forum Services WS [1] has also provided a requirement for number portability resolution by VoIPX providers. GSMA IPX plans for number portability resolution depend on the implementation of the PathFinder IPX Provider ENUM system. Prior to the point at which this is achieved, VoIPX providers will need to make use of other methods for number portability resolution. These may include (but are not limited to):

- Queries of national number portability databases where they exist and where the IPX P has access to them
- Use of third party number portability resolution services
- Queries or SIP INVITES directed to number block holding SPs

However it is possible for an IPX Provider to send traffic to a Service Provider, who, in turn, will transit the call to the recipient domestic Service Provider, if needed.

13 Accounting and Charging principles

The basic accounting and charging principles are discussed in section 12 of i3Forum’s IPX Core document[1]. The following are the issues related to the Voice over IPX service.

VoIPX is a specific product as voice is subject to termination rates (regulated or commercially negotiated) charged by the terminating Service Providers. Therefore, termination rates are generally minute-based. In a VoIPX context, there are costs to be covered: the termination defined by the terminating network and the transit defined by the IPX provider.

An IPX Provider is not obliged to provide separation of termination rate and transit fee unless commercially negotiated. Separation of termination and transit fees is also omitted if regulatory bodies or applicable law do not allow disclosure of termination rates.

13.1 Termination

Termination and transit fees (separate or merged) are generally minute-or second based. This reflects the commercial reality that the biggest part of the merged fee will in most cases be the termination cost which is minute or second based. In addition, all existing business support systems as well as commercial agreements and practises can continued be used.

Other non minute based termination models for termination are in theory possible but not identified in the international wholesale market today.

13.2 Transit

In case of a separate VoIPX transit fee, different accounting and charging models are in theory possible, for example:

- Minute/second based transit: defined per minute/second usage per destination or group of destinations or even ignoring the destination similar to the classic non IPX voice commercial practices.
- Installed sessions based transit: based on the capabilities provided by the IPX-P to send or receive VoIPX calls. Usage of the sessions is irrelevant, i.e. the fee is charged even if the sessions are not generated.
- Established sessions based transit: different from to the installed sessions based transit flat fee, the established sessions based transit fee is calculated per simultaneously established number of sessions. It is based on the established sessions provided by the IPX-P to send or receive VoIPX calls. This model can be stand alone or combined with the above installed sessions based settlement in the form of a minimum commitment combined with an option for occasional usage bursting.
- IP traffic based transit fee (bandwidth Mb/s or volume GB): relies on the same accounting principles and systems that are used for non-service aware IPX transport service and IP Transit service. They can be defined by installed or used capacity (Mb/s) or by volume (GB).

i3forum has evaluated the different accounting and charging models. Today the minute based model is the only relevant in the market and will be the predominant one for the foreseeable future. This model is the only one consistent with existing classic voice commercial models allowing continued use of certain practises and business support systems (e.g. billing systems) and agreements.

The other examples of theoretical models that i3forum does not deem mature and ready for market.