

EPS Roaming Guidelines
Version 27.1
12/02/2024

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document 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

Copyright © 2024 GSM Association

Disclaimer

The GSMA 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.

Compliance Notice

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

This Permanent Reference Document has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.34 - Policy and Procedures for Official Documents.

Table of Contents

1 Introduction 6
1.1 Overview 6
1.2 Scope 6
1.3 Definition of Terms 7
1.4 Document Cross-References 10
2 Architecture 14
2.1 Architecture Models 14
2.2 Interfaces 16
2.3 Features 17
2.3.1 SGs Interface for CS Fallback and SMS over SGs 17
3 Technical Requirements and Recommendations for Interfaces 17
3.1 General requirements for Inter-PMN interfaces 17
3.1.1 Inter-PMN IP backbone network requirements 17
3.1.2 Stream Control Transmission Protocol (SCTP) 17
3.1.2.1 Introduction 17
3.1.2.2 SCTP Parameters 19
3.1.3 Diameter 21
3.1.3.1 Introduction 21
3.1.3.2 Diameter Agents 21
3.1.3.3 End to End Diameter Architecture 22
3.1.3.4 Diameter Routing 25
3.1.3.5 Diameter Transport Parameter 26
3.1.3.6 Notification of ME Identity 26
3.1.3.7 QoS for Diameter messages 26
3.2 S8 Interface 26
3.2.1 Procedures 26
3.2.1.1 General 26
3.2.1.2 SGW Selection 27
3.2.1.3 PGW Selection 28
3.2.1.4 Combined SGW/PGW Selection 29
3.2.2 GTP 29
3.2.3 Void 30
3.2.4 Void 30
3.2.5 Transport layer engineering 30
3.3 S9 Interface 30
3.3.1 S9 implementation requirements 30
3.3.2 Guidelines for Diameter interface over S9 interface 30
3.4 S6a and S6d interface 30
3.5 Gy interface 31
3.5.1 Gy implementation requirements 31
3.5.2 Guidelines for Diameter interface over Gy interface 31
4 Technical Requirements and Recommendations for Legacy Interworking and Coexistence 31

4.1 Legacy Interworking scenarios 31
4.1.1 Introduction 31
4.1.2 VPMN has not implemented LTE 31
4.1.3 HPMN has not implemented LTE 32
4.2 Co-existence scenarios 33
4.2.1 Introduction 33
4.2.2 Possible scenarios 33
4.2.2.1 2G/3G Roaming Agreement Only 33
4.2.2.2 2G/3G and LTE Roaming Agreement 35
4.2.2.3 LTE Roaming Registrations 38
4.2.3 Consequences of different APN approaches when roaming 38
4.2.3.1 Consequences of the single APN approach when roaming 38
4.2.3.2 Consequences of the dual APN approach when roaming 41
4.2.3.3 Guidance regarding the APN approach when roaming 41
4.3 Inter-RAT Handover 41
4.3.1 Handover and access restriction to/from 2G/3G and LTE 41
4.3.1.1 Introduction 41
4.3.1.2 Handover restriction to/from 2G/3G and LTE (Active mode) 41
4.3.1.3 Access restriction for 2G/3G and/or LTE (Idle mode) 43
4.3.1.4 Handover of PDN Connections between GERAN/UTRAN and LTE 43
4.3.2 Handover to/from non-3GPP accesses and LTE 44
4.3.3 Bandwidth considerations 44
4.3.3.1 Issue description and possible cause 44
4.3.3.2 Possible solutions 45
4.3.4 ARP considerations at handover from LTE to 2G/3G 45
5 Technical Requirements and Recommendations for Services 45
5.1 Short Message Service (SMS) 45
5.1.1 SMS over SGs 45
5.1.2 SMS in MME 46
5.2 Voice 48
5.2.1 CS Fallback 48
5.2.1.1 General 48
5.2.1.2 Roaming Retry for CSFB procedure 49
5.2.1.3 Roaming Forwarding for CSFB procedure 50
5.2.1.4 Coexistence of Roaming Forwarding and Roaming Retry procedures 51
5.2.1.5 Recommended procedures 51
5.2.2 IMS Voice Roaming Architecture 51
5.2.2.1 General 51
5.2.2.2 void 51
5.2.2.3 IMS Voice Roaming Architecture for S8HR 51
5.2.2.4 Terminating Access Domain Selection 53
5.2.2.5 IMS Voice Roaming Restriction 53
5.2.3 void 53
5.3 MIoT location 53

6 Other Technical Requirements and Recommendations 54
6.1 Access Control 54
6.1.1 Access Control in the VPMN 54
6.1.1.1 Source SGSN/ MME enforcing access restriction during Inter-RAT RAU/TAU procedures 55
6.1.2 Access Control in the HPMN 56
6.1.3 Access Control in the VPMN for CS Fallback 56
6.2 Addressing 57
6.2.1 UE Addressing 57
6.2.1.1 SS7 57
6.2.1.2 IP 57
6.2.2 Network Element Addressing 58
6.2.2.1 IP and SS7 58
6.2.2.2 Fully Qualified Domain Names (FQDNs) 58
6.2.2.3 Diameter Realms 58
6.3 APN for IMS based services 58
6.3.1 Introduction 58
6.3.2 IMS well-known APN 59
6.3.2.1 Definition 59
6.3.2.2 Gateway Selection 59
6.3.2.3 Inter-PLMN roaming hand over 60
6.3.2.4 Network-initiated deactivation and re-activation of the PDN connection to the IMS well known APN 60
6.3.3 APN for Home Operator Services 61
6.3.3.1 Definition 61
6.3.3.2 Gateway Selection 62
6.3.3.3 Inter-PLMN roaming hand over 62
6.3.3.4 Network-initiated deactivation and re-activation of the PDN connection to the APN for Home Operator Services 62
6.3.3.5 Data Off related functionality 62
6.4 Emergency Service 63
6.4.1 General 63
6.4.2 Emergency PDN connection 63
6.4.3 S8HR and support of Anonymous Emergency Call 63
6.4.4 Emergency Call Indicator 64
6.5 Security 64
6.5.1 GTP Security 65
6.5.2 Diameter Security – “Hop by hop” Approach 68
6.5.2.1 Network Domain Security for IP 68
6.5.2.2 Network Layer and Transport Layer Security 70
6.5.2.3 Diameter Base Protocol Security 71
6.5.2.4 Cross-Layer Security 73
6.5.2.5 Diameter Application Security Depending on the Diameter Application (e.g. S6a, S9, Gy, ...) 74
6.5.2.6 Discovery of Peer PLMN Network Elements 74

6.5.2.7 Responsability Cascade 75
6.5.3 Diameter End-to-End Security 75
6.5.3.1 Introduction 75
6.5.3.2 Diameter End-to-End Signaling Security (DESS) 75
6.5.3.3 Interfaces to be protected 77
6.5.4 Risks from Interworking with Different Technology Generations and Signaling Protocols 77
6.6 Diameter Roaming Hubbing 79
6.6.1 Direct connection 79
6.6.2 Origin/Destination realm based routing 79
6.6.3 Destination realm modification 80
6.7 Default APN 80
6.8 E-UTRA-NR Dual Connectivity with EPC 81
6.8.1 GW Selection for E-UTRA-NR Dual Connectivity 82
6.9 TAC/LAC Restriction Guidelines 82
6.10 APN for UAS based services 82
6.10.1 Introduction 82
6.10.2 UAS well-known APN 82
6.10.3 Definition 82
6.10.4 Gateway Selection 83
7 Technical Requirements for QoS support 84
7.1 QoS Parameters definition 84
7.2 QoS management in the Home Routed architecture 85
7.2.1 Procedures involving QoS management 86
7.2.2 Requirements for the VPMN 88
7.2.3 Requirements for the HPMN 90
7.2.4 QoS control for IMS APN in the S8HR architecture 91
7.2.5 Support of QoS by the IPX/GRX 91
7.2.6 Enforcement of QoS by the VPMN 91
7.3 QoS control in the Local Break Out architecture 92
Annex A Testing Framework 94
Annex B Diameter Architecture Implementation 95
Annex C Background on Security Requirements 99
C.1 The need for Diameter Security 99
C.2 DNS Security 99
Annex D IPsec to protect IP transport 100
Annex E Guidelines for proposed minimum QoS parameters for S8HR roaming scenario 101
Annex F Document Management 103
F.1 Document History 103

1 Introduction

1.1 Overview

This document aims to provide a standardised view on how Long Term Evolution (LTE) and Evolved Packet Core (EPC) 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 and EPC. Consequently, this document makes references to current 3GPP specifications for GPRS in addition to those specifying solely LTE-Evolved Packet System (EPS) and EPC aspects, and also to other GSMA IREG PRDs. The main focus is to describe EPC over LTE, since the LTE access specifics are not covered in any other PRD. EPC over 2G/3G is also covered regarding the EPC aspects impacting the S4-SGSN and the Gn/Gp SGSN; the 2G/3G access specific aspects are covered in GSMA PRD IR.33 [10].

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 and EPC Roaming. The document addresses aspects which are new and incremental to EPC roaming in general, and using LTE access specifically: 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.

This PRD also covers Voice and SMS services using CS Fallback (CSFB) [25] and IMS Voice [30]. For IMS Voice [30], only the technical guidelines in Evolved Packet Core (EPC) layer are covered.

The PRD describes the interface S8 between the HPMN and VPMN. Going forward the PMIP protocol won’t be maintained for the S8 roaming interface. Only the GTP protocol is used for this interface.

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

1.3 Definition of Terms

Term	Description
3GPP	3rd Generation Partnership Project
ACL	Access Control List
AMBR	Aggregate MBR
APN	Access Point Name
ARP	Allocation Retention Priority
AVP	Attribute Value Pair
BBERF	Bearer Binding and Event Reporting Function
BG	Border Gateway
CER	Capabilities-Exchange-Request
CEA	Capabilities-Exchange-Answer
CN	Core Network
CSFB	Circuit Switched FallBack
Data Off	See PRD IR.92 [30]
Data Off Enabled Service	See PRD IR.92 [30]
DDoS	Distributed Denial of Service
DEA	Diameter Edge Agent
DESS	Diameter End-ti-end SIgnaling Security
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DRA	Diameter Routing Agent
EN-DC	E-UTRA-NR Dual Connectivity
ECGI	E-UTRAN Cell Global Identifier
EPC	Evolved Packet Core
EPS	Evolved Packet System (Core)
ESP	Encapsulated Security Payload
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
E2E	End-2-End
GBR	Guaranteed Bit Rate
GERAN	GSM/Edge Radio Access Network
GGSN	Gateway GPRS Service Node
GMLC	Gateway Mobile Location Centre
GMSC	Gateway MSC
GPRD	General Data Protection Regulation
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol

Term	Description
HLR	Home Location Register
HPMN	Home Public Mobile Network
HSPA	High-Speed Packet Access
HSS	Home Subscriber Server
HTTP	Hyper-Text Transfer Protocol
IE	Information Element
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identifier
IMEISV	IMEI Software Version
IMSI	International Mobile Subscriber Identity
IKE	Internet Key Exchange
IP-CAN	IP Connectivity Access Network
JSON	JavaScript Object Notation
LA	Location Area
ISH	IPX Service Hub
LAC	Location Area ode
LTE	Long Term Evolution (Radio)
MAP	Mobile Application Part (protocol)
MBR	Maximum Bit Rate
MIoT	Mobile Internet of Things
MME	Mobility Management Entity
MSC	Mobile services Switching Centre
MTC	Mobile Terminating Call
NE	Network Element
NR	New Radio
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
PDN-GW	Packet Data Network Gateway = PGW
PGW	PDN (Packet Data Network) Gateway
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PRD	Permanent Reference Document
Term	**Description**
PSI	Provide Subscriber Info (MAP)

QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RR	Resource Record
RTO	Retransmission Timeout (in SCTP)
RTT	Round Trip Time
SCTP	Stream Control Transmission Protocol
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SMLC	Serving Mobile Location Centre
TA	Tracking Area
SP	Service Provider
TAC	Tracking Area
TAU	Tracking Area Update
T-ADS	Terminating Access Domain Selection
TLV	Type-Length-Value
TMSI	Temporary Mobile Subscriber Identity
UAS	Unmanned Aircraft System
UE	User Equipment
Unsolicited downlink IP packet	An IP packet is an unsolicited downlink IP packet if: - the IP packet is sent towards the UE IP address; and - the IP packet is not related to an IP packet previously sent by the UE.
VMSC	Visited MSC
VPMN	Visited Public Mobile Network
Well-known APN	An APN whose value has a defined specific string of characters
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

Term	**Description**
Network Element	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 such as MME, SGW, PGW, HSS, and GTP Firewalls, as well as routers and gateways are considered network elements.

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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3"
5	3GPP TS 29.281	"General Packet Radio System (GPRS) Tunneling 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-Service Provider 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"

Ref	Document Number	Title
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	Void	Void
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 10
26	IETF RFC 6408	"Diameter Straightforward-Naming Authority Pointer (S-NAPTR) Usage"
27	3GPP TS 23.018	"Basic call handling; Technical realization" – Release 10
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
35	GSMA PRD_IR.23	"Organization of GSM International Roaming Tests"
36	GSMA PRD IR.35	"End–to–End Functional Capability Test Specification for Inter-PMN GPRS Roaming"
37	3GPP TS 33.210	"Network Domain Security (NDS); IP network layer security"
38	3GPP TS 33.310	"Network Domain Security (NDS); Authentication Framework"
39	3GPP TS 23.221	"Architectural Requirements"
40	GSMA PRD IR.21	“GSM Association Roaming Database, Structure and Updating Procedures”
41	3GPP TS 23.007	"Restoration procedures"
42	GSMA PRD IR.24	"End-to-End Functional Capability Specification for Inter-PLMN Roaming (Stage 4 Testing)"
43	3GPP TS 25.413	"UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling"

Ref	Document Number	Title
44	3GPP TS 48.018	"General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS protocol (BSSGP)"
45	3GPP TS 36.413	"Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)"
46	3GPP TS 29.002	"Mobile Application Part (MAP) specification"
47	GSMA PRD RCC.07	“Rich Communication Suite 5.1 Advanced Communications Services and Client Specification”
	void	void
49	3GPP TS 29.213	“Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping”
50	GSMA AA.51	IPX Definition and Releases, Version 1.0
51	3GPP TS 23.107	“Quality of Service (QoS) concept and architecture”
52	GSMA PRD IR.64	“IMS Service Centralization and Continuity Guidelines”
53	3GPP TS 29.118	"Mobility Management Entity (MME) - Visitor Location Register (VLR) SGs interface specification"
54	GSMA PRD IR.38	"LTE and EPC Roaming Testing"
55	GSMA PRD IR.94	"IMS Profile for Conversational Video Service"
56	3GPP TS 26.114	"IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction”
57	GSMA PRD BA.65	LTE Roaming Implementation Handbook
58	GSMA PRD FS.20	GPRS Tunneling Protocol (GTP) Security
59	3GPP TS 33.117	Catalogue of General Security Assurance Requirements, Technical Specification of the 3GPP.
60	GSMA PRD FS.19	Diameter Interconnect Security
61	3GPP TS 29.060	"General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface"
62	3GPP TS 33.107	3G Security; Lawful interception architecture and functions
63	3GPP TS 37.340	“Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity”
64	GSMA PRD WA.11	LAC TAC Guidelines and Agreement Template
65	IETF RFC 1034	DOMAIN NAMES - CONCEPTS AND FACILITIES
66	IETF RFC 1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
67	FS;21	Interconnect Signalling Security Recommendations
68	FS.34	Key management for 4G and 5G inter-PLMN security
69	GSMA PRD NG.120	MIoT location in roaming
70	GSMA PRD NG.128	LTE UNI Aerial Profile
71	3GPP TS 29.338	Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs).

2 Architecture

2.1 Architecture Models

The following diagrams are produced based on the network diagrams from 3GPP TS 23.401 [1] and 3GPP TS 23.402 Section 4.2 [2], covering

LTE Roaming Architecture;

GERAN/UTRAN Roaming Architecture with S4 SGSN;

GERAN/UTRAN Roaming Architecture with Gn/Gp SGSN connected to PGW (PDN (Packet Data Network) Gateway).

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.

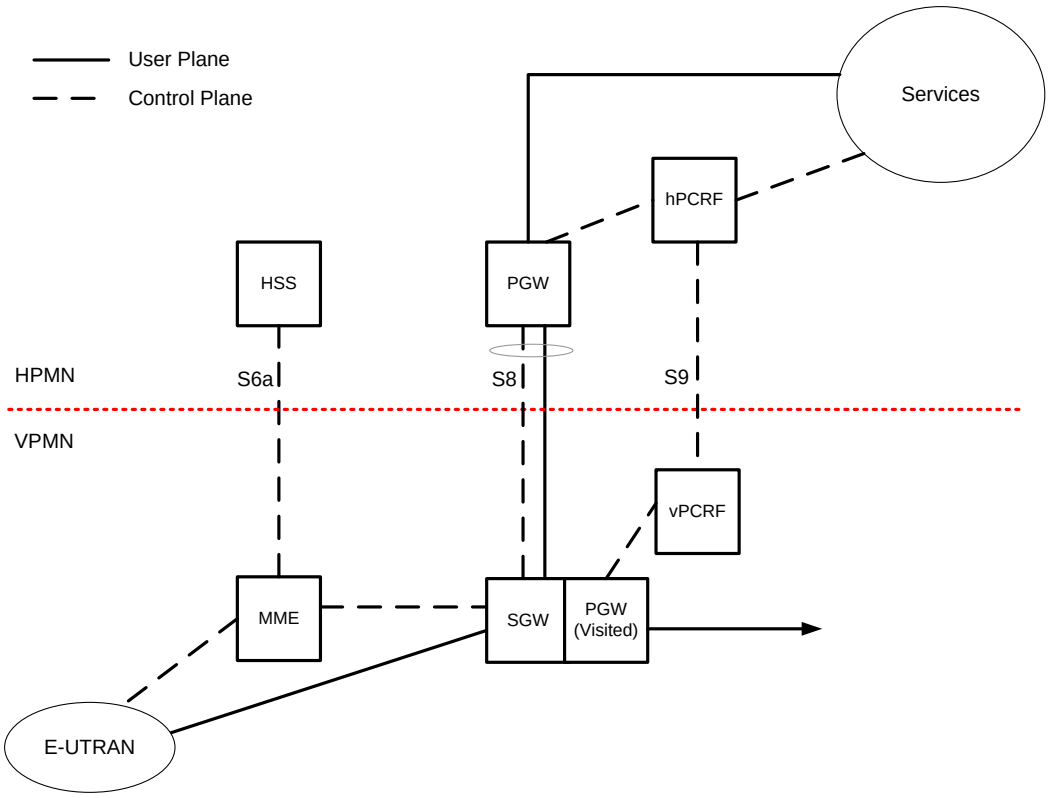

Figure 1: LTE Roaming Architecture

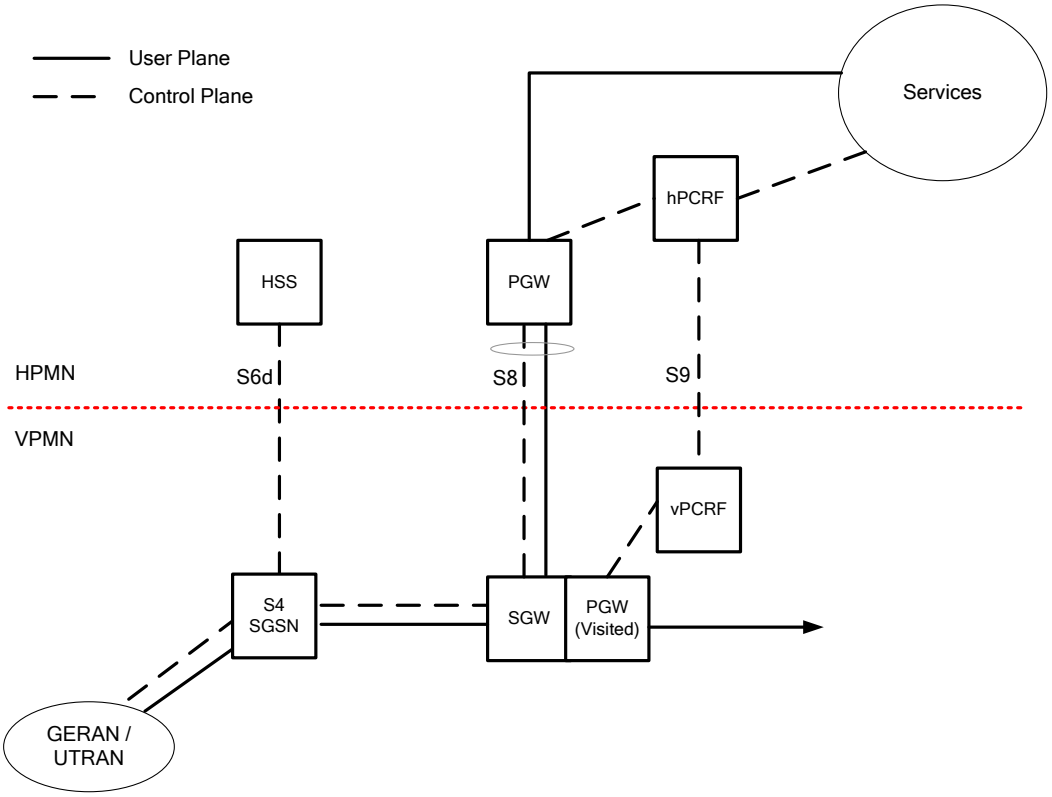

Figure 2: GERAN/UTRAN Roaming Architecture with S4 SGSN

Note 1: The S4 SGSN can also use MAP based Gr to the HLR/HSS (Home Location Register/ Home Subscriber Server) (see also 3GPP TS 23.060 [29]).

The S4 SGSN can also use Gp to GGSN (Gateway GPRS Service Node) or PGW (see also 3GPP TS23.401 [1]).

Guidelines concerning the co-existence of Gp and S8 interfaces are specified in the section 4.2 "Co-existence scenarios" of this document.

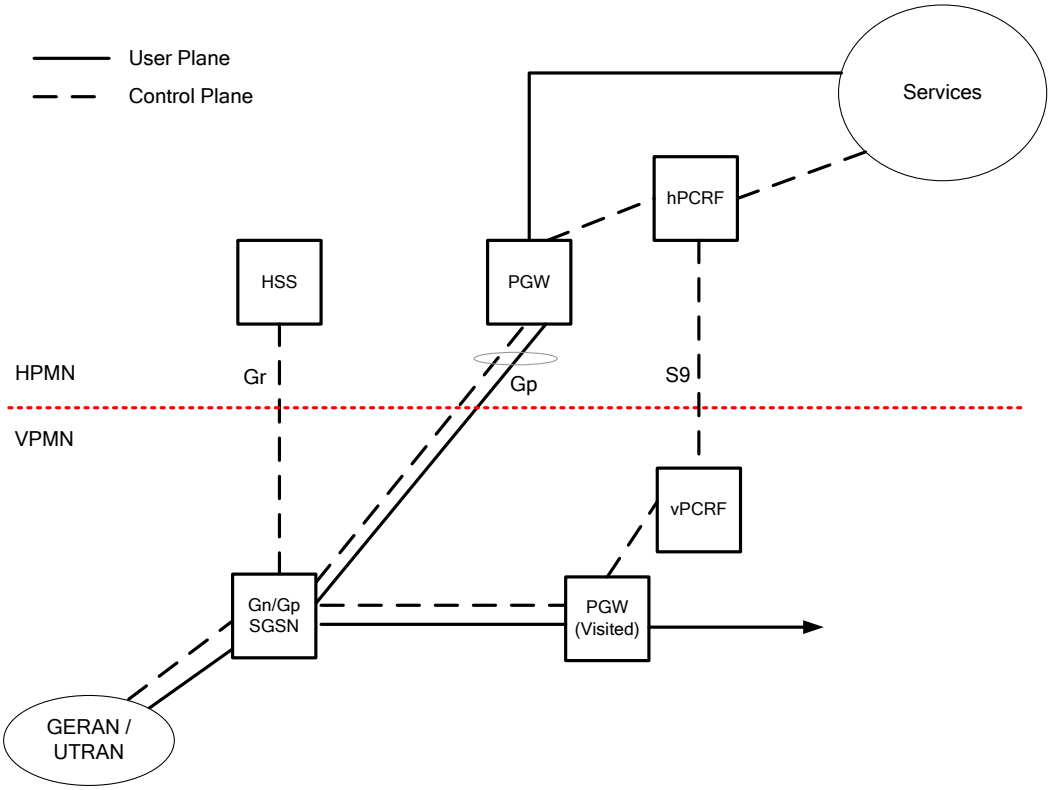

Figure 3: GERAN/UTRAN Roaming Architecture with Gn/Gp SGSN connected to PGW

Note 2: Roaming from non-3GPP access is not supported in this version of the document.

2.2 Interfaces

The following interfaces are relevant for LTE and EPC 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])
S4-SGSN - HSS	S6d	Diameter Base Protocol (IETF RFC 3588 [3]) and 3GPP TS 29.272 [8])
	Gr	See Notes below
SGW - PGW	S8	GTP (GTP-C 3GPP TS 29.274 [4] and GTP-U 3GPP TS 29.281 [5])
hPCRF - vPCRF	S9	Diameter Base Protocol (IETF RFC 3588 [3]) and 3GPP TS 29.215 [6])

Table 1: Relevant interfaces for LTE and EPC roaming

Note:

For Gr and Gp interfaces, see GSMA PRD IR.33 [10].

For co-existence of Gp and S8 interfaces, see section 4.2 "Co-existence scenarios" of this document.

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) and by MME/SGSN to find a PGW) uses standard DNS procedures and protocol, as specified in IETF RFC 1034 [6

5] and IETF RFC 1035 [66].

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

2.3 Features

2.3.1 SGs Interface for CS Fallback and SMS over SGs

A VPMN with LTE plus GSM and/or UMTS access(es) must support the SGs interface as defined in 3GPP TS 23.272 [25] for supporting CS Fallback and SMS over SGs for its inbound roamers. The details of how the SGs interface is used are described in Section 5.1 and Section 5.2 of the present document.

3 Technical Requirements and Recommendations for Interfaces

3.1 General requirements for Inter-PMN interfaces

3.1.1 Inter-PMN 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 this document and in GSMA 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 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	1/4
Valid.Cookie.Life	60 sec
Max.Init.Retransmits	8 attempts
HB.interval (Heartbeat interval)	30 sec
Max.Burst	4
HB.Max.Burst	1

Table 2: 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 three (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 3s)
RTO.Min	1.15 * Engineered RTT – See notes below (RFC 4960 default 1 sec)
RTO.Max	3 * Engineered RTT– See notes below (IETF RFC 4960 default 60sec)
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 (This means that every packet containing any data chunks is to be acknowledged individually)
Chunk Bundling Time	10-15ms

Table 3: Table of SCTP Parameters derived from IETF RFC 4960 [13]

Note 1: It is recognized 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.

Note 2: 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.

Note 3: 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 2 secs, 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.

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 is strongly recommended. The Diameter agent is named Diameter Edge Agent（DEA) hereafter. The DEA 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 four types of Diameter agent, namely Diameter Relay agent, Diameter Proxy agent, Diameter Redirect agent and Diameter Translation agent. For signalling in LTE Roaming only the Relay agent, the Proxy agent and the Translation Agent are relevant.

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

A Relay agent does NOT inspect the actual content of the message.

When a Relay agent receives a request, it will route the messages to other Diameter nodes based on the information found in the message, for example, Application ID and Destination-Realm. A routing table (Realm Routing Table) is looked up to find the next-hop Diameter peer.

A Relay Agent is non-application aware, i.e. it keeps transaction state but does not keep session state.

"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.

A Diameter proxy is application aware: it maintains the state of downstream peers to enforce resources usage, providing admission control and provisioning.

"Diameter translation" agent provides translation between two protocols (e.g. RADIUS<->Diameter, TACACS+<->Diameter).

According to its Realm Routing Table, a DEA can act as a Proxy for some Diameter applications (such as add/drop/modify AVP or perform AVP inspection) while acting as a Relay for all others (which is simply routing 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 DEA advertises the Relay application ID to the outer Diameter peers. By using the Relay, inter PMN routing is independent from inner domain applications. Note that the DEA is free to advertise the Proxy ID to inner Diameter peers.

It is therefore recommended that any DEA 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, through IPX Diameter Agent.

It is strongly recommended that DEA acts as Diameter proxy for each Diameter application supported by the PMN, through a IPX Diameter Agent. They can be implemented inside the PMN inner domain, inside the DEA or outsourced to the IPX provider. This is to provide functionalities such as admission/access control, policy control, add special information elements (AVP) handling. The DEA or the IPX Diameter Agent also provide topology hiding to protect the network elements and addresses from being exposed to foreign networks. The implementation of the topology hiding should not impair others features related to path validation. DEA, acting as either relay or proxy function can finally also perform filtering functionalities.

3.1.3.3 End to End Diameter Architecture

Figure 4 is a logical architecture that illustrates, at the Diameter application level, the position of the DEA in the PMN. It shows 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 DEAs must be secured by the Border Gateways as any other equipment exposed to the GRX/IPX unless they are outsourced to IPX providers.

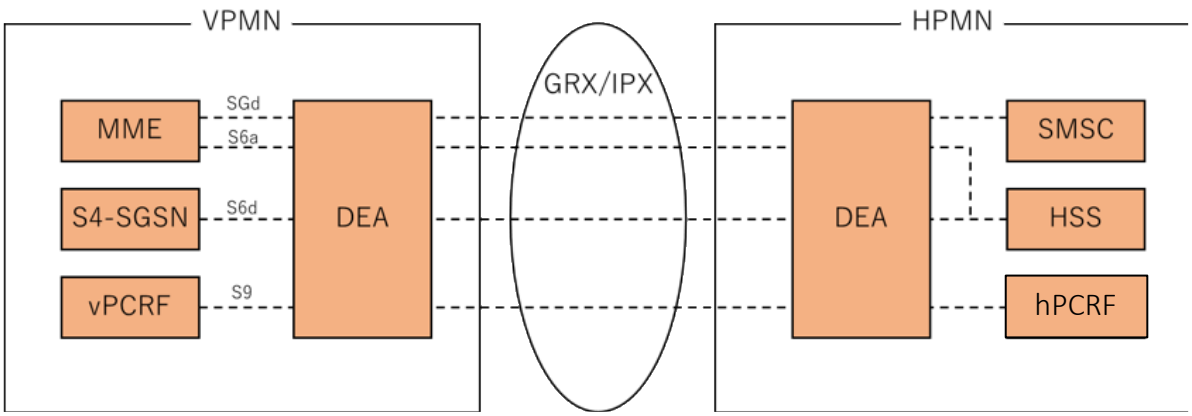

Figure 4: Diameter Roaming Implementation Architecture

Figure 5 illustrates a possible end to end Diameter Architecture implementation. It is a practical implementation with two DEAs 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 according to the three IPX connectivity options defined in GSMA AA.51 [50]:

Bilateral Transport only connectivity, with direct peer connections between DEAs and no IPX Diameter Agent in between, as shown in Figure 4

Bilateral Service Transit mode with PMN interconnection provided by IPX Diameter Agents.

Multi-lateral Service Transit mode with PMN interconnection provided by IPX Diameter Agents.

As mentioned in GSMA AA.51 [50], the two latter cases (Bilateral and Multi-lateral) define two different business models but are similar from a service connectivity perspective, as shown in Figure 5

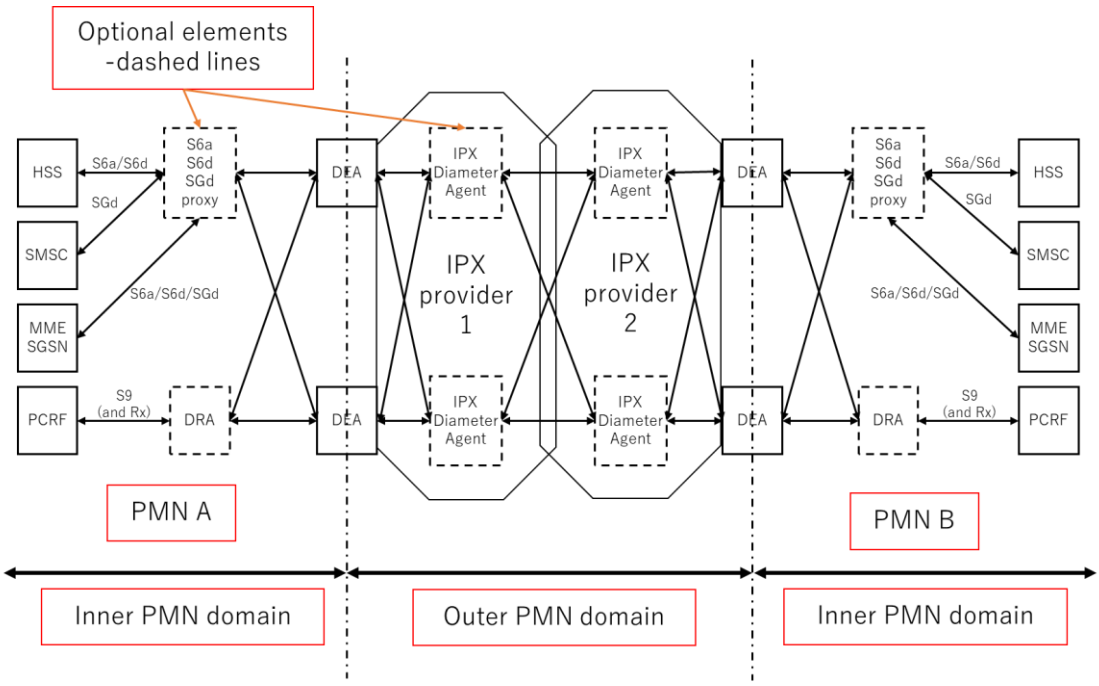

Figure 5: End to end Diameter Architecture

Note 1: The DRA (Diameter Routing Agent) shown in the figure above is defined in 3GPP TS 29.213 [49]. A DRA is a proxy or a redirect agent, which ensures that all Diameter sessions established over the Gx, S9, Gxx and Rx reference points to a certain IP-CAN session and reaching the same PCRF when multiple and separately addressable PCRFs have been

deployed in a Diameter realm. Note that a PMN that does not have multiple instances of EPC elements does not necessarily require DRA.

Note 2: To prevent Diameter procedure timer expiry between PMN end points, it is advised that processing time in the HSS, and any element involved in handling Diameter messages between PMNs illustrated in Figure 5, is kept as minimal as possible. This will ensure Diameter procedures between PMNs are completed before a timer elapses that may cause a procedure such as an Update Location to fail.

Diameter Routing

Diameter Routing on international network shall be performed based on the destination-realm AVP.

Therefore, it is mandatory to use the standard realm as detailed in 3GPP 23.003 [7] section 19.2:

“epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org".

The DEA or IPX Diameter Agent can discover the "next hop" agent using the search order recommended in Section 5.2 of IETF RFC 3588 [3]). This results to the following recommended search order:

1. The DEA consults its list of manually configured Diameter agent locations (that are static Routing Table entries); this list could derive from the IR.21 database [40].
2. The DEA performs a NAPTR query (RFC 3403) for a server in a particular realm (for example, the HPMN or the roaming hub). In this case, a GRX/IPX DNS (as per PRD IR.67 [21]) is used.

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>. In this case, the GRX/IPX DNS (as per PRD IR.67IR.67 [21]) is used.

For operational (SCTP is in connected mode) and security reasons, use of static configuration (step 1 above) for Diameter peering is recommended whatever the Diameter architecture is used.

Diameter request routing and forwarding decision is always tied to specifically supported applications unless Relay Agents are used. That means a DEA implemented as a Proxy Agent and possible Proxy Agent based Hubs shall support those applications that are required (such as S6a, S6d 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.

Note: Each of the three steps above has different security implications which are dealt with in Section 6.5 and in Appendix C.

According to RFC 3588 [3], answers are automatically routed back to the initial requestor, following the exact same path progressively discovered in the routing request.

This is performed thanks to hop-by-hop routing, consisting in mapping incoming and outgoing hop-by-hop identifiers to a given transaction and a sending Diameter peer.

Note: To facilitate troubleshooting, Diameter End Point hostname is recommended to include its network function or any deviation of this (e.g. “mme”, “hss1” …).

3.1.3.4 Diameter Routing

Diameter Routing on an international network shall be performed based on the destination-realm AVP.

Therefore, it is mandatory to use the standard realm as detailed in 3GPP 23.003 [7] section 19.2:

“epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org".

If the HPMN has multiple MCC/MNCs, the HPMN must have one Destination per MCC/MNC and advertise them in GSMA PRD IR.21, and the HPMN’s DIAMETER nodes (e.g. DEA, HSS) must handle all destination realms relevant to their subscriber’s IMSI by HPMN’s own responsibility

The DEA or IPX Diameter Agent can discover the "next hop" agent using the search order recommended in Section 5.2 of IETF RFC 3588 [3]). This results to the following recommended search order:

1. The DEA consults its list of manually configured Diameter agent locations (that are static Routing Table entries); this list could derive from the GSMA PRD IR.21 database [40].
2. The DEA performs a NAPTR query (RFC 3403) for a server in a particular realm (for example, the HPMN or the roaming hub). In this case, a GRX/IPX DNS (as per GSMA PRD IR.67 [21]) is used.
   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.
4. If no NAPTR records are found, the requester directly queries for SRV records: _diameter._sctp.<realm>. In this case, the GRX/IPX DNS (as per GSMA PRD IR.67 [21]) is used.

For operational (SCTP is in connected mode) and security reasons, use of static configuration (step 1 above) for Diameter peering is recommended whatever the Diameter architecture is used.

Diameter request routing and forwarding decision is always tied to specifically supported applications unless Relay Agents are used. That means a DEA implemented as a Proxy Agent and possible Proxy Agent based Hubs shall support those applications that are required (such as S6a, S6d 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.

Note: Each of the three steps above has different security implications which are dealt with in Section 6.5 and in Appendix C.

According to RFC 3588 [3], answers are automatically routed back to the initial requestor, following the exact same path progressively discovered in the routing request.

This is performed thanks to hop-by-hop routing, consisting in mapping incoming and outgoing hop-by-hop identifiers to a given transaction and a sending Diameter peer.

Note: To facilitate troubleshooting, Diameter End Point hostname is recommended to include its network function or any deviation of this (e.g. “mme”, “hss1” …).

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 sec. The Tc timer controls the frequency that transports the connection attempts done to a peer with whom no active transport connection exists.

3.1.3.6 Notification of ME Identity

MME must obtain ME Identity (IMEISV) of the device as part of the E-UTRAN Initial Attach procedure as specified in 3GPP TS23.401 [1]. The MME must then deliver the ME Identity to HPMN as Terminal-Information AVP in the Update Location Request message to HSS, as specified in 3GPP TS29.272 [8]. If IMEI AVP is present in the Terminal-Information AVP, then the Software-Version AVP must also be present.

If MME detects that the ME Identity is changed, the MME must notify HSS about an update of the ME Identity using the Notification Procedure as specified in 3GPP TS29.272 [8]. If IMEI AVP is present in the Terminal-Information AVP in the Notify Request message, then the Software-Version AVP must also be present.

3.1.3.7 QoS for Diameter messages

Both HPMN and VPMN must procure the QoS using the DiffServ Code Point (DSCP). The recommended DSCP values are defined in GSMA PRD IR.34 Section 6.2.7 [11].

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 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 (GTP in this case).

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 GTP protocols, the MME/SGSN performs SGW selection using the S-NAPTR procedure with:

"Service Parameters" = {"x-3gpp-sgw:x-s8-gtp"

"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 GTP protocols, the MME/SGSN performs PGW selection using the S-NAPTR procedure with:

"Service Parameters" = {"x-3gpp-pgw:x-s8-gtp"}

"Application-Unique String" = <APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

In addition, the VPMN SGSNs must support the Gateway selection procedure defined in TS 23.060 Annex A [29] including the UE-capability based gateway selection procedure (based on which an SGSN can be configured to give priority towards SGW/PGW for LTE capable UEs as defined in TS 23.060, Section 5.3.7.1 [29]).

This is required to ensure service continuity for a LTE roamer when moving from GERAN/UTRAN coverage to LTE one in some of the coexistence scenarios described in chapter 4.2.

Additionally, the PGW selection procedure can be enhanced by the APN-OI Replacement mechanism. This allows HPMN operators to introduce subscriber specific PGW selection. The HPMN can define a subscriber specific APN-OI replacement, which will be transported in the subscription information via HLR and HSS. SGSN and MME use the APN-OI replacement value for the DNS query which enables HPMN operators to assign specific PGW address pools via DNS. The detailed handling of APN-OI Replacement is described in 3GPP TS 23.003 [7], TS 23.401 [1] and TS 29.303 [17].

HPMN operators should be aware that the assignment of specific PGW pools will not work if the APN-OI replacement field is ignored by VPMN's SGSN or MME.

Note: The subscriber specific PGW selection is relevant for HPMNs requiring allocation of different PGW per subscriber while using same APN name for all subscribers.

.

3.2.1.3.2 VPMN Roaming

The details of selecting a PGW in VPMN are same as for HPMN Roaming, which is described in the previous section. Section 3.2.1.4 of this document describes further details of local PGW selection for LTE Voice Roaming architecture.

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/SGSN 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 two (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, fallback to GTP version 0 is no longer supported; this has significance if hybrid networks containing legacy nodes are sharing infrastructure.

Additionally, the 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:

- SGW IP address
- MCC/MNC information, present in Serving Network and/or User Location Information (ULI) IE as specified in 3GPP TS 29.274 [4]

The major drawbacks of using SGW 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.
- SGW IP addressing may not be clear when network sharing is implemented.

If a problem occurs in the HPMN, it cannot be unambiguously identified in which VPMN’s radio coverage the subscriber is roaming, as this is usually determined by the presented SGW IP address. As a result, the roaming subscriber could be billed by the HPMN for roaming in a VPMN that was never actually visited by the subscriber.

It is then highly recommended for all VPMNs to ensure that the Serving Network GTP Information Element is included in the GTP “Create Session request” and the "Update Session 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.

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

Note**:** The GTP Serving Network and/or ULI IE are specified in 3GPP TS 29.274 [4] and contain the MCC and MNC combination for the network operator.

3.2.3 Void

3.2.4 Void

3.2.5 Transport layer engineering

As considered by Annex C of TS 23.060 [29], IP MTU baseline over S8 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 need 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.

3.3 S9 Interface

3.3.1 S9 implementation requirements

The S9 interface implementation is not necessary.

Note**:** S9 would be needed if dynamic policy and charging control with home network control is required.

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 and S6d interfaces, the guidelines described in Section 3.1.3 apply.

If both HPMN and VPMN have S6d capability, S6d can be used. The use of S6d must be agreed between two PMNs as part of their bilateral roaming agreement.

If aforementioned condition is not met, then the interface between HSS and SGSN is Gr (GSM-MAP). If HPMN have Diameter-only HSS or if VPMN have S6d-only SGSN, a Diameter-MAP IWF must be implemented in between HPMN and VPMN. The responsibility of the IWF implementation belongs to the PMN that does not support the MAP Gr interface. The IWF can be outsourced to IPX, but this must be done by the responsible PMN.

3.5 Gy interface

3.5.1 Gy implementation requirements

The Gy interface enables online control of data usage by the Online Charging System (OCS) in the HPMN using preconfigured (static or standardized) policies in the VPMN.

3.5.2 Guidelines for Diameter interface over Gy interface

The Gy interface between PGW and Home OCS implements Diameter. For parameters and guidelines for the Diameter protocol see Sections 3.1.3.

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 scenario 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 6 below:

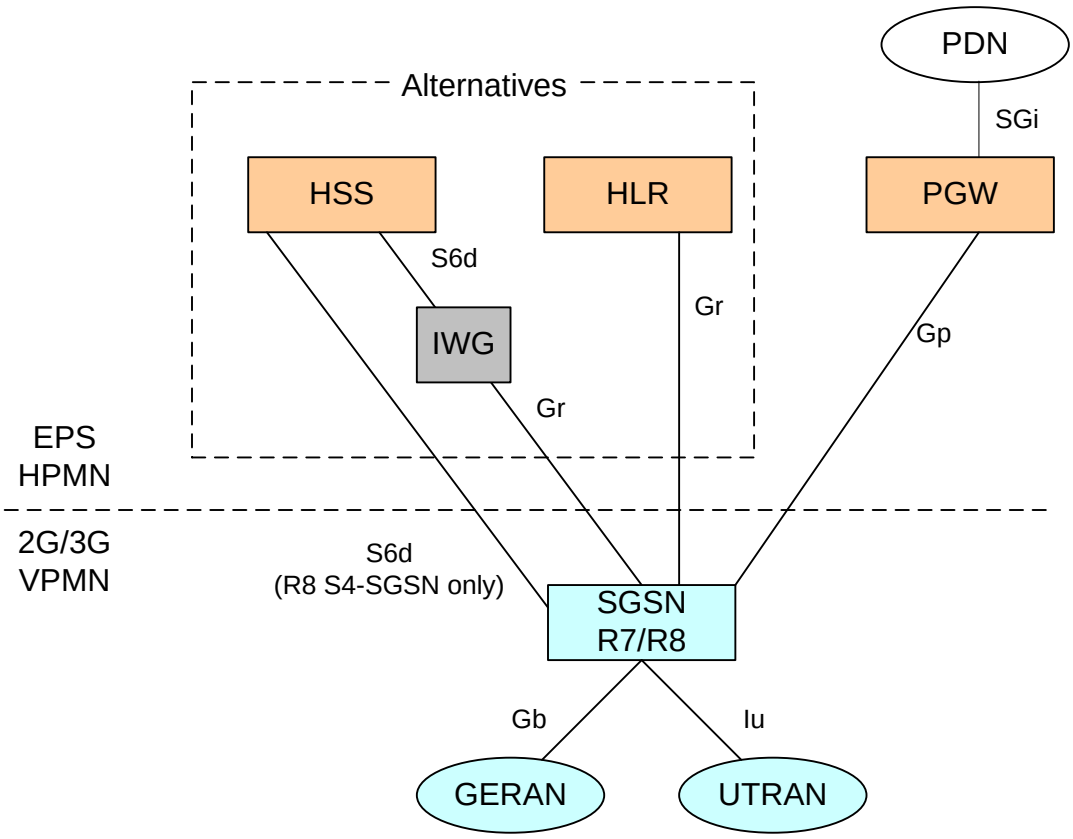

Figure 6: VPMN Legacy Roaming Architecture

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 7 below:

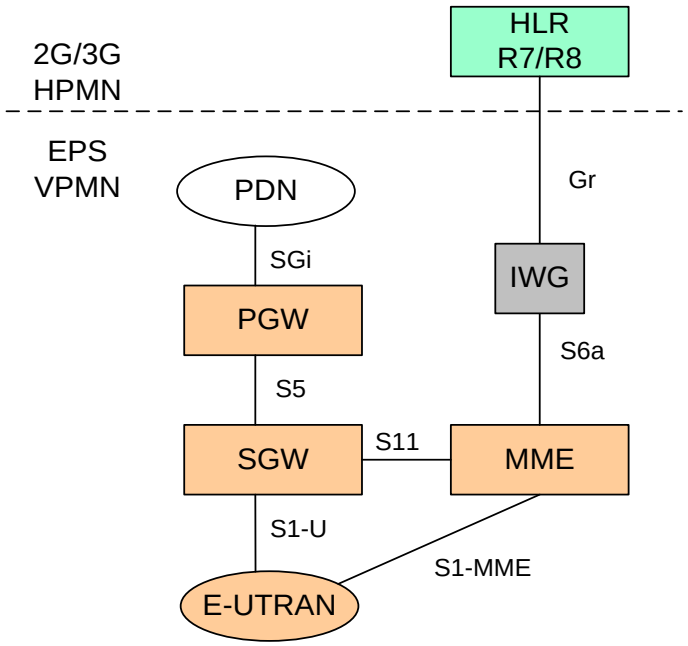

Figure 7: HPMN Legacy Roaming Architecture (local break-out)

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.

The 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.

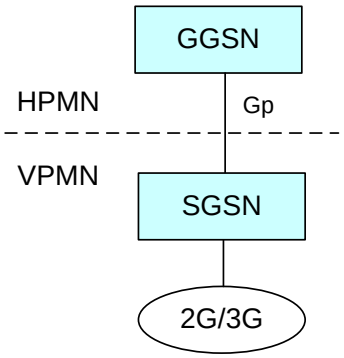

Figure 8: Scenario 1 - Legacy GPRS roaming

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.

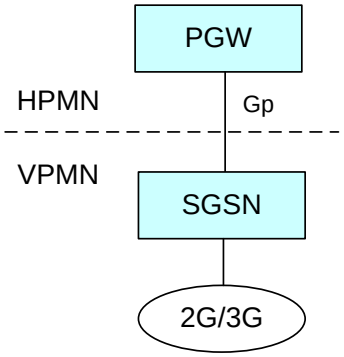

Figure 9: Scenario 2 - HPMN only has PGW as the gateway for roaming

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 HPMN uses different APNs for GGSN compared to PGW. If the HPMN uses the same APNs on both GGSN and PGW, then VPMN 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.

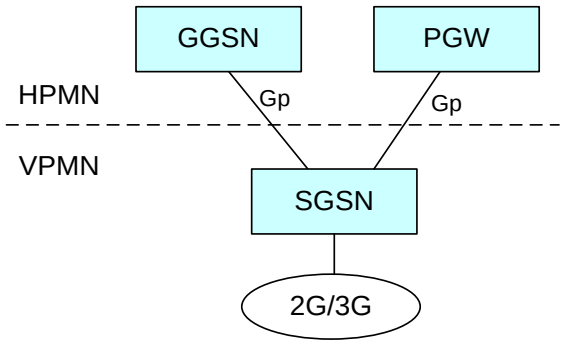

Figure 10: Scenario 3 - HPMN has both GGSN and PGW as the gateway for roaming

4.2.2.2 2G/3G and LTE Roaming Agreement

The following network configurations are permitted, if there is an LTE and 2G/3G roaming agreement between two PMNs. When two PMNs have an LTE and 2G/3G roaming agreement, an 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, PCRF, and MME are omitted in the figures.

DNS must consider both Rel-8 and preRel-8 query procedures defined in 3GPP TS 29.303 [8].

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 a Gp interface towards PGW and SGW has an S8 interface towards the 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.

For scenario 1, the DNS must contain BOTH S-NAPTR (Rel-8) and A/AAAA (pre Rel-8) record for APNs which is registered at PGW.

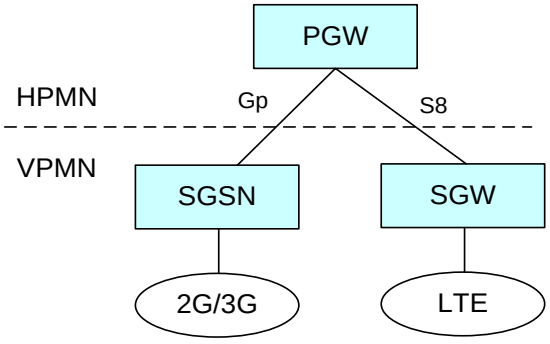

Figure 11: Scenario 1 - HPMN only has PGW as the gateway for roaming, 2G/3G Access via Gp interface

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

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

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

For scenario 2, A DNS must contain BOTH S-NAPTR (Rel-8) and A/AAAA (pre Rel-8) record for APNs which is registered at both the GGSN and PGW.

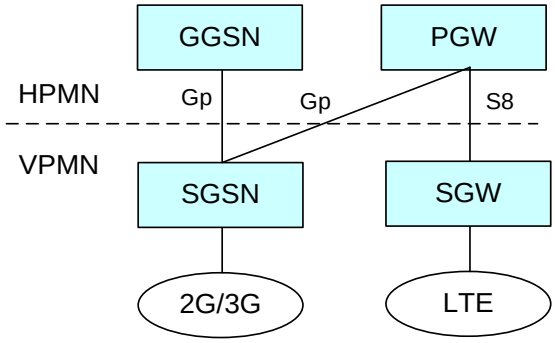

Figure 12: Scenario 2 - HPMN has both GGSN and PGW as the gateway for roaming, 2G/3G Access via Gp interface

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

This scenario depicts a case where a SGSN has a S4 interface towards the SGW, and the SGW has a S8 interface towards the PGW. In this scenario, Inter-RAT handover is anchored at SGW, if the 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.

For scenario 3, DNS must contain ONLY S-NAPTR (Rel-8) records for APNs which is registered at PGW.

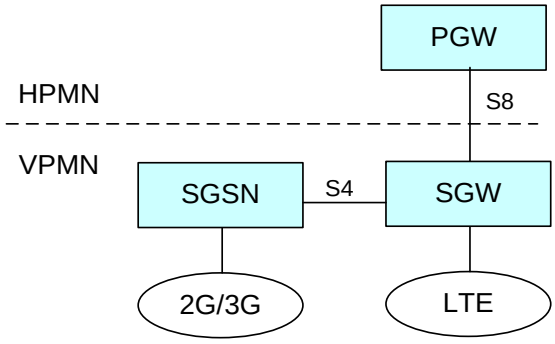

Figure 13: Scenario 3 - HPMN has only PGW as the gateway for roaming, 2G/3G Access via S8 interface

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 a S4 interface towards the SGW and also Gp interface towards the GGSN, and SGW has a S8 interface towards the 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 HPMN uses different APNs for GGSN compared to PGW. If the HPMN uses the same APNs on both the GGSN and PGW, then the VPMN SGSN must use UE-capability as follows: If the UE is LTE capable, then SGW/PGW must be selected, and if the UE is only 2G/3G capable, GGSN must be selected.

For scenario 4, DNS must contain BOTH S-NAPTR (Rel-8) and A/AAAA (pre Rel-8) records for APNs which is registered at BOTH GGSN and PGW

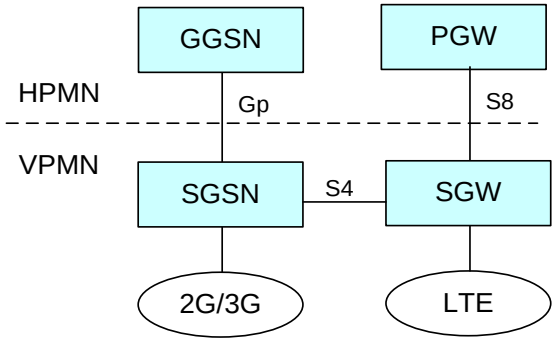

Figure 14: Scenario 4 - HPMN has both PGW and GGSN as the gateway for roaming, 2G/3G Access via S8 or Gp interface

In the following scenario. an operator supports Local Breakout (LBO) for roamers from its roaming partners. It is a requirement in 3GPP TS 23.060 [29] that an S4-based SGSN must for all active PDN connections for a certain UE use either S4 or Gn/Gp. Thus a VPMN must assure that both home-routed PDN connections and LBO PDN connections are using either S4 or Gn/Gp, depending on if Gp or S8 is used towards a certain HPMN. See also Figure 15 and 16, respectively. For gateway interface and protocol configurations, see Annex A in 3GPP TS 23.060 [29].

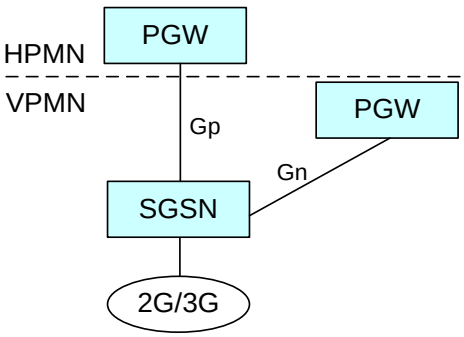

Figure 15: Scenario 5 – two PDN connections, one home-routed and one with LBO, and Gp is used towards HPMN

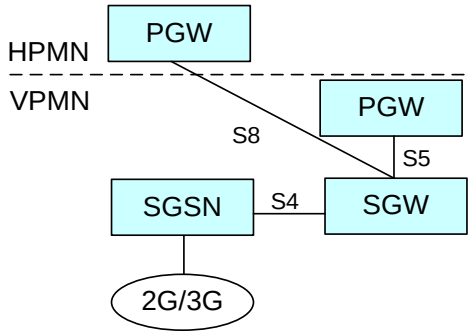

Figure 16: Scenario 6 – two PDN connections, one home-routed and one with LBO, and S8 is used towards HPMN

4.2.2.3 LTE Roaming Registrations

An HPMN may seek to restrict, individual subscribers from roaming on the LTE network of a VPMN, despite a commercial 2G/3G and LTE Roaming agreement.

It is recommended to operators, as the HPMN, when seeking to permit/deny roaming on the LTE network of a VPMN for its outbound roaming subscribers, that the HPMN bars LTE roaming at its HSS for subscribers who are not allowed to use EPS services:

3GPP offers Diameter rejections from the HSS that map to NAS cause code 15 “No suitable cells in this tracking area”. The preferred Diameter rejection message is “Unknown EPS Subscription” code 5420.”

Subscribers are restricted from the LTE network of the VPMN, but are able to try to attach to the VPMNs 2G/3G Radio Access network and be granted access based on applicable roaming agreement.

An attempt to setup the EPS default bearer, from the VPMN LTE network, will not occur, while the statistical reporting and alarming at the VPMN MME will not be negatively impacted.

4.2.3 Consequences of different APN approaches when roaming

When implementing LTE/EPC, an operator needs to decide which services will be offered to its LTE customers and also which APNs will be provisioned for the corresponding services. Internet access and MMS are examples of legacy services that will also be offered to LTE customers as well as 2G/3G customers. For legacy services, the operator has the choice between provisioning the same APNs (single APN approach for a single service) for LTE customers as those provisioned for 2G/3G customers or provisioning new APNs (dual APN approach for a single service) for LTE customers compared to those provisioned for 2G/3G customers. Although both choices are legitimate, the implications for an operator and its customers need to be considered. These are discussed in the following sub-sections.

4.2.3.1 Consequences of the single APN approach when roaming

The single APN approach has implications to the selected gateway in the following scenario:

Table 4 The same APN is provisioned to both 2G/3G customers and LTE customer for the same service.

Table 5 The HPMN is in transition phase and has not yet decommissioned its GGSNs. The corresponding scenarios are scenario 3 of chapter 4.2.2.1 and scenarios 2 and 4 of chapter 4.2.2.2.

Table 6 The 2G/3G customers must be connected to a GGSN for any HPMN specific reason.

Table 7 The VPMN supports the Gateway selection procedure defined in TS 23.060 Annex A [29] including the UE-capability based gateway selection procedure (based on which an SGSN can be configured to give priority towards SGW/PGW for LTE capable UEs as defined in TS 23.060, Section 5.3.7.1 [29]).

Table 8 Issue 1 occurs when the user swaps their 2G/3G provisioned (U)SIM into an LTE device (see below for more information).

The figure below illustrates issue 1. It corresponds to scenario 2 of chapter 4.2.2.2. The same issue occurs with the two other scenarios.

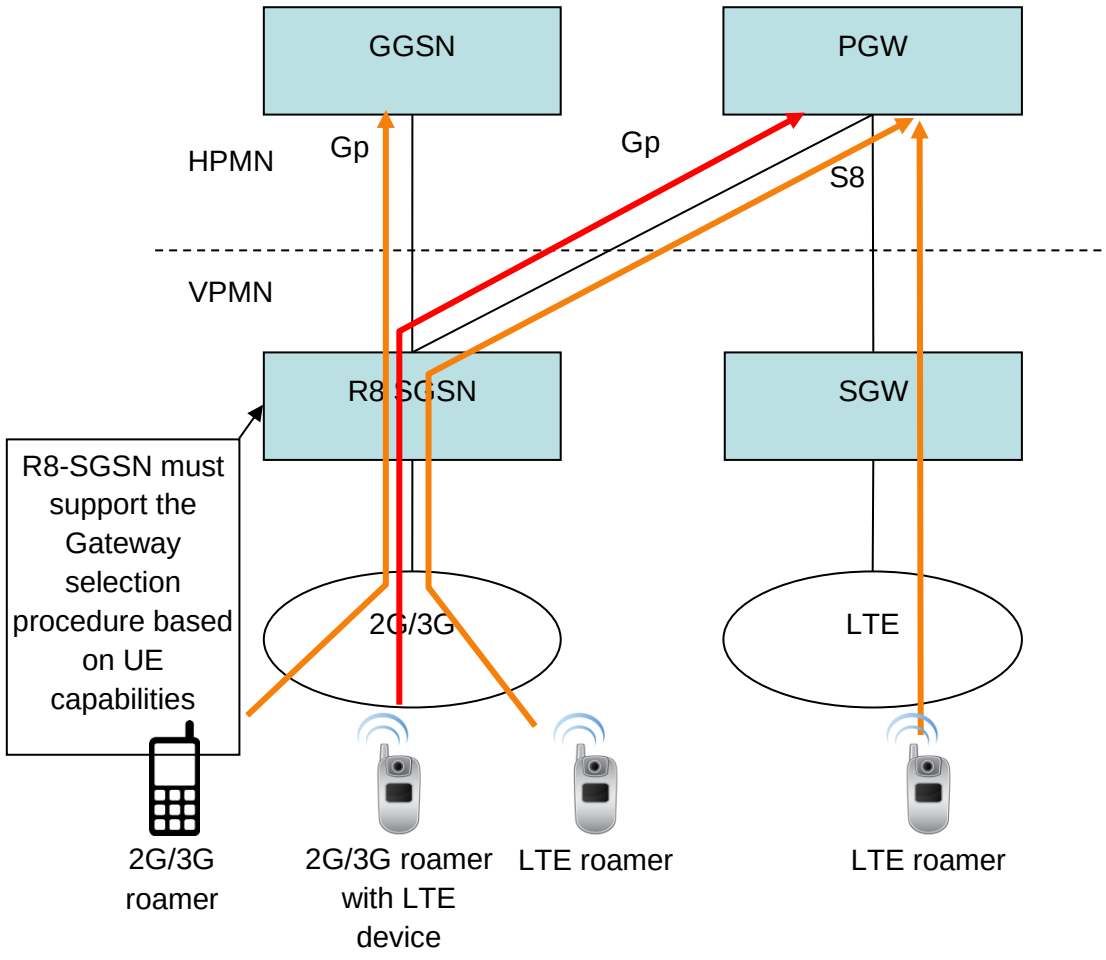

Figure 17: Gateway selection issue for a 2G/3G roamer with a LTE device

Due to the gateway selection procedure being based on both the APN and the UE capability, and not on any subscription information, the R8-SGSN will setup the IP connection of the 2G/3G roamer with the LTE device to the PGW and not to the GGSN as required by the HPMN.

Note**:** As soon as the HPMN decommissions its GGSNs, this issue disappears.

The single APN approach has also implications in this second scenario:

- The same APN is provisioned to both 2G/3G customers and LTE customer for the same service.
- The HPMN is in transition phase and has not yet decommissioned its GGSNs. The corresponding scenarios are scenario 3 of chapter 4.2.2.1 and scenarios 2 and 4 of chapter 4.2.2.2.
- The 2G/3G customers must be connected to a GGSN for any HPMN specific reason.
- The VPMN DOES NOT support the UE-capability based gateway selection procedure.
- Issue 2 occurs when the LTE roamer moves from the GERAN/UTRAN coverage to the LTE one.

In order to guarantee service continuity for subscribers moving between GERAN/UTRAN and LTE coverage it is required to anchor a packet session for LTE capable UEs at a PGW and not at a legacy GGSN.

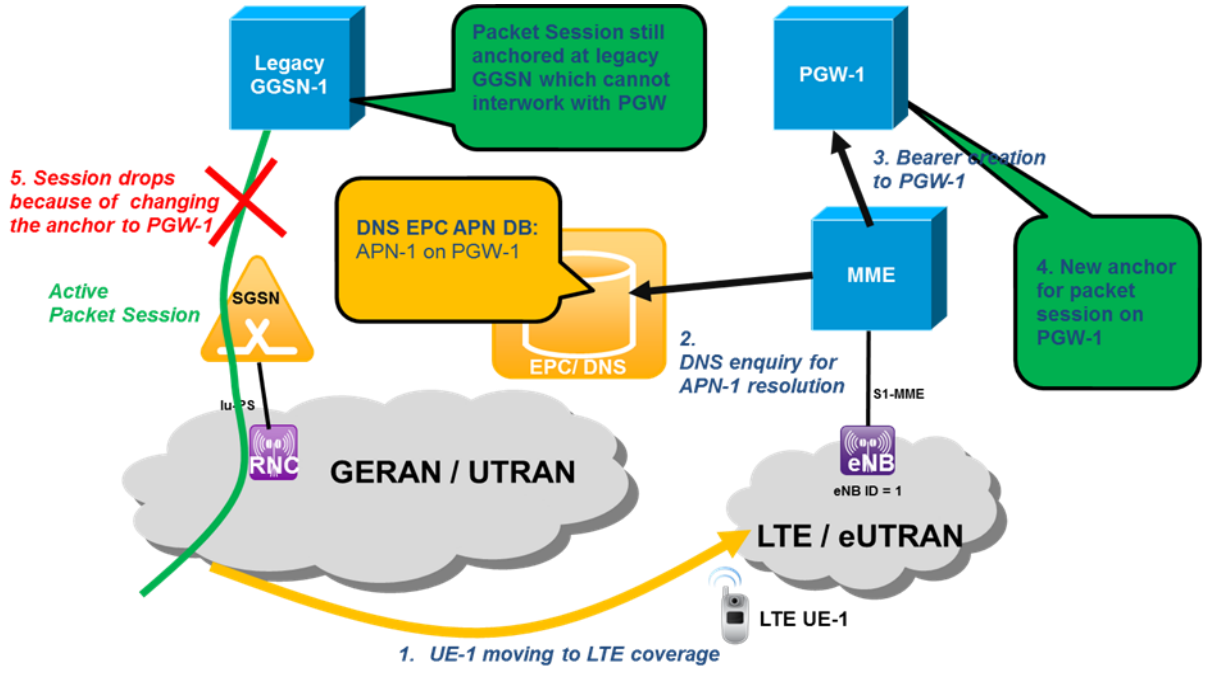

Figure 18: Service continuity issue for a LTE roamer

The PDP session setup under foreign GERAN/UTRAN will succeed if the SGSN does not support the UE-capability based gateway selection procedure. But if the subscriber is reaching LTE coverage in the VPMN and the UE is initiating an inter RAT change from GERAN/UTRAN to LTE the packet session will drop because the anchor will change (see above figure).

Note**:** As soon as the VPMN upgrades its SGSNs to support the UE-capability based gateway selection procedure or the HPMN decommissions its GGSNs, this issue disappears.

4.2.3.2 Consequences of the dual APN approach when roaming

If an operator decides to use dual APNs for its customers (where legacy APNs are provisioned for 2G/3G customers only and different APNs are provisioned for LTE customers), the following must be noted:

- Different APNs are provisioned for different customers (2G/3G and LTE customers) for the same service therefore requiring additional testing.
- 2G/3G roamers with legacy devices will continue to be anchored on the GGSN based on DNS queries by the SGSN.
- LTE roamers will be anchored on the PGW.
- A 2G/3G roamer using an LTE device (SIM swap scenario) will be anchored on the GGSN.
- An LTE roamer camping on UTRAN/GERAN will be anchored on the PGW. This ensures session continuity when the LTE roamer moves to LTE coverage.

Guidance regarding the APN approach when roaming

4.2.3.3 Guidance regarding the APN approach when roaming

Based on the considerations in sections 4.2.3.1 and 4.2.3.2, the HPMN operator should take into account when choosing the APN approach when roaming:

- If the HPMN has decommissioned its GGSNs, the single APN approach has no issues.
- If the HPMN is in transition phase and has not yet decommissioned its GGSNs, the dual APN approach has no issues.

Additionally, even if having a single EPS profile for both UTRAN and E-UTRAN access, GPRS and EPS profiles may have to co-exist and need to be coherent in terms of subscriptions.

As a consequence, and to guarantee session continuity and coherent QoS handling between 3G and LTE for dual APN approach, HPMN is recommended to deploy same couples of APN, PDN Type and, depending on local configuration, context-ID, on both Gr and S6a interfaces.

4.3 Inter-RAT Handover

4.3.1 Handover and access restriction to/from 2G/3G and LTE

4.3.1.1 Introduction

Requirements on handover to/from 2G/3G and LTE are partly captured in Section 4.2. The following sections outline requirements for the Inter-RAT handover.

4.3.1.2 Handover restriction to/from 2G/3G and LTE (Active mode)

As illustrated in Figure 19, an LTE capable UE in 2G/3G access can be frequently handed over to LTE and any active data connectivity can be severely disrupted under the condition that a roaming agreement exists for 2G/3G but not for LTE between the PMNs.

A similar problem can happen also when:

1. A UE in LTE access is handed over to 2G/3G under the condition that a roaming agreement exists for LTE but not for 2G/3G between the pmns; or
2. The subscriber does not have the subscription to use the specific access type (for example, LTE), even when a roaming agreement exists for both LTE and 2G/3G between the pmns.

Note 1: Item 1 described above is considered a migratory problem while operators update their existing roaming agreements to encompass all the radio accesses.

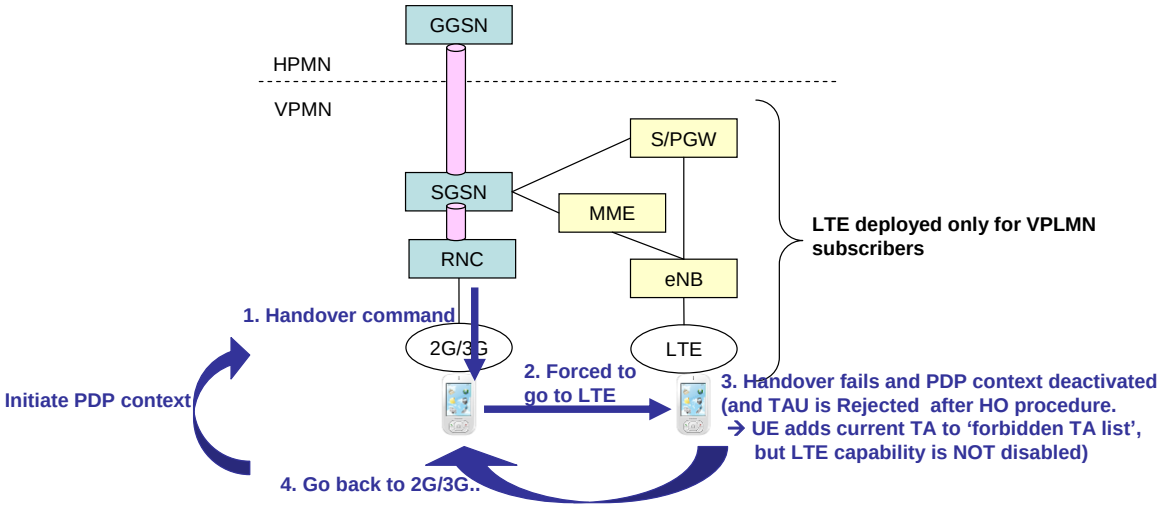

Figure 19: Possible service disruption scenarios

In order to avoid such service disruption for the inbound roamers, a PMN must utilise the functionality to restrict Inter-RAT handover as specified in 3GPP Rel-8 specifications as follows:

- For UTRAN and GERAN Iu-mode, if there is no LTE roaming agreement with the PMN of the inbound roamer, the SGSN and RNC must utilise "E-UTRAN Service Handover" IE to restrict handover to E-UTRAN, as specified in TS 23.060 [29] and TS 25.413 [43].
- For GERAN A/Gb-mode, if there is no LTE roaming agreement with the PMN of the inbound roamer, the SGSN and BSS must utilise "Service UTRAN CCO" IE to restrict handover to E-UTRAN, as specified in TS 23.060 [29] and TS 48.018 [44].
- For E-UTRAN, if there is no 2G/3G roaming agreement with the PMN of the inbound roamer, the MME and eNB must utilise "Handover Restriction List" IE to restrict handover to UTRAN/GERAN, as specified in TS 23.401 [1] and TS 36.413 [45].

The MME and SGSN are responsible for managing the list of roaming agreements. SGSN must be capable of handling “Access Restriction Data” IE as specified in TS 29.002 [46] and “Access-Restriction-Data” AVP as specified in TS 29.272 [8], and MME must be capable of handling ““Access-Restriction-Data” AVP as specified in TS 29.272 [8], so that they can appropriately set the IEs listed in section 4.3.1 when HLR/HSS indicates that there’s no necessary subscription to use the target access network.

The use of "Pre-redirect" feature (which is also known as “RRC reject with redirection”) must not be used unless implementation-specific mechanisms are in place to ensure that the UE is accepted by the target access network’s core network.

To allow VPMN to apply above functionalities, it is recommended that a HPMN includes appropriate access restriction data in the subscriber profile if the user does not have a subscription to use specific access technology, as specified in TS23.401 [1], TS 23.060 [29], and TS 23.221 [39].

4.3.1.3 Access restriction for 2G/3G and/or LTE (Idle mode)

If a roaming agreement exists for 2G/3G but not for LTE between the PMNs, then the following problematic scenario may exist:

- UE with LTE capability in idle-mode camping on 2G/3G reselects E-UTRAN.
- The UE sends a TAU Request message through eNodeB to MME.
- The MME finds that the authentication procedure fails and returns a TAU Reject message with the cause value #15.
- The UE adds the TA to the forbidden TA list and switches to 2G/3G.
- The steps (1) and (2) occur.
- The UE reads broadcasted system information, finds that the TA is in the forbidden TA list, and switches back to 2G/3G.
- The procedure repeats itself when the TA is removed from the forbidden TA list after implementation specific value between 12h - 24h (as specified in TS24.301 [32]).

The above problematic scenario causes unnecessary signalling traffic for RNC, SGSN, eNodeB, MME, and S-GW of VPMN.

A similar problem can happen also when a UE in idle-mode on LTE access moves to 2G/3G under the condition that a roaming agreement exists for LTE but not for 2G/3G between the PMNs.

The MME and SGSN are responsible for managing the list of roaming agreements. In order to prevent the above-described problematic scenario, the MME and SGSN must provide “Radio Access Technology / Frequency Selection Priority (RFSP) index” to eNB/RNC as specified in TS23.401 [1] and TS23.060 [29]. The RFSP index may be based on VPMN policy on access restriction data received from HPMN or on the roaming agreement. Based on the RFSP index provided, the eNB/RNC uses RRC signalling to provide camping policy to the UE to not camp on either LTE/2G/3G. The UE then does camp in idle mode only on the radio access covered by the RFSP index.

To allow VPMN to apply above functionalities, it is recommended that a HPMN includes appropriate access restriction data in the subscriber profile if the user does not have a subscription to use specific access technology, as specified in TS23.401 [1], TS 23.060 [29], and TS 23.221 [39].

4.3.1.4 Handover of PDN Connections between GERAN/UTRAN and LTE

If the UE has more than one PDN connection on LTE, then upon a handover from LTE to GERAN or UTRAN:

Table 9 If the GERAN or UTRAN does not support secondary PDP Contexts, then only the default bearer of each PDN connection will be maintained and the other (i.e. the dedicated) bearers will be released.

a) The GBR bearers (e.g. voice bearer, video bearer) on the PDN connection to the IMS well-known APN will be released during SRVCC procedure; and

b) All bearers other than the default bearer on all PDN connections will be released during handover of the packet bearers between E-UTRAN and GERAN/UTRAN. All sessions associated with the bearers released during handover will break.

- If the GERAN or UTRAN supports only one PDP context (i.e. concurrent PDP Contexts are unsupported) then only a single PDN connection will be maintained and the PDN connections to all APNs but one PDN connection will be released. Typically, the PDN connection to the Internet APN is retained with PDN connections to all other APNs (e.g. the IMS well-known APN) being released.
- If the GERAN or UTRAN supports more than one PDP context (i.e. concurrent PDP contexts are supported) both PDN connections to Internet APN and to IMS well-known APN can be maintained.

If the UE has only one PDN connection on GERAN/UTRAN that is not to the IMS well-known APN (e.g. a PDN Connection to the Internet APN), then upon handover from GERAN/UTRAN to LTE the UE will need to re-establish the PDN connection to the IMS “well-known” APN, see also GSMA PRD IR.92 [30]. Typically, this will occur after a TAU.

4.3.2 Handover to/from non-3GPP accesses and LTE

Roaming from/to non-3GPP access is not supported in this version of the document. Accordingly, the handover to/from non-3GPP accesses and LTE is not supported in this version of the document.

4.3.3 Bandwidth considerations

4.3.3.1 Issue description and possible cause

When a UE moves from a RAT with lower bandwidth such as 2G/3G to LTE, there is sometimes the case that the UE continues to have a similar bandwidth as in 2G/3G instead of getting a higher bandwidth in LTE.

One cause might be that the HLR is provisioned with a lower bandwidth than the HSS for the same APN, in case the operator has two separate nodes for HLR and HSS.

The basic assumption in the 3GPP specs is that the subscription data is the same irrespective of RAT, so that subscription data in SGSN for 2G as well as 3G is equal to subscription data for LTE in MME.

Note that at Inter-RAT Handover the MME will receive new subscription data from HSS at the end of the procedure, and it can be one option that the MME performs HSS Initiated Subscribed QoS Modification due to the bandwidth change at the end of the Inter-RAT Handover. This will however cause additional signalling all through the network.

4.3.3.2 Possible solutions

The issue described above can be solved by any of the following solutions:

- Subscriber Data: Assure that the bandwidth sent to SGSN from HSS/HLR is high enough to assure a satisfactory bandwidth on LTE.
- PCRF QoS modification at RAT change: Involve the PCRF in QoS modification at RAT change as specified in sections 5.4.3 of 3GPP TS 23.401 [1]. This requires the PDN GW to have a trigger to contact PCRF at RAT change.
- PGW QoS modification at RAT change: If PCRF is not deployed in the operator's network, the PGW can initiate QoS modification based on RAT change.

4.3.4 ARP considerations at handover from LTE to 2G/3G

It is recommended that VPMN and HPMN either support the Evolved ARP as defined in 3GPP TS 23.060 or align the M and H values which are defined in Appendix E of 3GPP TS 23.401 to avoid a possible modification of the ARP value. Modification of the ARP value result in a misalignment of the ARP value authorized in the EPS and the ARP value used in 3G, which may cause increased signalling and a deactivation of the PDP Context by the SGSN.

VPMN and HPMN independently derive the Rel 9 QoS parameter ARP using M and H values and, if supported, Rel 9 QoS parameter Evolved ARP, from the ARP value in LTE as described in to Annex E of 3GPP TS 23.401If VPMN and HPMN do not support Evolved ARP and do not have aligned M and H values, a lower QoS (higher ARP value) may be selected by VPMN and sent to the HPMN GnPGW. The GnPGW may ask PCRF to authorize the new QoS and thereafter it either accepts the value from SGSN or it attempts to modify the value.

Accepting the value will result in a change of the ARP value used in the EPS and the ARP value used in 3G. An attempt to change the ARP value may potentially lead to the deactivation of the PDP context. The causes for deactivation could be a violation of local policies in SGSN or that QoS upgrade is not allowed by the SGSN in the update response. If GnPGW has accepted a lower QoS (higher ARP), SGSN may try to change the ARP value again after receiving subscription data from HLR/HSS and then GnPGW may again ask PCRF to authorize the new QoS.

5 Technical Requirements and Recommendations for Services

5.1 Short Message Service (SMS)

5.1.1 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].

If a VPMN operates a network comprising LTE plus GSM and/or UMTS access(es) and if this VPMN provides a non-IMS SMS service as well as an LTE data service to visiting subscribers, then it must support SMS over SGs.

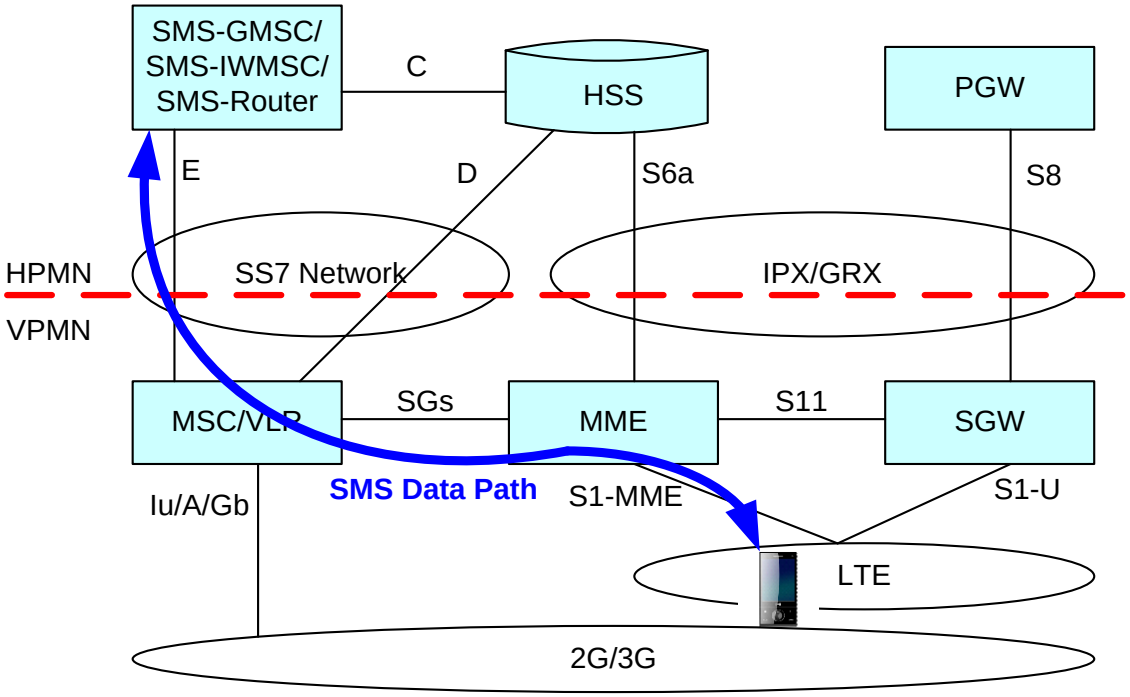

Figure 20: SMS over SGs Roaming Architecture

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

5.1.2 SMS in MME

SMS in MME is a means to provide C-Plane based SMS over LTE access without SGs reference point. SMS in MME is defined in 3GPP TS 23.272 [25].

If a VPMN hasn't SGs reference point(e.g. 3G sunset), then there is a possibility of providing SMS in MME.

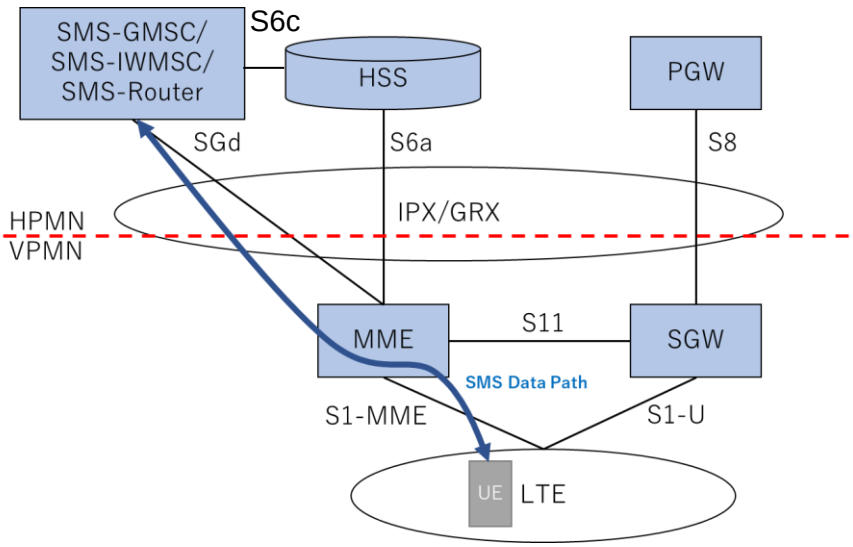

Figure 21: SMS in MME Roaming Architecture

The VPMN must support the following capability.

- Diameter connection and routing between MME to SMSC. For details, see section 3.1.3.
- An indication from MME to the HSS “feature support= SMS in MME Supported” based on the conditions specified in 3GPP TS 29.272 [8].
- An indication from MME to the HSS “SMS-Register-Request” based on the conditions specified in 3GPP TS 29.272 [8].
- MME send SMS-Register-Request to HSS if Notification of SMS over NAS(SGd) described in GSMA PRD IR.21 [40] is supported.
- Setting parameter of SMS-Register-Request is based on 3GPP TS 23.272 Annex C.8.1 [25].
- For details of MO/MT SMS, see 3GPP TS 29.338 [71].
- All others shall be in accordance with 3GPP TS 23.272 Annex C [25].

The HPMN must support the following capability

- Diameter connection and routing between SMSC to MME according to section 3.1.3
- HSS determines whether register MME for SMS or not according to Update Location Request (ULR) from MME, and response Update Location Answer(ULA) to MME.
- For details of conditions for registration, see 3GPP TS 23.272 Annex C.8.1 [25].
- For details for MO/MT SMS, see 3GPP TS 29.338 [71].
- All others shall be in accordance with 3GPP TS 23.272 Annex C [25].

5.2 Voice

5.2.1 CS Fallback

5.2.1.1 General

In some initial deployments, there will be no support of voice services on LTE. However, operators still want users on LTE to access the voice calls. This can be achieved by providing CSFB procedures. CSFB is defined in 3GPP TS 23.272 [25], in 3GPP TS 23.018 [27], and is introduced as an *interim* solution before IMS Voice is deployed. Release 10 compliant CSFB implementation is recommended for voice fallback as some of the Release 8 implementations are not deemed to be efficient enough.

If a VPMN operates a network comprising LTE plus GSM and/or UMTS access(es) and if this VPMN provides a non-IMS voice service as well as an LTE data service to visiting subscribers, then it must support CSFB for voice.

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

Note: Supporting (MAP) PSI (Provide Subscriber Info) in the MSC(-Server) and HLR according to 3GPP TS 23.018 [7] and 3GPP TS 29.002 [18] avoids unnecessary fallbacks to 2G/3G CS due to PSI, that can affect on-going PS sessions of the end user (e.g. suspended sessions if the UE fallbacks to 2G CS) and generate extra Update Locations when the UE switches between 2G/3G and LTE RATs.

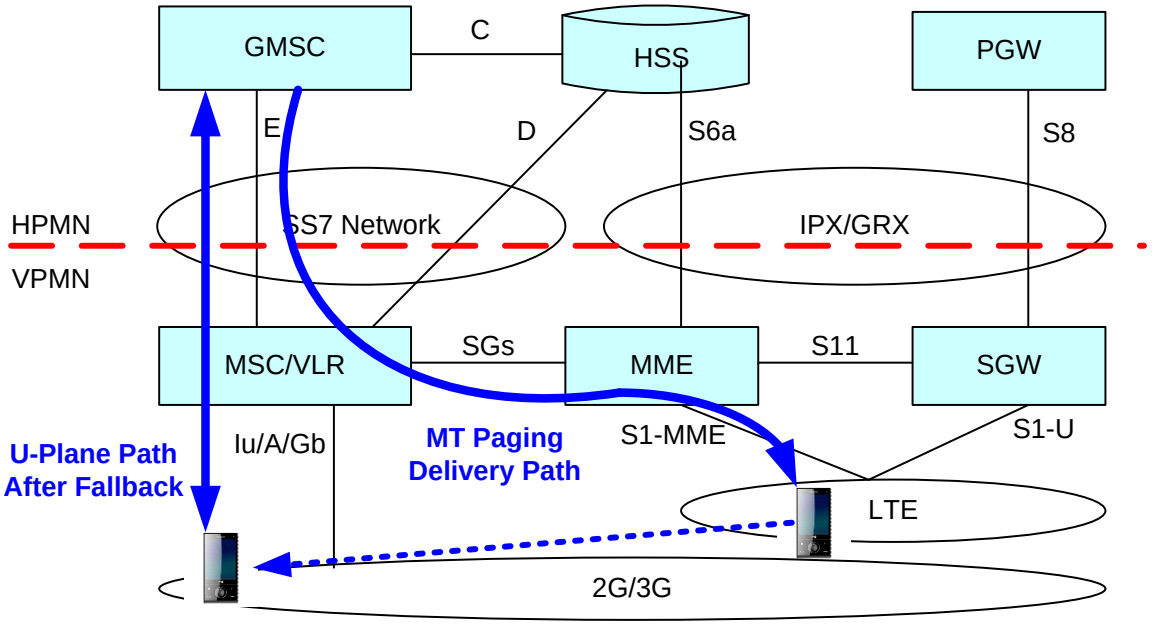

Figure 22: CSFB Roaming Architecture

When CSFB is provided for roaming, either the Roaming Retry procedure or the Roaming Forwarding one can be implemented in the VPMN and the HPMN; it may impact the roaming interfaces (see next sections for the procedures description).

It is highly recommended to implement one or the other procedure since it increases the Mobile Terminating Call (MTC) success rate. If the Roaming Retry procedure or the Roaming Forwarding one is not implemented, then the existing roaming interfaces for circuit switched services will remain unchanged.

The Roaming Retry procedure for CSFB is specified in 3GPP TS 23.272 [25].

Both VPMN and HPMN can implement the Roaming Retry procedure to avoid 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].

5.2.1.2 Roaming Retry for CSFB procedure

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.

The entire concept of CSFB 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) Lists 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.

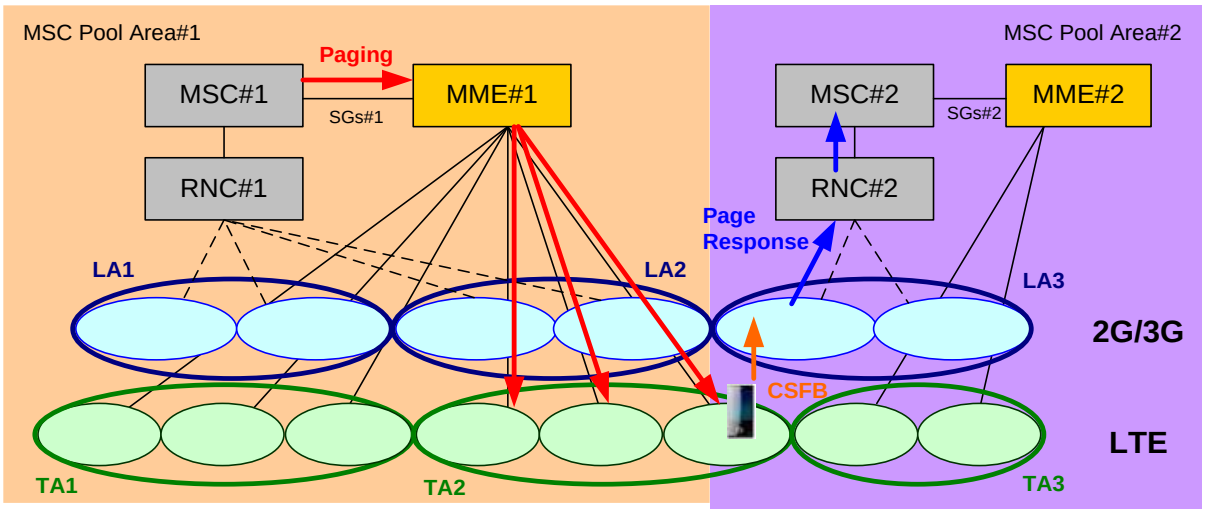

Table 10: CSFB issue due to TA/LA misalignment

When the TA List 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, Figure 22 depicts the case where the UE which is registered under TA2/LA2 of MSC1 receives a paging for an MTC. Depending on the geographical position of the UE when it falls back to 2G/3G, it may select 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 releasing the call leg established between the HPMN GMSC and MSC1 and re-establishing it from GMSC to MSC2, so that MSC2 will understand the paging response and will be able to setup the call. 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 fewer boundaries, but it does not fix it completely unless there is only one pool in the whole VPMN. 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. 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.

5.2.1.3 Roaming Forwarding for CSFB procedure

The Roaming Forwarding procedure for CS Fallback is specified in chapter 7.5a of 3GPP TS 23.272 [25]. This is an alternative solution to Roaming Retry to the problem of TA/LA misalignment that may cause Mobile Terminating Calls fail.

Roaming Forwarding allows forwarding the incoming call from MSC1 to MSC2 so that the Mobile Terminating Call (MTC) setup is successful.

The impacts on the VPMN and HPMN depend on whether the roamer's UE is paged with a Temporary Mobile Subscriber Identity (TMSI) and whether the VPMN has implemented the MAP Send Identification or not.

If the roamer's UE is paged with a valid TMSI when performing the MTC CSFB then the impact is limited to the VPMN. The VMSC must support the procedure using MAP Send Identification as specified in 3GPP TS 23.272 [25] in chapter 7.5a. There is no impact on the roaming interface.

In order to avoid paging the roamer's UE with IMSI when performing the MTC CSFB, the VPMN can implement the procedures for handling of CS services in specific cases as specified in 3GPP TS 23.272 [25] in chapter 4.8. This ensures that the UE and the network have a valid TMSI when paging the UE.

In some implementation cases, the VPMN does not allocate TMSI at all. Then roamer's UE is always paged with IMSI when performing the MTC CSFB. Support of the Roaming Forwarding procedure as specified in 3GPP TS 23.272 [25] in chapter 7.5a in both the HPMN and the VPMN is required to ensure call termination. The Roaming Forwarding procedure impacts on the roaming D interface are listed below:

- The new MSC/VLR includes the “MTRF Supported flag” in the MAP Update Location message sent to the HLR.
- The HLR includes the “MTRF Supported And Authorized” flag, the “new MSC number” and “new VLR number” in the MAP Cancel Location message sent to the old VLR.

5.2.1.4 Coexistence of Roaming Forwarding and Roaming Retry procedures

The procedures can coexist in the VPMN. The choice is at the initiative of the VPMN.

5.2.1.5 Recommended procedures

Whenever it is possible, it is strongly recommended to implement the Roaming Forwarding procedure using TMSI in paging for the following reasons.

- the Roaming Forwarding procedure has a lower call setup time than Roaming Retry
- if the roamer is paged with TMSI then there is no impact on the roaming interface at all

It is also recommended to implement the procedures for handling of CS services in specific cases as specified in 3GPP TS 23.272 [25] in chapter 4.8 to make sure that the UE is always paged with a valid TMSI.

5.2.2 IMS Voice Roaming Architecture

5.2.2.1 General

Details on IMS Roaming over EPS are described in GSMA PRD IR.65 [31].

If the conditions for IMS Voice Roaming (see sections 5.2.2.3) are not fulfilled, then:

During the Initial Attach procedure (irrespective of whether IMS well-known APN is configured to be the default APN or UE requested PDN connectivity procedure takes place):

- Voice domain selection in the UE takes place as specified in 3GPP TS 23.221 [39] (i.e. unless MME indicates the UE that “IMS Voice over PS” is supported, the UE will use CS Fallback or perform PMN re-selection, depending on the network capability and the UE configuration);

5.2.2.2 void

5.2.2.3 IMS Voice Roaming Architecture for S8HR

To support IMS Voice roaming using S8 Home Routed (as defined in GSMA PRD IR.65 [31]), both the PGW and the Proxy-Call Session Control Function (P-CSCF) are located in the HPMN. To select the correct PGW in the HPMN, the HPMN operator must not allow its LTE Voice subscribers to use VPMN addressing. See Section 6.3.3 for a detailed discussion related to gateway selection and a "well-known" Access Point Name usage related to LTE Voice Roaming.

For the VPMN and HPMN to enable S8HR IMS Voice roaming, the following conditions must be fulfilled in EPC and E-UTRAN. Conditions in IMS are not listed:

1. the VPMN must support the following IMS Voice capabilities:

- IMS well-known APN
- SIP Bearer with QCI=5;
- Voice media bearer with QCI=1;
- if videocall is supported, then Video media bearer with QCI=2 (or non-GBR QCI);
- Indication from MME to the UE “IMS VoPS (Support Indicator) = supported” if the VPMN has a roaming agreement that covers support of IMS voice with the HPMN as specified in clause 4.3.5.8 of 3GPP TS 23.401 [1];
- Indication from MME to the HSS "Homogeneous Support of IMS Voice over PS" based on the conditions specified in 3GPP TS 23.401[1].
- Lawful interception of IMS voice calls and SMS as per [62], and data retention
- For IMS emergency calls/sessions, see Section 6.4.

2. the HPMN must support

- IMS well-known APN
- SIP Bearer with QCI=5;
- Voice media bearer with QCI=1; and
- Video media bearer with QCI=2 (or non-GBR QCI).
- Downlink service level gating (to avoid additional and unexpected traffic on the signalling bearer) as described in 3GPP TS 23.401 [1] and 3GPP TS 23.203 [32]. This is also needed to avoid that additional and unexpected traffic on the signalling bearer reaches the lawful interception functions for S8HR in the VPMN.

As ARP settings are exclusively related to the VPMN service prioritization strategy and may change from one the VPMN to another, the following handling for the negotiation of the ARP value should be applied:

- For the establishment of the SIP bearer, the VPMN, may either apply the ARP Priority Level (PL) value received from HSS or apply values as per roaming agreement or local configuration. To prevent that the establishment of the SIP bearer fails, the HPMN should not upgrade the value of the ARP PL.
- For the establishment of the media bearer, the HPMN sends an ARP PL value as per roaming agreement or local configuration. The VPMN should allow the bearer establishment with the ARP PL value received from the HPLMN. However the VPMN may apply the ARP PL value as per roaming agreement or local configuration instead.

For the applicability of the ARP PL values in roaming refer to section 7.2.2.

In addition, in order to enable S8HR IMS Voice roaming, local regulatory requirements in the VPMN need to be fulfilled.

VPMN MME must control all QoS settings. For more details, see sections 7.1.2.1 and 7.1.3.

5.2.2.4 Terminating Access Domain Selection

Terminating Access Domain Selection (T-ADS) optimizes routing of MT calls so that they can be successfully delivered to the UE irrespective of whether or not the UE is camping in an area with IMS Voice over PS supported. For IMS Voice roaming using S8HR, if an HPMN requires T-ADS for its outbound roaming subscribers, then both the HPMN and VPMN must provide the needed functionality as described in GSMA PRD IR.64 [52].

5.2.2.5 IMS Voice Roaming Restriction

VoLTE roaming restriction allows the HPMN to restrict IMS Voice roaming per subscriber and / or per VPMN by excluding the IMS well-known APN from the subscriber data sent from HSS to the MME in the VPMN. If the MME does not receive the IMS well-known APN in the subscriber data, then the MME:

- Is recommended to set the indication “IMS VoPS (Support Indicator) = not supported” to the UE at Attach Accept or TAU Accept as described in section 4.3.5.8 of 3GPP TS 23.401 [1]; and
- Rejects an attempt by the UE to establish a PDN connection to the IMS well-known APN with #33 "requested service option not subscribed" as described in section 6.5.1.4.3 of 3GPP TS 24.301 [32].

Note 1: The MME provides the “IMS VoPS (Support Indicator) = supported” to the UE if the VPMN has a roaming agreement that covers the support of IMS voice with the HPMN as specified in clause 4.3.5.8 of 3GPP TS 23.401[1].

Note 2: HPMN is not required to delete the IMS well-known APN from the subscription profile when HPMN understands that the IMS voice cannot be provided for the corresponding customer in the registering VPMN. The MME of the VPMN needs to provide the adequate “IMS VoPS (Supported Indicator)” value reflecting the IMS voice roaming agreement.

5.2.3 void

5.3 MIoT location

GSMA PRD NG.120 [69] presents the technical alternatives to locate objects in roaming.

Location in LTE networks is described based on the GMLC/MME/SMLC architecture, using potentially different interfaces to retrieve location in roaming.

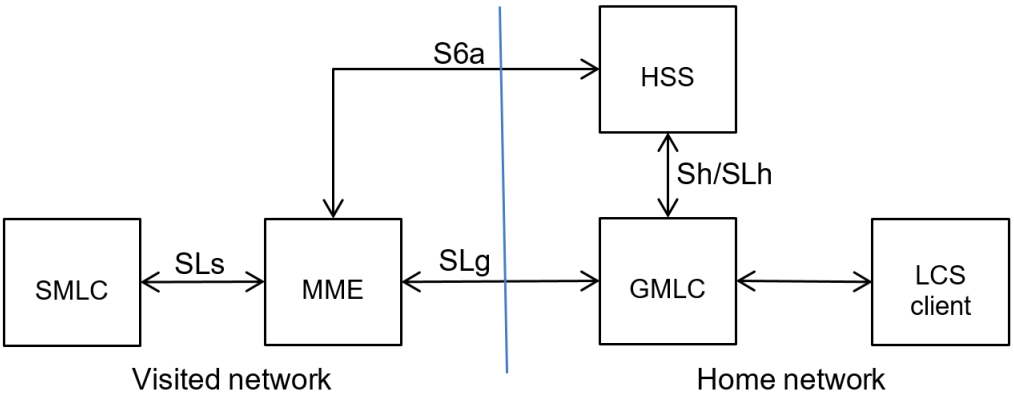

Figure 23GMLC/MME/SMLC architecture

In order to retrieve the location information, 2 different signalling messages could be used:

- S6a: Insert-Subscriber-Data-Request/Answer (IDR/IDA)
- SLg: Provide-Location-Request/Answer (PLR/PLA) (LCS architecture)

Based on those signalling messages, three solutions could be proposed in 4G to retrieve the Cell-Id and the associated geographical coordinates. The solution complexity and accuracy could vary depending on the visited network implementation:

- Cell-Id: the visited MME will provide the Cell-Id (ECGI) to the home GMLC
- Cell geographical coordinates: the visited MME will provide the geographical coordinates (latitude, longitude) of the cell to the home GMLC
- Object geographical coordinates: the visited MME (via the SMLC) will provide the geographical coordinates (latitude, longitude) of the object to the home GMLC

6 Other Technical Requirements and Recommendations

6.1 Access Control

6.1.1 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 MME in 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 is to be rejected, then the appropriate error cause is:

- Cause #15 (no suitable cells in Tracking Area) if the VPMN already has a Roaming Agreement with the HPMN covering other Radio Access Technologies (RATs). It forces the UE to reselect another RAT in the same PMN.
- Cause #11 (PLMN 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 PLMN list" in the USIM and the UE shall no more attempt to select this PMN. Cause #13 may also be used (to avoid permanent storage of PMN in the Forbidden PMN file in the USIM).

IMS Voice over PS Session supported indication shall be sent to a roaming UE (see 3GPP TS 23.401 [1] section 4.3.5.8) only if there is an IMS voice roaming agreement between HPMN and VPMN in place, i.e. the VPMN must indicate that IMS Voice over PS Session is supported on a per roaming partner basis.

Note: If the VPMN incorrectly indicates IMS Voice over PS session being supported in the event of being only a LTE roaming agreement between HPMN and VPMN but no IMS Voiceroaming agreement, then a IMS Voice capable roaming UE that is successfully registered in the IMS can fail to establish Mobile Originating Calls and cannot receive Mobile Terminating Calls under certain conditions (e.g. if attach was successful for EPS only or combined IMSI attached with SMS only, while the HPMN forwards a Mobile Terminating Call via CS domain).

Emergency calls indicator:

For IMS emergency calls/sessions, see Section 6.4.

6.1.1.1 Source SGSN/ MME enforcing access restriction during Inter-RAT RAU/TAU procedures

When the VPMN cannot prevent the UE to camp on the radio access (by using RFSP index as described in 4.3.1.3), then the following scenario may exist:

- The source serving node (i.e. MME or SGSN) has received the appropriate prohibited access restriction data in the subscriber profile.
- The UE performs Inter-RAT RAU/TAU procedure and hence the target node (i.e. SGSN/MME) sends Context Request message to the source serving node (i.e. MME/SGSN).
- The source serving node accepts the mobility procedure despite the access restriction.
- The above scenario causes unnecessary signalling traffic in both VPMN and HPMN:
- Signalling towards HSS to perform the location update procedure and
- Signalling towards the SGW/PGW to modify the existing session or to create a new session. After the RAU/TAU procedure is rejected towards the UE, the MME/SGSN has to perform rollback procedure to clean-up the session state at the target SGW/PGW.

To solve this problematic scenario, if the feature is supported by MMEs/SGSNs, it is recommended that the old SGSN/MME is allowed to reject the Context Request message from the new MME/SGSN based on Access-Restriction-Data received from HPMN as defined in 3GPP Rel-12 TS 29.274 [4] and TS 29.060 [60] and outlined in below:

- During Idle mode mobility from GPRS access (2G/3G) to LTE, if the target radio access type is restricted, the old SGSN may reject the SGSN Context Request message with cause "Target access restricted for the subscriber" (cause #231 in case Gn/Gp SGSN or cause #117 in case S4-SGSN). Then the new MME reject TAU procedure with cause #15 (no suitable cells in Tracking Area) forcing the UE to reselect another RAT in the same PMN.
- During Idle mode mobility from LTE access to GPRS (2G/3G), if the target radio access type is restricted, the old MME may reject the SGSN Context Request message with cause "Target access restricted for the subscriber" (cause #231 in case Gn/Gp SGSN or cause #117 in case S4-SGSN). Then the new SGSN reject RAU procedure with Cause #15 (no suitable cells in Location Area) forcing the UE to reselect another RAT in the same PMN.

6.1.2 Access Control in the HPMN

If the VPMN does not implement the requirements in the previous section, then the HPMN can implement its own access control feature in the HSS to protect its subscribers.

If the HPMN already has a Roaming Agreement with the VPMN covering other Radio Accesses, then the reject indication sent by the HSS back to the MME in the Update Location Answer must be mapped into cause #15 (no suitable cells in Tracking Area).

- It is recommended to use the reject indication DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION (5420) without Error Diagnostic, or with Error Diagnostic of GPRS_DATA_SUBSCRIBED as it must be mapped into cause#15 according to Table A.1 of TS29.272.
- As an alternative, the DIAMETER_ERROR_RAT_NOT_ALLOWED (5421) reject indication can be used instead but the MME must map it into cause#15 instead of cause #12 or cause#13.

If the HPMN has no Roaming Agreement with the VPMN then the HSS can send back Update Location Answer with reject indication set to DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004) without Error Diagnostic back to the MME. This reject indication must be mapped to cause #11 (PLMN Not Allowed).

6.1.3 Access Control in the VPMN for CS Fallback

If the VPMN does not implement CS Fallback feature and the VPMN has Roaming Agreement with the HPMN covering LTE, the VPMN must inform the UE that the VPMN does not support CS Fallback feature. This is compulsory to ensure roamers will be able to reselect the RAT which supports the voice according to CS Fallback capable UE's settings.

The mechanism to achieve this is that if UE performs Combined Attach or Combined Tracking Area Update procedure, MME shall accept this as "EPS only" with cause #18 (CS domain not available), see also clause 5.5.1.3.4.3 in 3GPP TS 24.301 [32]. If voice preferred UE receives cause #18, UE will select 2G or 3G, and if data preferred UE receives cause #18, UE will stay in LTE, following the rules as defined in 3GPP TS 23.221 [39] and 24.301[32].

If the VPMN only has a roaming agreement for E-UTRAN with the HPMN of the UE, upon receiving an SGs AP-LOCATION-UPDATE-REJECT message with either MM cause #11 or MM cause #13, then the MME should map the MM cause to EMM cause #18, as specified in Release 12 3GPP TS 29.118 [x]. This allows Data Centric UEs to stay in the same PMN, and Voice Centric UEs to select different PMN.

6.2 Addressing

6.2.1 UE Addressing

6.2.1.1 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 (The word 'capable' means that the UE is capable to establish/receive CS calls).
- The UE is capable of SMS.

6.2.1.2 IP

Every LTE capable UE allocates (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. 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 3.5.1 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 **:** The MME and SGW are assumed to always support the same PDN Types, since they are always in the same network that the VPMN is in.

Note : 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.

6.2.2 Network Element Addressing

6.2.2.1 IP and SS7

EPC is designed to be an "all IP" architecture. Thus, all EPC 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, S6d, S8, Gy and S9 interfaces. Internal addressing and routing is a decision for the Service Provider.

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.

6.2.2.2 Fully Qualified Domain Names (FQDNs)

All EPC 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 EPC/LTE network elements can be found in GSMA PRD IR.67 [21] and 3GPP TS 23.003 [7].

6.2.2.3 Diameter Realms

All EPC 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 EPC need to be provisioned in DNS).

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

6.3 APN for IMS based services

6.3.1 Introduction

The IMS well-known Access Point Name (APN) and an APN for related Home Operator Services are defined below. For more details on when these APNs are used, see GSMA PRD IR.65 [31] (for the general case), GSMA PRD IR.92 [30] (for Voice and SMS over LTE, IR.94 [55] (for video over LTE) and GSMA PRD RCC.07 [47] (for Rich Communication Suite).

Note: The APN for Home Operator Services was formerly known as the "APN for XCAP/Ut". Its name was changed after further IMS-based services beyond Supplementary Services configuration via IMS were identified in GSMA PRD RCC.07 [47] as needing to utilise a PDN located in the HPMN e.g. for XCAP, IMAP and HTTP.

For cases when the IMS well-known APN is kept if the UE moves into 2G/3G coverage, or when it is activated while the UE is in 2G/3G coverage, the Signalling Indication attribute (see also 3GPP TS 23.107 [51]) needs to be set in the QoS profile in the HLR / HSS.

For cases when the IMS well-known APN is activated while the UE is in 2G/3G coverage, the subscription setting defined in the gateway selection, see Section 6.3.2.2, must be taken into account in the HLR / HSS in order to ensure consistency between GPRS and EPS profiles.

In a transition phase, the IMS well-known APN might be used where only a data Roaming agreement is in place to handle other services (e.g. RCS) that are not covered by enforcing Roaming agreements. In that case, the traffic towards the APN shall be home-routed and bearer establishment procedures, including QoS handling, shall follow the same process as any other APN with home-routed traffic according to the data Roaming agreement as defined in section 3.2 and as well as to the QoS limits as defined in section 6A.1.1 and 7.1.2 of this document.

6.3.2 IMS well-known APN

6.3.2.1 Definition

The Network Identifier (NI) part of the APN must be set to "IMS" bythe UE. The APN Operator Identifier (OI) part of the full APN must be blank as it is appended to the NI part by the VPMN and its value depends on the HPMN whose PGW the UE is anchored.

For IMS emergency calls/sessions, see Section 6.4.

6.3.2.2 Gateway Selection

The IMS well-known APN a PGW in the HPMN when S8HR roaming. Therefore, when enabling IMS voice roaming for a subscriber, the following subscription settings must be taken into account for the IMS well-known APN:

- 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, if set, is set on a per VPMN basis.

  a) For IMS Voice roaming using S8HR, the "VPLMN Address Allowed" parameter must not be present or must be set to “NOTALLOWED (0)”.

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 does 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.

The gateway selection logic in all MME and SGSN must select a PGW in the same PMN for the IMS well-known APN for a particular subscriber, i.e., all must select a PGW in the HPMN.

Note: If not all SGSN and MME would select a PGW in the same PMN, then there are scenarios in which a PGW is selected for the IMS APN in the HPMN and the UE moves into an area where the PGW needs to be in the VPMN.

6.3.2.3 Inter-PLMN roaming hand over

If the PDN connection to the IMS well-known APN is maintained after moving from one PLMN to another, because an inter-PLMN roaming agreement is in place, then the PGW must disconnect the PDN connection to the IMS well-known APN unless the inter-PLMN roaming agreement in place allows this PDN connection to continue.

Note 1: This ensures that the PLMN where the UE has moved to provide the local PGW and the PDN connection to the IMS well-known APN, see also GSMA PRD IR.65 [31].

Note 2: The behaviour recommended in the present section may not apply in the case of national roaming; that case is FFS.

6.3.2.4 Network-initiated deactivation and re-activation of the PDN connection to the IMS well known APN

For network-initiated deactivation with reactivation of the PDN connection to the IMS well known APN, the network must support the procedures as specified in 3GPP TS 23.401 [1] sub clauses 5.4.4.1 and 5.10.3.

Note 1: Care needs to be taken when the MME needs to restore the PDN connection for many UEs to avoid signalling overload (for example in the case of node restart as specified in 3GPP TS 23.007 [41])

Note 2: Reactivation requested by the network when deactivating a PDN connection does not work with pre-Release 9 LTE UEs, but according to GSMA PRD

IR.92 [30] sub clause 2.4.2.1, a UE must always re-establish the PDN connection to the IMS “well known” APN if the PDN connectivity is lost.

6.3.3 APN for Home Operator Services

6.3.3.1 Definition

The Network Identifier (NI) part of the APN is undefined and must be set by the Home Operator. The requirements for the value of the APN NI are as follows:

- must be compliant to 3GPP TS 23.003 [7] section 9.1.2;
- must resolve to a PGW in the HPMN; and
- must not use the same value as the IMS well-known APN (as defined in Section 6.3.2.1).

Home operators can choose to reuse an APN for already deployed services (e.g. Internet access, WAP, MMS, etc.) or choose a new, specific APN for the APN for Home Operator Services. A comparison of both approaches is given in the table below:

Reusing an existing APN	Using a new/specific APN
Limits the number of PDN Connections required by a UE at any one time	May increase the number of PDN Connections required by a UE at any one time.
Separate charging, QoS and routing to other services (e.g. Internet access, WAP, MMS, etc.) may be more difficult or even cannot be applied on a per APN basis.	Separate charging, QoS and routing to other services (e.g. Internet access, WAP, MMS, etc.) may be easier to apply on a per APN basis.
Depending on UE implementation, Home Operator Services may be negatively affected if the user changes the APN value to receive another service that uses the same APN in a different way e.g. user changes the value to "euinternet" to receive Internet access from an LBO Provider when roaming (see IR.33 [10] for more information on LBO Providers).	Ensures UE implementations provide separate routing for Home Operator Services compared to others, and thus changes to APNs for other services will not affect the routing or availability of Home Operator Services.

Table 11: Relevant interfaces for LTE and EPC roaming

If using a new/specific APN, then the value "hos" (case insensitive) is recommended.

The APN Operator Identifier part of the full APN should be blank as it is automatically derived and appended to the NI part by the VPMN.

6.3.3.2 Gateway Selection

The APN for Home Operator Services utilises a PGW always in the HPMN. Therefore, when enabling IMS roaming for a subscriber, the following subscription settings must be taken into account for the APN for Home Operator Services:

- The bar on "All Packet Oriented Services" is not active
- The "VPLMN Address Allowed" parameter in the HSS is unset.

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 APN for Home Operator Services 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 APN for Home Operator Services and the APN for Home Operator Services is a new/specific APN (see section 6.3.3.1), 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 APN for Home Operator Services (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 does 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 APN for Home Operator Services as the Default APN.

6.3.3.3 Inter-PLMN roaming hand over

If the PDN connection to the APN for Home Operator Services is maintained after moving from one PLMN to another, because an inter-PLMN roaming agreement is in place, then the PGW need not disconnect the PDN connection to the APN for Home Operator Services unless the inter-PLMN roaming agreement in place enforces this PDN connection to discontinue.

Note 1: The behaviour recommended in the present section may not apply in the case of national roaming; that case is FFS.

6.3.3.4 Network-initiated deactivation and re-activation of the PDN connection to the APN for Home Operator Services

There are no requirements for the APN for Home Operator Services to be reactivated after a network-initiated deactivation. It is assumed a UE will activate PDN Connections to the APN for Home Operator Services only when required and subject to any other services also using the same APN.

6.3.3.5 Data Off related functionality

3GPP PS Data Off and 3GPP PS Data off Exempt Services have been defined in GSMA RPD IR.92 [30]. This section applies when the UE has activated 3GPP PS Data Off.

The home network supporting 3GPP PS Data Off, as defined in 3GPP Release 14 TS 23.401 [1], must only send IP packets for services that are configured as 3GPP PS Data Off Exempt Services.

Note: IPv6 Router Advertisement IP packets are an essential part of the UE IP address configuration. Although these packets do not belong to any specific 3GPP Data Off Exempt Services, they are still sent over the PDN connection.

6.4 Emergency Service

6.4.1 General

This section describes the emergency call for IMS roaming. IMS emergency services are provided to inbound roamers as per policy of the VPMN. It is recommended that the applicability of IMS emergency services is agreed between the VPMN and the HPMN in the IMS voice roaming agreement. For a description of the impact to VPMNs and HPMNs to support IMS Emergency services refer to GSMA PRD IR.65 [31].

As stated in clause 4.3.12.1 of 3GPP TS 23.401 [1], IMS emergency services can also as per policy of the VPMN be provided to inbound roamers without an IMS voice roaming agreement, inbound roamers with an IMSI that cannot be authenticated or inbound roamers without an IMSI.

Sections applicable to S8HR only are marked accordingly.

6.4.2 Emergency PDN connection

An emergency PDN connection is established to a PGW within the VPMN 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 VPMN, 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 specifications 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 PGW address used for emergency calls/sessions must be configured to the MME/SGSN.

6.4.3 S8HR and support of Anonymous Emergency Call

To support IMS emergency calls for inbound roamers, the VPMN must support anonymous emergency calls over IMS as described in GSMA PRD IR.92 [30], and GSMA PRD IR.65 [31].

Note: S8HR requires support for anonymous emergency calls over IMS.

IMS emergency calls are not supported by inbound roamers in cases where the VPMN

- supports IMS emergency procedures,

- has no IMS NNI relationship with HPMN and
- does not support/allow anonymous emergency calls.

6.4.4 Emergency Call Indicator

To control the domain of the emergency call, the VPMN MME must indicate the “Emergency bearer service indicator” (EMC BS) to “1” if the IMS emergency call is required, and to “0” if CS fallback emergency call is required. This bit can be set differently for own users and for inbound roaming users. The bit can have different values for different roaming partners. The value of the bit does not need to be homogeneous if emergency calls are provided on different domain depending on the roaming partners.

6.5 Security

Ensuring adequate security levels 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.

Due to interconnect and roaming, the inner PMN is exposed to other networks. Consequently, measures to securely allow partners to interconnect in a controlled way have to be deployed, without revealing confidential information or facilitating fraud/abuse. PMN operators and IPX Providers are advised to adhere to the recommendations which are given in this section.

As GRX/IPX, as defined in GSMA PRD IR.34 [11] is a dedicated Roaming/Interworking Network which is separate from the Internet, it is thought to be reliable and more secure than the Internet. Thus no extra security features are needed in the Service Provider to Service Provider interface in addition to those which are standardised for the protocols in use. Since the Internet Protocol (IP) is not secure, it is still highly recommended to implement adequate security tools and procedures to prevent, monitor, log and correct any potential security breaches at all levels. Typically, this means as a minimum implementing a firewall (FW), (Border Gateway (BG) is typically used in MNO (Mobile Network Operator) networks) to enable ACL (Access Control Lists) or similar mechanisms to prevent unwanted access to Service Provider core networks, such as:

- Certain types of traffic (for example Small ICMP packets, HTTP and IPSec).
- The BG should also be able to filter out unnecessary traffic coming from the Inter-Operator IP Backbone. (Specifically, everything that is not agreed in an IPX Provider agreement).
- Filter out all IP traffic other than that which has been originated from IP address ranges of commercial roaming partners.
- Signalling rate limiting and DoS/DDoS prevention for all network protocols that are utilised should be implemented to protect the PMN from flooding attacks.

More detailed information on security demands and solutions can be found in the GSMA PRD IR.77 [9]. Background on the security requirements in this section can be found in Annex C.

Note**:** The texts “SP” (= Service Provider) and “ISH” (= IPX Service Hub) in square brackets (“*[SP]*”, “*[ISH]*”) denote if a security requirement is to be met by the Service Provider and/or by the IPX Service Hub.

6.5.1 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 [58],
- 3GPP TS 33.117 [59].

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 particularly 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 manipulated 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 manipulated 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 manipulated 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.

The use of "GTP-aware" firewalls is considered good security practice for PMNs. When GTP-aware firewall is deployed for EPC/LTE, the firewall must support the GTPv2 protocol. GTP-aware firewalls 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") should be used with extreme caution. If the firewall is not upgraded to support the most recent 3GPP release of GTPv2 used by the network elements in the HPMN and VPMN, this feature breaks the extensiveness of GTP in that if either the HPMN or VPMN in a roaming partnership upgrade to a later 3GPP release of GTPv2, but have not upgraded the GTP-aware firewall in the other PMN, this results in any messages being dropped 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, can 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.

An in-depth coverage of GTP security is provided in PRD FS.20 [58].

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

6.5.2 Diameter Security – "Hop by hop" Approach

By default,Diameter does not provide end-to-end security on the application layer in the case of international roaming. Thus it relies on "hop-by-hop" security mechanisms on lower layers and it requires additional security measures. They are all covered in this section and PMN Operators and IPX Service Hubs are recommended to adhere to these requirements in order to achieve secure inter-PMN signalling for LTE Roaming.

Note: Please be referred to section 6.5.3 for the additional Diameter "end-to-end" solutions.

A detailed Diameter interconnect security assessment and associated recommendations are contained in PRD FS.19 [60].

All security requirements provided in this section are in force, whichever DIAMETER application handled by DIAMETER nodes (S6a, S6d, S9, Gy…) are used.

If the DEA is outsourced to the IPX Provider (see Figure B-6), the IPX provider is responsible for deploying and maintaining all the security measures described for the Service Provider in this section.

6.5.2.1 Network Domain Security for IP

The IP level security shall be enforced on each hop of the hop-by-hop architecture.

A hop is defined between 2 Diameter aware nodes (Diameter agent or Diameter end point) and IP level security measures on this hop shall be defined in order to guarantee following security services:

- Privacy, i.e. no third party gets access to the traffic between these two nodes
- Traceability, i.e. each node knows which previous party sent or forwarded a message
- IP anti-spoofing

Service providers are free to choose if they wish to have a direct bilateral connection to the peer Service Provider or if IPX Service Hubs are involved. As a consequence, the three options which are described next are applicable.

Note**:** The network elements in the figures are logical components and it is at the discretion of the IPX provider and PMN operator to decide if they are kept separate or joined in a single physical component.

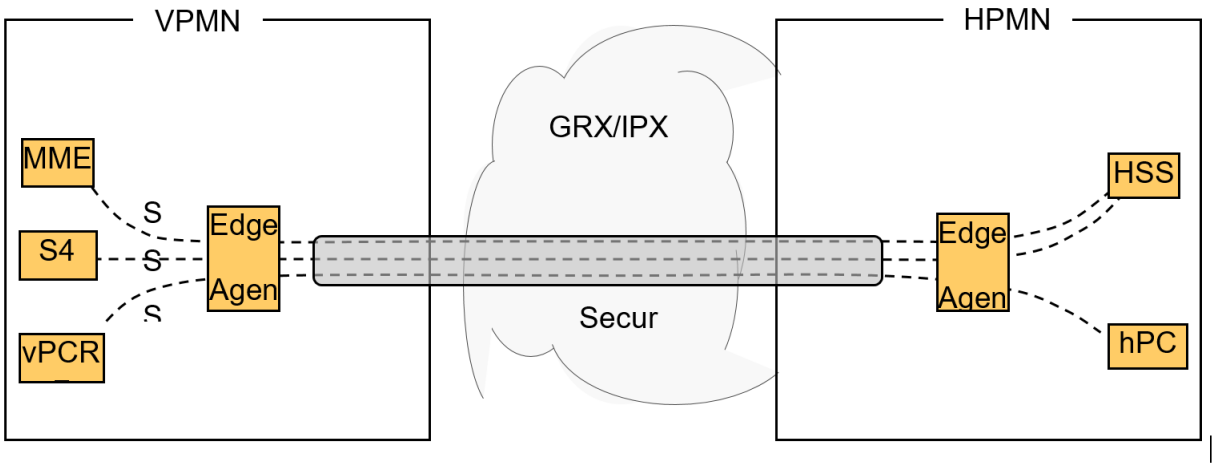

Figure 24: Security for IPX Transport connectivity

Figure 24 shows the PMN interconnection in bilateral mode with direct peer connections between PMN Edge agents, which is secured allows secured connections between PMNs.

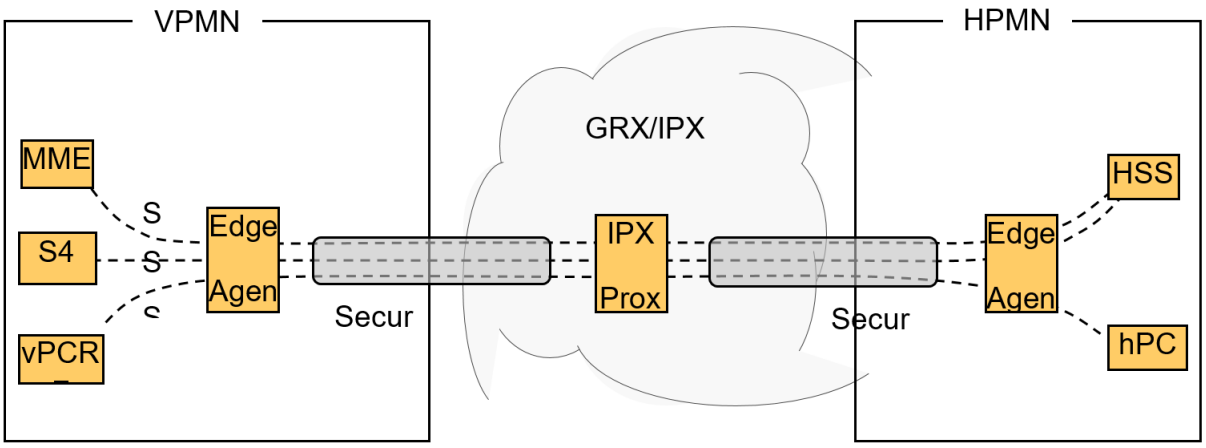

Figure 25: Security for IPX Service Hub connectivity

Figure 25 shows the PMN interconnection utilising the “IP Service Hub” connectivity option according to GSMA PRD IR.34 [11]. This option is secured hop-by-hop between each PMN and the Service Hub. The simplified cloud which is titled GRX/IPX may resemble one or two IPX providers. The security is only terminated at PMNs and Service Hubs. If there are two Service Hubs involved the communication between IPX Service Hubs shall be secured too. This is depicted in Figure 26.

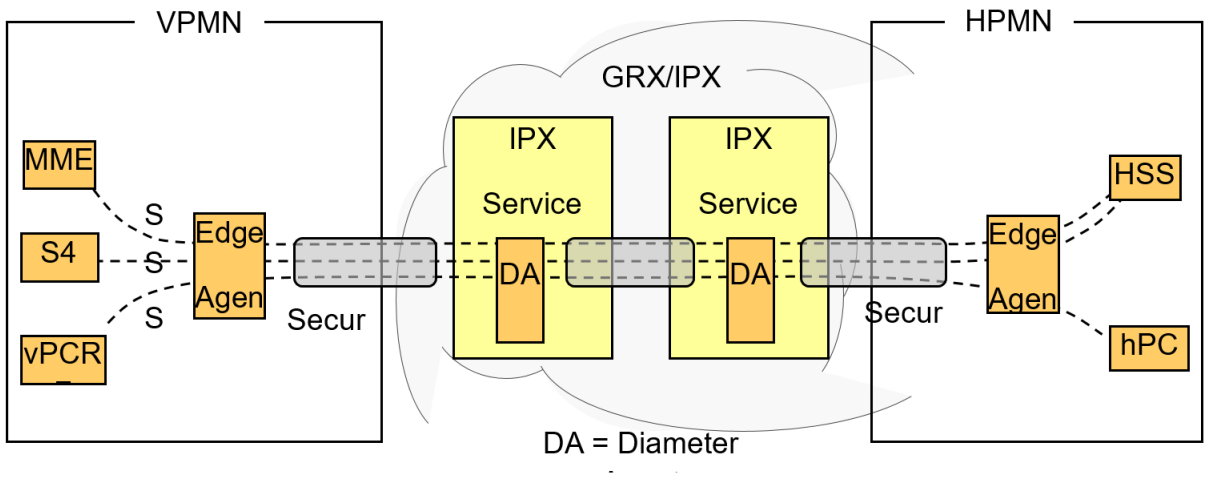

Figure 26: Security for connectivity with two IPX Service Hubs

According to GSMA PRD IR.34 [11], details of the “IPX Service Transit” connectivity option are for further study. If this option is used, it needs to follow the same security model as the “IP Service Hub” connectivity option.

In the figures above, a secure Diameter hop is depicted by a grey tunnel symbol. In any model, both ends of a secured hop are responsible for providing the above mentioned security services. The IP messages exchanged in each hop can be protected by one of the following technical network implementations:

- Direct physical connections
- IPsec connections (see Appendix D for more details)
- Other networks that create a logical bilateral link between the two ends of a Diameter hop connection (e.g. MPLS network)

These network implementations are the foundation to deliver the aforementioned security services privacy, traceability, and IP antispoofing.

6.5.2.2 Network Layer and Transport Layer Security

It is recommended to control which IP traffic can be sent and received within the secured connection. This is done for strict separation of the inner networks of PMN operators. If applied, a PMN cannot act as forwarder of IP traffic between PMNs and the PMN protects itself from unwanted traffic. Some network elements (at IP or Diameter level) on the network edge should apply the following IP filters.

There are different filters for the bilateral mode (see Figures 24), and for the transit mode (see Figures 25). For bilateral mode allowed IP addresses of the peer should be taken from the IR.21 RAEX DB. For transit mode peer IP addresses should be provided by the IPX provider.

[SP] IP filters for bilateral mode:

- Incoming IP packets should originate from the range of IP addresses which belong to the peer PMN at which the secure Diameter hop terminates.

- The destination IP address of incoming IP packets should belong to the range of IP addresses of the PMN which receives the packet.
- Outgoing IP packets should originate from the range of IP addresses of the PMN which sends the packet.
- The destination IP address of outgoing IP packets should belong to the range of IP addresses which belong to the peer PMN at which the secure Diameter hop terminates.
- *[SP]* IP filters for transit mode:
- Incoming IP packets should originate from one of the IP addresses of the Diameter Agents of the IPX Hub at which the secure Diameter hop terminates.
- The destination IP address of incoming IP packets should belong to the range of IP addresses of the PMN which receives the packet.
- Outgoing IP packets should originate from the range of IP addresses of the PMN which sends the packet.
- The destination IP address of outgoing IP packets should be one of the IP addresses of the Diameter Agents of the IPX Hub at which the secure Diameter hop terminates.

For further restriction, instead of allowing the entire range of IP addresses of a peer PMN or IPX Hub, dedicated IP addresses of DEA can be used.

[ISH] IPX Hubs should also implement these filters. However, since IPX Hubs communicate with Service Providers and with other IPX Hubs the filters differ in the sense that peer networks are not only PMN, but also a set of PMNs which are managed by the peer IPX Hub.

In the case where a PMN decides to outsource the DEA to their IPX-Provider (see Figure B-6, the IP filters should be applied anyway. The Border Gateway or the Edge Router can do this.

On transport layer packets should be restricted to the Diameter protocol only (i.e. the SCTP payload protocol ID (RFC 4960 sect 14.4) should be set to ‘DIAMETER’).

6.5.2.3 Diameter Base Protocol Security

Sanity checks on the application layer are required to only process allowable messages.

GSMA PRD FS.19 [60] has defined 4 categories related to Diameter security:

1. Low-Layer Format Filtering on IP, Host, Realms
2. Cat 1: Diameter Filtering on Application ID, Command Code
3. Cat 2: Filtering on AVPs Level (except origin related AVPs)
4. Cat 3: Category 3 Filtering on Diameter Message and Location

For the transit mode, the IPX providers shall screen the following AVP:

1. Realm of the sender SP (Low-Layer Format) : the first Diameter Agent which has direct connection with the sender SP is required to check that the realm contained in the Origin-Realm AVP in the request from the sender SP corresponds to the right sender network (as specified on reference 3GPP TS 29.272 [5] section 7.1.2 and GSMA IR.77 [9] as a binding requirement for IPX providers).

2. Message type of the sender SP (Cat 1): the first Diameter Agent which has direct connection with the sender SP is required to check that the Application-Id AVP in the request from the sender SP corresponds to the offer provided to the sender network by the IPX provider (GSMA IR.77 [9] as a binding requirement for IPX providers).

To cover all end-to-end Roaming applications (S6a, S6d, S9, Gy…) and based on the assumptions that DIAMETER Agent (DEA/IPX DA) should be used as Relay Agent, the checks are focusing on AVPs of the Base Protocol that are commonly used to route Requests: Origin Realm/Host, Destination Realm/Host, Application Id, Command Code or commonly used to provide routing related information, such as Route Record, Session id, Proxy Info.

The following additional rules should be done:

- *[SP]* Filter Diameter messages to accept only supported Application IDs, Command Codes, AVPs and flags.
- *[SP, ISH]* Compare all AVPs that identify the origin and the destination (that is Origin/Destination Realm/Host and Visited PMN ID) to determine consistency between them.
- *[SP]* Verify CER/CEA Diameter Messages against Diameter Servers and capabilities declared in IR.21 RAEX DB. Internal nodes should only accept CER messages from nodes that need to send them to them.
- *[SP]* Check if Origin Realm/Host is from a PMN which has a roaming agreement with that PMN. Information related to this PMN is taken from IR.21 RAEX DB during provisioning of the filter configuration in the DEA.
- *[SP, ISH]* Check if the Route Record AVPs (if they exist) are known in the documented route and possible for the source and destination given in the message.
- *[SP]* Egress Diameter messages are received by the DEA from an inner network element. They are only sent to their destination if all the AVPs which determine the origin are addressing a network element within the sending (i.e. one's own) PMN.
- *[SP]* Ingress Diameter messages are received by the DEA from an outer network element. They are only sent to their destination if all the AVPs which determine the destination are addressing a recipient which is inside one's own PMN.
- *[SP]* "Stateful" inspection which only permits ingress messages in a defined order, according to IETF RFC 3588 [3] states (e.g. no answer should be processed if no request has been issued).
- *[SP]* It is also recommended to check that requests are only received from peers for whom the application ID is authorized according to the contracts e.g. for location services etc.
- *[SP]* An AVP which may disclose internal information of a PMN but which is not required outside the PMN should be changed/removed from all egress messages ("topology hiding"). The general rules applied may be:

    a. To hide all Diameter Host Names.
    b. To hide the number of Diameter Nodes in the network by hiding routing and identity details.

- If the above check fails, then it is recommended by GSMA to use common Diameter error for this e.g. 5420, 5012 or 5005.

The DEA should determine messages to apply topology hiding based on:

c) Their connection type and origin.

d) Application Routing Rules-like criteria: Application-ID, Origin-Realm, Origin-Host, Destination-Realm, Destination-Host.

In addition, topology hiding should also prevent other networks from determining the routing used within a network by hiding the path that Diameter messages use when being routed through the network. This is accomplished by:

- Hiding Diameter names in Route-Record AVP and using generic names in their place.
- Reinserting the correct names if the request reenters the home network.
- Hiding Diameter host names in other base Diameter AVPs such as: Session-ID and Proxy-Info.
- To prevent other networks from discovering the number of hosts (e.g. HSS) in the network and their identity, topology hiding should hide:
- Diameter name in Origin-Host AVP in requests from a local host (e.g. HSS) to a foreign host (e.g. MME).
- Diameter name in Origin-Host AVP for answers from a local host (e.g. HSS) to a foreign host (e.g. MME).

In order to ensure that Diameter messages will be routed correctly, the Topology Hiding shall not alter origin-realm AVP as defined in 3.1.3.4 and it is encouraged to follow hostname naming rule as well.

6.5.2.4 Cross-Layer Security

There is a need to validate IP addresses against Diameter AVPs. Validation differs between bilateral mode and transit mode.

During the peering phase (SCTP associations setup and CER/CEA exchange), following rules should be followed to ensure that the peering is done with the right peer.

Bilateral mode:

- *[SP]* Check if the source IP address of ingress IP packets matches the IP address range of the PMN which is identified in the Origin Realm/Host AVP of the Diameter header in the message.
- *[SP]* Vice versa, check if the destination IP address of ingress messages matches the IP address range of the PMN which is identified in the Destination Realm/Host AVP of the Diameter header in the message.
- *[SP]* IP addresses and Diameter AVPs should also be checked against the entries in the IR.21 RAEX DB. If CER validation fails, then the answer message shall be returned with error code DIAMETER_UNKOWN_PEER.

Transit mode:

- *[SP]* At the PMN edge, check if the source IP address of ingress IP packets matches the IP address of the IPX Hub's DEA via which messages from the source PMN are received. The source PMN is identified by Origin Realm/Host in the message.
- *[SP]* Vice versa, at the PMN edge, check if the destination IP address of egress IP packets matches the IP address of the IPX Hub's DEA via which messages are sent to the destination PMN. The destination PMN is identified by Destination Realm/Host in the message.
- *[ISH]* The IPX Hub is required to make sure that it performs the cross layer checks for Diameter traffic that is received from directly connected Diameter peer Service Providers. In particular, it is required to check that the Origin-Realm AVP corresponds to the right network (cf. 3GPP TS 29.272 [8]). For an IPX Hub, the peer cannot only be a Service Provider. Another IPX Hub can be the peer as well. For such inter-Hub connections, the above cross layer checks are not strictly needed if all IPX Hubs perform the check on ingress traffic from Service Providers, but could be adapted accordingly.

In addition, for routing DIAMETER transactions (S6a, S6d, S9, Gy…) there are other controls that a DEA shall support in both modes:

- *[SP, ISH]* The DEA shall implement anti-spoofing mechanisms for all Diameter applications. To achieve such requirement, DEA shall implement a system of whitelist for each peer it is connecting. This list will contain the list of realms that the peer is authoritative on. If a message on any application is received with an origin-realm that is not part of this list, the request shall be rejected with a configurable error.
- [SP] The DEA shall not forward traffic from one outer network interface to another. It only forwards traffic from an inner to an outer interface or the other way round.

6.5.2.5 Diameter Application Security Depending on the Diameter Application (e.g. S6a, S9, Gy, ...)

Service Providers should implement additional application-specific security checks in Diameter end points. For S6a, for example, an additional check would be to compare contents of the S6a Visited-PLMN-ID AVP with the Base Protocol's Origin-Realm AVP, which in turn has been verified by the lower layer checks mentioned above.

6.5.2.6 Discovery of Peer PLMN Network Elements

According to Section 3.1.3.4 there are two possible mechanisms to discover the "next hop":

- Manually configured static entries in the Peer and Routing Tables;
- Dynamic Discovery using DNS (S)NAPTR.

From a security perspective it is recommended to use static entries. The use of dynamic discovery of DEA peers raises several security issues mainly if a GRX/IPX DNS is used. More details are discussed in Appendix C. If dynamic DEA discovery is chosen, the following requirements should be met by the DEA:

- [SP] The peer and routing table entries created via DNS should expire (or be refreshed) within the DNS TTL. According to IETF RFC 3588 [3], the routing table entry's expiration should match the peer's expiration value in the peer table.

- [SP] DNS RRs (Resource Record) should be validated via DNSSEC to protect against DNS-vectored attacks.
- [SP] The ACLs defined in Section 6.5.2.3 should be applied in order to verify roaming agreement and authorization for the DEA peer to act in the declared role for the declared capabilities.
- [SP] Security mechanisms should be implemented to protect DEA against DNS reflection/amplification attacks (see Annex C for more details).

6.5.2.7 Responsability Cascade

The investigation of the root causes of fraudulent interconnect traffic is often hindered by the fact that such investigation relies on the good will of each transit carrier to collaborate in order to identify the party who originated the fraudulent traffic. The investigation of fraudulent traffic often results in the party who originated the traffic to receive a warning from their access operator who usually withhold the identity of their customer who originated the fraudulent traffic as they are under no obligation to provide this identity. The lack of identification of the party who originated the fraudulent traffic often prevents identifying the root cause and by consequence allows fraudsters to use the services of operators for sending fraudulent traffic with a complete impunity.

Fraudsters often exploit a vulnerability of the SP/ISH who fails to support the security recommendations provided by this document.

Looking at security recommendation that have been described previously, it appears that ISH are the ones which can ensure such hop-by-hop security.

In case of a fault is discovered, the cascading responsibility should be applied, a SP asking to its ISH for finding the faulty network, the ISH asking to its partner and so on.

ISH should identify the party responsible for sending the fraudulent traffic and the method it has chosen to ensure this traceability. Otherwise, the ISH can be asked for some penalties, for example including not to receive payment for the fraudulent traffic.

6.5.3 Diameter End-to-End Security

6.5.3.1 Introduction

Diameter messages exchanged between service providers within the IPX ecosystem do not have any native integrity or confidentiality protection measures within the protocol. With the use of the Internet Protocol Security (IPsec/Transport Level Security (TLS), hop by hop protection is provided, however it does not provide an end to end security within the IPX ecosystem.

Due to the ‘hop by hop” routing nature of the Diameter protocol and the use of topology hiding within DEAs, a Diameter response always follows the same path as the Diameter request, making the Diameter protocol a “spoofing friendly” protocol for roaming support.

6.5.3.2 Diameter End-to-End Signaling Security (DESS)

GSMA PRD FS.19 provides guidelines on *what* to protect, *where* to protect and *how* to protect the end-to-end exchange of Diameter messages in the IPX ecosystem by adding integrity, authentication and confidentiality measures to the Diameter protocol itself. This is

associated with the protocol agnostic considerations for IPX end-to-end security in GSMA PRD FS.21 and the key management procedures in GSMA PRD FS.34.

Note: The general security guidelines for IPX providers and service providers with regards to Diameter Firewall should still be taken into account.

The operational strategy for the LTE Diameter Security is sketched in the following figure including the scenarios with both the lack of E2E security solution in SS7 and the full E2E security by design solution in 5G with HTTP2/JSON.

Some initial protection of the IPX trusted domain for LTE with Diameter, can be realized with the IPX security network operational and configuration measures by the Diameter Base Protocol Security checks provided in the in previous section:

1. Low-Layer Format filtering on the Origin-Realm AVP
2. Category 1 filtering on the Application-Id AVP.

The guidelines for Diameter End-to-End Security in GSMA PRD FS.19 describe the additional Diameter End-to-end Signalling Security (DESS) measures with the technical procedures in DEA/Firewall network elements for:

- DESS Phase 1 (Signature) – Authentication and Integrity protection
- DESS Phase 2 (Encryption) – Confidentiality protection on top of DESS Phase 1.

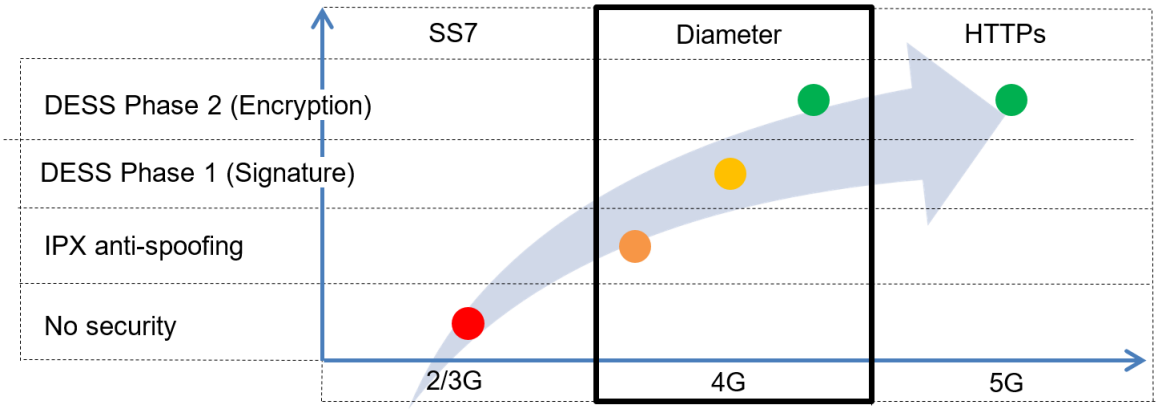

Figure 27 – Operational strategy for Diameter Security

The DESS security measures can be implemented in a stepwise approach because of the different business needs, operational consequences and implementation complexities:

- DESS Phase 1 (Signature) – the procedures for Authentication and Integrity protection are especially driven the by signalling security and provides MNOs insights if the information is modified or not, and if so, by which IPX carrier, so it provides visibility to the recipient MNO to guarantee that the information is not sent or manipulated by malicious sources.
- DESS Phase 2 (Encryption) – the procedures for Confidentiality protection to be provided on top of DESS Phase 1 are primarily driven by data protection reasons, like more strict GDPR requirements and the 5GS needs, and done by encrypting sensitive parts of the contents in the Diameter signalling messages.

Indicating the support of DESS Phase 1 means that Digital Signatures may be added to each Diameter message on the inter-PLMN. Indicating DESS Phase 2 means that, besides the authentication and integrity measures, confidentiality measures are supported. Note that confidentiality protection, due to its session-based nature, needs to be enabled bilaterally on a per inter-PLMN basis. Table 12 describes the protection capabilities per DESS phase:

DESS phase	Authentication and Integrity protection	Confidentiality protection
No support	No	No
DESS Phase 1 (Signature)	Yes	No
DESS Phase 2 (Encryption)	Yes	Yes

Table 12 – DESS support implications

At this point in time GSMA PRD FS.19 and GSMA PRD FS.34 only include the Diameter procedures and Diameter encoding elements for the implementation of DESS Phase 1. The additional procedures and encoding elements for DESS Phase 2 will be added in a future version of GSMA PRD FS.19 and GSMA PRD FS.34.

6.5.3.3 Interfaces to be protected

As in GSMA PRD FS.19, the advised implementation and use of this IPX Network End-to-End Security Solution for Diameter is as follows:

- **Existing S6a, S6d, S9 and S13 interfaces**
  Optional authentication, integrity measures on the existing S6a, S6d, S9 and S13 interfaces by introduction of DESS Phase 1 as summarized in **Error! Reference s ource not found.** above.
- **SMS on SGd/GGd interfaces**
  For the protection against SMS fraud it is advised to have at least the DESS Phase 1 implemented to detect SMS fraud via authentication and integrity protection. Any modified SMS message is potentially fraudulent and may be further analysed and blocked.
- **Future Diameter interfaces**
  It is advised to have the DESS Phase 1 implemented from the beginning to provide authentication and integrity protection on future Diameter interfaces.

6.5.4 Risks from Interworking with Different Technology Generations and Signaling Protocols

The security to end-users highly depends on the concatenation of all the technical elements involved for the communication including the protection capabilities supported by the device, the type of radio technology and the type of signaling.

A well-known attack strategy is downgrading attacks (or bidding down attacks) with the aim that the device connects to an older mobile system with less secure protection capabilities. In particular, these attacks are targeting weaknesses or imperfections in interworking solutions between different signaling protocols.

The specifics of these 5G, LTE (4G), 3G and 2G use cases are outlined in detail GSMA PRD FS.21 [65] for the following roaming scenarios:

a. 5G SA scenario
b. 5G NSA and native LTE scenarios
c. 5GC with EPC interworking scenarios
d. Native 2G and 3G scenarios.

Note: For the LTE (4G) use cases, only the native LTE roaming scenario b and the native 2G and 3G scenarios d apply from the above list.

As an illustration, Figure 28 shows in more detail the mobile native LTE roaming scenario b with end-to-end authentication and integrity protection by means of a Digital Signature with DESS Phase 1 per security perimeter segment. The diagram shows that this protection can only be supported for a 4G UE when the device is controlled with end-to-end DESS Phase 1 enhanced Diameter signaling support between the DEA/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 [60].

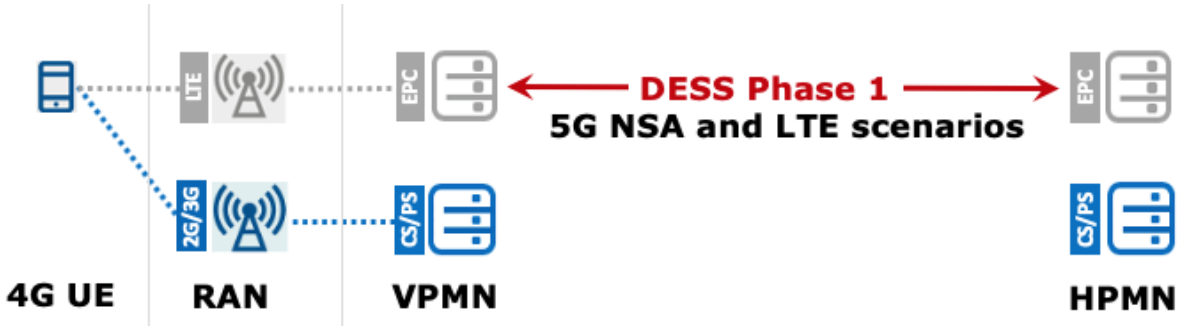

Figure 28 – Authentication and Integrity Protected Roaming Traffic Scenarios

Note: Typically, SS7 is used for the 2G and 3G roaming scenarios. However, for 3G PS, Diameter may also be used via the S6d interface.

The less protected of the roaming scenarios apply when the roaming traffic is exchanged via either the standard Diameter signaling (without the DESS enhancements) or via SS7 signaling. This is illustrated in Figure 29, and applies for the following roaming scenarios with a 4G UE:

- The native LTE roaming scenario with the standard Diameter support between the DEA/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 or by means of the SS7 signaling as specified in GSMA PRD FS.11.
- When the 4G UE is paging in 2G or 3G because then the roaming is being supported via SS7 signalling as specified in GSMA PRD FS.11.

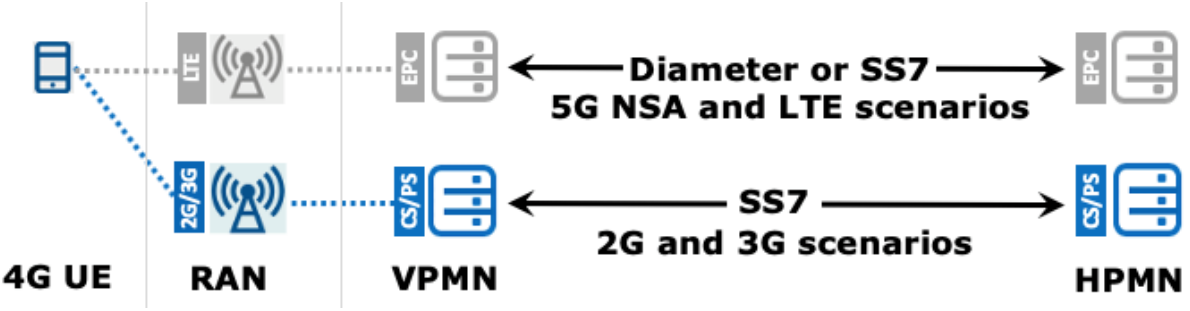

Figure 29 – Least Protected Roaming Traffic Scenarios

Note: Typically, SS7 is used for the 2G and 3G roaming scenarios. However, for 3G PS Diameter may also be used via the S6d interface.

Please be referred to GSMA PRD FS.21 [65] for a complete overview of the other scenarios and the security impact that is exposed via the network signaling by the parallelism of technologies like 2G, 3G, 4G and 5G in combination with the coexistence of SS7, Diameter and HTTP/2 signaling protocol suites.

6.6 Diameter Roaming Hubbing

To support LTE Roaming Hubbing, IR.80 defines three architecture alternatives: Direct connection, Origin/Destination realm based routing and Destination realm modification.

6.6.1 Direct connection

When using Direct connection architecture, the MNOs are directly connected via Diameter signalling with an Open Connectivity Roaming Hub (OCRH). The MNOs and OCRH are routing all Diameter messages based on Destination realm without manipulation. This alternative is depicted in Figure 26.

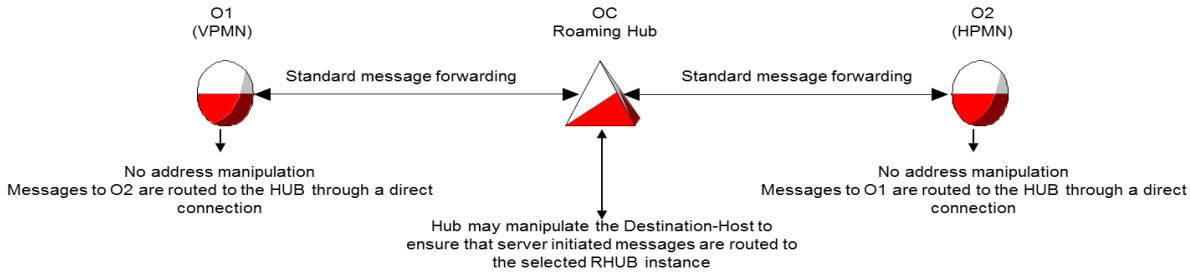

Figure 30: Direct connection

6.6.2 Origin/Destination realm based routing

In Origin/Destination realm based routing alternative the MNOs are connected to the OCRH through an IPX carrier. In order to achieve the Origin/Destination realm based routing, the IPXs must supply the MNOs with advanced Diameter routing capability based on Origin/Destination realm. The rule applied by the IPX provider is, if Origin realm is O1's realm and Destination realm is O2's realm, to route the Diameter message to OC Roaming HUB. This alternative is depicted in Figure 27.

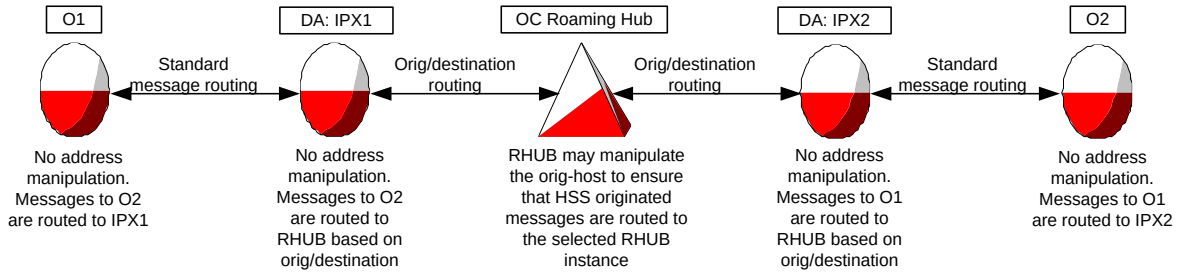

Figure 31: Origin/Destination realm based routing

6.6.3 Destination realm modification

In a Destination realm modification alternative, the MNOs are connected to the OCRH through an IPX carrier. Destination realm is modified by the IPX, appending the suffix ".hub-realm". The OCRH removes the suffix from the Destination realm to get back to the initial Destination realm and performs a standard routing based on the Destination realm.

Therefore, this alternative relies on an agreement between OCRH and O1 and implies that the IPX provider of O1 must support the Destination realm manipulation. This is depicted in Figure 28.

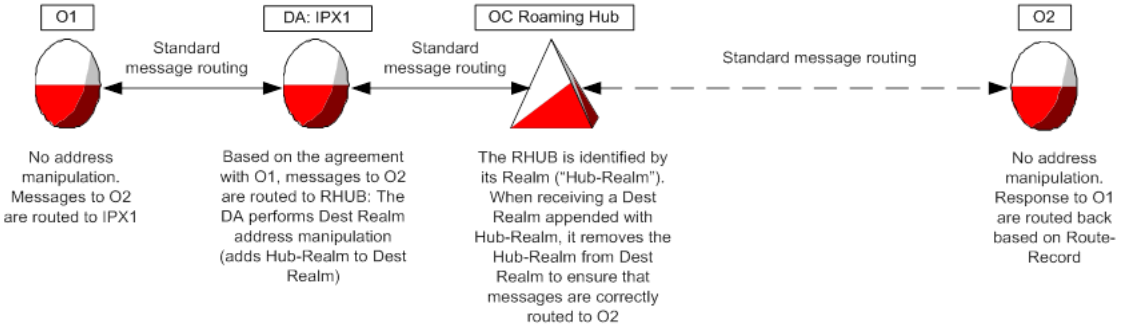

Figure 32: Destination realm modification

6.7 Default APN

The default APN can be set either to the IMS well-known APN or to an APN other than the IMS well-known APN, as described in section **Error! Reference source not found.** The c onsequences of selecting the one or the other APN as default APN are as follows:

If the default APN in the HSS is set to the IMS well-known APN, then

- A PDN connection to the IMS well-known APN is always established during the E-UTRAN initial attach for UE that supports GSMA PRD IR.92 [30], independent of whether the user is subscribed to any IMS service or not.
- A PDN connection to the IMS well-known APN is always established during the E-UTRAN initial attach for UE that does not support GSMA PRD IR.92 [30] and that does not provide an APN.
- The UE (which gets connected to the IMS well-known APN) needs to establish an additional PDN connection to an APN other than the IMS well-known APN in order to use non-IMS services, for example, to access the Internet, and is charged accordingly.

Note: The IMS well-known APN works in this scenario as a zero-charging “dummy” APN for the user that is not subscribed to any IMS service, that is, the UE is connected to the EPC but it is not able to use any data service.

If the default APN in the HSS is set to another APN than the IMS well-known APN, then

- A PDN connection to the IMS well-known APN is never established during the E-UTRAN initial attach for UE that supports GSMA PRD IR.92 [30], independent of whether the user is subscribed to any IMS service or not.
- A PDN connection to such default APN is always established during the E-UTRAN initial attach for a UE that does not provide an APN during initial attach, for example, for a UE that supports IR.92 [30].
- The UE that supports GSMA PRD IR.92 [30] and which gets connected to such default APN needs to establish an additional PDN connection to the IMS well-known APN to use IMS services as specified in GSMA PRD IR.92 [30].
- The UE (which gets connected to such default APN) is able to use the APN other than the IMS well-known APN for its purpose, for example, in case the default APN is configured to be the one used for Internet access, then the UE can access the Internet using the PDN connection that is established during the E-UTRAN initial attach.
- Unwanted data charging may occur on the PDN Connection to the APN other than the IMS well-known APN if the UE is configured to not use data when roaming, unless that APN other than the IMS well-known APN is a zero-charging APN. If default APN is the APN for Home Operator Services, see section 6.3.3.5 “Data off related functionality” of this document.

Irrespective of which APN is configured as default APN, the following should be considered:

- The default APN may be used also on other accesses than E-UTRAN, e.g., on UTRAN connected to S4 SGSN.
- The PDN connection to the default APN may be handed over between 3GPP accesses, e.g., between E-UTRAN and UTRAN, and used on target access.

Independent of being configured as the default APN or not, the IMS well-known APN is zero-charged on packet-level for some or all IMS services in case of local breakout (see PRD IR.65 [31]) and must not be used by any non-IMS application (see PRD IR.92 [30]). However, charging for the amount of data transferred may occur if the PDN connection to the IMS well-known APN is

- Home routed and used for IMS services.
- Used for IMS services that are not zero-charged on packet-level.

6.8 E-UTRA-NR Dual Connectivity with EPC

E-UTRA-NR Dual Connectivity (EN-DC) as specified in section 4.1.2 of 3GPP Release 15 TS 37.340 [63] and in section 4.3.2a of 3GPP Release 15 TS 23.401 [1] involves eNB as Master Node and en-gNB as Secondary Node, to provide radio resources to a given UE with active radio bearers. A single S1-MME termination point per each DC connected UE, exists between EPC (MME) and the master eNB.

The HPMN and the VPMN shall indicate the support of EN-DC using the bit set for “NR as Secondary RAT” in the Feature-List AVP as part of, Update Location Request/Update, Location Answer, Insert Subscriber Data Request and Insert Subscriber Data Answer, as specified in section 7.3.10 of 3GPP Release 15 TS 29.272 [8].

If both the HPMN and the VPMN support EN-DC, and if the MME has an Access Restriction for NR for a UE then the MME signals this Access Restriction to the E-UTRAN as part of Handover Restriction List and to the UE in Attach Accept, as well as in TAU Accept after the inter-RAT handover from GERAN/UTRAN.

Note: MME receives Access Restriction for a UE either in signalling from HSS, as specified in section 7.3.31 of 3GPP Release 15 TS 29.272 [8], or locally generated by VPMN roaming policy in the MME.

If the VPMN receives an Update Location Response or Insert Subscriber Data Request without the bit set for “NR as Secondary RAT” in the Feature-List AVP from the HPMN, the VPMN may restrict the access for NR as secondary RAT, based on local policy

6.8.1 GW Selection for E-UTRA-NR Dual Connectivity

For UEs supporting EN-DC and if the MME has no Access Restriction for NR (see NOTE in section 6.8), the MME may select SGWs and PGWs, supporting Dual Connectivity, as specified in section 5.12.2.1 of 3GPP Release 15 TS 29.303 [17].

If no candidate SGW and PGW is found, the MME must perform the gateway selection procedure without the Service Parameter “+nc-nr” appended to the ‘app-protocol name’, as specified in section 5.12.1.3 of 3GPP Release 15 TS 29.303 [17].

6.9 TAC/LAC Restriction Guidelines

TAC/LAC restrictions ensure roaming customers to only roam in the agreed areas of a Network. These restrictions can be used to prevent unexpected roaming charges within their provider’s service area or along border areas. The guidelines for implementing TAC/LAC restrictions in a roaming scenario are documented in GSMA WA.11

6.10 APN for UAS based services

6.10.1 Introduction

The UAS well-known Access Point Name (APN) is defined below. For more details on when this APN is used, see GSMA PRD NG.128 [70]

6.10.2 UAS well-known APN

6.10.3 Definition

The Network Identifier (NI) part of the APN must be set to “UAS”. The APN Operator Identifier (OI) part of the full APN must be blank as it is automatically derived and appended

to the NI part by the VPMN and its value depends on the PMN whose PGW the UE is anchored to i.e. VPMN when roaming and HPMN when not roaming.

6.10.4 Gateway Selection

The UAS well-known APN is anchored on a PGW in the HPMN when S8HR roaming. Therefore, when enabling UAS Critical and non-Critical communications for a subscriber, the following subscription settings must be taken into account for the UAS well-known APN:

- 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, if set, is set on a per VPMN basis.

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 UAS 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 UAS services are revoked for a subscriber whose Default APN is the UAS well-known APN, then the Default APN needs to be set to a different APN or else, the subscription is 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 UAS 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 does 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 UAS well-known APN as the Default APN.

The gateway selection logic in all MME and SGSN must select a PGW in the same PMN for the UAS well-known APN for a particular subscriber, i.e., all must select a PGW in the HPMN.

Note: If not all SGSN and MME would select a PGW in the same PMN, then there are scenarios in which a PGW is selected for the UAS APN in the HPMN and the UE moves into an area where the PGW needs to be in the VPMN.

7 Technical Requirements for QoS support

This section illustrates the required functionality that are needed in the VPMN and the HPMN in order to support QoS procedures for LTE and EPC roaming.

Support of QoS procedures whilst roaming has several aspects:

1. Ensuring that an outbound roamer will be given the expected level of QoS for the service they are using, within the limits of the roaming agreement.
2. Ensuring that the QoS parameters of an inbound roamer are within the limits of the roaming agreement.
3. Enforcement of the actual QoS by the VPMN.

7.1 QoS Parameters definition

According to Release 11 of 3GPP TS 23.401 [x] and TS 23.060 [y], several QoS parameters are assigned to EPS bearers (and used on both radio and core parts) depending on the type of bearer:

- For all bearers:

    a) QCI (QoS Class Identifier): it is an index to sets of node-specific settings that control bearer level packet forwarding treatment. A one-to-one mapping of standardized QCI values to standardized QoS characteristics is given in the tables below.

    b) ARP (Allocation Retention Priority): this is a set of 3 parameters used to decide whether a bearer establishment / modification request can be accepted or needs to be rejected due to resource limitations; it is composed of:

    i. ARP Priority Level (PL): relative priority of the resource request (range from 1 to 15 with 1 being the highest priority); and
    ii. ARP pre-emption Capability (PCI): ability of a bearer with higher ARP PL to pre-empt resources of another bearer having pre-emptable resources; and
    iii. ARP Pre-emption Vulnerability (PVI): possibility of bearer resource pre-emption by another bearer having higher ARP PL and ARP PCI.

Table 13 For non-Guaranteed Bit Rate (non GBR) bearers:

    a) UE-Aggregate Maximum Bit Rate (UE-AMBR): maximum bit rate allowed across all non GBR bearers; and

    b) APN-Aggregate Maximum Bit Rate (APN-AMBR): maximum bit rate allowed across all non GBR bearers for a given APN.

Table 14 For Guaranteed Bit Rate (GBR) bearers:

    a) Maximum Bit Rate (MBR): maximum bit rate allowed on the given GBR bearer; and

    b) Guaranteed Bit Rate (GBR): maximum bit rate up to which others parameters (delay, loss rate) are guaranteed on the given GBR bearer

Note: Above descriptions refer only to EPS parameters; Mapping between EPS and corresponding Release 99 QoS parameters can be found TS 23.401 [x] Annex E.

The following table is a subset of standardised QCI matrix provided in Release 15 of 3GPP TS 23.203 [34], table 6.1.7 and related to current well defined Roaming services:

QCI	Resource Type	Priority Level	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100 ms	10^{-2}	Conversational Voice
2		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3		3	50 ms	10^{-3}	Real Time Gaming
4		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
65		0.7	75 ms	10^{-2}	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66		2	100 ms	10^{-2}	Non-Mission-Critical user plane Push To Talk voice
67		1.5	100 ms	10^{-3}	Mission Critical Video user plane
75		2.5	50 ms	10^{-2}	V2X messages
5	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		9			
69		0.5	60 ms	10^{-6}	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling, MC Video signalling)
70		5.5	200 ms	10^{-6}	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)
79		6.5	50 ms	10^{-2}	V2X messages
80		6.8	10 ms	10^{-6}	Low latency eMBB applications (TCP/UDP-based); Augmented Reality

Table 15: Standardized QCI characteristics

7.2 QoS management in the Home Routed architecture

In theory, any QoS settings requested by the HPMN should be in accordance with the Roaming Agreement.

However, in order to protect its network against unwanted resources use, VPMN, through its MME/S4-SGSN, shall control the QoS.

7.2.1 Procedures involving QoS management

QoS management is required at UE, or PCRF/PGW initiated procedures that result in bearer establishment/modification/deletion or at HSS initiated procedure that results in bearer modification. QoS management is also required at any mobility procedures (including IRAT handover).

In a minimum configuration for early Roaming deployments, MME/S4-SGSN will possibly apply a reduction on the QoS profile it receives from HSS to comply with the Roaming Agreement. This validated QoS profile will be used by MME/S4-SGSN during an Initial Attach procedure to establish the default bearer, during a Tracking Area Update procedure or during HSS initiated subscribed QoS modification procedure.

It is then up to the HPMN to implement a PCC infrastructure which is mandatory if it provides services requiring dynamic QoS control. For instance, RTP based video streaming services require guaranteed bit rates and hence require the setup of a Guaranteed Bit Rate (GBR) bearer from the PGW that could be requested by the hPCRF. "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 PCC infrastructure remains inside the HPMN. See the architecture diagram below. The same PCC architecture is also used when the SGSN is directly connected to PGW (Gn/Gp SGSN architecture).

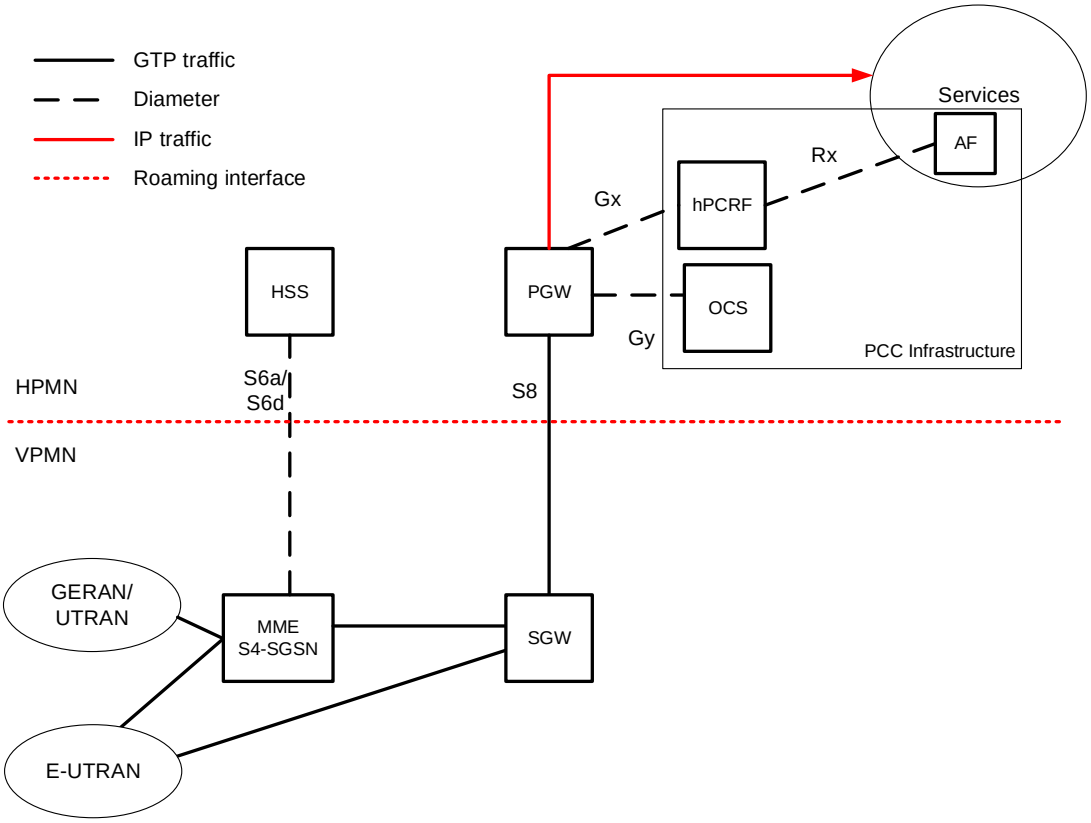

Figure 33: PCC Architecture with Home Routed architecture

This dynamic policy control is possible even if the VPMN has not implemented a PCC infrastructure for its own purpose.

However, there are requirements that must be fulfilled:

1. The VPMN must support the relevant bearer management procedures.
2. The VPMN and the HPMN must be able to ensure that QoS parameters of roamers are within the limits of the roaming agreement.
3. The VPMN must enforce the actual QoS.

Note: In order to smooth early roaming deployments, HPMN may avoid using dynamic procedures that may lead VPMN to reject them if QoS parameters values are not within the limits of the roaming agreement.

If QoS differentiation requires only the use of the default bearer (and no dedicated bearer), the PGW may modify this default bearer QoS parameters within the limits of the roaming agreement.

If services which require dynamic QoS and/or charging are deployed and the default bearer QoS is not sufficient, it is required that the VPMN supports the following bearer management procedures in EPC and in the RAN:

1. Dedicated bearer activation - this procedure is invoked by the PGW if for example the already established bearers' QoS cannot support the new requested service.
2. PGW initiated bearer modification – the PGW can initiate a bearer modification procedure based on HPMN decision or in response to AF initiated bearer modification.

7.2.2 Requirements for the VPMN

Control of QoS parameters within the VPMN MME/S4-SGSN can be split into different phases:

- QoS profile definition within the Roaming Agreement;
- MME/S4-SGSN checks customer QoS profile received from HSS over S6a/S6d interface against Roaming Agreement; and
- MME/S4-SGSN checks any QoS parameters sent by the HPMN PDN-GW on S8 interface
- During the default bearer creation (create_session_request/response)
- During any QoS dynamic procedure

With regards of section 7.1, a roaming QoS profile in MME/S4-SGSN is defined by:

- A list of allowed QCI (GBR and non-GBR) or allowed R99 QoS parameters equivalent to the QCI;
- A remapping Matrix for non-GBR QCIs (including QCI 5);
- Maximum values for ARP PL/PCI/PVI settings (Warning on the notion of maximum value for PCI/PVI); and
- Maximum values for UE- and APN-AMBR, MBR and GBR values (UL and DL).

If a QoS profile is not explicitly described during the roaming agreement definition, then the default profile, as described in "LTE Roaming Information" of VPMN IR.21 shall be implicitly considered.

Mobile Operators, have implemented in their networks many different QoS parameters for IMS services (QCI, ARP-PL, PVI, PCI, MBR etc.) that could vary from operator to operator.

There are several challenges to support this diversity in a roaming environment including:

1. Inconsistent roaming experiences from one partner network to another, including conflicting priorities during congestion. For example, an incoming roamer unlikely will get better treatment than the home subscribers for the same service
2. Complex roaming controls for inbound and outbound QoS management requiring manual efforts on a per-partner basis.
3. Complete failure to establish commercial roaming when the roaming partner does not accept the requested QoS profile.

To overcome these challenges, a minimum set of inbound roaming QoS parameters that all operators are strongly recommended to support to allow for a consistent and predictable S8HR roaming experience are proposed in Annex E. This will facilitate the VoLTE roaming

implementation and is one of the known blockers. It is understood that bilateral roaming agreements always take precedence if the operators choose to negotiate different QoS parameters, which may exceed the minimum settings. For example, operators requiring QCI=2 for video can negotiate through their bilateral roaming agreements. However, using other values for QoS parameters than recommended in Annex E creates a major risk of not being able to establish service in a roaming scenario, e.g. if using lower or higher values for MBR and GBR for IMS voice can result in not being able to establish an IMS voice call. In practice, very few operators support ViLTE in a roaming scenario, so utilizing a non-GBR does not harm the delivery of the service.

In order to ensure that a PDN connection can be established successfully without violating the above QoS profile for inbound roamers from a given HPMN, the following functionalities are required for the VPMN:

- When an inbound roaming UE performs an Attach, the MME of the VPMN shall, upon having received the inbound roamer's subscription from the HSS, compare the QCI and the APN-AMBR values as contained in the subscription for the chosen APN with the pre-configured range of supported QCIs and ARPs and the maximum value of APN-AMBR values for the HPMN. When an inbound roaming UE activates a PDP Context towards the S4-SGSN, the S4-SGSN of the VPMN compares the inbound roamer's subscribed EPS or R99 QoS parameters (see also section 7.1) from HSS or HLR with the preconfigured values. These ranges are configured based on the roaming agreement with the respective HPMN. If the QCI and APN-AMBR values are in line with the roaming agreement, then the MME/S4-SGSN shall accept these values.
- If the MME/S4-SGSN detects that the APN-AMBR value from the HSS in the HPMN violate the roaming agreement, the MME/S4-SGSN may downgrade the bandwidth and/or the ARP PL/PCI/PVI values to the configured limit based on the roaming agreement. If the HSS provided QCI violates the roaming agreement, it is recommended that the MME/S4-SGSN remaps this value into one of VPMN enforced QCI of the Roaming agreement.
- As the settings of ARP PL/PCI/PVI are exclusively related to the VPMN service prioritization strategy, the MME/S4-SGSN shall either apply the values received from the HSS or apply values as per roaming agreement or local configuration.

The same requirements apply when a roaming UE requests another PDN connection using the UE requested additional PDN connectivity procedure or when the HPMN updates the subscription of the outbound roamer using the HSS Initiated Subscribed QoS Modification procedure.

The VPMN shall also control QoS resulting from PCC procedures, involving Management through Default bearers, or enhanced Dynamic Management through Dedicated Bearers.

During session creation, dedicated bearer activation, or bearer modification, the VPMN's MME/S4-SGSN receives QoS parameters from the HPMN. The VPMN's MME/S4-SGSN shall compare the QCI, APN-AMBR, GBR and MBR values contained in the request with the

pre-configured range of supported QCI or its corresponding R99 QoS parameters, ARP, APN-AMBR, GBR and MBR values for the HPMN.

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

If the QCI, APN-AMBR, GBR and MBR values from the HPMN are within the pre-configured range, the MME/S4-SGSN shall accept the procedure. If the MME/S4-SGSN detects that APN-AMBR or MBR values are outside the range, the MME/S4-SGSN may downgrade APN-AMBR, MBR values to the values based on roaming agreement or reject the procedure. For QCI and GBR values, if the MME/S4-SGSN detects that a value is outside those ranges, the MME/S4-SGSN shall reject the procedure.

As the settings of ARP PL/PCI/PVI are exclusively related to the VPMN service prioritization strategy, the MME/S4-SGSN shall either apply the values received from the HSS or apply values as per roaming agreement or local configuration.

If there is a need to avoid downgrade of APN-AMBR and/or MBR values, the HPMN must ensure that QoS parameters from HPMN are within the limits of the roaming agreement, see also section 7.2.3.

When a roaming UE requests additional resources or requests modification of resources using the UE requested bearer resource modification procedure and the VPMN supports UE requested bearer resource modification requests, then this triggers a dedicated bearer activation, deletion or modification procedure initiated by the HPMN. In this case, the MME/S4-SGSN shall behave accordingly as described in the previous paragraph.

7.2.3 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 PDN-GW, which are in turn sent to the VPMN as part of all bearer management procedures.

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.

According to 3GPP TS 23.203 [34], and unless specified within the Roaming agreement for specific services, HPMN should not send ARP PL values between 1 and 8 for outbound roamers.

ARP PL 15 has not the same meaning for both RAN and CORE interfaces. ARP PL 15 means no priority in RAN (section 9.2.1.60 of 3GPP TS 36.413 [45]) and ARP PL 15 means the lowest priority in CORE (section 5.3.45 of 3GPP TS 29.212 [x]).

To avoid inconsistent handling of ARP PL 15 between HPMN and VPMN and to ensure smooth inter-operability for EPS roaming deployments, HPMN may choose not to send ARP PL 15 value for outbound roamers except if required by the roaming agreement.

In order to smooth early deployments, that is to ensure that a PDN connection can be established successfully the HPMN may choose to accept all QoS values (QCI, ARP, APN-AMBR) as received from the VPMN during all the procedures.

Note: Accepting all QoS values from VPLMN avoids explicit knowledge of roaming agreement values in HPLMN PCRF.

7.2.4 QoS control for IMS APN in the S8HR architecture

For the IMS “well known” APN using S8 Home Routed for IMS Voice Roaming, dedicated bearers are established to carry voice/video media. In order to minimize effect when these bearers are used for non-voice/video media services, the GBR value of these bearers (GBR bearer for voice, and optionally a second GBR bearer for video media) shall be controlled by VPMN, based on roaming agreement, to protect the network e.g. to avoid capacity overuse. The GBR values should be in accordance with 3GPP TS 26.114 [56] depending on the codec use by the HPMN.

For connections for an IMS “well known” APN using S8 Home Routed, the services and corresponding QCIs must be supported by the HPMN, as described in section 5.2.2.

Note: If either HPMN, VPMN, or both do not deploy necessary QoS related functions (i.e. QCI, ARP, APN-AMBR, GBR parameters, packet filters, and downgrading function) to support required QoS as agreed commercially between the HPMN and VPMN, there is a possibility that unnecessarily high QoS and/or wrong TFT are applied for applications on established bearers, and this might cause negative impacts on resource usage in VPMN.If VPMN is not able to control QoS settings and hence these are applied on all home routed APNs, the QoS settings associated with the IMS well known APN (QCI, ARP…) may be used also for other APNs than the IMS well known APN and get priority on all other customers, including domestic ones.

QCI characteristics are depicted in table x.

7.2.5 Support of QoS by the IPX/GRX

When one or more IPX/GRX providers are used in the path between the VPMN and the HPMN;

- The sending service provider is expected to map the QCI value to DSCP (differentiate service code point) on the corresponding GTP datagrams as per table 5 in section 6 of IR.34.

1. Example: a GTP datagram carrying QCI 1 voice should be tagged with the corresponding DSCP value “EF”.

- The IPX/GRX providers are expected to honour the requested QoS as per section 6 of IR.34 and transparently transfer the DSCP value to the next hop.

7.2.6 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 (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 for the QCIs covered by the roaming agreement.
- To apply the right Diffserv Code Points (DSCP) on all inter-PMN GTP-U flows of a given bearer depending on its QCI and as specified in IR.34 [11] section 6.2.6.
- To support GBR bearers and provide the requested guaranteed bit rates within the limits as agreed as part of the roaming agreement.
- For connections to an IMS “well known” APN using S8 Home Routed, the services and corresponding QCIs must be supported by the VPMN, as describe in section 5.2.2.

7.3 QoS control in the Local Break Out architecture

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

In this scenario and according to 3GPP, the PCC 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 vPCRF and a Policy and Charging Enforcement Function (PCEF). Both networks must have implemented a PCC infrastructure.

However, for IMS Voice, S9 interface is not required. The PCRF in the visited network is configured with static or standardized policy rules for roaming subscribers. The Gy interface (for online control of data usage) is optional. IMS Voice online charging is performed in the HPMN 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 hPCRF in the HPMN or to ask for its procedure approval as it has already been approved by the IMS in the HPMN.

See architecture diagram below. The same PCC architecture is used also for the case an SGSN is connected to PGW.

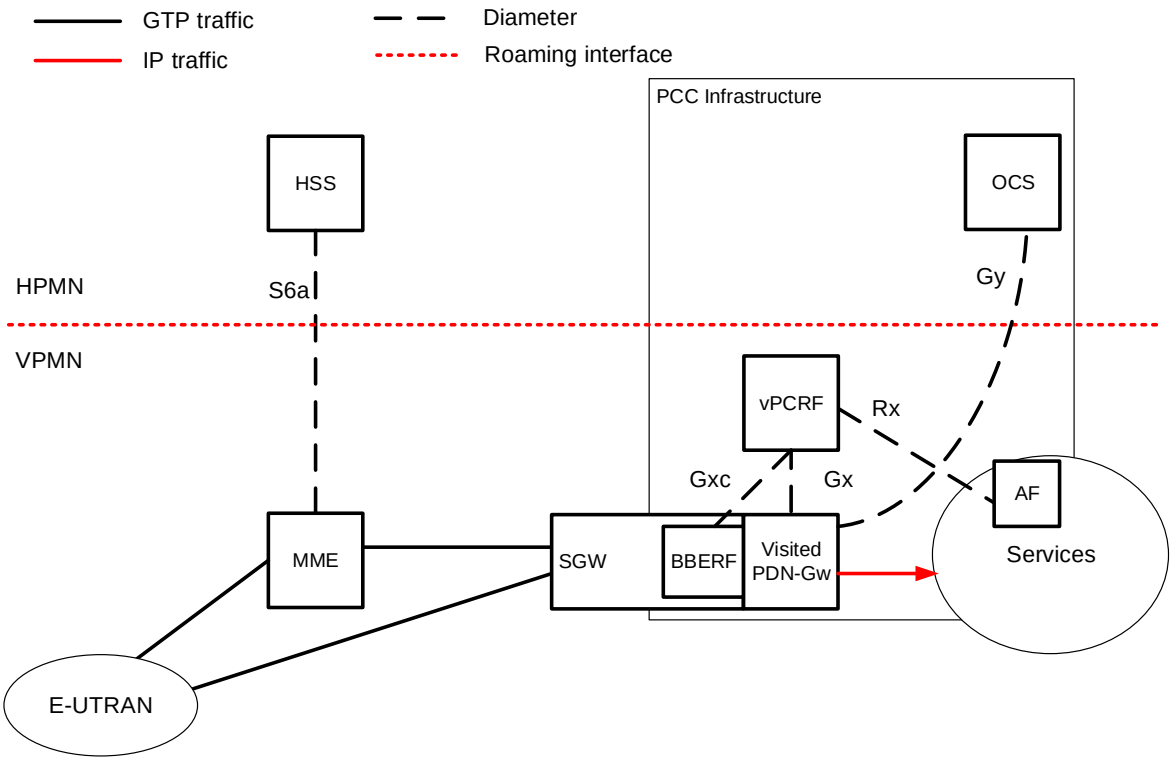

Figure 34: PCC Architecture with Local Break Out architecture

The VPMN must support the bearer management procedures in EPC and in E-UTRAN listed in Section 7.1.1.

It is also required that the VPMN follows the recommendations for QoS engineering in its network listed in Section 7.1.3.

Annex A Testing Framework

IREG test cases for LTE and EPC data roaming, CS Fallback and SMS over SGs are described in IR.23 [35] and IR.38 [54].

Annex B Diameter Architecture Implementation

Figure 31 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 (as defined in TS 29.213 [49]) for S9 and Rx applications.

The PMN has a bilateral interconnection with other PMNs.

Extended NAPTR [26] or static entries can be used at the DEA to find the inner application specific proxy.

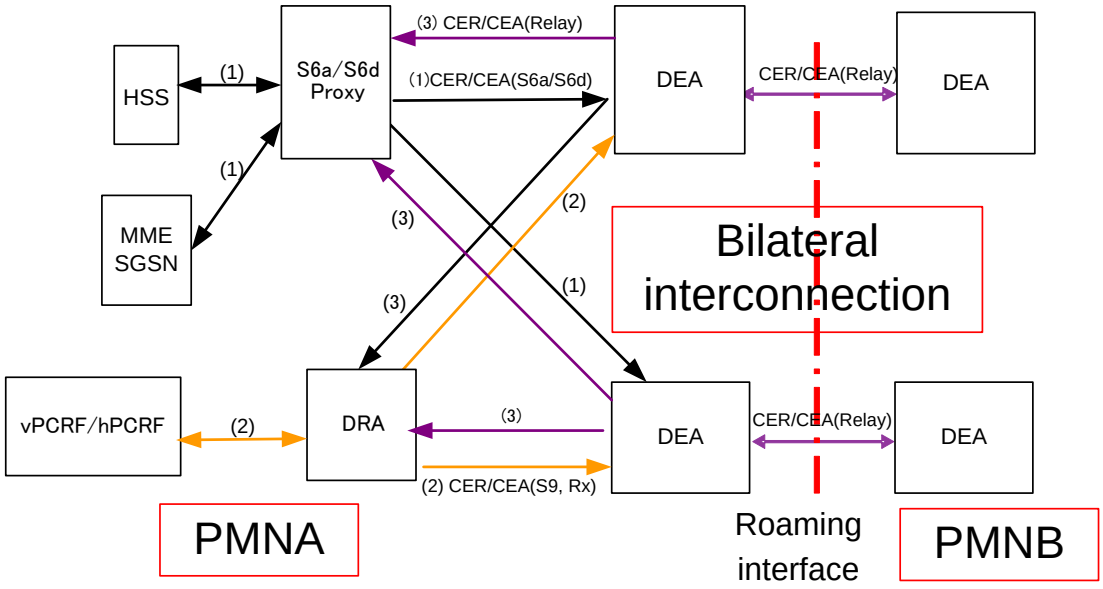

Figure 35: Diameter architecture example 1

Figure 32 illustrates the case where the PMN has implemented DEA that proxy all applications and no inner domain proxy.

The PMN has a bilateral interconnection with other PMNs.

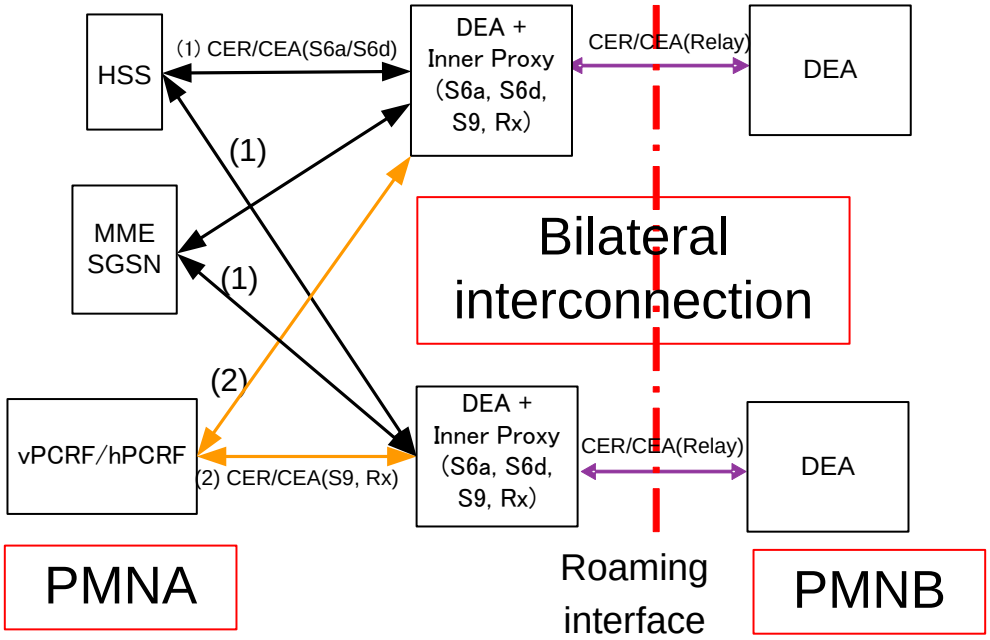

Figure 36: Diameter architecture example 2

Figure 33 illustrates the case where the PMN has DEAs that are application specific proxies and no inner domain one. The DEA relays the Application messages that it is not able to proxy to the other DEA(s).

The PMN has a bilateral interconnection with other PMNs.

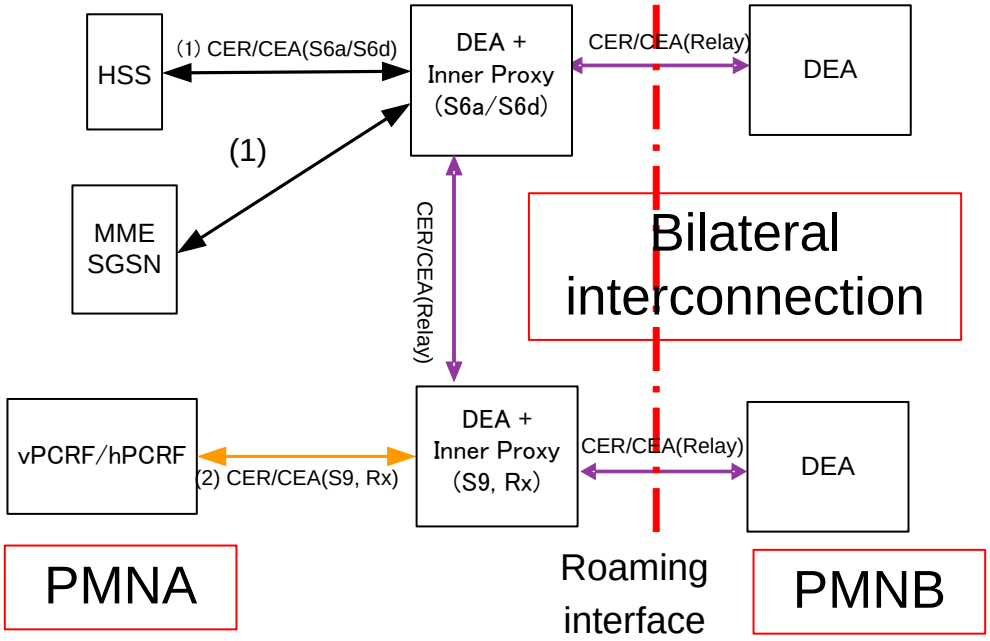

Figure 37: Diameter architecture example 3

Figure 34 illustrates another Diameter architecture implementation which is a variant of examples 1, 2 and 3 where the PMN has:

- DEAs that are S6a/S6d proxies and relays for other applications (S9 and Rx in the current example),
- A Diameter Routing Agent (as defined in TS 29.213 [49]) to manage S9 and Rx applications in the inner domain

The PMN has a bilateral interconnection with other PMNs.

The Extended NAPTR [26] or static entries can be used at the DEA to find the inner application specific proxy.

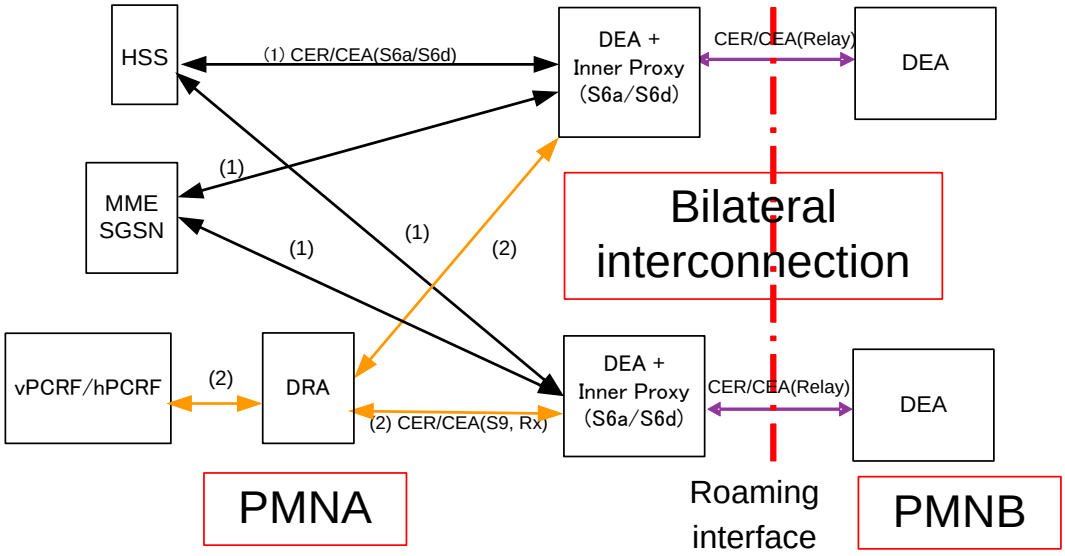

Figure 38: Diameter architecture example 4

Figure 35 illustrates the case where the PMN has implemented DEAs 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 either transit mode through IPX providers or in multi-lateral service hub, as defined in AA.51 [50].

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

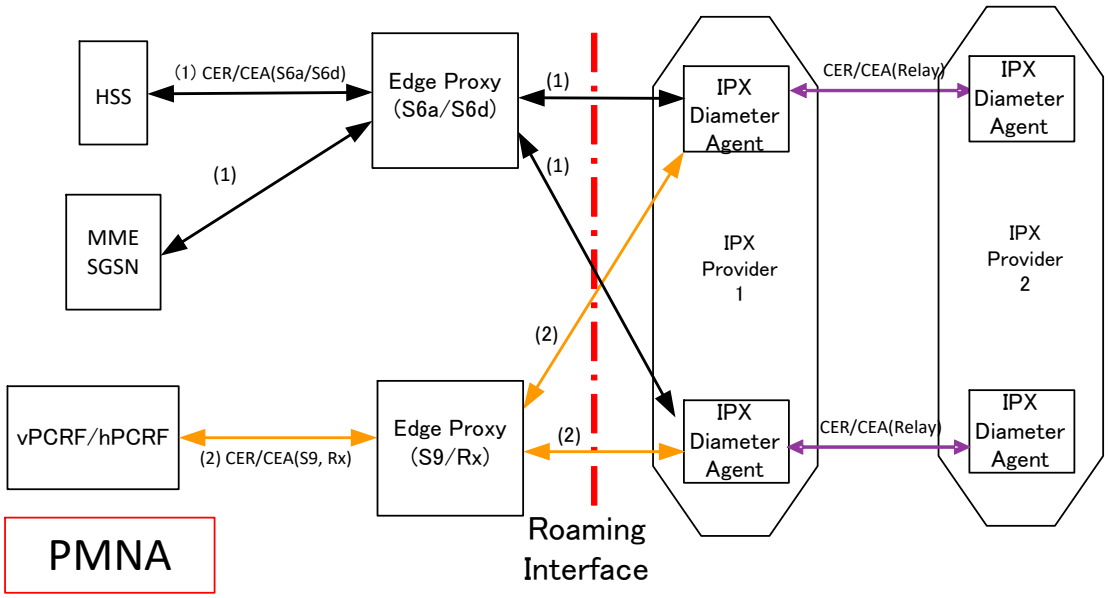

Figure 39: Diameter architecture example 5

Figure 36 illustrates the case where the PMN has outsourced DEAs to its IPX providers through the IPX Diameter Agent.

The interconnection with other PMNs is done in transit mode through IPX providers or in multi-lateral service hub, as defined in AA.51 [50].

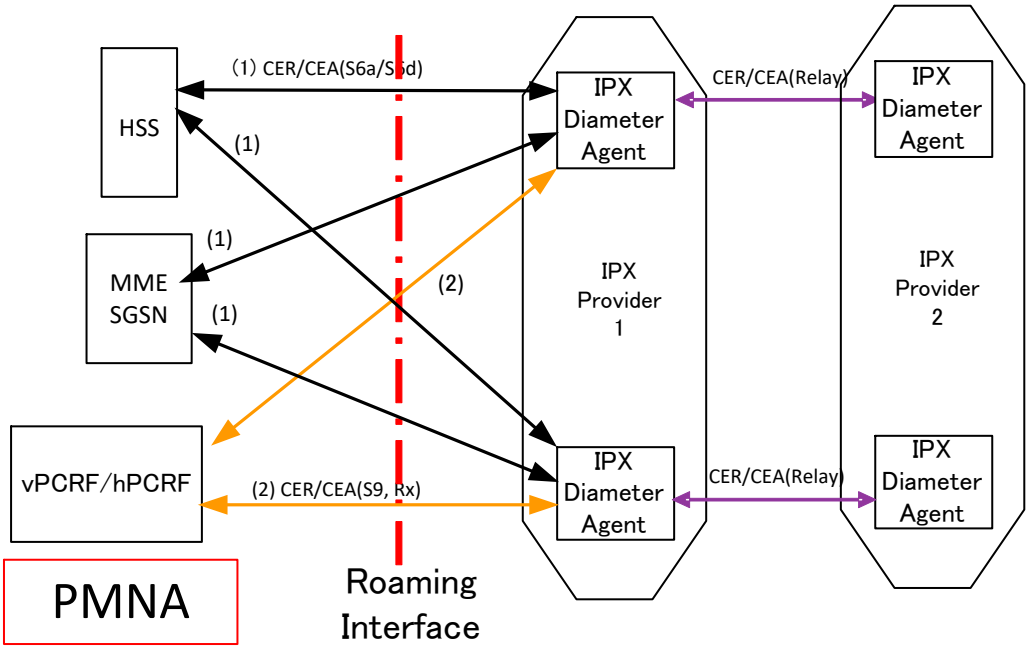

Figure 40: Diameter architecture example 6

Annex C Background on Security Requirements

This annex provides some background information and justification for the security requirements of Section 6.5.

C.1 The need for Diameter Security

Diameter IETF RFC 3588 [3] requires a TLS or IPSec tunnel at the network/transport layer starting from a Diameter agent and terminating at the Diameter peer in order to ensure authentication, data integrity and confidentiality (referred to as "*peer-to-peer*" security). In an "Internet Scenario" this setting is possible. However, in international roaming, secure tunnels are handled by SEGs and not by Diameter Agents. As a consequence, there is no "peer-to-peer" security.

When a TLS or IPSec tunnel is setup each agent has authenticated itself towards the peer while data integrity and confidentiality is guaranteed over the entire network. In international roaming these assumptions are not true:

- Authentication is performed by SEGs and not by Diameter Agents. Consequently, a Diameter Agent establishes a "trusted" relationship with a peer during exchange capabilities process involving CER/CEA messages but it has no way to authenticate it. This point becomes even more crucial when dynamic peer discovery is used.
- Diameter packets are not natively protected by encryption and integrity checks. This is acceptable for PMN-inner traffic because this network is trusted, Traffic to/from outer networks requires protection, in contrast.

As a consequence, a PMN is exposed to several fraud/attack vulnerabilities if the countermeasures described in section 6.5.2 are not applied.

C.2 DNS Security

The use of dynamic discovery for DEA peers raises several security issues related to DNS vulnerabilities/attacks mainly when a GRX/IPX DNS, outer to a PMN, is used. The approach is only as good as the security of the DNS queries along the way. At least two critical attacks to DNS infrastructure can be cited:

- An amplification and/or reflection attack can overload (DoS) a victim DEA with a huge number of unsolicited DNS answers.
- DNS Poisoning attack corrupts the association name/IP (i.e. Kaminsky attack). Once corrupted, the entry persists for a long time (TTL value). The result is that the DEA's routing table is improperly altered.

So, from a security perspective it is recommended to use static entries; to simplify network configuration management within a PMN, a centralized Diameter Redirect Agent (DRD, IETF RFC 3588 [3]) can be used. In this case, peer and routing table entries can be configured just once.

Annex D IPsec to protect IP transport

IPSec can be used on interfaces that use the Diameter protocol to protect its transport if no other appropriate security mean is in place. The use of IPSec between service providers or between service providers and IPX service hubs is based on bilateral agreement between those parties. This applies to both GRX and IPX.

LTE roaming adds Diameter as a new signalling protocol to the inter-operator interface. 3GPP TS 29.272 [8] specifies in section 7.1.2 that Diameter messages are secured by 3GPP TS 33.210 [37] Network Domain Security for IP (NDS/IP). NDS/IP specifies the use of IPsec Security Gateways (SEG) for interconnecting different Security Domains (for example operators A and B):

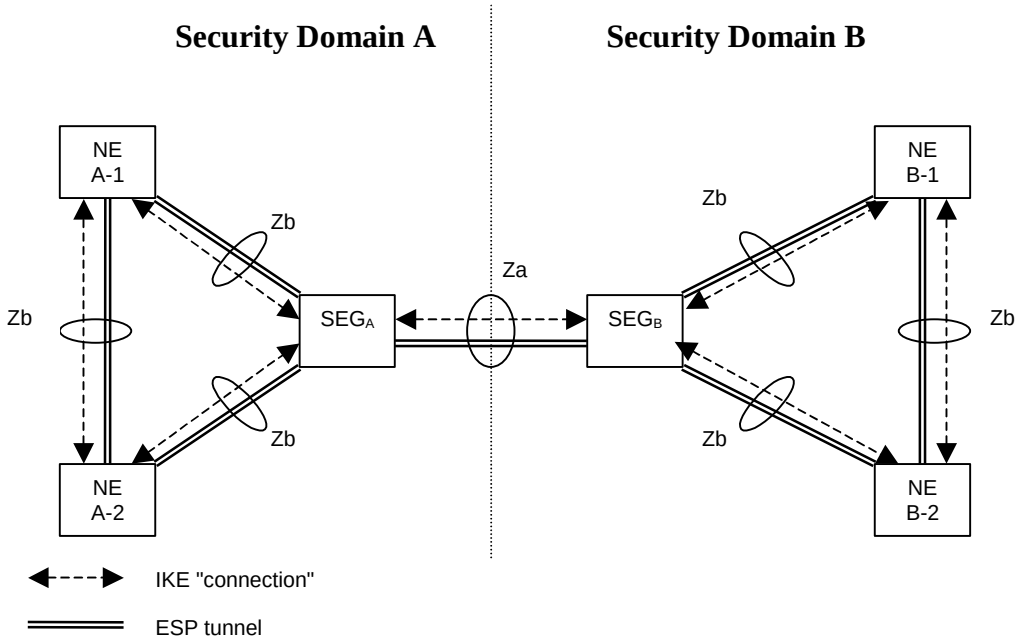

Figure 41: NDS/IP Architecture

The inter-domain Za interface consists of two parts: the IPsec Encapsulating Security Payloads (ESP) tunnel that carries the actual Diameter traffic, and the Internet Key Exchange (IKE) connection which is used to establish the IPsec ESP tunnel between the two Security Domains. 3GPP TS 33.210 [37] defines which versions of the protocols should be used. The use of IKE with pre-shared keys is also standardised in 3GPP TS 33.210 [37]

When two PMNs establish an LTE Roaming Agreement, they may also agree the properties of the Za interface, and the pre-shared key that authenticates this specific connection.

Alternatively, two PMNs may also agree to use certificates for mutual SEG authentication. The use of IKE with certificates is standardised in 3GPP TS 33.310 [38]. Both authentication methods (pre-shared keys and certificates) may coexist in parallel. If certificates are used, it is recommended to use certificates signed by a recognized signing authority (CA) and to adopt a mechanism to verify their validity.

Note**:** IP addresses and certificates of the SEGs may be published in IR.21 [40], but a pre-shared key needs to be kept secret between each two roaming partners.

Annex E Guidelines for proposed minimum QoS parameters for S8HR roaming scenario

This annex describes the recommended QoS parameters for the S8HR roaming scenario which represent the basic minimum QoS parameters that the home and visited operators are encouraged to support to avoid problems when launching commercial IMS voice roaming. Although this is primarily for IMS services, these recommendations include QoS settings for all services, including traditional internet traffic. These recommendations may be updated in the future to include RCS services. Bilateral agreements allow operators to negotiate other values.

The proposed QoS values and corresponding services are shown in Table 7:

Parameter	Minimum recommended roaming QoS values						
Service	IMS Voice		IMS Signalling4		IMS Video		Internet
QCI	1		5		8		9
ARP-PL	12		12		14		14
ARP-PVI	Disable[5]	Enabled[5]	Disable[5]	Enabled[5]	Enabled[5]		Enabled[5]
ARP-PCI	Enabled[5]	Disable[5]	Enabled[5]	Disable[5]	Enabled[5]	Disable[5]	Disable[5]
MBR-UL	156[3]						
MBR-DL	156[3]						
GBR-UL	156[3]						
GBR-DL	156[3]						

Table 16 Roaming QoS values

Note 1: Values not shown in the table are out-of-scope of this recommendation and should beagreed bilaterally between operators prior to use.

Note 2: Values in this table are the values that an inbound operator at a minimum should support for GBR and non-GBR bearers. If a lower priority is requested for any parameter, it should be accepted (e.g. ARP-PL=14 has a lower priority than 12 hence it will be accepted for QCI=1). If a higher priority is requested by HPMN, MME/S4-SGSN shall either apply the values received from HPMN or apply values as per roaming agreement or local configuration as per Section 7.2.2.

Note 3: MBR and GBR settings (in kbps) are based on the highest values needed to support three concurrent streams of QCI1 voice for all codecs, profiles, and level in TS 26.114 Annex E. Currently, AMR-NB, RTT, AMR-WB, EVS 13.2, EVS 24.4 are covered. If more codecs are added in the future, this table needs to be updated. Using lower or higher values for MBR and GBR for IMS voice can result in not being able to establish an IMS voice call and complete failure of setting up commercial roaming.

Note 4: IMS signalling may include SIP signalling for IMS Voice, IMS Video, SMS over IP, and RCS services.

Note 5: These are recommended PCI and PVI values; however, the bearer request should not be denied based on PCI or PVI; instead, the VPMN can change the requested PCI and/or PVI and accept the request. PVI downgrade is used to change the HPMN Disabled request to Enabled in the VPMN while PCI downgrade is used to change the HPMN Enabled request to Disabled in the VPMN, and vice versa for PVI/PCI upgrade.

Annex F Document Management

F.1 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

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
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
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

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
8.0	31 May 2012	Inclusion of the following CRs: MCR 018: Diameter security for LTE roaming MCR 019: GTP Firewalls MCR 020: Not mandating support for UE initiated bearer requests: MCR 021: Access Control in VPMN for CS Fallback MCR 022: IMEI notification from VPLMN to HPLMN MCR023: Disconnect connection to IMS APN MCR024: Implementing decision on HTTP/XCAP use MCR025: General Cleanup ofLTE Data Roaming Guideline MCR026: Support of SGs Interface mCR027: Inter-RAT Handover requirements	Packet#54, #55, #56 IREG#62 DAG#92	Itsuma Tanaka, NTT DOCOMO
9.0	29 November 2012	Inclusion of the following CRs: MCR028: Support of S4 SGSN and Gn/Gp SGSN in EPC MCR029: Default APN Guideline MCR030: Technical Requirements for static and dynamic QoS support for LTE MCR031: Introduction of MT Roaming Forwarding scenario 1	Packet#58, #59, #60, #61 IREG#63 DAG#99	Itsuma Tanaka, NTT DOCOMO

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
10.0	10 July 2013	Inclusion of the following CRs: CR1001: Addition of a new Diameter error cause for a better access control in the VPMN CR1002: Co-existence of Gr and S6d interfaces CR1003: Entire Document Review by SIGSG CR1004: Disconnection and reactivation of the PDN connection to the IMS APN CR1005: QoS for Diameter CR1006: Consequences of the single APN scenario CR1007: Security for LTE Roaming CR1008: Network Layer and Transport Layer Filters CR1009: IMS APN not as APN for XCAP (Ut) CR1010: CSFB IREG Test CR1011: Inter-RAT Pingpong avoidance CR1012: Guidance regarding the APN approach when roaming PRD editor has performed the following tasks: Correction of PRD title (as agreed in MCR028) Editorial changes (Font face and size, removal of hyperlinks, review of Latin terms, correction of wrong reference numbering)	Packet#62, #63, #64 IREG#64 DAG#104	Itsuma Tanaka, NTT DOCOMO

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
11.0	16 December 2013	Inclusion of the following CRs: CR1013: IMS APN on 2G and 3G Access CR1014: Diameter over IPX CR1015: QoS and roaming agreements CR1016: Bandwidth considerations for Inter-RAT HO CR1017: Signalling indication set by HSS in case of IMS APN CR1019: T-ADS for roaming subscribers PRD editor has performed the following tasks: Editorial changes (Font face and size, removal of hyperlinks, removal/correction of wrong auto-numbering)	Packet#65, #66, #67, #68 IREG#65 DAG#	Itsuma Tanaka, NTT DOCOMO
12.0	1 December 2014	Inclusion of the following CRs: IR.88 CR1018 Reject Cause for CSFB UEs without 2G3G Roaming Agreement IR.88 CR1021 Further clarification for default APN – revisited IR.88 CR1022 DIAMETER Security Updates IR.88 CR1023 Updating IREG Test references in Annex A IR.88 CR1024 2G, 3G and LTE roaming agreements and LBO IR.88 CR1025 DIAMETER Security Updates IR.88 CR1026 PS and EPS Context-ID alignment IR.88 CR1027 Implementation of outcome of the White Paper on 'APN for XCAPIMAPHTTP traffic' Editorial changes by PRD editor	Packet #69, #70, #71, #72, #73, #74, #75 IREG #66 IREG #67	Itsuma Tanaka (NTT Docomo, Inc.) Ralf Keller (Ericsson) Cédric Bonnet (Orange) Catherine Livet (Tata Communications Services (Bermuda) Limited) Nick Russell (BlackBerry Limited)

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
13.0	20 May 2015	Inclusion of the following CRs: IR.88 CR1029 Definition of Hubbing Architecture for LTE IR.88 CR1030 Clarifications on QoS Bearer Management and CSFB Support IR.88 CR1031 IMS APN behavior clarification when no IMS agreement IR.88 CR1032 Clarification of DNS records for 2G, 3G and LTE Roaming Agreement Scenarios IR.88 CR1033 Alignment to IR 33 VPMN identification for end user billing shall be based on MCC-MNC IR.88 CR1034 building origin destination host name and realm in consensus with topology hiding Editorial changes by PRD editor	Packet #76, #77, #78, #79, NG #1	Mihaela Ambrozie (Vodafone Roaming Services S.) Sajid Soormally (Alcatel Lucent) Cédric Bonnet (Orange) Gert Oster (Ericsson) Merieme El Orch (Orange) Stefan Dalluege (Vodafone GmbH)
13.1	26 May 2015	Late inclusion of IR.88 CR1028 Data Off and unsolicited downlink IP packets Editorial changes by PRD editor	NG #1	Ralf Keller (Ericsson) Cédric Bonnet (Orange)
14.0	10 February 2015	Inclusion of the following CRs: IR.88 CR1035 PGW selection consistent in all MMEs and SGSNs IR.88 CR1036 S8HR Changes for VoLTE S8HR Roaming IR.88 CR1037 ARP Considerations IR.88 CR1038 PDN connection to IMS APN at IRAT HO to-from 2G3G IR.88 CR1039 Emergency Service Support indicator constraints for Roaming S8HR IR.88 CR1040 IR.88 PMIP removal IR.88 CR1041 LTE Registrations Recommendation IR.88 CR1042 PCC in IMS Voice Roaming Architecture Editorial changes by PRD editor	Packet #80, #81, #82, #83, NG #2	Ralf Keller (Ericsson) Javier Sendin (GSMA) Mana Kaneko (NTT Docomo, Inc.) Masahide Murakami (NTT Docomo, Inc.) Cédric Bonnet (Orange) Mark McGinley (AT&T Mobility)
15.0	3 November 2016	Inclusion of the following CRs: IR.88 CR1043 Gy and S9 roaming interface clarification IR.88 CR1044 IP MTU constraints IR.88 CR1045 QoS Management	Packet #84, #85, #86, #87, #88 NG #3, NG #4,	Ralf Keller (Ericsson) Cédric Bonnet (Orange)

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
16.0	5 July 2017	Inclusion of the following CRs: IR.88 CR1046 GTP Security IR.88 CR1047 Diameter routing clarifications IR.88 CR1048 Support of target access restriction IR.88 CR1049 S8HR Alignment with 3GPP Release 14 IR.88 CR1050 S8HR correction Editorial changes by PRD editor	Packet #89, #90, #91, #92, NG #5	Sven Lachmund (Deutsche Telekom AG) Cédric Bonnet (Orange) Antti Pasanen (Nokia) George Foti (Ericsson) Leopold Murhammer (T-Mobile Austria GmbH)
17.0	18 December 2017	Inclusion of the following CRs: IR.88 CR1051 Diameter Procedure Timer Expiry Mitigation IR.88 CR1052 IR.88 on Alignment of Data Off with 3GPP” IR.88 CR1053 VoLTE Roaming Restriction	Packet #94, #95, NG #6	Scott Bailey (British Telecommunications PLC) Jorgen Axell (Ericsson) Ralf Keller (Ericsson)
18.0	7 June 2018	Inclusion of the following CRs: IR.88 CR1054 S8HR LI Alignment with 3GPP Release 14 IR.88 CR1055 E-UTRAN NR Dual Connectivity with EPC	Packet#96, #96, NG #7	George Foti (Ericsson) George Foti (Ericsson)
19.0	7 May 2019	Inclusion of following CRs: IR.88 CR1056 LTE and EPC Roaming Guidelines IR.88 CR1057 QoS Support in Roaming IR.88 CR1058 Clarifications concerning E-EUTRA-NR Dual Connectivity with EPC IR.88 CR1059 Update to include reference to TAC-LAC guidelines PRD IR.88 CR1060 Updating Access Control in the VPMN		Javier Sendin (GSMA) Kathleen Leach (Sprint Corporation) Jo Takahashi (NTT DOCOMO, Inc Kathleen Leach (Sprint Corporation) Azumi Matsusako (NTT DOCOMO, Inc.)

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
20.0	16 Oct 2019	IR.88 CR1061 IPX Diameter security IR.88 CR1062 Updating QoS Parameters definition		Marc Balon (Orange) Fabrizio Fiorucci (Telecom Italia SpA)
21.0	18 May 2020	IR.88 CR1063 Updating Emergency calls indicator Add IETF RFC 1034 [65] and IETF RFC 1035 [66] in Cross Reference		Azumi Matsusako (NTT DOCOMO, Inc.) Editor

22.0	November 2020	IR.88 CR1064 Clarification of deployment models for Diameter Phase 1 IR.88 CR1065 Remove HSPA voice roaming architecture IR.88 CR1066 Recommendation for S8HR IR.88 CR1067 MIoT location in roaming IR.88 CR1068 Reference corrections IR.88 CR1070 ARP Values for the establishment of VoLTE bearers IR.88 CR1071 Update of Title IR.88 CR1072 Emergency Bearer Services for Roaming IR.88 CR1073 Clarifications concerning GW Selection in EN-DC IR.88 CR1074 ARP Values for the establishment of VoLTE bearers IR.88 CR1075 QOS Parameters IR.88 CR1076 Multiple Realm for Multiple IMSI's		Marc Balon (Orange) Ralf Keller (Ericsson) Ralf Keller (Ericsson) Marc Balon (Orange) Boris Antsev (T-Mobile USA) Steffen Habermann (Telekom Deutschland GmbH) Sajid Soormally (Nokia) Steffen Habermann (Telekom Deutschland GmbH) Jo Takahashi (NTT DOCOMO, Inc.) Ralf Keller (Ericsson); Steffen Habermann (Telekom Deutschland GmbH) Wayne Cutler (GSMA) Eddy GOFFIN (ORANGE)
23.0	May 2021	IR.88 CR1077 Wording adaptation to 4G context IR.88 CR1078 VoLTE replacement by IMS voice or even S8HR depending on the context IR.88 CR1079 Update to QoS Table in Annex E		Eddy GOFFIN (ORANGE) Eddy GOFFIN (ORANGE) Wayne Cutler (GSMA)

24.0	May 2021	IR.88 CR1080 IR.88 CR on OI-Replacement	NG	Eddy GOFFIN (ORANGE)
25.0	Nov 2022	IR.88 CR1081 IR.88 New Section for UAS Well-Known APN IR88 CR1083 Adding additional emergency call text IR88 CR1084 Typo Correction section 5.2.2.5 IR88 CR1085 ew Section for SMS in MME	NG NG NG NG	Jignesh Patel (Verizon) Wayne Cutler (GSMA Eddy GOFFIN (ORANGE Belgium nv/SA) Javier Sendin (GSMA)
26.0	May 2023	NRG 017_001 IR.88 not Following QoS Recommendation R4 NRG 017_004 IR.88 guideline on gating r1	NG	Tero Jalkanen (Telia Company), Ralf Keller (Ericsson) Ralf Keller (Ericsson)
27.0	Feb 2024	NRG 019_006 IR.88 CR1090RaKe correction of IMS APN description r2	NG	Ralf Keller (Ericsson)
27.1	Feb 2024	GERI 004_012 IR.88 CR1069_Adding reference to FS.21 (missed CR)	NG	Pieter Veenstra (NetNumber)

Other Information

Type	Description
Document Owner	Networks / Packet
Editor / Company	Eddy Goffin / 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.

8