GPRS Roaming Guidelines

Version 10.0

05 July 2017

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

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

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.1.1 Scope 4
1.1.2 Architecture and Interfaces 4
1.2 Definition of Terms 5
1.3 Document Cross-References 6
2 Roaming Scenarios 7
3 Fundamental GPRS Functionality Technical Requirements & Recommendations 7
3.1 Introduction 7
3.2 Inter-PLMN IP backbone network requirements 8
3.2.1 IP address & routing 8
3.2.2 DNS 8
3.3 Access Point Name (APN) 8
3.3.1 General 8
3.3.2 APN Components 9
3.3.3 Types of APN 12
3.4 Addressing 13
3.4.1 UE Addressing 13
3.4.2 Network Element Addressing 15
3.4.3 The Transition to IPv6 16
3.5 PDP Types 18
3.5.1 Introduction 18
3.5.2 No PDP Context 19
3.5.3 IPv4 only PDP Context 19
3.5.4 IPv6 only PDP Context 20
3.5.5 Dual stack IPv4 and IPv6: IPv4 only PDP Context and IPv6 only PDP Context 20
3.5.6 Dual stack IPv4 and IPv6: IPv4 and IPv6 in single PDP Context 21
3.5.7 Limiting QoS for inbound roamers to the limits of the roaming agreement 22
3.5.8 Enforcement of QoS by the VPMN 23
4 Additional GPRS Functionality Technical Requirements & Recommendations 23
4.1 Introduction 23
4.2 Control of multiple, concurrent PDP Contexts 23
4.2.1 Definition 23
4.2.2 Recommendations 24
4.3 Flow Based Charging 24
4.3.1 Definition 24
4.3.2 Recommendations 25
4.4 Automatic Device Detection 25
4.4.1 Definition 25
4.4.2 Recommendations 25

4.5 Direct Tunnel Functionality 25
4.5.1 Definition 25
4.5.2 Recommendations 26
4.6 VPMN identification for network sharing and end user billing 26
4.6.1 Introduction 26
4.6.2 Recommendations 27
4.7 Technical Requirements for Dynamic Policy and Charging Control 27
4.7.1 Network Requested Secondary PDP Context Activation and GGSN-Initiated PDP Context Modification Procedures 28
4.7.2 Limiting QoS for inbound roamers to the limits of the roaming agreement 29
4.7.3 Enforcement of QoS by the VPMN 29
4.8 Security Considerations 29
4.8.1 GTP Security 29
5 Interworking with the LTE/EPC 32
Annex A Known Issues and Solutions 33
A.1 GTP version 0 and version 1 Interworking Problem 33
A.1.1 Introduction 33
A.1.2 VPLMN solution 33
A.1.3 HPLMN solution 33
A.2 IP source address of GTPv1 response messages 34
A.3 GPRS QoS Classes 34
Annex B Document Management 35
B.1 Document History 35
B.2 Other Information 36

1 Introduction

1.1 Overview

1.1.1 Scope

Throughout this PRD, the term "GPRS" is used to denote both 2G GPRS and 3G Packet Switched ("PS") service. Please see GSMA PRD IR.88 [15] for details of LTE data roaming.

This document provides recommendations on how GPRS networks can interwork in order to provide GPRS capabilities when users roam onto a network different from their HPMN.

It refers to current 3GPP specifications for GPRS and other GSMA PRDs where necessary, in particular GSMA PRD IR.34 [8], GSMA PRD IR.40 [16] and GSMA PRD IR.35 [9].

1.1.2 Architecture and Interfaces

GPRS roaming is achieved using the standardised interfaces detailed in 3GPP TS 23.060 [1]. The GPRS architecture is shown below in Figure 1.

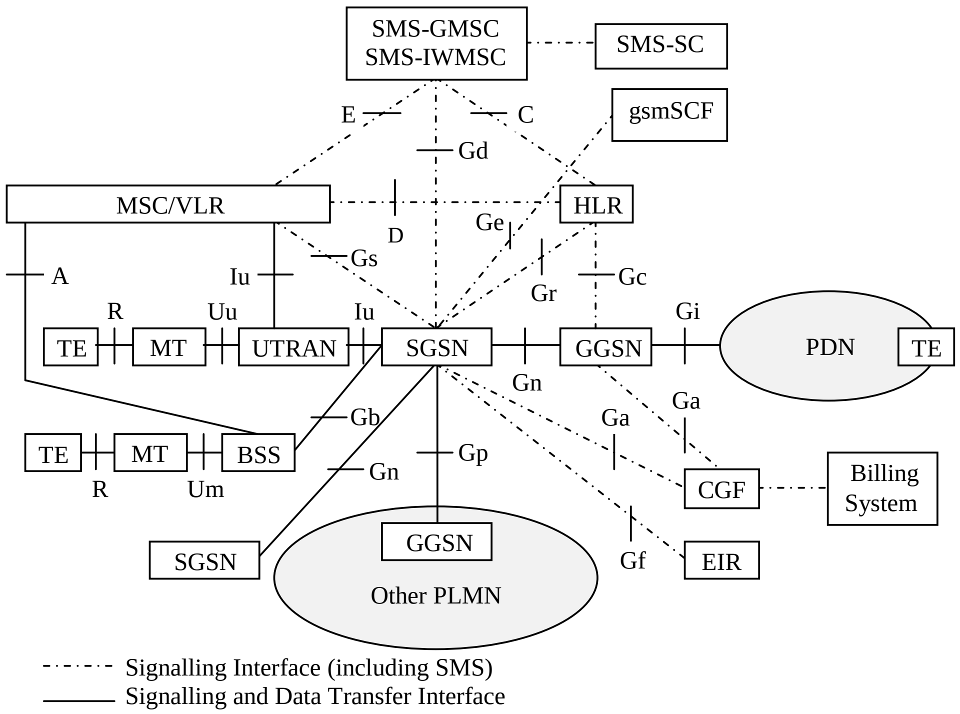

Figure 1: Overview of the GPRS Logical Architecture

See 3GPP TS 23.060 [1] for more information on the specification of each interface. Note that the "TE" and "MT" entities above are functions of the User Equipment (UE).

The following interfaces are relevant for GPRS roaming and are detailed as follows:

Nodes	Interface ID	Protocol
SGSN – HLR	Gr	MAP (3GPP TS 29.002 [3])
SGSN – SMS-IWMSC/GMSC	Gd	
SGSN – GGSN	Gn/Gp	GTP (3GPP TS 29.060 [4])
SGSN – SGSN	Gn	

Table 1: interfaces relevant for GPRS roaming

Notes:

- The procedures and message flows for all the above interfaces are described in 3GPP TS 23.060 [1].
- The SGSN – SGSN interface is used in roaming only when inter-PLMN Hand Over is supported.
- The SGSN – GGSN interface when used within a single PLMN is known as the Gn interface. When used between PLMNs it is known as the Gp interface.

The inter-PLMN DNS communications interface (used by the SGSN to find a GGSN) uses standard DNS procedures and protocol, as specified in IETF RFC 1034 [5] and IETF RFC 1035 [6].

The services that networks may support are detailed in GSMA PRD SE.20 [10].

The charging requirements for GPRS in a roaming environment are detailed in GSMA PRD BA.27 [11].

1.2 Definition of Terms

Term	Description
3GPP	3rd Generation Partnership Project
ADD	Automatic Device Detection
APN	Access Point Name
BG	Border Gateway
DNS	Domain Name System
EIR	Equipment Identity Registry
FQDN	Fully Qualified Domain Name
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GTP	GPRS Tunnelling Protocol
HGGSN	Home GGSN
HLR	Home Location Register

HPLMN	Home Public Land Mobile Network
IE	Information Element
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPX	IP Packet eXchange
MAP	Mobile Application Part (protocol)
MCC	Mobile Country Code
MNC	Mobile Network Code
MS	Mobile Station
NE	Network Element
PCC	Policy and Charging Control
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMN	
PRD	Permanent Reference Document
QoS	Quality of Service
SGSN	Serving GPRS Support Node
SS7	Signalling System #7
TLV	Type-Length-Value
VGGSN	Visited GGSN
VPLMN	Visited Public Land Mobile Network
WAP	Wireless Application Protocol

Term	Description
Network Eelement	Any active component on the network that implements certain functionality that is involved in sending, receiving, processing, storing, or creating data packets. Network elements are connected to networks. In the mobile network, components like the SGSN, GGSN, MME, SGW, PGW, HLR, HSS, and GTP Firewall, as well as routers and gateways are network elements.

1.3 Document Cross-References

Ref	Document Number	Title
1	3GPP TS 23.060	"GPRS Service Description; Stage 2"
2	3GPP TS 23.003	"Numbering, addressing and identification"
3	3GPP TS 29.002	"Mobile Application Part (MAP) specification”
4	3GPP TS 29.060	"General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface"

5	IETF RFC 1034	"Domain Names – Concepts and Facilities"
6	IETF RFC 1035	“Domain Names – Implementation and Specification”
7	Void	Void
8	GSMA PRD IR.34	“Inter-PLMN Backbone Guidelines”
9	GSMA PRD IR.35	“End to End Functional Capability specification for Inter-PLMN GPRS Roaming”
10	GSMA PRD SE.20	“GPRS and WAP Service Guidelines”
11	GSMA PRD BA.27	"Charging and Accounting Principles"
12	Void	
13	GSMA PRD IR.67	"DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers"
14	GSMA PRD IR.21	“GSM Association Roaming Database, Structure and Updating Procedures”
15	GSMA PRD IR.88	"LTE Roaming Guidelines"
16	GSMA PRD IR.40	"Guidelines for IP Addressing and AS Numbering for GRX/IPX Network Infrastructure and User Terminals"
17	3GPP TR 23.975	"IPv6 Migration Guidelines"
18	3GPP TS 23.107	"Quality of Service (QoS) concept and architecture"
19	3GPP TS 23.401	"General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”
20	PRD FS.20	GPRS Tunnelling Protocol (GTP) Security
21	PRD IR.77	InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers, binding Permanent Reference Document of the GSMA.
22	3GPP TS 33.117	Catalogue of General Security Assurance Requirements, Technical Specification of the 3GPP.
23	3GPP TS 23.251	Network sharing; Architecture and functional description

2 Roaming Scenarios

3 Fundamental GPRS Functionality Technical Requirements & Recommendations

3.1 Introduction

This section describes, and provides recommendations where appropriate, the fundamental GPRS and GPRS Tunnelling Protocol (GTP) functionality that is required at a minimum to enable GPRS roaming between PLMNs.

3.2 Inter-PLMN IP backbone network requirements

3.2.1 IP address & routing

The requirements in GSMA PRD IR.34 [8] and GSMA PRD IR.40 [13] shall apply for the routing and addressing between PLMNs for the Gp interface. This includes the requirements on Border Gateways. Internal IP addressing and routing is a decision for the PLMN.

3.2.2 DNS

In GPRS, the SGSN utilises a DNS in order to resolve an Access Point Name (APN) (this procedure is detailed in section 3.3) and to resolve the FQDN of another SGSN (as used in inter-SGSN hand-overs). The DNS system used for these procedures will be hosted in accordance with the general requirements for Inter-PLMN IP backbone networks as specified in GSMA PRD IR.34 [8], and general requirements for DNS as specified in GSMA PRD IR.67 [13].

Since user data is encapsulated in GTP packets, the user cannot "see" the GRX/IPX network. As such, any FQDNs in URLs or any other addressing should be resolved by the Internet DNS. Care should be taken by the PLMN in order to prevent DNS requests from end users being sent to the DNS used by the SGSN e.g. GRX/IPX network's DNS.

3.3 Access Point Name (APN)

3.3.1 General

The Access Point Name (APN) is an 8-bit ASCII character string that contains the user and network’s desired IP access preference and is used to create the logical connection between UE and External PDN. Its maximum overall length is 100 characters.

3.3.2 APN Components

Overview

The APN consists of the following parts:

- Network ID – points to the access point within a GPRS PLMN
- Operator ID – points to a GPRS PLMN

The complete APN is a fully qualified domain name (FQDN) of the format:

<Network Identifier>.<Operator Identifier>.gprs

Since the Access Point Name (APN) is an FQDN, it is therefore a logical name for (an) IP address(es) that will be associated with the PDP Context of the UE. This APN IP address will be used to create the connection between the UE and the PLMN GPRS terminating node (GGSN) that provides the connectivity to the required external PDN.

This is detailed further in 3GPP TS 23.003 [2], with more recommendations below.

Network Identifier

The Network Identifier is defined in 3GPP TS 23.003 [2] to be a string of a maximum of 63 characters, and it is recommended that its value be either a standardised value or an Internet reserved domain name (some values are prohibited, as defined in section 9.1.1 of 3GPP TS 23.003 [2]). It is used to identify the users' chosen PDN to which to connect the UE. It can be used to point to a GGSN in the HPLMN or in the VPLMN, depending on the presence of the "vplmnAddressAllowed" flag in the subscriber profile (enabled on a per APN, per subscriber basis, and downloaded from the HLR to the SGSN), and also the Operator Identifier appended to it either by the SGSN or by the subscriber himself.

The Network Identifier is provided by the subscriber when establishing a PDP Context. If the subscriber provides the whole APN (as depicted in 3.1.3.2.1 above), rather than just the Network Identifier, then the SGSN skips appending an Operator Identifier followed by the label ".gprs", and instead attempts to resolve the given full APN. In conjunction with the "vplmnAddressAllowed" flag in the subscriber profile, this can be used to enable the subscriber to control whether or not a HGGSN or VGGSN is used. This is depicted in Figure 9, below, where the subscriber opts to use the HGGSN.

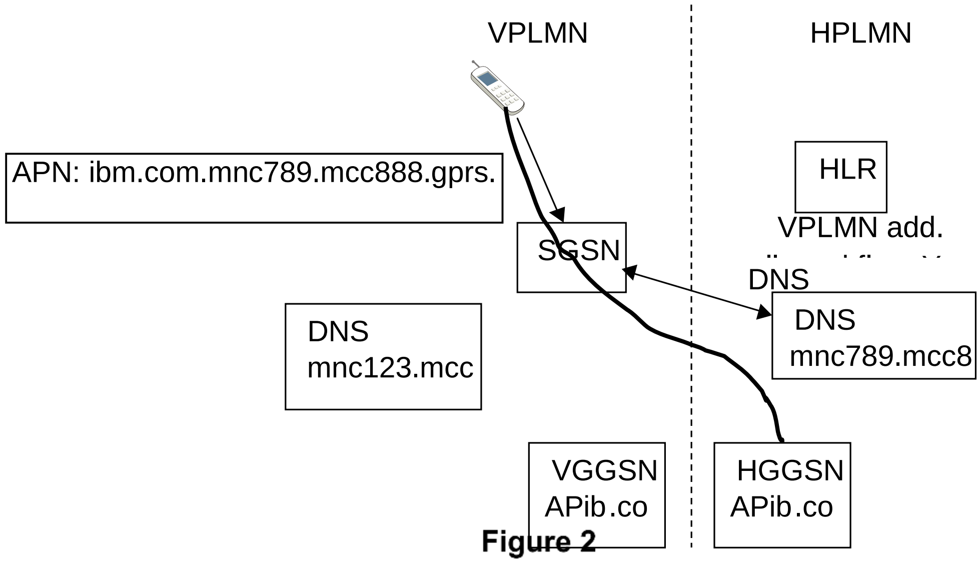

Figure 3: Subscriber enters whole APN.

In order for the subscriber to select a VGGSN, he would use the MNC and MCC of the VPLMN in the Operator Identifier part of the APN. In addition, of course, the "vplmnAddressAllowed" flag would again have to be set by his HPLMN.

To make provisioning simpler for the subscriber, just the Network Identifier should be used (perhaps by pre-provisioning in UE or PC connection software), and control over if/when to use a VGGSN controlled by the subscriber's HPLMN.

The HPLMN can prohibit a VGGSN to be used by a subscriber for a given APN (and thus force that subscribers to always use the HGGSN for that APN), by simply disabling the vplmnAddressAllowed flag. . In this instance, the SGSN will append an Operator Identifier of the HPLMN to the Network Identifier, and the subscriber will then use the HGGSN, as depicted in Figure 10, below.

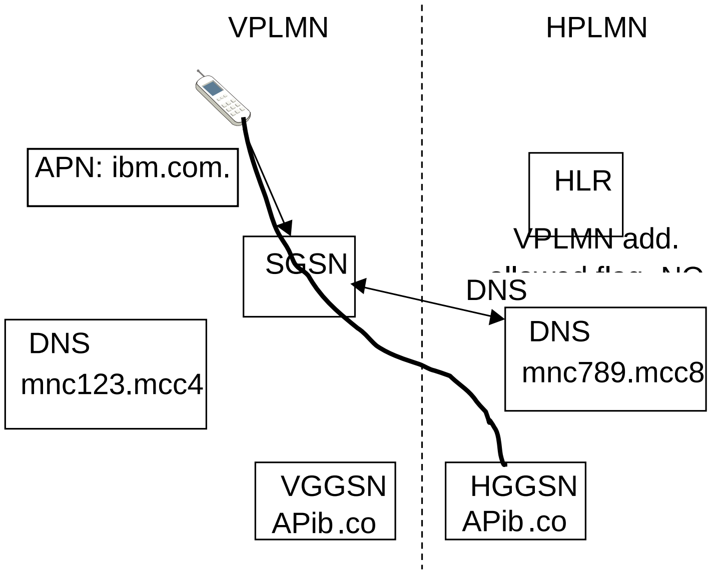

Figure 4: Subscriber has APN of ibm.com set with VPLMN allowed flag set to No.

In order to enable the subscriber to use a VGGSN for a given APN, the HPLMN simply enables the "vplmnAddressAllowed" flag, which then instructs the SGSN to append an Operator Identifier of the VPLMN to the Network Identifier.

In the subscriber supplying only a Network Identifier in the PDP Context activation and the HPLMN enabling VGGSN use by enabling the "vplmnAddressAllowed" flag, problems can arise with the PDN to which the Network Identifier points to. In particular, problems are likely to occur if a customer specific Network Identifier is shared between different parts of the company in various countries or regions. These customers may request the same value be used in the Network Identifier (e.g. the same .com or .org domain name) in different GPRS networks for the countries in which they have resident staff. This is depicted in Figure 11.

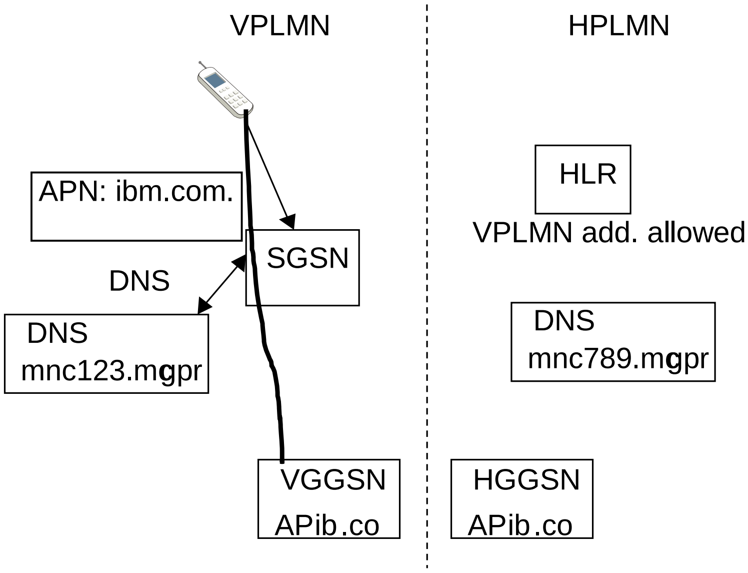

Figure 5: Visited and Home network have IBM.com as a registered Network ID

Although 3GPP TS 23.003 [2] recommends to use domain names reserved on the Internet for uniquely identifying customer specific PDNs, this solution has the disadvantage that the customer is responsible for the uniqueness of the APN Network Identifier between *all* PLMNs to which they have a subscription/commercial agreement. The correct operation of the GPRS service thus depends on the careful behaviour of customers, which may or may not be manageable.

In order to guarantee uniqueness of APN Network Identifiers between PLMNs, the following is recommended:

- Provide only HGGSN roaming for the customer.
- If VGGSN roaming is required for the customer, then:
    - Inform the customer to not provide their chosen Internet domain name to any other PLMN with whom they will use GPRS roaming (perhaps formalised as part of a commercial agreement); or
    - Use the customer's chosen Internet domain name in conjunction with an HPLMN owned Internet reserved domain name e.g. a Network Identifier of "ibm.com.vodafone.co.uk".

Operator Identifier

The Operator Identifier is defined in 3GPP TS 23.003 [2]. It consists of the label "mnc" followed by the MNC and the label "mcc" followed by the MCC, e.g. "mnc015.mcc234". Use of the HPLMN's or VPLMN's MNC/MCC is dependent on whether a HGGSN or VGGSN (respectively) is used.

GSMA PRD IR.67 [13] allows for "human readable" Operator Identifiers. However, their usage is not widespread and cannot be guaranteed to be resolvable by SGSNs in all VPLMNs. Therefore, its usage should be limited e.g. to non-roaming scenarios only.

3.3.3 Types of APN

General

There are two types of APNs:

- Service APN
- Wildcard APN

These are both explained in the following sections.

Service APN

The Service APN is recognised by the APN Network ID consisting of just one label i.e. a network ID without any separating dots. This enables a Service APN to be differentiated from a normal Network Identifier i.e. a Network Identifier that contains at least one dot.

The services to be supported and their *Service APN names* is described in GSMA PRD SE.20 [10].

If the service is not supported in the visited network, a GGSN in the home network will be used instead. In this case, the resolved GGSN can vary dependent on the SGSN that makes the request (location based) or dependent on the workload of the GGSN.

The GGSN that the Service APN has resolved to must provide the service agreed upon as specified by GSMA PRD SE.20 [10].

The Service APN may provide a subscriber with transparent access to the service requested, thus removing the requirement for authentication, policing, packet filtering, or NAT.

No guaranteed quality of service can be associated with a Service APN.

Wildcard APN

A Wildcard APN is an APN that contains a wildcard identifier (defined in 3GPP TS 23.003 [2] to be an asterisk - '*') stored in the subscriber's profile in the HLR and downloaded to the SGSN at attachment. This enables the following when the subscriber activates a PDP Context:

- A "default" APN has to be chosen by the SGSN, if no APN is requested
- Any PDP Context with dynamic PDP address may be activated towards any requested APN

GGSNs have the ability to recognise if a subscriber is using the wildcard functionality, and may deny the attempted PDP Context activation. It is recommended that this functionality be enabled, in order to block subscribers attempting to fraudulently access PDNs that are not allowed access to i.e. APNs not in the subscriber profile.

3.4 Addressing

3.4.1 UE Addressing

SS7

A GPRS capable UE may be assigned an MSISDN. However, it must be assigned an MSISDN by the HPMN in any of the following conditions:

- The UE is also CS capable (so needs to establish/receive CS calls).
- The UE is capable of SMS.

IP

General

A GPRS capable UE is assigned (either statically or dynamically) one or more IP addresses (of type Public or Private) per PDP Context activation for the duration of the connection, a procedure which may not occur for GPRS capable UEs (it depends on the services the UE supports and to which the user is subscribed). If a UE can support more than one simultaneous active primary PDP Context, then one IP address will be required for each. The version of the IP address allocated (i.e. IPv4 or IPv6), is dependent on the requested

PDP Type of the PDP Context by the UE, and the PDP Types supported in the core network. For more information on PDP Types see section 3.5.

The requirements in GSMA PRD IR.40 [13] must be adhered to for the IP addresses assigned to a UE for each of its PDP Contexts.

A UE's IP address is **not** associated with the Intra or Inter-PLMN IP backbone network, and strict separation of ranges used is required as specified in GSMA PRD IR.34 [8]. Any UE IP datagrams that are routed over these networks are tunnelled, as mandated in GSMA PRD IR.34 [8].

Public vs Private IP addressing

In IPv6, public versus private IP addressing is FFS.

In IPv4, private and public addressing can be used. Each has its own advantages and disadvantages as described in GSMA PRD IR.40 [13]. The choice of which to use when depends upon many factors. One key factor is the type of service offered and how the PLMN operator has configured it in their network.

Static IP Address Allocation

Use of static IP addresses in GPRS is specified in section 9.2.1 of 3GPP TS 23.060 [1]. A static IP Address is assigned to a user by the HPLMN, and held in the user’s subscription record within the HLR (a copy of which is sent down to the SGSN at GPRS attach).

A static IP address restricts the user to only use PDP Contexts in their HPLMN (HGGSN) with specified APNs. The user will have to have an IP address dynamically allocated by the VPLMN in order to enable use of PDP Contexts established to a VGGSN. Thus, this may restrict a user whilst roaming.

In addition, the IP address issued to the user cannot be reused by any other user, so this has the disadvantage of exhausting IP address ranges as well as increasing burden upon O&M.

Therefore, static IP address allocation is discouraged.

Dynamic IP Address Allocation

Use of static IP addresses in GPRS is specified in section 9.2.1 of 3GPP TS 23.060 [1]. A dynamic IP address is assigned to a user at each PDP Context activation and is liable to change with each new PDP Context activation.

The GGSN may itself assign an IP address to a user (it can retrieve such data during AAA (i.e. RADIUS or Diameter) procedures with a AAA server), or, it may leave it to some other mechanism e.g. DHCP, stateless address auto-configuration.

For PDP Contexts of type "PPP" (Point-to-Point Protocol), dynamic IP address allocation is always performed.

Dynamic IP address allocation is recommended to be used over static address configuration.

Address assignment responsibilities

The entity that owns the PDN connected to the GGSN via the Gi interface has general responsibility for assigning IP addresses to the UE for a PDP Context (associated with the APN). This could be the PLMN itself or a 3rd party such as an ISP, corporate entity, etc. However, the PLMN has the responsibility to work with and advise the PDN owning entity the UE connectivity and addressing requirements associated with the services to be supported.

The following diagram represents the UE IP addressing assignment responsibility.

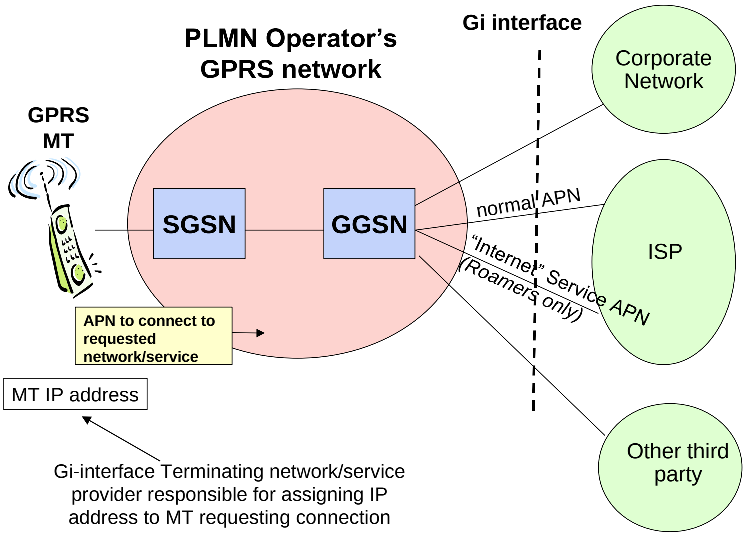
Gi interface
PLMN Operator's
GPRS network
Corporate Network
GPRS MT
SGSN
GGSN
normal APN
ISP
"Internet" Service APN
(Roamers only)
APN to connect to requested network/service
MT IP address
Gi-interface Terminating network/service provider responsible for assigning IP address to MT requesting connection
Other third party

Figure 6: UE IP address assignment responsibility

In the diagram above, the UE can request access to various types of network/services, each being identified by the APN sent by the UE. For example:

- APN=wap.genie.co.uk (to request WAP service access offered by the ISP, "Genie"). The MT IP address is "owned" by the Genie ISP (Private)
- APN=email.xyz.co.uk (to request access to email services from the corporate, "xyz"). The MT IP address is "owned" from the corporate's allocated address space (Public or Private)
- APN=internet (to request access to the Internet). The MT address is "owned" by the network (Public)

3.4.2 Network Element Addressing

The SGSN and GGSN network elements require IP addresses. The requirements in GSMA PRD IR.34 [11], GSMA PRD IR.40 [12] shall apply for the routing and addressing used for the Gp interface. The SGSN requires a SS7 Global Title, in order to support the relevant MAP and CAP based interfaces (see section 1.1.2 for more information).

Internal addressing and routing is a decision for the Service Provider.

As considered by Annex C of TS 23.060 [1], IP MTU baseline over Gp interface is 1500 octets, assuming that GTP packets are exchanged between IPv4 addressed equipment.

Both VPMN and HPMN shall then engineer their internal networks in order to ensure that an IPv4 packet of 1500 octets, including IP, UDP and GTP headers, will be transmitted to the remote party with no fragmentation, taking into account:

- A VPMN that want to internally deploy IPv6 and/or IPSec needs to ensure that layer 2 payload is dimensioned accordingly (i.e. > usual Ethernet 1500 octets payload); and
- If using MSS clamping, a HPMN that wants to use IPv6 for end-user bearers needs to reduce MSS clamping value to take into account IPv6 overheads

3.4.3 The Transition to IPv6

General

IPv4 addresses are imminently to exhaust. Sometime in the future, the entirety of the operators' networks (including radio access networks and core networks, services and applications) and UEs may well all support IPv6 and the legacy IPv4 may be retired. However, a mixture of both IPv4 and IPv6 will need to coexist for quite some time while the transition from IPv4 to IPv6 takes place. During the transition, various components of operators' networks, and thus the roaming ecosystem, will be at different stages of transition towards IPv6.

During the transition period, UEs, VPMNs, HPMNs and services can be IPv4 only, IPv6 only, or dual stack IPv4 and IPv6. In the GPRS system, IPv4 and IPv6 connections can be used using separate PDP Contexts (one for IPv4 and one for IPv6), or one PDP Context for both IPv4 and IPv6 (using the newer PDP Type of "IPv4v6" – see section 3.5 for more information).

In all the solutions discussed below, for interworking IPv6 to/from IPv4 for IPv6 only connected UEs, it is recommended to use NAT64 at the Interworking Function (IWF) and for interworking IPv4 to/from IPv6 for IPv4 only connected UEs, it is expected that the UE will take care of the interworking using a tunnelling based solution, for example: 6rd, 6to4, IPinIP, and so on. Therefore, operators must not block such kind of tunnels for their subscribers and inbound roaming subscribers.

Home GGSN Roaming

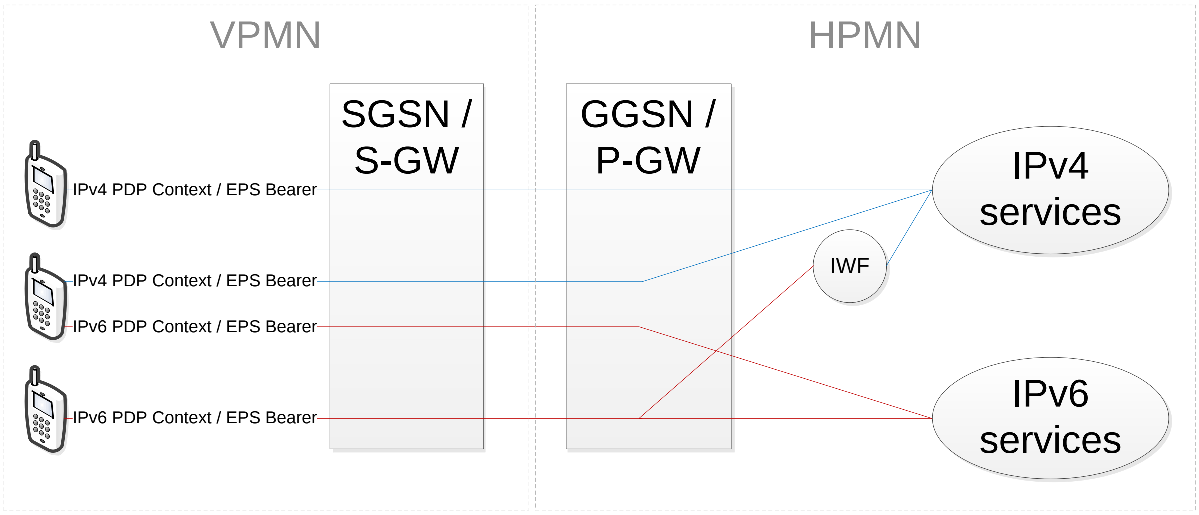
VPMN
HPMN
SGSN / S-GW
GGSN / P-GW
IPv4 PDP Context / EPS Bearer
IPv4 PDP Context / EPS Bearer
IPv6 PDP Context / EPS Bearer
IPv6 PDP Context / EPS Bearer
IWF
IPv4 services
IPv6 services

Figure 7: Access to HPMN Based Services

Once the roaming UE has been successful in establishing a PDP Context and has acquired IP addresses, it can then access HPMN based services as follows:

- If the UE has only an IPv4 address then it can access IPv4 services directly but cannot access IPv6 services without employing some special tunnelling mechanism over the IPv4 connection.
- If the UE has both IPv4 and IPv6 addresses then it can access IPv4 services directly with the IPv4 address and IPv6 services directly with the IPv6 address.
- If the UE has only an IPv6 address then it can access IPv6 services directly and IPv4 services with the help of an IWF in the HPMN.

Direct access to VPMN based services is not possible in this roaming scenario.

Visited GGSN Roaming

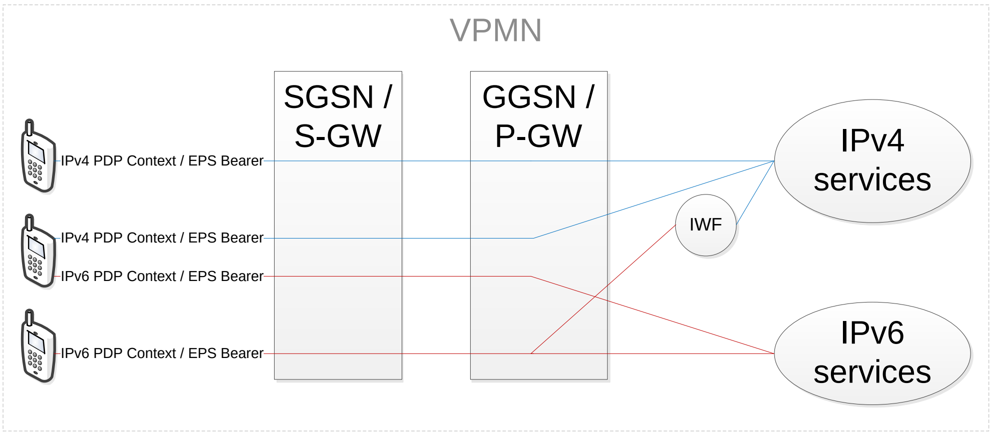
VPMN
SGSN / S-GW
GGSN / P-GW
IPv4 PDP Context / EPS Bearer
IPv4 PDP Context / EPS Bearer
IPv6 PDP Context / EPS Bearer
IPv6 PDP Context / EPS Bearer
IWF
IPv4 services
IPv6 services

Figure 8: Access to VPMN Based Services

Once the roaming UE has been successful in establishing a PDP Context and has acquired IP addresses, it can then access VPMN based services as follows:

- If the UE has only an IPv4 address, then it can access only IPv4 services directly but cannot access IPv6 services without emplying some special tunnelling mechanism over the IPv4 connection.
- If the UE has both IPv4 and IPv6 addresses, then it can access IPv4 services directly with the IPv4 address and IPv6 services directly with the IPv6 address.
- If the UE has only an IPv6 address, then it can access IPv6 services directly and IPv4 services with the help of an IWF in the VPMN.

Direct access to HPMN based services is not possible in this roaming scenario.

3.5 PDP Types

3.5.1 Introduction

The following table lists the different PDP Types (as defined in 3GPP TS 23.060 [1]) that can be requested by devices and used over the Gn and Gp interfaces, and provides recommendations on their use.

PDP Type	Brief explanation and recommendations
PPP	This PDP Type is no longer supported in LTE networks, therefore its use should be avoided in subscriptions that could use an LTE capable device.
IPv4	In general, all VPMNs today support at least this PDP Type in order for GPRS roaming to work.
IPv6	This PDP Type was added in 3GPP R99, therefore its support should be ubiquitous amongst VPMNs where 3G and/or GTPv1 is supported.
IPv4v6	This PDP Type was added in 3GPP Rel-8 and should be supported in networks that support LTE. It is recommended that any APN configured with this PDP Type is configured also with the IPv4 and IPv6 PDP Types.

To support inbound roamers that utilise home GGSN roaming (see section 3.4.3.2), the support of PDP Types in SGSNs must be documented in the appropriate field of the VPMN operator's GSMA PRD IR.21 (or the IR.21 database) [14].

To support inbound roamers that utilise visited GGSN roaming (see section 3.4.3.3), the support of PDP Types in all GGSNs that are used for inbound roamers for visited GGSN roaming must be documented in the appropriate field of the VPMN operator's GSMA PRD IR.21 (or IR.21 database) [14].

SGSNs compliant with older 3GPP releases can modify unknown PDP Types in PDP Context Activation requests to a PDP Type of "IPv4", before requesting connectivity to a GGSN. Even if the GGSN allows the modified PDP Context Request, this can cause unpredictable device behaviour, which in the worst cases results in the device failing to establish a PDP Context at all or continually retrying to establish a PDP Context to its originally requested PDP Type. It is highly recommended that SGSNs support the PDP Type "IPv4v6" (as also required in LTE networks – see GSMA PRD IR.88 [15]), regardless of whether or not the VPMN supports LTE, which not only solves the aforementioned problem but also reduces device-SGSN signalling during PDP Context activation for dual-stack IPv4 and IPv6.

The following sub-clauses identify the different use cases under which different PDP Contexts will be established for the IPv4, IPv6 and IPv4v6 PDP Types, and provides necessary guidelines therein.

3.5.2 No PDP Context

Under the following conditions, the UE will not have any IP connections, and as a result, the UE will not be able to access any IP services:

PDP Type(s) requested by UE	PDP Type supported in SGSN	PDP Types allowed by APN configuration in HLR and in GGSN
IPv4v6	IPv4	IPv6
IPv4 and IPv6	IPv4	IPv6
IPv6	IPv4	Any combination

Table 2: The UE will not have any IP connections

This use case occurs for IPv4 only VPLMN inbound roamers attempting to connect to a HPMN implementing scenario 3 of 3GPP TR 23.975 [17] (UE connecting to IPv6 only APN and accessing IPv4 services through a NAT64). It is used for when the HPMN faces an IPv4 address shortage.

In order to avoid this use case from occurring, an HPMN must not configure its subscriber's for IPv6 only APNs and must support IPv4 or IPv4v6 in addition to supporting IPv6 PDP Type on its GGSNs (i.e. IPv6 only APNs should be avoided on the GGSN) when such subscribers can roam to IPv4 only VPMNs.

For more ubiquitous and seamless roaming, support for at least IPv6 PDP Type in addition to the IPv4 PDP Type is highly recommended. Support for IPv4v6 PDP Type in addition to IPv4 and IPv6 PDP Types is also recommended.

3.5.3 IPv4 only PDP Context

Under the following conditions, the UE will have only an IPv4 connection, and as a result, the UE will be able to access only IPv4 services in the HPMN:

PDP Type(s) requested by UE	PDP Type(s) supported in SGSN	PDP Types allowed by APN configuration in HLR and in GGSN
IPv4v6	IPv4	IPv4v6
IPv4v6	IPv4	IPv4 and IPv6
IPv4v6	IPv4	IPv4
IPv4v6	IPv4 and IPv6	IPv4
IPv4v6	IPv4v6	IPv4

PDP Type(s) requested by UE	PDP Type(s) supported in SGSN	PDP Types allowed by APN configuration in HLR and in GGSN
IPv4 and IPv6	IPv4	IPv4v6; or IPv4 and IPv6
IPv4 and IPv6	IPv4; or IPv4 and IPv6; or IPv4v6	IPv4
IPv4	IPv4; or IPv4 and IPv6; or IPv4v6	IPv4; or IPv4 and IPv6; or IPv4v6

Table 3: The UE will have only an IPv4 connection

3.5.4 IPv6 only PDP Context

Under the following conditions, the UE will have only an IPv6 connection, and as a result, the UE will be able to access IPv6 services in the HPMN:

PDP Type(s) requested by UE	PDP Type(s) supported in SGSN	PDP Types allowed by APN configuration in HLR and in GGSN
IPv4v6; or IPv4 and IPv6	IPv4 and IPv6; or IPv4v6	IPv6
IPv6	IPv4 and IPv6; or IPv4v6	IPv4 and IPv6; or IPv4v6; or IPv6

Table 4: The UE will have only an IPv6 connection

In the above scenario, in order for the UE to access IPv4 services, the HPMN should deploy a NAT64 as suggested in 3GPP TR 23.975 [17].

3.5.5 Dual stack IPv4 and IPv6: IPv4 only PDP Context and IPv6 only PDP Context

Under the following conditions, the UE will have both IPv4 and IPv6 connectivity through separate PDP Contexts (but to the same APN) and as a result, will be able to access both IPv4 and IPv6 services in the HPMN (and without the need for any NAT64):

PDP Type(s) requested by UE	PDP Type(s) supported in SGSN	PDP Types allowed by APN configuration in HLR and in GGSN
IPv4v6	IPv4 and IPv6	IPv4v6
IPv4v6	IPv4 and IPv6; or IPv4v6	IPv4 and IPv6
IPv4 and IPv6	IPv4 and IPv6; or IPv4v6	IPv4 and IPv6; or IPv4v6

Table 5: The UE will have both IPv4 and IPv6 connectivity through separate PDP Contexts

3.5.6 Dual stack IPv4 and IPv6: IPv4 and IPv6 in single PDP Context

Under the following conditions, the UE will have both IPv4 and IPv6 connectivity through one PDP Context and as a result, will be able to access both IPv4 and IPv6 services in the HPMN (and without the need for any NAT64):

PDP Type requested by UE	PDP Type supported in SGSN	PDP Types allowed by APN configuration in HLR and in GGSN
IPv4v6	IPv4v6	IPv4v6

Table 6: The UE will have both IPv4 and IPv6 connectivity through one PDP Context

The use of an IPv4v6 PDP Context enables IPv4 and IPv6 connectivity with less signalling and PDP Context resources than with two separate IPv4 and IPv6 PDP Contexts.

Currently IR.40 GSMA document only gives guidelines about IPv4 addressing. As soon as UE get IPv4v6 connectivity through IPv4v6 EPS Bearer/PDP Context, IPv4v6 addressing guidelines should be incorporated in IR.40 GSMA document.

Managing QoS during primary PDP Context setup or update
This section illustrates the functionalities that are needed in the VPMN and the HPMN to avoid IP connectivity failure when the QoS requested by roamers and the QoS supported or provided according to the roaming agreement by the VPMN are different.

The management of QoS during primary PDP context setup whilst roaming must:

1. Ensure a successful IP connectivity setup
2. Ensure that the QoS parameters of an inbound roamer are within the limits of the roaming agreement
3. Enforce the actual QoS by the VPMN.

3.5.7 Limiting QoS for inbound roamers to the limits of the roaming agreement

3.5.7.1 Requirements for the VPMN:

To ensure a primary PDP connection can be established successfully and updated while at the same time not violating the QoS policies of the VPMN for inbound roamers from a given HPMN, the following functionality is required for the VPMN:

- When an inbound roaming UE requests the establishment of a primary PDP context, the SGSN of the VPMN shall compare the QoS requested values restricted by the subscribed QoS profile received from the HLR for the chosen APN with the pre-configured range of supported QoS profiles for the HPMN.

Note: These ranges are configured based on the roaming agreement with the respective HPMN.

R99 QoS parameters (i.e. excluding eARP and mapped ARPr99 if supported on GTPv1 by both VPMN and HPMN) are then negotiated as follow:

- In case the SGSN detects that a value is outside those ranges, the SGSN shall change/downgrade the related value to a configured default value for the related HPMN.
- If the QoS parameter values are in line with the roaming agreement, then the SGSN shall accept these values without modification..
- In case the SGSN supports the QoS upgrade functionality signalled by the Upgrade QoS Supported flag and the HPMN upgrades the QoS negotiated values in the Create PDP Context answer outside the pre-configured range of supported QoS profiles for the HPMN then, the SGSN shall downgrade the QoS profile values according to the configured default values for the related HPMN and send back an Update PDP Context request with the No QoS negotiation indication.

If both VPMN and HPMN support eARP functionalities on GTPv1, eARP values should be negotiated as described in 3GPP TS 23.060 [4]. The SGSN should compare the value sent by the GGSN with the supported QoS profile for this specific HPMN and decide to accept or reject the connection accordingly. In that case the ARP value is derived based on Annex E of 3GPP TS 23.401 [19].

The same requirements apply to the SGSN-Initiated PDP Context Modification Procedure and to the MS-Initiated PDP Context Modification Procedure.

3.5.7.2 Requirements for the HPMN:

To ensure a primary PDP context can be established successfully, the following functionality is required for the HPMN:

- When the HPMN receives a Create PDP Context request and the Upgrade QoS Supported bit of the Common Flags IE is set to 0 or is absent, then the HPMN shall accept or downgrade the QoS values as received from the VPMN.
- When the HPMN receives a Create PDP Context request and the Upgrade QoS Supported bit of the Common Flags IE is set to 1 then the HPMN is allowed to

upgrade the QoS values as received from the VPMN. If the HPMN upgrades the QoS profile values then it shall make sure that the QoS values sent back to the VPMN in the Create PDP Context response are within the pre-configured range of supported QoS profiles for the HPMN.

- When the HPMN receives an Update PDP Context request with the No QoS negotiation indication then the HPMN shall accept the QoS values as received from the VPMN.

3.5.8 Enforcement of QoS by the VPMN

If a VPMN has agreed to provide QoS in a roaming agreement, then the VPMN is required to engineer its access and core networks to fulfil the correspondent performance characteristics (Traffic Class, Delivery order, Transfer delay, bit rates, residual bit error ratio, etc.) according to 3GPP TS 23.107 [18].

4 Additional GPRS Functionality Technical Requirements & Recommendations

4.1 Introduction

This section describes, and provides recommendations where appropriate, some of the additional enhancements to GPRS and the GPRS Tunnelling Protocol (GTP). These features are not required in order for GPRS roaming to work, however, they provide additional capabilities for VPLMNs and/or HPLMNs.

4.2 Control of multiple, concurrent PDP Contexts

4.2.1 Definition

In more modern GPRS equipment (both network and terminal equipment), it is possible for a subscriber to set-up a connection to the one PDN, e.g., the Internet, and then later setup another connection to another PDN e.g. corporate LAN. There is a security issue in doing this in that packets from the Internet could possibly get forwarded on to the subscriber's corporate LAN and vice versa (using the subscriber's terminal equipment as a router). The only available methods of stopping this right are solutions at the IP layer (layer 3) such as firewall software on the terminal equipment, which for large corporate organisations may not be very viable to maintain. In addition, the user could (knowingly or unknowingly) easily disable such software.

In recognition of this potential security issue, 3GPP standardised in Rel-6 a method of controlling this at the layer 2 of the protocol stack i.e. GTP. The solution enables policing of PDP Context creations at the GGSN and in some cases where signalling can be saved, at the SGSN.

For each APN a new "APN Restriction" field is added to the APN information in the GGSN. The "APN Restriction" field takes the values of 1 to 4 inclusive (see the last four rows of the table below for the definition of each value).

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value of PDP contexts allowed to be established
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (e.g. who use MMS)	1
4	Private-2	Corporate (e.g. who do not use MMS)	None

Table 7: APN Restriction

Upon PDP Context creation, the SGSN determines the maximum APN Restriction value based on all (if any) currently active primary PDP Contexts and includes this in the Create PDP Context Request message it sends to the GGSN. If there is currently only one primary PDP Context established and the type of the APN Restriction is Private-2, the SGSN may optionally (as an enhancement) deny any further primary PDP Contexts being established, rather than leaving it to the GGSN to determine this. This is beneficial as it saves on (sometimes inter-PLMN) signalling between SGSN and GGSN.

It is noted that the solution works only for networks who differentiate services by use of different APNs. If the non-standardised "single APN" solution is used, this method may not work (or at least, may require modification).

4.2.2 Recommendations

It is recommended that operators configure APNs for access to WAP and MMS as APN restriction type Public-1 (value 1). It is also recommended that APNs for access to the public Internet (i.e. the "internet" APN) have the APN restriction type set to Public-2.

For APNs that give corporate customers access to their corporate LANs/Intranets, it should be agreed between mobile network operators and their respective corporate customers which restriction type best suites the corporate customer (commonly private-1 or private-2 restriction types).

4.3 Flow Based Charging

4.3.1 Definition

Flow Based Charging is a feature added in 3GPP Rel-6 that enables a finer granularity of charging to be performed at the GGSN than just duration or number of bytes sent/received in a PDP Context. This mainly consists of "deep packet inspection" in order to provide a more user understandable bill e.g. bill on number of web pages viewed. In addition, such information as location of the subscriber (geographically and also local time zone), what radio access technology is being used (e.g. 2G, 3G) and even what content is being downloaded/uploaded can be taken into account, however, this is subject to the SGSN implementing extra functionality to provide this information in real-time to the GGSN.

Flow Based Charing can be applied to both pre-pay and post-pay charging (also known as "on-line" and "off-line" charging, respectively). More details on this feature for both charging models can be found in section 15.1.1a of 3GPP TS 23.060 [1].

4.3.2 Recommendations

In the HGGSN roaming scenario (as described in section 2.2.2), Flow Based Charging can be used with or without additional billing agreements between the HPLMN and VPLMN (since the Flow Based Charging is performed on the GGSN). However, in order to realise the full benefits of FBC, the SGSN needs to provide additional information at PDP Context creation and update (it also needs to provide more frequent updates e.g. when intra-SGSN 2G/3G handovers occur). It should also be noted that the SGSN may continue to send its charging data as per standard inter-PLMN accounting; therefore, the HPLMN should still expect to receive it.

In the VGGSN roaming scenario (as described in section 2.2.3), Flow Based Charging should only be used in agreement with the HPLMN. Where such agreements exist, charging in the SGSN can be disabled for subscribers from the Flow Based Charging enabled HPLMNs to save on inter-PLMN traffic.

4.4 Automatic Device Detection

4.4.1 Definition

Automatic Device Detection (ADD) is a feature added in 3GPP Rel-6 that enables the HPLMN to "know" the current IMEI being used by the subscriber, even when that subscriber is roaming. This in turn, enables the HPLMN to perform device specific rendering of media for example, WAP/web pages, video size and codecs for streaming, as well as other functionality such as supplementary services and features supported by specific devices and EIR interrogations by the HPLMN.

More details can be found in section 15.5 of 3GPP TS 23.060 [1].

4.4.2 Recommendations

The SGSN in the VPMN must support reporting IMEISV to HLR/HSS.

EIR checks by the HPLMN may not be necessary if both the HPLMN and VPLMN connect to the GSMA's CEIR.

4.5 Direct Tunnel Functionality

4.5.1 Definition

The Direct Tunnel Functionality is a feature added in 3GPP Rel-7 that enables the routing of GTP User plane (GTP-U) packets directly between an RNC and GGSN (so removes the SGSN from the routing), whilst retaining the GTP Control plane (GTP-C) routing via the SGSN. This has the benefit of reducing the user plane capacity required on SGSNs. However, this functionality can only be used in the VGGSN roaming scenario, and of course, when the subscriber is in their HPLMN.

It should be noted that this functionality is defined only for subscribers on 3G, as direct routing between the BSS and GGSN is not possible. This is because, unlike the RNC, the BSS does not support GTP-U.

More information can be found in section 15.6 of 3GPP TS 23.060 [1].

4.5.2 Recommendations

Since the SGSN is removed from the GTP-U path, any Legal Intercept (LI) requirements on the GTP-U will have to be realised at the GGSN. Therefore, LI support on the GGSN is required in such cases.

4.6 VPMN identification for network sharing and end user billing

4.6.1 Introduction

End user billing depends on the VPMN. Different approaches could be implemented by the HPMN to identify the VPMN in real time, using the following GTP signalling information:

- SGSN IP address
- MCC/MNC information, present in Routing Area Identity (RAI) and/or User Location Information (ULI) IE as specified in 3GPP TS 29.060 [4]

The major drawbacks of using SGSN IP addresses are the following:

- IP addresses change frequently and could cause billing issues if not known by the HPMN Online Charging System. Whereas, the MCC/MNC combination clearly identifies the VPMN.
- SGSN IP addressing is not clear when SGSN sharing is implemented

SGSN sharing occurs when a single SGSN (or pool of SGSNs) is shared by two or more PMN's radio coverage. That is, a single range of Gp backbone IP addresses are presented to an HPMN for more than one VPMN, or from another perspective, a number of SGSNs from different VPMNs share the same IP address range.

A problem occurs in the HPMN, in that it cannot unambiguously identify in which VPMN's radio coverage the subscriber is roaming, as this is usually just determined by the presented SGSN IP address. This in turn can result in the roaming subscriber being billed by the HPMN for roaming in a VPMN that was never actually visited by the subscriber.

Note 1: RAI IE is mandatory to be sent from Release 8 of 3GPP TS29.060 [4] and the ULI IE is mandatory to be sent from Release 11 of 3GPP TS29.060 [4].

Note 2: In network sharing architecture, RAI and ULI IE might not be consistent respect to the MCC/MNC. The HPMN should then carefully define its preferences between all the possible identifiers to allow it apply billing (e.g. ULI > RAI > SGSN @IP address).

Note 3: An MCC/MNC change may only be reported to the HPMN in RAI and not in ULI IE.

Multi-Operator Core Network (MOCN) and Gateway Core Network (GWCN) are network sharing configurations where RAN is shared (3GPP TS 23.251 [23]) and the shared RAN broadcasts additional information in the broadcast system information to supply the PLMN-Ids of the multiple core network operators. To cope with UEs not supporting this additional information it is required for the shared GERAN/UTRAN to broadcast a MCC/MNC value in the legacy RRC information element for conventional PLMN-Id that does not identify any of the sharing core network operators (Common PLMN ID).

4.6.2 Recommendations

For all VPMNs, the Routing Area Identity (RAI) and/or User Location Information (ULI) GTP Information Element must be included in the GTP “Create PDP Context request” and the "Update PDP Context request" messages from the VPMN to the HPMN, in order to convey to the HPMN the VPMN used by the subscriber. The HPMN then has the possibility to extract this information to enable the billing system to unambiguously identify the correct VPMN in which the subscriber has roamed.

In case of GWCN and MOCN network sharing in VPMN (3GPP TS 23.251 [x]), unless otherwise stated by the HPMN, the VPMN is recommended to communicate the serving core network MCC/MNC value to the HPMN in both RAI and ULI IE. From Release 12.4.0 onwards of 3GPP TS 29.060 [4] it becomes mandatory to communicate the serving core network MCC/MNC value to the HPMN in both RAI and ULI IE.

This mechanism will significantly reduce the requirements on HPMN Online Charging Systems to frequently update their SGSN IP address databases.

Note 1: Prior to 3GPP release 12.4.0, it is unclear whether the VPMN should send Common PLMN ID or any serving network MCC/MNC in both RAI and ULI IE. HPMN should then be ready to cope with both Common PLMN ID and serving network MCC/MNC.

Note 2: The GTP RAI and ULI IE are specified in 3GPP TS 29.060 [4] and contain the MCC and MNC combination for the network operator.

In addition, the VPMNs using SGSN sharing must publish the use of the GTP RAI Additional MCC/MNC and/or ULI Additional MCC/MNC in GSMA PRD IR.21 [14].

4.7 Technical Requirements for Dynamic Policy and Charging Control

The chapter below deals with requirements that must be fulfilled by the HPMN and the VPMN if dynamic policy and charging control is required for some services when roaming.

The architecture diagram below shows the Home GGSN roaming architecture including the Policy and Charging Control system.

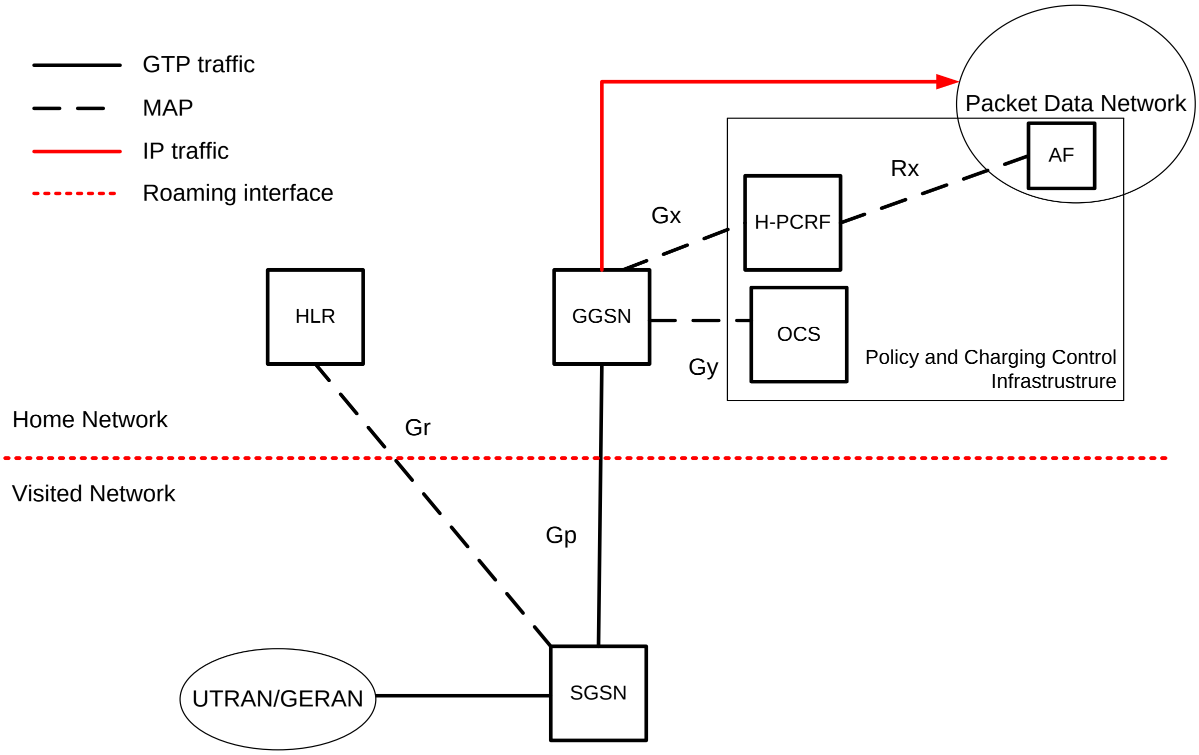

Figure 9: Policy and Charging Control Architecture with Home GGSN roaming

With the Home GGSN roaming architecture, the entire Policy and Charging Control infrastructure remains inside the HPMN. Therefore dynamic policy control is possible although the VPMN has not implemented a Policy and Charging Control infrastructure for its own purpose. However, there are requirements that must be supported by the VPMN:

1. The VPMN must support the Network Requested Secondary PDP Context Activation Procedure (see section 4.7.1).
2. The VPMN must support the GGSN-Initiated PDP Context Modification Procedure (see section 4.7.1).
3. The VPMN must support the Secondary PDP Context activation procedure
4. The VPMN and the HPMN must ensure that QoS parameters of roamers are within the limits of the roaming agreement (see section 4.7.2).
5. The VPMN must enforce the actual QoS (see section 4.7.3).

4.7.1 Network Requested Secondary PDP Context Activation and GGSN-Initiated PDP Context Modification Procedures

If services which require dynamic QoS and/or charging in roaming situation, it is required that the VPMN supports the following management procedures:

1. Network Requested Secondary PDP Context Activation – this procedure is invoked by the GGSN if for example the already established context' QoS cannot support the new requested service.
2. GGSN-Initiated PDP Context modification – the GGSN could initiate a GGSN-Initiated PDP Context modification procedure based on HPMN decision or in response to AF initiated PDP context modification.

3. Secondary PDP Context activation – this procedure is at the initiative of the UE because the QoS of the primary PDP context is not suitable for a new service required by the customer.

4.7.2 Limiting QoS for inbound roamers to the limits of the roaming agreement

4.7.2.1 Requirements for the VPMN

In case of:

1. Update Primary or Secondary PDP Context request from the GGSN.
2. Activate secondary PDP Context request from the UE.
3. Update Primary or secondary PDP Context request from the UE.

The VPMN shall negotiate the QoS parameters as described in section 3.6.1.

Note: when VPMN's SGSN receives an "Initiate PDP Context Activation Request", it shall transfer all the required QoS parameters to the UE (except ARPrelease99 or eARP that it should remind for next step) in order for this last one to initiate the "Activate secondary PDP Context request". In that case, the QoS negotiation is performed as described above.

4.7.2.2 Requirements for the HPMN

When a Policy and Charging infrastructure is deployed in the HPMN, then the HPMN's PCRF provides the QoS parameters to the HPMN's GGSN, which are in turn sent to the VPMN as part of all bearer management procedures listed in section 7.1.1.

In order to ensure that the requested QoS sent to a VPMN is within the limits of the roaming agreement, the HPMN's PCRF shall – in case of an outbound roamer - only provide QoS parameters (QCI, ARP, APN-AMBR or GBR and MBR, respectively) to the HPMN's PDN-GW, which are within the limits of the roaming agreement with the respective VPMN.

4.7.3 Enforcement of QoS by the VPMN

If a VPMN has agreed to enforce QoS in a roaming agreement, then the VPMN is required

- To engineer its access and core networks to fulfil the correspondent performance characteristics (Traffic Class, Delivery order, Transfer delay, bit rates, residual bit error ratio…) according to 3GPP TS 23.107 [18].
- To support GBR bearers and provide the requested guaranteed bit rates within the limits as agreed as part of the roaming agreement.

4.8 Security Considerations

4.8.1 GTP Security

The GTP is exposed to attacks through the GRX/IPX Network or through the Internet. Attackers either abuse the GTP interface exposed to the network, or they send their own messages to the network element (NE) in order to receive messages back that reveal information the attackers are interested in. If GTP interfaces are exposed to unauthorised third parties, they can:

- Obtain user information, such as location, encryption key for air interface, and authentication key for air interface;
- Hijack the packet data session of a user;
- Reconfigure network elements and/or take control of them.

All mobile network operators are affected and they are required to deploy the countermeasures that are described below in order to protect their networks, customers, and networks of peer PMN operators.

GTP is spoken in all Releases of the Mobile Network. It depends on the core network which protocol version of the GTP is used for inter-operator signalling. As this document is for LTE and EPC roaming, GTP v2 is covered here.

For security considerations only the interfaces and connections to other networks outside the domain of a mobile network operator are relevant in this document. Key for network security is to protect these. All the others are internal to the mobile network of a single operator and out of scope.

There is the need to protect the network, network elements, services, and the applications on all the layers of the network stack. For security, data link layer, network layer (IP), transport layer (UDP), and the application layer (GTP) of the network stack need to be considered. Some security measures are applied independently on each layer, others are cross-layer measures that deal with multiple layers. Only a comprehensive approach to security will result in an effective counter of any attack. By a secure network architecture, by a strict separation of networks, and by filtering on the network stack, the PMN operator ensures that only the traffic needed and only to/from those communication partners that actually need to talk to the mobile network can enter and leave the domain of the PMN operator. For network element security the PMN operator ensures that all network elements are configured securely to avoid attackers take control of the NE.

In regards to secure network architecture, security on the network stack, separation, filtering, and network element security aspects are common to many networks, network protocols and network elements, and they are covered in the following documents.

- PRD IR.77 [9],
- PRD FS.20 [56],
- 3GPP TS 33.117 [57].

The above documents are applicable and important to the same extent as this section is applicable and important to PMN operators.

Once a communication partner can reach the GTP network service on a PGW, SGW or MME, it is important to define for what purpose the communication is used. While intra-PMN operator communication with GTP reflects the 3GPP S3, S4, S5, S11, and S16 interfaces, communication with roaming partners is based on the 3GPP S8 interface.

A GTP firewall should be deployed between the EPC and the IPX Network. This GTP firewall shall filter GTP messages in a way that only GTP messages that belong to the S8 interface are allowed. All the others shall be discarded and optionally logged. This way it is ensured that no unwanted GTP messages enter or leave the mobile network. A list of GTP messages that belong to the S8 interface can be found in PRD FS.20 [56].

> **Note:** It is good security practice in general to log events of policy violation for potential later fraud detection and prosecution.

The GTP firewall should also be able to detect floods/denial of service attacks and provide means to rate limit GTP-C messages with different levels of granularity e.g. per PGW/SGW, PGW/SGW group, roaming partner, or globally.

GTP message length should be restricted by the GTP firewall to a configurable maximum. This way code injection attacks are made difficult or even impossible.

Whenever possible it should be determined if the GTP messages make sense. If they don't , the messages shall not be processed any further. These plausibility checks are also a task for the GTP firewall.

Useful GTP message validity checks are:

- Presence of mandatory Information Elements (IE);
- Correct sequence of IEs;
- Correctness of message length;
- Correctness of Type-Length-Value (TLV) format of IEs;
- Correctness of GTP version.

Useful GTP message plausibility checks are (see below for explanation):

- Validity of IP addresses in GTP messages;
- Cross layer checks for validity of information that appears in multiple layers (e.g. IP addresses in IP header and GTP message IEs);
- Validity of information in IEs representing the roaming partner (i.e. IP addresses and IMSIs);
- Validity of information in IEs representing a roaming subscriber (i.e. IMSI and MSISDN);
- GTP-in-GTP encapsulation detection.

Validity of IP addresses in GTP messages: To check all the IP addresses inside GTP messages that point to NEs is a particulary useful information. The IEs of a GTP message often contain IP addresses of MME, SGW, PGW, UE, and sometimes even more. These IP addresses are attractive targets for attackers. If attackers can modify them, they are able to redirect traffic to their equipment. The GTP firewall should maintain a so-called *handover group* per peer PMN. That is a list of IP address segments per peer PMN that belong to their NEs. The GTP firewall can determine if IP addresses in GTP messages match a particular handover group. If they do, the messages are considered plausible. If they don't, they shall not be processed any further and an error message shall be returned.

Cross layer checks: Some NEs interpret only some of the information in GTP messages. When a message enters the network at the edge, messages shall be checked for plausibility of information on all layers. If, for example, IP addresses in layer 3 (IP header) differ from IP addresses in respective IEs in the GTP message (layer 5), this is a hint for a forged or mainipulated message. The GTP firewall shall detect and discard these messages.

Validity of information in IEs representing the roaming partner: Several IEs represent the roaming partner. These are IP addresses, MCC, MNC, prefix of IMSI, and APN. The GTP firewall shall check if all this information points to the same roaming partner. If this information is inconsistent, this is a hint for a forged or mainipulated message. The GTP firewall shall detect and discard these messages.

Validity of information in IEs representing a roaming subscriber: Several IEs represent the roaming subscriber. These are IMSI and MSISDN. A suitable NE should check if all this information points to the same roaming subscriber. If this information is inconsistent, this is a hint for a forged or mainipulated message. The network element shall detect and discard these messages.

GTP-in-GTP encapsulation detection: The 3GPP specification does not consider GTP-in-GTP encapsulation. The GTP firewall should detect and discard all encapsulated messages, as some GTP implementations cannot interpret them correctly. These faulty network elements interpret the encapsulated GTP message rather than the outer GTP message. This would allow an attacker to craft their payload that is transported through the mobile network in a way that network elements of the mobile network interpret user payload. This is critical for mobile network integrity and shall be prevented.

An in-depth coverage of GTP security is provided in PRD FS.20 [56].

PRD IR.33 addresses GTPv0 and GTPv1 security for legacy mobile core network.

5 Interworking with the LTE/EPC

All recommendations related to interworking with LTE/EPC are specified in IR.88 [15].

Annex A Known Issues and Solutions

A.1 GTP version 0 and version 1 Interworking Problem

A.1.1 Introduction

When an Operator upgrades its GPRS nodes to GTPv1 it must still provide support for nodes, which support only GTPv0. As such, an Operator will want to try to contact another Operator using GTPv1 first, but if that fails, it should fall back and try GTPv0. The problem comes when trying to establish when to fall back to using GTPv0. This is because GTPv1 runs on different UDP/IP ports than GTPv0 and in the 3GPP standards (specifically 3GPP TS 23.060 [1] and 3GPP TS 29.060 [4]) it is not clearly defined how an SGSN or GGSN discovers whether or not the other supports GTPv1. That is, there is nothing at the application layer (GTP) to negotiate which version of GTP to use. Therefore, an SGSN and GGSN needs to first try contacting the other using GTPv1 and wait for an error at the IP layer to occur before trying to contact it again using GTPv0.

This error at the IP layer is defined in 3GPP TS 29.060 [4] as a time out (T3 RESPONSE multiplied by N3 REQUESTS). However, if an SGSN or GGSN has to wait for a time out to occur before trying GTPv0, then this reduces the amount of time given to the rest of the chain of nodes in a GPRS activation and hence increases the possibility of the UE (or indeed the actual user) giving up on the current PDP Context activation.

To overcome this, it is recommended that Operators should support GTPv1. However, until all PLMNs support GTPv1 it is strongly recommended that the following configuration be made in the network; both from an HPLMN point of view and from a VPLMN point of view.

A.1.2 VPLMN solution

Many SGSN vendors provide a local cache table within each SGSN that can store GTP versions associated with IP addresses. This means that for a configurable time period, the SGSN "knows" which version of GTP the destination GSN supports and so when setting up a GTP connection it does not have to attempt using GTPv1 if it already knows that the destination does not support it.

It is therefore recommended that Operators make full use of such tables within SGSNs. Doing this will reduce the number of re attempts that have to be made to establish a GTP connection.

A.1.3 HPLMN solution

Many firewalls are configured to simply "drop" packets (i.e. do not send back any error to the sender) destined for ports which do not have a service running on them. This means that a GTPv1 capable SGSN in a foreign network trying to contact a GTPv0 only GGSN in a subscriber's home network will have to wait for a specific period of time before re attempting the connection using GTPv0. The same applies for Inter-MNO Operator IP handover when the SGSN in the old network supports GTPv1 and the SGSN in the new network supports only GTPv0.

It is therefore recommended that Operators who do not yet support GTPv1 configure their firewalls on their GGSNs (and/or any border gateways at the edge of the network) to "deny" packets destined for the GTPv1 signalling/control plane port (UDP/IP port 2123) by sending back ICMP message 3 "destination unreachable" with error code 3, "Port unreachable". Doing this will greatly reduce the time taken for an SGSN to realise that the destination does not support GTPv1.

A.2 IP source address of GTPv1 response messages

Unlike GTP version 0, in GTP version 1 the GGSN is allowed to send GTP response messages back to an SGSN with the source IP address set to an IP address different to that which was in the destination address of the associated GTP request message. The change was made in 3GPP to optimize internal processing of GGSNs.

Unfortunately, many firewalls (i.e. GTP-aware stateful firewalls) expect the source IP address of a GTP response message to always be the same as the destination IP address of the respective GTP request message and hence, if the response is received from a different IP address, the firewall will drop the response message and not pass it on for further processing. Note that this behaviour by the firewall is perfectly valid for GTP version 0 where such IP address usage is specifically prohibited.

This can also have adverse effects for PLMNs who implement "traffic engineering" to control and balance their IP traffic.

It is therefore strongly recommended that Operators configure their GGSNs to always respond to GTP request messages using the source IP address that the GTP request message was sent to. If this is not possible, then a range of IP addresses that a GGSN is able to respond from shall be communicated and agreed between the HPLMN and VPLMN.

A.3 GPRS QoS Classes

GPRS Release 97 defines QoS parameters at the HLR level. However, it does not define QoS functionalities (e.g. scheduling in SGSN or GGSN). Furthermore, the GSM radio access network is not aware of subscription details. These facts are noted in 3GPP and a new definition of QoS classes and functions were introduced to GPRS Release 99 (GTPv1).

Mapping of the GPRS Release 97 and Release 99 QoS classes into IP service QoS parameters will be necessary later. Forthcoming GPRS release specific QoS issues should remain open for further study.

For data roaming taking place between two networks of different generations, i.e. 3G (GPRS R99/UMTS) and 2.5G (GPRS R97/98), Service Providers should comply with the IP QoS definitions for GPRS R97/98.

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.0.1	22 June 1999	Table of Contents presented at IREG GPRS #4 meeting and commented upon	IREG	GSMA
0.0.2	20 August 1999	First draft of document for IREG GPRS group discussion (5th Meeting)	IREG	GSMA
1.0	21 September 1999	Issued First Version for approval	IREG	GSMA
1.0.1	22 September 1999	Modified Section 8.2 for approval	IREG	GSMA
2.0	23 September 1999	Approved by IREG#37	IREG	GSMA
3.0	1 October 1999	PL Doc 162/99. Approved at Plenary 42	IREG	GSMA
3.1	27 April 2000	CR#01, PL Doc 032/00 approved at Plenary 43	IREG	GSMA
3.2	3 April 2003	SCR 02	IREG	GSMA
3.3	15 October 2004	SCR 03: New section for descriptions of new GTP features and associated configuration.	IREG	GSMA
3.4	21 July 2009	CR 04: Remove duplicate and redundant information, and general tidy-up.	IREG	GSMA
4.0	30 December 2010	CR 05: Identifying VPLMN when SGSN sharing is used	IREG#59 EMC	Massimo Chiavacci, Telecom Italia Sparkle
5.0	30 March 2011	CR 06: IP Addressing Alignment	Packet #48 IREG #60 DAG #79	Massimo Chiavacci,Telecom Italia Sparkle
6.0	26 May 2011	CR007 - Addition of details from the IPv6 EMC Task Force's IPv6 Transition Whitepaper	DAG#81	Massimo Chiavacci, Telecom Italia Sparkle
7.0	5 June 2014	DAG Doc 99_011 MCR008_to_IR33 “introduction_of_qos_management_in_gprs_roaming” IR.33 CR1001 “IMEISV notification and Automatic Device Detection” & IR.33 CR1002 “Addition of details from the IPv6 EMC Task Force's IPv6 Transition Whitepaper - LBO”	IREG	Vincent Danno, Orange
8.0	20 May 2015	Inclusion of the following CRs: IR.33 CR1003 PDP Types support IR.33 CR1004 VPMN identification For end user billing shall be based on MCC-MNC IR.33 CR1005 Corrections and precisions on QoS parameter negotiation, Editorial changes by PRD editor	Packet #69, #70, #71, #72, #73, #74, #75, #76, #77, #78, #79 IREG #66 IREG #67 NG #1	Nick Russell (BlackBerry Limited), Marc Balon (Orange), Cédric Bonnet (Orange)

9.0	3 November 2016	Inclusion of the following CR: IR.33 CR1006 IP MTU constraints Editorial changes by PRD editor	Packet #80 to #87 NG #2 to #4	Cédric Bonnet (Orange)
10.0	5 July 2017	Inclusion of the following CR: IR.33 CR1007 GTP Security (new section) IR.33 CR1008 Use of common PLMN ID Editorial changes by PRD editor	Packet #88 to #93 NG#5	Sven Lachmund (Deutsche Telekom AG) Cédric Bonnet (Orange)

B.2 Other Information

Type	Description
Document Owner	Networks/Packet
Editor / Company	Cédric Bonnet, Orange

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.