IR.77 InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers

Version 5.1

15 April 2025

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

The need to define an adequate level of security is critical and this document sets out how this can be achieved. This document, together with the Permanent Reference Document (PRD) IR.34 **Error! Reference source not found.**, describes a set of common guidelines to achieve an adequate security level on the IPX Network.

This PRD contains a set of binding and non-binding security requirements. All the requirements which are classified as binding are mandatory for all current and future IPX services and all participants on the IPX, unless stated otherwise. Participants on the IPX are any entities which send/receive IP packets on the IPX, such as IPX Providers and PLMN Operators, Fixed Network Operators and any other Service Providers.

All participants on the IPX are required to contribute to overall IPX security. Only if all the participants deploy and maintain their part of the security measures, can it be ensured that the IPX is a secure and reliable network for inter-Service Provider data exchange. Having a secure and reliable IPX Network is a prerequisite for mobile roaming and interconnect.

The Inter-Service Provider IP Backbone is called IPX in this document and is defined in GSMA PRD IR.34 **Error! Reference source not found.**. Additional information is defined in GSMA PRD IR.40 0 and GSMA PRD IR.67 0. Services which are defined on top of the IPX – the so-called IPX Services – are defined in GSMA PRD IR.34 **Error! Reference source not found.**, GSMA PRD IR.88 0 and GSMA PRD IR.90 0. More IPX Services may be defined in the future, which may lead to the creation and publication of additional GSMA PRDs.

In addition to collaboratively contributing to IPX security, each participant needs to protect their own internal network by themselves.

1.2 Scope

The document defines security requirements for Service Providers and IPX Providers to enhance their network security.

In particular, this document focuses on the following key topics:

- Internal security of the IPX Network,
- Security between the various IPX Provider networks,
- Security in Service Provider networks when it is related to IPX,
- Security between a Service Provider and the IPX,
- Security of data in terms of confidentiality, authenticity and integrity (e.g. by means of Internet Protocol Security (IPsec)) if it is needed for network level security,
- Tunnels, where needed, to hide the network from end-users.

User Terminal security, radio link network security and non-IP based signalling data (e.g. SS7) are not in the scope of the present document.

1.3 Motivation

From LTE onwards, the All-IP networks became reality. Since all the networks – mobile networks, fixed networks, user plane, control plane, management plane, and the Internet – are all based on IP, faults and mistakes can propagate to other networks and attackers may cross network borders to misuse the networks for their purposes. This is why inherent IPX security is a primary goal of the mobile industry.

In the past, the inter-PLMN signalling networks were considered secure because there used to be a small amount of peers on the network. This has changed as additional Service Providers who offer complementary services are also connected to the IPX. Experience shows that there is always a small number of Service Providers who try to exploit the IPX to commit fraud. Effective security measures are to be deployed to counter all the obvious attacks.

The benefit of focusing on IPX security is that certain kinds of attacks – including fraud – can be mitigated. There will be no need for complex fraud detection and management systems. As a consequence, investment in security pays-off in the long run as operational costs and fraud losses are reduced. All players on the IPX need to participate in order to make this objective come true. Thus, all IPX Providers and Service Providers are urged to adhere to the requirements of this PRD.

1.4 Definitions

Term	Description
AS	In the Internet model, an Autonomous System (AS) is a network segment that consists of a collection of sub-networks with hosts interconnected by a set of routes. See RFC 4271 0.
BG	Border Gateway, router with optional firewall functions (Network Address Translation (NAT), Topology Hiding) between intra-Service Provider and Inter-Service Provider IP Backbone networks.
BGP	Border Gateway Protocol (BGP) is an inter-Autonomous System routing protocol. The current version of BGP is BGP-4.
DNS	Domain Name System. For additional information, refer to PRD IR.67 0 and TS 184 010 0.
End User Traffic	Traffic from a User Equipment to another User Equipment (UE-to-UE) or from a User Equipment to a Server (UE-to-Server). Server-to-Server traffic is excluded.
GRX	GPRS Roaming eXchange. Provides for routing, interconnecting and some additional services, such as DNS. Generally used for GPRS/UMTS roaming, MMS interworking and WLAN roaming. GRX is an IPX Service.
GRX Provider	A Provider that offers GRX service only.
Internal Network	A network which is fully owned and operated by an organisation and which is only accessible by this organisation. Networks which do not belong to this organisation do not have access to the internal network. Office LAN and Management LAN are two examples for an internal network. By definition, networks that do not belong to that organisation (e.g. the IPX Network or the Internet) cannot be Internal Networks.
Inter-Service Provider IP Backbone	The collection of interconnected GRX and IPX Providers' networks, the so called IPX Network. This is the technical fundament of the global IP-based network that is shared by Service Providers and IPX Providers.
IPX	IP Packet eXchange. The entity providing the IPX functions and services. At the interconnection level, IPX is used to mean a network. At a service level, it refers to the entire ecosystem created by the Inter-Service Provider IP

Term	Description
	Backbone (i.e. the IPX Network) and all the IPX Services that are offered on top.
IPX Network	Synonym for Inter Service Provider IP Backbone.
IPX Provider	A Provider that operates a part of the IPX Network and that offers IPX services and may also offer GRX services.
IPX Provider Network	The part of the IPX Network that is operated by one particular IPX Provider. All IPX Provider Networks together build the global IPX Network.
IPX Service	A service which is provided on top of the IPX Network, such as Diameter Signalling Service, SIP Signalling, RCS Hubbing, or the GRX. This service is offered by IPX Providers. For more details see PRD IR.34 **Error! Reference source not found.**.
IPX Service Hub	An entity on the IPX Network, operated by an IPX Provider, which provides one or more IPX Service(s).
IPX Service Community	Some IPX Services are separated from other IPX Services in separate VLANs. Service Providers and Service consumers need to join the same IPX Service Community to be able to provide/use the service. In which way IPX Services are separated into different Service Communities is defined by PRD IR.34 **Error! Reference source not found.** and the additional PRDs that describe the IPX Services.
Network Element	Any equipment on the network which processes data according to its purpose. Examples for network elements are routers, switches, gateways, servers, firewalls.
Network Service	A server on the network provides a network service by listening on a TCP or UDP port, which is reachable by the means of sending IP packets to the server over the network.
Participant	An entity which has access to a network to exchange data on this network.
PDN	Packet Data Network, typical Packet Data Networks are Internet, GRX/IPX, corporate networks.
Private Network	A network where network elements and hosts have publicly non-routable, so called “private” IP addresses. BCP 5 0 defines these networks for IPv4 networks. In IPv6, publicly non-routable IP addresses are “link-local”, “site-local”, and “unique-local”. RFC 4193 0 and RFC 4291 0 define these networks.
Routing Instance	An environment in which routing decisions for IP packets are made based on routing rules that are collected in a routing table. All IP packets that reach this routing instance on a network element while being on transit, can be routed to any destination listed in the routing table. In order to have multiple routing instances on the same network element for disjoint/isolated networks, technical means below the Network Layer (Layer 3 on the ISO OSI network model) shall be deployed.
Service Provider	Mobile Network Operator (MNO), fixed network operator or other type of Operator connecting to Inter-Service Provider IP Backbone for roaming and/or interworking purposes.
Service Provider Network	An IP network which is fully owned and operated by a Service Provider and which is connected to the IPX Network and reachable from the IPX.
Secure Tunnel	Tunnel able to guarantee traffic isolation, data authentication, integrity and confidentiality.
Sharee	The sharee uses a resource which is controlled and owned by the sharer. By using the resource, the sharee is subject to the conditions by which the sharer allows the sharee to use the resource.
Sharer	The sharer is in possession of a resource which is owned and controlled by the sharer. The sharer allows another entity – the sharee – to use this resource. Both the sharer and the sharee use the resource, while the sharer keeps the responsibility and accountability for using this resource according to applicable rules. Sources for these applicable rules are both this PRD and an agreement between the sharer and the sharee.

Term	Description
VPN	Virtual Private Network; Extends a private network across a public network. For the hosts that are joined to the private network via VPN, the network appears as if it was directly connected to the private network. The transport network that is traversed by the VPN connection is transparent to the members of the VPN. A VPN can either be established at ISO OSI layer 2 or 3. Multiple technologies exist. Examples are: MPLS path with VR, ATM Circuit, or IPSec.

To unambiguously understand the difference between the types of networks, the following figures illustrate their purpose and boundaries.

All figures share the same meaning of the graphical elements, as depicted in the legend below.

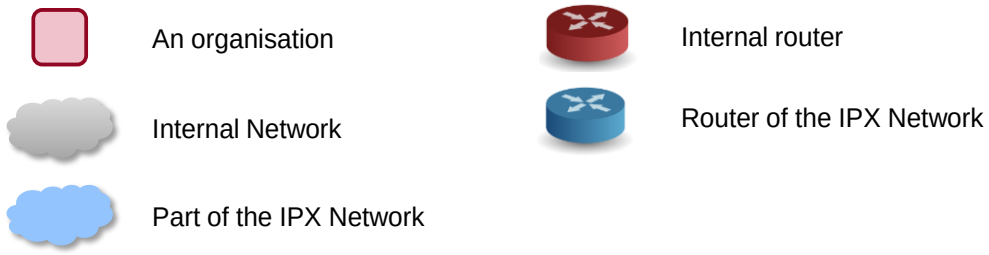

Figure 1:Legend of graphical elements of all figures in this document

The figure below illustrates a logical separation of networks, their owners and the purpose of the networks. IPX Provider Networks and Service Provider Networks are part of the IPX Network, whereas all the other networks are not. Furthermore, IPX Providers and Service Providers also operate networks which are owned by them but which are outside the IPX Networks. These latter networks are Internal Networks, such as a Management Network or the Office Network.

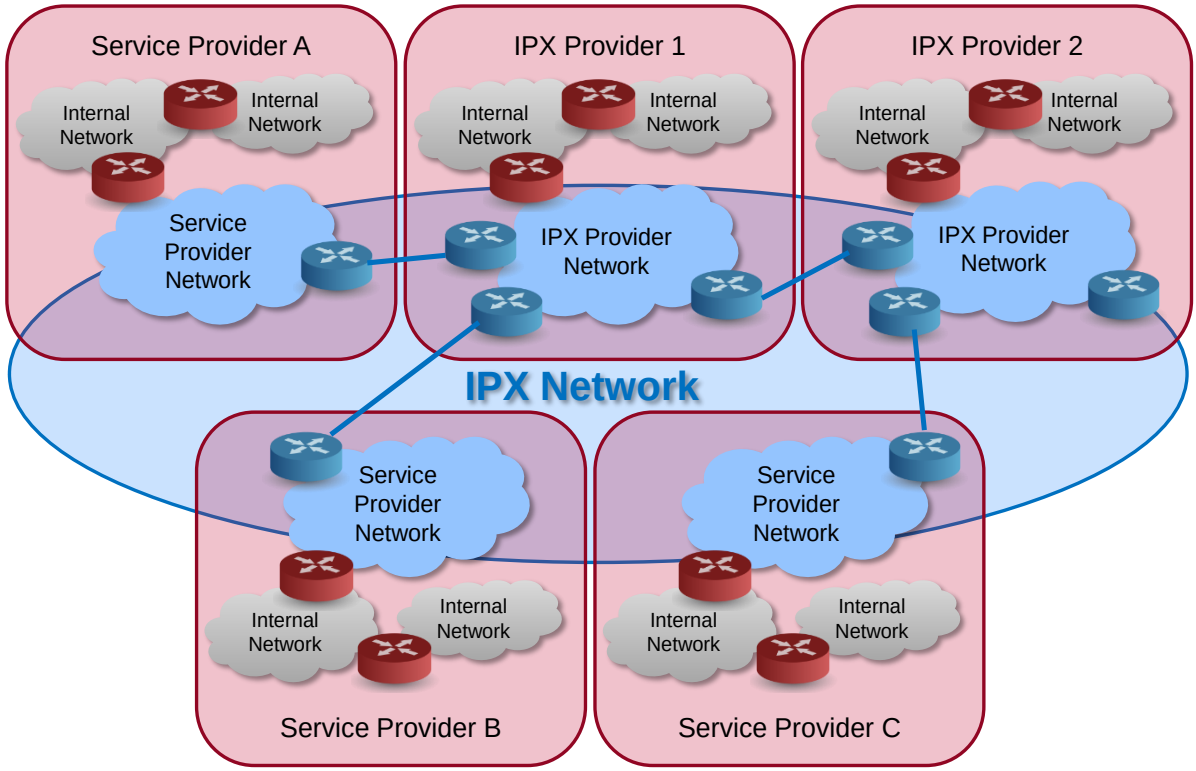

Figure 2: Schematic overview logical separation of networks

1.5 Abbreviations

Term	Description
AS	Autonomous System
AVP	Attribute Value Pair
BG	Border Gateway
BSR	Binding Security Requirement
DoS	Denial of Service
DDoS	Distributed Denial of Service
GTP	GPRS Tunneling Protocol
HTTP	Hypertext transfer protocol
HTTPS	Secure Hypertext transfer protocol
IMS	IP Multimedia Subsystem (specified by 3GPP)
IP	Internet Protocol
ISP	Internet Service Provider
LTE	Long Term Evolution (Radio)
MNO	Mobile Network Operator
MPLS	Multiprotocol Label Switching
n/a	Not applicable
NSR	Non-binding Security Requirement
PGW	PDN (Packet Data Network) Gateway
PMIP	Proxy Mobile IP
PRD	Permanent Reference Document
SGW	Serving Gateway
SIP	Session Initiation Protocol (defined by IETF)
SNMP	Simple network management Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control System
UE	User Equipment

Term	Description
UMTS	Universal Mobile Telecommunications System, i.e. “3G”
VPN	Virtual Private Network
VR	Virtual Router

1.6 References

Ref	Doc Number	Title
[1]	BCP 5	“Address Allocation for Private Internets”, IETF Best Current Practice, IETF. (At the time of writing also known as RFC 1918.)
[2]	BCP 38	“Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, IETF Best Current Practice, IETF. (At the time of writing also known as RFC 2827.)
[3]	BCP 84	“Ingress Filtering for Multihomed Networks”, IETF Best Current Practice, IETF. (At the time of writing also known as RFC 3704.)
[4]	PRD AD.12	“Terminology Database – Approved Words and Acronyms”, GSMA.
[5]	PRD IR.21	“GSM Association Roaming Database, Structure and Updating Procedures”, GSMA.
[6]	PRD IR.33	“GPRS Roaming Guidelines”, GSMA.
[7]	PRD IR.34	“Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines)”, GSM Association.
[8]	PRD IR.40	“Guidelines for IPv4Addressing and AS numbering for GPRS Network Infrastructure and Mobile Terminals”, GSMA.
[9]	PRD IR.61	“WLAN Roaming Guidelines (Inter-Operator Handbook)”, GSMA.
[10]	PRD IR.65	“IMS Roaming & Interworking Guidelines”, GSMA.
[11]	PRD IR.67	“DNS Guidelines for Operators”, GSMA.
[12]	PRD IR.85	“Roaming Hubbing Provider Data”, GSMA.
[13]	PRD IR.88	“LTE Roaming Guidelines”, GSMA.
[14]	PRD IR.90	“RCS Interworking Guidelines”, GSMA.
[15]	RFC 4193	“Unique Local IPv6 Unicast Addresses”, IETF Standards Track Proposed Standard, IETF.
[16]	RFC 4271	“A Border Gateway Protocol 4 (BGP-4)”, IETF Standards Track Draft Standard, IETF.
[17]	RFC 4291	“IP Version 6 Addressing Architecture”, IETF Standards Track Draft Standard, IETF.
[18]	RFC 4364	“BGP/MPLS IP Virtual Private Networks (VPNs)”, IETF Standards Track Proposed Standard, IETF.
[19]	RFC 4381	“Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)”, IETF Informational Memo, IETF.
[20]	RFC 5920	“Security Framework for MPLS and GMPLS Networks”, IETF Informational Memo, IETF.
[21]	TS 184 010 V3.1.1 (2011-08)	“Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN);ENUM & DNS Principles for an Inter-Service Provider IP backbone network”, ETSI.
[22]	TS 23.060	“General Packet Radio Service (GPRS); Service Description; Stage 2”, 3GPP.
[23]	TS 23.228	“IP Multimedia Subsystem (IMS); Stage 2”, 3GPP.
[24]	TS 29.060	“General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface”, 3GPP.
[25]	PRD FS.19	“Diameter Interconnect Security”, GSMA.
[26]	PRD NG.137	‘IPX requirements’

1.7 Conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, “may not”, and “optional” in this document are to be interpreted as described in GSMA PRD AD.12 0.

The following explains how to read the tables in Sections 3 and 4. Each table represents one requirement. The requirement BSR 10 is used as an example here.

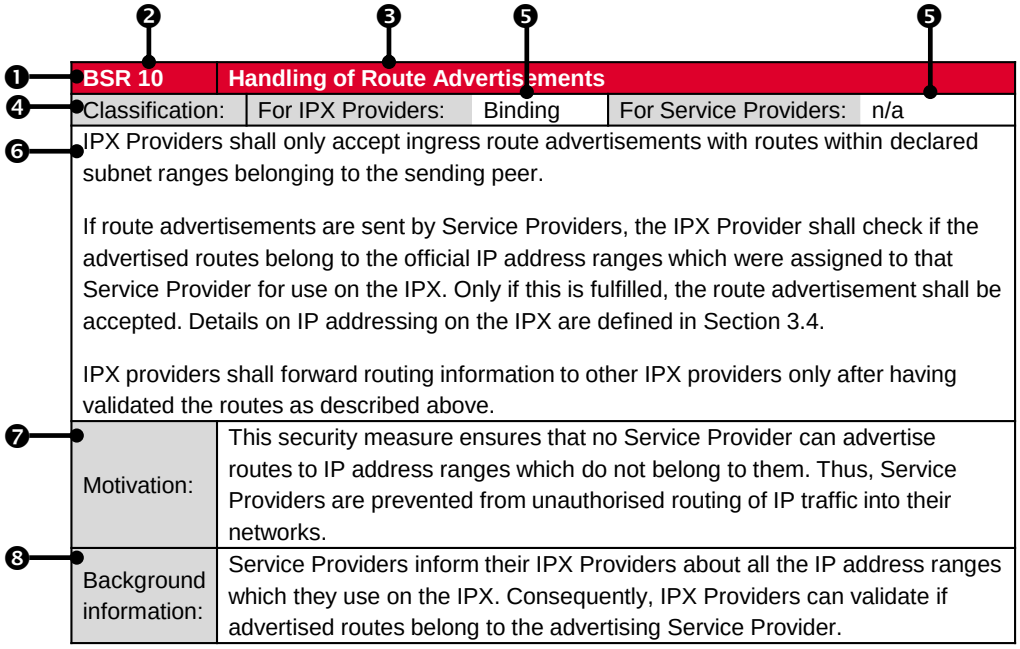

Figure 3: Illustration of the structure of requirements in this document

□	Indicates if the requirement is binding (BSR = Binding Security Requirement) or non-binding (NSR = Non-binding Security Requirement).
□	The number of the requirement. Together with its classifier BSR or NSR it is unique in the document.
□	Title of the requirement which briefly describes what the requirement is about.
□	This line classifies the requirement, insofar as it defines on who it is binding. There is a classification for both IPX Providers and Service Providers as described in □:
□	Classifies the requirement for IPX Providers and Service Providers and valid classifications are: • Binding – the entire requirement is binding; • Non-binding – the entire requirement is non-binding, but it is recommended to implement it entirely; • n/a – not applicable – the entire requirement is not applicable
□	Definition of the requirement itself and what is to be done. This text is normative.
□	Text explaining why this requirement has been defined. It explains which security improvement is achieved by fulfilling this requirement. This text is informational and non-normative.
□	Text which provides background information to provide a broader context for the requirement. This text is intended to provide a clearer explanation of the requirement background. This text is informational and non-normative.

Table 1: Conventions on how to read the requirements in this document

2 Security Basics and Principles

2.1 2.1 Introduction

Due to interconnection and roaming, the internal Service Provider network is exposed to other external networks. Consequently, measures to securely allow partners to interconnect

in a controlled way have to be deployed, without revealing confidential information or facilitating fraud/abuse.

Ensuring that adequate security levels are in place is not just a matter of deploying the right technology in the right place. It is critical that the IPX is based on a secure network design and that proper procedures are adequately defined and continuously adhered to throughout the entire security chain, particularly at an operational level.

Security cannot be achieved by just one Service Provider or IPX Provider within the network, it requires that every single participant in the network fulfils their part of the requirements.

2.2 High Level Security Objectives

In a high level approach to IPX security, the following key security objectives have to be achieved. The IPX infrastructure together with its security features shall:

- Ensure that any data which is transferred on the IPX cannot be tampered with or altered by unauthorised parties, by, for example, real-time traffic interception (man in the middle), traffic injection or replay attacks;
- Ensure that information is protected from unauthorised interception and disclosure;
- Be able to validate that all parties involved in data communication are who they claim to be.

Only if these objectives are achieved, trustworthy communication on the IPX between legitimate peers is possible. Such a secure network between Service Providers is the key benefit of the IPX when compared to public networks, such as the Internet.

This document defines how these objectives can be achieved.

3 Binding Security Requirements

The security requirements described in this section define what is to be done and how it is to be done to achieve IPX Network security. These requirements are binding for all participants in the IPX Network unless stated otherwise.

3.1 3.1Packet Filters

Various filter rules must be applied by both IPX Providers and Service Providers on their networks. Only traffic from genuine IP addresses shall be transported and networks shall be protected from each other. Anti-packet spoofing measures must be implemented within the IPX Network.

BSR 01	**IP Packet Filtering at all Network Edges**			
Classification:	**For IPX Providers:**		**For Service Providers:**	
Each Service Provider and IPX Provider shall filter ingress and egress traffic at the network edge between the IPX Network and the Service Provider's network (e.g. by Access Control Lists (ACLs) or firewall rules): Ingress IP packets with source IP addresses belonging to private networks shall be dropped. Egress IP packets with destination IP addresses belonging to private networks shall be dropped.				

BSR 01	IP Packet Filtering at all Network Edges
Ingress IP packets with a source address belonging to the IP range assigned to internal networks shall be dropped. Egress IP packets with a destination address belonging to the IP range assigned to internal networks shall be dropped. IPX Providers and Service Providers shall apply filtering on the network interface where ingress IP packets from the communication partner are expected. Depending on the application and the IPX Service, there may be a need for additional application layer filters, such as GTP-Firewalls (see PRD IR.88 0) or Diameter Agents (see PRD IR.88 0). For IPX Services additional PRDs apply. Application layer filters are defined there, if required. If Service Providers bilaterally decide to encrypt their traffic payload, IPX Providers shall carry that traffic through the IPX. If Service Providers use IP addresses from a private network for their links to their IPX Provider, these private IP addresses shall not be dropped. Any other private source/destination addresses shall be dropped as defined here. See BSR 14 for details.	
Motivation:	Applying these IP packet filters ensures that only legitimate data traffic can be sent across network boundaries. The filters are also a measure against IP source address spoofing, as packets are only accepted if they have a source address which belongs to the sending network.
Background information:	It is up to the owner of the network, which network element applies these filters, as long as packets are filtered directly at the network edge. For example, the Border Gateway (BG) or a separate firewall are suitable. It is important to apply the filters on the network interface to which the peer is connected at the network edge. Only at this network interface can network traffic be unambiguously assigned to the connected peer. In combination with the knowledge of the IP address ranges which belong to that peer, sanity checks and anti-spoofing measures can be applied to IP packets. All these filters apply to the outer IP headers. Some IP packets contain tunnelled IP packets and they have more than one IP header. For routing on the IPX, only the outer IP header is relevant. This is where all rules are applied.

BSR 02	IP Packet Filtering on Service Provider Networks		
Classification:	For IPX Providers:		For Service Providers:
Each Service Provider shall filter ingress and egress traffic in addition to BSR 01 as follows: Only accept those network layer (layer 3) and transport layer (layer 4) protocols (i.e. IPv4, IPv6, ICMPv4. ICMPv6, TCP, UDP, SCTP, etc.) which are agreed to be used with the peers on the IPX. A peer in this context is the IPX Provider which connects the Service Provider to the IPX Network or another Service Provider with which a roaming agreement exists. Allowable traffic is: User data traffic and signalling traffic between two peer Service Providers according to PRD IR.21 0 RAEX database and PRD IR.85 0 roaming hub database, if a roaming agreement exists between these two Service Providers. Limited to only those application layer protocols and ports (e.g. GTP, Diameter), which are to be accessible according to the roaming agreement. Troubleshooting traffic between Service Providers and their respective IPX Providers via which they are connected to the IPX Network if mutually agreed. Accept ingress IP packets only if there is a route back to the source of the IP packet via the IPX Network. Egress IP packets with a source address not belonging to a valid address range of a network of the sending Service Provider (e.g. internal networks) shall be dropped. It is the Service Provider's responsibility to determine the plausibility of incoming messages prior to processing them on the destination host.			
Motivation:	Applying these IP packet filters ensures that only data traffic where legitimate protocols are used can be sent across network boundaries. This reduces the attack surface of the Service Provider’s network.		
Background information:	Good practice is to apply these filters (on a firewall or the Border Gateway (BG)) at the network edge to the IPX with individual rules per peer. Routing is not		

BSR 02	IP Packet Filtering on Service Provider Networks
	affected by these filters, as routing is organised dynamically by BGP (RFC 4271 0). By that, routing will always work, but the firewall limits communication only to allowed peers. Only accepting IP packets if there is a route back to the source is a feature that is also supported by BGP.

BSR 03	IP Packet Filtering on IPX Provider Networks		
Classification:	For IPX Providers:		For Service Providers:
IPX Providers shall deploy IP anti-spoofing protection on the IPX Network to ensure that Service Providers cannot successfully use forged IP addresses. The filter rules of BSR 01 contain IP anti-spoofing rules. In addition, BCP 38 0 and BCP 84 0 shall be implemented. On the IPX Network, IPX Providers do not filter on the transport layer (layer 4) or higher. The IPX transports any traffic that is exchanged between legitimate Service Providers and IPX Service Hubs. IPX Providers shall protect their internal networks (other than the IPX Network e.g. management network, office network, etc.) and shall apply the following filters at the edge to the IPX Network: All IP packets transmitted between the IPX Network and internal networks shall be dropped. Only accept those network layer (layer 3) and transport layer (layer 4) protocols (i.e. IPv4, IPv6, ICMPv4. ICMPv6, TCP, UDP, etc.) which are required for communication between the management network and the IPX. Egress IP packets with a source address not belonging to a valid address range of a network of the sending IPX Provider (e.g. internal networks) shall be dropped. Service Providers may partially or fully outsource their routing to the IPX Provider to which the Service Provider is connected. In this case, the IPX Provider shall apply all the filtering rules of BSR 01 and BSR 02 on behalf of the Service Provider on the network edge between these two parties' networks. A bilateral agreement between the two parties is required to define the details.			
Motivation:	Applying these filters protects internal networks of the IPX Provider from attacks from the IPX Network. This makes the IPX Network more robust and secure as attackers cannot gain access to management systems and other components which would allow the attacker to reconfigure network elements on the IPX Network.		
Background information:	Networks of IPX Service Hubs and Internal networks of IPX Providers need the same protection and isolation as Service Provider networks. This is why the filters shall also be applied to networks which are owned/operated by IPX Providers but which are not the IPX Network.		

3.2 3.2 Isolation of the IPX Network

The IPX Network shall be physically or logically separated from all other networks that are not part of the IPX Network, including, but not limited to, the Internet, management networks, IPX Provider internal office networks, and other IP networks which are operated on the same infrastructure as the IPX Network.

BSR 04	Isolation of the IPX Network		
Classification:	For IPX Providers:		For Service Providers:
Isolation of the IPX Network shall be done by having a physically separate network (on the Physical Layer, layer 1) or by logical separation on the Data Link Layer (layer 2) of the ISO OSI network stack model. It shall be ensured that users of networks other than the IPX Network have no means of access to the IPX Network. No IP packet or routing information shall be disclosed outside the IPX Network. All the following rules apply:			

BSR 04	Isolation of the IPX Network
• Network isolation shall be performed on all links (i.e. network connections) on the network. • Network isolation shall be performed on all network elements, including, but not limited to, routers, gateways, switches, and interconnection points. • If isolation is done logically, there must be separate routing instances on the network elements for the IPX Network and the other networks. In other words, networks shall not share the same routing tables and routing processes on network elements. This can only be achieved by isolating on a layer below the Network Layer (i.e. below layer 3). This requirement holds for both IPX Provider Networks and Service Provider Networks.	
Motivation:	Isolating the IPX makes sure that only those entities that need legitimate access to the IPX Network actually have access to the IPX Network and all the IPX Services. This reduces the attack surface of IPX Services and network elements on the IPX Network as illegitimate entities have no access to them.
Background information:	Isolation is only effective if all network elements and links enforce isolation. A comprehensively secure network design and configuration is needed. Every network element which processes IP packets must enforce the separation without exception. Every link (i.e. connection) between network elements must also be kept separate from other networks' traffic. Separation on a layer below layer 3 ensures that information from layer 3 (IP addresses, IP subnet ranges, routing tables) cannot be used to influence routing. If an attacker crafts a forged IP packet, the IP packet cannot break out of the boundaries that are defined by the separation on the lower layers. It is good practice to combine Virtual Router (VR) with MPLS to have separation on both the communication link and the network element. VR provides separate routing tables and processes for each MPLS VPN. Resources on MPLS and MPLS security on the Internet are RFC 4364 0, RFC 4381 0 and RFC 5920 0. It is also good practice to use VLANs and to make sure that the IPX Network and all the other networks are each operated in a separate VLAN and that they are fully separated. Note that common routing tables, access control lists (ACLs) and layer 3 VPNs that add additional IP headers to IP packets do not provide isolation at all. Thus, they must not be used. Isolation on layer 2 protects IP networks from being accessed by other separated networks. It does not protect against manipulation on transit. For example, it is not enough to only deploy MPLS. It is widely assumed that MPLS per se is secure. This is not the case, as MPLS just adds a label to the packet. Packets can still be altered, forged and read by any hop on transit. This requires all hops on transit to be trusted.

BSR 05	Isolation of IPX Service Communities		
Classification:	For IPX Providers:		For Service Providers:
Each IPX Service Community is isolated from all other Service Communities. A Service Provider, when connecting to the IPX, connects explicitly to Service Communities. Via Service Communities, only those Service Providers are reachable which are connected to the same IPX Service Community. Details are defined in PRD IR.34 **Error! Reference source not found.**. All Service Providers and IPX Providers shall ensure that Service Communities are isolated at all times and that IP traffic cannot cross Service Communities. This isolation also holds for all network edges between Service Providers and IPX Providers. Isolation of Service Communities can be done physically or logically.			
Motivation:	Isolating IPX Service Communities from each other ensures that only those players that participate in an IPX Service Community can actually access services that are offered there. This creates a closed community where illegitimate entities cannot access the services. This reduces the attack surfaces of the services, as		

BSR 05	Isolation of IPX Service Communities
	they are only accessible by those who signed an agreement to join the community.
Background information:	Which IPX Services are provided in which IPX Service Community is defined in PRD IR.34 **Error! Reference source not found.** and additional PRDs that define IPX Services.

BSR 06	Access to the IPX Network		
Classification:	For IPX Providers:		For Service Providers:
Service Providers must ensure that only legitimate networks have access to the IPX Network. A legitimate network is a network which has network elements that communicate with peers on the IPX Network based on an agreement between the peers or intermediate parties. Such a network either belongs to a Service Provider that is directly connected to the IPX Network or it belongs to a Service Provider that shares another Service Provider's connection to the IPX Network. No Service Provider shall route/forward any traffic coming from or going to the IPX Network to any other than a legitimate network as defined above. Traffic from the IPX Network either terminates at the Service Provider or at one of the Sharee Service Provider networks. Otherwise, it is discarded by the Service Provider. Traffic to the IPX Network either originates from a network of the Service Provider or one of its Sharee Service Providers. Otherwise, it is discarded by the Service Provider.			
Motivation:	There shall by no means be a connection between the IPX Network and any other (public) network which is not legitimate. This reduces the attack surfaces of network elements on the IPX Network as the network elements are only accessible by those who are legitimate participants in the IPX Network.		
Background information:	Service Providers shall ensure that they do not establish illegitimate connections and that they do not configure routes through their networks to establish such connections. Only network elements that are supposed to communicate with parties on the IPX Network shall have access to the IPX Network. For Mobile Network Operators, this is typically limited to the Mobile Core Network. The network architecture shall be designed, implemented, and configured accordingly.		

BSR 07	Shared Access to the IPX Network		
Classification:	For IPX Providers:		For Service Providers:
Service Providers can share their connection to the IPX. If they do so, they shall fulfil the following requirements: There is exactly one Service Provider that has the connection to an IPX Provider. This is the *sharer* in the context of this requirement. One or more other Service Providers – called *sharee* in the context of this requirement – are subcontractors. They are connected to the sharer's network to access the IPX Network via the sharer's network. Each sharer shall inform their IPX provider that they share their network with other Service Providers. Each sharer shall inform their IPX provider about the network range which is used by the sharee(s) on the IPX Network. The IPX Provider can then route IP packets accordingly on the IPX Network. The sharer has full responsibility and liability for its IPX connection that it shares with all its sharees. This means in particular that the sharer shall apply all applicable security requirements of this document on the connection between the sharer and the sharee(s). These are: BSR 01 through BSR 06 and BSR 10.			
Motivation:	One of the key security goals of this PRD is to ensure IP anti-spoofing on the IPX. According to BSR 01, this is implemented by the IPX Providers. If a Service Provider shares its connection to the IPX Network, the sharing Service Provider (i.e. the sharer) shall apply the same filters on the connection to the sharees, as the IPX Provider applies on the connection to the sharer. By that, the sharer, among others, drops all spoofed IP packets sent to the IPX by the sharee.		

	The sharer needs to inform its IPX Provider about network sharing so that the IPX Provider can allow IP packets with source addresses from a sharee's network being sent to the IPX.
Background information:	Whenever a connection to the IPX Network is shared among multiple Service Providers, there shall always be one Service Provider among them who officially owns the connection to the IPX Provider. Evenly shared ownership and responsibility shall not be allowed.

BSR 08	**Handling of Inter-Service Provider Traffic**		
Classification:	**For IPX Providers:**		**For Service Providers:**
Inter-Service Provider traffic, such as signalling and data roaming traffic, shall exclusively be transported on the IPX Network or via dedicated bilateral links. Public networks shall not be used for such traffic. The only exception from this requirement that may exist in special cases is a secured VPN to tunnel IPX through other networks. Requirements from Section 3.5 apply.			
Motivation:	Transporting inter-Service Provider traffic only through the IPX Network and dedicated bilateral links ensures that the data is only accessible to a limited number of parties. This increases integrity and confidentiality of the data being transported and it reduces the attack surface of network elements and IPX Services.		
Background information:	If the Internet was used for inter-Service Provider traffic, the attack surface would be unnecessarily high. Any attacker worldwide could aim at exploiting this communication. This is a threat to dependability of inter-Service Provider communication.		

BSR 09	**Isolation of Management Interfaces**		
Classification:	**For IPX Providers:**		**For Service Providers:**
Access to network elements shall only be granted from Internal Networks, such as a management network. From the transport network – i.e. the IPX Network and Service Provider Networks – it shall not be possible to access services on network elements. Network elements shall either physically or logically separate routed/switched traffic on the transport network from traffic accessing the network elements. There shall also be no routing information to the management networks available inside the transport network. Network elements can be either managed in-band or out-of-band. For in-band management, no separate logical or physical network is used. In this case, all Network Services on the network element shall be bound to a loopback interface with its own IP address that is not reachable from the IPX Network. Out-of-band management refers to a separate physical or logical network that connects management interfaces of the network elements. In the out-of-band case, the management interface shall only be accessible from the management network.			
Motivation:	This kind of isolation ensures that network services on management interfaces or management IP addresses are only accessible by management networks, but not by any peer Service Provider or peer IPX Provider. The network element is not accessible on the IPX Network. Only its functionality to process traffic, e.g. routing, can be used on the IPX Network. By that, the network element does not expose itself to attacks which are targeted to network services that are running on the network elements directly.		
Background information:	This requirement applies for IPX Providers for all network elements on the IPX Network and for Service Providers for all network elements on Service Provider Networks.		

3.3 Routing

Anti-route spoofing measures must be implemented within the IPX. It is the IPX Provider's responsibility to check that its customers are advertising only valid IP-networks that belong to them. Further details on routing and handling of route advertisements are defined in PRD IR.34 **Error! Reference source not found.**.

BSR 10	**Handling of Route Advertisements**			
Classification:	**For IPX Providers:**		**For Service Providers:**	
IPX Providers shall only accept ingress route advertisements with routes within declared subnet ranges belonging to the sending peer. If route advertisements are sent by Service Providers, the IPX Provider shall check if the advertised routes belong to the official IP address ranges which were assigned to that Service Provider for use on the IPX Network. Only if this is fulfilled, the route advertisement shall be accepted. IPX Providers shall forward routing information to other IPX Providers only after having validated the routes as described above.				
Motivation:	This security measure ensures that no Service Provider can advertise routes to IP address ranges which do not belong to them. Thus, Service Providers are prevented from unauthorised routing of IP traffic into their networks.			
Background information:	Service Providers inform their IPX Providers about all the IP address ranges which they use on the IPX Network. They do so by publishing these IP address ranges in the PRD IR.21 0 RAEX DB and by notifying their IPX Providers directly (e.g. in the contract between these two). Consequently, IPX Providers can validate if advertised routes belong to the advertising Service Provider. IPX Providers shall accept Route Advertisements from their client Service Providers only if the sending ASN belongs to the sending Service Provider and if the Route Advertisement is being sent via the link by which the Service Provider is connected to the IPX Provider. If a Service Provider performs network sharing with another Service Provider, the sharing Service Provider may also advertise the network of the Sharee Service Provider. Details on IP addressing on the IPX are defined in Section 3.4.			

BSR 11	**Default Routes in Service Provider Networks**			
Classification:	**For IPX Providers:**		**For Service Providers:**	
Service Providers shall not configure a default route (AKA "route of last resort") on their Service IP Edge routers which are connected to IPX providers. All IP routes to peer Service Providers peer/partner Service Providers shall be dynamically learned from IPX Provider(s) via BGP on the Service Provider's IP Edge routers which are interconnected to IPX Provider(s). As a result of IPX Provider filtering according to BSR 10, these IP routing advertisements from the IPX Provider(s) should align with the IP ranges from peer/partner Service Providers which are declared on the PRD IR.21 0 RAEX database and the PRD IR.85 0 roaming hub database. If, and only if an IPX Provider maintains routing tables on behalf of a customer Service Provider, the Service Provider can configure a default route which is pointing to the IPX Provider. In this case, the IPX Provider shall do the following in addition: Adhere to BSR 02 on behalf of the Service Provider, and Not configure a default route for ingress IP traffic from the customer Service Provider.				
Motivation:	This ensures that IP traffic is only sent to those peers on the IPX to which a Service Provider intends to send IP packets. IP traffic cannot be sent to other networks mistakenly. If an IPX Provider maintains routing tables on behalf of a customer Service Provider, the IPX Provider acts on behalf of the Service Provider w.r.t. routing. In			

BSR 11	Default Routes in Service Provider Networks
	this case, the IPX Provider shall comply with all those routing-related security requirements which are binding for the Service Provider so that the customer Service Provider experiences the same level of security as a Service Provider that takes care of routing on its own.
Background information:	Note: A Service Provider only needs to have IP routes to peer/partner Service Providers for “non-service-aware” services, such as Data Roaming, which do not use full proxy devices within the IPX Provider(s). For “service-aware” services, the IP routes which a Service Provider needs are those of the full proxy devices (signalling routers, STPs, SIP signalling+media proxies, etc.) which reside in the IPX Provider(s) network(s), not in the partner Service Providers’ networks.

3.4 Assignment of IP Addresses

According to PRD IR.34 **Error! Reference source not found.**, public addressing shall be applied in all Service Provider IP Backbone network elements, which are advertised or visible to other Service Providers. Using public addressing means that each Service Provider has a unique address space that is officially reserved from the Internet addressing authority.

BSR 12	Use of Official IP addresses for IPX			
Classification:	For IPX Providers:		For Service Providers:	
Service Providers shall not use their officially assigned IP addresses which are reserved for the IPX in any other network than their Service Provider Network. IP addresses which are used for the IPX Network and for Service Provider Networks shall not be accessible/visible on public networks, such as the Internet. No routing shall be possible from public networks to these IP addresses. Service Providers should only advertise these addresses on the IPX Network and on their own Service Provider Network.				
Motivation:	Using only the officially assigned IP addresses on the IPX Network supports isolation of the IPX from other networks.			
Background information:	NOTE: Service Providers may use an IP subnet of officially assigned IP addresses on the IPX which is smaller than a /24 network. If this subnet is a subset of a larger network that is used by the Service Providers on the Internet, the Service Provider is not allowed to exclude this subnet from their BGP route advertisements on the Internet. The Service Provider must ensure that no host is reachable on this subnet on the Internet. There shall be no routing from the Internet to these IP addresses on the IPX Network. NOTE: As defined in Section 1.4, the term “Service Provider Network” only refers to the IP network(s) of a Service Provider that is connected to the IPX Network. A Service Provider Network contains one or more hosts or network elements which communicate with peers on the IPX Network. All other IP networks of the Service Provider shall not use IP addresses that are reserved for the IPX Network.			

BSR 13	No Routing of UE Addresses on the IPX Network			
Classification:	For IPX Providers:		For Service Providers:	
Networks with IP address ranges of User Equipment (UE) of the customers and Internet-facing hosts shall not have any routing information to reach IP address ranges which are assigned to the IPX Network. No routing information to IP address ranges which are assigned to UEs shall be configured or advertised on the IPX and on Service Provider Networks.				

Motivation:	Not routing UE addresses makes sure that UE and Internet traffic cannot address network elements on the IPX Network. The infrastructure on the IPX Network and on Service Provider Networks is fully transparent to the UE. This ensures network isolation and it also mitigates possible routing issues due to configuration mistakes on routers on the IPX Network and on Service Provider Networks.
Background information:	IPX Providers do not know address ranges of UE. They shall only route traffic between peers they know, as defined in Section 3.3. This results in having no routing information for UE addresses on the IPX Network. All UE traffic must be tunnelled through the IPX Network as defined in BSR 16.

BSR 14	**Use of Private IP Addresses on the IPX Network**		
Classification:	**For IPX Providers:**		**For Service Providers:**
Service providers can use private IP addresses for their network elements which are connected to the IPX Network. If Service Providers do so, they shall fulfil the following requirements: The next hop towards the IPX Network, i.e. the IPX Provider must unambiguously know which Service Provider is connected to the IPX Provider by a given IP address or IP address range. Private IP addresses are allowed only for the direct connection between a Service Provider and its IPX Provider. The network elements of the Service Provider that are connected to the IPX Network shall be reachable unambiguously on the entire IPX Network with official IP addresses only. Only official IP addresses shall be published in the PRD IR.21 0 RAEX database and in the PRD IR.85 0 roaming hub database for Service Providers. IPX Providers shall ensure an unambiguous mapping between the private IP addresses which they use towards their client Service Providers and the official IP addresses which they use on the IPX Network on behalf of this Service Provider One official IP address shall not be used for more than one Service Provider.			
Motivation:	For unambiguous routing and for a clear mapping of Service Providers and their IPX Services to IP addresses, official IP addresses shall be used on the IPX Network. Some IPX Services require Service Providers to clearly identify their peer Service Provider by its IP address. This is why IP addresses shall not be used for more than one Service Provider.		
Background information:	Some Services (e.g. Diameter signalling or MAP signalling) terminate IP on each hop. If the IPX Provider knows how to reach the next hop – i.e. a network element of a Service Provider – private IP addresses can be used. Other services, which require peers on the IPX Network to directly connect to Service Providers on IP level, require NAT at the IPX Provider which serves the Service Provider's IPX Network access.		

3.5 IPX Tunnelling Through Public Networks

Whenever IPX Network internal data traffic is transported through public networks, a secure communication channel is required.

BSR 15	**IPX Tunnelling Through Public Networks**		
Classification:	**For IPX Providers:**		**For Service Providers:**
If a public network (e.g. the Internet) is used to tunnel IPX traffic, a secure communication channel must be established prior to data exchange. IPsec must be used to secure all the communication. Encryption, integrity protection and authentication shall be enabled. Unauthenticated IP packets must be dropped. None of the tunnelled networks shall be visible/accessible on the public network. Only encryption and signature algorithms which are considered as secure by the security			

BSR 15	IPX Tunnelling Through Public Networks
community[1] shall be used. The use of algorithms shall be revisited periodically to determine if the algorithms are still considered secure. If they are no longer considered secure, stronger algorithms and/or key lengths shall be chosen. It is up to a bilateral agreement between the parties who establish the tunnel, to define which algorithms are used. Dedicated equipment shall be used to establish the tunnel. Network elements of the IPX shall not be used as tunnel endpoint. The equipment that is used as tunnel endpoints must not be accessible by anybody from the public network. Only the peer tunnel endpoint and only the required protocol (i.e. IPSec and IKE) shall be accessible on the public network. The tunnel endpoints must be configured securely and hardened as defined in BSR 17. An IPSec tunnel must be used for all IPX traffic as soon as it is transported via a public network. This also includes User Equipment Traffic, even though User Equipment Traffic is already tunnelled (see Section 3.6). This is required, as the tunnel for User Equipment traffic does not provide any security for the payload.	
Motivation:	This contributes to IPX isolation. The network through which the IPX is tunnelled cannot access the IPX Network and IPX Network traffic is not disclosed to that network.
Background information:	From PRD IR.34 **Error! Reference source not found.** version 7.0 onwards, QoS is required with every IPX Service. Using IPsec tunnels over the Internet does not support QoS. This is why tunnelling the IPX through public networks should be disregarded. Dedicated security gateways shall be used to terminate the IPsec tunnel. None of the already existing network elements on the IPX Network or on a Service Provider Network shall be used. This is to make sure that only these dedicated security gateways are exposed to the public network. NOTE: As the whole infrastructure (IPX Network and Service Provider Networks) is planned and operated in a secure way as described in this document, it is not necessary to encrypt every data stream and network segment. However, encryption shall be applied where defined in this PRD and in other PRDs which define IPX Services.

3.6 User Equipment Traffic Tunnelling Through the IPX Network

The IPX Network is transparent to end users. Consequently, end users shall not be able to address any network element on the IPX Network.

BSR 16	User Equipment Traffic Tunnelling Through the IPX Network		
Classification:	For IPX Providers:		For Service Providers:
Service Providers shall encapsulate all UE (User Equipment) originating and targeting traffic by utilising tunnelling protocols for transporting any UE traffic through the IPX Network. It is a Service Provider's decision where that tunnel starts in its network. The parties involved in the communication decide by agreement where the other endpoint of the tunnel is located. It terminates either at the peer Service Provider or at an IPX Service Hub. The tunnel to be used depends on the IPX Service. PRD IR.34 **Error! Reference source not found.** describes all the IPX Services and refers to further PRDs for each IPX Service.			

[1] There is no consistent view on adequate key lengths among the cryptography experts. However, there is some tendency. In order to determine suitable cryptographic algorithms and key lengths, cryptography experts from the academia should be consulted. Some organisations and public authorities also provide recommendations. The one perfect source of information does not exist. The Web site www.keylength.org, which is owned and maintained by a security consultancy company, gives useful information about algorithms and key lengths. It also provides links to useful resources. The use of this Web site's content is not binding. This footnote is informational and non-normative.

BSR 16	User Equipment Traffic Tunnelling Through the IPX Network
Motivation:	Tunnelling of UE traffic ensures that no UE can address and access network elements on the IPX Network and on Service Provider Networks.
Background information:	All UE traffic is transported through these tunnels. It is the Service Provider's responsibility to only send UE traffic which adheres to the definitions in the PRDs which are referred to in this requirement. Should UE traffic be encrypted by the user, the UE traffic is also transported through these tunnels. The form of UE traffic shall have no impact on using or not using tunnels for UE traffic.

3.7 Secure Configuration of Network Elements, Network Services and IPX Services

Network elements and network services shall be configured securely. Default configurations are often insecure.

BSR 17	Secure Configuration of Network Elements and Services			
Classification:	For IPX Providers:		For Service Providers:	
The following configuration shall be applied to all network elements, network services, and IPX Services on the IPX Network and on IPX Provider Networks: Disable all unnecessary network services on network elements. Enable only those network services on all network elements which are necessary for their regular operation and those which are needed for management. Network element hardening. All network elements which are involved in traffic processing of any kind on the IPX Network and on Service Provider Networks must be hardened according to the device manufacturer's hardening guides and possibly additional widely used/accepted hardening guides. Typically, the default configuration of network elements is insecure. Bind network services to network interfaces and/or IP addresses. Network services must be bound to only those network interfaces and/or IP addresses on a network element where they are needed. No service shall listen on all interfaces/IP-Addresses. (Example: SSH is only needed on the management interface but not on the interface that is accessible on the IPX Network.) Secure configuration of services. Whenever a network service (e.g. DNS) or an IPX Service (e.g. Diameter Signalling) is offered on the IPX Network, this service shall be configured and maintained securely. The hardening guides of the supplier of the service shall be applied. Services shall only provide the functionality which is actually needed on the IPX. All unused functionality shall be disabled. Management protocols shall not be accessible from the IPX Network. Patch Management. All network elements and services shall only be operated using the latest version of software and firmware to ensure that known vulnerabilities that are fixed by the vendor are no longer existing on the network elements. A patch management process is to be established that obtains, tests, and rolls-out patches as timely as possible.				
Motivation:	Secure configuration of network elements and services reduces the attack surface, as services which are not needed are not available and services which are needed are only available on the interface on which they are needed. If a service turns out be vulnerable to an attack, a reduced number of potential attackers has access to these network elements. Once a vulnerable network service is exploited, the attacker can reach out to further network elements which are accessible from the exploited one. If a network service is critical for the IPX, e.g. DNS, the attacker may also manipulate the DNS database and the DNS server would respond with incorrect name resolutions. This would reroute traffic on the IPX Network to the attacker's network.			
Background information:	The most likely reason for an attacker to succeed in gaining control of a network element is given by insecure configuration and by running outdated versions of services which have vulnerabilities. Secure configuration and up-to-date network elements are crucial for IPX security.			

3.8 IPX Provider Peering

The entire worldwide IPX Network consists of interconnected IPX Providers who share their IPX Provider Networks. The following security requirements apply for this interconnection.

BSR 18	IPX Provider Peering		
Classification:	For IPX Providers:		For Service Providers:
IPX Providers shall not use the Internet (or any other public network) for peering. Dedicated public shared peering points and direct bilateral private peering are the only allowed options. Peering shall be done for the IPX Network only. No other network or traffic shall be mixed with the IPX Network. Physical or logical isolation is required. If in extraordinary cases other networks are used to reach other IPX Providers, the connection must be secured as defined in Section 3.5. As the IPX consists of several VLANs for different IPX Services – Service Communities – it shall be ensured that these VLANs are also kept segregated at all peering points. For details on Service Communities, see PRD IR.34 **Error! Reference source not found.**.			
Motivation:	This requirement contributes to isolation of the IPX from other networks. The isolation of networks, which is granted by all IPX Providers, needs to be performed at all peering points as well.		
Background information:	An IPX Provider may also have connections to additional networks. For example, an IPX Provider may also be an Internet Service Provider (ISP). The IPX Provider shall ensure that segregation of the IPX Network from any other network is performed on all network elements, including IPX peering.		

BSR 19	Equal Security Level for IPX Provider Peers		
Classification:	For IPX Providers:		For Service Providers:
IPX Providers shall verify that their peer IPX-Providers have the same level of security, demonstrated by documentation as required in Section 3.10.			
Motivation:	This requirement helps to ensure that a common set of standard practices is in place by all the participants on the IPX. If peer IPX Providers do not adhere to the security requirements of this PRD, security of the entire IPX is endangered. This would for instance allow rogue Service Providers to inject IP packets with spoofed source IP addresses into the IPX Network. Spoofed source IP addresses are often used to commit fraud.		
Background information:	NOTE: This text will be moved to either the accreditation process of IPX Providers or to the agreement template between IPX Providers. This will be an activity of the GSMA Working Group GRXIPX Once it is included there it will be removed from PRD IR.77. This requires a Change Request (CR) sometime in the future.		

BSR 20	Route Advertisement over Peering		
Classification:	For IPX Providers:		For Service Providers:
IPX Providers shall adhere to the following when advertising routes to peer IPX Providers: Only advertise valid networks to peering partners (see also PRD IR.34 **Error! Reference source not found.**, PRD IR.40 0, PRD IR.21 0, and PRD IR.85 0). Do not advertise default routes. Do not advertise private address prefixes. Do not advertise addresses which are not part of the IPX Network. Do not advertise multicast routes.			
Motivation:	These rules, together with other rules in this document, ensure that only valid IP traffic is transported through the IPX Network. Certain classes of attacks, where IP		

BSR 20	Route Advertisement over Peering
	packets are forged, or where IP packets are rerouted, are not possible if all these requirements are fulfilled.
Background information:	Only valid routes shall be advertised to peer IPX Providers and only if the corresponding networks are actually reachable through the network which advertises them.

3.9 Incident Response

Incident response helps in quickly getting the network back to normal operation once an attack or miss-configuration that caused the security breach is identified.

BSR 21	Incident Response		
Classification:	For IPX Providers:		For Service Providers:
IPX Providers and Service Providers shall put in place adequate procedures to respond to any security breach and to restore normal service within a reasonable time. Procedures are considered adequate in the context of this requirement, if they define at least the following: Personnel in charge of determining security breaches, investigating the security breaches, finding solutions to counter the breaches, and deploying these solutions; Personnel in charge of decision making for mitigating the security breach; Responsibilities for all the tasks necessary for mitigating a security breach Assign contact persons and publish their contact details internally at the IPX Provider and to client Service Providers; Time frames which are acceptable for the involved personnel to detect and mitigate the security breaches; Processes to follow once a security incident occurs; A service level agreement which describes how incident response is performed. Details shall be agreed bilaterally between IPX Providers and their client Service Providers. A Service Level Agreement (SLA) shall be signed between these parties as a legally binding contract for this purpose. Responsibilities shall be clearly defined therein, too. IPX Providers and Service Providers shall have expert staff and suitable equipment readily available and in operation to identify and counter security incidents. IPX Providers shall resolve incidents in a self-contained way for their client Service Providers, involving peer IPX Providers if necessary.			
Motivation:	Having incident response procedures in place helps cleaning up impacted network elements and getting them back to normal operation following a security breach.		
Background information:	NOTE: This text will be moved to either the accreditation process of IPX Providers or to the agreement template between IPX Providers. This will be an activity of GSMA GRXIPX. Once it is included there it will be removed from this document. This requires a Change Request (CR) sometime in the future.		

3.10 Security Documentation

The security documentation describes all the security measures and processes in place.

BSR 22	Security Documentation		
Classification:	For IPX Providers:		For Service Providers:
Each IPX Provider shall demonstrate that they have effective security measures, tools and processes in place. This covers all levels of security: physical security, technical security, network security, information security, personnel security, security processes, monitoring, tool chains, security processes, incident response processes, fraud prevention, and fraud detection.			

BSR 22	Security Documentation
To demonstrate that IPX Providers have security means/tools/processes in place, they shall provide evidence to their customer Service Providers. A bilateral agreement between IPX Providers and their customer Service Providers defines what they consider as evidence. There are two options: • The IPX Provider undertakes a security audit by a third party auditing organisation which issues a certificate that proves that the above is in place. The IPX Provider shall present the certificate to their client Service Providers. The client Service Provider shall accept the auditing organisation as a trusted auditor prior to undertaking the security audit. • The IPX Provider provides documents to their client Service Providers which describe in a complete and comprehensible way all the above mentioned security measures/tools/processes which are deployed and actively applied at the IPX Provider. Whichever option is chosen, information provided to Service Providers must be detailed enough to allow the Service Provider to judge the IPX Provider's security.	
Motivation:	Providing a security certificate to Service Providers helps Service Providers to establish trust in their IPX Providers. Since Service Providers transfer business critical data through the IPX, Service Providers require a reliable and trusted IPX.
Background information:	It is up to the bilateral agreement between an IPX Provider and their client Service Providers to what level of detail the security certificate shall prove compliance. NOTE: This text will be moved to either the accreditation process of IPX Providers or to the agreement template between IPX Providers. This will be an activity of GSMA GRXIPX, once it is included there it will be removed from this document. This requires a Change Request (CR) sometime in the future.

3.11 Signalling Security

Diameter is an application layer protocol that is being used for signalling between Service Providers. This subsection covers the security related to the Diameter protocol, specifically to reduces the attack surface by screening the realm of the sender Service Provider (Cat0) and the type of message sent (Cat1).

For better security handling of Diameter messages, they are categorised (Cat0, Cat1, …) as described in PRD FS.19 0.

BSR 23	Diameter Message Screening		
Classification:	For IPX Providers:		For Service Providers:
Each IPX Provider shall implement screening on incoming Diameter messages, received on the IPX Diameter Agent from the Service Provider's Diameter Edge Agent. Different filtering categories are defined in GSMA PRD FS.19 0. Two categories shall be implemented in the first Diameter Agent which has direct connection to the sender Service Provider: The IPX Provider shall screen the realm of the sender Service Provider (Low-Layer Format): the first Diameter Agent which has direct connection to the sender Service Provider is required to check that the realm contained in the Origin-Realm AVP in the request from the sender Service Provider corresponds to the right sender network (PRD FS.19 0 references 3GPP TS 29.272, section 7.1.2). If a message is received with an origin-realm that is not part of the whitelist (list containing sender Service Provider realm and optionally defined partners like MVNO, …), the request shall be rejected with a configurable error messate. Use of a common Diameter error is recommended for this (e.g. 5420, 5012 or 5005). The IPX Provider shall screen the message type of messages received from the sender Service Provider (Cat1): the first Diameter Agent which has direct connection to the sender Service Provider is required to check that the application-ID AVP in the request from the sender Service Provider corresponds to the offer provided to the sender network by the IPX Provider. If a message is received with an application-ID that is not part of the Cat1 whitelist (authorized application-ID: S6a/S6d, S6c, SGd, Rx, S9, S13, …), the request shall be rejected with a configurable error		

BSR 23	Diameter Message Screening
message. Use of a common Diameter error is recommended for this (e.g. 3002-UNABLE_TO_DELIVER).	
Motivation:	The main idea is to build a trusted IPX/Diameter domain, in which all IPX/Diameter providers should protect the Diameter signalling at the border of the IPX by checking the origin realm/application-ID for all incoming Diameter messages. This is a fundamental security improvement: IPX Providers will stop fraudulent traffic which could affect IPX DRA and/or Service Providers. This will reduce the attack surface and increase the difficulty of performing an attack
Background information:	Signalling vulnerabilities are an important topic for mobile network operators. There are significant issues related to privacy (location tracking), Denial of Service or fraud. These problems were first detected on SS7 signalling used for 2G/3G roaming and SMS interconnection, but are also arriving progressively on Diameter signalling used for 4G roaming. Providing Diameter security to Service Providers helps Service Providers to establish trust in their IPX Providers. Since Service Providers transfer business critical data through the IPX, Service Providers require a reliable and trusted IPX.

4 Non-binding Security Requirements

In contrast to the previous sections, the security requirements which are listed in this section are non-binding. However, IPX Providers and Service Providers are advised to fulfil these requirements whenever possible. The requirements in this section are more detailed than the others. As a consequence, there may be networks where some of these requirements are not applicable. These non-binding requirements are by no means less important for overall IPX security than the binding requirements. Should the network architecture and the overall environment of the network allow for fulfilling these non-binding requirements, they are meant to be fulfilled.

4.1 4.1Secure Configuration of Network Elements

Default configurations of network elements are often insecure. In addition to BSR 17, the following security requirements should be applied.

NSR 01	**Secure Configuration of Network Elements**		
Classification:	**For IPX Providers:**		**For Service Providers:**
The following configuration should be applied to all network elements on the IPX Network and on Service Provider Networks: Change all default passwords and assign strong individual passwords. No network element should keep its default password for any user account when being deployed. For all user accounts strong passwords (including special characters) should be used which are only known to a small number of people within the organisation who owns/operates the network element. Encrypt and authenticate all management traffic. Only encrypted protocols should be used for managing network elements. All management traffic should be authenticated. Authenticity of the origin should be validated mutually each time a management session is initiated. Insecure protocols (such as FTP, HTTP, LDAP, Telnet) should not be used. Secure protocols (such as SFTP, FTPS, HTTPS, LDAPS, SSH, IPsec) should be used instead. If SNMP is used, only SNMPv3 or above should be used. If the network element has a Web interface, disable unused HTTP commands. If HTTP servers are used on network elements, unused commands (such as OPTIONS, HEAD) should be disabled. Enable authentication, validation and confidentiality protection for vendor-specific network protocols. Some network elements communicate through vendor-specific network protocols. These are needed for operation or maintenance. If such protocols are used, it should be ensured that network elements authenticate each other, that input transported by these protocols is validated and that traffic is encrypted. This refers to management traffic only.			
Motivation:	As management systems and protocols are used to fully control network elements, it is business critical to ensure that attackers cannot gain access to management systems and management traffic.		
Background information:	In addition to these requirements for network elements, the management network should be designed securely and it should be strictly separated from other internal networks.		

4.2 Continuous Availability and Robustness

IPX Providers should design and implement their backbone in a way that traffic peaks, unexpected contents of IP packets, floods of IP packets and any other possibly disruptive events (e.g. power outage, fire in the data centre) do not lead to disruption of availability. Service Providers should do the same on the network edge of their Service Provider Networks to the IPX Network.

NSR 02	Continuous Availability and Robustness		
Classification:	For IPX Providers:		For Service Providers:

The following should be deployed on the IPX Network and on Service Provider Networks: Network elements should be deployed to ensure adequate redundancy. Backup network elements should be deployed which can take over the tasks of the primary network element if the primary network element fails. A comprehensive redundancy concept should be developed and deployed. • Network elements should be protected against overload situations which are caused by a flood of IP packets in a short timeframe. Network elements should always be in a stable state regardless of the traffic they receive. • IPX Providers should deploy carrier grade network elements on the IPX Provider Network if they decide to go for logical separation of the IPX Network from other networks. In such a setting, IPX Providers should configure network elements to ensure that overload situations (e.g. Denial of Service attacks) on some logical link will not have an impact on stability and throughput of the IPX Network.

Motivation:	Attacks, such as Denial-of-Service (DoS) and unexpected faults should not lead to unavailability of network elements on the IPX Network.
Background information:	Physical separation of the IPX Network from other networks is preferred over logical separation, as in physically separated networks other networks cannot influence the IPX Network. However it is up to the IPX Provider to decide whether separation is performed physically or logically.

NSR 03	Robust Dynamic Routing on the IPX Network		
Classification:	For IPX Providers:		For Service Providers:

IPX Providers should disconnect their client Service Providers if these Service Providers suddenly send numerous Route Advertisements in a short timeframe or for a long period.

Motivation:	Robustness of routing on the IPX Network is important for making sure that Service Providers can reach each other via the IPX Network at any time. Changes in routing information are rare. A large number of Route Advertisements indicates faulty or malicious behaviour. To save the IPX Network from negative impact, the Service Provider who causes this behaviour should be disconnected until normal behaviour reoccurs.
Background information:	Reasonable thresholds for configuring automated disconnect should be determined by tests. IPX Providers should inform their customer Service Providers about the configured values.

4.3 IPX Provider Peering

In addition to the requirements from Section 3.8, IPX providers should adhere to the following security requirements.

NSR 04	Agree to Code of Conduct		
Classification:	For IPX Providers:		For Service Providers:

IPX Providers are advised to mutually agree to adhere to the security code of conduct as attached to this PRD in Annex A.

Motivation:	By agreeing to the code of conduct, IPX Providers agree to adhere to a certain level of security. This agreement is important for a worldwide high security level throughout the IPX. For Service Providers this is a prerequisite for performing business critical data exchange on the IPX Network.
Background information:	A diverse level of security throughout the various IPX Provider Networks would lead to weaknesses that could be exploited by attackers or fraudsters. The Code

NSR 04	Agree to Code of Conduct
	of Conduct should define a minimum level of security. All IPX Providers are encouraged to adhere to it.

NSR 05	Peering Router Security		
Classification:	For IPX Providers:		For Service Providers:
The following settings should be applied to all Peering Routers which interconnect an IPX-Provider to a peer IPX-Provider: Disable Proxy ARP. Disable IP directed broadcasts. Disable multicast. Disable Spanning tree Bridge Protocol Data Units (SBPDU). Use exactly one globally unique Media Access Control (MAC) address per network interface. Disable all discovery protocols (e.g. CDP, IRDP). Do not perform any Internet Control Message Protocol (ICMP) redirects. Do not advertise peering location IP prefixes to peers.			
Motivation:	Any traffic that is useless on the peer network should be dropped at the network edge of each IPX Provider. Certain classes of attacks, where IP packets are forged or where IP packets are injected, are not possible if all these requirements are fulfilled.		
Background information:	It is the easiest to determine useless traffic at the network edge. As a consequence IPX Providers should sanitise incoming IP packets prior to routing them.		

NSR 06	Route Advertisement over Peering		
Classification:	For IPX Providers:		For Service Providers:
IPX Providers should adhere to the following when advertising routes to peer IPX Providers: Do not advertise routes of another IPX Provider to a third IPX Provider.			
Motivation:	If IPX Providers do not re-advertise routes of other IPX Providers, they cannot modify these routes. Certain classes of attacks, where IP packets are forged, or where IP packets are rerouted, are not possible.		
Background information:	The “no more than two hops” rule applies on the IPX. This rule says that each Service Provider shall traverse at most two IPX Provider Networks to reach a peer Service Provider with its IP traffic (see PRD IR.34 **Error! Reference source not found.**). In all cases where the IPX sticks to this rule, there is no need to re-advertise routes of another IPX Provider to a third IPX Provider. Some IPX Providers report that the “no more than two hops” rule is not yet fully applied on the IPX globally. For security reasons, all IPX Providers are encouraged to fulfil this rule as soon as they can.		

4.4 Routing

NSR 07	Filtering of Routing Advertisements		
Classification:	For IPX Providers:		For Service Providers:
It is good security practice to only accept route advertisements in the IP Edge Router at the Service Provider’s network edge, for peer Service Providers with which a roaming agreement exists. Technically, this can be done by configuring BGP route import filters which only accept IP route prefixes which match the originating AS number(s) that the partner Service Providers have declared in the PRD IR.21 0 RAEX database and in the PRD IR.85 0 roaming hub database.			

NSR 07	Filtering of Routing Advertisements
Implementing ASN filtering must be done very carefully in order to avoid impacting IPX service availability. There is currently no mature automated way of updating BGP AS filters on Service Providers' Edge routers when other Service Providers' AS Numbers change. If a Service Provider chooses to implement BGP ASN filtering of other Service Providers' IP address range advertisements, the Service Provider **shall** commit to update their BGP ASN filters (BGP import policy configuration) within the IR.21 SLA time period in order to avoid IPX service failures to the other Service Providers when they change their AS numbers used on the IPX.	
Motivation:	By implementing this, the Service Provider controls that IP reachability is limited to peers which have a contractual relationship. This also indirectly contributes to the overall security of the IPX by adding an extra degree of security at the Service Provider's edge.
Background information:	Note that this is a secondary security mechanism for Service Providers which does not have any service awareness. The primary mechanisms of securing the Service Provider's Network and prevention of connectivity subject to commercial agreements comes from a combination of Application Layer Enforcement Point filtering (e.g. GTP-aware firewalls, DEAs, STPs, IBCF, TrGw, etc.) implemented by Service Providers (BSR 01, BSR 02, IR.88), good isolation & segregation of IPX related network & services (BSR 04 through BSR 09), and IPX Providers only accepting legitimate IP route advertisements from their customer Service Providers (BSR 10).

Annex A Security Code of Conduct

This security statement defines the requirements to be satisfied by the Parties to the Agreement as they connect to the IPX Point of Interconnection. The ratification of these security requirements is mandatory for the Parties to this Agreement.

In the context of this agreement, the legal entities that sign this agreement are either called “Parties”, or “IPX Providers”. One legal entity out of the group of these legal entities is either called “Party” or “IPX Provider”.

A.1 General Security Requirements

The Parties will only interconnect via an IPX Point of Interconnection that is isolated from public Internet connections.

The Parties are responsible for screening the traffic towards their IPX Point of Interconnection device.

A.2 Security Requirements

A.2.1 IPX Security Measures

The following requirements relate to internal measures implemented within each specific IPX Provider Network.

All binding requirements of the GSMA Permanent Reference Document (PRD) IR.77 are mandatory and must be fulfilled by the IPX Providers.

IPX Providers agree to additionally fulfil the non-binding requirements of IR.77. Exceptions are defined in Section A.3.2.

The version of IR.77 which was the latest officially approved and published version by the GSMA at the time of signing this agreement applies. The applicable version of IR.77 shall not be older than version 3.0.

Whenever the GSMA issues an update to IR.77 and approves it formally, the new version is effective for all IPX providers. In the context of this agreement, the IPX Providers decide together and agree how and when they will apply all the changes from the new version of IR.77 to their networks. This agreement shall be made not later than three months after the GSMA has approved and published the new version of IR.77. Depending on the complexity of the changes to IR.77 the IPX providers have time for fulfilling the new IR.77 requirements as follows:

- In general, one year after approval and publication of a new version of IR.77, the IPX Providers concerned by this agreement shall have implemented all the changes from the new version of IR.77.
- In cases where the IPX Providers depend on availability of products by third party vendors, the above mentioned time frame is extended to two years.

A.2.2 Connectivity Configuration Requirements

Connection: Connection to the Point of Interconnection secured location shall be made using leased line, Frame relay, MPLS VRF, Layer 2 VLAN or ATM. No public Internet connection shall be used at the Point of Interconnection

Physical Connectivity: Parties will only connect equipment to the Point of Interconnection shared infrastructure that they control and operate on their own. Parties will not connect any other equipment on behalf of third parties to the shared infrastructure.

Infrastructure: A shared infrastructure is used to connect each peering partner's (i.e. each Party's) equipment. In the long term, peering partners will have a choice between using a common shared LAN infrastructure administered by a recognised Third Party or direct links between their respective equipment.

Connection Permissions: Parties do not touch equipment and/or cabling owned by other members of the Point of Interconnection without the explicit permission of the member owning that equipment.

Monitoring: Parties do not install "sniffers" to monitor traffic passing through the Point of Interconnection, except through their own ports.

Allowed Connectivity: Parties do not directly connect any other third parties who are not peering members via circuits to their equipment hosted at the Point of Interconnection.

A.2.3 Network Configuration:

Protocols: Parties shall, on all interfaces connected to the shared Point of Interconnection, disable: ICMP redirects, CDP, IRDP, Directed broadcasts, IEEE802 Spanning Tree, Interior routing protocol broadcasts, and all other MAC layer broadcasts except ARP.

Default Route: No "route of last resort" shall be configured towards any other IPX Provider Network. That is, Parties will not advertise routes with a next-hop other than that of their own routers without the prior written permission of the advertised member and the advertisee member.

Routing: Parties shall not generate unnecessary route flapping, or advertise unnecessarily specific routes in peering sessions with other Members across the shared infrastructure. Each member shall ratify common "route flap dampening" measures defined separately in the technical and operational guidelines.

Route Advertisements: Parties will not forward traffic across the shared infrastructure unless either the traffic follows a route advertised by a valid member of the IPX Network or where prior written permission of the member to whom the traffic is forwarded has been given. IP packets to the root DNS or interim IPX DNS must be allowed. Networks will be summarized for each IPX Provider Network.

IP-Traffic through the peering point is allowed if and only if Parties follow the GSMA common rules that are documented in the PRD IR.34 **Error! Reference source not found.** and PRD NG.137 [26], issued by the GSMA.

A.2.4 Transit Traffic

Transit Traffic is a matter of bilateral agreement and is not mandated or handled in this document.

A.3 Voluntary Bilateral Agreements

This section may be agreed between the Parties and the following topics can be handled on a bilateral basis, if required.

A.3.1 Authentication and Encryption:

More precise protocol requirements may be defined if deemed appropriate.

Transit traffic allowances may be set if desired.

MD5/SHA1 password uses: purpose and password requirements may be defined here. The password itself is agreed outside this agreement and transferred via a secure communication channel between the Parties.

A.3.2 Exceptions to Fulfilment of Non-Binding Security Requirements

Section A.2.1 defines which security measures must be adhered to by all the involved Parties concerned by this agreement. This section defines which of the non-binding security requirements of IR.77 will not be fulfilled by one or more of the Parties. A reason must be given for all non-binding requirements which are not fulfilled. None of the binding security requirements can be dismissed.

#	Requirement heading	Details of the requirement which are not fulfilled	Reason for not fulfilling the requirement
NSR			
Party/Parties who do/does not fulfil this requirement			

A.3.3 Other Requirements Agreed between the Parties

A.3.4 Other Agreements

A.4 Signatures

This section lists all names, full addresses and signatures of all the Parties that arrange for this agreement.

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	15 Oct 2007	Version approved at IREG #53 adapted from SG17 produced by Security Working Group and contributes from GRX WP		
2.0	14 Nov 2008	Document approved at EMC		
2.1	3 Dec 2009	Minor CR001, bringing LTE related topics to document Adding also new GSMA cover sheet and new PRD format	GRX WP	Jari Weckman/ TeliaSonera Finland
3.0	3 Dec 2014	CR1001 This is to reflect the changes in the demand of security for the IPX since the last update of this document. In the approval process, the document shall become binding.	PSMC	Rosalia d'Alessandro, Telecom Italia, Italy
4.0	5 Nov 2015	CR 1003, This CR clarifies the wording used in BSR11 as well as separate the BGP ASN filtering mentioned in the background section of BSR11 into a new Non-binding security requirement.	NG	Rosalia d'Alessandro, Telecom Italia, Italy
5.0	29 Occt 2019	CR 1004, New binding requirement BSR 023 on Diameter security has been added.	NG	Sven Lachmund, Deutsche Telekom
5.1	April 2025	CR1005 AA.51 to NG.137	ISIG-NG	Sven Lachmund, Deutsche Telekom

B.1.1 Other Information

Type	Description
Document Owner	NG
Editor / Company	Sven Lachmund, Deutsche Telekom

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.