International Interconnection forum for services over IP (i3 Forum)

(www.i3Forum.org)

Source: Workstream "Technical Aspects"

Keywords: Voice over IPX

Technical Specification for Voice over IPX service

(Release 3.0, May 2012)

Date	Rel.	Subject/Comment
May 14th 2012	3	Alignment with i3F Interconnect document release 5
Oct. 27th 2011	2	Alignment with i3F Interconnect document release 4 – Inclusion of IPV6 references and deletion of some media options
Oct. 10th 2010	1	First Release of the document based on GSMA specifications and previous i3F deliverables

Executive Summary

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.

It is well known that GSMA defines the IPX model as a global, trusted and controlled IP backbone, consisting of a number of competing IPX carriers (IPX Providers) that will interconnect Service Providers according to mutually beneficial business models.

In this 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,

from Carriers (IPX Providers), as the entity offering interconnection services, serving any IPX compliant SP at the proper level of technical and economic efficiency,

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

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 with the identification of the proper standard/coding for routing, addressing, marking the IP packet;
    - Signalling with the support of SIP-I (specified by ITU-T) and SIP (specified by IETF) signalling protocols;
    - Media with the listing of the codecs, and their features;
    - Security with the support of the capabilities to be provided by Border Functions;
    - Quality of service measuring model encompassing the parameters' definition, guidelines for achieving these measurements and their related metrics;
    - Service Routing with the description and service impacts of the concepts of "confined routing" and "break-in/ break-out";
- differentiates from current GSMA specification on some specific topics which have been matter of analysis and study between MNO representatives and i3 Forum.

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 as technical and commercial options outside the IPX environment, as per i3 Forum specifications [*i3 Forum , "Technical Interconnection Model for International Voice Service", Release 5, May 2012*], and Service Providers/Carriers are free to request/offer Internet-based services according to their own policies. Consequently, the existing interconnection model between Carriers and the new IPX model are both legitimate and will co-exist being that Service Provider and IPX Provider (Carriers) are free to request / to offer the model more suitable for their own commercial / technical policies.

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

Table of Contents

1 Scope and Objective of the document

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 [9].

GSMA establishes the IPX model as a global, trusted and controlled IP backbone that will interconnect Service Providers 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 [9]. The IPX environment will consist of a number of IPX carriers (IPX Providers) in competition, selling interconnect services to Service Providers. The IPX Providers' networks will be mutually interconnected where there is demand by Service Providers.

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 [1], 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
3pcc	Third Party Call Control
3PTY	Three-Party conference
ACL	Access Control List
ACM	Address Complete Message
ACR	Anonymous Call Rejection
AF	Assured Forwarding
ALG	Application Level Gateway
ALOC	Average Length Of Conversation
AMR	Adaptive Multi-Rate
AMR-NB	Adaptive Multi-Rate Narrow Band
AMR-WB	Adaptive Multi-Rate Wide Band
AMS-IX	AMSterdam Internet eXchange
ANM	Answer Message
AS	Autonomous System
ASP	Application Service Provider
ASR	Answer Seizure Rate
ATM	Asynchronous Transfer Mode
BA	Behavior Aggregate
BE	Best Effort
BFD	Bidirectional Forwarding Detection
BGCF	Breakout Gateway Control Function
BGP	Border Gateway Protocol
BICC	Bearer Independent Call Control
BSS	Business Support System
CBC	Cipher Block Chaining
CC	Country Code
CCITT	Consultative Committee for International Telegraphy and Telephony
CD	Call Deflection during alerting
CDR	Call Detail Record
CF	Call Forwarding
CHF	Call Handling Function
CIN	Calling Party's Number
CLI	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CN	Comfort Noise
CN	Core Network
COLP	Connected Line identification Presentation
COLR	Connected Line identification Restriction
CPN	Called Party's Number
CPU	Central Processing Unit
CS	Circuit Switched
CS-ACELP	Conjugate-Structure Algebraic-Code Excited Linear Prediction
CSCF	Call Session Control Function
CSMA/CD	Carrier Sense Multiple Acces/Collision Detect
CUG	Closed User Group
CW	Call waiting
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
Diffserv	Differentiated Services
DNS	Domain Name Service
DoS	Denial of Service
DPO	Dynamic Port Opening
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
DTX	Discontinuous Transmission
DWDM	Dense Wavelength Division Multiplexing
E2E	End to end
EF	Expedited Forwarding
EG	ETSI Guide
ENUM	E.164 NUmber Mapping

ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
EXP	MPLS header EXPerimental use field
FNO	Fixed Network Operator
FoIP	Fax over IP
GIC	Group Identification Code
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSDN	Global Software Defined Network
GSM	Groupe Speciale Mobile
GSMA	GSM Association
GSN	Global Subscriber Number
HW	Hardware
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
IC	Identification Code
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFP	Internet Facsimile Protocol
IFT	Internet Facsimile Transfer
IKE	Internet Key Exchange
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPI	IP Interconnect
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
ISP	Internet Service Provider
ISUP	ISDN User Part
ITU	International Telecommunications Union
IVR	Interactive Voice Response
KPI	Key Performance Indicator
LBR	Low Bit Rate
M3UA	MTP 3 User Adaptation
MAP	Mobile Application Part
MF	Multi-Field Classifier
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MGW	Media Gateway
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
MPLS	Multi Protocol Label Switching
MTP	Message Transfer Part (SS7)
MVNO	Mobile Virtual Network Operator
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NB	Narrow Band
NDC	National Destination Code
NER	Network Efficiency Ratio
NGN	Next Generation Network
NN	National Number
NNI	Network to Network Interface
OCN	Original Called Number
OIP	Originating Identity Presentation

OIR	Originating Identity Restriction
OLO	Other Licensed Operator
OSS	Operations Support System
PCM	Pulse Code Modulation
PDH	Plesiochronous Digital Hierarchy
PE-router	Provider Edge router
PGAD	Post Gateway Answer Delay
PGRD	Post Gateway Ringing Delay
PHB	Per-Hop Behaviour
PLMN	Public Land Mobile Network
POS	Packet Over Sonet
PP	Packetisation Period
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
RgN	Redirecting Number
RI	Redirecting Information
ROHC	RObust Header Compression
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
SCCP	Signaling Connection Control Part (SS7)
SCTP	Stream Control Transmission Protocol
SDES	Source DEScription
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SGF	Signaling Gateway Function
SIGTRAN	Signaling Transport suite of Protocols
SIGTRAN	SIGnalling TRANsport
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
SPRT	Simple Packet Relay Transport
SR	Sender Report
SRTP	Secure Real Time Protocol
SS7	Signalling System 7
STQ	Speed processing Transmission and Quality aspects
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE MPLS	Traffic Engineering MPLS
tel-URI	Telephone Uniform Resource Identifier
THP	Traffic Handling Priority
TIP	Terminating Identification Presentation
TIR	Terminating Identification presentation Restriction
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TOS	Type Of Service
TPKT	Transport protocol data-unit Packet
TSG	Trunk Sub Group
TUP	Telephone User Part
UDP	User Datagram Protocol
UDPTL	facsimile UDP Transport Layer

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUI	User-to-User Information
UUS1	User to user signalling 1
VAD	Voice Activity Detection
VBD	Voice Band Data
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoIPX	Voice over IPX
VPN	Virtual Private Network
WB	Wideband

3 References

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

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

[3] i3 Forum “IP International Interconnections for Voice and other related services“, Release 3.0, June 2010

[4] VOID

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

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

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

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

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

[10] GSMA AA.80 “Agreement for IP Packet eXchange (IPX) Services”, Version 4.1, July 2011

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

[12] GSMA IR.34 “Inter-PLMN Backbone Guidelines”, Version 5.0, December 2010

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

[14] GSMA IR.40 “Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminals”, Version 6.0, March 2011

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

[16] IETF RFC 1918 “Address Allocation for Private Internets”, February 1996

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

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

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

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

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

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

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

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

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

[26] IETF RFC 3393 “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)”, November 2002

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

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

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

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

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

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

[33] IETF RFC 4193 “Unique Local IPv6 Unicast Addresses”, October 2005

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

[35] IETF RFC 4271 “A Border Gateway Protocol 4 (BGP-4)”, January 2006

[36] IETF RFC 4733 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, December 2006

[37] IETF RFC 4855 “Media Type Registration of RTP Payload Formats”, February 2007

[38] 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

[39] IETF RFC 5806 “Diversion Indication in SIP”, March 2010

[40] IETF RFC 5880 “Bidirectional Forwarding Detection”, June 2010

[41] IETF RFC 5881 “Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)”, June 2010

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

[43] 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

[44] ANSI T1.105 “SONET - Basic Description including Multiplex Structure, Rates and Formats”

[45] ITU-T Recommendation E.164 “The international public telecommunication numbering plan”, 1997

[46] ITU-T Recommendation E.411 “International Network Management – Operational guidance”, March 2000

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

[48] ITU-T Recommendation E.437 “Comparative metrics for network performance management”, May 1999

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

[50] ITU-T Recommendation G.707 “Network Node Interface for the Synchronous Digital Hierarchy(SDH)”, 01/2007

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

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

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

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

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

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

[57] ITU-T Recommendation V.150 “Modem-over-IP networks: Foundation”, July 2003

[58] ITU-T Recommendation V.150.1 “Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs”, January 2003

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

[60] ITU-T Recommendation Y.1540 “Internet Protocol Data Communications Services - IP Packet Transfer and availability performance parameters”, November 2007

[61] 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

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

[63] 3GPP TS 23.107 “Quality of Service (QoS) concept and architecture”, 2009

[64] IEEE 802.3 “Telecommunications and Information Exchange Between Systems--Specific Requirements Part 3: CSMA/CD Access Method and Physical Layer Specifications”, 2008

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 QoS, 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).

   In the scope of this document only E.164 numbers shall be used as destination address. These numbers shall be used in tel-URI and SIP URI formats as described in section 9.

3) **IPX Provider (IPX P)**: A business entity (such as an IP Carrier) offering IP interconnect capabilities to Service Providers, possibly through interconnection with other IPX Providers for one or many IPX services compliant with the IPX operation 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.

   The above definition of Service Provider, IPX Provider and End-to-end are still valid in the VoIPX context.

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

5 IPX Reference Configuration for Voice service

5.1 General Configuration

The general IPX reference configuration for Voice Services is given in the following figure with only 2 IPX Providers depicted.

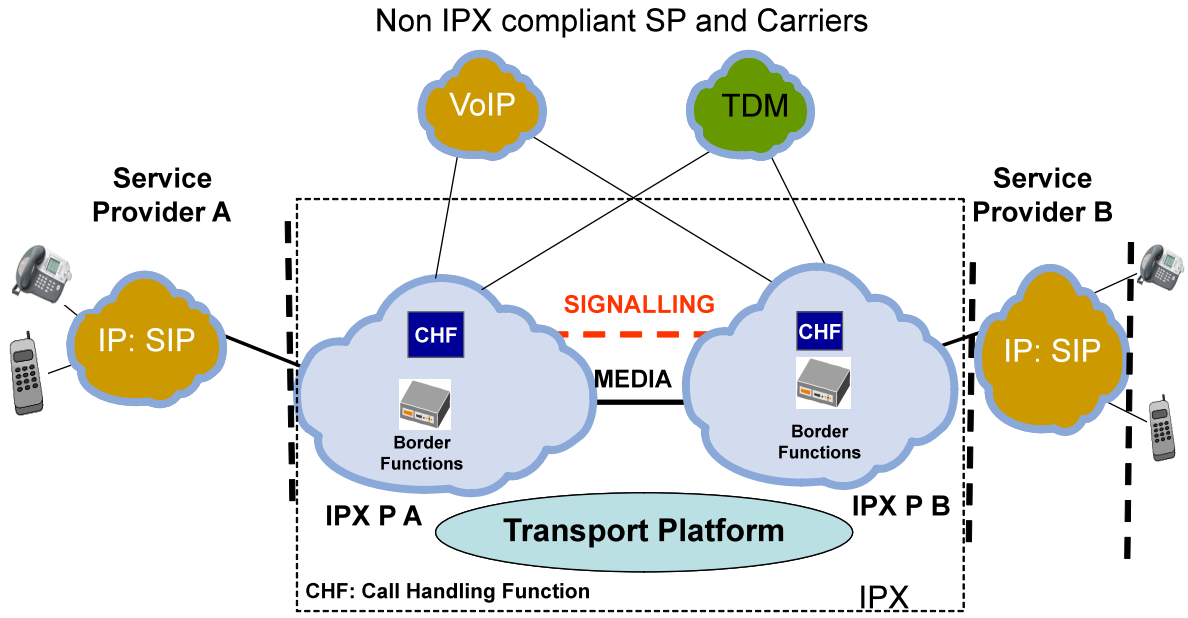

Figure 1 - General IPX Reference Configuration for Voice Services

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, QoS and security shall be fulfilled. Further details can be found in section 12.5.

Different types of transport functions over the interconnection for both from Service Provider to IPX Provider and between IPX Providers are given in Section 6.

The geographical scope of the IPX domain is given in 0. The end-to-end (E2E) interconnection responsibility (to be intended from SP-to-SP) is defined from egress port of the interconnecting element of the originating Service Provider network towards its own IPX Provider, to the ingress port of the interconnecting element of the terminating Service Provider. In this context, end-to-end corresponds to the above definition "from Service Provider premises to Service Provider premises".

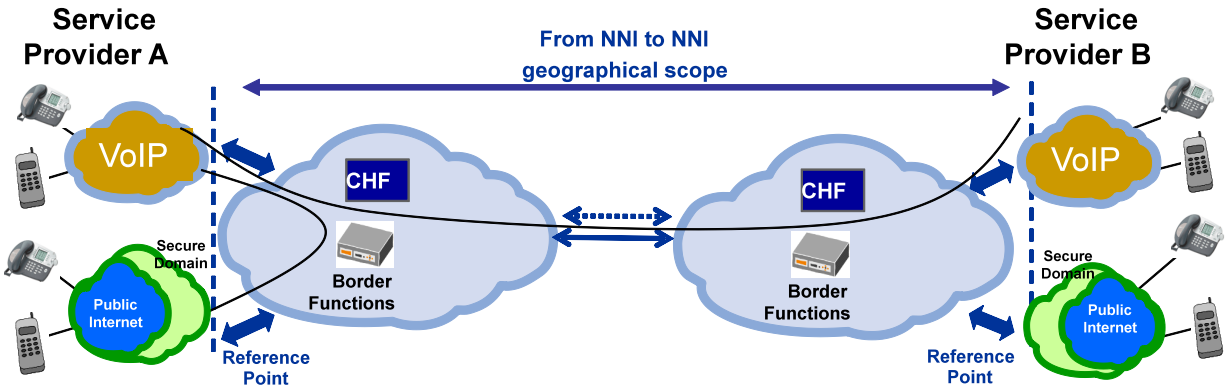

Figure 2 - Geographical scope of an IPX communication

The following basic requirements apply:

- More than one IPX Provider can be involved in the end-to-end (SP-to-SP) connection
- Even though the focus of this document is on voice service, IPX being a multiservice platform, the interconnection functions are intended to be multiservice, capable of providing multiple quality levels and modular (i.e., some functions are not needed for specific service models and/or specific end-to-end services)
- The interconnection functions are intended to provide a “private communication path” (i.e., separated and protected from the Public Internet)
- Security functions shall be implemented among interconnection functions.
- The entity that provides the interconnecting physical line between SP and IPX Provider is responsible for ensuring the SLA’s for that physical line (as described in AA.80 [10] annex 8)
- For services other than voice new requirements can be added.

5.2 Architecture of the IPX Domain for Voice Services

0below provides an overall sketch of the IPX domain together with compliant Service Providers and Non-Compliant Service Providers and Carriers.

Compliant Service Providers generate IP traffic towards IPX providers across interfaces specified in the following sections. Each compliant SP can interconnect to one or more IPX Providers.

IPX Providers can implement both direct (i.e. bilateral) interconnections and shared (i.e. multilateral) interconnections. A shared multilateral interconnection can be implemented in private and/or public locations where IPX Providers can meet.

The private locations would be those set up by a group of IPX Providers and the public ones will be those created by a third party with open access to IPX Providers.

Note: in the GSMA IPX related documents, the public locations are described as Peering Points.

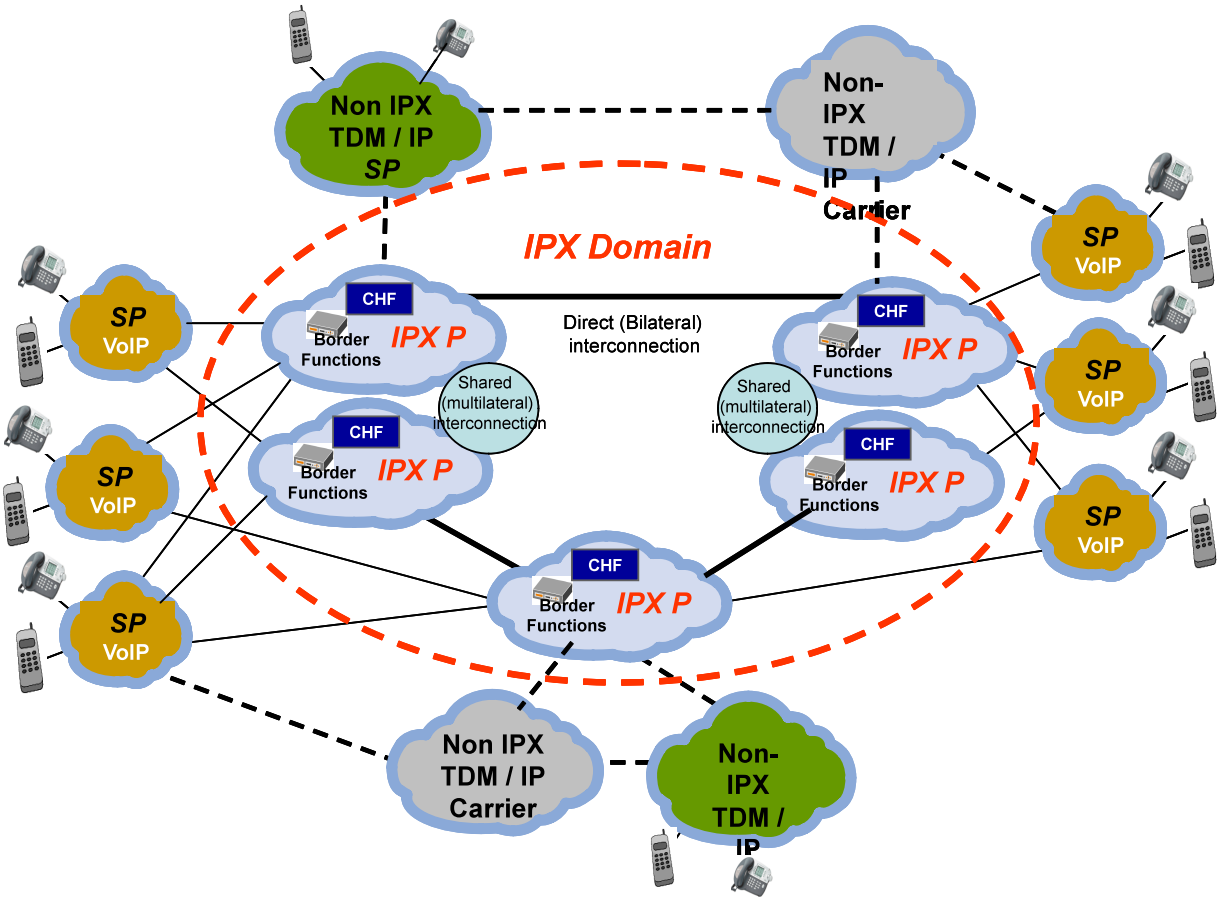

Figure 3 - Example IPX domain

As of early 2012, the GSMA has identified/set-up three public locations (Peering Points) in AMS-IX Amsterdam, Equinix Ashburn and Equinix Singapore for GRX/IPX services that can be used for VoIPX services. As the IPX/VoIPX traffic develops the number of public locations could increase. See also section 14 Annex A - Architecture of VoIPX platform.

5.2.1 Break-in / break-out Concepts

Allowing break-in/break-out via 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 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 MNOs would have to keep TDM interconnects operational in parallel to IPX-based interconnects in order to have access to these providers;
- Break-out / break-in interconnections support a faster deployment of IPX services for voice as it breaks the dependency on all networks migrating to IP at the same time.

5.2.1.1 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 the security of the end-to-end (SP-to-SP) connection is maintained and remaining capabilities are unaffected and are compliant with the commercial agreement between originating SP and IPX Provider.
- Due to network faults within the IPX domain which make the break-out route the only way to terminate the call. In this case the security is maintained unaffected. 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.

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

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 IPX Proxy in the VoIPX environment

The IPX proxy is a conceptual network element described in GSMA IR.34 [12] Annex B. 0below depicts the IPX proxy in a VoIPX environment. Inside one IPX Provider's network the IPX Proxy consists of all equipment and functions from the ingress Border Function up to and inclusive of the egress Border Function. This includes the Call Handling Function, but also other functions (e.g., media or signalling protocol conversion or IPv4/v6 translation, if required). The network between Provider Edge routers and Border Functions are not part of the IPX Proxy.

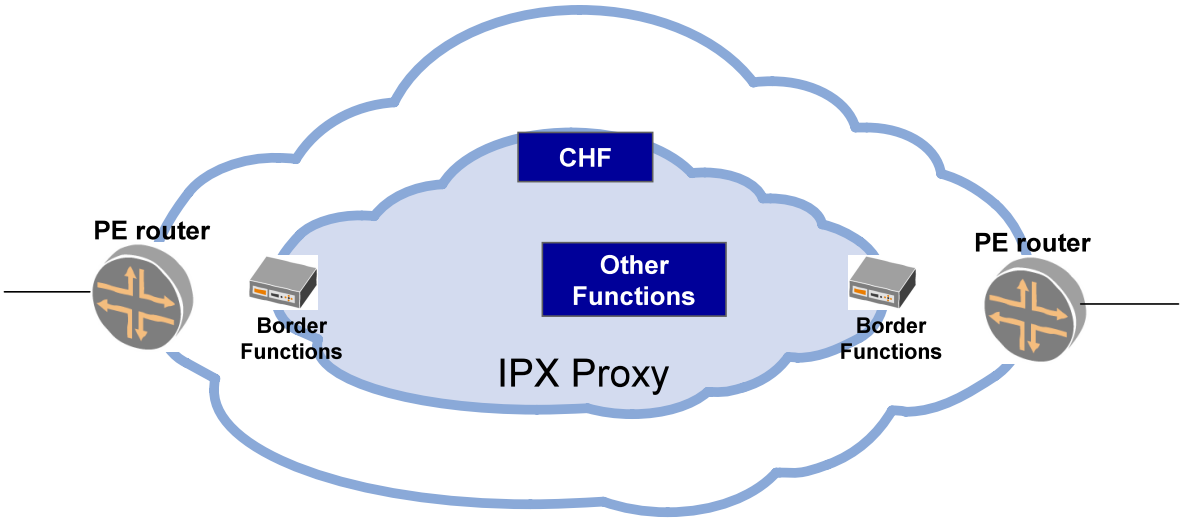

Figure 4 - IPX Proxy concept in VoIPX service

5.4 Connectivity Options

The IPX consists of two layers:

the Transport Layer provides connectivity between two Service Providers. This layer provides a guaranteed QoS bit-pipe function,

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.

5.4.1 Bilateral – Transport Only (transport without service awareness)

According to GSMA IPX White Paper section 6.2.1 *a bilateral connection between two Service Providers using the IPX transport layer with guaranteed QoS end-to-end. In this case, settlement is independent of the IPX Domain but connectivity still operates within IPI key business principles. Cascading of responsibilities (such as QoS) applies but not cascading of payments (Cascade billing). Each Service Provider will also pay their respective IPX Provider for the transport capacity, potentially depending on the level of QoS provided.*

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).

5.4.2 Bilateral - Service Transit (transport with service awareness)

According to GSMA IPX White Paper section 6.2.2 *a bilateral connection between two Service Providers using the IPX Service layer and the IPX Transport layer with guaranteed QoS end-to-end. Within Service Transit, traffic is transited though IPX Providers but prices (termination charges) are agreed bilaterally between Service Providers and settlement of termination charges can be performed bilaterally between the Service Providers or via the IPX Providers (upon the Service Provider's choice).*

This connectivity mode is considered out of scope for this document being not clear some business and technical implications given by possible hybrid configurations (i.e. one SP requesting the Service Transit connectivity mode towards another SP requesting the Transport Only connectivity mode).

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

According to GSMA IPX White Paper [9] section 6.2.3 *a multilateral connection using Hub functionality: Hubbing/multilateral connectivity is where traffic is routed from one Service Provider to multiple destinations/Interworking partners through a single agreement with an IPX Provider. Cascading of responsibilities applies. Cascading of payments may be applied depending on the service.*

This connectivity mode is the one in which the IPX Providers bring more value to the Service Providers and thus is the focus of this document.

5.4.4 Obligations for Connectivity Options for IPX Providers

The scope of this document is limited to the Multilateral – Hubbing connectivity mode.

An IPX provider is not obliged to offer all connectivity options: Transport, Service Transit and/or Service Hubbing.

5.5 Relationship to other IPX services

In document IR.34 [12], GSMA provides guidelines and technical information on how Inter Service Provider IP Backbone networks are set up, and how Service Providers will connect to it. The Inter Service Provider IP Backbone is defined as the collection of interconnected GRX and IPX Providers' networks, where the IPX is considered as an evolution of the GRX.

The IPX platform allows for the interconnection of any type of Service Providers (MNO, FNO, ISP, ASP, etc) and introduces the concept of end-to-end (i.e. from Service Provider premises to Service Provider premises) QoS as well as cascade billing.

The first three releases of this document, being dedicated to the specification of Voice over IPX, do not address some specific GSMA requirements pertaining to data services, but i3 Forum Carriers intend to expand the scope of this document to data services in next releases with the objective to address the whole set of GSMA requirements and to implement, as a target, a fully converged multiservice architecture.

As a result, the i3 Forum endorses the intrinsic value of the IPX model in terms of service integration and, notwithstanding the scope of this document is limited to voice service, each Carrier, acting as IPX Provider, can develop integrated service offerings encompassing one or more data services.

6 Transport Functions

This section recommends alternative reference transport configurations for implementing the NNI between a Service Provider and an IPX Provider and the NNI between two IPX Providers.

Assuming the IPX domain as a global private infrastructure, interconnecting managed IP networks, carrying different types of traffic, the interconnections between these networks shall be private, i.e. no unidentified third parties are able to affect the service.

In order to retain the private interconnection feature the following conditions have to be satisfied:

- Only VoIPX or other IPX services traffic is exchanged across the interconnection.
- All the involved IP addresses in the IPX address space (i.e., *PE router* interface, *P router* interface, border function interface) cannot be reached from unidentified entities via Public Internet and, as defined in GSMA IR.34 [12] have to be public, but they shall neither be announced onto nor be reachable from the Public Internet.
- The VoIP traffic, from the PE router to the border functions in a IPX Provider/SP's domain, shall be secured, either physically or logically, from Internet Transit traffic.

This security can be achieved:

- **Physically**: by implementing separated and dedicated networks for the two types of traffic.
- **Logically**: implementing different mechanisms such as native MPLS, Virtual Private Network (at layer 2 and 3) and tunnelling (e.g. IP Sec).

6.1 Internet Protocol Versions

Bilateral Voice over IPX interconnections may occur using either IPv4 or IPv6 network protocols; in the context of this document IP refers to both IPv4 and IPv6 protocol versions. IPv4 refers to the commonly deployed protocol version using 32 bit addressing and IPv6 to the protocol version using 128 bit addressing.

There are currently no generally deployed solutions that allow transparent interworking between these two IP protocol versions for Voice over IPX interconnection scenarios. Therefore the scenarios described within this section can use either IPv4 or IPv6 protocol versions but versions cannot be mixed on the same logical interconnect; both parties in the interconnection shall be using the same protocol version. Border Function within each IPX Provider network will require to be able to perform interworking between logical interconnects operating on IPv4 and IPv6.

6.2 Generic Cases of Transport Configurations

6.2.1 Case 1- Layer 1 interconnection

In this configuration a dedicated physical link (provided by one involved operator (IPX P/SP), or by the two involved operators, or by an identified third party) is implemented between PE routers or layer 2 switches, or directly between border functions.

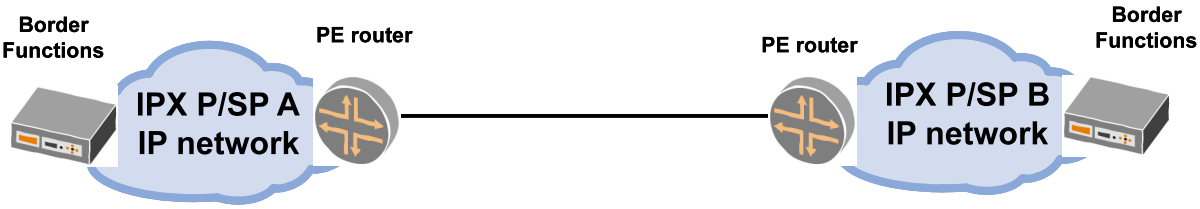

Figure 5 - Layer 1 Private-oriented Interconnection Configuration

6.2.2 Case 2- Layer 2 interconnection

In this configuration a dedicated physical link (provided by one involved operator (IPX P/SP), or by the two involved operators, or by an identified third party) is implemented between PE routers or layer 2 switches, or directly between border functions passing through an Ethernet switch network run by a third party (e.g., telehouse/carrier hotel owner, Internet Exchange Point owner). The switch provider will assign specific *VLAN*s for each interconnection allowing for the aggregation of several interconnections over the same physical link.

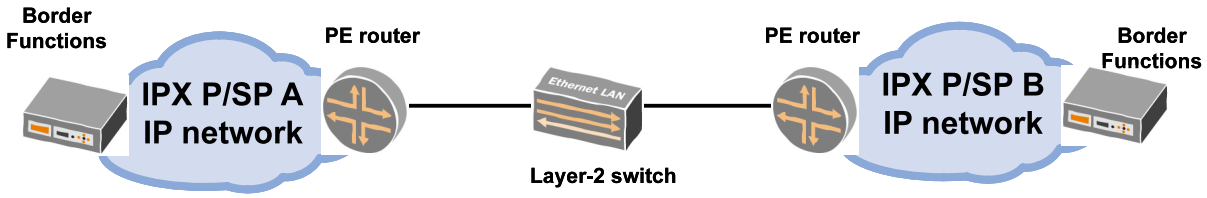

Figure 6 - Layer 2 Private-oriented Interconnection Configuration

A shared interconnection (see Sec. 5.2) is a special case of this model in which multiple carriers are interconnected in the same layer 2 network as is described in [12] section 6.4.

6.2.3 Case 3- Layer 3 interconnection

In this configuration a dedicated virtual link is implemented between PE routers passing through a third party IP private network. The 3rd party IP network provider will establish a VPN between the carriers' networks and shall provide *QoS* mechanisms and shall guarantee appropriate SLAs. The 3rd party IP network provider and both carriers will be required to use the same IP protocol version: IPv4 or IPv6.

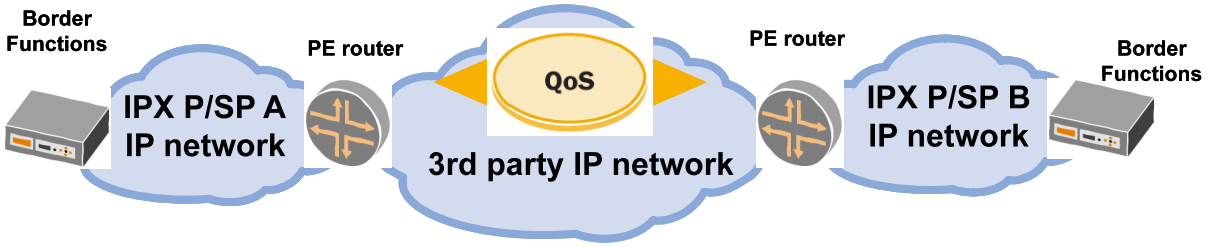

Figure 7 - Layer 3 Private-oriented Interconnection Configuration

6.2.4 Case 4- Layer 3 interconnection via Public Internet

As a special case, in this configuration, an SP is connected to an IPX Provider via the Public Internet using either IPv4 or IPv6 by means of a VPN and using IP Sec encryption for signalling information.

In agreement with GSMA IR.34 [12] this configuration should be used in case the previous three configurations cannot be implemented both for technical and/or commercial reasons and it should never be used to interconnect two IPX P.

Figure 8 - Internet IPSEC SP/P Interconnection Configuration

6.3 Transport Configurations for SP to IPX P interconnection

For Service Provider to IPX Provider interconnection, the following transport configurations (as illustrated in Section 6.2) can be implemented:

1) Case 1 as a direct layer 1 private interconnection (e. g., via a leased line).
2) Case 2 as layer 2 private interconnection (e.g., via an Ethernet switch).
3) Case 3 as layer 3 private interconnection (e.g., via a 3rd party private IP network using a Virtual Private Network connection).
4) Case 4 as a layer 3 interconnection via Virtual Private connection over the Public Internet using IPSec as the encryption scheme.

6.4 Transport Configurations for IPX P to IPX P interconnection

For IPX Provider to IPX Provider interconnection the following transport configurations (as illustrated in Section 6.2) can be implemented:

6.4.1 Direct Interconnection

For IPX Provider to IPX Provider interconnection the following transport functions can be implemented:

1) Case 1 as a direct layer 1 private interconnection (e. g. via a leased line).
2) Case 2 as layer 2 private interconnection (e.g. via an Ethernet switch).

6.4.2 Shared Interconnection

For IPX Provider to IPX Provider interconnection, the shared interconnection (case 2 transport function of section 6.2.2) is most attractive when a sufficient number of IPX Providers are willing to interconnect in public/private locations. Typically the shared interconnection configuration is set up by a third party such as a Telehouse or similar.

6.5 Physical Interconnection Alternatives

The physical interface of the interconnection can be either, SDH POS – based or Ethernet-based (i.e., fast-ethernet, gigabit-ethernet or 10gigabit-ethernet).

6.5.1 SDH-based transport Systems

The ITU-T Recommendations G. Series shall be considered as reference documents, among these the ITU T Recommendation ITU-T G.707 [50].

For North America another reference document is ANSI T1.105 [44].

6.5.2 Ethernet-based transport Systems

The IEEE recommendations 802.3 [64] for Ethernet communication together with enhanced ethernet technologies such as fast-ethernet, giga-ethernet and 10giga-ethernet have to be considered (e.g. ISO/CIE 8802-3).

6.5.3 Interconnection redundancy

The level of redundancy of a specific interconnection can be enhanced by increasing the number of involved Border Functions. Additional redundancy can be achieved by increasing the number of involved PE routers by geographical separation.

6.6 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 Bandwidth (kbit/s)	IPv6 Bandwidth (kbit/s)
G.711	20	104.720	113.520
G.729	20	43.120	51.920
G.729	40	25.960	30.360

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.

6.7 IP Routing and IP Addressing

6.7.1 IP Routing

For all the above interconnection configurations, it is mandatory to announce only those IP addresses that need to be reached by the interconnecting IPX Provider.

The BGP protocol v4 should be used to exchange routes between different networks (both SP and IPX–P).

GSMA IR.34 [12] defines the use of certain BGP communities. This use does not affect the VoIPX as defined in this document.

It is recommended to tune timer parameters to appropriate values for the specific implementation, to ensure timely failure detection and convergence suitable for VoIP traffic. In addition, BFD [40][42] could also be used to speed up link failure detection and subsequent protocol convergence.

6.7.2 IP Addressing

The IPv4 addressing scheme shall be supported. The IPv6 addressing scheme is optional and can be agreed on a bilateral basis.

For the IPX address space IPX Providers will use only IP addresses assigned by IANA or related bodies as described in [14].

6.7.3 IP Packet Marking

In IR.34 [12] section 8.2 the following traffic classification, based on 3GPP's definitions in [63], is described:

QoS Information		**Diffserv PHB**	**DSCP**
Traffic Class	**THP**		
Conversational	N/A	EF	101110
Streaming	N/A	AF41	100010
Interactive	1	AF31	011010
	2	AF21	010010
	3	AF11	001010
Background	N/A	BE	000000

Note: Traffic Handling Priority (THP) specifies the relative importance of applications that belong to the Interactive traffic class

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

Traffic Type	**GSMA Traffic Class**

Voice Media	Conversational
Voice Signalling	Conversational or Interactive

Note: There is no agreement as whether the signalling has to be treated in the Expedited Forwarding ([19][20]) or Assured Forwarding ([18]) Per Hop Behaviours.

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

7 Signalling Functions

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

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 [1]

7.1.2 SIP signalling protocol profile

The SIP profile shall comply with RFC 3261 [21] 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 [31] which addresses SIP Timers specification, is optional. The IPX Provider receiving the INVITE message shall comply with IETF RFC 3261 [21] section 16.8 if IETF RFC 4028 [31] is not supported**.**
- The P-Asserted-Identity header defined in RFC 3325 [24] shall be transported transparently if present.
- The Privacy header defined in RFC 3323 [23] shall be supported.
- The Diversion header defined in RFC 5806 [39] shall be supported.
- The History-Info header defined in RFC 4244 [34] 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 then it is recommended to include the P-Asserted-Identity header, but in this case bi-lateral agreement should dictate final treatment (IETF RFC 3323 [23], 3325 [24]). When the SIP message is passed to a trusted domain, the P-Asserted-Identity header should not be removed (IETF RFC 3325 [24]).

7.1.3 SIP Message support

SIP methods as listed in the Interconnection Model [1], section 7.1.3 shall be supported.

7.1.4 SIP Header support

SIP headers as listed in the Interconnection Model [1], 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 [1], 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 [46] 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 [8].

8 Media Functions

This section discusses the recommendations for the voice path, fax and voice band data for VoIPX interconnections. For more information of the voice path, please refer to the i3 Forum – Technical Whitepaper on Voice Path Engineering [2].

Media functions in VoIPX interconnections should ensure the following:

- Transport for all the services;
- Transcoding, where required and applicable.

A VoIPX interconnection shall support the following services:

- Voice phone calls using different codecs;
- DTMF support;
- Fax connections;
- Modem connections.

These above listed services shall be accessible for both TDM and VoIP subscribers.

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 [27] and IETF RFC 3611 [29]. 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 [28]. The list of protocol parameters defined in this RFC [28] 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 [28]. 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 [28].
- 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 [25] (static PT 13 (8 kHz) or dynamic).
- Telephone Events (DTMF tones) as defined in the Section 3.3 of IETF RFC 4733 [36](dynamic)
- Telephone tones as defined in the Section 4.4 of IETF RFC 4733 [36] (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 [28].

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 [28] Section 2.

8.1.1.8 Security - security services and algorithms

According to RFC 3550 [27] 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 [15], 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 [28]. 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 [28] 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 [28] 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 [27] 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 [27].

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 below. 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 any transcoding related matter 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 are expected to 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 [37]

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 [38]

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 a 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 WB_AMR are taken from GSMA PRD IR.36 [13] and RFC 4867 [38]. The requirements for G.722 are taken from Dect-ND ETSI EN 300 175-8 [62]

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,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 [38]

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" [2].

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 [2] 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:

- transcoding should be avoided whenever possible, due to the impact on speech quality and delay;
- 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 is necessary and this companding conversion will 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;
- in the case of fixed-mobile interconnection, transcoding, if necessary, should always be performed by mobile service providers;

An extensive treatment of voice quality impairments generated by codec and/or transcoding functions is given in [2].

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 ([54], [55] y [56])
- VBD according to ITU-T V.152 [59]
- Pseudo VBD fax pass through

8.6.1 8.6.1 Fax over IP guidelines

T.38 fax relay ([54], [55] y [56]) shall be supported as the first choice. ITU-T T.38 version 0 (06/1998) [54] is mandatory, latest version 5 (09/2010) [56] 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 [53] 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 [59] 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 Modem connections

To enable point to point modem connections TDM–IP–TDM the following method shall be used:

- Modem relay according to ITU-T V150.1. [58]
- VBD according to ITU-T V.152 [59]
- Pseudo VBD modem pass through

8.7.1 MoIP Guidelines

Modem relay as defined in ITU-T V150.1 [58] should be used as the first choice.

It is also possible but not recommended to use Voice Band Data (VBD) mode, as defined in ITU-T V.152 [59] 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. In the latter case protocol stack should be: RTP\UDP.

Call discrimination procedure in case of modem TDM–IP–TDM connection should be performed according to V.150.1 [58] Section 20. Interworking procedure between T.38 and V.150.1 should be as in T.38 Annex F [56].

8.8 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 which can be encountered by a 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 [1], 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 [1], section 9.2.

9 Numbering and Addressing Scheme (E.164-based)

This deliverable is E.164-based [45]. The objective of this section is to define the format of numbers and addresses which 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 [21] and SIP-I [46]. 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 [45]. 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 [45] 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 [45] (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 [30]. 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 3996 [31]. 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 [21] section 19.1.1.

An example of a SIP-URI would be:

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

10 Security Functions

This section discusses the recommendations for security for international IP voice interconnections on the IPX. For more information please refer to the i3forum – Technical White Paper on Security for IP Interconnections [7].

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 [7]

10.3 Security Threats

An extensive discussion of security threats is given in i3 Forum White Paper on Security for IP Interconnection reference [7]

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

i3 Forum 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 [11] 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; [17][35]
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.

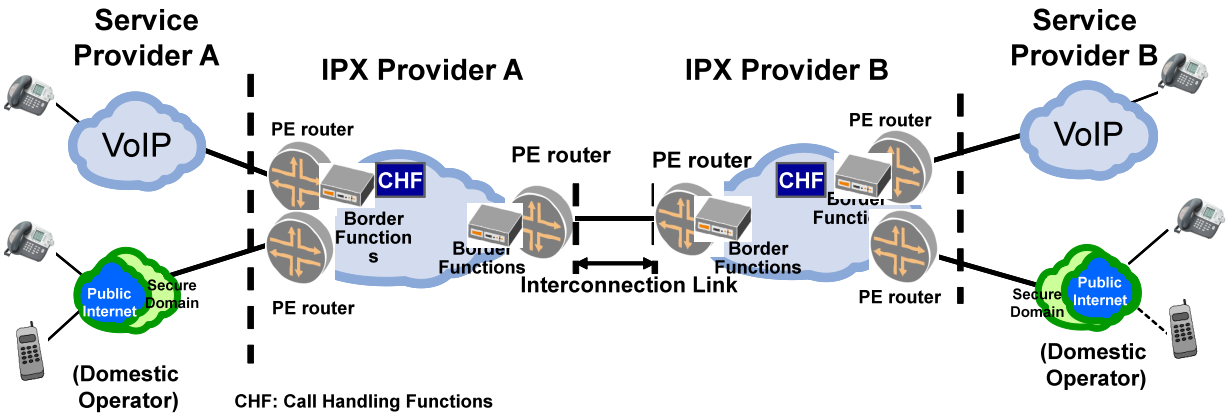

Figure 9 - Reference configuration for QoS measurement

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 [61].

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

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

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 [51] 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 [49] 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 [51]) using formula in ITU-T Rec G 107 Annex B [49]. 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 [48]:

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

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[2].

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 [46] with the following formula:

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

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

- 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.

[2] 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.

ASR depends on the user behaviour[3].

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 [47] released in 2002 with the following formula:

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

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

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:

[3] 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.

- 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.

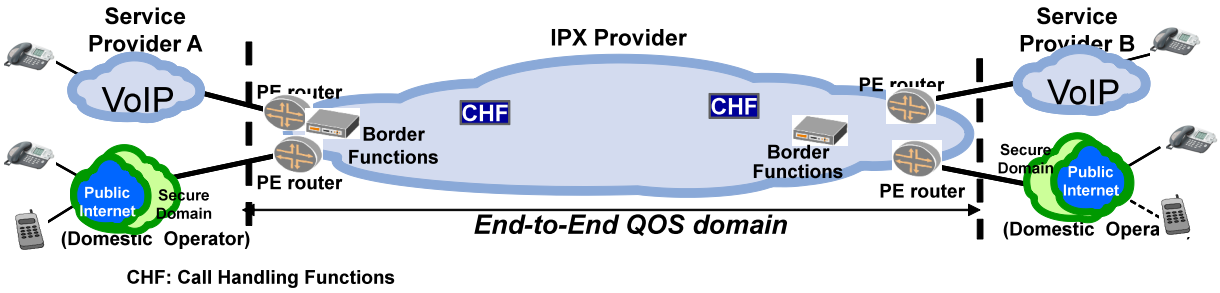

Figure 10 - QoS measurements for single network domain

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[4]: 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 [37]

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 [49] 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 [43] 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.

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.

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

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.

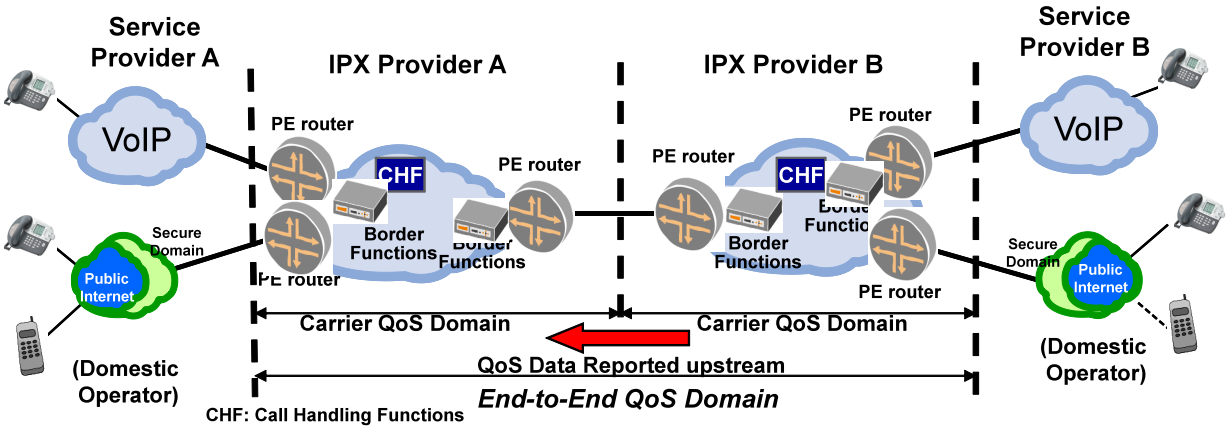

Figure 11- Aggregation based approach

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 [42].

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 [22] to establish a loopback connection. Also, guidelines on handling RTP [27], as well as usage of RTCP [37] and RTCP XR [29] 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.

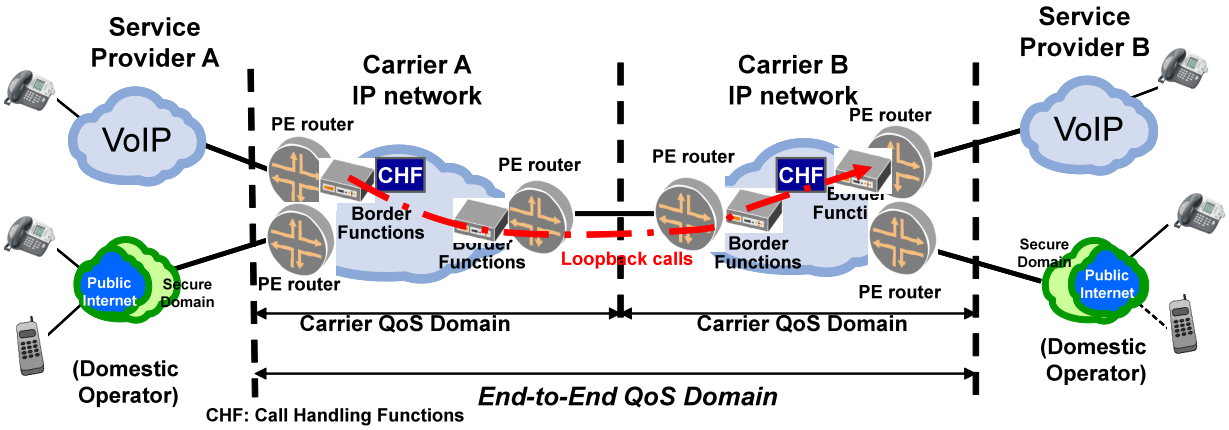

Figure 12- Media Loopback approach

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 which 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 which, 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 recommend that not more than 2 IPX–Ps be involved in the SP-SP (end–to–end) communications, unless otherwise addressed by a specific 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 [11] section 6 no opt-in/opt-out scheme has to be supported for the VoIPX service.

12.5 Break-in / break-out connectivity

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.

12.6 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 for terminating a voice call but, as a matter of fact, 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 ([5] and [6]) 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

13.1 Transit fee depending on destination

Transit fee (compensation charged by the IPX Provider for all the offered service excluding termination fee) for Multilateral Hubbing Service IPX connectivity options can vary and depends on the destination.

13.2 Charging transparency

An IPX P 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 disclosure of termination rates is not allowed by regulatory bodies or applicable law.

13.3 Accounting and Charging capabilities

The information flow to be exchanged from the transport and switching platforms with the relevant OSS/BSS systems is outside the scope of this document.

The information recorded in the Call Detail Record (CDR) shall support settlement and performance. The scope of this section includes only the data that require for exchange the information for settlement and performance. The CDR may also serve as a troubleshooting tool for certain information. This section does not address the format of the CDR in a IPX Provider's network nor the collecting method. Each IPX Provider may have additional proprietary fields for internal uses, which is not in the scope of this section.

Since calls may be originated or terminated in TDM or VoIP network, the CDR shall support data attributes for these two types of calls and services. A comprehensive list of these attributes can be found on [1].

14 Annex A - Architecture of VoIPX platform

The following text is based on the joint GSMA's IPIA and i3 Forum activities carried out in 2009.

14.1 Reachability / Coverage: interconnection obligations for IPX Providers

Every IPX Provider will provide the list of SPs that can be reached through the IPX domain by an SP contracting it. An SP may connect/contract more than one IPX P in order to reach all SPs that it is interested in by combination of the list of SPs of those IPX Ps.

In order to ensure that the Voice over IPX service develops in a way that is consistent with its core requirements of efficiency, quality of Service and security, it is important that a framework is defined that enabled IPX Providers to efficiently establish interconnection arrangements with other IPX Providers, in a manner that both minimises the physical distance that traffic has to travel between Service Providers, and is commercially sustainable to IPX Providers.

14.2 Global Interconnect Locations

It is expected that the IPX will re-utilise Interconnect locations that have already been established for GRX (IPX Zone Interconnect Locations in the following Table), as the IPX/GRX DNS has been deployed at these locations and it also minimises additional investment costs from IPX Providers.

IPX Zones	Shared Interconnection Location	Regions in each IPX Zone
Americas	Equinish Ashburn	North America (East Coast), North America (West Coast), Central America (incl. Caribbean), South America
Asia	Equinix Singapore	East Asia, South Central Asia, South East Asia, West Asia, Oceania
Europe & Africa	AMS-IX Amsterdam	West Europe, North Europe, East Europe, south Europe, Africa

Note: for the list of countries in each region please refer to section 8.3.2 of IR.34 [12]

The number of IPX Zones may increase as the IPX develops, and the level of commercial traffic over the IPX justifies this investment, but this shall be mutually agreed by a representative group of IPX Providers and Service Providers.

IPX Provider Interconnection Evolution

In order to assure DNS resolution, an IPX Provider will initially have to connect to one of the above IPX Zone Interconnect Locations to enable it to offer an IPX Service to any of its perspective Service Providers.

When the IPX Provider has ten or more Service Providers within an IPX Zone, it shall interconnect in that zone to the other IPX Providers who are present at that IPX Zone, subject to the other IPX Provider(s) having at least 10 Service Providers in that same IPX Zone.

It should be noted that IPX Providers are free to negotiate Private Interconnection Terms with other IPX Providers in an IPX Zone, as it may be more efficient for an IPX Provider to do this rather than connect to the IPX Zone Interconnect Location.