IPX White Paper

Version 1.2

22 March 2007

Security Classification Category (**see next page*****)***		
Unrestricted		

Security Information - UNRESTRICTED

This document is subject to copyright protection. The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association

Copyright Notice

Document History

Version	*Date*	*Brief Description*	*Editor / Organisation*
0.1	7 August 2006	First Merged Draft based on inputs from IPXFoc, GRXEv and IPX Project	T Jalkanen – TeliaSonera, E Sacco – Telecom Italia R Davies – GSMA
0.2-0.8	August 2006	Editorial improvements by editorial team	B Hunter – Vodafone A Dodd, D Cox, R Davies - GSMA
0.9	23 August 2006	Issue for EMC#46	IPX Project Team
1.0	5 September 2006	Whitepaper approved by EMC for internal use by GSMA. Identical to 0.9	IPX Project Team
1.1	6 October 2006	Revision to capture traffic separation/security issue.	IPX Project Team
1.2	22 March 2007	Minor revisions to unrestrict document	A Dodd GSMA

Table of Contents

EXECUTIVE SUMMARY

Mobile and Fixed Network Operators are evolving towards IP infrastructures with the advent of 3G, IMS and NGNs. The interconnect medium between these networks and towards ISPs is expected to be IP. The GSMA IPI project has identified commercial requirements for this environment which maintain the benefits of the Telecoms industry approach whilst introducing the advantages of IP technology.

This white paper sets out the agreed position of GSMA operators, describing the commercial and technical principles of an inter-operator network environment which delivers these IPI requirements. As a working title the network is called an IP Packet Exchange – IPX. The purpose of the paper is to document is to describe the concept of the IPX commercially and technically.

The IPX is a global, private, IP network which supports end-to-end quality of service and the principle of cascading interconnect payments. In order to provide these features the IPX is service aware unlike the Internet and the GRX.

The IPX environment will consist of a number of IPX carriers operating in open competition, selling interconnect services to Service Providers (mobile and fixed operators). The IPXs will be mutually interconnected where there is demand from Service Providers. Both IPX carriers and Service Providers will participate in and be subject to IPX governance to ensure the quality, security, and the technical and commercial principles of the environment are maintained. The definition and nature of IPX governance is not in scope of this paper.

The IPX may be used to interconnect any IP service. To provide interoperability (commercially and technically) amongst the community of Service Providers the interconnect aspects of the services must be standardised. An IPX is free to support any of the services they consider viable. A Service Provider may negotiate interworking with any IPX on a per service basis. An IPX may offer other non-standardised value-added services to requesting Service Providers, provided they do not conflict with the operation of the standardised IPX services.

The IPX supports three interconnect models, which Service Providers are free to choose on a per service basis:

- Bilateral Transport Only –the IPX provides transport at a guaranteed QoS. Each Service Provider will pay their respective IPX Provider costs for transport. The bilateral agreement is between end Service Providers and any payment of termination charges is a mater for the Service Providers.
- Bilateral Service Transit –the IPX provides QoS based transport and cascading interconnect payment facilities. This enables an originating Service Provider to make a single payment to their IPX Provider who passes on a payment on to the next IPX Provider in the value chain who pays the final termination charge to the terminating Service Provider.
- Multilateral Hub Service –the IPX provides QoS transport and cascading interconnect payments to a number of interconnect partners via a single agreement between the Service Provider and IPX. This “one-to-many” mode is operationally highly efficient for the Service Provider. Charging transparency is a requirement on both IPXs and Service Providers in this mode.

End-to-end quality is a key requirement for the IPX environment. Service Providers and IPX carriers alike will be subject to SLAs (and on a per service basis). The SLAs will be enforced by the principle of cascading responsibility, governance and by contracts. The appended SLA template describes all technical aspects of the environment covered by the SLA including the local tail and IPX peering/interconnect points.

The IPX architecture consists of a transport network capable of providing end-to-end quality of service, for example the conversational traffic class, in a private network. Transparent service proxies handle service aware functions, such as multilateral connectivity management and service transaction accounting. They can also support protocol interworking where Service Providers use different protocol versions for a common service. Security is provided by establishing a separate routing domain from the Internet and by the separation of traffic within the IPX. Peer-to-peer traffic is separated from server-to-server traffic as the former is considered a higher security risk. Security also relies on the establishment of a trusted environment whereby all connecting parties implement robust security in their own networks. These features represent a relatively simple evolution of the GRX concept.

This paper also sets out a series of commercial principles and a technical architecture which are applicable to any current and future IP service. The IPX will provide predictable and consistent quality of service for customers, rapid service rollout and market reach, new interworking revenues for IP Services and operational efficiency through multilateral agreements. The IPX uses the proven concepts of a private network from the GRX and the Service Proxy architecture from the GSMA SIP Trials.

1 DOCUMENT PURPOSE

The document is a whitepaper describing the commercial requirements for an IPX Provider, the technical architecture and the functional requirements for an interworking/roaming interconnect network that meets the requirements of the IPI Framework Business Architecture (see Section 3.3).

The purpose of this document is to set out the common position of GSMA operators for the IP Packet eXchange (IPX). This document is the stepping-stone between the “requirements” of the IPI Business Architecture and the “solution” to be developed in GSMA interworking specifications. It can also be used as the basis for discussion with external parties.

A Glossary and list of Definitions is given in Appendix A and B respectively.

2 SCOPE

2.1 In Scope

- Roaming and interworking legs for IP services
- Commercial requirements
- Technical description of generic functions and architecture (topology, routing, peering, addressing, security model, interface specification and so on)
- Quality of Service support
- Charging and accounting functions
- Basic descriptions of selected end-user services

2.2 Out of Scope

- Governance issues
- Detailed definitions of end-user services
- Functions specific to end-user services
- Standards aspects
- Network management
- Details of regulatory and legal aspects
- Interconnect charging models for premium-rate services
- Detailed Service Definitions
- Circuit Switched to Packet Switched voice/video conversion handled by IPX
- Back-office functions (such as OSS/BSS, invoicing and settlement)
- Accounting formats
- Detailed conformance testing/certification
- Load-balancing and high availability considerations
- Access to corporate networks
- Authentication, authorization and registration of end-users
- Regulatory requirements

3 INTRODUCTION

3.1 IP Interworking – Market Need

Following the widespread deployment of packet infrastructures using the GSM and UMTS air interfaces, Mobile Network Operators (MNOs) are expected to launch a wide range of new data services. At the same time, Fixed Network Operators (FNOs) are deploying Next-Generation Networks (NGNs) and ISPs are offering an ever-increasing number of services. Whilst competing, these commercial entities have the common objective of delivering traffic to each other in a profitable and cost effective way. The common protocol of these networks and services is the Internet Protocol (IP).

Service providers (MNOs, FNOs, ISPs and ASPs) need to maximise their connectedness through interworking and roaming arrangements for their subscribers to appreciate the full value of these services. The problem, simply stated, is how to make these arrangements in a controlled and efficient manner. The GSMA IPI project has produced a vision for an IP services business architecture that ensures that services are fully interconnected and supported by a sustainable commercial model. The project has laid out the requirements for a solution to this IP interconnection problem and these are documented in the IPI Framework Business Architecture. As a result there is a need for an industry wide commercial and technical interworking environment to be set up. The solution is an IP Packet eXchange (IPX) concept designed to be universally applicable to different types of Service Provider and provide controlled QoS.

3.2 IP Interworking – IPX Concept

The IPX will be 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. The IPX is different from the Internet and the GRX in that only Service Providers under contractual agreement may use it and it is service aware. The market for the features and functions of the IPX is expected to exist from mid-2007.

The IPX environment will consist of a number of IPX carriers operating in open competition, selling interconnect services to Service Providers. The IPXs will be mutually interconnected where there is demand by Service Providers. Both IPX carriers and Service Providers will be subject to IPX governance to ensure the quality, security and the technical and commercial principles of the environment are maintained. The definition and nature of IPX governance is not in scope of this paper.

Both models of interconnection using the IPX (on-net model) or some external alternative, such as the Internet, leased-line or an autonomous private network (off-net model) are legitimate and will co-exist. For many services and interconnection scenarios, the IPX will have clear advantages and will make it the solution of choice.

With the requirement for roaming in the packet services domain the GSMA developed a private network called a GRX. The current GRX is a network that supports GSM, 3G and WLAN (authentication) data roaming traffic between GSM MNOs for the best-effort traffic class. The GRX also supports the emergence of interworking services handling MMS and unnamed best-effort traffic class services using any control protocol. The GRX is documented in IR.34 *Inter-PLMN Backbone Guidelines*.

The IPX builds on the GRX concept adding:

- Connectivity to non-GSM operators
- A variety of charging models over and above volume-based
- End-to-end QoS for roaming and interworking (currently QoS for roaming is not supported by all GRXs)
- IPI based bilateral interworking support for specified services
- IPI based multilateral interworking support for specified services over a single Service Provider to IPX connection (in addition to the existing MMS Hubbing)
- Support for any IP services on a bilateral basis with end-to-end QoS

The high-level business requirements driving the IPX architecture are summarised below. These are taken from the IP Interworking Framework Business Architecture and from the GSM community's experience of managing IP services.

3.3 IP Interworking - Business Requirements

The business objective is for a variety of IP service providers to transfer traffic between each other under controlled circumstances, in compliance with minimum quality criteria via understood business models.

- The key business principles of the IP Interworking Framework Business Architecture are:
- *End-to-End focused service delivery* – with emphasis on Quality of Service and universal charging principles
- *Service interoperability* – universal service interworking (fixed and mobile)
- *Third party management* – managed access, clear enablers (for example, wholesale billing)
- *Customer protection* – against misuse for example, identity theft, fraud, invasion of privacy, unsolicited content, and so on
- *Initiating party pays* – drives market penetration/usage, matches "willingness to pay", limits issues associated with Spam
- *Cascading revenues* through the intermediary carrier from end-to-end, enabling simplified commercial agreements
- *Supporting value-based pricing* – the ability to offer different end user price reflecting consumer preferences and quality infrastructure investments
- Increased customer choice
- *Service Reach:* Involve service providers other than GSM mobile operators
- *Security:* Maintain isolation of backbone from the Internet, sessions driven from handsets
- *Service Quality:* Conformance to strict SLAs for each service
- *Accounting:* Support a wide range of accounting schemes
- *Scalability:* In terms of dimensioning and geographical reach
- *Redundancy/Availability:* Using alternate routing and multiple Points of Interconnect
- *Flexibility:* Allow the rapid deployment of new services

The IPX is the GSMA proposed IP interconnection option; members are free to choose whether or not to adopt this architecture. However where the IPX is employed services provided will be in strict compliance with the IPX specifications.

The IPI Framework Business Architecture suggests that IPX Providers will support a variety of interconnect principles (examples: session based, data volume based, event based, Calling Party Pays, Initiating Party Pays, Recipient Party Pays, Revenue distribution, and others). These principles typically may vary on a per service basis. The general Value Based Charging Principle applies in any case.

A brief description of IPX services is given in section 4 and their estimated introduction timescales in section 5. Commercial requirements are provided in section 6 and regulatory requirements in section 7. Sections 8 and 9 give an overview of the technical architecture and the technical features of the IPX.

The template for an IPX SLA is attached to this whitepaper as Annex A for reference.

4 IP SERVICES

4.1 General

This section provides examples of IP services where interworking is required and the IPX is relevant. It is expected that new IP services or categories of services will emerge for which the IPX is relevant. For example, a category for multiplayer games might be developed in the future.

The IPX itself is not responsible for offering end-user services; the IPX provides the interconnect between the parties who offer the end-user services. The IPX has to support various functions so that a customer of Service Provider “A” can set up a session with a customer of Service Provider “B” via the IPX.

In order to support the commercial business models and technical aspects of service awareness, IP services transported over the IPX must be standardised and documented in a service specification. One of the inputs to each service specification will be the corresponding GSMA Service Definition PRD. As a minimum, the elements of a service specification consist of the QoS requirement, the charging principles and the SLA. The service specification determines how the IPX is configured to support any particular service. Service specifications will be produced from time-to-time, as the market requires. It is expected that all participating service providers, such as Fixed Network Operators and ISPs, will influence and agree to these service specifications.

4.2 Standardised Services

4.2.1 IP Voice Telephony

The IPX will be used to support IP voice telephony services, that is, Voice over IP (VoIP).

The voice service may be terminated on a circuit or packet bearer. IPX providers may offer conversion of Voice over IP to circuit switched voice as a value-added function. This might apply to the “circuit-switched” voice or the packet voice. However, the technical specification of these conversions is out of scope of this whitepaper.

Voice telephony is a real-time service that will be allocated a conversational QoS traffic class. Critically, tight end-to-end latency control must be maintained for voice telephony services and consideration of this is vital in ensuring an effective and successful IPX.

There are essentially two types of VoIP to be considered:

- Voice originating on a circuit bearer (for example, GSM voice) and then encapsulated in RTP/UDP/IP protocols. Here, the signalling likely to be used is SIP-I. This is termed 3GPP Release 4 voice.
- Voice originating on a packet bearer (for example, SIP or IMS voice). Again, the media will be carried as RTP/UDP/IP, but the standardised signalling for the voice is SIP.

4.2.2 IP Video Telephony

IP Video Telephony will be supported by the IPX.

As with IP voice telephony, the video may have originated on a circuit or packet bearer. Video telephony is a real-time service that will be allocated a conversational QoS traffic class.

IP Video Telephony will use the same protocols for the signalling and media as IP Voice Telephony; only the format of the media streams will be different.

4.2.3 PoC

PoC (Push-to-talk over Cellular) is a real-time half-duplex VoIP service standardized by OMA. PoC uses IMS as an underlying service platform.

PoC provides the ability for one person to communicate with a pre-defined list of others without the inconveniences, long set-up delays or inefficiencies of a circuit-switched conference call.

For inter-operator purposes PoC servers are connected to each other via the IPX for the exchange of talk bursts. Signalling related to PoC is transferred between IMS core systems using SIP. SIP/SIMPLE based Presence is an optional part of OMA PoC.

The PoC service will require that the IPX support the transport of signalling (SIP), talk bursts (RTP and RTCP) and potentially also Presence (SIP) used in PoC NNI.

4.2.4 Instant Messaging

Instant messaging (IM) is a form of communication between two or more people using text messages (and possibly small graphical images). IM usually relies on presence information to ensure that messages can be delivered to recipients instantly.

A number of different standards and protocols exist for IM. Examples are: OMA IMPS, IETF/OMA SIP/SIMPLE and XMPP (*Jabber*). In SIP/SIMPLE IM can use either page mode with SIP MESSAGE method or session mode with MSRP protocol.

The IM and Presence service will require that the IPX support the transport of different protocols such as SSP, SIP and XMPP as used by IM and Presence on inter-operator interface. Additionally, the IPX might support conversions between different IM and Presence protocols and formats as a value added service. The IPX may therefore support IM through IPX SIP Proxy functions (in the case of only SIP/SIMPLE only) or through non-SIP proxy functions (for other protocols). These functions may be supported through a common hardware platform. Details of these proxies are out of scope for this document.

4.2.5 Presence

Presence provides a way for users to communicate their status (online, offline, busy and so on) to another user or set of users. It provides an indication of willingness or capability to communicate and will thus act as a means to stimulate communication by IM, PoC, Voice call or other means.

Presence is typically regarded as an enabler for other services. It may be explicitly defined as part of the service (such as PoC and IM), or the presence may be defined separately as a generic enabler.

OMA have defined a generic presence enabler based around the SIP/SIMPLE protocol.

4.2.6 Video Share

The Video Share service allows a user to share video (either live or pre-recorded) with another user, whilst maintaining a voice call. Video Share is seen as a way for users to extend their communication experience into the visual domain. It can be regarded as a stepping-stone to future deployment of full-duplex video telephony. It is an early example of an IMS combinatorial service.

Video Share is not standardized anywhere, but vendors have implemented an interoperable service based on a technical definition document produced for GSMA SIP Trial purposes. For further details of the Video Share service, please see GSMA SIP Trial document Video Share Definition.

The video session is sent over a PS connection in real-time simultaneously with the ongoing CS call. Video Share is a one-to-one combinational service utilizing 3GPP compliant IMS core systems.

Video sessions are set up using SIP and video is transferred using RTP. Video Share uses a Peer-to-Peer model, that is, applications are built in terminals, and thus a separate application server in the network is not needed. The IPX is used to route signalling and media related to the Video Share service between operators. As it relies on simultaneous use of CS and PS bearers, it requires the use of a 3G terminal.

The Video Share service will require that the IPX support the transport of SIP and RTP protocols with a QoS capability.

4.3 Non-standardised Services

The IPX will provide the transport for many services that are run on a bilateral basis with settlement independent of the IPX provider. In this scenario, the IPX provider does not provide service-based charging. In these cases, the IPX provider functions as a “bit-pipe” although they may provide QoS support. It may be expected that the amount paid would be dependent upon the QoS provided. In such instances, the service does not need to be explicitly detailed in a service definition.

5 COMMERCIAL CONTEXT - TIMESCALES

Building upon a number of well-advanced initiatives and developments, the IPX could be expected to undergo a rapid rollout. The timescales for the introduction of various IP services are shown in the table below. These dates have been discussed and aligned within the GSMA and represent an agreed forecast at the time of writing. However, they are subject to change as a result of further review.

5.1 IP Service Timescales

	R4 Voice	*R4 Video*	*SIP/IMS Voice*	*SIP/IMS Video*	*IM Ph1*	*IM Ph2*	*VS Ph 1*	*VS Ph2*	*PoC*
3GSM	2008	~2008	2008	~2008	Ph 1 Feb 2007 (Bilateral /Transport) Mid-2007 (Multilateral)	Mid 2007	Q2-Q3 2007	~2008	~2008
GSMA Business Priority	High	Low	High	Low	High	Medium	High	Low	Low
CDMA2000	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
NGN FNO	~2008	~2008	~2008	~2008	TBD	TBD	TBD	TBD	NA
Other Fixed	~2008	~2008	~2008	~2008	TBD	TBD	TBD	TBD	NA
ISP	~2008	~2008	~2008	~2008	Mid 2007	Mid 2007	NA	~2008	NA
ASP	~2008	~2008	~2008	~2008	TBD	TBD	TBD	TBD	NA
Content Providers	Low Priority								

Table 1 – Estimated Dates for interworking of IPX services within the communities

Table 1 above shows the earliest dates expected for interworking of the example services that use IPX. Operators are free to use IP interconnection models other than IPX. Therefore, they may choose to launch service interworking using another model and adopt interworking using IPX later than that quoted above. The estimated timescales for the features of the IPX are outlined in Table 2, Section 9.8.

	MMS	*Presence*	*SMS/IP*
3GSM	Available	End 2007	Available
GSMA Business Priority	NA	High	NA
CDMA2000	TBD	TBD	TBD
NGN FNO	NA	NA	TBD
Other Fixed	NA	NA	TBD
ISP	TBD	End 2007	TBD
ASP	TBD	TBD	TBD
Content Providers	Low Priority		

Table 1 - continued

6 IPX COMMERCIAL REQUIREMENTS

The following sections set out the commercial environment where by IPXs will reliably support a system of interconnecting service providers.

6.1 IPX BUSINESS RULES

The following sections list the criteria that will be applied for an IPX Provider to operate, and the criteria that must be met for a Service Provider to connect to the IPX. The purpose of these criteria is to ensure that the IPX domain is properly managed to meet the minimum commercial and technical requirements of the stakeholders.

An IPX provider may support one or more IPX services. It is not mandatory for IPX providers to support all IPX services.

6.1.1 IPX operation criteria

An IPX provider shall:

- Interconnect with all other IPX providers offering the same IPX services so that Service Providers only need to connect to one IPX to enable interworking with other parties connected to other IPXs;
- A maximum of two IPXs shall be utilised in the end-to-end transit of data between Customers connected to an IPX. A relaxation to this rule may be applied where it does not prevent the terms of the SLA being met;
- Support interconnect billing model for the IPX service. (That is, Calling Party Pays, Receiving Party Pays, Revenue Share, Data Volume Based, duration based charging and so on);
- Comply with the SLA for the IPX Service and provide test result verification;
- Make available end-to-end performance test results;
- Implement GSMA specified fraud prevention mechanisms per IPX service;
- Implement GSMA specified security mechanisms per IPX service;
- Offer multilateral interconnection capability per IPX service;
- Support routing and addressing requirements of IPX services;
- Provide transparency of charging that is, IPX transit rate with termination cost separately identified to the respective terminating network.
- Provide flexibility to interconnect or not to interconnect with certain Service Providers or to certain IPX Services on the IPX network. Each Customer (that is, Service Provider) should be able to determine and contract with its IPX provider(s) based upon which other Customers and IPX Services it wants to connect through the IPX, so only agreed Services and Customers are connected.
- Support route-visibility feature where this feature is supported by the service;
- The IPX will be capable of supporting both multilateral and bilateral commercial agreements. In the case where a bilateral agreement exists between operators, the IPX may provide the transport only functionality, and may not be required to apply service-based charging. In other cases is may be required to support both transport and charging functionality between Customers in a bilateral agreement. This will be defined on a Customer-by-Customer basis.

6.1.2 IPX connection criteria

The following basic technical and commercial requirements shall apply to any Service Provider who elects to connect to the IPX. These requirements shall be detailed further during the course of the IPX Project:

Commercial

- Signed Interconnect Agreement with IPX for respective service
- Compliant with all SLAs relevant to the IPX services offered
- Agreement to both way interworking of respective service
- Declared service termination costs of respective service
- Ability to support IP interconnect termination charging

The Customer that is connecting to the IPX shall assume full technical and commercial responsibility for any third parties (that is, aggregators, MVNOs and so on) it has connected to its network, where these third parties connect Services to the IPX through that Customer.

Technical

- Ability to support IPX addressing requirements (including the support of number portability)
- Compliant with security and access requirements of IPX project
- Satisfied end-to-end service testing criteria established by IPX project
- Support service specific end-to-end QoS requirements

The IPX shall not be an exclusive network for utilisation by MNOs, either wholly or partially. The IPX may be utilised by non-mobile Customers for other forms of IP based services (that is, ISP to ISP, ISP to Fixed traffic and so on), providing these services do not impact on other Customers connected to the IPX, in line with the IPX Operation Criteria detailed in Section 6.1.1 above.

6.2 Connectivity Models

The IPX will be open to all business entities offering IP Services where interworking will benefit their respective customer bases. Figure 1 below shows examples of interconnection scenarios between the main business entities within the IPX. This is known as the IPX domain. The IPX consists of two layers:

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

Service Awareness or the **Service Layer** provides establishment of connections and management of billing and settlements for a service.

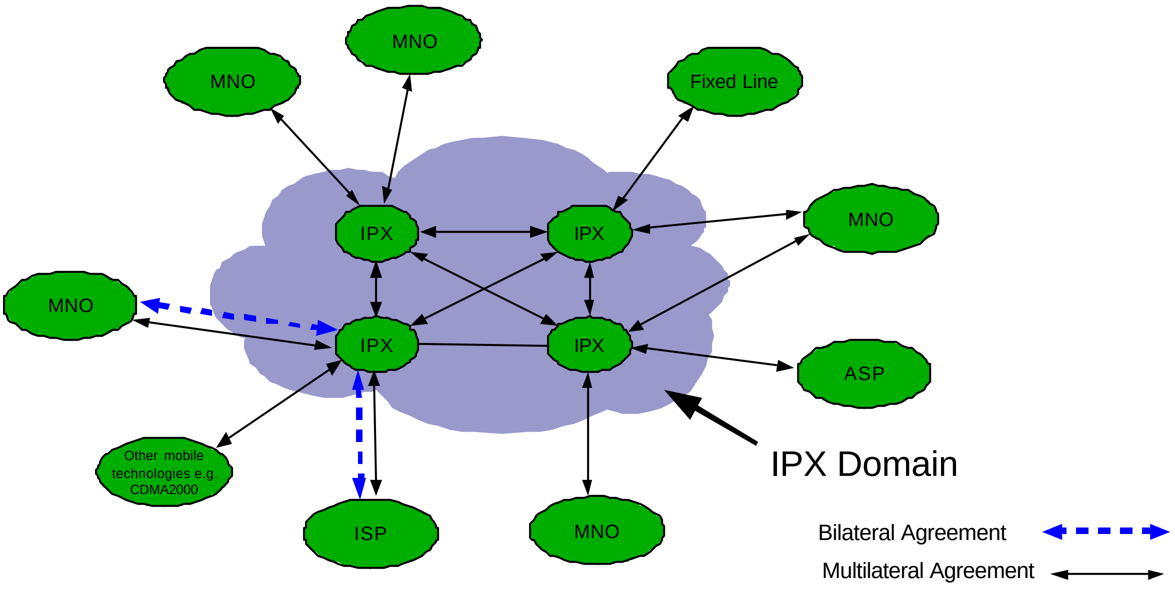

Figure 1: IPX Domain

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

6.2.1 Bilateral - Transport Only (transport without service awareness)

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 model is depicted in Figure 2 below:

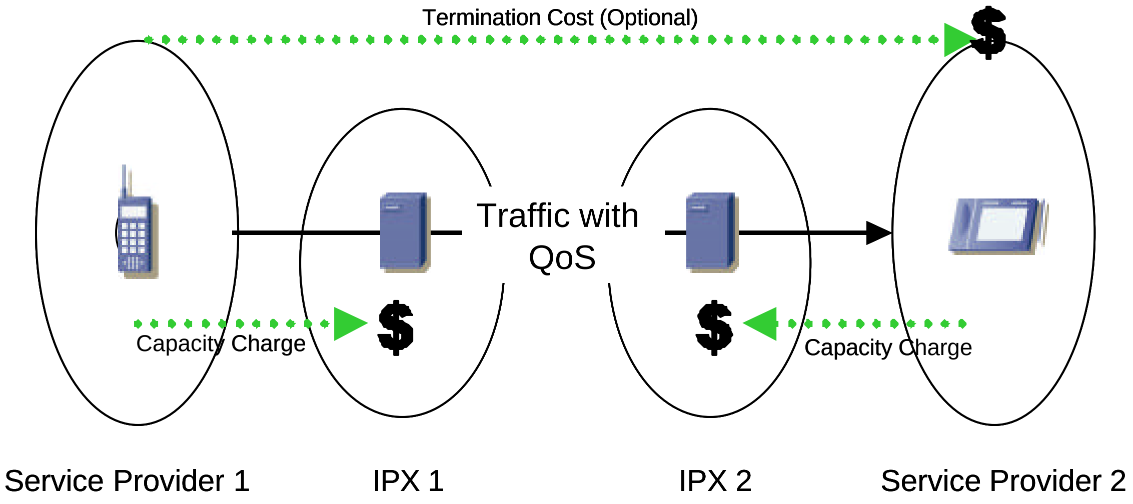

Figure 2: Transport Only Model

Bilateral connectivity:

6.2.2 Bilateral - Service Transit (transport with service awareness)

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).

Cascade billing (for transport and/or service layer) and other associated facilities provided by the IPX Provider (on the Service layer) may be applied depending on the service. Therefore, through Service Transit, the following connections can be implemented: 1) Bilateral connectivity with routing performed within the IPX Domain and within IPI key business principles but settlement of termination charges performed bilaterally between the ending parties and 2) Bilateral connectivity with both routing and settlement of termination charges performed under the IPX Domain and within IPI key business principles.

The transit fee owed to the IPX Providers is always cascaded. Cascading of responsibilities and payments fully apply (on both IPX Transport layer and IPX Service Layer).

This model is depicted in Figure 3 below:

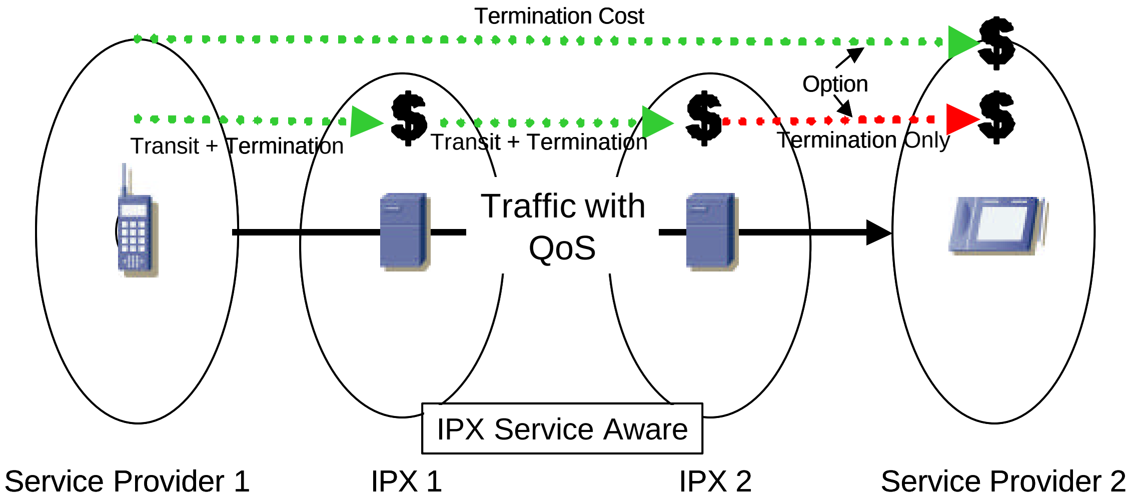

Figure 3: Service Transit Model (any transport charging omitted for clarity)

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

A multilateral connection using Hub functionality. Hubbing/multilateral connectivity is where traffic is routed from one Service Provider to tens/hundreds of destinations/Interworking partners through a single agreement. Cascading of responsibilities applies. Cascading of payments may be applieddepending on the service (on both IPX Transport layer and IPX service layer).

This model is depicted in Figure 4 below:

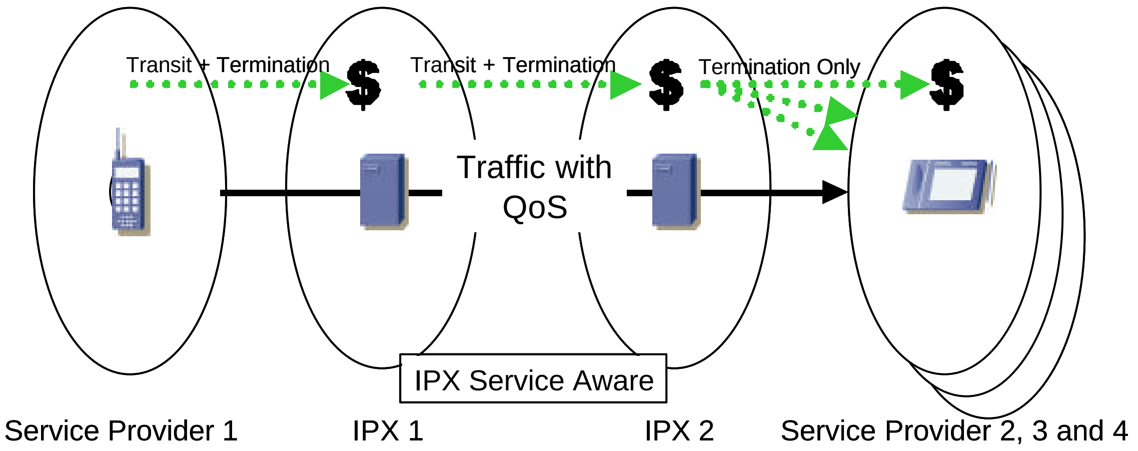

Figure 4: Hubbing Model (any transport charging omitted for clarity)

The benefits of using the IPX Multilateral connectivity include the following:

- Solves the “many-to-many” problem of connecting between tens or hundreds of Service Providers
- One commercial agreement opens connectivity and service Interworking with tens/hundreds of Service Providers
- Routing of traffic to tens/hundreds of Service Providers can be handled via a single route between the originating network and the IPX Provider, thus helping to speed up connection set-ups.
- Changes in the Interworking partner networks cause modifications only in the IPX Hub Functionality, not in all other Service Provider’s networks.
- The ability to pass service payments between the initiating Service Provider and the receiving Service Provider (in the case of the Initiating Party Pays model) via the intermediary IPX Providers without the need to have a direct contractual relationship between the two ending parties.
- The ability to manage and maintain an adequate level of QoS, security, anti-fraud, etc. end-to-end, throughout the whole value chain, even in the case where more than one IPX Provider is involved in the traffic transmission/handling.

A table showing the contracts in place and the settlement that takes place in each of these connection models is given in Appendix D.

6.3 End-to-End Responsibilities

In order for the interworking environment to work reliably for all participants a principle of cascading end-to-end responsibility will be embedded in the commercial and technical specifications governing the IPX Framework.

6.3.1 Cascading of responsibilities

Cascading of responsibilities means that an IPX Provider must be held responsible for the actions of the next IPX Provider (when the transit of traffic will need to pass through more than one IPX Provider from the originating network to the terminating network). This is, to support not only cascading payments for the functions performed but also cascading the responsibility for an end-to-end SLA, security and anti-fraud measures. IPX providers will have to provide an answer on how they can meet this requirement.

The cascading principles suggest that the first connected IPX Provider is held responsible for the actions of the next one (implying cascading of penalties where applicable) – since the next one is considered a subcontractor of the first one (first IPX Provider is a customer of the next).

Conditions regarding KPIs and SLA will apply in the inter-IPX Providers' relationship (IPX Interconnection).

The IPX Providers will have to develop appropriate commercial/technical interconnection procedures, including Inter-IPX settlement. IPXs will be required to interconnect to one another and to offer a single ubiquitous capability to Service Providers regardless of the geographic location of the destinations/Interworking partners and in compliance to the IPI principles.

Such inter-IPX Providers' relationships shall be implemented in accordance with the content of the agreements reached between the IPX Providers and the Service Providers (see future IWG SOLU Template Agreement for IPX services and IWG QoSI SLA in Annex A), since the commitments held between the IPX Providers will have to enable IPX Providers to offer IPX services end-to-end in the framework of the commitments given to the Service Providers.

6.3.2 End-to-end guarantee

Crucial to achieving and to establishing a fully fledged cascading principle, end-to-end quality must be guaranteed. To guarantee end-to-end quality, relevant "ends" must be clearly defined, meaning that a it must be clear where a responsibility begins and where it ends. All parties involved, within the IPX Domain, must sign their name to their responsibility before interconnecting.

Apart from any general or individual requirements, for example, because of local legislation, each party must comply with a common IPX SLA and associated KPIs defining where the responsibility of each party involved in the end-to-end delivery begins and where it ends. This must be closely linked to physical point of interconnect and to the provider of the local loop connection. Service Providers and IPX Providers will be required to comply with the SLA contained in Annex A.

When using IPX services, the Service Providers shall get a commitment from the IPX Provider on the QoS/level of performance for end-to-end traffic transmission irrespective of the fact that the traffic has been transmitted through another IPX Provider involved in the traffic handling. This means that Service Providers must make a commitment to the IPX provider on performance.

The IPX Provider shall deliver to the Service Provider weekly and/or monthly reports on the QoS measured on the end-to-end service offered to the Service Provider.

Such reports shall also include the levels of performance registered on any IPX Provider's network where involved in the delivery/handling of the Service Provider's traffic.

The recommended levels of performance on IPX services and the details on the content of the QoS reports are contained in the SLA template in Annex A. The target values will be developed by the relevant IPX Governance or GSMA groups and specified in service definitions.

In order for all parties (Service and IPX Providers) to monitor and moderate traffic and hence guarantee quality end-to-end, the handling of traffic must be transparent. This implies that every traffic flow generated for an individual service, according to its SLA and KPI, must be traceable all the way from its originating party, through IPX Providers, to its terminating party.

End-to-end transparency and traceability can be supported for some services via network protocols. This is the preferred method and is termed on-line reporting. Where on-line reporting is not possible due to limitations of certain protocols, off-line reporting is required. This is essentially reporting manually how traffic is routed and will have to be implemented by the IPX Providers involved in the traffic handling for:

- The originating Service Provider to have full visibility of the routes used to carry its traffic to the terminating networks.
- The terminating Service Provider to have full visibility on the network where the traffic has been originated and all the parties (IPX Providers) involved in the traffic termination.

The off-line reporting must be considered only where on-line reporting is not technically feasible.

6.4 IPX Charging and Billing Requirements

Where cascading payments is required by a service each party involved in the transport of traffic is compensated for its efforts in providing services to the end–user. This may be done (depending on the service and interconnect mode) via a cascade accounting mechanism, as is common in the PSTN interconnection (voice interconnect) environment.

6.4.1 General requirements

In this model the following key principle applies:

- The party who perceives a value in offering a service should pay for utilised network capacity. That is, the party who generates revenue from the transaction pays for the required transfer of data across the IPX domain. Typically, this will be the initiating Service Provider. However, depending on the specific service implemented over the IPX, there might be different parties (Service Providers) paying for the different streams of data within one data session.

According to the cascade model:

- The IPX Provider will manage in total the billing and financial relationship with the Service Providers involved in the traffic delivery and with any other IPX Provider involved in the traffic handling.
- It is the responsibility of the IPX Provider to establish the appropriate billing arrangements with all the parties involved in the traffic delivery, to ensure that the end-to-end service works in a transparent manner.
- Cascade Billing offers Service Providers the opportunity to receive a single invoice from the IPX Provider for all incoming and outgoing traffic on their network.
- Each Service Provider shall specify its Termination Charge to the IPX Provider on a per Service Provider basis. This means that Service Providers are entitled to quote different termination charges per different Interworking Partner
- In the case of Service Transit and Hubbing/multilateral connectivity, the IPX Provider applies its Service Fee to the client Service Provider, and shall ensure transparency on the Service Provider's Termination Charges
- The hubbing functionality for multilateral arrangements implies that payments will be passed from the initiating party to the receiving parties through involved IPX providers. Thus, there is no need for direct commercial and financial relationships between the initiating and receiving parties (as opposed to that of a bilateral arrangement). This cascading of payments through IPX providers is enabled from end-to-end, allowing for simplified billing and payment through a small number of commercial agreements.
- In general, the IPX Provider shall invoice the Service Provider for the IPX functions offered in respect of all Chargeable Events (a definition of Chargeable Event is to be given on a per service basis), which have taken place during "the monthly Invoice Period" in a transparent model.

- Transparency in this context means a clear split, at invoice level, of the Service Fees and the Service Provider's Termination Charges (see paragraph below on charging transparency).
- The IPX provider must implement - without a separate charge - the necessary interconnection with any IPX Provider involved in the traffic transmission towards all destinations/Interworking partners requested by the Service Provider.
- Service Providers will only have to pay ONE transit fee. For settlement between IPXs, in the case where more than one IPX is used, it is assumed that transit fee is shared between the IPX providers. Inter IPX Provider costs may be transparent to SP1 and SP2 but this is not a requirement.

The charging principles discussed in this section refer to the relationship between the Service Provider and the IPX Provider. They will form the basis for any contractual agreements. Individual service Providers and IPX providers are free to negotiate additional terms and conditions provided they do not compromise the principles above

The IPX charging requirements outlined above apply in all cases regardless of the interconnection model used.

It is assumed that the IPX Provider will offer the Service Provider a pricing structure based on "transit fee" plus a "recipient's termination rate"(that is, the termination fee applied by the terminating party for termination of traffic on its network). If more than one IPX is used for the delivery, it is expected that the two IPX Providers settle according to a pre-existing wholesale agreement (which takes into account cascading responsibilities).

6.4.2 IPX Transport Only charging (bilateral interconnect scenario)

The use of the IPX Transport Only model, implies that the two Service Providers exchanging traffic have entered into a direct contract, outlining the cost of termination for each type of traffic exchanged or service used - similar to existing GSM roaming and SMS/MMS interworking agreements. In this case, service/application level charging would not be subject to an agreement between a Service Provider and the IPX Provider.

Charging for the IPX Transport Only function itself is subject of a separate agreement between the Service Provider and the IPX Provider. In this case, there is no cascade billing and each Service Provider involved in the bilateral relationship pays its IPX Provider for the network capacity.

6.4.3 IPX Service Transit charging (bilateral interconnect scenario)

When the IPX Service Transit model is used, there is a bilateral agreement between two Service Providers and the transit is being done through one or more IPX Providers.

In this case, cascade billing applies. For Service Transit there are two settlement models:

1. The settlement of termination charges takes place between the two Service Providers via the IPX Providers involved. The transit fee is settled directly between the originating Service Provider and its IPX provider and between the IPX Providers involved in the traffic chain up to the last IPX Provider who will pass on the termination charge to the terminating Service Provider.
2. There is a direct settlement of termination charges bilaterally between the two Service Providers. In this case, the cascade billing principle applies only to the transit cost (fee) that is settled directly between the originating Service Provider and its IPX Provider. They will then settle with the other IPX Providers involved in the traffic chain according to their interconnect/IPX interconnection arrangement.

6.4.4 IPX Multilateral connectivity/Hubbing function charging (multilateral interconnect scenario)

In the scenario of IPX Hubbing function, there should be no commercial relationship between the two involved Service Providers, between which traffic is exchanged (similar to conventional international voice interconnect via carriers).

Hence, service/application based charging (for hubbing functions) as well as charging for the IPX Transport should be subject to the single agreement between a Service Provider and an IPX Provider.

The agreement between the Service Provider and the IPX Provider will define the chargeable event as well as the attached cost to the Service Provider of initiating a service and of delivering it through the IPX, for each type of service delivered.

It is assumed that charging for each service may be service specific (for example, session based, event based or duration based), but should comply in any case with the Value Based Charging principle and with the cascading principle of the IPI Framework.

Using the IPX Multilateral connectivity/Hubbing model, the following charging options are possible:

- Separate charging for the IPX Transport layer and the IPX Service layer (that is, multilateral Service Specific interconnection). The advantage of this is more “flexibility” - Providing an IPX transport and IPX Hubbing Function may in fact imply different charging
- Integrated charging, where charging for transport (access to network capacity) becomes part of the IPX Multilateral connectivity/Hubbing function charging. The advantage of this is a consistent implementation of IPI Framework, simplicity (no hidden cost)

The requirements for charging and accounting data, taken from the IPI Framework Business Architecture, are further detailed in Appendix E.

6.4.5 Financial settlement requirements

Ref.	***Requirement***	***Solution***
1	Settlement mechanisms	Will be defined in the individual agreements between Service Providers, between the latter and IPX Providers and among IPX Providers, on a case by case basis
2	Settlement	IPX providers will settle directly with Service Providers.

6.5 Commercial Considerations and Contractual arrangements

6.5.1 Background – IPX contracts

Delivering services across the IPX Domain requires contractual relationships between Service Provider(s) and IPX Provider(s). These contracts will define for example, how payments for the provision of the IPX transport only function, cost of access to the IPX Provider (such as bandwidth) and carriage (for example, packets/bytes) is paid by the Service Provider to the IPX Provider and vice versa. This section sets out general requirements underpinning these contracts.

The IPX provider shall include in the contract with the Service Provider, the relationship required with any Service Provider on whose network the traffic has to be terminated and any IPX Provider involved in the traffic termination. This is to ensure the proper IPX service (both of simple Transport Only, Service Transit or Hubbing) and therefore the proper functioning of the interworking between Service Providers end-to-end.

Stating the above, it is expected that the Service Provider will need to negotiate and sign only one contract with the IPX provider to gain access to a range of service to be implemented with a large number of Service Providers, directly or indirectly connected to the IPX Domain.

This means that IPX transport//hubbing through more than one IPX Provider, whenever applicable, is part of the service rendered by the first IPX provider.

Establishment of the IPX Domain will include two phases:

- First Contractual relationship between all IPX providers having a PoP or a Customer (Service Provider) in the region, for the activation of a qualified interconnection/IPX Interconnection between IPX providers able to guarantee appropriate handling of IPX Transport only/ IPX Service Transit and IPX Hubbing functionality (on account of connected Service Providers), according to agreed QoS.
- Second Contractual relationship between the IPX provider and the Service Provider, in a way that will enable the Service Provider to interact with all other requested Service Providers.

It is important to note that these contracts applying to an IPX Provider, do not preclude Service Providers setting up one or more bilateral agreements with other IPX providers or Service Providers either not aligned with, or outside, the IPI model, provided these arrangements do not compromise the IPX environment. *Example:* If Service Provider A chooses to connect to Service Provider B, via other arrangements outside the IPI Framework, Service Provider A will be held responsible (in relation to the IPX Domain), for any actions taken by Service Provider B. The choice taken by Service Provider A, implies that Service Provider B is indirectly connected to the IPX domain, and thus Service Provider A must take full responsibility for the actions of both A and B.

6.5.2 Contractual requirements

Ref.	***Requirement***	***Solution***
1	The interconnection model used will be chosen by the Service Provider	Service providers will be able to decide how they interact with IPX Providers. Contractual arrangements will range from a bilateral to a multilateral, fully managed model. For many Service Providers a combination of these arrangements is likely. [Note that this does not preclude establishing one or more bilateral arrangements between Service Providers or IPX Providers outside the IPI framework.]
2	Service Providers have free choice of IPX Providers and destinations/Interworking Partners (Service Providers)	A fundamental principle of IPX Domain is that participating Service Providers will choose which partners (IPX Providers and Service Providers) they wish to interconnect with, and for which services. This will form part of the contractual arrangements. 1) *Choosing IPX*: A Service Provider must have the option of choosing IPX Provider per service and will be free to change IPX Providers if this is desired. Service Providers also have the option

		of connecting to more than one IPX Provider. For a Service Provider to be able to change IPX Provider (especially within a short timeframe) contracts and tools must be standardised as much as possible. 2) *Choosing participants*: See section 6.6 - multilateral interworking relationship management
3	Inter-IPX provider arrangements will be based on the IPX Framework Agreement	IPX Providers will set up contractual arrangements between themselves to handle service interworking, routing, control & accounting for managed IPX traffic. These will be based on the IPX Framework Agreement that will be specified by the GSMA
4	Freedom to negotiate contracts with third party providers	Service Providers remain free to negotiate their own contracts directly with third party providers of content, services etc. Traffic resulting from these contracts can be routed through IPX Providers, for example, via a bilateral transit arrangement as described in previous sections. Before an IPX Provider allows a Service Provider to interconnect, that Service Provider must take *full responsibility* for all "non/indirect IPX traffic" (third party traffic example: content). A Service Provider can in turn interconnect to Fixed operators, ASPs, ISPs etc who are not themselves connected to an IPX Provider. Everything outside the "IPX domain", interacting with the IPX-domain, must be compliant with the IP framework.

6.6 Multilateral Interworking Relationship Management

This section only applies to the case of a multilateral connectivity/hubbing functions.

In the ongoing management of multi-lateral agreements where new Service Providers are being added to an IPX hub and can be opened to connection to the other Service Providers on the hub it is important for the industry to take a coordinated approach in order to avoid administrative complexity.

There are two approaches:

- Opt-out or Black listing is where Service Providers automatically agree to be connected to all other Service Providers on a hub unless they opt-out. This facilitates rapid expansion of the market and low administration since no action needs to be taken for existing Service Providers to be connected to new Service Providers and vice-versa.
- Opt-in or White Listing is where Service Providers actively agree on a case-by-case basis to connect to another Service Provider. This means that both parties have to agree to interconnect before traffic may pass. The role out of agreements is likely to be slower as a consequence.

Whilst Opt-Out/Black Listing provides convenience there is less control for Service Providers and even in severe cases of non-compliance by partners it can be difficult to shut down traffic from connected parties. For example, the opportunity to shut down traffic will individually depend on local legislation (refer to previous and current regulatory practise on fraudulent/arbitrary traffic-flows such as SIM-Boxes/GSM-gateways).

In the light of the above, it appears that at this stage the market is not ready to adopt the Opt-out/Black lists and thus it is generally recommended that the Opt-In/White Lists mechanism is adopted for both the transport and the service layer. This recommendation should be reviewed on a service-by-service basis and either model can be adopted for a service upon agreement by the industry.

In the Opt In/White list model it is the responsibility of the IPX Provider to provide the client Service Provider with a continuously updated list of potential destinations/interworking partners (Service Providers) directly or indirectly connected (via other IPX Provider). The IPX Provider will offer the Service Provider the following set of information:

a) The names of all available Service Providers (destinations/interworking partners)
b) The Service Providers' Termination Charges
c) All relevant configuration and service parameters of the Service Providers
d) All routes that will be used to reach the listed Service Providers (destinations/interworking partners)
e) Updates in the list of all potential destinations/interworking partners (Service Providers) will be made during each invoicing period (one calendar month) or each time there is a new Service Provider added to the list.

It should be noted that the list of Service Providers provided by an IPX Provider includes all the other Service Providers reachable through interconnected hubs. IPX Providers must make arrangements for the regular interchange of Service Provider lists.

7 REGULATORY REQUIREMENTS

The IPX will need to meet the relevant regulatory requirements, particularly where it is used for national interconnect. Regulatory requirements remain for further study.

8 IPX NETWORK ARCHITECTURE

8.1 IPX Network Model

A private IP backbone network model is proposed for the IPX. Other models exist, but do not meet all the IP interconnection needs of the IPI project. Even though a number of other private networks might be available, the only existing common inter-operator backbone, which is widely tested and commercially used globally for years, is the GRX. Therefore, the IPX will build upon and extend the existing GRX backbone. The general requirements for the IPX are the same, that is, as listed in IR.34 and Security Code of Conduct documents. For example, security, spoofing prevention, isolation from the Internet and traffic management, are needed from the IPX.

The proposed model of IPX is not mandatory. Among a restricted set of operators (for example, in a national scenario) a bilateral connection such as leased line could be set up, or the Internet or some private network other than the IPX could be utilized. For most operators, the optimum solution may be a combination of both possibilities, for example, the IPX for some international connections while bilateral connections for the national scenario. It will be up to individual operators to decide which option best suits his needs. The *IPX is just one alternative*, even though in many cases it can clearly be seen to be the most beneficial solution for inter-operator IP traffic, as demonstrated within this document.

A simplified high-level architecture of the IPX is illustrated in the figure below (covering both roaming and interworking cases):

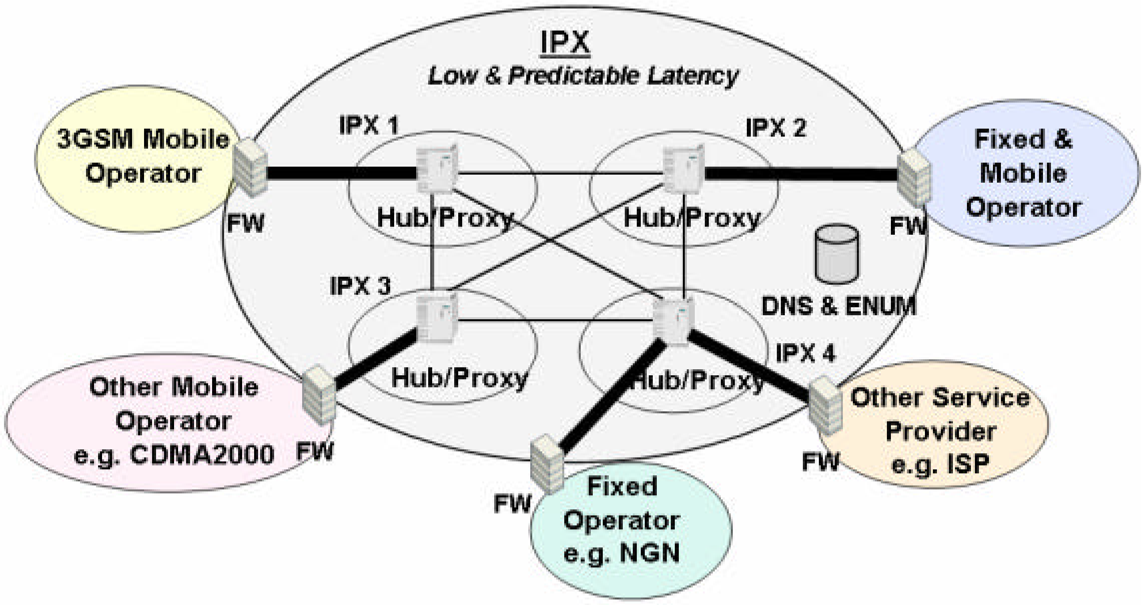

Figure 5: IPX Network

The IPX network ("IPX Cloud") consists of separate and competing IPX carriers (IPX Providers) that are all connected to each other via a number of peering points. The IPX is isolated from the public Internet.

Different Service Providers are connected to the IPX network via separate local loops (or "local tails") implemented between each Service Provider and the IPX carrier that the Service Provider has chosen to use. This same model applies to all Service Providers connected to the IPX, regardless of whether they are mobile or fixed. The local loop that is used is a matter for agreement between the IPX carrier and the Service Provider; it is out of scope to be specified in this document. However, the local loop should not be part of an external network, such as the Internet.

Redundancy concepts are likely to be utilised throughout the IPX network to increase availability. A Service Provider may also connect to more than one IPX provider.

GTP tunnels are used to carry data roaming traffic within the IPX.

8.2 IPX Proxies

Application-aware proxies implement service awareness for billing and multilateral connectivity management in the IPX.

From a service platform (such as IMS core system or MMSC) perspective the inclusion of the IPX is transparent and does not impose any additional requirements or constraints than, for example, a leased line or Internet.

Proxies are a key concept in the IPX; they support multilateral connectivity in a scaleable and efficient manner. After a connection is opened between the proxy and the Service Provider core network, adding a new interworking partner will be much simpler than when using a bilateral model.

The use of a Proxy does not automatically mean the use of a multilateral commercial agreement; it is entirely possible to use a Proxy within the IPX only for traffic routing purposes and to make agreements bilaterally depending on Service Provider decision. In other words, the way agreements are made can be separated from the technical arrangement model.

Using a Proxy an IPX Provider can facilitate access to multiple Service Providers via a single agreement as well as accounting and settlement functions, meaning a single partner for all inter-Service Provider accounting (that is, One Stop Shopping). Such multilateral connectivity functionality is configurable on a per Service Provider basis, giving black/white lists as required.

It should be noted that some of the functions listed below are not standardized. For example, details of transcoding between different voice codecs or conversion between different SIP profiles offered by IPX. These functions may be handled by end Service Providers or as value-added functions by IPX Providers through IPX Proxies. It is left as an implementation issue for IPX carriers to decide if they are commercially viable functions and to Proxy vendors to decide how to implement them.

8.2.1 Generic proxy functions

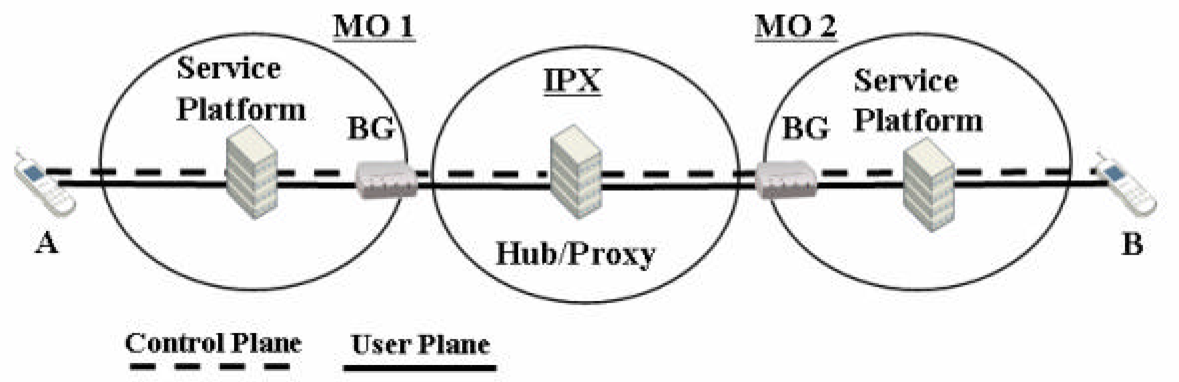

Figure 6: Proxy in IPX

Figure 6 shows the high-level architecture of inter-Service Provider traffic traversing Proxy element within IPX network using any type of IP based traffic. For simplicity, only a single proxy is shown. In some scenarios, two hubs/proxies may be present between any two Service Providers.

Generic technical features required from the Proxy element:

- Session based accounting (resulting from proxy log files/CDRs)
- Capability of transporting both control plane and user plane packets between different IP multimedia networks
- Security functions (such as access control)
- IPv4 / IPv6 transition – if not handled by other network elements
- Media protocol conversion / transcoding - if needed
- Signalling protocol conversion – if not handled by other network elements
- Destination address look-up (including number portability) – if not solved by originating Service Provider
- Support the ability to trace the originator of a service and the hubs/proxies used in its delivery wherever possible

This last feature might require the hubs/proxies to pre-send their addresses to a specified field in the protocol supporting that service. For example, proxy addresses can be added in the VIA fields in SIP or in the RECEIVED field in SMTP. It is recognized that not all services, protocols and equipment are currently able to support this feature. Where it is available, it should be used, and where it is not available steps should be taken to introduce it. The recorded route fields of previous hubs/proxies should be transmitted unaltered to the terminating Service Provider (that is, one proxy should not change or delete the fields of another).

Practical advantages of using a Proxy:

- Minimize configuration changes in a Service Provider network caused by modifications performed in interworking partner networks
- Handle IP version and protocol conversions, as well as other functions required by Service Providers (such as address resolution/number portability handling), on their behalf
- Handle overlapping IP addresses typically used by Service Providers
- Single point for the generation of inter-Service Provider charging data

For various types of traffic, separate Hub/Proxies will be deployed within the IPX. It is an implementation issue whether these elements will be separate or combined into one network node. The Proxy types include:

- IPX SIP Proxy
- MMS Hub
- Wireless LAN Roaming Proxy
- IM/Presence Proxy

Further information about MMS Hubs and Wireless LAN Roaming Proxies is available in Appendix C. Further information about the IPX SIP Proxy is given below. Other types of Hub and Proxy may be defined for future services if required.

8.2.2 Proxy-to-proxy connectivity

Proxy-to-proxy connectivity should be implemented in such a way that it can be used for all IPX services. The interface between proxies is similar to the interface between a service platform (such as an IMS core system) and an IPX Proxy.

General requirements for Proxy-to-Proxy connectivity:

- IPX Proxy-to-IPX Proxy connections shall use IPv6 if proxies are routing traffic between two IPv6 based Service Providers or between an IPv6 based Service Provider and an IPv4 based Service Provider
- A proxy shall not modify IPv6 based IP addresses in the user plane (if no IPv4 related conversion is needed)
- GRE tunnels between proxies may be needed, due to for example, requirement for IPv6 to be used in IPv4 based GRX network
- Only GRX routable IP addresses will be used in inter-proxy interface (for any IPv4 based GRE tunnel outside address)

For further information about IPX Proxies, please see Annex B in IR.34.

8.2.3 IPX SIP Proxy

An IPX SIP Proxy is a SIP proxy with additional functionality to meet the Service Provider requirements. It is transparent to IMS terminals and core systems, that is, the inclusion of an IPX SIP Proxy causes no modifications to IMS specifications or implementations. The interfaces used between an IMS and an IPX SIP Proxy are the standard Mw and Gi interfaces as specified by 3GPP. An IPX SIP Proxy is also transparent to the application/service; it is possible to run any SIP based service via the IPX SIP Proxy (including new Peer-to-Peer applications regardless of the user-plane protocol).

An IPX SIP Proxy may relay both user plane and control plane, or just the control plane, based on the Service Provider preference. If a Service Provider wishes the IPX SIP Proxy to relay only the control plane, the user plane traffic may be sent directly between the service-providers.

An IPX SIP Proxy can function in SIP proxy or in B2BUA modes. If only the control plane is routed via an IPX SIP Proxy, then SIP proxy mode can be used.

9 IPX TECHNICAL REQUIREMENTS

9.1 Protocols

9.1.1 IP versions

Service Providers connected to IPX can use either IPv4 or IPv6, depending on their own policies and decisions. Currently, private IPv4 addresses are widely used for mobile terminals and this will probably continue. Therefore, the *IPX environment has to support both IPv4 and IPv6, including support for private addressing*.

This means that the IPX must have the capability to route traffic end-to-end using either IPv4 or IPv6. It must also have the capability to support conversions between IPv4 and IPv6 and vice versa. This would allow, for example, interworking between an IPv4 based Service Provider and an IPv6 based Service Provider without either party having to make major modifications to their own core networks. In other words, it is possible for a Service Provider to outsource the handling of any possible IP version conversions to the Proxy of an IPX provider, even though in many cases the most optimal solution would be to handle this in the Service Provider’s network.

Static IPv6-over-IPv4 tunnels may also be required for some IPv6 deployment scenarios.

Native IPv6 support should be provided between any two IPv6 based Service Providers. Unnecessary IP version conversions are to be avoided as far as possible. This would allow the intermediate IPX element to function as transparently as possible. End-to-end support for IPv6 could be offered in the first phase by using a static IPv6-to-IPv4 tunnel over the IPX network.

IPv6 offers clear advantages especially for Peer-to-Peer services and is seen as the ultimate long-term goal for the IPX.

9.1.2 Lower layer protocols

If the IPX approach is to be successful, it is essential that new services can be deployed quickly and with minimal overhead.

For this reason, the IPX should be open to any IP *protocol* (media or signalling) unless otherwise stated. The IPX should retain the capability to block unwanted traffic (by protocol, port or IP address). Service Providers retain the right to block any protocols they wish at the entrance to their own networks.

9.1.3 Higher layer protocols

One important protocol used in IPX is SIP (Session Initiation Protocol), which is the preferred control plane to manage session-based IP communication services and applications. SIP was chosen by the 3GPP to support multimedia platforms such as IMS, and is widely used by fixed operators for VoIP services - ETSI NGN also use SIP as their basic signalling protocol. The IPX should support the SIP profile used in 3GPP as well as other SIP profiles, including conversions between these if needed.

Non-SIP related protocols can also be run over IPX, for example SIGTRAN or SMTP for MMS interworking. For further information about the different services used in IPX, see Chapter 4.

Known IPX services will have a service definition that specifies the protocols that are used to support that service. In contrast, the use of a particular protocol does not imply the use of a particular service. For example, MMS and Email might both use SMTP. Where an ambiguity exists, it may be necessary for the IPX to be able to read a service identifier field, for example, a Communication Service ID tag that may be included with the relevant SIP signalling.

By default, the IPX service-aware nodes (that is, hubs and proxies) should block any traffic that does not conform to a recognized commercial service. Service Providers may, if they so choose, request that their IPX provider allow all services to be allowed to pass to/from their own network. Service Providers are free to block any services at the entrance to their own networks.

9.1.4 Protocol conversion

A Proxy will be able to provide conversion support for signalling traffic. For example, an IPX SIP Proxy will take care of any conversions necessary between 3GPP SIP and non-3GPP SIP profiles, if they are not already handled by any other network component. Similarly, an IM proxy may be capable of converting between different IM protocols.

9.1.5 Transcoding

A Proxy will be able to provide transcoding, if needed. This can be seen as a non-mandatory, value-added function that may be offered by IPX Providers to their Service Provider customers. It should not be regarded as a feature that will be performed by the IPX in all cases to allow complete interoperability between all different services. In many cases, a more optimal solution is for Service Providers to perform transcoding themselves (for example, via IMS core system), but nevertheless, the IPX can offer this function if needed. In such cases, the relevant transcoding control mechanisms and protocols must be supported.

For example, in the case of OMA PoC interworking over the IPX, an IPX SIP Proxy shall be capable of translating between 3GPP AMR and 3GPP2 EVRC codecs, if no other network node (such as PoC server or IMS core system) or terminal is capable of providing this required function.

9.2 Addressing

It is important to notice that end-user addressing and addressing used inside IPX network are different.

9.2.1 IP address allocation

The allocation of IP addresses to end-users is a matter for the Service Provider themselves (see section 9.2.4 on private addresses). Any nodes or elements within the IPX, or those within Service Providers' networks that are visible to the IPX, must use public addresses that are allocated by the Internet addressing authority. This ensures that these addresses are unique. However, these addresses *must not* be advertised to the public Internet, and must not be directly reachable from it (see Section 9.7).

9.2.2 End-user addressing

The methods of end-user addressing that must be supported by the IPX will be specified in the service definition for each service. For most IP services these may be in the form of URIs such as those used for email, MMS or for SIP services, with a format (user-name part and domain name part) specified by the IPX governance body.

Many IP services will also require addressing based on E.164 numbers (for example, MSISDNs). In the most part, ENUM will be used to resolve E.164 numbers to URIs/URLs specific to a service for example, MMS or IMS. However, MAP ISIS look-ups may also be used where appropriate for example, for MMS. All E.164 numbers used on the IPX must be used in accordance with the local numbering authority who issued the numbers/number ranges, as well as in accordance with any extra rules set by the IPX governance body.

9.2.3 Addressing of IPX elements

Network elements of the IPX itself will be addressed by Fully Qualified Domain Names (FQDNs) and or URIs with a format (user-name part and domain name part) specified by the IPX governance body. This includes network elements of the Service Providers that must be reachable from the IPX. Addresses of IPX elements should not be visible to end-users and are only used for routing between network nodes and/or tracing purposes.

9.2.4 Handling of private IPv4 addresses

Mobile terminals are frequently allocated private IPv4 addresses by MNOs. These private addressing schemes are not coordinated between MNOs and it cannot be guaranteed that the address spaces do not overlap. These private addresses are not routable in the IPX network.

For client-server services, such private addresses are not problematic for routing across the IPX because it handles only the server-to-server traffic legs. For traffic sent to/from the IPX, network elements such as CSCF, IMS Application Servers, and MMSC, and others are expected to use public addresses that are routable within the IPX (though not advertised to the Internet).

For SIP based Peer-to-Peer services where parties have overlapping addresses, Network Address Translation (NAT) must be performed on the user-plane traffic (that is, the media) to allow the service to be routed over the IPX. The Service Providers involved may perform this NAT function themselves, or may opt to ask their IPX provider to carry it out on their behalf using a function in an IPX SIP Proxy. The IPX SIP Proxy takes into account the required transport protocol (UDP, TCP) for the media while making the port reservation.

For those Peer-to-Peer services using protocols such as SIP and SDP where IP addresses are included within the protocol this NAT function also requires that the IPX SIP Proxy must function as an Application Layer Gateway (ALG). The IPX SIP Proxy must alter the SIP signalling associated with the peer-to-peer service to replace instances of the private network address within the SIP and SDP with the public network address to which it has been translated. This ensures that media traffic destined for the initiating terminal will be routed across the IPX to this public address at the IPX SIP Proxy, from where it can be forwarded back to the terminal with a private IP address across a GRE tunnel.

Using public IPv4 addresses for terminals is not a long-term solution. Terminals would need to be allocated public addresses from a limited address pool that makes it impossible to have large-scale deployment of such terminals.

The use of IPv6 addresses for terminals can eliminate the need for an IPX SIP Proxy to function as a NAT and ALG, if functions such as transcoding are not needed.

9.3 Routing

The IPX network layer refers to the IPX network and elements within it, for example: Border Gateways, DNS/ENUM equipment and the outside interfaces of Hubs/Proxies. The service/user layer refers to the IP addresses of end-users. The service/user layer might include the IMS core system elements and inside interfaces of Hubs/Proxies.

In the initial phases, static routing at the service level can be deployed in the IPX. In addition, the IPX SIP Proxy will contain a list or database of source and destination domains and IP addresses where to forward these packets. The following should be verified:

- Signalling source is who it pretends to be; match source IP and source domain
- Signalling source and destination have a relationship; that is, contract between domains
- Signalling destination is routable; there is a destination IP for that destination domain

Service level routing varies from one service to another, for example routing in MMS is different from SIP routing. In the case of SIP traffic, one possibility is that IPX SIP Proxy finds the destination domain from the SIP Route header (when functioning in SIP proxy mode) or from the SIP Request-URI (when functioning in B2BUA mode) and uses it and the mapping to find the IP address where the packet will be forwarded.

If SIP Route header is used, traffic can use the same route for originator to recipient as for recipient to originator (see asymmetric routing below).

As the IPX increases in size, maintenance of static routing tables in the IP level will become a greater challenge and the IPX will need to adopt dynamic routing protocols. Dynamic routing between Service Providers minimizes the amount of management work in the event of a change in a Service Providers IP address space (that is, new address ranges are applied). In addition, dynamic routing makes it possible to have redundant connections to IPXs. Therefore dynamic routing is a requirement for IPX.

It is recommended that the address space used for a Service Provider’s network will be advertised to IPX providers with BGP-4 routing protocol. Similarly, it is recommended that IPX providers advertise all addresses of connected service providers. Each Service Provider using the BGP-4 routing protocol should have an AS (Autonomous System) number acquired from the Internet addressing authority or from the GSMA. The acquired AS number should be used as an originating AS when that Service Provider advertises its own IP addresses to IPX.

The service provider may screen unwanted routes by selecting address ranges of their partners based the attributes carried on BGP-4 routing messages.

It is recommended that service providers follow the following BGP-4 advertisement rules:

- No host specific route advertisements should be made to the IPX networks (no mask /32 advertisements)
- Advertised routes should be summarized in service provider and IPX connection point whenever possible. Summarizing smaller subnets into bigger blocks will minimize the size of routing tables and stabilize network advertisements
- Service providers should only advertise their own core public IP address range into the IPX
- Networks advertised by a service provider should originate from the AS number owned by that service provider (AS path should start with that service providers AS number)
- If these BGP advertisements style rules are followed, the number of advertised networks and filter management will be minimized.
- IPX Providers should exchange routing information and traffic between all IPX nodes wherever there is a commercial relationship. An IPX provider should be responsible for distributing all inter-service provider BGP-4 information to all its peers. IPX providers should advertise its customer networks to peering partners after that customer has fulfilled the security requirements. The service providers and IPX provider are responsible for ensuring that their networks are invisible to and inaccessible from the public Internet (see security section 9.7).

9.3.1 Asymmetric routing

In some instances, there may be a choice of routes from one Service Provider to another through the IPX. Technically, the routes used at the service level could be asymmetric. That is, a packet sent as part of a service from Service Provider A to Service Provider B could take one route whilst a packet for the same service from Service Provider B to Service Provider A could take a different route, possibly involving different IPX providers. However, there may be good commercial reasons to prevent such asymmetric routing for any given service, for example, fraud detection.

Where the chargeable event for a service includes a return path (for example, MMS + Acknowledgement), then the same route through the IPX should be traversed. For other services, it may be a commercial choice whether or not asymmetric routing is allowed. The decision on whether or not to permit asymmetric routing for a service should be documented in the service description.

It is also technically possible that the media traffic and the signalling traffic for a service could take different routes through the IPX. Where a choice exists, the same IPX providers should be traversed for both signalling and media.

9.4 DNS

The Domain Name System (DNS) of the IPX is completely separate from the DNS on the Internet. This is purposely done to add an extra layer of security to the IPX.

The IPX Root DNS node(s) that Service Providers see are known as "Slave Root" DNS Servers and are commonly provisioned by the IPX provider of that Service Provider. However, the Service Providers themselves can also provision these Slave Root DNS Servers if they so wish. Each Slave Root DNS Server is synchronised with a "back-end" Root DNS Server known as the "Master Root". This is known as a "Zone Transfer" and ensures that the data is the same in all IPX Providers' and Service Providers' Slave Root DNS Servers. Figure 7 below depicts this:

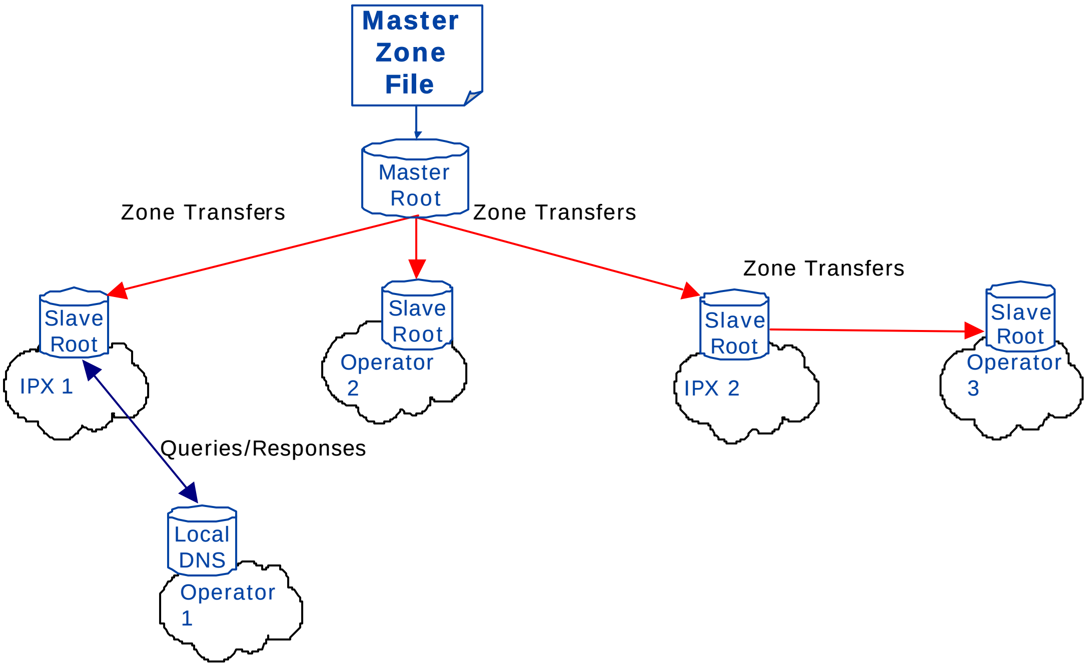

Figure 7: High-level Architecture of DNS Hierarchy in IPX

The data in the Master Root DNS Server is known as the Master Zone File. The population of the data that goes into the Master Zone File has a number of sources, mainly Service Providers, IPX Providers and IPX Providers acting on behalf of Service Providers. The Master Zone File for the GRX is policed and validated by the GSMA to ensure such things as correct sub-domain allocation. The usage and operational support arrangements for the IPX Master Root DNS Server are not yet determined.

There may be specific DNS configuration considerations needed for GPRS roaming, WLAN Roaming, and IMS and for other applications (such as MMS). These are detailed for the GRX in IR.67.

9.5 Carrier ENUM

ENUM as specified by 3GPP and IETF is a method of translating between E.164 (telephone) numbers and Internet addresses (URIs). ENUM is needed where the customer/terminal understands a telephone number, but the network needs Internet addresses for routing. Several of the IP services that will use IPX will require ENUM. ENUM is basically an addition to the DNS, and the DNS structure described in the section above will support it.

The IPX will use an Infrastructure ENUM that is set-up, managed and maintained separately from Public ENUM. Unlike Public ENUM, the Infrastructure ENUM supporting IPX will only be accessible (for both population and queries) by Service Providers, IPX providers or by other delegated parties such as those supporting a particular country. Only the relevant Service Provider or a delegated representative may populate the ENUM entries for their particular subscribers.

Whilst technically fairly simple, the deployment of an infrastructure ENUM functionality in the IPX will be faced with a number of political, regulatory and other issues. For example, the demands of number portability within various regions increase the complexity of the ENUM functions. The ENUM system shall handle all the number portability considerations of using E.164 numbers for user addressing. The deployment of an infrastructure ENUM is the object of a further GSMA project.

ENUM queries may originate from a Service Provider element (for example, MMSC or S-CSCF) or may be delegated to an IPX element such as the IPX SIP Proxy. Terminals also need to be able to support tel URI and/or ENUM queries. It should be noted that ENUM can support a number of different services, that is, it is not in any way tied just to IMS or SIP. Details of the process for ENUM queries are contained in IR.67.

Within the IPX environment, each country may choose to use a single-root or a no-root scheme as outlined below. A key goal is to have country level delegation of ENUM successfully deployed ASAP (influenced by GSMA).

9.5.1 Single-root

ENUM queries are made via the private domain e164enum.net. This exists only in the IPX private network and each IPX network DNS must fully support it. ENUM data is stored in networks connected to the IPX also supporting this domain.

9.5.2 No-root

Should a country wish to use a no-root scheme, all originating Service Providers must be aware of this and program their DNS with special rules about “how to” launch a query to that particular country code. These rules either identify or route the ENUM query to the IPX provider which can resolve the country code or can take some other action.

The IPX has a special relationship with a no-root ENUM provider for specific country codes and is able to route ENUM queries to that provider.

9.5.3 Querying function

The IPX may store copies of ENUM data from other sources and may offer a querying capability as a value added function.

9.6 Quality of Service (QoS)

9.6.1 QoS requirements and signalling

The IPX will carry real-time services such as voice telephony, video telephony or streaming video and it is expected to provide a consistent and high quality of service. This quality of service is required for both interworking and roaming traffic.

For each service, the required quality of service parameters will be provided in the service definition. These parameters will then be used in the SLAs that will be agreed between Service Providers and IPX providers per GSMA service.

There are six QoS traffic classes in IPX:

- Conversational
- Streaming
- Interactive 1
- Interactive 2
- Interactive 3
- Background

Each QoS traffic class has a requirement for the maximum values for the *delay, jitter and packet loss.* These parameters and values have been defined for the GRX in IR.34. The values for delay will be in the form of a geographic matrix to take into account the varying path lengths. Other QoS requirements will also be defined for each service, for example service availability.

IP Packets entering the IPX will be marked with a DiffServ Code Point (DSCP) that indicates the QoS Traffic Class to which that packet belongs. If no explicit packet marking is done, the traffic will be treated as belonging to the background (default) QoS Traffic Class. These markings must be preserved end-to-end across the IPX.

Even though tunnels (such as GRE) are used in IPX, QoS can be guaranteed. This can be done by making sure that the tunnelling device is capable of copying QoS related class parameters to the GRE packet headers.

9.6.2 Meeting QoS requirements in IPX

Achieving the QoS specified for the service in the SLA is a matter for the IPX provider. Traffic Engineering principles are being established by the GRX Working Party for the GRX. These principles can be re-used for the IPX. It is expected that IPX providers will comply with the following principles:

1. Control

   The use of a managed and redundant backbone (such as IPX) is essential to provide an environment where latency (for example, delay and delay jitter) is both bounded and predictable and sustained within requirements. External networks (such as the Internet) should not be used to form parts of the IPX.
2. Peering Points

   To ensure low end-to-end delays for the transport of conversational and streaming class services, QoS, cascade payment and other IPX requirements, IPX providers will need to ensure that suitable peering points are established. Real-time services may be used across continental boundaries and over very long distances. Peering-points must be established which minimize the geographical distance a packet must traverse, as well as the number of IP hops in the path. The equipment at the IPX peering point requires the functionality to support media traffic classes between IPXs in an unbroken stream, in such a way that peering point will not become a bottleneck for the overall IPX environment.

3. Dimensioning

   The bandwidth offered by local loop shall be dimensioned according to traffic engineering principles to support the forecast traffic mix such that the local loop is not the bottleneck in the IPX environment. The links and peering points between IPX providers must similarly be dimensioned to avoid a bottleneck. IPX providers may also choose to over-dimension their networks to enhance some QoS performance parameters related with throughput.

4. DiffServ Network Capability

   Effective network dimensioning depends upon reliable traffic forecasts that may be hard to obtain. Furthermore, the IPX may need to cope with sudden background class traffic surges. For example when a messaging service that has a backlog due to a fault is repaired, a surge can be created.

   IPX providers may therefore choose to make their network DiffServ capable to better meet the QoS demands of the different traffic classes. As described above, Service Providers will indicate the QoS traffic class for a packet using DiffServ. The queuing algorithms and other techniques that might be used with DiffServ are a decision left to the IPX providers.

9.6.3 Monitoring of QoS

The monitoring of the QoS is specified in the SLA template attached as Annex A.

9.7 Security

9.7.1 General

The IPX is totally separated, that is, inaccessible and invisible, from the public Internet at the routing and DNS levels. Peering points must also be isolated from the public Internet. Access to the IPX is only for trusted Service Providers. All connections in the IPX are agreement based, that is, there is always some level of trust involved because of the commercial agreements existing between interworking/roaming partners.

The security level of the IPX shall be in line with the guidelines given in GSMA PRD IR.34 and GRX Security Code of Conduct documents.
Note: In this section peering member and peering partner mean the same thing, that is, an IPX carrier connected to an IPX peering point.

Network devices isolation: Management access to IPX network devices shall be restricted to a small set of management stations located in protected and secured areas, using encrypted passwords. To prevent access to the devices by malicious casual visitors, local management access to network devices shall be prevented by ensuring physical security via locked access unless temporarily enabled by authorised people

IP address origin: Each IPX provider shall make all reasonable efforts to ensure that the IP addresses presented by Service Providers are valid; that is, issued by either an IPX provider or an Internet address registration authority. Each IPX provider shall ensure that all packets sent by any connected Service Provider originate from that Service Provider only, and not from any other Third Party Service Provider connected to that Service Provider then acting as transit

VPN isolation: Protection against eavesdropping from other Virtual Private Networks (VPNs) running over the same IP infrastructure as the IPX VPN shall be guaranteed

Anti-spoofing: Both anti-route and anti-packet spoofing measures shall be implemented to prevent any connected Autonomous System from falsely diverting data from its intended destination to an unauthorised location, or to mimic another device not belonging to that AS with the intention of intercepting data designated for that device

Denial of service: Adequate measures to protect network resources such as IPX root DNS servers against flooding attacks shall be implemented

Network security policies: Each IPX provider shall have well defined internal security policies, covering confidentiality, integrity and availability, with well-defined network security organisation and procedures

IPSec based local loops: When IPSec tunnel is used for local loop the required Layer 3 firewalls and intrusion detection software are implemented on those connections. Incoming connections (initiated from the Internet) must be blocked. If an IPSec tunnel is used to connect Service Providers to the IPX, then the IPX provider shall ensure that authentication and encryption are used between the Service Provider and the IPX. Networks and AS-numbers must not be advertised to Internet

Default Route: No "route of last resort" shall be configured towards any other peering IPX. That is, peering members may not advertise routes with a next-hop other than that of their own routers without the prior written permission of the advertised Party and the advertiser

Route Advertisements: Peering members may not forward traffic across the shared infrastructure unless either the traffic follows a route advertised in a peering session or where prior written permission of the Member to whom the traffic is forwarded has been given. IP packets to the root DNS must be allowed. Networks should be summarized customer/IPX bases. Host routes are not allowed to be used

Physical Connectivity: Peering members may only connect equipment that is controlled and operated by that member to the Point of Interconnection shared infrastructure. Parties may not connect any other equipment on behalf of Third parties to that shared infrastructure

Allowed Connectivity: Peering members may not directly connect any other Third Party who is not peering members via circuits to their equipment hosted at the Point of Interconnection

A connection between a Service Provider and the IPX should use a Border Gateway (BG) to protect the Service Providers core network from the IPX network. Details of this node are out of scope for this document, but the basic principles are already used today for GRX. A BG includes functions such as CoS capable firewall (potentially service aware) with routing capability.

In the IPX, protocol restrictions are generally not needed because other features are relayed upon to achieve the necessary level of security. The rules for the blocking of protocols and services are described in sections 9.1.2 and 9.1.3. In the IPX network it is possible to remove spoofing, flooding and similar type of attacks. This means that it is always possible find a correct originating Service Provider of IP packet within IPX environment.

Due to the commercial models used in IPX, Service Providers connecting to the IPX environment have a commercial interest in maintaining their own network so as to prevent the creation of unwanted traffic. Every Service Provider will therefore aim to stop SPAM according to criteria identified by recipient networks and contractual arrangements.

9.7.2 IPX traffic separation

User traffic such as peer-to-peer media flows may represent more of a security threat because they might be used by a malicious end-user to attack elements of a Service Provider’s network or the IPX itself. There is therefore a requirement for the transport of peer-to-peer media flows within GRE tunnels in the IPX.

User traffic and network traffic should be separated within the IPX to increase security through isolation. Further details of IPX traffic separation are included in the separate paper attached as Annex B.

9.7.3 IPSec VPN usage

Encryption of user traffic on the IPX is not needed since the IPX is a secure environment. Service Providers are free to use IPSec VPNs *over the IPX* but their use is strongly discouraged because of the added complexity and performance impacts. Any forms of VPNs that use the public Internet to form any part of the IPX, other than the local tail, are unacceptable because of the quality of service and security concerns. *A Service Provider or IPX provider not operating according to these rules are in breach of contract, SLA or governance and subject to predefined penalties.*

The use by a Service Provider of an Internet IPSec VPN for the local tail is strongly discouraged unless there is no viable alternative. The IPX governance body should maintain checks to investigate cases where it is claimed that no viable alternative exists to ensure that an Internet IPSec local loop is not preferred simply because it is the lowest cost alternative.

If an Internet IPSec VPN remains the only option for the local loop, the Service Provider concerned needs to recognize the quality of service and security risks, and must take suitable steps, together with their IPX provider, to mitigate and contain these risks.

9.8 IPX Feature Introduction

Not all features of the IPX are required at its initiation. The following table gives some estimates of when certain features will be required, based on the dependencies of the services that will use them (see section 5). It should be noted that some of these features already exist, or are already in development. This represents a forecast at the time of writing and is subject to change.

Feature	*Required*
WRP	Q2 2007
Charging (Bilateral)	Q2 2007
GPRS (not SA)	Q2 2007
Flooding prevention	Q2 2007
Multi-connection control	Q2 2007
Charging (Multilateral)	Q2 2007
ENUM	Q3 2007
Number Portability	Q3 2007
IPX SIP Proxy	Q3-2007
IPv6 Support	Optional Q2-Q3 2007
NAT	Optional Q2-Q3 2007
Other Proxies	IM mid 2007, MTA end 2007
Transcoding	Optional 2008
GPRS (SA)	2010

Table 2 - IPX Feature Timescales

10 CONCLUSIONS

The concept of an IPX to meet the IP interconnection needs of Service Providers for IP Service Interworking and Roaming has been introduced in this whitepaper. The IPX is one alternative; it is not mandatory, but represents the GSMA vision of the most effective approach. There are currently other potential models available and this situation will continue in the future.

The IPX reuses many key elements and principles already used commercially in the GRX for years; it is not a completely new and untested environment. Primarily, the IPX adds the support for QoS guarantees and allows for the selective use of proxies for supporting multilateral interworking arrangements. Basic elements of the IPX (such as IPX Proxies) have been successfully tested in a global multi-operator, multi-vendor environment since early 2005.
The IPX adopts the successful and established business model for voice interconnection and applies it to IP Service interworking. Its development does not therefore pose a major commercial challenge.

The IPX is a simple solution to meeting the needs of the IPI Framework Business Architecture and to ensure a highly developed, competitive and flexible market for IP service interworking. It establishes a means of interconnection through IPX Proxies to other Service Providers that is scaleable. It will result in many efficiency benefits for operators when using the multilateral model.

As well as the generic benefits of the IPX, there will be additional service-specific advantages that have not been discussed in this paper. The IPX is the first complete and sustainable IP interconnection environment that enables the adoption and usage of IP Services. This will benefit both Service Providers and their customers.

APPENDIX A: GLOSSARY

Term	*Definition*
ASP	Application Service Provider
B2BUA	Back-to-Back User Agent
BG	Border Gateway
BGP	Border Gateway Protocol
CDR	Call Detail Record
CoS	Class of Service
CSCF	Call State Control Function
DiffServ	Differentiated Services
DNS	Domain Name System
DSCP	DiffServ Code Point
ENUM	tElephone NUmber Mapping
FNO	Fixed Network Operator
GRE	Generic Route Encapsulation
GRX	GPRS Roaming eXchange
GTP	GPRS Tunnelling Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPI	IP Interworking
IPSec	IP Security
IPX	IP Packet eXchange
ISP	Internet Service Provider
KPI	Key Performance Indicator
MMSC	Multimedia Message Service Centre
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NGN	Next-Generation Network
PoC	Push-to-talk over Cellular
PRD	Permanent Reference Document
QoS	Quality of Service
RTP	Real-Time Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

APPENDIX B: DEFINITIONS

Some terms used in this document are explained below.

Carrier ENUM: A Service Providers-only Private ENUM that is separated from the Public ENUM (which is located in Internet and used by end-users). Carrier ENUM is synonymous with Operator ENUM but for our purposes we will only refer to the term Carrier ENUM.

End User: A customer of an operator or a service provider (Fixed, ISP or ASP) using an IP service that is interconnected via the IPX.

Hubbing: Hubbing or hub-service in this context is when an IPX is performing multilateral interconnection, fully enabling interconnection of specified end-user services, as offered by Service Providers.

Interworking: The term "*interworking*" in this concept means exactly the same as the term "interconnection" in 3GPP. While generally speaking "interworking" is used only when talking about connection between different systems, here for example "IMS interworking" means that two IMS networks are connected through an IP network to enable SIP control (Mw interface) and transport of user plane (Gi interface).

IPX: IP Packet eXchange. The entity providing the IPX functions. In the interconnection context, IPX is used to mean an interconnection at the service level.

IPX Provider: A business entity (such as an IP Carrier) offering IP interconnect capability for one or many IPX services compliant with the IPX operation criteria and compliant with the defined SLA and interconnect agreement for that service.

IPX Proxy: A service aware IPX network element that supports service interworking. The term hub may also be used to refer to a form of IPX Proxy. Hubs and proxies facilitate a multilateral model for each service.

IPX Service: An IP Service using the IPX as a means of interconnection that is provided by a Service Provider to an end-user.

Peer-to-Peer: Services such as Video Share or VoIP where the communication is between applications resident in the user's terminal. Other services such as PoC, MMS, SMS etc are termed client-server services because they always send media first to a server before it is forwarded to the recipient.

Service Provider: A business entity entering into a contractual relationship with IPX provider(s). Thus, "service provider" includes MNOs, FNOs (for example, fixed broadband operators and NGNs), ISPs, ASPs and so on.

Transparent Hubs/Proxies: A hub or proxy that is used to support a service is *transparent* if the end-user of that service is not able to detect the use or otherwise of the hub or proxy. A hub or proxy may also be *transparent* to another systems if its use or otherwise does not *substantially* alter the configuration of the other system.

APPENDIX C - REFERENCES

1. IPI Framework Business Architecture, IP Inter-working: IPI.05-2006
2. GSMA PRD IR.34 Inter PLMN Backbone Guidelines
3. GSMA PRD IR.52 MMS Interworking Guidelines
4. GSMA PRD IR.61 WLAN Roaming Guidelines
5. GSMA PRD IR.65 IMS Roaming and Interworking Guidelines
6. GSMA PRD IR.67 DNS Guidelines for Operators
7. GSMA PRD IR.68 QoS Sensitive Roaming Principles
8. GSMA PRD IR.72 SIGTRAN Basic Design Principles
9. GSMA PRD IN.04 MMS Hubbing Handbook
10. GSMA GRX Security Handbook (a.k.a. Security Code of Conduct)
11. GSMA WLAN Roaming Proxy document
12. GSMA IPI Framework Business Architecture
13. GSMA IPX Framework document
14. GSMA Guidelines for end-to-end GRX Service Level Agreement between Mobile Operation and Carriers
15. GSMA SIP Interoperability Trial v1.0
16. GSMA SIP Trial Campaign Technical Definition TCVS01
17. GSMA IPX Proxy Requirements

APPENDIX D: INTERCONNECT MODEL COMPARISON

It is useful to compare bilateral with multilateral agreements for the following (simplified) case in which there is a flow of traffic from Service Provider 1 (SP1) to Service Provider 2 (SP2) via IPX Provider 1 (IPX1) and IPX Provider 2 (IPX2) within the IPX Domain:

Type	***Contracts in place***	***Settlement***
IPX Transport Only	Direct end-to-end negotiation between SP1 and SP2 Contract between SP1 and IPX 1 in place for IPX Transport only function Contract between SP2 and IPX 2 in place for IPX Transport only function Contract between IPX1 and IPX2 for transferring of interconnection traffic between them	Cost of IPX Transport only (for network capacity) is paid by SP1 to IPX1 Cost of IPX Transport only (for network capacity) is paid by SP2 to IPX2 No settlement between IPX1 and IPX2. Termination rate is paid by SP1 to SP2. No cascade billing
IPX Service Transit	Direct end-to-end negotiation between SP1 and SP2 Contract between SP1 and IPX 1 in place for IPX Service Transit Contract between SP2 and IPX 2 in place for IPX Service Transit Contract between IPX1 and IPX2 for transferring of interconnection traffic between them	Settlement of termination charges between SP1 and SP2 can be made via IPX1 and IPX2 or directly In the case of settlement of termination charges via IPX 1 and IPX2: - Cost of IPX Service Transit is paid by SP1 to IPX1 (and has to cover remuneration for IPX 1 and IPX 2 and SP2's Termination charge) - IPX2 is responsible for paying the termination fee to SP2, - IPX1 is responsible towards SP1 for QoS up to SP2, and the level of performance (example: anti-fraud and security) offered by IPX2. - IPX2 is responsible only towards SP2 in accordance to their agreement In the case of direct settlement of termination charges between SP1 and SP2: - Termination rate is paid by SP1 to SP2 - Cost of IPX Service Transit is paid by SP1 to IPX1 (and has to cover remuneration for IPX 1 and IPX 2) - IPX1 is responsible towards SP1 for QoS up to SP2, and the level of performance (example: anti-fraud and security) offered by IPX2. - IPX2 is responsible only towards SP2 in accordance to their agreement In both cases above: Payment and responsibilities apply for both specified service and transport. IPX1 and IPX2 settle according to a pre-existing wholesale agreement (note: granted cascading responsibilities are

Type	*Contracts in place*	*Settlement*
		fulfilled) For settlement between IPXs, it is assumed that transit cost (fee) is shared between the IPX providers. Inter IPX Provider costs may be transparent to SP1 and SP2 but it is not required.
IPX Hubbing	SP1 has an agreement with IPX1, covering interconnection of SP1 with selected other Service Providers (including SP2) over the IPX Domain SP2 has an agreement with IPX2, covering interconnection of SP2 with selected other Service Providers (including SP1) over the IPX Domain Contract between IPX1 and IPX2 for the transferring of interconnection traffic between them	Costs for managing traffic are paid by SP1 to IPX1 according to a pre-agreed pricing structure defined by their commercial agreement (i.e. based on “service (hubbing) fee” + “recipient’s termination rate”) Costs for terminating traffic are paid by IPX2 to SP2, according to a pre-agreed pricing structure defined by their agreement IPX1 and IPX2 settle according to a pre-existing wholesale agreement For settlement between IPXs, it is assumed that transit cost (fee) is shared between the IPX providers. Inter IPX Provider costs may be transparent to SP1 and SP2 but this is not a requirement. Payment and responsibilities apply for both specified service and transport. IPX2 is responsible for paying the termination fee to SP2. IPX1 is responsible towards SP1 for QoS up to the terminating Service Providers, and the level of performance (example: anti-fraud and security) offered by IPX2. IPX2 is responsible only towards SP2 in accordance to their agreement

APPENDIX E: DETAILED REQUIREMENTS FOR CHARGING AND ACCOUNTING DATA

Ref.	***Requirement***	***Solution***
1	Product specific charging Support for a range of interconnect charging and accounting principles	The IPI Framework suggest that IPX Providers will support a variety of interconnect principles (example: session based, data volume based, event based, Calling Party Pays, Initiating Party Pays, Recipient Party Pays, Revenue distribution, and others). These principles typically may vary on a per service basis. The general Value Based Charging Principle applies in any case. Options for charging for messages such as, Presence information, location, subscribe status and administrative message, unsubscribe, and so on, shall be foreseen. A more defined set of chargeable events will be introduced as the IPX network evolves and new services become available.
2	Provision of transport and transit - based charging data	IPX Providers shall be capable of providing inter-provider charging data. **NOTE: This is not needed in the case of Pure IPX transport** because in that case each Service Provider is simply paying its IPX Provider for the network capacity. There is no payment between the IPX Providers involved.
3	Provision of service-based charging data	IPX Providers shall be capable of providing service-based charging data according to IPI accounting principles in accordance to the definition of the chargeable event for a specific service. This may include, such as: SIP-based user discovery and support for the different charging objects (example: peak charging, billing, and destination-sensitive billing) required for specific services. Standard call detail records (CDRS) will be used where possible.
4	Provision of means to correlate charging data	IPX Providers shall be capable of providing means to correlate charging data according to respective charging principles deployed
5	Logging service usage	IPX Providers shall be capable of providing means to log service usage (at an appropriate level of aggregation) to correlate the charging information generated at transport, service, application and content levels by involved parties for charging and dispute resolution. The option of logging for Administrative Messages (Presence, subscribe, unsubscribe, and others) shall be foreseen.

Ref.	***Requirement***	***Solution***
6	Interfacing between inter-connect billing systems	IPX Providers shall be capable of supporting the required external interface(s) for interconnection with the major Service Providers' billing systems. IPX Providers' OSS systems shall be compatible with those of Service Providers such that the necessary billing and accounting information can be exchanged and all necessary fields are preserved throughout the service delivery chain.
7	Identifying the terminating network	Invoices produced by IPX Providers shall be sufficiently detailed to identify the originating and terminating network.
8	Unbundled pricing structure	IPX Provider pricing shall be unbundled to identify separately the termination charge on the destination network, and the charge applied by the IPX for the transiting/transporting the respective traffic.
9	Service interoperability agreement for Transport, Transit or Hub connection	The charges to be paid by a Service Provider for each initiated transaction (basically for the IPX Hub or IPX Service Transit and the IPX Transport only) terminated through the IPX network, as well as the compensation received by the Service Provider for each service or transaction terminated on its network shall be defined within the agreement (or Interconnect Agreement) between a respective IPX Provider and Service Provider.
10	Transport interoperability agreement	The charges to be paid by a Service Provider for transport to the IPX Provider shall be defined within the agreement (or Interconnect Agreement) between a respective IPX Provider and Service Provider

ANNEX A: SERVICE LEVEL AGREEMENT FOR END TO END IPX SERVICE BETWEEN SERVICE PROVIDERS AND IPX PROVIDERS

"IPX Tranport SLA template v0.51.doc"

ANNEX B: IPX ARCHITECTURE SECURITY

grxev_11_003_ipx_a
rchitecture_security.