LTE Roaming Guidelines

Version 7.0

31 January 2012

*This is a **Non-Binding** permanent reference document of the GSM Association.*

Security Classification – NON CONFIDENTIAL GSMA Material

Copyright Notice

Antitrust Notice

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

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Scope 5
1.3 Definition of Terms 5
1.4 Document Cross-References 6

2 Architecture 7
2.1 Architecture models 7
2.2 Interfaces 8
2.3 Features 9

3 Technical Requirements and Recommendations For Interfaces 9
3.1 General requirements for Inter-PLMN interfaces 9
3.1.1 Inter-PLMN IP backbone network requirements 9
3.1.2 Stream Control Transmission Protocol (SCTP) 9
3.1.2.1 Introduction 9
3.1.2.2 SCTP Parameters 9
3.1.3 Diameter 11
3.1.3.1 Introduction 11
3.1.3.2 Diameter Agents 11
3.1.3.3 End to End Diameter Architecture 12
3.1.3.4 Diameter Routing 13
3.1.3.5 Diameter Transport Parameter 14
3.2 S8 Interface 14
3.2.1 Procedures 14
3.2.1.1 General 14
3.2.1.2 SGW Selection 15
3.2.1.3 PGW Selection 15
3.2.1.4 Combined SGW/PGW Selection 16
3.2.2 GTP 16
3.2.3 PMIP 16
3.2.4 PMIP-GTP Interworking 16
3.3 S9 Interface 16
3.3.1 S9 implementation requirements 16
3.3.2 Guidelines for Diameter interface over S9 interface 17
3.4 S6a and S6d interface 17

4 Technical Requirements and Recommendations for Legacy Interworking and Coexistence 17
4.1 Legacy Interworking scenarios 17
4.1.1 Introduction 17
4.1.2 VPMN has not implemented LTE 17
4.1.3 HPMN has not implemented LTE 18
4.2 Co-existence scenarios 19
4.2.1 Introduction 19

4.2.2 Possible scenarios 20
4.2.2.1 2G/3G Roaming Agreement Only 20
4.2.2.2 2G/3G and LTE Roaming Agreement 21
4.3 Inter-RAT Handover 23
4.3.1 Introduction 23
4.3.2 Handover to/from 2G/3G and LTE 23
4.3.3 Handover to/from Non-3GPP Accesses and LTE 23
5 Technical Requirements and Recommendations for Services....23
5.1 Introduction 23
5.2 Short Message Service (SMS)....23
5.2.1 SMS over SGs 23
5.3 Voice....24
5.3.1 CS Fallback....24
5.3.1.1 General.... 24
5.3.1.2 Roaming Retry for CS Fallback procedure.... 25
5.3.2 LTE Voice Roaming Architecture....26
6 Other Technical Requirements and Recommendations....27
6.1 Introduction 27
6.2 Access Control....27
6.2.1 Introduction 27
6.2.2 Access Control in the VPMN....27
6.2.3 Access Control in the HPMN....27
6.3 Addressing....28
6.3.1 UE Addressing....28
6.3.1.1 SS7.... 28
6.3.1.2 IP.... 28
6.3.2 Network Element Addressing....29
6.3.2.1 IP and SS7 29
6.3.2.2 Fully Qualified Domain Names (FQDNs).... 29
6.3.2.3 Diameter Realms 29
6.3.3 APN for IMS based services 29
6.3.3.1 Introduction.... 29
6.3.3.2 Definition of the IMS well-known APN 30
6.3.3.3 Gateway selection.... 30
6.3.4 Emergency PDN connection 30
6.4 Security....31
6.5 Hubbing 31
7 TECHNICAL REQUIREMENTS FOR DYNAMIC POLICY AND CHARGING CONTROL....31
7.1 Home Routed architecture and S8 protocol is GTP 31
7.2 Home Routed architecture and S8 protocol is PMIP....33
7.3 Local Break Out architecture....34
8 Annex A: Testing Framework 35
9 Annex B: Diameter Architecture Implementation 35

10 Document Management 40
Document History..40
Other Information 42

1 Introduction

1.1 Overview

This document aims to provide a standardised view on how Long Term Evolution (LTE) networks can interwork in order to provide “Next Generation Mobile Network” capabilities when users roam onto a network different from their HPMN. Expectations of the “Next Generation Mobile Network” capabilities are described in the GSMA Project Document: Next Generation Roaming and Interoperability (NGRAI) Project Scope White Paper [16].

There is much commonality between existing “Data” roaming using General Packet Radio Service (GPRS) and the capabilities and dependencies of LTE. Consequently this document makes references to current 3GPP specifications for GPRS in addition to those specifying solely LTE-Evolved Packet System (EPS) aspects, and also to other GSMA IREG PRDs.

Throughout this PRD, the term "GPRS" is used to denote both 2G GPRS and 3G Packet Switched (PS) service.

1.2 Scope

This PRD presents material about LTE Roaming. The document addresses aspects which are new and incremental to LTE: It recognises that much of the data-roaming infrastructure is reused from GPRS and High-Speed Packet Access (HSPA) Roaming, and for which information and specification is found in other PRDs.

Note: This version of the PRD only covers the LTE-only data-card roaming from LTE access. Roaming from non-3GPP access is not supported in this version of the document.

1.3 Definition of Terms

Term	Description
ARP	Allocation Retention Priority
BBERF	Bearer Binding and Event Reporting Function
BG	Border Gateway
CSFB	Circuit Switched FallBack
DEA	Diameter Edge Agent
DRA	Diameter Routing Agent
EPS	Evolved Packet System (Core)
GBR	Guaranteed Bit Rate
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HPMN	Home Public Mobile Network
HSS	Home Subscriber Server
IP-CAN	IP Connectivity Access Network
LA	Location Area
LTE	Long Term Evolution (Radio)
MAP	Mobile Application Part (protocol)
MME	Mobility Management Entity
MSC	Mobile services Switching Centre
MTC	Mobile Terminating Call
OCS	Online Charging System

PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PGW	PDN (Packet Data Network) Gateway
PMIP	Proxy Mobile IP
QCI	QoS Class Identifier
RTO	Retransmission Timeout (in SCTP)
RTT	Round Trip Time
SCTP	Stream Control Transmission Protocol
SGW	Serving Gateway
TA	Tracking Area
VMSC	Visited MSC
VPMN	Visited Public Mobile Network

1.4 Document Cross-References

Ref	Document Number	Title
1	3GPP TS 23.401	“GPRS Enhancements for E-UTRAN Access”
2	3GPP TS 23.402	“Architecture enhancements for non-3GPP Accesses”
3	IETF RFC 3588	“Diameter Base Protocol”
4	3GPP TS 29.274	“Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3”
5	3GPP TS 29.281	“General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)”
6	3GPP TS 29.215	“Policy and Charging Control (PCC) over S9 reference point”
7	3GPP TS 23.003	“Numbering, addressing and identification”
8	3GPP TS 29.272	“MME and SGSN related interfaces based on Diameter protocol”
9	GSMA PRD IR.77	“Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers”
10	GSMA PRD IR.33	“GPRS Roaming Guidelines”
11	GSMA PRD IR.34	“Inter-PLMN Backbone Guidelines”
12	GSMA PRD IR.40	“Guidelines for IPv4 Addressing and AS Numbering for GRX/IPX Network Infrastructure and User Terminals”
13	IETF RFC 4960	“Stream Control Transmission Protocol”
14	GSMA PRD SE20	“GPRS Data Service Guidelines in Roaming”
15	GSMA PRD BA27	“Charging and Accounting Principles”
16	GSMA NGRAI	“Next Generation Roaming and Interoperability (NGRAI) Project Scope White Paper”
17	3GPP TS 29.303	“Domain Name System Procedures; Stage 3”
18	IETF RFC 3958	“Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)”
19	IETF RFC 3403	“Dynamic Delegation Discovery System (DDDS). Part Three: The Domain Name System (DNS) Database”
20	IETF RFC 5213	"Proxy Mobile IPv6”
21	GSMA PRD IR.67	“DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers”

22	GSMA PRD IR.80	“Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model”
23	3GPP TS 29.275	“Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling Protocols”
24	3GPP TS 29.305	“InterWorking Function (IWF) between MAP based and Diameter based interfaces”
25	3GPP TS 23.272	"Circuit Switched Fallback in Evolved Packet System; Stage 2" Release 9
26	IETF draft-dime-extended-naptr-02	"Diameter Extended NAPTR"
27	3GPP TS 23.018	"Basic call handling; Technical realization" – Release 9
28	3GPP TS 32.425	"Telecommunication management; Performance Management (PM); Performance measurements Evolved Universal Terrestrial Radio Access Network (E-UTRAN)" – Release 9
29	3GPP TS 23.060	"General Packet Radio Service (GPRS); Service description; Stage 2"
30	GSMA PRD IR.92	"IMS Profile for Voice and SMS"
31	GSMA PRD IR.65	"IMS Roaming and Interworking Guidelines"
32	3GPP TS 24.301	"Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3"
33	3GPP TS 23.167	"IP Multimedia Subsystem (IMS) emergency sessions "
34	3GPP TS 23.203	"Policy and charging control architecture" - Release 9

2 Architecture

2.1 Architecture models

The following diagram is produced based on the network diagrams from 3GPP TS 23.401 Section 4.2 [1] and 3GPP TS 23.402 [2] Section 4.2 that define the Architectures for LTE-EPS systems.

There is a range of permutations of the roaming architecture dependent on whether the users’ traffic is Home Routed, broken out from the Visited Network with Home Operator’s application, or broken out from the Visited Network with Visited Operator’s application functions only.

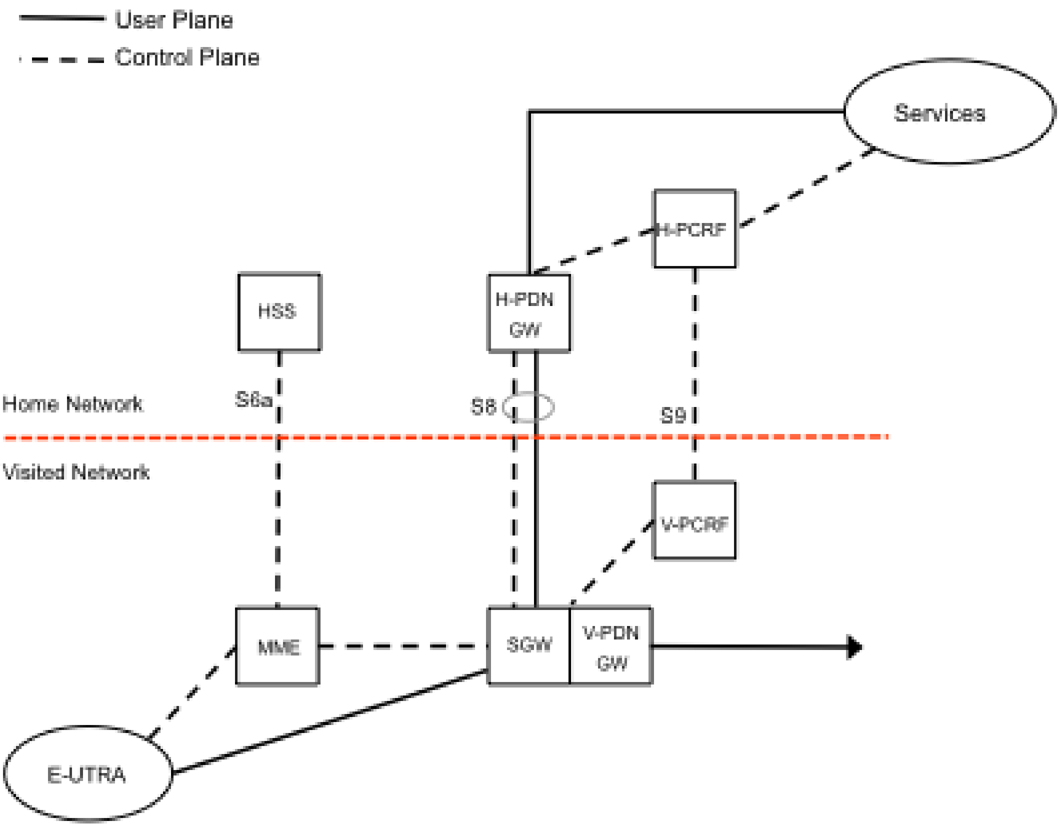

Figure 2.1-1: Roaming Architecture

Note: Roaming from non-3GPP access is not supported in this version of the document.

2.2 Interfaces

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

Nodes	Interface ID	Protocol
MME - HSS	S6a	Diameter Base Protocol (IETF RFC 3588 [3]) and 3GPP TS 29.272 [8])
SGW - PGW	S8	GTP (GTP-C 3GPP TS 29.274 [4] and GTP-U 3GPP TS 29.281 [5]) or PMIP (IETF RFC 5213 [20]) and 3GPP TS 29.275 [23])
hPCRF - vPCRF	S9	Diameter Base Protocol (IETF RFC 3588 [3]) and 3GPP TS 29.125 [6])

Table 2.2-1: Relevant interfaces for LTE roaming

Notes:

- The procedures and message flows for all the above interfaces are described in 3GPP TS 23.401 [1] and 3GPP TS 23.402 [2].
- The Serving GPRS Support Node - Home Subscriber Server (SGSN – HSS) interface may be either S6d (Diameter) or Gr (MAP), depending on co-platform legacy situation.

- The inter-PMN Domain Name System (DNS) communications interface (used by the SGSN to find a Gateway GPRS Support Node (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 [14].

The charging requirements for LTE in a roaming environment are detailed in GSMA PRD BA.27 [15].

2.3 Features

<< Text to be inserted - quick explanations followed by pointers to relevant parts of sections 3 and onwards e.g. ISR, LBO, SMS, Voice. >>

3 Technical Requirements and Recommendations For Interfaces

3.1 General requirements for Inter-PLMN interfaces

3.1.1 Inter-PLMN IP backbone network requirements

The requirements for IP addressing and routing are contained within GSMA PRD IR.33 [10], GSMA PRD IR.34 [11] and GSMA PRD IR.40 [12]. In addition, the GRX/IPX DNS (as per PRD IR.67 [21]) is used.

It is considered that the GRX/IPX is a trusted environment and therefore there is no need for additional security functions over and above those specified in GSM PRD IR.34 [11].

3.1.2 Stream Control Transmission Protocol (SCTP)

3.1.2.1 Introduction

The Stream Control Transmission Protocol (SCTP), as defined in IETF RFC 4960 [13], is specified for the transport of the Diameter Base Protocol (IETF RFC 3588 [3]) in section 7 of 3GPP TS 29.272 [8].

SCTP was originally designed to transport Public Switched Telephone Network (PSTN) signalling messages over IP networks, but is recognised by the IETF as being capable of broader usage.

SCTP is a reliable transport protocol operating on top of a connection-less packet switched network protocol such as IP. It offers the following services to its users:

1. acknowledged error-free non-duplicated transfer of user data,
2. data fragmentation to conform to discovered path MTU size,
3. sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages,
4. optional bundling of multiple user messages into a single SCTP packet,
5. network-level fault tolerance through supporting of multi-homing at either or both ends of an association.

The design of SCTP includes appropriate congestion avoidance behaviour, and a resistance to flooding and masquerade attacks.

3.1.2.2 SCTP Parameters

It is recommended that the IETF default values defined in IETF RFC 4960 [13] Section 15 are used for the following parameters:

Parameter	Value
RTO.Alpha	1/8
RTO.Beta	¼
Valid.Cookie.Life	60 secs
Max.Init.Retransmits	8 attempts
HB.interval (Heartbeat interval)	30 secs
Max.Burst	4
HB.Max.Burst	1

Table 3.1.2.2-1: Table of SCTP Parameters set as in IETF RFC 4960 [13]

The settings of Retransmission Timeout (RTO) and Retransmission Attempt parameters are set to optimise early discovery of path or endpoint failure, while reducing the impact of randomly lost packets.

The setting of the RTO parameters is linked to the engineered Round Trip Time (RTT) for the connection.

- **RTO.min** should be set to the roundtrip delay plus processing needed to send and acknowledge a packet plus some allowance for variability due to jitter; a value of 1.15 times the Engineered RTT is often chosen.
- **RTO.max** is typically 3 times the Engineered RTT.
- **RTO.Initial** is typically set the same as RTO.Max.
- **Path.Max.Retrans** parameter value is the maximum number of retransmissions on a single path, before a path is dropped. It needs to be set large enough to ensure that randomly lost packets to do cause a path to drop accidently. Typical values are 4 Retransmission (per destination address) for a Single-Homed association, and 2 Retransmission (per destination address) for a Multi-Homed association.
- **Association.Max.Returns** parameter value is the maximum number of retransmissions for a give association (which may comprise multiple paths). It is typically set to Path.Max.Retrans times “Number of paths”.

Parameter	Value
RTO.Initial	Value of RTO.Max (IETF RFC 4960 default 3 secs)
RTO.Min	1.15 * Engineered RTT – See notes below (RFC 4960 default 1sec)
RTO.Max	3 * Engineered RTT– See notes below (IETF RFC 4960 default 60 secs)
Association.Max.Retrans	Value of Path.Max.Retrans * Number of paths. (IETF RFC 4960 default 10 Attempts)
Path.Max.Retrans	2 or 4 attempts (per destination address) depending on single/multi Homing architecture (IETF RFC 4960 default 5 attempts per destination address)
SACK Delay	0 sec added (IETF RFC 4960 requirement: Delay must be <500ms)
SACK Frequency	1 (i.e. every packet containing any data chunks is to be acknowledged individually)
Chunk Bundling Time	10-15ms

Table 3.1.2.2-2: Table of SCTP Parameters derived from IETF RFC 4960 [13]

Notes:

- It is recognised that setting RTO parameters per destination is not practical, unless all SCTP traffic is being forwarded to a single or low number of sites handling a “Hub function”.
- GSMA PRD IR.34 Section 8.3.2 [11] contains a table of roundtrip delays between endpoints throughout the world. The maximum value in this table is of the order of 650ms and the minimum value of the order of 50ms.
- The dynamic value of RTO rapidly adjusts to a value marginally greater than the current Round Trip Time (RTT) of the path: the RTO.Initial, RTO.Max and RTO.Min parameter set the boundary conditions for this convergence.
- Accordingly if it is desired to choose a set of universal values for all destinations, then the values of RTO.Max and RTO.Initial should be 2s, and the value for RTO.Min should be set to 60ms. Further experience with the use of SCTP over the GRX/IPX is needed to assess the benefits of tuning RTO parameters.

3.1.3 Diameter

3.1.3.1 Introduction

3GPP TS 23.401 [1] and TS 23.402 [2] define a direct Diameter interface between the network elements of the visited network (Mobility Management Entity (MME), Visited Policy and Charging Rules Function (vPCRF) and SGSN) and the network elements of the home Network (HSS and Home Policy and Charging Rules Function (hPCRF)). Diameter Base Protocol (IETF RFC 3588 [3]) defines the function of Diameter Agents. Diameter Extended NAPTR (IETF draft-jones-dime-extended-naptr-01 [26]) defines enhancements to the Diameter Routing mechanisms.

3.1.3.2 Diameter Agents

In order to support scalability, resilience and maintainability, and to reduce the export of network topologies, the use of a PMN-edge Diameter agent (named Diameter Edge agent hereafter) is strongly recommended; the Diameter agent is considered as the only point of contact into and out of an operator’s network at the Diameter application level. For network level connectivity see section 3.1.1.

The Diameter Base Protocol [3] defines two types of Diameter agent, namely Diameter Relay agent and Diameter Proxy agent.

"Diameter Relay" is a function specialised in forwarding Diameter messages.

- A Relay agent does NOT inspect the actual contents of the message.
- When a Relay agent receives a request, it will route messages to other Diameter nodes based on information found in the message e.g. Application ID and Destination-Realm. A routing table (Realm Routing Table) is looked up to find the next-hop Diameter peer.

"Diameter Proxy" includes the functions of Diameter Relay and the following in addition:

- The biggest difference from Diameter Relay is that a Diameter Proxy CAN process non-routing related AVPs. In other words, a Diameter Proxy can actually process messages for certain Diameter applications.
- Therefore, a Diameter Proxy CAN inspects the actual contents of the message to perform admission control, policy control, add special information elements (AVP) handling.

According to its Realm Routing Table, a Diameter Edge agent (DEA) can act as a Proxy for some Diameter applications (that is add/drop/modify AVP, perform AVP inspection…) while acting as a Relay for all others (that is simply route messages based on Application ID and Destination-Realm). However, one Diameter equipment can only advertise itself as one type of Agent to one Diameter peer.

It is recommended that the Diameter Edge agent advertises the Relay application ID to the outer Diameter peers. By using the Relay, inter PLMN routing is independent from inner domain applications. Note that the Diameter Edge agent is free to advertise the Proxy ID to inner Diameter peers.

It is therefore recommended that any Diameter Edge agent is able to relay or proxy all applications supported by the PMN to inner proxies, inner relays or inner destination agents.

However, if the above mentioned recommendations cannot be implemented by PMN, the PMN may outsource the deployment of Diameter Relay to IPX. The details of this option can be found in GSMA PRD IR.34 [11].

It is strongly recommended to deploy Diameter proxies for each Diameter application supported by the PMN. They can be implemented inside the PMN inner domain, inside the Diameter Edge agent or outsourced to the IPX provider. This is to provide functionalities such as admission control, policy control, add special information elements (AVP) handling.

Annex B provides the implementation examples of the Diameter architecture implementation.

3.1.3.3 End to End Diameter Architecture

Figure 3.1.3.3-1 is a logical architecture that illustrates, at the Diameter application level, the position of the Diameter Edge agent in the PMN. They are the Diameter flow point of ingress to the PMN.

Border Gateways are not presented in this logical architecture as they are not involved in Diameter procedures but the Edge Agents must be secured by the Border Gateways as any other equipment exposed to the GRX/IPX unless they are outsourced to IPX providers.

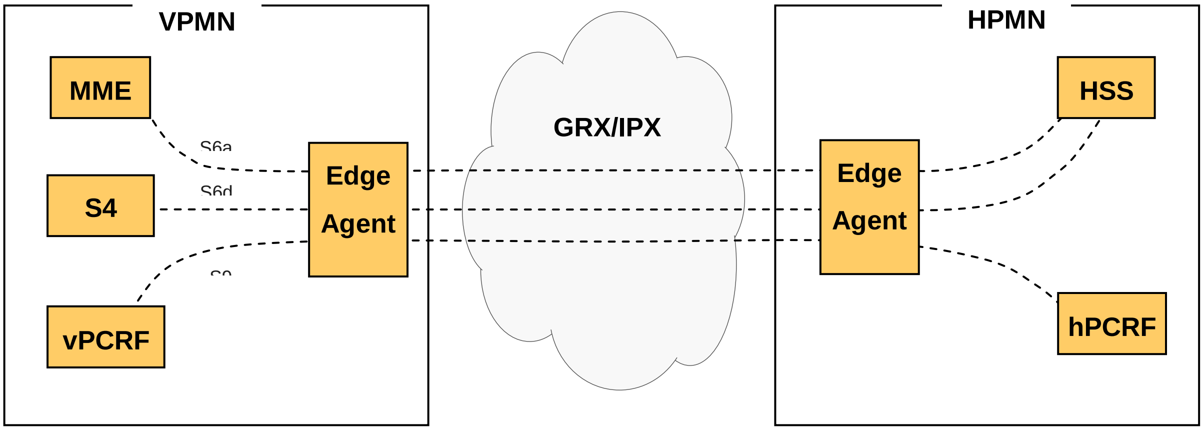

Figure 3.1.3.3-1: Diameter Roaming Implementation Architecture

Figure 3.1.3.3-2 illustrates a possible end to end Diameter Architecture implementation. It is a practical implementation with two Diameter Edge Agents ensuring load balancing and resiliency.

Please refer to Annex B for a complete description of possible architecture implementations.

The interconnection between PMN can be implemented in two modes:

- Bilateral mode with direct peer connections between PMN Edge agent and no IPX agent in between
- Transit mode with PMN interconnection by IPX Agents.

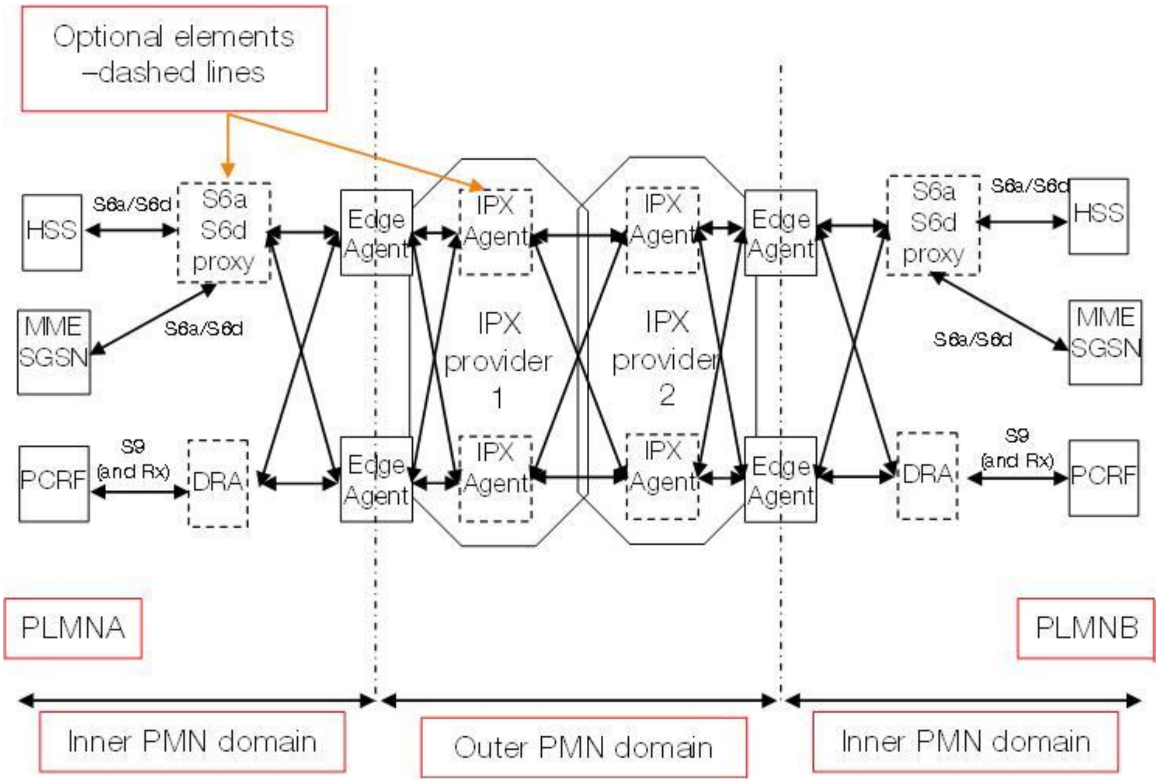

Figure 3.1.3.3-2: End to end Diameter Architecture

3.1.3.4 Diameter Routing

The GRX/IPX DNS (as per PRD IR.67 [21]) is used. The Edge agent can discover the “next hop” agent using the search order recommended in Section 5.2 of IETF RFC 3588 [3] excluding the step 2). This results to the following recommended search order:

1. The Diameter Edge agent consults its list of manually configured Diameter agent locations; this list could derive from the IR.21 DB.
2. The Diameter Edge agent performs a NAPTR query (RFC 3403) for a server in a particular realm (for example, the HPMN or the roaming hub).
    - These NAPTR records provide a mapping from a domain to the SRV record for contacting a server with the specific transport protocol in the NAPTR services field.
    - The services relevant for the task of transport protocol selection are those with NAPTR service fields with values “AAA+D2x”, where x is a letter that corresponds to a transport protocol supported by the domain (D2S for SCTP).
3. If no NAPTR records are found, the requester directly queries for SRV records: _diameter._sctp.<realm>.

The use of NAPTR query (step 2 above) is recommended for Diameter Edge Agent (DEA) discovery (the mechanism used by the outgoing DEA to determine the address on the far-end DEA) in the case of direct bilateral roaming. The realm referred above means the Home

Network Realm of the Root Network Access Identifier (NAI) described in chapter 19 of 3GPP TS 23.003 [7].

When a Roaming Hub is used, then PMNs that are using a Roaming Hub as a “Solution Provider” will need to use Option 1, in order to route all Diameter Application traffic to the Hub for onward routing to their Roaming partners. The Diameter clients such as MMEs can be configured with a default route toward Proxy Agent for traffic destined to other than home realm. (Additional mechanisms may be possible, and this aspect is currently being handled as part of the Hubbing design for Diameter routing.)

Diameter request routing and forwarding decision is always tied to specifically supported applications unless Relay Agents are used. That means a Diameter Edge agent implemented as a Proxy Agent and possible Proxy Agent based Hubs shall support those applications that are required (such as S6a and/or S9) to enable inter-operator roaming. Support for new applications must be added as they are required on the roaming interfaces.

The specific Relay Application ID 0xffffffff (in hexadecimal) as assigned by the IETF needs to be advertised for a Diameter Relay Agent towards a VPMN.

3.1.3.5 Diameter Transport Parameter

It is recommended that the default value defined in section 12 of IETF RFC 3588 [3] is used for Timer Tc, which is 30 seconds. The Tc timer controls the frequency that transport connection attempts are done to a peer with whom no active transport connection exists.

3.2 S8 Interface

3.2.1 Procedures

3.2.1.1 General

The Serving Gateway (SGW) and PDN (Packet Data Network) Gateway (PGW) selection procedures specified for the EPS in 3GPP TS 29.303 [17] include relevant changes with respect to the GGSN discovery procedures defined in previous releases of 3GPP:

- The Release 8 behaviour includes the existing GPRS procedures plus additional functionality since the PGW (as opposed to the GGSN) now can support more than one protocol (GPRS Tunnelling Protocol (GTP) and now Proxy Mobile IP (PMIP)) and there is sometimes a desire to have the PGW and SGW collocated or topologically close to each other with respect to the network topology.
- New DNS records are required to distinguish between different protocols and interfaces and assist in the more complicated selections.

Selection is performed using the S-NAPTR procedure (“Straightforward- Name Authority Pointer (NAPTR)” procedure), which requires DNS NAPTR records to be provisioned as described in IETF RFC 3958 [18].

IETF RFC 3958 [18] describes the Dynamic Delegation Discovery System (DDDS) application procedures for resolving a domain name, application service name, and application protocol to target server and port by using both NAPTR and SRV resource records. It also describes how, following the DDDS standard, the NAPTR records are looked up, and the rewrite rules (contained in the NAPTR records) are used to determine the successive DNS lookups until a desirable target is found.

Note: The S-NAPTR use of the NAPTR resource record is exactly the same as defined in IETF RFC 3403 [19] from the DNS server and DNS infrastructure point of view.

The PMN operator shall provision the authoritative DNS server responsible for the APN-FQDN with NAPTR records for the given APN-FQDN and corresponding PGWs under the APN-FQDN.

Assuming the SGW is in the visiting network and the APN to be selected is in the home network then the S-NAPTR procedure shall use “Service Parameters” that select the interface (S8 in this case) and the protocol (either GTP or PMIP).

In all cases, the S-NAPTR procedure returns an SRV record set (a set of FQDNs identifying potential PGW and SGW candidates), or an A/AAAA record set (IP addresses identifying potential PGW and SGW candidates), or a DNS error.

When provisioning NAPTR records in the DNS, NAPTR flags "a" for A/AAAA records or "s" for SRV records should always be used. The use of NAPTR flag "" should be avoided. If used, the precautions mentioned in Section 4.1.2 of 3GPP TS 29.303 [17] shall be taken into consideration.

3.2.1.2 SGW Selection

SGW selection is performed by the MME/SGSN at initial attach or PDN connection establishment procedure. This occurs in the VPMN or the HPMN (non-roaming scenarios).

SGW selection is performed by using the S-NAPTR procedure with:

- "Service Parameters“ = {desired reference point, desired protocol}
- “Application-Unique String” = the TAI FQDN (per 3GPP TS 23.003 [7])

For example, in a roaming scenario with Home routed traffic (S8) and assuming there is a choice between PMIP and GTP protocols, the MME performs SGW selection using the S-NAPTR procedure with:

- "Service Parameters“ = {"x-3gpp-sgw:x-s8-gtp", "x-3gpp-sgw:x-s8-pmip“}
- “Application-Unique String” = tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Note: Strictly speaking, SGW selection is outside the scope of this PRD, but is applicable during the PGW/SGW collocated case.

3.2.1.3 PGW Selection

3.2.1.3.1 HPMN Roaming

PGW selection is performed by the MME/SGSN at initial attach or PDN connection establishment.

PGW selection is performed by using the S-NAPTR procedure with:

- "Service Parameters“ = {desired reference point, desired protocol}
- “Application-Unique String” = the APN FQDN (per 3GPP TS 23.003 [7])

For example, in a roaming scenario with Home routed traffic (S8) and assuming there is a choice between PMIP and GTP protocols, the MME performs PGW selection using the S-NAPTR procedure with:

- "Service Parameters“ = {"x-3gpp-pgw:x-s8-gtp", "x-3gpp-pgw:x-s8-pmip“}
- “Application-Unique String” = <APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

3.2.1.3.2 VPMN Roaming

<<Text to be added later>>

3.2.1.4 Combined SGW/PGW Selection

For locally routed traffic (local break-out in the VPMN) then PGW/SGW collocation is possible. In this case the MME compares the two record sets (one for PGW and one for SGW candidates) and looks for a match of the canonical-node name (which conveys a collocated SGW/PGW):

- If there are multiple PGW/SGW collocated nodes in the 2 record-sets, weights and priorities are used to select the optimal collocated PGW/SGW that serves the user's cell.
- If there is a failure to contact the collocated node, the non-collocated nodes are used.

3.2.2 GTP

The S8 interface (GTP based) uses GTP version 1 for the User plane, and GTP version 2 for the Control plane. Nodes supporting the S8-GTP based interface are compliant to 3GPP TS 29.274 [4] Release 8 or later, and 3GPP TS 29.281 [5] Release 8 or later. Accordingly drop-back to GTP version 0 is no longer supported; this has significance if hybrid networks containing legacy nodes are sharing infrastructure.

3.2.3 PMIP

Nodes supporting the S8-PMIP based interface are compliant to 3GPP TS 23.402 [2] and 3GPP TS 29.275 [23] Release 8 or later.

3.2.4 PMIP-GTP Interworking

The PMIP-GTP interworking is not supported by 3GPP specifications. The PMN supporting PMIP must deploy GTP based S8 or Gp interface in order to interwork with GTP-S8/Gp based PMN, unless the GTP-S8 based PMN also deploys PMIP based S8.

3.3 S9 Interface

3.3.1 S9 implementation requirements

The S9 interface implementation can be necessary if the service requires dynamic policy and charging control from the HPMN.

S9 existence depends on the roaming architecture and S8 protocol.

S8 protocol Architecture	GTPv2	PMIP
Home Routed	Not required	Required (NOTE 1)
Local Break Out	Required (NOTE 1)only if dynamic policy and charging control with home network control is required)	Required (NOTE 1)

NOTE 1: only if dynamic policy and charging control with home network control is required

Table 3.3.1-1: S9 interface implementation

3.3.2 Guidelines for Diameter interface over S9 interface

The S9 interface between PCRFs implements Diameter. Parameters and guidelines for the Diameter protocol will be same as those of S6a (see sections 3.1.3 and 3.4).

3.4 S6a and S6d interface

For S6a interface, the guidelines described in section 3.1.3 apply.

Note: S6d interface is "out of scope" in this version of GSMA PRD IR.88.

4 Technical Requirements and Recommendations for Legacy Interworking and Coexistence

4.1 Legacy Interworking scenarios

4.1.1 Introduction

It is anticipated that most commercial LTE-device roaming configurations will use Release 8 (or later) capabilities at the Home and Visited networks (in HSS, SGW, PDN Gateway, and if applicable PCRFs).

There are two options for the support of authentication, registration and subscription download when roaming to Release 8 SGSNs. This architecture will typically occur when both networks support LTE. The two options are to either continue using MAP based Gr interface, or to use the Diameter based S6d interface.

4.1.2 VPMN has not implemented LTE

In cases where the Visited Network has not implemented LTE, then the roaming takes place in accordance with GPRS/HSPA recommendations. In particular:

- It is assumed that the MAP-Diameter IWF function is performed by the EPS operator.
- The PDN Gateway in HPMN implements the Gp interface towards the SGSN in VPMN.
- The HPMN implements the Gr interface or supports Gr functionality via an IWF to enable the authentication of its customers in the VPMN.
- From the 2G/3G VPMN, the EPS HPMN “looks like” a GPRS network.
- No changes to the existing GTPv1 and MAP roaming interfaces at the VPMN are required.

The architecture is shown on Figure 4.1.2-1 below:

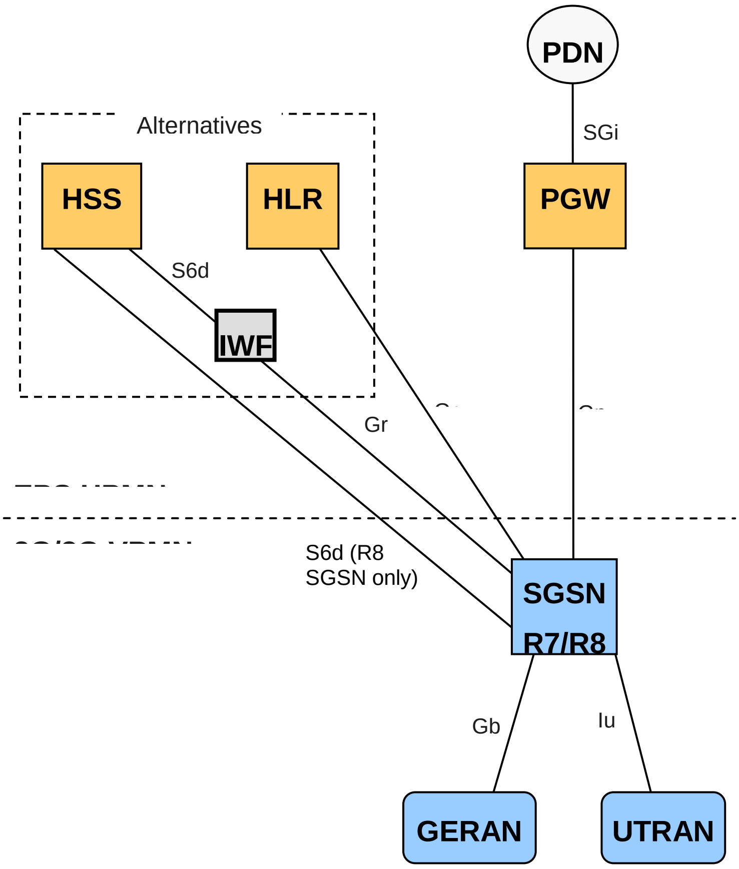

Figure 4.1.2-1: VPMN Legacy Roaming Architecture

4.1.3 HPMN has not implemented LTE

In cases where the Home Network has not implemented LTE, then it is likely that the VPMN and the HPMN have not signed an LTE addendum to their Roaming Agreement. Such a case is described in section 6.2.2 and the HPMN subscribers shall not be allowed to attach to the Enhanced Universal Terrestrial Radio Access Network (E-UTRAN). This does not prevent the customers of the 2G/3G HPMN accessing the home routed application by attaching to the 2G/3G networks in the VPMN (if available and a 2G/3G roaming agreement exists with the HPMN).

It has to be noted that service disruption risk for inbound roamers is very high in that scenario as the customers of the 2G/3G HPMN cannot use the E-UTRAN deployed in the VPMN for Home-Routed applications. Home-Routing support would require an IWF between S8 and Gp but the feasibility of such IWF has not been studied by 3GPP.

However in the case where Home Network has not implemented LTE, and customers use local break-out in the VPMN **for all data services**, then the customers of the 2G/3G HPMN can use the E-UTRAN accesses deployed in the VPMN if the following conditions are met (3GPP TS 29.305 [24]):

- There is an explicit agreement with the HPMN to allow this roaming scenario.
- The HPMN is fully aware that none of the services requiring Home Routing will work.
- The VPMN (or the HPMN, or a third party) has deployed an IWF between S6a and Gr (a MAP-Diameter translator).

- The MME in VPMN can do the mapping of the subscription data for Gn/Gp SGSN provided by the HLR.
- The HLR has been upgraded with support for LTE security parameters (KASME) and supports Gr+ interface (Release 8 or latter shall be supported).

The architecture is shown in Figure 4.1.3-1 below:

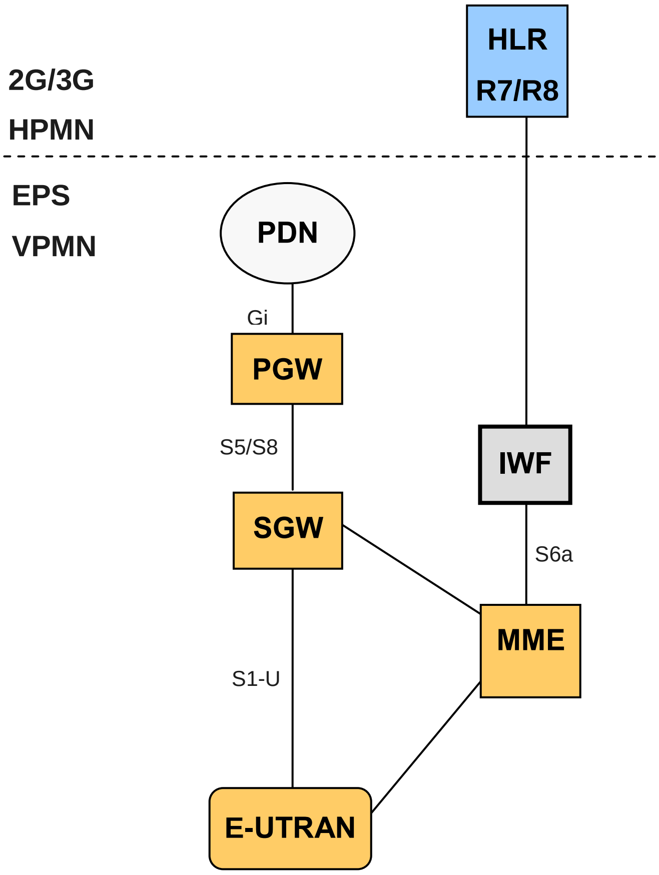

Figure 4.1.3-1: HPMN Legacy Roaming Architecture (local break-out)

4.2 Co-existence scenarios

4.2.1 Introduction

It is anticipated that both LTE roaming and 2G/3G roaming are provided at the same time between two PMNs, or, both or either PMNs may have deployed LTE but they only have 2G/3G roaming agreement.

This section describes roaming scenarios when LTE co-exists with 2G and 3G, and provides technical guidelines for operators to provide interconnectivity regardless of which kind of architecture the either side deploys.

Which scenario to adopt must be agreed between two PMNs as part of their bilateral roaming agreement. The deployment of any other roaming scenarios is not recommended.

4.2.2 Possible scenarios

4.2.2.1 2G/3G Roaming Agreement Only

The following network configurations are allowed, if there is only 2G/3G roaming agreement between two PMNs. When two PMNs have only 2G/3G roaming agreement, only the use of Gp interface is allowed.

Note: For simplicity, HSS is omitted in the figures.

Scenario 1: Legacy GPRS Roaming

This scenario depicts a legacy GPRS roaming model which SGSN has Gp interface towards GGSN only. HPMN may also have PGW for internal use, but that is not used for roaming in this case.

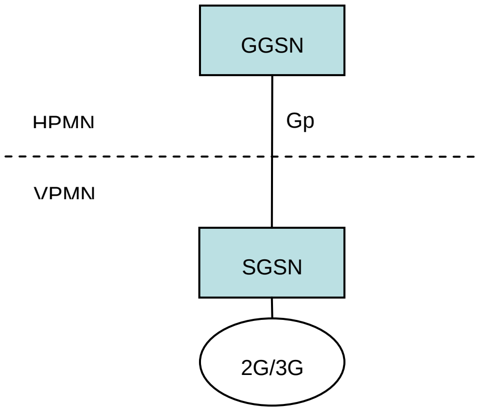

Figure 4.2.2.1-1: Scenario 1 - Legacy GPRS roaming

Scenario 2: HPMN only has PGW as the gateway for roaming

This scenario depicts a case where SGSN has Gp interface towards PGW only. HPMN may also have GGSN for internal use, but that is not used for roaming in this case.

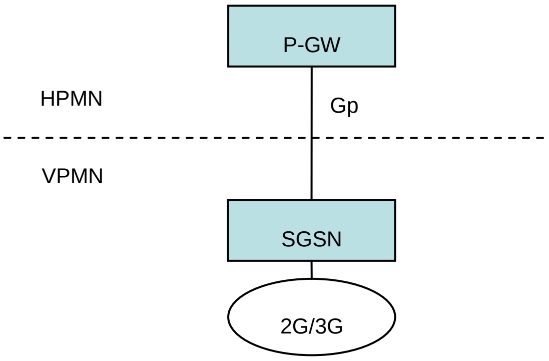

Figure 4.2.2.1-2: Scenario 2 - HPMN only has PGW as the gateway for roaming

Scenario 3: HPMN has both GGSN and PGW as the gateway for roaming

This scenario depicts a case where SGSN has Gp interface towards GGSN and PGW. The SGSN can select between using GGSN and PGW if the HPLMN uses different APNs for GGSN compared to PGW. If the HPLMN uses the same APNs on both GGSN and PGW, then VPLMN SGSN must use UE-capability as follows: If UE is LTE capable, then PGW must be selected, and if the UE is only 2G/3G capable, GGSN must be selected.

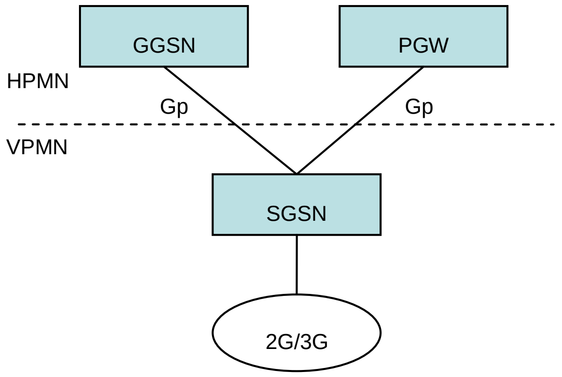

Figure 4.2.2.1-3: Scenario 3 - HPMN has both GGSN and PGW as the gateway for roaming

4.2.2.2 2G/3G and LTE Roaming Agreement

The following network configurations are allowed, if there is LTE and 2G/3G roaming agreement between two PMNs. When two PMNs have LTE and 2G/3G roaming agreement, Inter-RAT handover must be made available. Also, 2G/3G access via both Gp and S8 interfaces towards PGWs in one PMN is prohibited that is a VPMN can only have either Gp or S8 towards PGWs in HPMN.

Note: For simplicity, HSS and PCRF are omitted in the figures.

Scenario 1: HPMN only has PGW as the gateway for roaming, 2G/3G Access via Gp interface.

This scenario depicts a case where SGSN has Gp interface towards PGW and SGW has S8 interface towards PGW. In this scenario, Inter-RAT handover is anchored at PGW. HPMN may also have GGSN for internal use, but that is not used for roaming in this case.

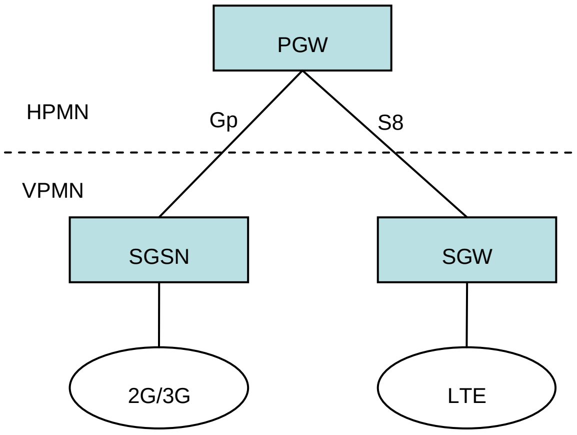

Figure 4.2.2.2-1: Scenario 1 - HPMN only has PGW as the gateway for roaming, 2G/3G Access via Gp interface

Scenario 2: HPMN has both GGSN and PGW as the gateway for roaming, 2G/3G Access via Gp interface.

This scenario depicts a case where SGSN has Gp interface towards PGW and GGSN, and SGW has S8 interface towards PGW. In this scenario, 2G/3G data access will be provided over Gp interface, and Inter-RAT handover is anchored at PGW.

The SGSN can select between using GGSN and PGW if the HPLMN uses different APNs for GGSN compared to PGW. If the HPLMN uses the same APNs on both GGSN and

PGW, then VPLMN SGSN must use UE-capability as follows: If UE is LTE capable, then PGW must be selected, and if the UE is only 2G/3G capable, GGSN must be selected.

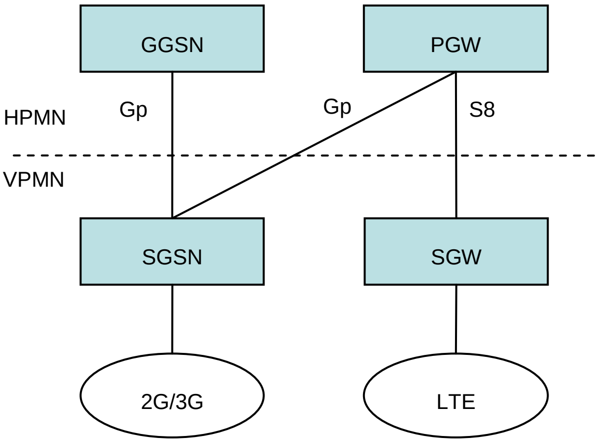

Figure 4.2.2.2-2: Scenario 2 - HPMN has both GGSN and PGW as the gateway for roaming, 2G/3G Access via Gp interface

Scenario 3: HPMN has only PGW as the gateway for roaming, 2G/3G Access via S4/S8 interfaces.

This scenario depicts a case where SGSN has S4 interface towards SGW, and SGW has S8 interface towards PGW. In this scenario, Inter-RAT handover is anchored at SGW if SGW doesn't change or PGW if SGW changes. HPMN may also have GGSN for internal use, but that is not used for roaming in this case.

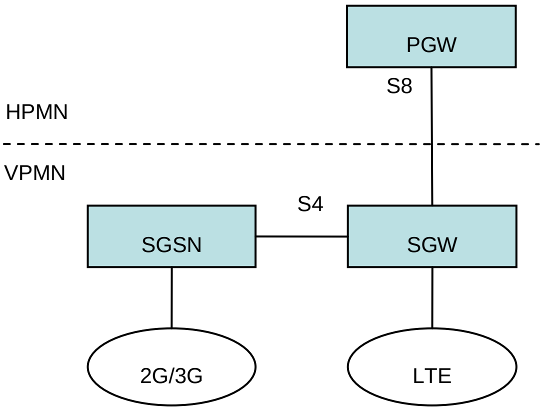

Figure 4.2.2.2-3: Scenario 3 - HPMN has only PGW as the gateway for roaming, 2G/3G Access via S8 interface

Scenario 4: HPMN has both PGW and GGSN as the gateway for roaming, 2G/3G Access via S4/S8 or Gp interfaces.

This scenario depicts a case where SGSN has S4 interface towards SGW and also Gp interface towards GGSN, and SGW has S8 interface towards PGW. In this scenario, Inter-RAT handover is anchored at SGW if SGW doesn't change, or PGW if SGW changes.

The SGSN can select between using GGSN and SGW/PGW if the HPLMN uses different APNs for GGSN compared to PGW. If the HPLMN uses the same APNs on both GGSN and PGW, then VPLMN SGSN must use UE-capability as follows: If UE is LTE capable, then SGW/PGW must be selected, and if the UE is only 2G/3G capable, GGSN must be selected.

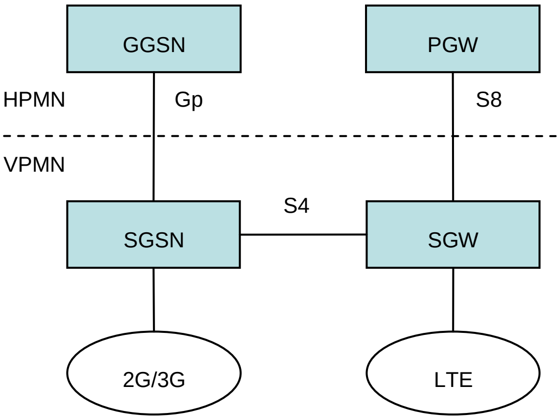

Figure 4.2.2.2-4: Scenario 4 - HPMN has both PGW and GGSN as the gateway for roaming, 2G/3G Access via S8 or Gp interface

4.3 Inter-RAT Handover

4.3.1 Introduction

<<Text to be added later>>

4.3.2 Handover to/from 2G/3G and LTE

<<Text to be added later>>

4.3.3 Handover to/from Non-3GPP Accesses and LTE

<<Text to be added later>>

5 Technical Requirements and Recommendations for Services

5.1 Introduction

<<Text to be added later>>

5.2 Short Message Service (SMS)

5.2.1 SMS over SGs

SMS over SGs is a means to provide C-Plane based SMS over LTE access without forcing UE to fall back to overlay 2G/3G accesses. SMS over SGs is defined in 3GPP TS 23.272 [25].

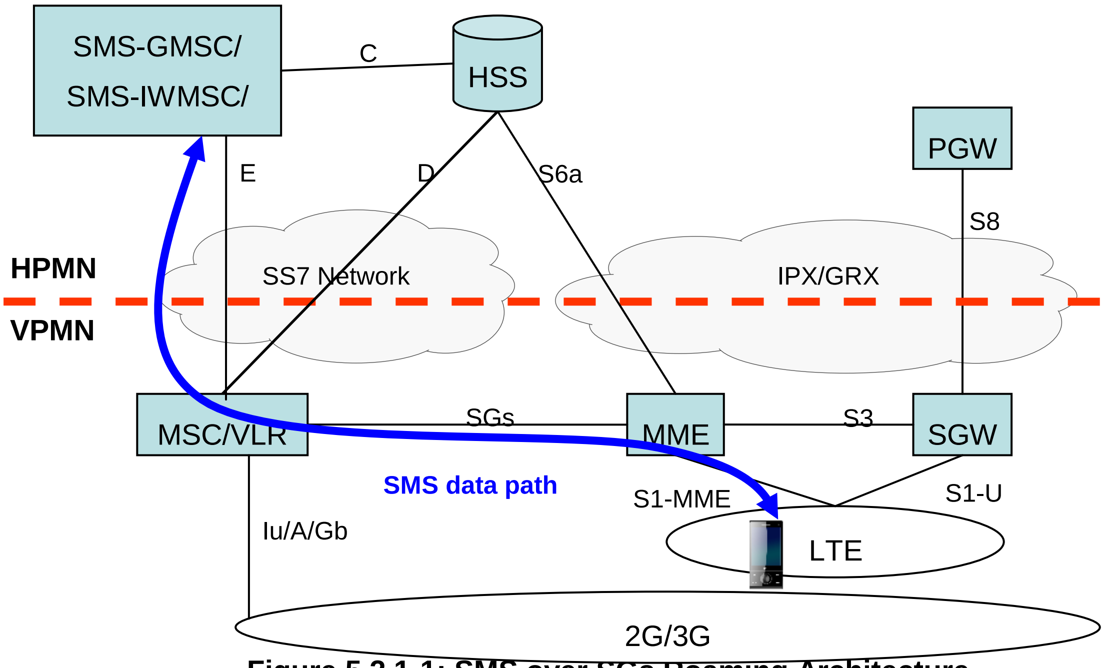

Figure 5.2.1-1: SMS over SGs Roaming Architecture

When SMS over SGs is provided for roaming, existing roaming interfaces for SMS services (E interface) will be used without any changes. Therefore, there is no new guideline required for SMS over SGs.

5.3 Voice

5.3.1 CS Fallback

5.3.1.1 General

In some initial deployments, there will be no support of voice services on LTE. However, operators still want users on LTE to participate in voice calls. This can be achieved by providing CS Fallback procedures. CS Fallback is defined in 3GPP TS 23.272 [25], in 3GPP TS 23.018 [27] sections 5.2.1 and 5.2.2, and is introduced as an 'interim' solution before VoLTE is deployed. Release 9 compliant CS Fallback implementation is recommended for voice fallback as some of Release 8 implementations are not deemed to be efficient enough.

During the CS Fallback procedure, UE camping in LTE will be handed over to overlay 2G/3G access right after the call request is made. CS Fallback can be used for voice, Location Services (LCS) and Call-Independent supplementary services (e.g. USSD).

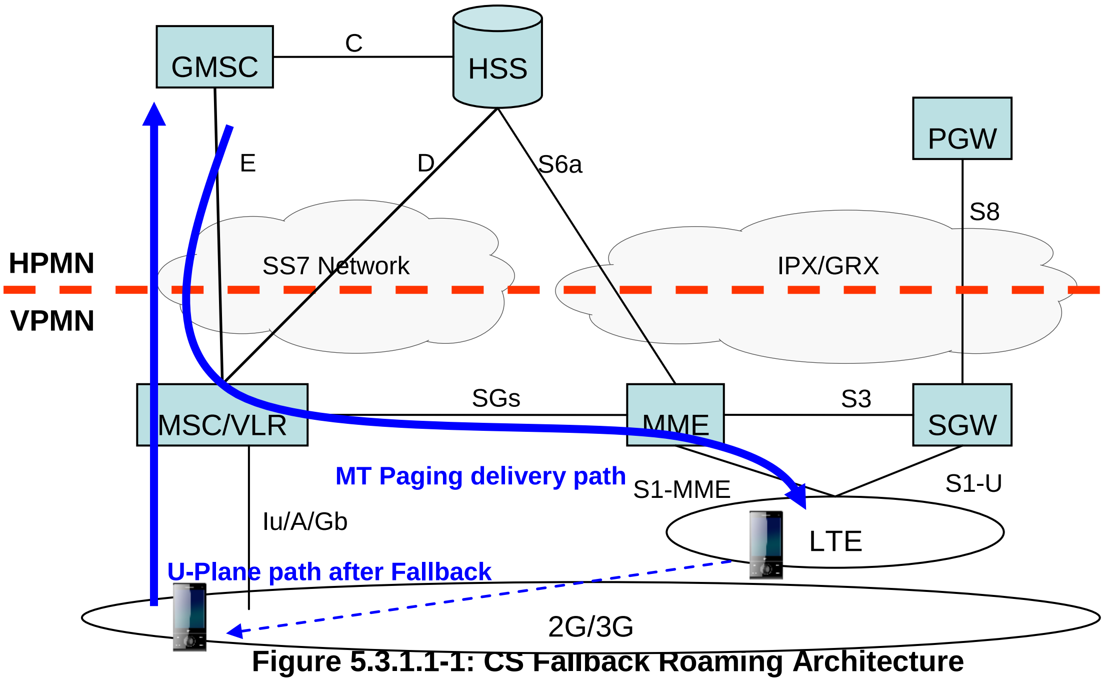

Figure 5.3.1.1-1: CS Fallback Roaming Architecture

When CS Fallback is provided for roaming, the Roaming Retry procedure can be implemented in the VPMN and the HPMN; it impacts the roaming interfaces (see next section for the procedure description).

Roaming Retry implementation is highly recommended since it increases the Mobile Terminating Call (MTC) success rate. If the Roaming Retry procedure is not implemented then the existing roaming interfaces for circuit switched services will remain unchanged.

5.3.1.2 Roaming Retry for CS Fallback procedure

The Roaming Retry procedure for CS Fallback is specified in chapter 7.5 of 3GPP TS 23.272 [25].

Both VPMN and HPMN can implement the Roaming Retry procedure to avoid Mobile Terminating Call (MTC) failures as explained below. In particular, HLR/HSS, Gateway MSC (GMSC) and Visited MSC (VMSC) shall support the procedure as specified in 3GPP TS 23.272 [25].

The Roaming Retry procedure impacts on the roaming interfaces are listed below.

D interface modification:

The HLR/HSS must send the MT Roaming Retry Information Element in the MAP Provide Roaming Number message.

E Interface implementation:

The E interface between the VPMN and HPMN must be implemented. The GMSC and VMSC must support the Resume Call Handling MAP procedure. So far, the E interface between PMNs has never been implemented. IREG will update or create the processes including test specification, IR.21 and other documents to make sure that this new interface is correctly implemented and remains operational.

The entire concept of CS Fallback relies on a careful and combined radio engineering of the Location Areas and Tracking Areas at the MSC (pool) area boundaries. More precisely, the Tracking Areas (TA) at MSC pool area boundaries must be configured such that they do not extend beyond the coverage of the corresponding Location Areas (LA).

The following figure illustrates a LA-TA misalignment on the MSC coverage boundaries.

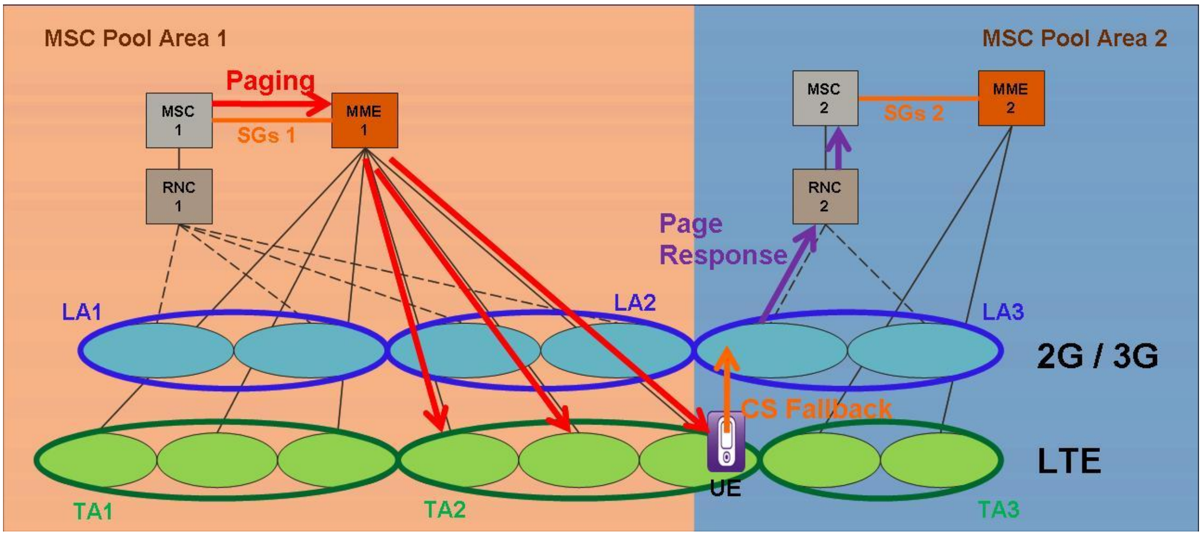

Figure 5.3.1.2-1: CS Fallback issue due to TA/LA misalignment

When the TA coverage extends beyond the LA one then there will be some cases where the UE will actually fall-back on a 2G/3G cell belonging to another MSC than the one where it registered during the combined EPS/IMSI Attach or the combined Tracking Area Update/Location Area Update. For instance, the UE registered under TA2/LA2 of MSC1 receives a paging for an MTC, falls-back to 2G/3G and may eventually reselects a cell in LA3 of MSC2. In such situation, the UE will send the paging response to MSC2, which is not aware of the call establishment and does not have the subscriber's profile. So without Roaming Retry procedure, such MTC would fail.

Roaming Retry allows transferring the incoming call from MSC1 to MSC2, so that MSC2 will understand the paging response and being able to setup the call. In this case, the call setup time will increase (compared to the case where the UE is under the coverage of the MSC it is registered in), but the call will be successful.

It is not realistic that LTE and 2G/3G radio coverage could perfectly match. Note that the issue occurs only at MSC boundaries so MSC pools decrease the number of the occurrence of such issue as there are shorter boundaries. But it does not fix it completely unless there is only one pool in the whole VPLMN. 3GPP also defined a method to help operators keep Las and TAs in alignment. This is described in TS 32.425 [28] from Rel-9 and onward in chapter 4.9.1. This method facilitates the configuration of TA boundaries with LA boundaries by gathering statistics in E-UTRAN (from the inbound inter-RAT mobility events of all UEs) of the most common LAs indicated in the Radio Resource Connection signalling.

5.3.2 LTE Voice Roaming Architecture

To support LTE Voice roaming (as defined in IR.65), both the PGW and the Proxy-Call Session Control Function (P-CSCF) are located in the visited PLMN. In order to select the correct PGW in the visited PLMN, the home PLMN operator has to allow its LTE Voice subscribers to use visited PLMN addressing. See section 6.3.3 for detailed discussion related to gateway selection and a "well-known" Access Point Name usage related to LTE Voice Roaming.

The architecture also assumes that the PCC framework is deployed as an integral part of the IMS services in general. If the visited PCRF requires guidance and confirmation from the home network, then Dynamic PCC and the corresponding S9 interface need to be deployed to exchange policy information between the vPCRF and the hPCRF.

6 Other Technical Requirements and Recommendations

6.1 Introduction

<<Text to be added later>>

6.2 Access Control

6.2.1 Introduction

<< Text to be added later >>

6.2.2 Access Control in the VPMN

Without an explicit agreement from the HPMN, the VPMN must block the access of Inbound roamers into their LTE access network. This is compulsory to ensure roamers will not experience any service disruption because the necessary technical requirements have not been implemented and tested with the HPMN.

The VPMN shall implement the same access control feature that exists today in MSC and SGSN. One mechanism to achieve this is based on the IMSI range. In this mechanism, the subscriber is either rejected (with the appropriate reject cause (as defined in 3GPP TS 24.301 [32])) or allowed to “Attach” and perform the subsequent Tracking Area Update procedures.

If the procedure shall be rejected, then the appropriate error cause is:

- Cause #15 (no suitable cells in Tracking Area) if the Visited Public Mobile Network (VPMN) already have a Roaming Agreement with the HPMN covering other Radio Access Technology (RAT)s. It forces the User Equipment (UE) to reselect another RAT in the same PMN.
- Cause #11 (PMN Not Allowed) if the VPMN has no roaming agreement with the Home Public Mobile Network (HPMN). It forces the UE to perform a PMN reselection. UE shall store the PMN identity in the "forbidden PMN list" in the card and the UE shall no more reselect this PMN. The cause #13 may also be used (to avoid permanent storage of PMN in the Forbidden PMN file in the SIM card).

6.2.3 Access Control in the HPMN

If the VPMN does not implement the above requirements then the HPMN should also implement its own access control feature in the HSS to protect its subscribers.

Based on the error code received in the Update Location Acknowledge message as described in Section 5.2.2.1 of 3GPP TS 29.272 [8], it is possible to limit access to certain RAT types of VPMN. The MME shall map it to appropriate error cause values as follows:

- The “RAT Not Allowed” error code shall be mapped to cause #15 (no suitable cells in Tracking Area) if the VPMN already have a roaming agreement with the HPMN covering other RAT types. It forces the UE to reselect another RAT in the same PMN.
- The “Roaming Not Allowed” error code shall be mapped to cause #11 (PMN Not Allowed) if the VPMN has no Roaming Agreement with the HPMN. It forces the UE to perform a PMN reselection. UE shall store the PMN identity in the "forbidden PMN list" in the card and the UE shall no more reselect this PMN.

6.3 Addressing

6.3.1 UE Addressing

6.3.1.1 SS7

An LTE capable UE may be assigned an MSISDN (optional because it is an optional element on the S6a interface). However, it must be assigned an MSISDN by the HPMN in any of the following conditions:

- The UE is 2G CS capable, 3G CS capable or both (i.e. capable to establish/receive CS calls).
- The UE is capable of SMS.

6.3.1.2 IP

Every LTE capable UE is allocated (either statically or dynamically) one or more IP addresses (at least one per PDN Connection). The requirements in GSMA PRD IR.40 [12] must be adhered to for IP addresses used.

For the type of IP address allocated (that is public or private) and the method by which an address is assigned (that is statically or dynamically), the requirements and recommendations in GSMA PRD IR.33 [10] section 3.1.4.1 apply with the following exceptions:

- Where "PDP Context" is used, this should be interpreted as "PDN connection".
- Where "GGSN" is used, this should be interpreted as "P-GW".
- Where "SGSN" is used, this should be interpreted as "MME".

The version of IP address(es) allocated (that is IPv4 or IPv6) depends on the PDN Types requested by the UE and supported in the core network. The requirements and recommendations in GSMA PRD IR.33 [10] section 3.1.5 apply with the following exceptions:

- Where "PDP Context" is used, this should be interpreted as "PDN connection".
- Where "PDP Type" is used, this should be interpreted as "PDN Type".
- Where "GGSN" is used, this should be interpreted as "P-GW".
- Where "SGSN" is used, this should be interpreted as "MME and SGW".

Note 1: The MME and SGW are assumed to always support the same PDN Types, since they are always in the same network that is VPMN.

Note 2: Unlike the Gn/Gp SGSN, the MME/SGW and S4-SGSN must support the PDN/PDP Type of IPv4v6. The PDN/PDP Type of IPv4v6 is specified in 3GPP TS 23.401 [1].

In addition to the above, for PMNS that have UMTS and/or GSM and deploy their LTE/EPC with IPv6 support must also support handover of IPv6 bearers to UMTS/GSM.

6.3.2 Network Element Addressing

6.3.2.1 IP and SS7

LTE is designed to be an "all IP" architecture. Thus, all LTE network elements require an IP address. The requirements in GSMA PRD IR.34 [11], GSMA PRD IR.33 [10] and GSMA PRD IR.40 [12] shall apply for the routing and addressing used for the S6a, S8 and S9 interfaces. Internal addressing and routing is a decision for the Service Provider.

Although LTE was designed to be an "all IP" architecture, some network elements also support SS7 too for legacy interworking for example S4-SGSN. Thus, such nodes will continue to require an SS7 Global Title.

6.3.2.2 Fully Qualified Domain Names (FQDNs)

All LTE network elements that have an IP address, in the most part are assigned one or more FQDNs (the number is generally based on the number of interfaces). The following FQDNs as defined in 3GPP TS 23.003 [7] are mandatory in order to enable discovery by another node, and should be provisioned on the PMN's DNS Server which is used by roaming partners:

- APN-FQDN
    - format is: <APN NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- TAI-FQDN
    - format is: tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC> .mcc<MCC>.3gppnetwork.org

Recommendations on FQDNs for LTE network elements can be found in GSMA PRD IR.67 [21] and 3GPP TS 23.003 [7].

6.3.2.3 Diameter Realms

All LTE nodes that have an interface that use a Diameter based protocol need to have a Diameter realm associated with them. Diameter realms have the appearance of a domain name or FQDN, in that they consist of labels separated by dots. However, in essence they are another form of addressing. Diameter realms can be resolved using DNS, but this is optional (see section 3.1.3 for more information on when Diameter realms in LTE need to be provisioned in DNS).

Recommendations on Diameter realms for LTE network elements that have an interface that utilise a Diameter based protocol can be found in GSMA PRD IR.67 [7] and 3GPP TS 23.003 [21].

6.3.3 APN for IMS based services

6.3.3.1 Introduction

To facilitate roaming for IMS based services, especially Voice over LTE roaming, an IMS “well-known” Access Point Name (APN) used for IMS services is defined below. For more details on when this is used, see GSMA PRD IR.65 [31] (for the general case) and GSMA PRD IR.92 [30] (for Voice over LTE roaming).

6.3.3.2 Definition of the IMS well-known APN

The APN name must be “IMS”, which is also the APN Network Identifier part of the full APN. The APN Operator Identifier part of the full APN depends on the PLMN whose PGW the UE is anchored to. For IMS emergency calls/sessions, see section 6.3.4.

6.3.3.3 Gateway selection

When enabling IMS roaming for a subscriber, the following subscription settings must be taken into account:

- The bar on “All Packet Oriented Services” is not active
- The bar on “Packet Oriented Services from access points that are within the roamed to VPMN” is not active
- The "VPLMN Address Allowed" parameter in the HSS is set on a per VPMN basis. The HPMN must set the "VPLMN Address Allowed" parameter for the IMS "well known" APN only if a roaming agreement for IMS voice is in place between the HPMN and that VPMN and the user is subscribed to an IMS service that requires it. The VPMN must allow for the "VPLMN Address Allowed" setting for the IMS "well known" APN in the VPMN.

Note: The term ‘access point’ is used to indicate the PGW or part of the PGW that is specified by a particular APN.

If the IMS well-known APN is set to the default APN, then the gateway selection logic follows the "Default APN was selected" procedures described in Annex A.2 of 3GPP TS 23.060 [29]. If IMS services are revoked for a subscriber whose Default APN is the IMS well-known APN, then the Default APN needs to be set to a different APN or else, the subscription barred completely. This is to prevent a complete denial of service to the subscriber and unnecessary traffic on the RAN and CN.

If the UE provides the IMS “well-known” APN (because it is not the default APN), then the gateway selection logic follows the “An APN was sent by the MS” procedures described in Annex A.2 of 3GPP TS 23.060 [29]. The UE should not provide the APN Operator Identifier so that the expected gateway selection logic will be the same as in the case where the network provided the IMS well-known APN as the Default APN. Further details on UE using the IMS well-known APN in Voice over LTE deployments are in GSMA PRD IR.92 [30].

6.3.4 Emergency PDN connection

An emergency PDN connection is established to a PDN GW within the VPLMN when the UE wants to initiate an emergency call/session due to it detecting the dialling of a recognised emergency code (similar to how TS12 calls are recognised by UEs in CS). Any APN included by the UE as part of the emergency request is ignored by the network. This is further detailed in 3GPP TS 23.167 [33], Annex H. The emergency PDN connection must not be used for any other type of traffic than emergency calls/sessions. Also, the APN used for emergency calls/sessions must be unique within the VPLMN, and so must not be any of the well-known APNs or any other internal ones than what is used for emergency. Whilst the 3GPP standards do not provide any particular APN value, the value of “sos” is recommended herein. The APN for emergency calls/sessions must not be part of the allowed APN list in the subscription. Either the APN or the PDN GW address used for emergency calls/sessions must be configured to the MME/SGSN.

6.4 Security

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 Provider in a network, it requires that every single Provider is fulfilling their part of the requirements.

As GRX/IPX (as defined in GSMA PRD IR.34 [11]) is thought to be a secure and reliable Roaming/Interworking Network, no extra features, such as IPSec, are needed in the Service Provider to Service Provider interface. It is still highly recommended to implement adequate security tools and procedures to prevent, monitor, log and correct any potential internal security breaches at all levels. Typically, this means as minimum implementing FW (BG is typically used in MNO (Mobile Network Operator) networks) to implement ACL (Access Control Lists) or similar mechanisms to prevent unwanted access to Service Provider core, such as:

- Certain types of traffic (for example Small ICMP packets, HTTP and IPSec).
- The Border Gateway (BG) should also be able to filter out unnecessary traffic coming from the Inter-Operator IP Backbone. (In other words, basically everything what is not agreed in IPX Provider agreement).
- Filter out all other IP traffic than those which has been originated from IP address range of commercial roaming partners.

The use of "GTP-aware" firewalls is considered good security practice for PMNs. However, the feature of comparing received GTP messaging against a "white list" of expected Information Elements (IEs) and their length and/or values (sometimes referred to as a "GTP Integrity Check"), must NOT be used. This is because such a feature breaks the extensiveness of GTP in that if either the HPMN or VPMN in a roaming partnership upgrade to a later release of GTPv2, the GTP-aware firewall in the other entity will drop any messages that contain any new (and thus "unrecognised") IEs or old IEs with different lengths and/or values. This silent discarding of GTP messaging can cause PDN connections to fail and, in the worst case, even deny any new PDN connections from being created. In this case, since LTE must have a default PDN connection, it will cause the UE's whole attachment to the VPMN to fail. This feature (“GTP Integrity Check”) is thus fatal to the success of LTE roaming going forward and should be disabled.

More detailed information of security demands and solutions can be found from GSMA PRD IR.77 [9].

6.5 Hubbing

Whilst the contents of this PRD describe guidelines and define procedures for bilateral roaming in LTE, the guidelines are equally valid for a roaming architecture which includes hubbing of the S6a and S6d interface. The Hubbing Architecture for LTE is defined in GSMA PRD IR.80 [22].

7 TECHNICAL REQUIREMENTS FOR DYNAMIC POLICY AND CHARGING CONTROL

7.1 Home Routed architecture and S8 protocol is GTP

It is up to the HPMN to implement a Policy and Charging infrastructure implementation, but it is required if the HPMN provides services requiring dynamic policy and charging control. For instance, RTP based video streaming services require guaranteed bit rates and hence require the setup of a GBR bearer from the PDN-GW that could be requested by the Home PCRF. “Anti-bill shock” is another example where PCC can be helpful. When the customer reaches the amount of money or roaming data defined by the HPMN legal authority, the PCRF or the OCS can ask the PGW to terminate the PDN connection.

In this scenario and according to 3GPP, the entire Policy and Charging Control infrastructure remains inside the HPMN. See architecture diagram below.

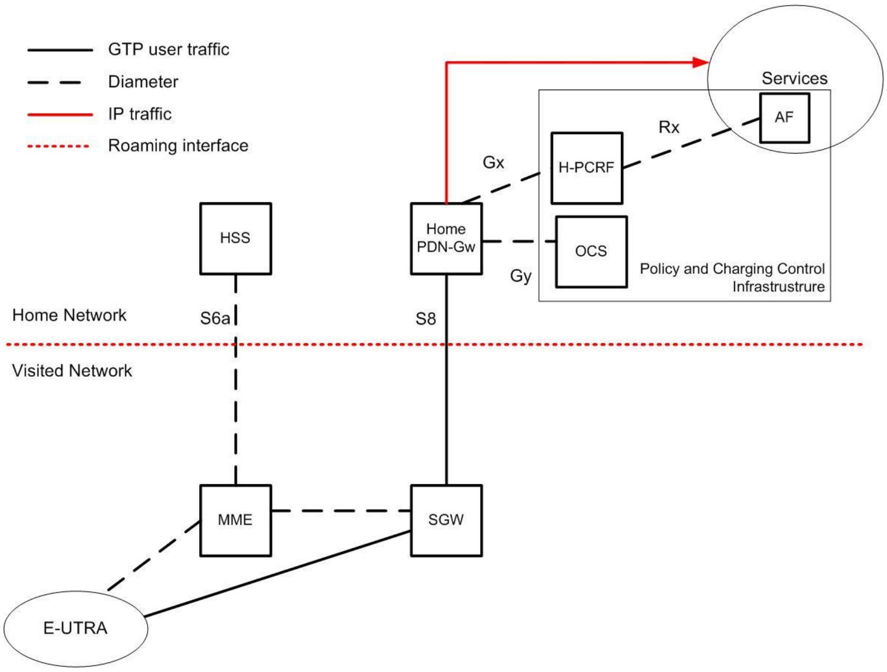

Figure 7.1-1: Policy and Charging Control Architecture with Home Routed architecture and S8 GTP based

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.

If services which require dynamic QoS and/or charging are deployed, it is required that the VPMN supports the following bearer management procedures in EPC and in E-UTRAN:

1. Network initiated dedicated bearer creation – this procedure is invoked by the PGW if the default bearer QoS cannot support the new requested service.
2. UE request for additional resources – this procedure can be invoked by the UE when requesting a new service and if the default bearer QoS is not suitable for it.
3. PGW initiated QoS bearer modification – the PGW could initiate a bearer modification procedure based on HPMN decision or in response to AF initiated bearer modification.
4. MME initiated QoS bearer modification – this procedure could be invoked if the subscribed QoS profile has been changed.
5. QoS modification of a bearer initiated by the UE – this procedure allows the UE to request the network new resources or a modification of the already reserved resources.

It is also required that the VPMN accepts the requested bearer QoS values (QCI, Allocation and Retention Priority, bit rates) that have been agreed as part of the roaming agreement and has engineered its access and core networks to fulfil the correspondent performance characteristics (Resource Type, Priority, Packet delay Budget and the Packet Error Loss rate) according to 3GPP TS 23.203 [34] Table 6.1.7: Standardized QCI characteristics.

It is recommended that the VPMN provides the Priority to the bearer according to QCI characteristic.

GBR bearers must be supported and the VPMN must provide the requested guaranteed bit rates within the limits as agreed as part of the roaming agreement.

If the bearer is non GBR, the VPMN can provide a different bit rate than the one requested by the roamer's UE or the Home PGW (provided this has been negotiated between the partners).

The VPMN can provide a different Allocation and Retention Priority unless this has been agreed otherwise between the partners.

7.2 Home Routed architecture and S8 protocol is PMIP

In this scenario and according to 3GPP, the policy and charging control infrastructure is not completely inside the HPMN. Dynamic Policy Control is only possible if the VPMN has implemented the Bearer Binding and Event Reporting Function in the Visited SGW and a V-PCRF. The partners must also implement the S9 interface.

See architecture diagram below.

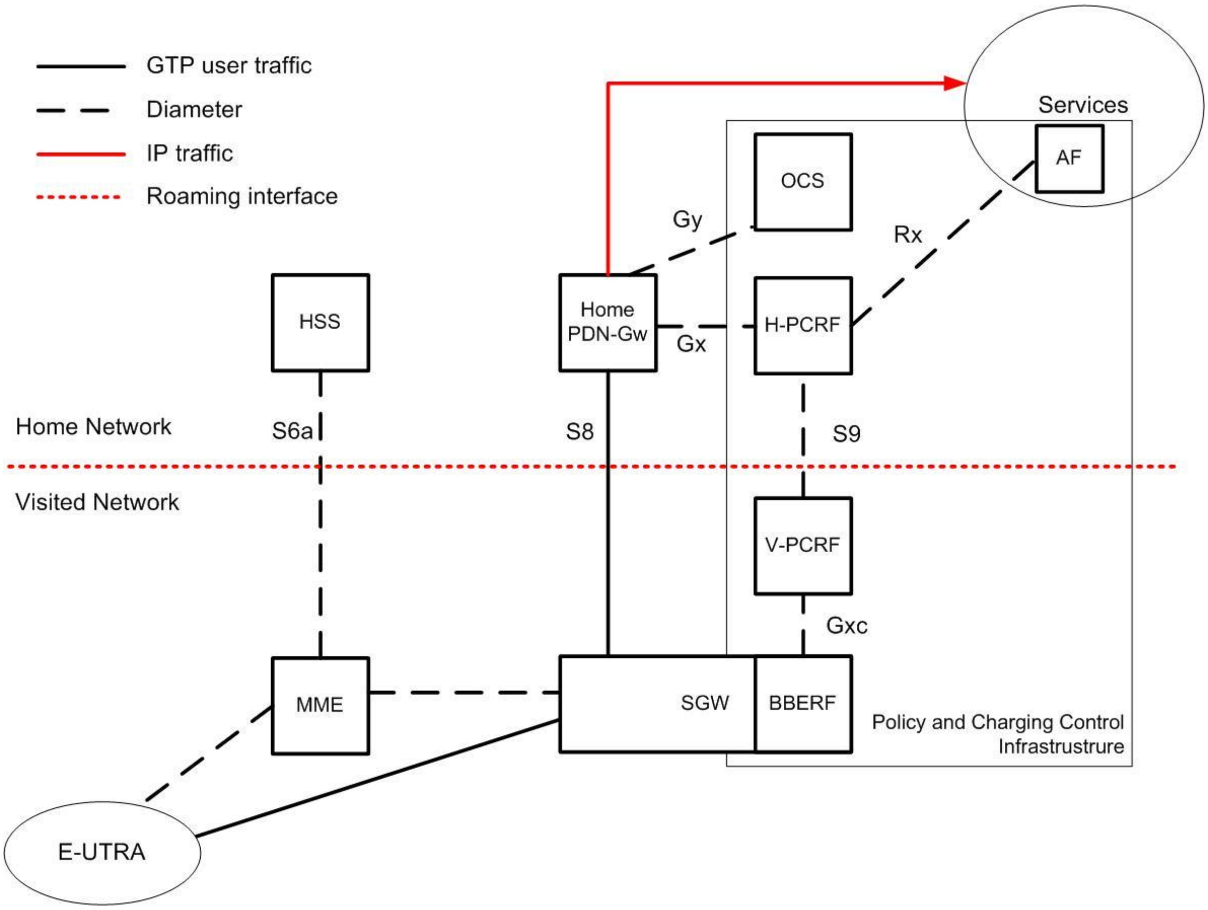

Figure 7.2-1: Policy and Charging Control Architecture with Home Routed architecture and PMIP based

It is also required that the VPMN follows the above recommendations for QoS engineering in its network.

7.3 Local Break Out architecture

This is the architecture for IMS roaming (as defined in [30]) with some more details of the PCC architecture.

In this scenario and according to 3GPP, the policy and charging control infrastructure is shared between the HPMN and the VPMN. Dynamic Policy Control is only possible if the VPMN has implemented its own PCC infrastructure that is to say a V-PCRF, a Policy and Charging Enforcement Function and a BBERF if PMIP is the S5 protocol. Both networks must have implemented a PCC infrastructure.

As this scenario is the one for Voice over LTE, it is highly recommended to implement PCC in both networks. However for VoLTE, S9 and Gy interfaces are optional. VoLTE online charging is performed in the HPLMN IMS and does not require charging at bearer level. As the procedure to setup a dedicated bearer for the voice call is also specified in [31], there is no need to inform the H-PCRF or to ask for its procedure approval as it has already been approved by the IMS in the HPMN.

See architecture diagram below.

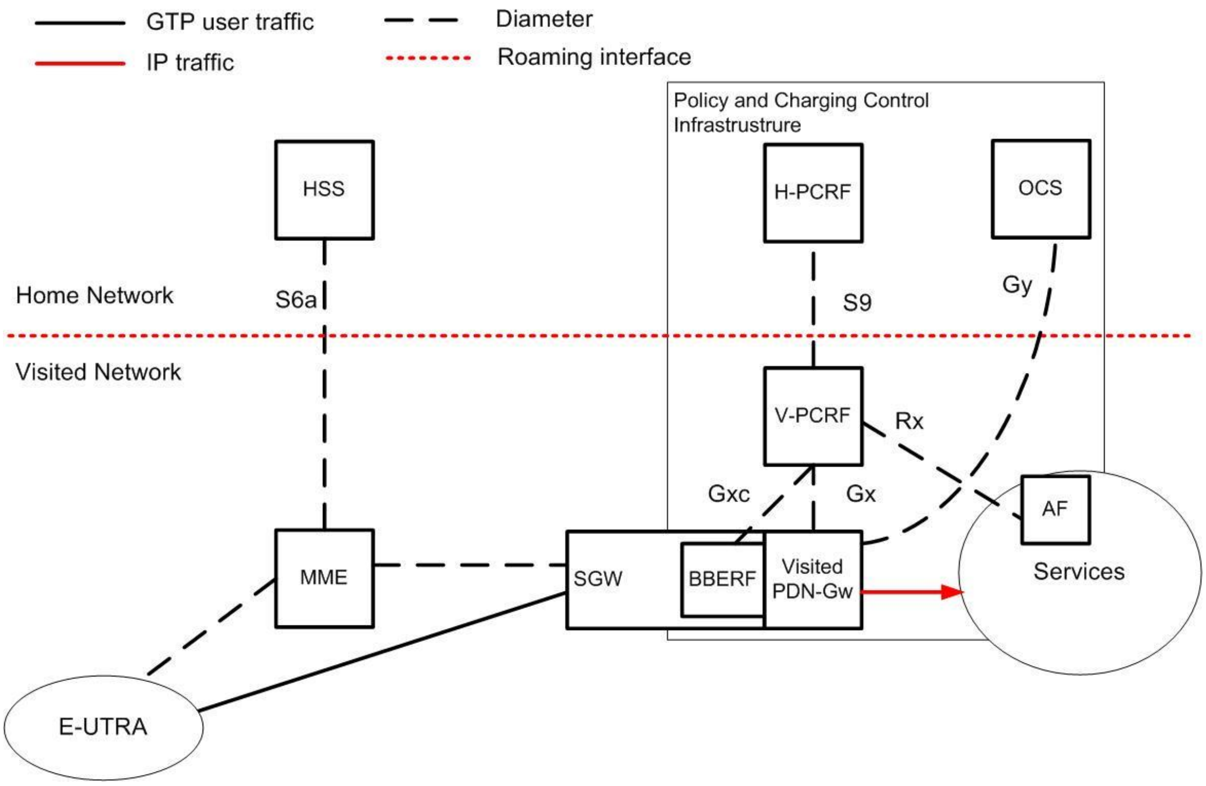

Figure 7.3-1: Policy and Charging Control Architecture with Local Break Out architecture

If GTP is S5 protocol, then the VPMN must support the bearer management procedures in EPC and in E-UTRAN listed in 7.1.

If PMIP is S5 protocol, then the VPMN must support the bearer management procedures in EPC and in E-UTRAN listed in 7.2.

It is also required that the VPMN follows the recommendations for QoS engineering in its network listed in 7.1.

8 Annex A: Testing Framework

<<Text to be added later>>

9 Annex B: Diameter Architecture Implementation

Figure B-1 illustrates the case where the PMN has implemented relays at the edge and application specific proxies in the inner domain including a Diameter Routing Agent for S9 and Rx applications.

The PMN has a bilateral interconnection with other PMNs.

Extended NAPTR [26] can be used at the Edge Agent to find the inner application specific proxy.

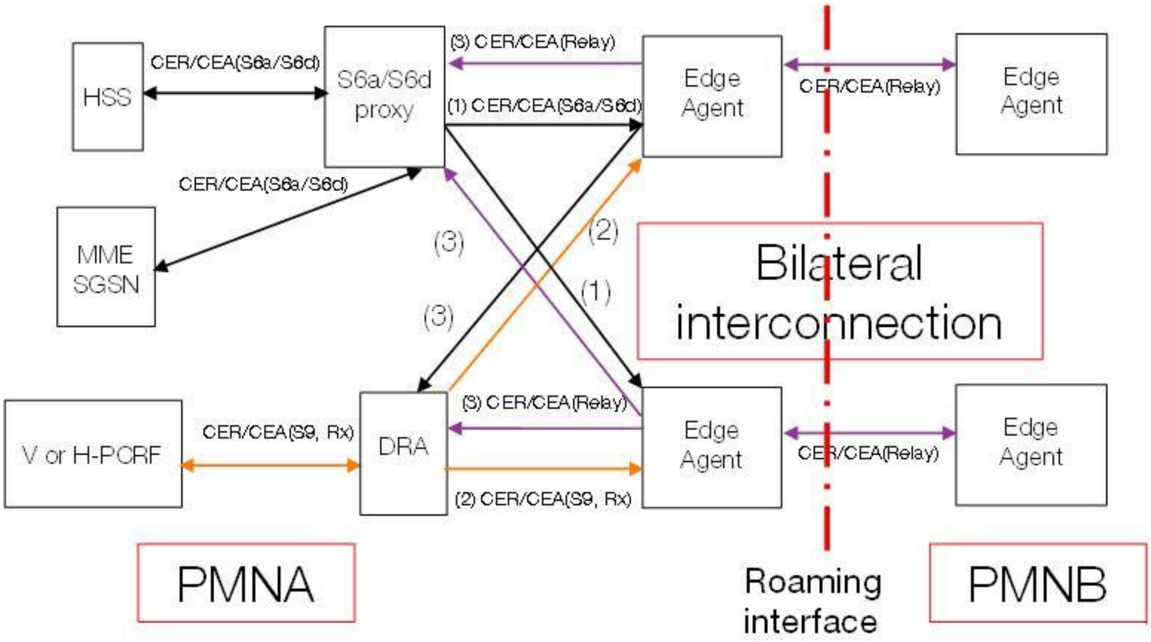

Figure B-1: Diameter architecture example 1

Figure B-2 illustrates the case where the PMN has implemented Edge agents that proxy all applications and no inner domain proxy.

The PMN has a bilateral interconnection with other PMNs.

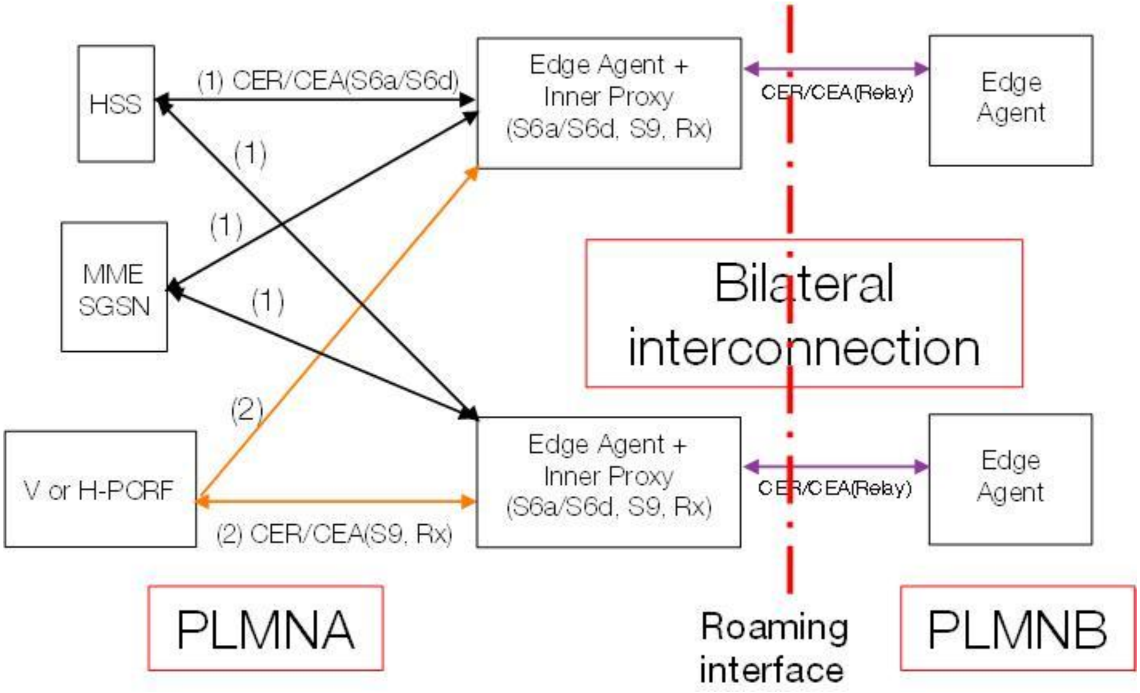

Figure B-2: Diameter architecture example 2

Figure B-3 illustrates the case where the PMN has Edge agents that are application specific proxies and no inner domain one. The Edge agent relays the Application messages that it is not able to proxy to the other Edge agent(s).

The PMN has a bilateral interconnection with other PMNs.

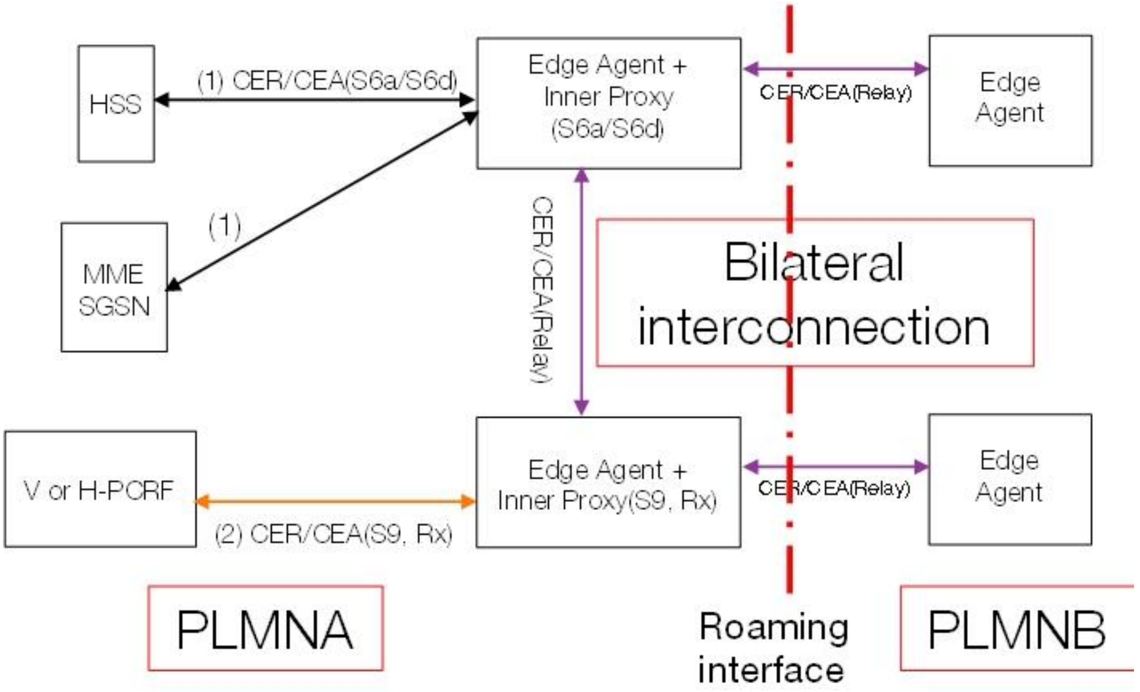

Figure B-3: Diameter architecture example 3

Figure B-4 illustrates another Diameter architecture implementation which is a variant of examples 1, 2 and 3 where the PMN has:

- Edge agents that are S6a/S6d proxies and relays for other applications (S9 and Rx in the current example)

- A Diameter Routing Agent to manage S9 and Rx applications in the inner domain

The PMN has a bilateral interconnection with other PMNs.

The Extended NAPTR [26] can be used at the Edge Agent to find the inner application specific proxy.

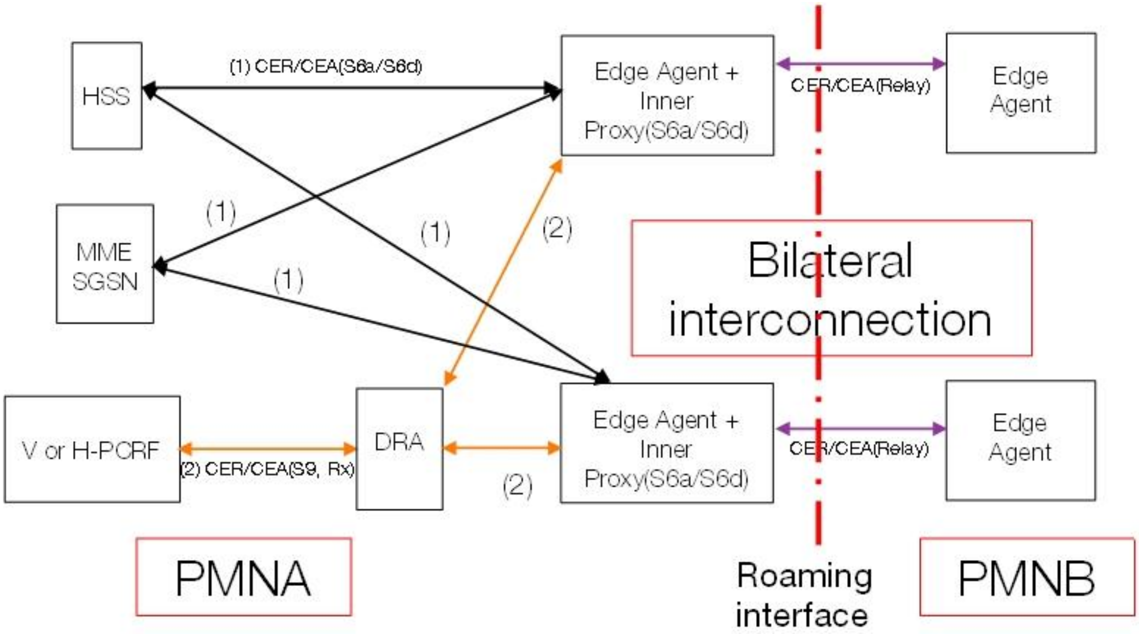

Figure B-4: Diameter architecture example 4

Figure B-5 illustrates the case where the PMN has implemented Edge agents that are application specific proxies. More those proxies are not able to relay messages of other applications to inner domain agents. The IPX providers and the PMN agreed to have application specific routing at the edge so avoiding it between PMNs.

The interconnection with other PMNs is done in transit mode through IPX providers.

The Extended NAPTR [26] can be used at the IPX Agent to find the application specific Edge proxy.

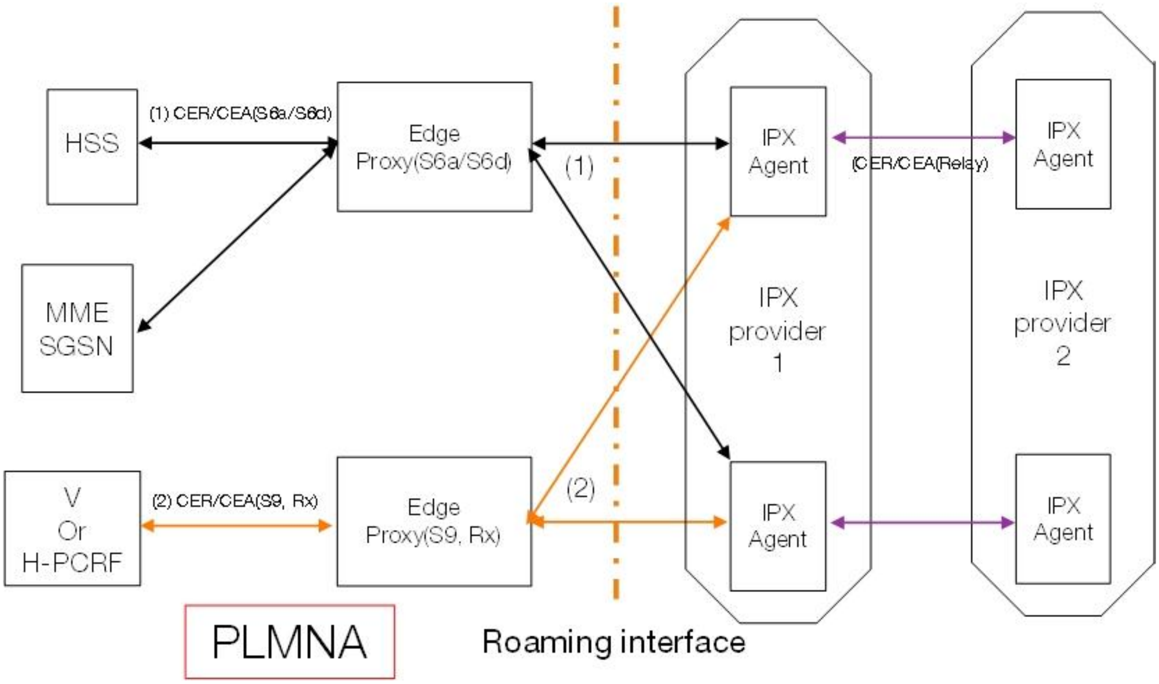

Figure B-5: Diameter architecture example 5

Figure B-6 illustrates the case where the PMN has outsourced Edge agents to its IPX providers.

The interconnection with other PMNs is done in transit mode through IPX providers.

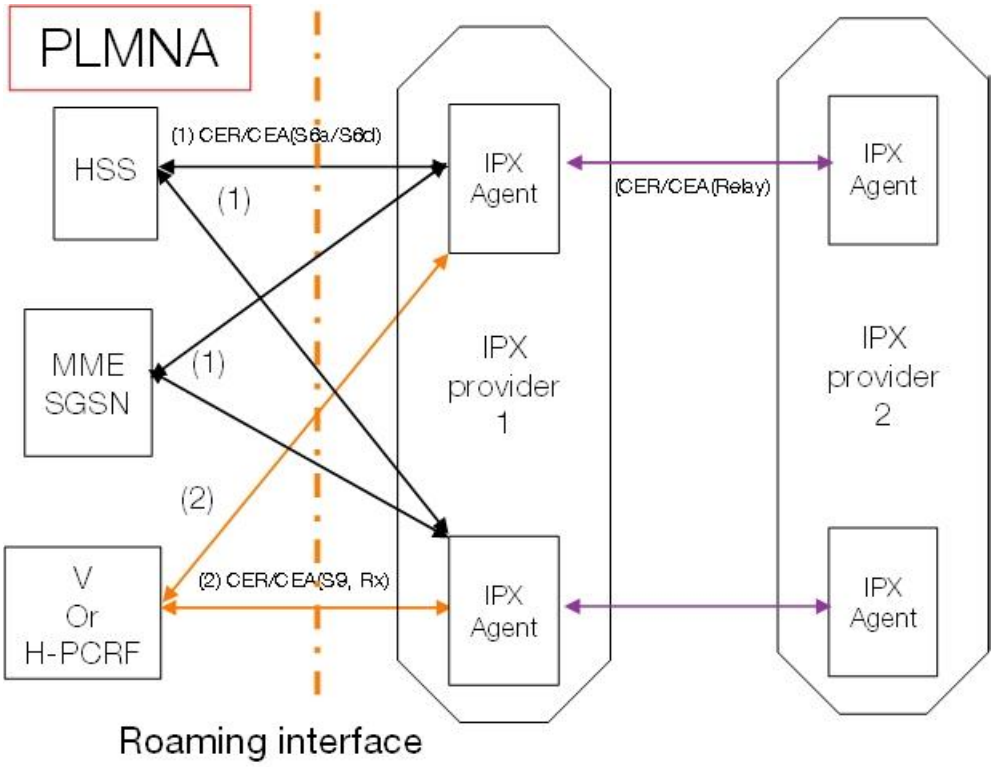

Figure B-6: Diameter architecture example 6

10 Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.0.20	7 Aug 2009	Initial version input for RILTE #3		
0.0.22	21 Aug 2009	Baseline version following RILTE #3		
0.0.24	24 Sept 2009	Baseline version following RILTE #4		
0.0.26	12 Oct 2009	Consolidation of RILTE #4 Action Points and subsequent emails		
0.0.28	20 Oct 2009	Version for review at RILTE #5		
1.0	28 Oct 2009	Approved at RILTE #5, for submission to IREG #57	IREG #57	John Boggis, Vodafone
2.0	1 June 2010	Major restructure and addition of some new sections	IREG#58 EMC#84	John Boggis, Vodafone
3.0	21 October 2010	Inclusion of the following CRs: • MCR 002: 2G/3G and LTE Co-existence Scenarios • MCR 003: Document the roaming retry procedure for CSFB • MCR 004: Diameter Roaming Architecture • MCR 005: PMIP-GTP Interworking • MCR 006: Gateway Selection in SGSN • MCR 007: VoLTE Roaming Architecture Additions	IREG #59 DAG #77 EMC #89	Nick Russell, Vodafone
3.1	17 February 2011	Inclusion of mCR 008: LTE Voice Roaming Architecture	Packet #48	Nick Russell, Vodafone
4.0	21 March 2011	Inclusion of the following CRs: • MCR 009: IP addressing alignment • mCR 010: Clarification on IMS APN usage	Packet #48 IREG #60 DAG #79	Nick Russell, Vodafone
5.0	18 May 2011	Change of Editor, section numbering correction on 'Document Management' and Inclusion of the following CRs: • MCR 011: IMS APN and IMS Emergency call • MCR 013: Addition of details from the IPv6 EMC Task Force's Ipv6 Transition Whitepaper • MCR 014: IMS "well-known" APN as Default APN	Packet #50 IREG #60 DAG #81	Itsuma Tanaka, NTT DOCOMO

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
6.0	31 August 2011	Inclusion of the following CRs: • MCR012: Policy and Charging • mCR015: correcting inconsistencies • MCR 016: PDN/PDP Type of IPv4v6 Editorial changes by the editor to update numbering of figures and some references quoted in the text.	Packet #52 IREG #60 DAG#84	Itsuma Tanaka, NTT DOCOMO
7.0	31 January 2012	Inclusion of MCR017r3: Gateway selection for IMS APN	Packet#54 IREG#60 DAG#88	Itsuma Tanaka, NTT DOCOMO

Other Information

Type	Description
Document Owner	IREG / Packet
Editor / Company	Itsuma Tanaka / NTT DOCOMO

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@gsm.org Your comments or suggestions & questions are always welcome.