Inter-Operator IP Backbone Security Requirements

For Service Providers and Inter-operator IP backbone Providers

2.0

15 October 2007

This is a non-binding permanent reference document of the GSM Association.

Security Classification Category (see next page)	
Unrestricted	X

Security Classification - UNRESTRICTED

Copyright Notice

Document History

Version	Date	Brief Description
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
Changes Since Last Version		

Other Information

Type	Description
Document Owner	GSMA IREG Packet
Revision Control	As Required
Document editor/company	Jari Weckman, TeliaSonera Finland

Feedback

This document is intended for use by the members of GSMA. 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 mailto:prd@gsm.org. Your comments or suggestions are always welcome.

1 GLOSSARY

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. [ref]
BG	Border Gateway, router with optional firewall functions (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 [ref]. The current version of BGP is BGP-4
DNS	Domain Name System. For additional information, refer to IR.67 [ref].
DoS	Denial of Service attack
DDoS	Distributed Denial of Service Attack
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 Provider	A Provider that offers GRX service only
GTP	GPRS Tunneling Protocol[ref]
HTTP	Hypertext transfer protocol
HTTPS	Secure Hypertext transfer protocol
IMS	IP Multimedia Subsystem (specified by 3GPP)
Inter-Service Provider IP Backbone	The collection of interconnected GRX and IPX Providers' networks
IP Backbone Provider	A business entity that provides Inter-Service Provider IP Backbone Service. Either a GRX or an IPX/GRX Provider
IPX	IP Packet eXchange. The entity providing the IPX functions. At the interconnection level, IPX is used to mean an interconnection at a service level. Also refers to the collection of all interconnected IPX Provider's networks
IPX Provider	A Provider that offers IPX services and may also offer GRX services
PDN	Packet Data Network, typical Packet Data Networks are Internet, GRX/IPX, corporate networks

Service Provider	Mobile, fixed operator or other type of Operator connecting to Inter-Service Provider IP Backbone for roaming and/or interworking purposes
SIP	Session Initiation Protocol (defined by IETF)
SNMP	Simple network management Protocol
SSH	Secure Shell
Tacacs	Terminal Access Controller Access Control System
UMTS	Universal Mobile Telecommunications System, i.e. “3G”
VPN	Virtual Private Network; Can be done either at OSI layer 2 or 3. MPLS path, tunnel, VRF or ATM Circuit and IPSec tunnels are typically used to build VPN’s

2 INTRODUCTION

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 PRD IR.34 [ref] describes a set of common guidelines of an Inter Service Provider IP Backbone to achieve an adequate security level.

PRD IR.34 gives an overall description of the Inter-Operator IP backbone environment. This document concentrates providing the detailed security requirements for Inter-Operator backbone Providers and Service Providers connecting to the Inter-Operator IP Backbone. These requirements are necessary for both security and to provide a quality service together with interworking, under all conditions.

2.1 End-to-End security

An overriding need for ”end to end security” of operator services is acknowledged, but the security chain includes a number of distinct security elements that can be summarised as follows. The security of:

- Subscriber profile data and user terminals
- Radio infrastructure elements and communication
- Service Provider networks, including gateways to external PDNs or other IP networks such as the Internet.
- Inter-Operator IP Backbone network
- Various different Inter-Operator IP Backbones
- Service Provider backbone networks
- Service Provider and Inter-Operator IP Backbone connection

2.2 In Scope

The document gives guidelines to Service Providers to enable enhancement of their own network security.

This document concentrates on IP layer security in Inter-Service Provider IP Backbone networks and associated peering points. Security issues at the Service Provider level are covered if those are provided via a direct link to achieve the aims of a secure and quality orientated, interworking network between Service Providers.

This paper therefore focuses on the following key topics:

- Internal security of Inter-Operator IP Backbone network
- Security between the various Inter-Operator IP Backbones
- Security in Service Provider backbone networks when it is related to Inter-Operator IP backbone
- Security between an Service Provider and the Inter-Operator IP Backbone
- Proposed tasks for Service Providers and Inter-Operator IP Backbone providers to ensure continuous security in an Inter-Operator IP backbone environment
- Security of data encryption (IPSEC) if it is needed for network level security.
- Tunnels, when those are needed to hide network from end-users

2.3 Out of Scope

User Terminal security and radio link network security are not in scope of the present document.

2.4 General Security Principles

Ensuring adequate security levels are in place is not just a matter of deploying the right technology in the right place. It is critical 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 in a network, it requires that every single Service Provider is fulfilling their part of the requirements..

It has been observed that end-user traffic causes the most problems and so it has been agreed that all end user traffic shall not be transmitted without secure tunnels through an inter-operator IP backbone. It has been agreed that GTP tunnel protocol [ref] is used in GPRS and UMTS roaming traffic (as defined in 3GPP TS 29.060 [ref]), GRE tunnels (as defined in IETF RFC 2784 [ref]) shall be used for all user to user traffic in SIP/IMS based connections. See chapter 3.4. for more information about tunnelling.

The security measures shall provide the minimum security features listed in the following sections 2.4.1 to 2.4.4.

2.4.1 Continuous Availability and Operability

Inter-Operator IP Backbone node elements shall be able to continue to provide services under all conditions. Such measures will prevent DoS attacks (Denial of Service), DDoS (Distributed DoS).

2.4.2 Data Integrity

The Inter-Operator IP Backbone infrastructure together with it's security features shall ensure that the any data transiting cannot be tampered with or altered in any way, through interception (man in the middle) (Replay) attacks. In addition, appropriate mechanisms to prevent IP source address spoofing should be deployed

2.4.3 Confidentiality

Information shall be protected from unauthorised interception and disclosure. Close control over data distribution and the isolation of the distribution infrastructure is the first step to guarantee confidentiality.

Encryption of traffic is not seen as necessarry in an Inter-Operator network, the network itself is secure and transparent for end-users. Encryption is needed in the case that a local loop, or some other part of network is built over the internet or other IP network infrastucture. An end-user and/or Service Provider may choose to encrypt their traffic, and in that case the Inter-Operator IP backbone carries that encrypted traffic (but obviously does not take part in encryption/decryption at all).

2.4.4 Fraud Management

Procedures to respond to any security breach and to restore normal service within a reasonable time should be in place in the Inter-Operator IP Backbone infrastructure.

Security can be assured through the use of a variety of security administration measures that cover physical security, logical security and personnel security. Security guidelines should be described and demonstrated to peering partners and customers.

3 INTER-OPERATOR IP BACKBONE SECURITY RULES

This section describes what security measures shall be implemented within each part of a single Inter-Operator IP Backbone to sustain an adequate level of security between connected Service Providers. All Inter-Operator IP Backbone providers shall demonstrate that they have adequate security measures in place at their location(s) of operation by providing a copy of their company fraud and security policy. Where third parties are used to fulfil any security arrangements a copy of any contracts with those third parties shall be provided.

.

3.1 Route and Packet Filtering

Anti route spoofing and anti packet spoofing measures must be implemented within the Inter-Operator IP Backbone. It is the Inter-Operator IP backbone Provider's responsibility to check that their customer is advertising only valid IP-networks. Inter-Operator IP backbone providers shall ensure that only traffic from valid IP addresses is transmitted to the network.

The use of firewalls at the peering point is not common practice. In the ISP Internet world this may not be required if all peering partners enforce the same level of anti-spoofing measures.

Anti-Route Spoofing

Inbound route filtering shall be implemented at the Inter-Operator IP Backbone edge. This prevents erroneous or malicious route advertisements from arising that could impact traffic flowing through the Inter-Operator IP Backbone. Only routes within declared subnet ranges will be accepted from Service Providers.

Anti-Packet Spoofing

Inbound packet filtering shall be implemented to screen ingress traffic based on source IP address. This is equivalent to having a basic stateless firewalling function implemented on the network access device so that only packets with declared and checked source addresses can be forwarded within the community. This ensures that the origin of the IP packet transiting over the Inter-Operator IP Backbone is from the Inter-Operator IP Backbone link of the Service Provider identified as owning the corresponding originating node/address.

3.2 Inter-Operator IP Backbone VPN Isolation

The Inter-Operator IP Backbone infrastructure shall be logically isolated from other network VPNs and the public Internet, either implemented on the same-shared infrastructure or reachable via dedicated gateway(s).

It is critical that members of separate VPNs built on shared infrastructure, or members of separate networks with interconnection gateways to the shared infrastructure supporting the Inter-Operator IP Backbone, shall not be able to eavesdrop and gain access to either IP packets or routing information.

VPN isolation can be provided through various architectures and implementations involving all three OSI layers 1, 2 and 3. Layer 1 solutions imply the use of dedicated physical lines for the Inter-Operator IP Backbone infrastructure, which is not cost effective. Other solutions use Layer 2 dedicated circuits over shared physical infrastructures (such as dedicated Frame Relay DLCIs or ATM PVCs), or using Layer 3 IP technologies such as MPLS VPN (e.g. using RFC 2547 [ref] VPNs).

3.3 Public Internet Isolation

Most hackers initiate attacks towards private networks via badly secured Internet connections or gateways, special care should be taken to ensure that the Inter-Operator IP Backbone provider’s core infrastructure provides adequate protection against intruders coming from the public Internet. Anti-hacking provisions should consider internal and external risks and shall include detection, reporting and protection processes. Particular attention shall be paid to the configuration of firewalls, routers, routing protocols, remote access controls and procedures.

Inter-Operator IP Backbone and Service Provider networks will not be advertised to the public Internet. Inter-Operator IP Backbone networks can be part of larger supernet advertised to the Internet but the specific routes that belong to the Inter-Operator IP Backbone or Service Provider core networks shall not be known inside the ISPs' and the non-GPRS/UMTS customers' networks. Inter-Operator IP Backbone and Service Provider networks shall not be accessible from the Internet. This means that all connections from the Internet are denied, be they desired or otherwise.

Secured and monitored Internet Gateways should be used and, ideally, separate infrastructure should be used to carry Inter-Operator IP Backbone traffic. Detection systems should be used to identify unauthorised network access attempts and the system should provide the Inter-Operator IP Backbone provider with activity reporting and alarms. Procedures should be in place to resolve alarms and these should include escalation procedures for events that cannot be readily resolved. The system should produce full audit logs for any event, tracing and resolution.

3.3.1 Local Tail over Internet

If an Service Provider and Inter-Operator IP Backbone provider together chooses to use an Inter-Operator IP Backbone solution using the public Internet to connect the Service Provider to the Inter-Operator IP Backbone infrastructure, then IPsec or an equivalent data encryption solution shall be used. Inter-Operator Backbone shall ensure that Service Provider or Inter-Operator backbone networks shall not be advertised to internet.

3.4 Tunnels

One of the main principles of Inter-Operator IP Backbone network is that the network is transparent (invisible) for end-users. This way the network itself is safe from end-user attacks. All end-to-end traffic will be encapsulated within tunnels when traffic is flowing through the network. Service Providers are responsible to separate their end user traffic to tunnels, and Inter-Operator IP Backbone providers shall ensure that end-user IP’s are not advertised in the backbone. Server to server (For example CSCF to CSCF SIP control) traffic can be transmitted without tunnels through Inter-Operator IP Backbone
It is agreed that all Data-roaming traffic is using GTP tunnels between GGSN and SGSN nodes, IMS/SIP based end user to end user traffic shall be encapsulated to GRE tunnels between Service Provider network and IPX proxies as well between IPX proxies. It is an Service Provider decision as to where that tunnel starts in a Service Provider network. The following diagram given overview of tunnel concepts

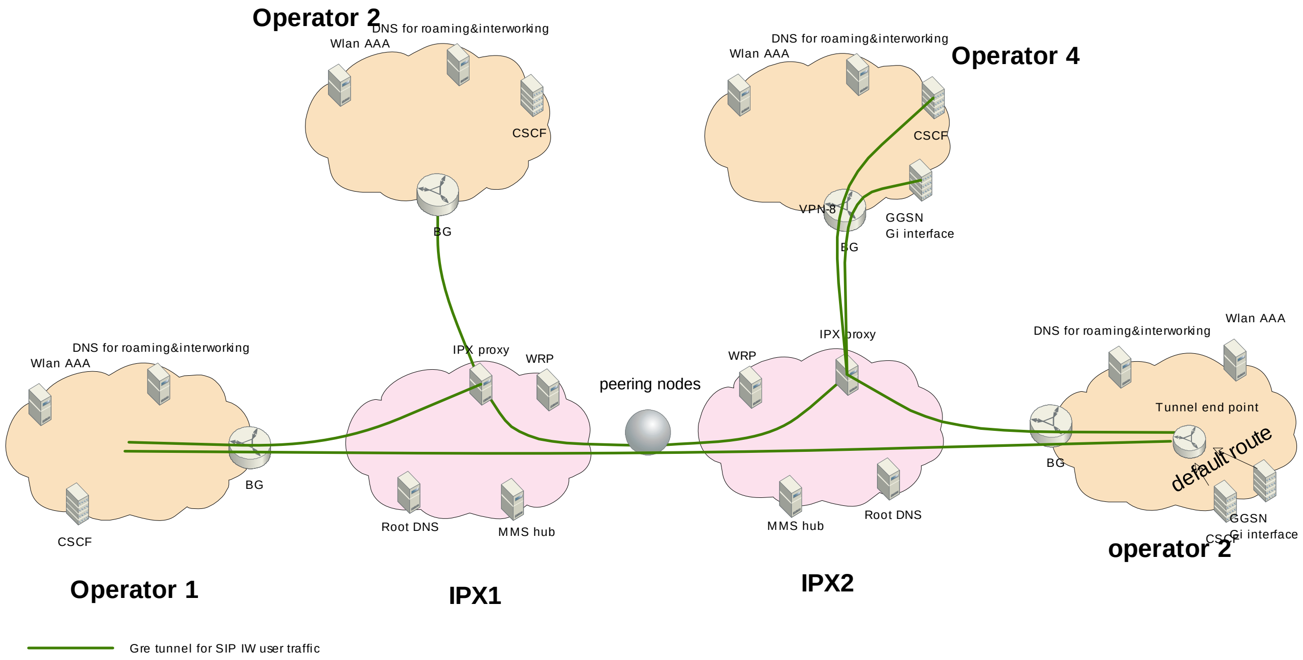

Figure 1 : Tunnels

3.5 Device access control

It is essential that both Inter-Service IP Backbone Providers and Service Providers implement tight access control to network equipment. All unnecessary protocols shall not be supported and strong passwords to equipment services shall be provided and changed regularly. For management purposes it is preferred that Inter-Service IP Backbone Providers and Service Providers have a separate out of band management network, and it’s information is not advertised outside of Inter Service IP Backbone Provider or Service Provider Network. Connection to network equipment shall be allowed only from the management network and defined IP addresses.

It is preferred that, local access to equipment located within the Service Providers’ premises is disabled and temporarily enabled only when local on-site intervention is required. Those access devices not located within the Inter-Operator IP Backbone provider’s own secured premises are considered potential attack targets, and should be kept completely isolated to minimise the risk. This covers both management and read access.

3.5.1 Protocol Restrictions

It is desired that whenever possible telnet access to equipments is denied and SSH or similar encrypted, protocols are used. If telnet has to be used then TACACS and similar kind of user authentication methods should be used to provide more security to equipment access.

If SNMP is used to get information from equipment it is preferred to use as a minimum SNMP v3 [ref] SNMP connections shall be limited to only the management section of that network. Also SNMP write access rights should be limited to the required services in equipment.

Certain equipment offers support for HTTP, this should only be allowed if HTTPS protocol is used, and if a set of services, where contact via HTTPS, can be limited in the equipment.

All other services except for those specified above should be disabled.

There is also plenty of vendor specific protocols or systems which can be used to manage equipment, and as such special care should be used when implementing these to either Inter Service IP Backbone Provider or Service Provider Network

4 PEERING SECURITY RULES

The Public Internet shall not be used to interconnect Inter-Operator IP Backbones through peering. At designated peering points, Inter-Operator IP Backbone equipment shall be used only for Inter-Operator IP Backbone purposes.

Special care should be paid to the Inter-Operator IP Backbone provider peering partners to ensure that the same level of security is enforced by each other. A lax Inter-Operator IP Backbone peering partner may compromise the entire roaming community.

Therefore, it is proposed that security code of conduct (Annex A of this document) be part of any bi-lateral peering agreement between the Inter-Operator IP Backbone providers. This allows any peering partner to request evidence of security measures, and their implementation, from any other peering partner at any given time and this helps ensure that a common set of standard practices is in place.

4.1 Peering types

Inter Service IP Backbone Providers may arrange peering with multiple different solutions:

- Private peering - which may be arranged in an agreed location or a leased line solution between Inter Service IP Backbone providers premises
- Public peering, own infrastructure – where peering provider arranges equipment only for this service
- Public peering, shared infrastructure – where peering provider offers VLAN type of service for Inter Service IP Backbone Providers use

No matter which peering model has been chosen all peering security rules needs to be fulfilled

4.2 Peering environment security

Inter Service IP Backbone Providers shall implement following list of settings to its peering router:

- Proxy AAP Shall be disabled
- ICMP redirects are not allowed
- IP directed broadcasts are not allowed
- Spanning tree BPDUs are switched of
- Duplex and speed settings of port are not in auto negotiation (except GigabitEthernet interfaces)
- Only one globally unique MAC address is used per interface

- Discovery protocols (such as CDP and IRDP) are switched off
- Multicast is switched off
- Peering location IP prefixes shall not be advertised to peers

4.3 Route advertisement over peering

It is essential that the Inter Service IP Backbone provider advertises only valid networks to its peering partner. More precise information of valid IP's can be found from PRD IR.40 [ref] and PRD IR.34 [ref] documents Default route, loopback and private IP address prefixes are explicitly denied advertisement.

Inter Service IP Backbone Providers are not allowed to advertise routes from one Inter Service IP Backbone Provider to another Inter Service IP Backbone Provider. IP addresses used in the peering environment are not allowed to be advertised outside of their own network, in any peering place or any peering connection.

It is expected that Inter Service IP Backbone Providers shall implement proprietary route flapping rules towards themselves to ensure stability of peering connection and whole network infrastructure.

Multicast routes shall not be advertised to peering partners and multicast functionality should be disabled from network.

5 SECURITY RULES FOR SERVICE PROVIDER CONNECTING TO INTER-OPERATOR BACKBONE

5.1.1 Network Access

Inter-Operator IP Backbone and connected Service Provider networks shall not be accessible from the Internet. This means that all connections from the Internet are denied, be they desired or otherwise.

5.2 Tunnels

One of the main principles of Inter-Operator IP Backbone network is that network is transparent (invisible) for end-users. This way the network itself is safe from end-user attacks. Basically all end-to-end traffic will be encapsulated within tunnels when traffic is flowing through network. Service Providers are responsible for separating their end user traffic tunnels. Figure 1 in this document gives an overview.

5.2.1 Explicit Traffic Filtering

In addition to standard anti-spoofing measures, which should be implemented as a matter of course, further optional traffic filtering can be implemented within the customer access router or within the Service Provider's border gateway. Traffic should be limited both inbound and outbound to only required protocols.

5.2.2 Protection of Customer’s Network

The responsibility for protecting the LAN infrastructure behind the Inter-Operator IP Backbone provider’s access router located on the Service Providers’ premises, (and thus the entire private network located behind it), remains with the Service Provider.

The Inter-Operator IP Backbone provider can only ensure that no security breaches occur on the provider network and that all traffic carried within the Inter-Operator IP Backbone comes from a valid declared source that belongs to a connected customer and is part of the Inter-Operator IP Backbone community. However, it is up to each individual customer to protect themselves against attacks coming from “community insiders”, i.e. The end-users of this community. Service Providers shall note also that Inter-Operator IP backbone does not always restrict protocols (unless specifically requested to do so in contractual agreement), so Service Providers need to have proper controls in place to filter valid and invalid traffic from roaming/interworking partner Service Providers.

A security conscious Service Provider shall put adequate security tools and procedures in place to prevent, monitor, log and correct any potential internal security breaches at all levels. The Inter-Operator IP Backbone network used is one element of a complete security policy. Typically, the BG needs to be able to implement ACL (access control lists) or similar mechanisms to prevent certain types of traffic, if not already implemented on the Inter-Operator IP Backbone provider access router. The BG should also be able to filter out unnecessary traffic coming from the Inter-Operator IP Backbone, such as HTTP, which should not be coming from an Inter-Operator IP Backbone. If the BG is used as a shared BG and not just a dedicated BG for connecting to the Inter-Operator IP Backbone, it should be able to filter out traffic per port/interface (i.e. implement ACL at the interface/sub-interface level).

5.3 IP addressing and routing

End user IP addresses are not permitted to be advertised in the GRX/IPX routing domain. Network element (such as GGSN’s, Tunnel end points, CSCF’s) shall be advertised in GRX/IPX routing domains. IP addressing shall follow the rules described in IR.34 and IR.40 documents

6 ENCRYPTION AND IPSEC

As the whole infrastructure (Inter-Operator IP Backbone and Service Provider networks) is planned in a secure way as described in this document, it is not necessary to encrypt every data stream and network segment. If Service Providers bilaterally decide to encrypt their traffic, Inter-Operator IP Backbone Providers shall carry that traffic too. Note end users can decide to use encryption for their traffic, and that traffic shall also be carried normally in tunnels through network.

The only segment where Inter Service IP Backbone provider shall encrypt traffic as a matter of course is when they choose to use the internet or another public IP network for providing connectivity to Service Providers. The minimum encryption in these cases is 3DES IPSec protocol. These legs need to fulfil all security demands described in this document as well as those in IR.34 [ref] or AA.80 [ref].

7 CONCLUSION AND RECOMMENDATION

It is strongly recommended that Annex A of this document should be approved as a security appendix to all Inter-Operator IP Backbone peering agreements.

REFERENCES

[1] PRD IR.34 Inter-PLMN IP Backbone Guidelines

[2] 3GPP TS 23.060: " General Packet Radio Service (GPRS); Service Description; Stage 2"

[3] IETF RFC 4271: "A Border Gateway Protocol 4 (BGP-4)"

[4] 3GPP TS 29.060: " General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface"

[5] GSMA PRD IR.67: "DNS Guidelines for Operators"

[6] GSMA PRD IR.65 “IMS Roaming & Interworking Guidelines”

[7] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2”

[8] GSMA PRD AA.80 “General Terms & Conditions For Agreement for IP Packet eXchange (IPX) Services”

[9] GSMA PRD IR.40 “Guidelinesfor IPv4Addressing and AS numbering for GPRS Network Infrastucture and Mobile Terminals”

GPA *Security code of conduct*

Harold Syfrig *Security code of conduct November 2001*

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 Inter-Operator IP Backbone Point of Interconnection. The ratification of these security requirements is a mandatory for the Parties to this Agreement.

GENERAL SECURITY REQUIREMENTS

The Parties will only interconnect via an Inter-Operator IP Backbone PX Network environment that is isolated from public Internet connections.

The Parties are responsible for screening the traffic towards their Inter-Operator IP Backbone Point of Interconnection device.

MANDATORY SECURITY REQUIREMENTS

Intra-Inter-Operator IP Backbone Security Measures

The following requirements relate to internal measures implemented within each specific Inter-Operator IP Backbone.

1. ***Network Devices Access Control.*** Only necessary services shall be enabled on network equipment. All the enabled services shall be restricted to a small set of management stations located in protected and secured areas. To prevent access to the devices by unauthorised visitors with malicious intent , local management access to network devices shall be prevented by ensuring physical security via locked access unless access is temporarily enabled by suitably authorised personnel.
2. ***IP Address Origin***. Each Inter-Operator IP Backbone shall make all reasonable efforts to ensure that the IP addresses presented by the Service Providers are valid; i.e. issued by either the Inter-Operator IP Backbone provider or any Internet address registration authority. Each Inter-Operator IP Backbone 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 AS connected to that Service Provider acting as transit.
3. ***VPN Isolation***. Protection against eavesdropping from other Virtual Private Networks (VPNs) running over the same IP infrastructure as the Inter-Operator IP Backbone VPN shall be guaranteed.
4. ***Anti-Spoofing***. Both route and packet anti-spoofing measures shall be implemented to prevent any connected GPRS/UMTS Operator Autonomous System to falsely divert data from its intended destination to an unauthorised location, or to mimic another device not belonging to that system with the intention of intercepting data designated for that device.
5. ***Denial of service***. Adequate measures shall be implemented to protect network resources such as Inter-Operator IP Backbone root DNS servers against flooding attacks.

6. ***Network security policies***. Each peering partner shall have well defined internal security policies, covering confidentiality, integrity and availability, with well-defined and audited network security organisation and procedures.
7. ***Public Internet connections***. If a Inter-Operator IP Backbone network is connected to the public Internet it shall guarantee that adequate measures such as Layer 3 firewalls and intrusion detection software are implemented on those connections. Incoming connections (initiated from the Internet) should be blocked. If the public Internet is used to connect Service Providers to the Inter-Operator IP Backbone, then the Inter-Operator IP Backbone provider shall ensure that authentication and encryption are used between the Service Provider and the Inter-Operator IP Backbone. Networks and autonomous system numbers must not be advertised to Internet.

Inter-Inter-Operator IP Backbone Security Measures

The following requirements relate to the security measures implemented between the Parties at any Point of Interconnection.

Hardware:

1. **Connection:** Connection to the PX secured location shall be made using leased line, Frame relay, MPLS VRF, IPVPN or ATM. No public Internet connection shall be used at the Point of Interconnection
2. **Physical Connectivity:** Peering members will only connect equipment that is controlled and operated by that member to the Point of Interconnection shared infrastructure. Parties will not connect any other equipment on behalf of Third parties to that shared infrastructure.
3. **Infrastructure:** A shared infrastructure is used to connect each peering partner'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.
4. **Connection Permissions:** Parties will not touch equipment and/or cabling owned by other members without the explicit permission of the member owning that equipment.
5. **Monitoring:** Peering members will not install "sniffers" to monitor traffic passing through the Point of Interconnection, except through their own ports.
6. **Allowed Connectivity:** Peering members will not directly connect any other Third Parties who are not peering members via circuits to their equipment hosted at the Point of Interconnection.

Configuration:

1. **Protocols:** Peering members must, on all interfaces connected to the shared LAN infrastructure, disable: ICMP redirects, CDP, IRDP, Directed broadcasts, IEEE802 Spanning Tree, Interior routing protocol broadcasts, and all other MAC layer broadcasts except ARP.
2. **Default Route:** No "route of last resort" shall be configured towards any other peering Inter-Operator IP Backbone. That is, peering members will 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 advertisee party.

3. **Routing**: Peering members 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.
4. **Route Advertisements:** Peering members will 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 or interim IPX DNS must be allowed. Networks will be summarized customer/Inter-Operator IP Backbone bases. Host routes will not be used.
5. **IP-**Traffic through peering point is allowed as default and Peering Partners will follow the GSMA common rules written in the document IR.34

Transit Traffic

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

BILATERAL VOLUNTARY CONDITIONS

This section may be bilaterally agreed between both parties and the following topics can be handled on bilateral basis, if required.

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

Other Requirements: