

Technical Specification Group Services and System Aspects **TSGS#6(99)538**
Meeting #6, Nice, France, 15-17 December 1999

Source: TSG SA WG2
Title: Coversheet for 23.060
Agenda Item: 5.2.3

Release 1999 Submission form for 23.060

Work Area / Item:		3G TS 23.060			
Affects:	UE/MS: X	CN: X	UTRAN: X	Compatibility Issues: Yes: X No:	
Expected Completion Date:		March 2000 (TSG SA#7)			
Services impacted:		UMTS packet services, GPRS			
Specifications affected:		-			
Tasks within work which are not complete:		<p>Shall anonymous access be supported for UMTS or GPRS 99? An LS has been sent to S1 to ask for guidance.</p> <p>Subclause 6.8.4: Shall the MS be able to send its IMSI encrypted? This issue is still being discussed in S3.</p> <p>Subclause 9.3: Shall the max N-PDU size be different from 1500 octets?</p> <p>Subclause 12.1.1: Is TCP support for UMTS on Gn and IuPS needed? S2-99D41 suggests that TCP is supported in the user plane for both Gn and IuPS.</p> <p>Subclause 15.1.3: Fair charging for UMTS to be determined.</p>			
Consequences if not included in Release 1999:		-			
Accepted by TSG#		for late inclusion in Release 1999:			

Abstract of document:

3G TS 23.060 is the signalling and network aspects stage-2 service description for packet-domain services in UMTS and GPRS.

Contentious Issues:

No particular contentious issues expected.

3G TS 23.060 V3.1.0 (1999-10)

Technical Specification

**3rd Generation Partnership Project;
Technical Specification Group Core Network;
Digital cellular telecommunications system (Phase 2+);
General Packet Radio Service (GPRS);
Service description;
Stage 2
(3G TS 23.060 version 3.1.0)**



Reference

3TS/TSGS-0123002U

Keywords

Numbering, Addressing

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.org>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 1999, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword.....	10
1 Scope.....	11
2 References	11
3 Definitions, abbreviations and symbols.....	13
3.1 Definitions	13
3.2 Abbreviations.....	14
3.3 Symbols	15
4 Main Concepts.....	16
4.1 Main GPRS Concepts	17
4.2 Main UMTS Concepts	17
5 General Packet Domain Architecture and Transmission Mechanism.....	17
5.1 Packet Domain Access Interfaces and Reference Points	17
5.2 Network Interworking.....	18
5.2.1 PSPDN Interworking.....	18
5.2.2 Internet (IP) Interworking	18
5.3 High-Level Functions	19
5.3.1 Network Access Control Functions	19
5.3.1.1 Registration Function.....	19
5.3.1.2 Authentication and Authorisation Function	19
5.3.1.3 Admission Control Function.....	19
5.3.1.4 Message Screening Function	20
5.3.1.5 Packet Terminal Adaptation Function	20
5.3.1.6 Charging Data Collection Function	20
5.3.2 Packet Routeing and Transfer Functions.....	20
5.3.2.1 Relay Function.....	20
5.3.2.2 Routeing Function	20
5.3.2.3 Address Translation and Mapping Function.....	20
5.3.2.4 Encapsulation Function	20
5.3.2.5 Tunnelling Function.....	20
5.3.2.6 Compression Function	21
5.3.2.7 Ciphering Function.....	21
5.3.2.8 Domain Name Server Function	21
5.3.3 Mobility Management Functions.....	21
5.3.4 Logical Link Management Functions for GPRS	21
5.3.4.1 Logical Link Establishment Function	21
5.3.4.2 Logical Link Maintenance Functions	21
5.3.4.3 Logical Link Release Function	21
5.3.5 Radio Resource Management Functions	21
5.3.6 Network Management Functions.....	21
5.4 Logical Architecture	22
5.4.1 Packet Domain Core Network Nodes.....	22
5.4.2 Packet Domain PLMN Backbone Networks	23
5.4.3 HLR.....	23
5.4.4 SMS-GMSC and SMS-IW MSC.....	23
5.4.5 GPRS Mobile Stations	24
5.4.6 UMTS Mobile Stations	24
5.4.7 Charging Gateway Functionality.....	24
5.5 Assignment of Functions to General Logical Architecture	25
5.6 User and Control Planes	26
5.6.1 User Plane for GPRS.....	26
5.6.1.1 MS – GGSN	26
5.6.1.2 GSN – GSN.....	27
5.6.2 User Plane for UMTS	27

5.6.2.1	MS – GGSN	27
5.6.2.2	GSN – GSN	28
5.6.3	Control Plane.....	28
5.6.3.1	MS – SGSN for GPRS	28
5.6.3.2	MS – SGSN for UMTS	29
5.6.3.3	SGSN - HLR.....	29
5.6.3.4	SGSN - MSC/VLR	30
5.6.3.5	SGSN - EIR.....	30
5.6.3.6	SGSN - SMS-GMSC or SMS-IW MSC	30
5.6.3.7	GSN - GSN.....	31
5.6.3.8	GGSN - HLR.....	31
5.6.3.8.1	MAP-based GGSN - HLR Signalling	31
5.6.3.8.2	GTP and MAP-based GGSN - HLR Signalling	32
6	Mobility Management Functionality	32
6.1	Definition of Mobility Management States	32
6.1.1	Mobility Management States for GPRS	32
6.1.1.1	IDLE (GPRS) State	32
6.1.1.2	STANDBY State	32
6.1.1.3	READY State	33
6.1.1.4	State Transitions and Functions.....	34
6.1.2	Mobility Management States for UMTS	36
6.1.2.1	PMM-DETACHED State	36
6.1.2.2	PMM-IDLE State	36
6.1.2.3	PMM-CONNECTED State	36
6.1.2.4	State Transitions and Functions.....	36
6.1.2.4.1	Error Cases.....	38
6.2	Mobility Management Timer Functions.....	38
6.2.1	READY Timer Function for GPRS.....	38
6.2.2	Periodic RA Update Timer Function.....	39
6.2.3	Mobile Reachable Timer Function.....	39
6.3	Interactions Between SGSN and MSC/VLR.....	40
6.3.1	Administration of the SGSN - MSC/VLR Association	40
6.3.2	Combined RA / LA Updating.....	41
6.3.3	CS Paging for GPRS	41
6.3.3.1	Paging Co-ordination for GPRS	42
6.3.4	CS Paging for UMTS	43
6.3.4.1	Network Operation Modes for UMTS.....	43
6.3.5	Non-PS Alert.....	44
6.3.6	MS Information Procedure.....	44
6.3.7	MM Information Procedure	44
6.4	MM Procedures	45
6.5	PS Attach Function	45
6.5.1	GPRS Attach Function	45
6.5.2	UMTS PS Attach Function	49
6.6	Detach Function.....	52
6.6.1	MS-Initiated Detach Procedure	53
6.6.2	Network-Initiated Detach Procedure.....	54
6.6.2.1	SGSN-Initiated Detach Procedure.....	54
6.6.2.2	HLR-Initiated Detach Procedure	55
6.7	Purge Function.....	55
6.8	Security Function.....	56
6.8.1	Authentication	56
6.8.1.1	Authentication of GSM Subscriber in GSM.....	56
6.8.1.2	Authentication of UMTS Subscriber in UMTS.....	57
6.8.1.3	Authentication of GSM Subscriber in UMTS.....	58
6.8.1.4	Authentication of UMTS Subscriber in GSM.....	58
6.8.2	User Identity Confidentiality.....	59
6.8.2.1	User Identity Confidentiality for GPRS.....	59
6.8.2.2	User Identity Confidentiality for UMTS.....	59
6.8.2.3	P-TMSI Signature.....	59

6.8.2.4	P-TMSI Reallocation Procedure.....	59
6.8.3	User Data and GMM/SM Signalling Confidentiality	60
6.8.3.1	Scope of Ciphering	60
6.8.3.2	Ciphering Algorithm.....	60
6.8.3.3	Start of Ciphering	60
6.8.4	Identity Check Procedures	61
6.8.5	Data Integrity Procedure for UMTS.....	61
6.9	Location Management Function	61
6.9.1	Location Management Procedures for GPRS.....	62
6.9.1.1	Cell Update Procedure.....	62
6.9.1.2	Routeing Area Update Procedure	62
6.9.1.2.1	Intra SGSN Routeing Area Update	63
6.9.1.2.2	Inter SGSN Routeing Area Update	64
6.9.1.3	Combined RA / LA Update Procedure	66
6.9.1.3.1	Combined Intra SGSN RA / LA Update	66
6.9.1.3.2	Combined Inter SGSN RA / LA Update	68
6.9.2	Location Management Procedures for UMTS.....	70
6.9.2.1	Routeing Area Update Procedure	71
6.9.2.2	Serving RNC Relocation procedure	74
6.9.3	Periodic RA and LA Updates	78
6.10	Tunnelling of non-GSM Signalling Messages Function	78
6.10.1	Uplink Tunnelling of non-GSM Signalling Messages Procedure.....	79
6.10.2	Downlink Tunnelling of non-GSM Signalling Messages Procedure.....	79
6.11	Subscriber Management Function.....	80
6.11.1	Subscriber Management Procedures	80
6.11.1.1	Insert Subscriber Data Procedure	80
6.11.1.2	Delete Subscriber Data Procedure	81
6.12	Service Request Procedure for UMTS.....	81
6.12.1	Service Request Initiated by MS Procedure	81
6.12.2	Service Request Initiated by Network Procedure.....	83
6.13	UMTS-GPRS Intersystem Handover.....	84
6.13.1	Intersystem Handover within an RA between Cells in Different Systems.....	84
6.13.1.1	UMTS to GPRS Handover	84
6.13.1.2	GPRS to UMTS Handover	86
6.13.2	Intersystem Handover at RA Change	87
6.13.2.1	UMTS to GPRS Handover	87
6.13.2.2	GPRS to UMTS Handover	90
6.14	Classmark Handling.....	92
6.14.1	Radio Access Classmark	93
6.14.2	SGSN Classmark.....	93
7	Network Management Functionality	93
8	Radio Resource Functionality	93
8.1	Radio Resource Functionality for GPRS	93
8.1.1	Cell Selection and Reselection	93
8.1.2	Discontinuous Reception.....	94
8.1.3	Radio Resource Management.....	94
8.1.3.1	Layer Functions	94
8.1.3.2	Model of Operation	94
8.1.3.2.1	Dynamic Allocation of Radio Resources	94
8.1.4	Paging for GPRS Downlink Transfer.....	95
8.2	Radio Resource Functionality for UMTS	95
8.2.1	Radio Resource Management.....	95
8.2.2	RRC State Machine.....	96
8.2.3	Paging Initiated by CN.....	96
8.2.3.1	PS Paging Initiated by 3G-SGSN Without RRC Connection for CS.....	97
8.2.3.2	PS Paging Initiated by 3G-SGSN With RRC Connection for CS.....	98
8.2.4	Paging Initiated by UTRAN.....	98

9	Packet Routing and Transfer Functionality	99
9.1	Definition of Packet Data Protocol States.....	99
9.1.1	INACTIVE State	99
9.1.2	ACTIVE State	99
9.2	PDP Context Activation, Modification, and Deactivation Functions.....	100
9.2.1	Static and Dynamic PDP Addresses.....	100
9.2.2	Activation Procedures	101
9.2.2.1	PDP Context Activation Procedure	101
9.2.2.1.1	Secondary PDP Context Activation Procedure	103
9.2.2.2	Network-Requested PDP Context Activation Procedure.....	104
9.2.2.2.1	Successful Network-Requested PDP Context Activation Procedure	105
9.2.2.2.2	Unsuccessful Network-Requested PDP Context Activation Procedure	105
9.2.2.3	Anonymous Access PDP Context Activation Procedure	107
9.2.3	Modification Procedures	108
9.2.3.1	SGSN-Initiated PDP Context Modification Procedure.....	109
9.2.3.2	GGSN-Initiated PDP Context Modification Procedure.....	109
9.2.3.3	MS-Initiated PDP Context Modification Procedure	110
9.2.4	Deactivation Procedures.....	111
9.2.4.1	PDP Context Deactivation Initiated by MS Procedure.....	111
9.2.4.2	PDP Context Deactivation Initiated by SGSN Procedure	112
9.2.4.3	PDP Context Deactivation Initiated by GGSN Procedure.....	112
9.2.4.4	Anonymous Access PDP Context Deactivation Initiated by MS Procedure.....	113
9.2.4.5	Anonymous Access PDP Context Deactivation Initiated by GGSN Procedure.....	113
9.3	Packet Routing and Transfer Function	114
9.4	Relay Function.....	114
9.5	Packet Terminal Adaptation Function	115
9.6	Encapsulation Function.....	115
9.6.1	Encapsulation Between GSNs.....	115
9.6.2	Encapsulation Between 3G-SGSN and RNC	115
9.6.2	Encapsulation Between 2G-SGSN and MS.....	115
9.6.3	Encapsulation Between RNC and MS.....	115
10	Message Screening Functionality	115
11	Compatibility Issues	116
12	Transmission.....	116
12.1	Transmission Modes	116
12.1.1	GTP-U Transmission Modes.....	116
12.1.2	LLC Transmission Modes for GPRS	116
12.1.3	RLC Transmission Modes.....	117
12.2	Logical Link Control Functionality for GPRS	117
12.2.1	Addressing	117
12.2.2	Services	117
12.2.3	Functions.....	117
12.3	Subnetwork Dependent Convergence Functionality for GPRS.....	118
12.3.1	Services	118
12.3.2	Subfunctions.....	119
12.4	PDCP for UMTS	119
12.5	Octet Stream Protocol Functionality.....	119
12.5.1	PAD Function.....	121
12.5.1.1	Packet Assembler	121
12.5.1.1.1	Buffer Full.....	121
12.5.1.1.2	Inactivity Timer Expiry.....	121
12.5.1.1.3	Maximum Buffer Delay Timer Expiry.....	121
12.5.1.1.4	Special Character	121
12.5.1.1.5	Change in Flow Control State	121
12.5.1.1.6	Immediate Forwarding Request	121
12.5.1.2	Packet Disassembler	121
12.5.2	Quality of Service.....	121
12.6	Point-to-Point Protocol Functionality	122

12.6.1	User Plane for PDP Type PPP	122
12.6.2	Functions	122
12.7	Gb Interface for GPRS	123
12.7.1	Physical Layer Protocol	123
12.7.2	Link Layer Protocols	123
12.7.3	BSS GPRS Protocol	123
12.7.3.1	Inter-dependency of the BSSGP and LLC Functions	124
12.7.3.2	BSSGP Addressing	124
12.7.3.3	BVCI Contexts in BSS and in SGSN	125
12.7.3.4	Flow Control Between SGSN and BSS over the Gb Interface	125
12.7.3.5	BSS Context	125
12.7.3.5.1	BSS Packet Flow Context Creation Procedure	126
12.7.3.5.2	SGSN-Initiated BSS Packet Flow Context Modification Procedure	126
12.7.3.5.3	BSS-Initiated BSS Packet Flow Context Modification Procedure	127
12.7.3.5.4	BSS Packet Flow Context Deletion Procedures	127
12.8	Iu Interface for UMTS	127
12.8.1	Physical Layer Protocols	128
12.8.2	Higher-Layer Protocols	128
12.8.2.1	Higher-Layer Protocols for User Data Transport	128
12.8.2.1.1	Consistent Sequence Numbering of PDUs on Iu and Gn Interfaces	128
12.8.2.2	Higher-Layer Protocols for Signalling Transport	129
12.8.3	Iu Release Procedure	129
12.8.4	Location Reporting Procedure	130
12.9	Abis Interface for GPRS	130
12.9.1	Remote Packet Control Unit	131
13	Information Storage	132
13.1	HLR	132
13.2	SGSN	134
13.3	GGSN	136
13.4	MS	137
13.5	MSC/VLR	138
13.6	BSS for GPRS	138
13.7	RNC for UMTS	139
13.8	Recovery and Restoration Procedures	139
13.8.1	HLR Failure	139
13.8.2	SGSN Failure	139
13.8.3	GGSN Failure	140
13.8.4	VLR Failure	140
13.8.5	BSS Failure for GPRS	140
13.8.6	RNC Failure for UMTS	140
14	Identities	140
14.1	IMSI	140
14.2	Packet TMSI	141
14.3	NSAPI and TLLI for GPRS	141
14.4	PDP Address	142
14.5	TID	142
14.6	Routeing Area Identity	142
14.7	UTRAN Registration Area Identity for UMTS	143
14.8	Cell Identity	143
14.9	GSN Addresses	143
14.9.1	GSN Address	143
14.9.2	GSN Number	143
14.10	RNC Addresses	143
14.10.1	RNC Address	143
14.10.2	RNC Number	143
14.11	Access Point Name	143
15	Operational Aspects	144
15.1	Charging	144

15.1.1	Charging Information	144
15.1.2	Reverse Charging	145
15.1.3	Fair Charging for UMTS	145
15.2	Quality of Service Profile	145
15.2.1	Precedence Class	145
15.2.2	Delay Class	146
15.2.3	Reliability Class	146
15.2.4	Throughput Classes	146
15.2.4.1	Peak Throughput Class	146
15.2.4.2	Mean Throughput Class	147
16	Interactions with Other GSM Services	147
16.1	Point-to-point Short Message Service	148
16.1.1	Mobile-terminated SMS Transfer	148
16.1.1.1	Unsuccessful Mobile-terminated SMS Transfer	148
16.1.2	Mobile-originated SMS Transfer	150
16.2	Circuit-switched Services for GPRS	150
16.2.1	Suspension of GPRS Services	150
16.2.2	GPRS and Dedicated Mode Priority Handling	151
16.3	Supplementary Services	152
Annex A (normative): APN and GGSN Selection		153
A.1	Definitions	153
A.2	Selection Rules	153
Annex B (normative): Internet-Hosted Octet Stream Service		160
B.1	Direction of Connection Setup	160
B.2	Bearer	160
B.3	Setup Data	160
B.3.1	Protocol Type – TCP or UDP	160
B.3.2	Host Name	161
B.3.3	Port Number	161
B.3.4	PAD Parameters	161
B.4	Flow Control	161
B.5	Break Signal	161
B.6	Connection Establishment Procedure	161
B.6.1	Fully User-Specified Establishment	162
B.6.2	Default Internet Endpoint Parameters Establishment	162
B.7	Connection Termination	162
B.7.1	MS-initiated TCP IHOSS Connection Termination	162
B.7.2	MS-initiated UDP IHOSS Connection Termination	162
B.7.3	Internet Host Initiated TCP IHOSS Connection Termination	163
B.8	Quality of Service	163
B.9	Security	163
B.9.1	Authentication of the GPRS User	163
B.9.2	Malicious Reconfiguration of the GPRS Device	163

B.10 Maintenance..... 163

Annex C (informative): Figures..... 164

Annex D (informative): Tables 167

Annex E: Change History 168

History..... 169

Foreword

This Technical Specification has been produced by the 3GPP.

The present document defines the stage-2 service description for a General Packet Radio Service (GPRS) within the digital cellular telecommunications system (Phase 2+).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 Indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the specification;

1 Scope

The present document defines the stage-2 service description for the packet domain, which includes the General Packet Radio Service (GPRS) in GSM, and the packet side of UMTS. CCITT I.130 [29] describes a three-stage method for characterisation of telecommunication services, and CCITT Q.65 [31] defines stage 2 of the method.

This document does not cover the Access Network functionality. GSM 03.64 [11] contains an overall description of the GSM GPRS Access Network. UMTS 25.301 contains an overall description of the UMTS Terrestrial Radio Access Network.

2 References

[All references need to be checked once release 99 stabilizes.]

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

- [1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".
- [2] GSM 01.61: "Digital cellular telecommunications system (Phase 2+); GPRS ciphering algorithm requirements".
- [3] UMTS 22.060: "General Packet Radio Service (GPRS); Service description; Stage 1".
- [4] UMTS 23.003: "Numbering, addressing and identification".
- [5] UMTS 23.007: "Restoration procedures".
- [6] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".
- [7] UMTS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".
- [8] UMTS 23.040: "Technical realization of the Short Message Service (SMS); Point-to-Point (PP)".
- [11] GSM 03.64: "Digital cellular telecommunications system (Phase 2+); Overall description of the General Packet Radio Service (GPRS) Radio interface; Stage 2".
- [12] UMTS 24.007: "Mobile radio interface signalling layer 3; General aspects".
- [13] UMTS 24.008: "Mobile radio interface layer 3 specification; Core Network Protocols – Stage 3".
- [14] GSM 04.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control / Medium Access Control (RLC/MAC) protocol".
- [15] GSM 04.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) – Serving GPRS Support Node (SGSN); Logical Link Control (LLC) layer specification".

- [16] GSM 04.65: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) – Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCCP)".
- [17] UMTS 27.060: "General Packet Radio Service (GPRS); Mobile Station (MS) supporting GPRS".
- [18] GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre - Base Station System (MSC - BSS) interface: Layer 3 specification".
- [19] GSM 08.14: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Gb interface layer 1".
- [20] GSM 08.16: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Network Service".
- [21] GSM 08.18: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".
- [22] GSM 08.60: "Digital cellular telecommunications system (Phase 2+); Inband control of remote transcoders and rate adaptors for Enhanced Full Rate (EFR) and full rate traffic channels."
- [23] UMTS 29.002: "Mobile Application Part (MAP) specification".
- [24] UMTS 29.016: "General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface network service specification".
- [25] UMTS 29.018: "General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface layer 3 specification".
- [26] UMTS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".
- [27] UMTS 29.061: "General Packet Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN)".
- [28] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".
- [28a] GSM 12.15: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Charging".
- [29] CCITT Recommendations I.130: "General modelling methods – Method for the characterisation of telecommunication services supported by an ISDN and network capabilities of an ISDN".
- [30] CCITT Recommendation E.164: "Numbering plan for the ISDN era".
- [31] CCITT Recommendation Q.65: "Methodology – Stage 2 of the method for the characterization of services supported by an ISDN".
- [32] CCITT Recommendation V.42 bis: "Data communication over the telephone network – Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures".
- [33] CCITT Recommendation X.3: "Packet assembly disassembly facility (PAD) in a public data network".
- [34] CCITT Recommendation X.25: "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

- [35] CCITT Recommendation X.28: "DTE / DCE interface for a start-stop mode data terminal equipment accessing the packet assembly / disassembly facility (PAD) in a public data network situated in the same country".
- [36] CCITT Recommendation X.29: "Procedures for the exchange of control information and user data between a packet assembly / disassembly (PAD) facility and a packet mode DTE or another PAD".
- [37] CCITT Recommendation X.75: "Packet-switched signalling system between public networks providing data transmission services".
- [38] CCITT Recommendation X.121: "International Numbering Plan for Public Data Networks".
- [39] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).
- [40] IETF RFC 791 (1981): "Internet Protocol" (STD 5).
- [41] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).
- [42] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).
- [43] IETF RFC 1034 (1987): "Domain Names – Concepts and Facilities" (STD 7).
- [44] IETF RFC 1661 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).
- [45] IETF RFC 1542 (1993): "Clarification and Extensions for the Bootstrap Protocol".
- [46] IETF RFC 2002 (1996): "IPv4 Mobility Support".
- [47] IETF RFC 2131 (1997): "Dynamic Host Configuration Protocol".
- [48] Bellcore GR-000301 Issue 2 December 1997: "Public Packet Switched Network Generic Requirements (PPSNGR)".
- [49] TIA/EIA-136 (1999): "TDMA Cellular / PCS"; Arlington: Telecommunications Industry Association.
- [50] UMTS 25.301: "Radio Interface Protocol Architecture".
- [51] UMTS 25.303: "UE Functions and Interlayer Procedures in Connected Mode".
- [52] UMTS 25.331: "RRC Protocol Specification".
- [53] UMTS 25.401: "UTRAN Overall Description [UMTS <spec>] ".
- [54] UMTS 23.121: "Architectural Requirements for Release 1999".
- [55] UMTS 25.322: "RLC Protocol Specification".
- [56] UMTS 25.412: "UTRAN Iu Interface Signalling Transport".
- [57] UMTS 25.323: "FFS".

3 Definitions, abbreviations and symbols

3.1 Definitions

Refer to UMTS 22.060 and UMTS 25.401.

- 2G- / 3G- The prefixes 2G- and 3G- refers to functionality that supports only GSM GPRS or UMTS, respectively, e.g., 2G-SGSN refers only to the GSM GPRS functionality of an SGSN. When the prefix is omitted, reference is made independently from the GSM GPRS or UMTS functionality.

3.2 Abbreviations

For the purposes of the present document the following abbreviations apply. Additional applicable abbreviations can be found in GSM 01.04 [1].

AA	Anonymous Access
APN	Access Point Name
ATM	Asynchronous Transfer Mode
AUTN	Authentication Token
BG	Border Gateway
BSSAP+	Base Station System Application Part +
BSSGP	Base Station System GPRS Protocol
BVCI	BSSGP Virtual Connection Identifier
CCU	Channel Codec Unit
CDR	Call Detail Record
CGF	Charging Gateway Functionality
CGI	Cell Global Identification
CK	Cipher Key
CS	Circuit Switched
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGPRS	Enhanced GPRS
GEA	GPRS Encryption Algorithm
GGSN	Gateway GPRS Support Node
GMM/SM	GPRS Mobility Management and Session Management
GSIM	GSM Service Identity Module
GSN	GPRS Support Node
GTP	GPRS Tunnelling Protocol
GTP-C	GTP Control Plane
GTP-U	GTP User Plane
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IHOSS	Internet-Hosted Octet Stream Service
IK	Integrity Key
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internet Packet eXchange
ISP	Internet Service Provider
KSI	Key Set Identifier
L2TP	Layer-2 Tunnelling Protocol
LL-PDU	LLC PDU
LLC	Logical Link Control
MAC	Medium Access Control
MIP	Mobile IP
MNRF	Mobile station Not Reachable Flag
MNRG	Mobile station Not Reachable for GPRS flag
MNRR	Mobile station Not Reachable Reason
MTP2	Message Transfer Part layer 2
MTP3	Message Transfer Part layer 3
NGAF	Non-GPRS Alert Flag
NS	Network Service
NSAPI	Network layer Service Access Point Identifier
NSS	Network SubSystem
OSP	Octet Stream Protocol
P-TMSI	Packet TMSI
PCU	Packet Control Unit
PDCH	Packet Data CHannel
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network

PDP	Packet Data Protocol, e.g., IP or X.25 [34]
PDU	Protocol Data Unit
PPF	Paging Proceed Flag
PPP	Point-to-Point Protocol
PTM	Point To Multipoint
PTP	Point To Point
PVC	Permanent Virtual Circuit
RA	Routeing Area
RAC	Routeing Area Code
RAI	Routeing Area Identity
RANAP	Radio Access Network Application Protocol
RLC	Radio Link Control
RNS	Radio Network Subsystem
RNTI	Radio Network Temporary Identity
RRC	Radio Resource Control
SGSN	Serving GPRS Support Node
SM	Short Message
SM-SC	Short Message service Service Centre
SMS-GMSC	Short Message Service Gateway MSC
SMS-IWMSC	Short Message Service Interworking MSC
SN-PDU	SNDCP PDU
SNDC	SubNetwork Dependent Convergence
SNDCP	SubNetwork Dependent Convergence Protocol
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TFT	Traffic Flow Template
TID	Tunnel Identifier
TLLI	Temporary Logical Link Identity
TOM	Tunnelling Of Messages
TRAU	Transcoder and Rate Adaptor Unit
UDP	User Datagram Protocol
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
URA	UTRAN Registration Area
USIM	User Service Identity Module
UTRAN	UMTS Terrestrial Radio Access Network

3.3 Symbols

For the purposes of the present document the following symbols apply:

Ga	Charging data collection interface between a CDR transmitting unit (e.g., an SGSN or a GGSN) and a CDR receiving functionality (a CGF).
Gb	Interface between an SGSN and a BSS.
Gc	Interface between a GGSN and an HLR.
Gd	Interface between a SMS-GMSC and an SGSN, and between a SMS-IWMSC and an SGSN.
Gf	Interface between an SGSN and an EIR.
Gi	Reference point between GPRS and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs.
Gr	Interface between an SGSN and an HLR.
Gs	Interface between an SGSN and an MSC/VLR.

Iu	Interface between the RNS and the core network. It is also considered as a reference point.
kbit/s	Kilobits per second.
Mbit/s	Megabits per second. 1 Mbit/s = 1 million bits per second.
R	Reference point between a non-ISDN compatible TE and MT. Typically this reference point supports a standard serial interface.
Reporting Area	The service area for which an MS's location shall be reported.
Service Area	The location accuracy level needed for service management purposes in the 3G-SGSN, e.g., a routing area or a cell. The 3G-SGSN can request the SRNC to report: i) the MS's current service area; ii) when the MS moves into a given service area; or iii) when the MS moves out of a given service area.
Um	Interface between the mobile station (MS) and the GPRS fixed network part. The Um interface is the GPRS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GPRS services through this interface.
Uu	Interface between the mobile station (MS) and the UMTS fixed network part. The Uu interface is the UMTS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the UMTS services through this interface.

4 Main Concepts

The packet domain uses a packet-mode technique to transfer high-speed and low-speed data and signalling in an efficient manner. The packet domain optimises the use of network and radio resources. Strict separation between the radio subsystem and network subsystem is maintained, allowing the network subsystem to be reused with other radio access technologies.

A common packet domain Core Network is used for both GPRS and UMTS. This common Core Network provides packet-switched (PS) services and is designed to support several quality of services levels in order to allow efficient transfer of non real-time traffic (e.g., intermittent and bursty data transfers, occasional transmission of large volumes of data) and real-time traffic (e.g., voice, video). Applications based on standard data protocols and SMS are supported, and interworking is defined with IP networks and X.25 networks. Charging should be flexible and allow to bill according to the amount of data transferred, the QoS supported, and the duration of the connection.

The Serving GPRS Support Node (SGSN) keeps track of the individual MSs' location and performs security functions and access control. The SGSN is connected to the GPRS base station system through the Gb interface and/or to the UMTS Radio Access Network through the Iu interface.

The Gateway GPRS Support Node (GGSN) provides interworking with external packet-switched networks, and is connected with SGSNs via an IP-based packet domain PLMN backbone network.

The Charging Gateway Functionality (CGF) collects charging records from SGSNs and GGSNs.

The HLR contains GPRS and UMTS subscriber information.

The SMS-GMSCs and SMS-IWMSCs support SMS transmission via the SGSN.

Optionally, the MSC/VLR can be enhanced for more-efficient co-ordination of packet-switched and circuit-switched services and functionality: e.g., combined GPRS and non-GPRS location updates.

In order to access the PS services, an MS shall first make its presence known to the network by performing a PS attach. This makes the MS available for SMS over PS, paging via the SGSN, and notification of incoming PS data.

In order to send and receive PS data, the MS shall activate the Packet Data Protocol context that it wants to use. This operation makes the MS known in the corresponding GGSN, and interworking with external data networks can commence.

User data is transferred transparently between the MS and the external data networks with a method known as encapsulation and tunnelling: data packets are equipped with PS-specific protocol information and transferred between

the MS and the GGSN. This transparent transfer method lessens the requirement for the PLMN to interpret external data protocols, and it enables easy introduction of additional interworking protocols in the future.

4.1 Main GPRS Concepts

New GPRS radio channels are defined, and the allocation of these channels is flexible: from 1 to 8 radio interface timeslots can be allocated per TDMA frame, timeslots are shared by the active users, and up and downlink are allocated separately. The radio interface resources can be shared dynamically between speech and data services as a function of service load and operator preference. Various radio channel coding schemes are specified to allow bitrates from 9 to more than 150 kbit/s per user. EGPRS is an enhancement of GPRS allowing higher bitrates on the radio interface. The higher bitrates are achieved by using a new modulation and new coding schemes in the MS and the BSS.

Three GPRS MS modes of operation are supported: An MS in class-A mode of operation operates GPRS and other GSM services simultaneously. An MS in class-B mode of operation monitors control channels for GPRS and other GSM services simultaneously, but can only operate one set of services at one time. An MS in class-C mode of operation exclusively operates GPRS services.

User data can be compressed and protected with retransmission protocols for efficiency and reliability.

GPRS security functionality is equivalent to the existing GSM security. The SGSN performs authentication and cipher setting procedures based on the same algorithms, keys, and criteria as in existing GSM. GPRS uses a ciphering algorithm optimised for packet data transmission. A GPRS ME can access the GPRS services with SIMs that are not GPRS-aware, and with GPRS-aware SIMs.

Cell selection may be performed autonomously by an MS, or the base station system instructs the MS to select a certain cell. The MS informs the network when it re-selects another cell or group of cells known as a routing area.

4.2 Main UMTS Concepts

In UMTS, radio resources are allocated to MSs in a very flexible manner. Depending on the level of activity, MSs are allocated shared contention-based radio resources or dedicated radio resources for user packet transmission.

Three UMTS MS modes of operation are supported in UMTS: The PS/CS mode of operation corresponds to class-A mode operation in GPRS. The PS mode of operation corresponds to class-C mode operation in GPRS. The CS mode of operation is the outside the scope of this specification.

UMTS security functionality is equivalent to or of higher functionality than the existing GSM/GPRS security. UMTS may use a security algorithm different from GSM/GPRS. The 3G-SGSN performs the authentication procedure, and the RNC performs the ciphering procedure based on the algorithm for UMTS.

In UMTS, different levels of mobility procedures are executed depending upon the MS state. When an MS has an active RRC connection to UTRAN, the MS performs either UTRAN Registration Area updating procedures or handover or cell update procedures depending on the level that UTRAN is tracking the MS position. When an MS does not have an active RRC connection (i.e., it is in idle mode), the MS performs RA updating procedures. In all the procedures, the cell selection is controlled by the network by setting cell selection parameters and/or restriction information.

5 General Packet Domain Architecture and Transmission Mechanism

5.1 Packet Domain Access Interfaces and Reference Points

Each PLMN has two access points, the radio interface (labelled Um in GPRS and Uu in UMTS) used for mobile access and the R reference point used for origination or reception of messages. The R reference point for the MSs is defined in UMTS 27.060 [17].

An interface differs from a reference point in that an interface is defined where specific information is exchanged and needs to be fully recognised.

There is an inter PLMN interface called Gp that connects two independent packet domain networks for message exchange.

There is also a PLMN to fixed network (typically a packet data network) reference point called Gi. Gi is defined in UMTS 29.061 [27].

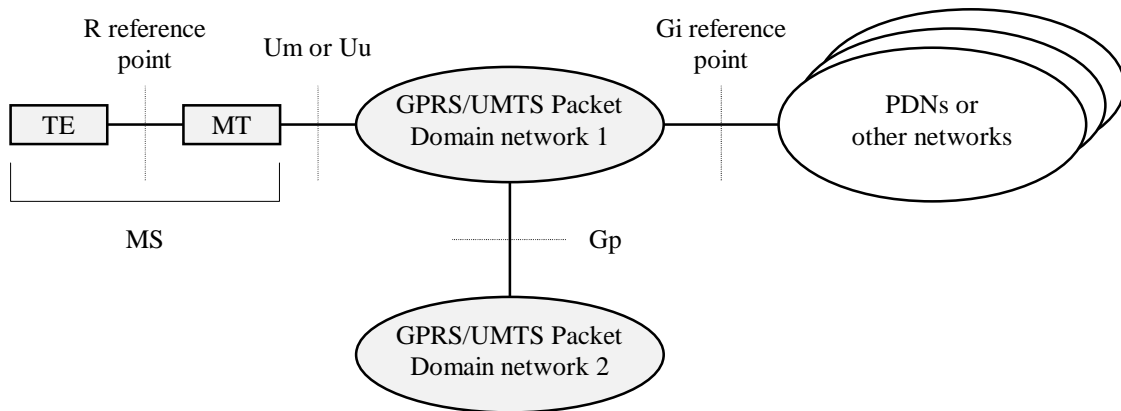


Figure 1: Packet Domain Access Interfaces and Reference Points

There may be more than a single network interface to several different packet data (or other) networks. These networks may both differ in ownership as well as in communications protocol (e.g., X.25, TCP/IP etc.). The network operator should define and negotiate interconnect with each external (PDN or other) network.

5.2 Network Interworking

Network interworking is required whenever a packet domain PLMN and any other network are involved in the execution of a service request. With reference to Figure 1, interworking takes place through the Gi reference point and the Gp interface.

The internal mechanism for conveying the PDP PDU through the PLMN is managed by the PLMN network operator and is not apparent to the data user. The use of the packet domain data service may have an impact on and increase the transfer time normally found for a message when communicated through a fixed packet data network.

5.2.1 PSPDN Interworking

The packet domain shall support interworking with PSPDN networks. The interworking may be either direct or through a transit network (e.g., ISDN). GPRS shall support both X.121 [38] and E.164 [30] addresses.

The packet domain shall provide support for X.25 virtual circuits and X.25 fast select. X.75 [37] or X.75' [48] may be used for interworking with X.25 PDNs.

The packet domain TEs have addresses provided by the packet domain service operator and belong to the packet domain. The PSPDN TE sends data to the packet domain TE by use of the packet domain PLMN DNIC (Data Network Identification Code) or equivalent that uniquely identifies the packet domain network.

5.2.2 Internet (IP) Interworking

The packet domain shall support interworking with networks based on the internet protocol (IP). IP is defined in RFC 791 [40]. The packet domain may provide compression of the TCP/IP header when an IP-datagram is used within the context of a TCP connection.

In a similar way to the PSPDN X.25 case, the packet domain PLMN service is an IP domain, and mobile terminals offered service by a service provider may be globally addressable through the network operator's addressing scheme.

5.3 High-Level Functions

The following list gives the logical functions performed within the packet domain network. Several functional groupings (meta-functions) are defined which each encompasses a number of individual functions:

- Network Access Control Functions.
- Packet Routing and Transfer Functions.
- Mobility Management Functions.
- Logical Link Management Functions (GPRS only).
- Radio Resource Management Functions.
- Network Management Functions.

5.3.1 Network Access Control Functions

Network access is the means by which a user is connected to a telecommunication network in order to use the services and/or facilities of that network. An access protocol is a defined set of procedures that enables the user to employ the services and/or facilities of the network.

User network access may occur from either the mobile side or the fixed side of the network. The fixed network interface may support multiple access protocols to external data networks, for example X.25 or IP. The set of access protocols to be supported is determined by the PLMN operator.

Individual PLMN administrations may require specific access-control procedures in order to limit the set of users permitted to access the network, or to restrict the capabilities of individual users, for example by limiting the type of service available to an individual subscriber. Such access control procedures are beyond the scope of the specifications.

In addition to the standard data transfer, the packet domain may support anonymous access to the network. The service allows an MS to exchange data packets with a predefined host that can be addressed by the supported interworking protocols. Only a limited number of destination PDP addresses can be used within this service. IMSI or IMEI shall not be used when accessing the network thus guaranteeing a high level of anonymity. Therefore, no authentication and ciphering functionalities are foreseen for anonymous access.

[It is FFS whether anonymous access shall be supported in UMTS.]

5.3.1.1 Registration Function

Registration is the means by which a user's Mobile Id is associated with the user's packet data protocol(s) and address(es) within the PLMN, and with the user's access point(s) to the external PDP network. The association can be static, i.e., stored in an HLR, or dynamic, i.e., allocated on a per need basis.

5.3.1.2 Authentication and Authorisation Function

This function performs the identification and authentication of the service requester, and the validation of the service request type to ensure that the user is authorised to use the particular network services. The authentication function is performed in association with the Mobility Management functions.

5.3.1.3 Admission Control Function

The purpose of admission control is to calculate which network resources are required to provide the quality of service (QoS) requested, determine if those resources are available, and then reserve those resources. Admission control is performed in association with the Radio Resource Management functions in order to estimate the radio resource requirements within each cell.

5.3.1.4 Message Screening Function

A screening function concerned with filtering out unauthorised or unsolicited messages is required. This should be supported through packet filtering functions.

5.3.1.5 Packet Terminal Adaptation Function

This function adapts data packets received / transmitted from / to terminal equipment to a form suitable for transmission across the packet domain network.

5.3.1.6 Charging Data Collection Function

This function collects data necessary to support subscription and/or traffic fees.

5.3.2 Packet Routeing and Transfer Functions

A route is an ordered list of nodes used for the transfer of messages within and between the PLMN(s). Each route consists of the originating node, zero or more relay nodes and the destination node. Routeing is the process of determining and using, in accordance with a set of rules, the route for transmission of a message within and between the PLMN(s).

5.3.2.1 Relay Function

The relay function is the means by which a node forwards data received from one node to the next node in the route.

5.3.2.2 Routeing Function

The routeing function determines the network node to which a message should be forwarded and the underlying service(s) used to reach that GPRS Support Node (GSN), using the destination address of the message. The routeing function selects the transmission path for the "next hop" in the route.

Data transmission between GSNS may occur across external data networks that provide their own internal routeing functions, for example X.25, Frame Relay or ATM networks.

5.3.2.3 Address Translation and Mapping Function

Address translation is the conversion of one address to another address of a different type. Address translation may be used to convert an external network protocol address into an internal network address that can be used for routeing packets within and between the PLMN(s).

Address mapping is used to map a network address to another network address of the same type for the routeing and relaying of messages within and between the PLMN(s), for example to forward packets from one network node to another.

5.3.2.4 Encapsulation Function

Encapsulation is the addition of address and control information to a data unit for routeing packets within and between the PLMN(s). Decapsulation is the removal of the addressing and control information from a packet to reveal the original data unit.

Encapsulation and decapsulation are performed between the support nodes of the packet domain PLMN(s), and between the serving support node and the MS.

5.3.2.5 Tunnelling Function

Tunnelling is the transfer of encapsulated data units within and between the PLMN(s) from the point of encapsulation to the point of decapsulation. A tunnel is a two-way point-to-point path. Only the tunnel endpoints are identified.

5.3.2.6 Compression Function

The compression function optimises use of radio path capacity by transmitting as little of the SDU (i.e., the exterior PDP PDU) as possible while at the same time as preserving the information contained within it. Only IP header compression is supported in UMTS.

5.3.2.7 Cipherring Function

The cipherring function preserves the confidentiality of user data and signalling across the radio channels and inherently protects the PLMN from intruders.

5.3.2.8 Domain Name Server Function

The Domain Name Server function resolves logical GSN names to GSN addresses. This function is standard Internet functionality according to RFC 1034 [43], which allows to resolve any name for GSNs and other nodes within the packet domain PLMN backbone networks.

5.3.3 Mobility Management Functions

The mobility management functions are used to keep track of the current location of an MS within the PLMN or within another PLMN.

5.3.4 Logical Link Management Functions for GPRS

[The UMTS signalling connection could also be considered as a logical link. Should it be describe here?]

Logical link management functions are concerned with the maintenance of a communication channel between an individual MS and the PLMN across the radio interface. These functions involve the co-ordination of link state information between the MS and the PLMN as well as the supervision of data transfer activity over the logical link.

Refer to GSM 04.64 [15] for further information.

5.3.4.1 Logical Link Establishment Function

Logical link establishment is performed when the MS attaches to the PS services.

5.3.4.2 Logical Link Maintenance Functions

Logical link maintenance functions supervise the logical link status and control link state changes.

5.3.4.3 Logical Link Release Function

The logical link release function is used to de-allocate resources associated with the logical link connection.

5.3.5 Radio Resource Management Functions

Radio resource management functions are concerned with the allocation and maintenance of radio communication paths, and is performed by the Access Network. Refer to GSM 03.64 for further information on the GSM GPRS radio. Refer to UMTS 25.301 for further information on the UMTS radio.

5.3.6 Network Management Functions

Network management functions provide mechanisms to support O&M functions related to the packet domain.

The SGSN may send location information to the MSC/VLR via the optional Gs interface. The [FFS: 2G-]SGSN may receive paging requests from the MSC/VLR via the Gs interface.

5.4.2 Packet Domain PLMN Backbone Networks

There are two kinds of backbone networks. These are called:

- intra-PLMN backbone network; and
- inter-PLMN backbone network.

The intra-PLMN backbone network is the IP network interconnecting GSNs within the same PLMN.

The inter-PLMN backbone network is the IP network interconnecting GSNs and intra-PLMN backbone networks in different PLMNs.

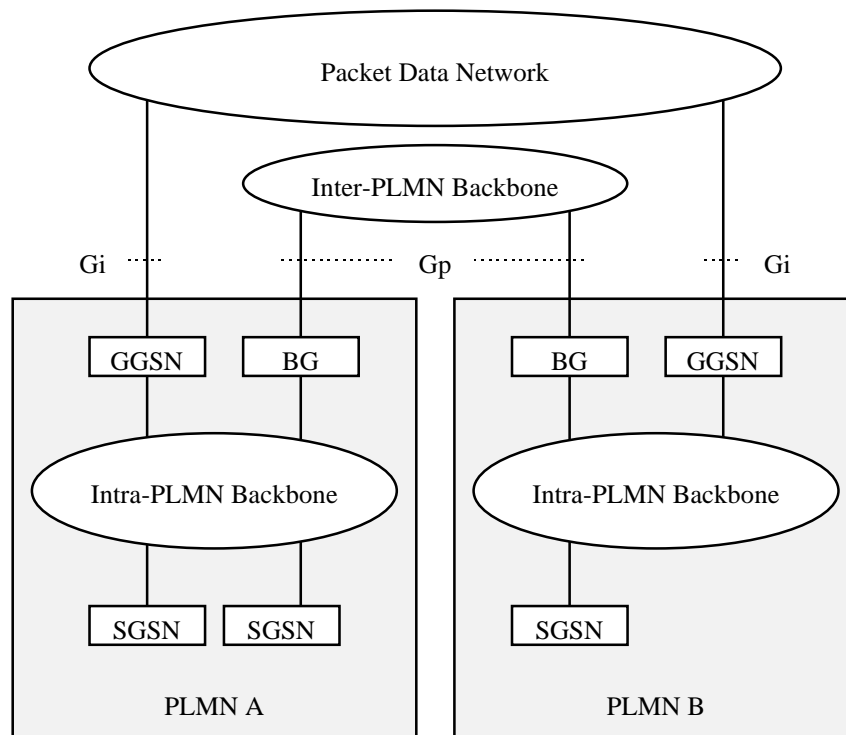


Figure 3: Intra- and Inter-PLMN Backbone Networks

Every intra-PLMN backbone network is a private IP network intended for packet domain data and signalling only. A private IP network is an IP network to which some access control mechanism is applied in order to achieve a required level of security. Two intra-PLMN backbone networks are connected via the Gp interface using Border Gateways (BGs) and an inter-PLMN backbone network. The inter-PLMN backbone network is selected by a roaming agreement that includes the BG security functionality. The BG is not defined within the scope of the packet domain. The inter-PLMN backbone can be a Packet Data Network, e.g., the public Internet or a leased line.

5.4.3 HLR

The HLR contains packet domain subscription data and routing information. The HLR is accessible from the SGSN via the Gr interface and from the GGSN via the Gc interface. For roaming MSs, HLR may be in a different PLMN than the current SGSN.

5.4.4 SMS-GMSC and SMS-IWMSC

The SMS-GMSC and SMS-IWMSC are connected to the SGSN via the Gd interface to enable the SGSN to support SMS.

5.4.5 GPRS Mobile Stations

A GPRS MS can operate in one of three modes of operation. The mode of operation depends on the services that the MS is attached to, i.e., only GPRS or both GPRS and other GSM services, and upon the MS's capabilities to operate GPRS and other GSM services simultaneously.

- Class-A mode of operation: The MS is attached to both GPRS and other GSM services, and the MS supports simultaneous operation of GPRS and other GSM services.
- Class-B mode of operation: The MS is attached to both GPRS and other GSM services, but the MS can only operate one set of services at a time. In network operation mode III (see subclause "Paging Co-ordination"), an MS that is capable of monitoring only one paging channel at a time cannot operate in class B mode of operation. In this case, such an MS shall revert to class-C mode of operation.
- Class-C mode of operation: The MS is exclusively attached to GPRS services.

NOTE: Other GSM technical specifications may refer to the MS modes of operation as GPRS class-A MS, GPRS class-B MS, and GPRS class-C MS.

5.4.6 UMTS Mobile Stations

A UMTS mobile station can operate in one of three modes of operation. However, these operation modes are different from the ones in GPRS due to the capabilities of UTRAN to multiplex CS and PS connections, due to paging co-ordination for PS services and CS services that are offered by the CN or the UTRAN (as defined in subclause "Paging Co-ordination for UMTS"), etc. The different UMTS mobile station operation modes are defined as follows:

- PS/CS mode of operation: The MS is attached to both the PS domain and CS domain, and the MS is capable of simultaneously operating PS services and CS services. This mode of operation is equivalent to the GPRS class-A mode of operation.
- PS mode of operation: The MS is attached to the PS domain only and may only operate services of the PS domain. However, this does not prevent CS-like services to be offered over the PS domain (e.g., VoIP). This mode of operation is equivalent to the GPRS class-C mode of operation.
- CS mode of operation: The MS is attached to the CS domain only and may only operate services of the CS domain. However, this does not prevent PS-like service to be offered over the CS domain. The CS mode of operation is outside the scope of this specification.

All combinations of different operation modes as described for GPRS and UMTS MSs shall be allowed for GSM/GPRS and UMTS multisystem terminals.

5.4.7 Charging Gateway Functionality

The Charging Gateway Functionality (CGF) is described in GSM 12.15 [28a].

5.5 Assignment of Functions to General Logical Architecture

The functions identified in the functional model are assigned to the logical architecture.

Table 1: Mapping of Functions to Logical Architecture

Function	2G-MS	3G-MS	BSS	UTRAN	2G-SGSN	3G-SGSN	GGSN	HLR
Network Access Control:								
Registration								X
Authentication and Authorisation	X	X			X	X		X
Admission Control	X	X	X	X	X	X		
Message Screening							X	
Packet Terminal Adaptation	X	X						
Charging Data Collection					X	X	X	
Packet Routeing & Transfer:								
Relay	X	X	X	X	X	X	X	
Routeing	X	X	X	X	X	X	X	
Address Translation and Mapping	X	X		X	X	X	X	
Encapsulation	X	X		X	X	X	X	
Tunnelling				X	X	X	X	
Compression	X	X		X	X			
Ciphering	X	X		X	X			X
Mobility Management:	X	X			X	X	X	X
Logical Link Management:								
Logical Link Establishment	X				X			
Logical Link Maintenance	X				X			
Logical Link Release	X				X			
Radio Resource Management:	X	X	X	X	X			

5.6 User and Control Planes

5.6.1 User Plane for GPRS

5.6.1.1 MS – GGSN

The user plane consists of a layered protocol structure providing user information transfer, along with associated information transfer control procedures (e.g., flow control, error detection, error correction and error recovery). The user plane independence of the Network Subsystem (NSS) platform from the underlying radio interface is preserved via the Gb interface. The following user plane is used in GPRS:

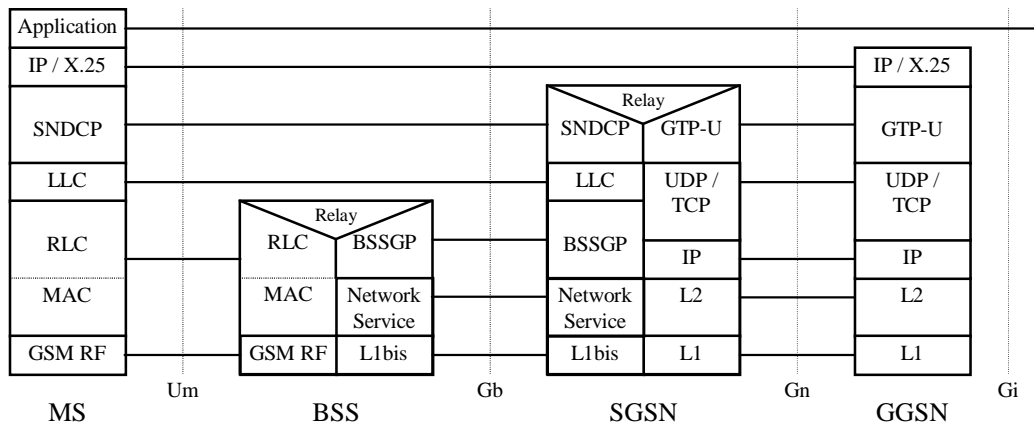


Figure 4: User Plane for GPRS

Legend:

- GPRS Tunneling Protocol for the user plane (GTP-U): This protocol tunnels user data between GPRS Support Nodes in the backbone network. All PDP PDUs shall be encapsulated by the GPRS Tunneling Protocol. GTP is specified in UMTS 29.060 [26].
- TCP carries GTP PDUs in the backbone network for protocols that need a reliable data link (e.g., X.25), and UDP carries GTP PDUs for protocols that do not need a reliable data link (e.g., IP). TCP provides flow control and protection against lost and corrupted GTP PDUs. UDP provides protection against corrupted GTP PDUs. TCP is defined in RFC 793 [42]. UDP is defined in RFC 768 [39].
- IP: This is the backbone network protocol used for routing user data and control signalling. The backbone network may initially be based on the IP version 4 protocol. Ultimately, IP version 6 shall be used. IP version 4 is defined in RFC 791.
- Subnetwork Dependent Convergence Protocol (SNDCP): This transmission functionality maps network-level characteristics onto the characteristics of the underlying network. SNDCP is specified in GSM 04.65 [16].
- Logical Link Control (LLC): This layer provides a highly reliable ciphered logical link. LLC shall be independent of the underlying radio interface protocols in order to allow introduction of alternative GPRS radio solutions with minimum changes to the NSS. LLC is specified in GSM 04.64.
- Relay: In the BSS, this function relays LLC PDUs between the Um and Gb interfaces. In the SGSN, this function relays PDP PDUs between the Gb and Gn interfaces.
- Base Station System GPRS Protocol (BSSGP): This layer conveys routing- and QoS-related information between BSS and SGSN. BSSGP does not perform error correction. BSSGP is specified in GSM 08.18 [21].
- Network Service (NS): This layer transports BSSGP PDUs. NS is based on the Frame Relay connection between BSS and SGSN, and may be multi-hop and traverse a network of Frame Relay switching nodes. NS is specified in GSM 08.16 [20].
- RLC/MAC: This layer contains two functions: The Radio Link Control function provides a radio-solution-dependent reliable link. The Medium Access Control function controls the access signalling (request and grant)

procedures for the radio channel, and the mapping of LLC frames onto the GSM physical channel. RLC/MAC is defined in GSM 04.60 [14].

- GSM RF: As defined in GSM 05 series.

5.6.1.2 GSN – GSN

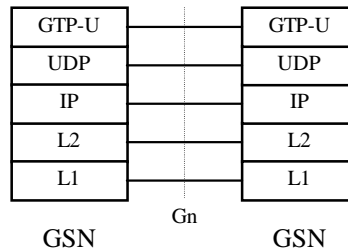


Figure 5: User Plane GSN - GSN

Legend:

- GPRS Tunnelling Protocol for the user plane (GTP-U): This protocol tunnels user data between SGSNs and GGSNs, and between SGSNs, in the backbone network.
- User Datagram Protocol (UDP): This protocol transfers user data between GSNs. UDP is defined in RFC 768.

5.6.2 User Plane for UMTS

5.6.2.1 MS – GGSN

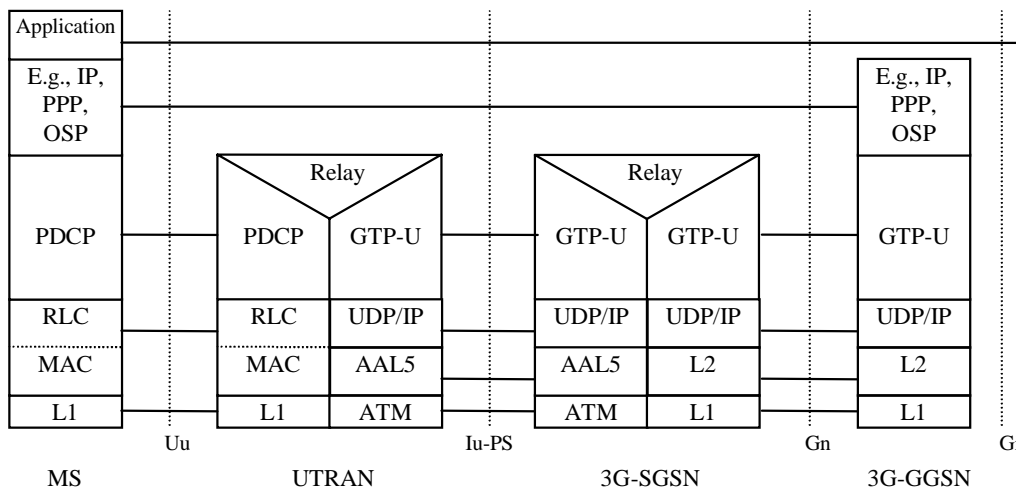


Figure 6: User Plane for UMTS

Legend:

- Packet Data Convergence Protocol (PDCP): This transmission functionality maps higher-level characteristics onto the characteristics of the underlying radio-interface protocols. PDCP provides protocol transparency for higher-layer protocols. PDCP supports e.g., IPv4, PPP, OSP, and IPv6. Introduction of new higher-layer protocols shall be possible without any changes to the radio-interface protocols. PDCP provides protocol control information compression. PDCP is specified in UMTS 25.323.

NOTE: Unlike in GPRS, user data compression is not supported in UMTS, because the data compression efficiency depends on the type of user data, and because many applications compress data before transmission. It is difficult to check the type of data in the PDCP layer, and compressing all user data requires too much processing.

- GPRS Tunnelling Protocol for the user plane (GTP-U): This protocol tunnels user data between UTRAN and the 3G-SGSN, and between the GSNs in the backbone network. All PDP PDUs shall be encapsulated by GTP. GTP is specified in UMTS 29.060.
- UDP/IP: These are the backbone network protocols used for routeing user data and control signalling.
- Radio Link Control (RLC): The RLC protocol provides logical link control over the radio interface. There may be several simultaneous RLC links per MS. Each link is identified by a Bearer Id. RLC is defined in UMTS 25.322.

[Add text for ATM and MAC.]

5.6.2.2 GSN – GSN

This user plane is the same as for GPRS, see subclause "GSN – GSN" above.

5.6.3 Control Plane

The control plane consists of protocols for control and support of the user plane functions:

- controlling the packet domain network access connections, such as attaching to and detaching from the packet domain network;
- controlling the attributes of an established network access connection, such as activation of a PDP address;
- controlling the routeing path of an established network connection in order to support user mobility; and
- controlling the assignment of network resources to meet changing user demands.

The following control planes are used in both GPRS and UMTS unless specifically indicated:

5.6.3.1 MS – SGSN for GPRS

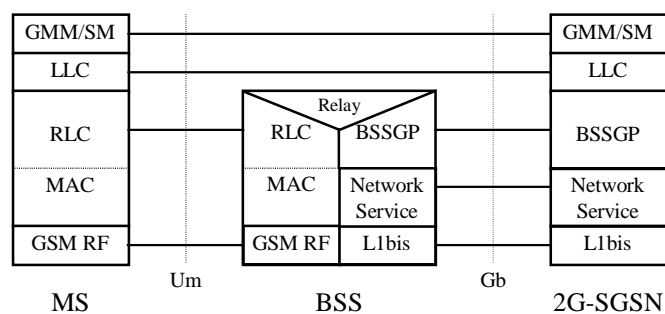


Figure 7: Control Plane MS – 2G-SGSN

Legend:

- GPRS Mobility Management and Session Management (GMM/SM): This protocol supports mobility management functionality such as GPRS attach, GPRS detach, security, routeing area update, location update, PDP context activation, and PDP context deactivation, as described in clauses "Mobility Management Functionality" and "PDP Context Activation, Modification, and Deactivation Functions".

5.6.3.2 MS – SGSN for UMTS

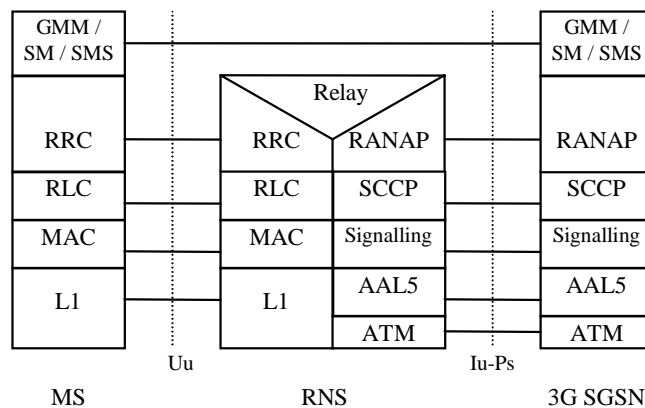


Figure 8: Control Plane MS - 3G-SGSN

Legend:

- UMTS Mobility Management and Session Management (GMM/SM): GMM supports mobility management functionality such as attach, detach, security, and routing area update, as described in clause "Mobility Management Functionality". SM supports PDP context activation and PDP context deactivation, as described in subclause "PDP Context Activation, Modification, and Deactivation Functions".
- SMS supports the mobile-originated and mobile-terminated short message service described in UMTS 23.040.
- Radio Access Network Application Protocol (RANAP): This protocol encapsulates and carries higher-layer signalling, handles signalling between the 3G-SGSN and UTRAN, and manages the GTP connections on the Iu interface. RANAP is specified in UMTS 25.413. The layers below RANAP are defined in UMTS 23.121.
- Radio Link Control (RLC): The RLC protocol offers logical link control over the radio interface for the transmission of higher layer-signalling messages and SMS. RLC is defined in UMTS 25.322.

5.6.3.3 SGSN - HLR

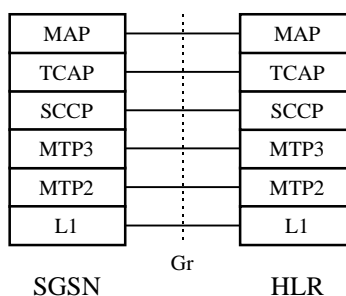


Figure 9: Control Plane SGSN - HLR

Legend:

- Mobile Application Part (MAP): This protocol supports signalling exchange with the HLR, as defined in UMTS 29.002 [23], with enhancements for GPRS as described in the present document.
- TCAP, SCCP, MTP3, and MTP2 are the same protocols as used to support MAP in CS PLMNs.

5.6.3.4 SGSN - MSC/VLR

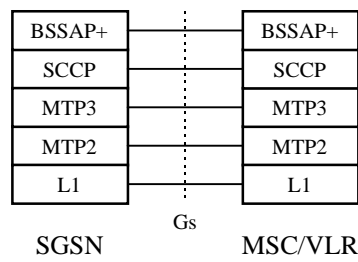


Figure 10: Control Plane SGSN - MSC/VLR

Legend:

- Base Station System Application Part + (BSSAP+): A subset of BSSAP procedures supports signalling between the SGSN and MSC/VLR, as described in subclause "Mobility Management Functionality" and in UMTS 29.018 [25]. The requirements for the lower layers are specified in UMTS 29.016 [24].

5.6.3.5 SGSN - EIR

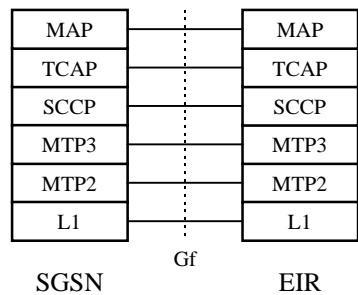


Figure 9: Control Plane SGSN - EIR

Legend:

- Mobile Application Part (MAP): This protocol supports signalling between the SGSN and the EIR, as described in subclause "Identity Check Procedures".

5.6.3.6 SGSN - SMS-GMSC or SMS-IW MSC

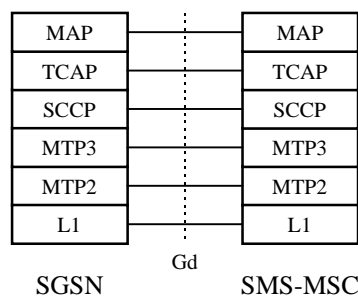


Figure 11: Control Plane SGSN - SMS-GMSC and SGSN - SMS-IW MSC

Legend:

- Mobile Application Part (MAP): This protocol supports signalling between the SGSN and SMS-GMSC or SMS-IW MSC, as described in subclause "Point-to-point Short Message Service".

5.6.3.7 GSN - GSN

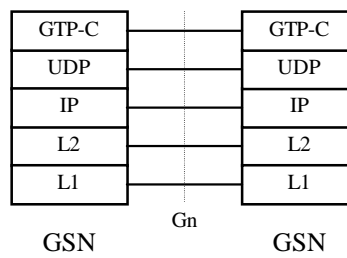


Figure 12: Control Plane GSN - GSN

Legend:

- GPRS Tunnelling Protocol for the control plane (GTP-C): This protocol tunnels signalling messages between SGSNs and GGSNs, and between SGSNs, in the backbone network.
- User Datagram Protocol (UDP): This protocol transfers signalling messages between GSNs. UDP is defined in RFC 768.

5.6.3.8 GGSN - HLR

This optional signalling path allows a GGSN to exchange signalling information with an HLR. There are two alternative ways to implement this signalling path:

- If a SS7 interface is installed in the GGSN, the MAP protocol can be used between the GGSN and an HLR.
- If a SS7 interface is not installed in the GGSN, any GSN with a SS7 interface installed in the same PLMN as the GGSN can be used as a GTP-to-MAP protocol converter to allow signalling between the GGSN and an HLR.

5.6.3.8.1 MAP-based GGSN - HLR Signalling

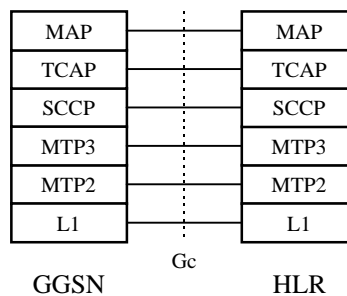


Figure 13: Control Plane GGSN - HLR Using MAP

Legend:

- Mobile Application Part (MAP): This protocol supports signalling exchange with the HLR, as described in subclause "Network-Requested PDP Context Activation Procedure".

5.6.3.8.2 GTP and MAP-based GGSN - HLR Signalling

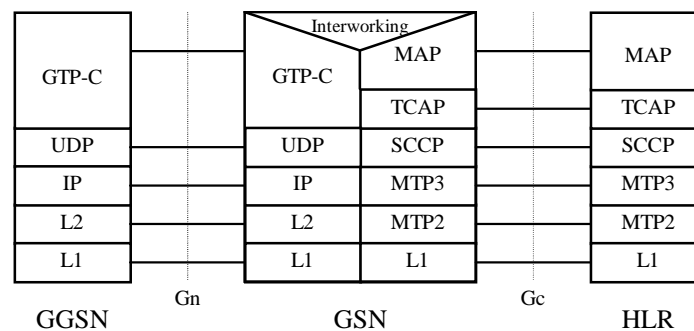


Figure 14: Control Plane GGSN - HLR Using GTP and MAP

Legend:

- GPRS Tunnelling Protocol for the control plane (GTP-C): This protocol tunnels signalling messages between the GGSN and the protocol-converting GSN in the backbone network.
- Interworking: This function provides interworking between GTP and MAP for GGSN - HLR signalling.

6 Mobility Management Functionality

6.1 Definition of Mobility Management States

The Mobility Management (MM) activities related to a subscriber are characterised by one of three different MM states. The MM states for a GPRS subscriber are IDLE, STANDBY, and READY, and the MM states for a UMTS subscriber are PMM-DETACHED, PMM-IDLE, and PMM-CONNECTED. Each state describes a certain level of functionality and information allocated. The information sets held at the MS and the SGSN are denoted MM context.

In the non-anonymous access case, the MM state relates only to GPRS MM activities of a subscriber. The MM state is independent of the number and state of PDP contexts for that subscriber.

In the anonymous access case, the MM state relates to GPRS MM activities of an MS represented only by an Auxiliary TLLI.

6.1.1 Mobility Management States for GPRS

6.1.1.1 IDLE (GPRS) State

In GPRS IDLE state, the subscriber is not attached to the GPRS mobility management. The MS and SGSN contexts hold no valid location or routing information for the subscriber. The subscriber-related mobility management procedures are not performed.

PLMN selection and GPRS cell selection and re-selection processes are performed by the MS.

Data transmission to and from the mobile subscriber as well as the paging of the subscriber are not possible. The GPRS MS is seen as not reachable in this case.

In order to establish MM contexts in the MS and the SGSN, the MS shall perform the GPRS Attach procedure.

6.1.1.2 STANDBY State

In STANDBY state, the subscriber is attached to GPRS mobility management. The MS and SGSN have established MM contexts as described in clause "Information Storage".

Pages for data or signalling information transfers may be received. It is also possible to receive pages for the CS services via the SGSN. Data reception and transmission are not possible in this state.

The MS performs GPRS Routing Area (RA) and GPRS cell selection and re-selection locally. The MS executes mobility management procedures to inform the SGSN when it has entered a new RA. The MS does not inform the SGSN on a change of cell in the same RA. Therefore, the location information in the SGSN MM context contains only the GPRS RAI for MSs in STANDBY state.

The MS may initiate activation or deactivation of PDP contexts while in STANDBY state. A PDP context shall be activated before data can be transmitted or received for this PDP context.

The SGSN may have to send data or signalling information to an MS in STANDBY state. The SGSN then sends a Paging Request in the routing area where the MS is located if PPF is set. If PPF is cleared, then paging is not done. The MM state in the MS is changed to READY when the MS responds to the page, and in the SGSN when the page response is received. Also, the MM state in the MS is changed to READY when data or signalling information is sent from the MS and, accordingly, the MM state in the SGSN is changed to READY when data or signalling information is received from the MS.

The MS or the network may initiate the GPRS Detach procedure to move to the IDLE state. After expiry of the mobile reachable timer the SGSN may perform an implicit detach in order to return the MM contexts in the SGSN to IDLE state. The MM and PDP contexts may then be deleted.

6.1.1.3 READY State

In READY state, the SGSN MM context corresponds to the STANDBY MM context extended by location information for the subscriber on cell level. The MS performs mobility management procedures to provide the network with the actual selected cell. GPRS cell selection and re-selection is done locally by the MS, or may optionally be controlled by the network.

An identifier of the cell, the Cell Global Identity including RAC and LAC, is included in the BSSGP header of the data packet from the MS, see GSM 08.18.

The MS may send and receive PDP PDUs in this state. The network initiates no GPRS pages for an MS in READY state, pages for other services may be done via the SGSN. The SGSN transfers downlink data to the BSS responsible for the subscriber's actual GPRS cell.

The MS may activate or deactivate PDP contexts while in READY state.

Regardless if a radio resource is allocated to the subscriber or not, the MM context remains in the READY state even when there is no data being communicated. The READY state is supervised by a timer. An MM context moves from READY state to STANDBY state when the READY timer expires. In order to move from READY state to IDLE state, the MS initiates the GPRS Detach procedure.

6.1.1.4 State Transitions and Functions

The movement from one state to the next is dependent on the current state (IDLE, STANDBY, or READY) and the event occurred (e.g., GPRS attach).

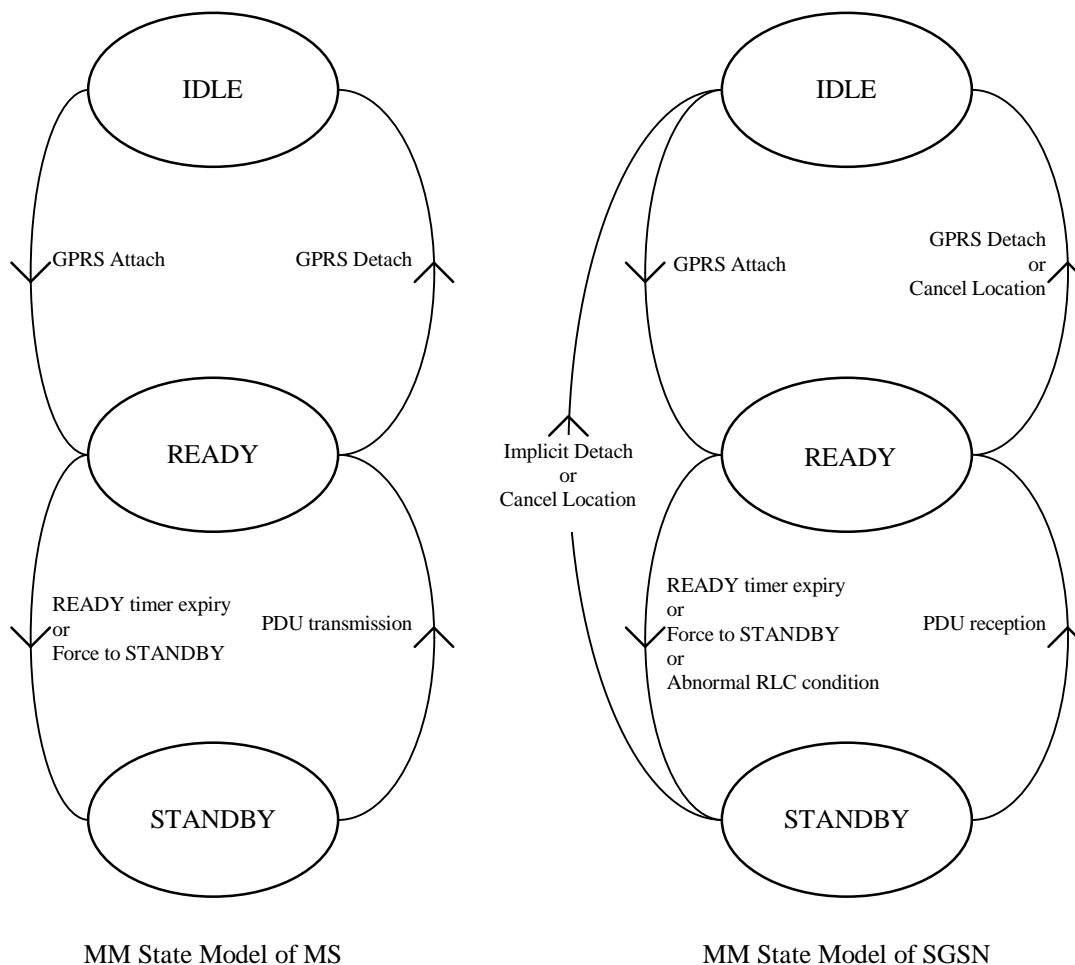


Figure 15: Functional Mobility Management State Model

Figure 15 describes the following state transitions:

Moving from IDLE to READY:

- GPRS Attach: The MS requests access and a logical link to an SGSN is initiated. MM contexts are established at the MS and SGSN.

Moving from STANDBY to IDLE:

- Implicit Detach: The MM and PDP contexts in the SGSN shall return to IDLE and INACTIVE state. The MM and PDP contexts in the SGSN may be deleted. The GGSN PDP contexts shall be deleted.
- Cancel Location: The SGSN receives a MAP Cancel Location message from the HLR, and removes the MM and PDP contexts.

Moving from STANDBY to READY:

- PDU transmission: The MS sends an LLC PDU to the SGSN, possibly in response to a page.
- PDU reception: The SGSN receives an LLC PDU from the MS.

Moving from READY to STANDBY:

- READY timer expiry: The MS and the SGSN MM contexts return to STANDBY state.

- Force to STANDBY: The SGSN indicates an immediate return to STANDBY state before the READY timer expires.
- Abnormal RLC condition: The SGSN MM context returns to STANDBY state in case of delivery problems on the radio interface or in case of irrecoverable disruption of a radio transmission.

Moving from READY to IDLE:

- GPRS Detach: The MS or the network requests that the MM contexts return to IDLE state and that the PDP contexts return to INACTIVE state. The SGSN may delete the MM and PDP contexts. The PDP contexts in the GGSN shall be deleted.
- Cancel Location: The SGSN receives a MAP Cancel Location message from the HLR, and removes the MM and PDP contexts.

For anonymous access, a reduced Mobility Management State Model consisting of IDLE and READY states is used. The AA MM state machine is independently handled by the MS and the network and may coexist with an IMSI-based MM state machine. Several AA MM state machines may coexist in the same MS and SGSN simultaneously.

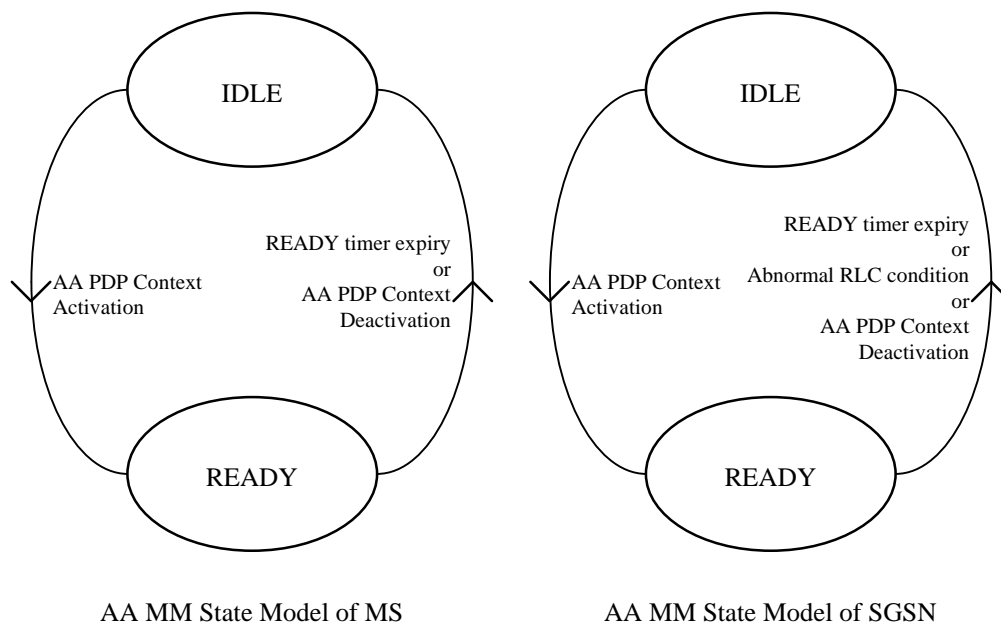


Figure 16: Functional Anonymous Access Mobility Management State Model

Figure 16 describes the following state transitions for anonymous access:

Moving from IDLE to READY:

- AA PDP Context Activation: The MS requests an anonymous access and a logical link to an SGSN is initiated. MM contexts are established at the MS and SGSN, and PDP contexts are established at the MS, the SGSN, and a GGSN.

Moving from READY to IDLE:

- READY timer expiry: The MM and PDP contexts in the MS, the SGSN, and the GGSN are deleted.
- Abnormal RLC condition: The SGSN MM context shall be deleted in case of delivery problems on the radio interface or in case of irrecoverable disruption of a radio transmission.
- AA PDP Context Deactivation: The network (either the SGSN or the GGSN) initiates the AA PDP Context Deactivation procedure, e.g., due to malicious usage of the anonymous service. The MM and PDP contexts in the MS, the SGSN, and the GGSN shall be deleted.

6.1.2 Mobility Management States for UMTS

6.1.2.1 PMM-DETACHED State

In the PMM-DETACHED state there is no communication between the MS and the 3G-SGSN. The MS and SGSN contexts hold no valid location or routing information for the MS. The MS MM state machine does not react on system information related to the 3G-SGSN. The MS is not reachable by a 3G-SGSN, as the MS location is not known.

In order to establish MM contexts in the MS and the SGSN, the MS shall perform the PS Attach procedure. When the PS signalling connection is established between the MS and the 3G-SGSN for performing the PS attach, the state changes to PMM-CONNECTED in the 3G-SGSN and in the MS. The PS signalling connection is made up of two parts; an RRC connection and an Iu connection.

6.1.2.2 PMM-IDLE State

The MS location is known in the 3G-SGSN with an accuracy of a routing area. Paging is needed in order to reach the MS, e.g., for signalling. The MS and SGSN have established MM contexts as described in clause "Information Storage".

The MS shall perform a routing area update if the RA changes. Signalling towards the HLR is needed if the 3G-SGSN does not have an MM context for this MS.

The MS and 3G-SGSN shall enter the PMM-CONNECTED state when the PS signalling connection is established between the MS and the 3G-SGSN.

PS detach changes the state to PMM-DETACHED. The 3G-SGSN may perform an implicit PS detach any time after the MS reachable timer expiry. The MS's MM context is deleted, preferably after a certain (implementation dependent) time. The HLR may be informed about the deletion (see subclause "Purge Function").

6.1.2.3 PMM-CONNECTED State

The MS location is known in the 3G-SGSN with an accuracy of a serving RNC. In the PMM-CONNECTED state, the location of the MS is tracked by the serving RNC. The MS performs the routing area update procedure when RAI in the MM system information changes.

When an MS and a 3G-SGSN are in the PMM-CONNECTED state, a PS signalling connection is established between the MS and the 3G-SGSN.

In the 3G-SGSN, PS signalling connection release or failed downlink transfer with cause "IMSI unknown in RNC" changes the state to PMM-IDLE.

The MS shall enter the PMM-IDLE state when its PS signalling connection to the 3G-SGSN has been released or broken. This release or failure is explicitly indicated by the RNC to the MS or detected by the MS (RRC connection failure). The radio connection shall also be released if a URA update fails because of "RRC connection not established", or if the URA update timer expires while the MS is out of coverage.

After a signalling procedure (e.g., routing area update), the 3G-SGSN may decide to release the PS signalling connection, after which the state is changed to PMM-IDLE.

PS detach changes the state to PMM-DETACHED.

6.1.2.4 State Transitions and Functions

The figure below introduces the MM states for a UMTS subscriber (PMM). The states and activations are further described below.

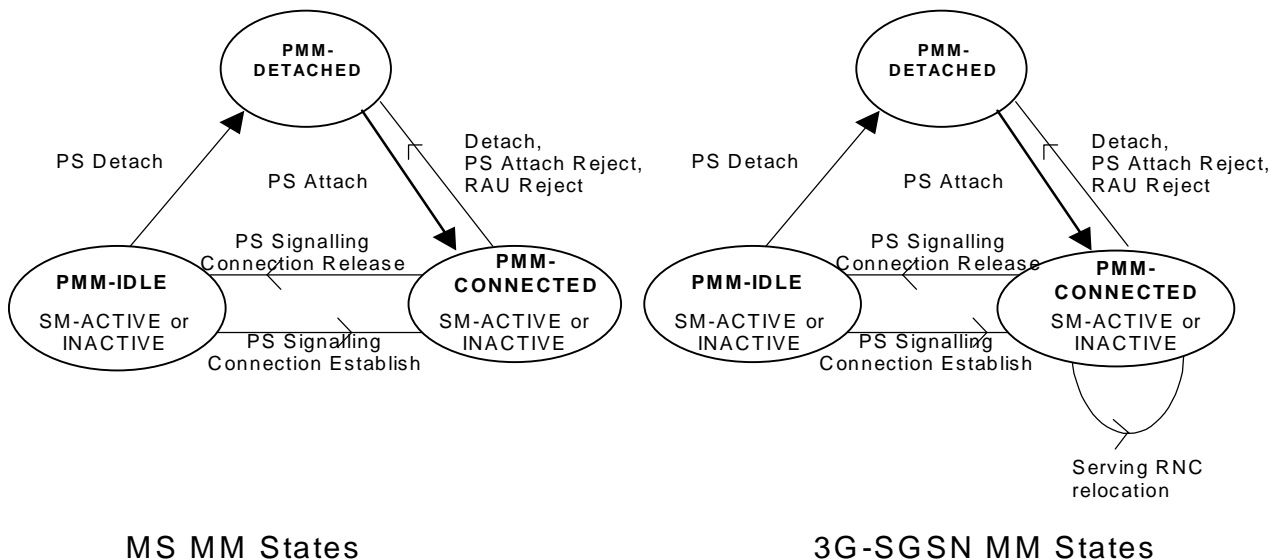


Figure 17: PMM State Model

NOTE: In both the PMM-IDLE and the PMM-CONNECTED states, session management may or may not have activated a PDP context. The consequence is that in PMM-CONNECTED state, only a signalling connection may be established. In PMM-IDLE state, a PDP context may be established, but no corresponding connection over the Iu interface nor the radio are established.

Moving from PMM-DETACHED to PMM-CONNECTED in the MS:

- PS Attach: The MM context shall move to the PMM-CONNECTED state when a PS signalling connection is established between the MS and the 3G-SGSN for performing a PS attach. If the PS attach is accepted an MM context is created in MS.

Moving from PMM-CONNECTED to PMM-DETACHED in the MS:

- PS Detach: The MM context shall move to the PMM-DETACHED state when the PS signalling connection is released between the MS and the 3G-SGSN after the MS has performed a PS detach or after the network-initiated PS detach is performed. The MM context in the MS may be deleted.
- RAU Reject: The MM context shall move to the PMM-DETACHED state when the PS signalling connection is released between the MS and the 3G-SGSN after a RAU is rejected by the 3G-SGSN. The MM context may be deleted.
- PS Attach Reject: The MM context shall move to the PMM-DETACHED state when the PS signalling connection is released between the MS and the 3G-SGSN after a PS attach is rejected by the 3G-SGSN. The MM context may be deleted.

Moving from PMM-CONNECTED to PMM-IDLE in the MS:

- PS Signalling Connection Release: The MM context shall move to the PMM-IDLE state when the PS signalling connection is released.

Moving from PMM-IDLE to PMM-CONNECTED in the MS:

- PS Signalling Connection Establishment: The MM context shall move to the PMM-CONNECTED state when the PS signalling connection is established between the MS and the 3G-SGSN.

Moving from PMM-IDLE to PMM-DETACHED in the MS:

- Implicit PS Detach: The MM context shall locally move to the PMM-DETACHED state, e.g., in the case of removal of the battery, the USIM, or the GSIM from the TE.

Moving from PMM-DETACHED to PMM-CONNECTED in the 3G-SGSN:

- PS Attach: The MM context shall move to the PMM-CONNECTED state when a PS signalling connection is established between the MS and 3G-SGSN for performing a PS attach. If the PS attach is accepted, an MM context is created in 3G-SGSN.

Moving from PMM-CONNECTED to PMM-DETACHED in the 3G-SGSN:

- PS Detach: The MM context shall move to the PMM-DETACHED state when the PS signalling connection is released between the MS and the 3G-SGSN after the MS has performed a PS detach or after the network-initiated PS detach is performed. The MM context in the 3G-SGSN may be deleted.
- RAU Reject: The MM context shall move to the PMM-DETACHED state when the PS signalling connection is released between the MS and the 3G-SGSN after a RAU is rejected.
- PS Attach Reject: The MM context shall move to the PMM-DETACHED state when a PS signalling connection is released between the MS and the 3G-SGSN after a PS attach is rejected by the 3G-SGSN.

Moving from PMM-CONNECTED to PMM-IDLE in the 3G-SGSN:

- PS Signaling Connection Release: The MM context shall move to the PMM-IDLE state when the PS signalling connection is released.

Moving from PMM-IDLE to PMM-CONNECTED in the 3G-SGSN:

- PS Signaling Connection Establishment: The MM context shall move to the PMM-CONNECTED state when the PS signalling connection is established.

Moving from PMM-IDLE to PMM-DETACHED in the 3G-SGSN:

- Implicit PS Detach: The MM context may locally move to the PMM-DETACHED state after expiry of the MS Reachable timer. The MM and PDP context(s) in the 3G-SGSN may be deleted, preferably after an implementation-dependent time.

6.1.2.4.1 Error Cases

In case of an error, the PMM state of the MS and the 3G-SGSN may lose synchronisation. In this case the MS may be in the PMM-IDLE state while the 3G-SGSN is in the PMM-CONNECTED state.

NOTE: The opposite (MS in the PMM-CONNECTED state and SGSN in the PMM-IDLE state) shall never happen because the 3G-SGSN may not have the RAI where the MS is really located, so downlink transfer is impossible until the periodic URA update timer expires.

This situation is recovered by a successful RAU moving the MS to the PMM-CONNECTED state, or by a failed downlink transfer with cause "IMSI unknown in RNC", triggering a paging procedure from the 3G-SGSN.

NOTE: An RNC shall not release the Iu connection if it could not inform the MS that the radio connection was released.

6.2 Mobility Management Timer Functions

6.2.1 READY Timer Function for GPRS

The READY timer function maintains the READY timer in the MS and SGSN. The READY timer controls the time an MS remains in READY state in the MS and the SGSN. The READY timer shall be reset and begin running in the MS when an LLC PDU is transmitted, and in the SGSN when an LLC PDU is correctly received. When the READY timer expires, the MS and SGSN MM contexts shall return to STANDBY state. In case of anonymous access the MM context shall be deleted.

The length of the READY timer shall be the same in the MS and SGSN. The initial length of the READY timer shall be defined by a default value. The SGSN, and only the SGSN, may change the length of the READY timer by transmitting a new value in the Attach Accept, Routing Area Update Accept, or AA PDP Context Accept messages.

If the READY timer length is set to zero, the MS shall immediately be forced into STANDBY state. If the timer length is set to all 1s (binary), then the READY timer function shall be deactivated, i.e., the timer no longer runs and the MS remains in READY state.

6.2.2 Periodic RA Update Timer Function

The Periodic RA Update Timer function monitors the periodic RA update procedure in the MS. The length of the periodic RA update timer is sent in the Routing Area Update Accept or Attach Accept message. The periodic RA update timer is unique within an RA. Upon expiry of the periodic RA update timer, the MS shall start a periodic routing area update procedure.

NOTE: An MS is said to be in packet domain coverage if it can access packet domain services. These services may be provided by GPRS or by UMTS.

If the MS is in coverage but out of packet domain coverage when the periodic RA update timer expires, then, if the MS is CS-attached to a network in network operation mode I, the periodic location update procedure (or other appropriate location update procedure) shall be started immediately. In addition, and irrespective of whether or not the MS was CS-attached, regardless of the network operation mode, the periodic RA update procedure (or other appropriate update procedure) shall be started as soon as the MS returns to packet domain coverage.

If the MS is out of coverage when the periodic RA update timer expires then:

- if the MS is both CS and PS-attached and returns to coverage in a cell that supports packet-domain services in network operation mode I, then the combined RA / LA update procedure with CS attach requested shall be started as soon as the MS returns to coverage;
- if the MS is both CS- and PS-attached and returns to coverage in a cell that supports packet-domain services in network operation mode II or III, or if a PS only-attached MS returns to coverage in a cell that supports packet-domain services, then the periodic RA update procedure shall be started as soon as the MS returns to coverage; or
- if the MS returns to coverage in a cell that does not support packet-domain services, and if the MS is CS-attached, then the periodic location update procedure (or other appropriate location update procedure) shall be started as soon as the MS returns to coverage in that cell. In addition, and irrespective of whether or not the MS was CS-attached, the periodic RA update procedure (or other appropriate update procedure) shall be started as soon as the MS returns to packet-domain coverage.

If the MS lost packet-domain coverage but the periodic RA update timer did not expire while out of packet-domain coverage, then, the MS shall not perform the periodic RA update procedure because of the MS's return to packet-domain coverage.

If the MS lost coverage but the periodic RA update timer did not expire while out of coverage, then the MS shall not perform the periodic RA update procedure because of the MS's return to coverage.

6.2.3 Mobile Reachable Timer Function

The Mobile Reachable Timer function monitors the periodic RA update procedure in the SGSN. The mobile reachable timer shall be slightly longer than the periodic RA update timer used by an MS.

The mobile reachable timer is stopped when the READY state or PMM-CONNECTED state is entered. The mobile reachable timer is reset and started when the state returns to STANDBY or PMM-IDLE.

If the mobile reachable timer expires, the SGSN shall clear PPF. Typically, in GPRS, this causes the SGSN to stop sending GPRS paging or CS paging messages to the MS, but other features (e.g., MSC/VLR-based call forwarding) may happen immediately. PPF is set when the next activity from the MS is detected. The MM and PDP contexts shall be kept in the SGSN.

When an MS first registers in an SGSN, then PPF is set.

6.3 Interactions Between SGSN and MSC/VLR

The interactions described in this subclause shall be supported if the optional Gs interface is installed.

An association is created between SGSN and MSC/VLR to provide for interactions between SGSN and MSC/VLR. The association is created when the VLR stores the SGSN number and the SGSN stores the VLR number. The association is used for co-ordinating MSs that are both PS-attached and CS-attached.

The association supports the following actions:

- IMSI attach and detach via SGSN. This makes combined PS / CS attach and combined PS / CS detach possible, thus saving radio resources.
- Co-ordination of LA update and RA update, including periodic updates, thus saving radio resources. A combined RA / LA update is sent from the MS to the SGSN. SGSN forwards the LA update to the VLR.
- Paging for a CS connection via the SGSN.
- Alert procedures for non-PS services.
- Identification procedure.
- MM Information procedure.

6.3.1 Administration of the SGSN - MSC/VLR Association

The SGSN - MSC/VLR association is created at the following occasions:

- Combined CS / PS attach.
- GPRS attach when the MS is already CS-attached.
- Combined RA / LA update when the MS performs CS attach and is already PS-attached.

Combined RA / LA update when an CS and PS-attached MS changes from an area of network operation mode II or III to an area of network operation mode I.

The association is initiated by the SGSN. The SGSN creates an association by sending a BSSAP+ message concerning a particular MS to the VLR. To get the VLR number, the SGSN translates the current RAI to a VLR number via a translation table. During a CS connection, an MS in class-B mode of operation (GPRS only) cannot perform PS attach nor routeing area updates, only MSs in class-A mode of operation can perform these procedures. If a PS attach was made during a CS connection, the association shall be initiated by a combined RA / LA update after the CS connection has been released.

The association is updated on the following occasions:

- When an MS changes VLR.
- When an MS changes SGSN.

The association is not updated during a CS connection.

When the MS is in idle mode (see GSM 03.22), the association is updated with the combined RA / LA updates procedure.

In relation with a CS connection, the association is managed in the following way:

MS in class-A or CS/PS mode of operation:

An MS in class-A or CS/PS mode of operation makes RA updates but no combined RA / LA updates during the CS connection. In the case when the MS changes SGSN, the SGSN (according to normal RA update procedures, see subclause "Inter SGSN Routeing Area Update") updates the HLR and the GGSN, but not the VLR, about the new SGSN number.

In the case when the MS changes MSC during the CS connection, the subscriber data still remains in the old VLR until the CS connection is released and a combined RA / LA update or LA update is made. The association is also not updated during the CS connection.

After the CS connection has been released, a combined RA / LA update is performed (if there has been a change of RA, or if a PS attach was performed and the new cell indicates network operation mode I), and the association is updated according to combined RA / LA update procedures, see subclause "Combined RA / LA Update Procedure". If the new cell indicates network operation mode II or III, then the MS performs an LA update.

MS in class-B mode of operation (GPRS only):

An MS in class-B mode of operation does not make any RA updates during a CS connection. The SGSN number therefore remains the same during the CS connection and needs not be updated in the VLR. In the case when the MS changes MSC during the CS connection, the subscriber data still remains in the old VLR until the CS connection has been released and a combined RA / LA update or LA update is made. Therefore, the VLR number remains the same during the CS connection. After the CS connection has been released, the MS shall perform an RA update and an LA update if the RA has changed and the new cell indicates network operation mode II or III, or a combined RA / LA update if the RA has changed and the new cell indicates network operation mode I. The association is updated according to the combined RA / LA update procedures, see subclauses "Inter SGSN Routeing Area Update" and "Combined RA / LA Update Procedure".

The SGSN - MSC/VLR association is removed at the following occasions:

- At IMSI detach.
- At GPRS detach.

When the MSC/VLR receives an LA update via the A or Iu interface from an MS for which an association exists, then the MSC/VLR shall remove the association without notifying the SGSN. When the SGSN receives a (non-combined) RA update from an MS for which an association exists, then the SGSN shall remove the association without notifying the MSC/VLR. When the MSC/VLR receives a BSSAP+ MS Unreachable message from the SGSN indicating that PPF is cleared, then the state of the association shall not be changed at the MSC/VLR.

6.3.2 Combined RA / LA Updating

When the MS is both CS and PS-attached, the LA and RA updating is done in a co-ordinated way to save radio resources if supported by the network operation mode. When the MS enters a new RA in network operation mode I, then the MS sends a Routeing Area Update Request message to the SGSN, as described in subclause "Combined RA / LA Update Procedure". The LA update is included in the RA update. The SGSN then forwards the LA update to the MSC/VLR. The MSC/VLR optionally returns a new VLR TMSI that is sent to the MS via the SGSN.

An MS in class-A mode of operation involved in a CS connection makes only RA updates and no combined RA / LA updates to the SGSN.

An MS in class-B mode of operation involved in a CS connection does not make any updates during the CS connection.

An MS in class-C mode of operation never makes combined RA / LA updates.

6.3.3 CS Paging for GPRS

When an MS is both IMSI and GPRS-attached in a network that operates in mode I, then the MSC/VLR executes paging for circuit-switched services via the SGSN. If the MS is in STANDBY state, then it is paged in the routeing area and in the null routeing area (see subclause "Routeing Area Identity"). If the MS is in READY state, then it is paged in the cell. The paging procedure is supervised in the MSC by a paging timer. The SGSN converts the MSC paging message into an SGSN paging message.

The CS Paging procedure is illustrated in Figure 18. Each step is explained in the following list.

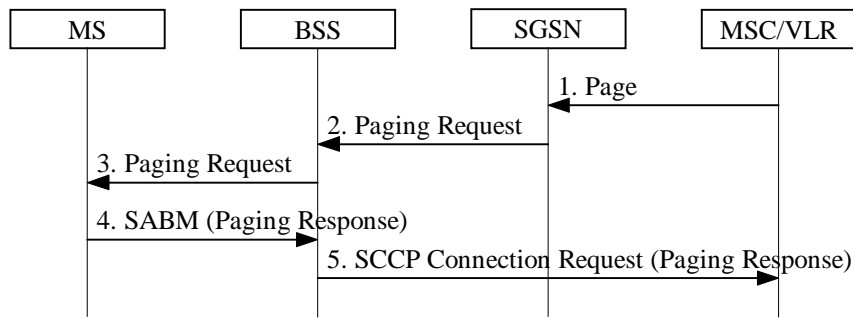


Figure 18: CS Paging Procedure

- 1) The SGSN receives a Page (IMSI, VLR TMSI, Channel Needed, Priority, Location Information) message from the MSC. Channel Needed is defined in GSM 08.08 [18] and indicates to the MS which type of CS channel is needed to be requested in the response. VLR TMSI and Channel Needed are optional parameters. Priority is the circuit-switched paging priority parameter as defined in GSM 08.08. The SGSN maps Priority to QoS.
- 2) The SGSN sends a BSSGP Paging Request (IMSI, TLLI, VLR TMSI, Area, Channel Needed, QoS) message to the BSS serving the MS. Area is derived from either the MS's MM context in the SGSN or, if no such information is available, from the Location Information received from the MSC/VLR. Area indicates a single cell for a READY state MS or a routing area for a STANDBY state MS. VLR TMSI and Channel Needed are included if received from the MSC. If Channel Needed was not received from the MSC, then a default Channel Needed parameter indicating circuit-switched paging is included by the SGSN. QoS indicates the priority of this Paging Request relative to other Paging Request messages buffered in the BSS. If the location area where the MS was last known to be located has an associated null routing area, then the SGSN shall send an additional BSSGP Paging Request message to each BSS serving this null RA.
- 3) The BSS translates the incoming BSSGP Paging Request message into one radio Paging Request message per cell. If a dedicated radio resource is assigned to the MS in a cell, then the BSS transmits one Paging Request (VLR TMSI or IMSI, Channel Needed) message on this radio resource, without stopping possibly ongoing data transfers for the MS. Otherwise, the BSS pages the MS with one Paging Request (VLR TMSI or IMSI, Channel Needed) message on the appropriate paging channel in each addressed cell. This is described in GSM 03.64.
- 4) Upon receipt of a Paging Request message for a circuit-switched service the MS may accept to respond to this request and shall then follow the CS procedures for paging response (random access, immediate assignment, and paging response) as specified in GSM 04.08 [13].
- 5) When received at the BSS, the Paging Response message is sent to the MSC which shall then stop the paging response timer.

6.3.3.1 Paging Co-ordination for GPRS

The network may provide co-ordination of paging for circuit-switched and packet-switched services. Paging co-ordination means that the network sends paging messages for circuit-switched services on the same channel as used for packet-switched services, i.e., on the GPRS paging channel or on the GPRS traffic channel, and the MS needs only to monitor that channel. Three network operation modes are defined:

- Network operation mode I: the network sends a CS paging message for a GPRS-attached MS, either on the same channel as the GPRS paging channel (i.e., the packet paging channel or the CCCH paging channel), or on a GPRS traffic channel. This means that the MS needs only to monitor one paging channel, and that it receives CS paging messages on the packet data channel when it has been assigned a packet data channel.
- Network operation mode II: the network sends a CS paging message for a GPRS-attached MS on the CCCH paging channel, and this channel is also used for GPRS paging. This means that the MS needs only to monitor the CCCH paging channel, but that CS paging continues on this paging channel even if the MS has been assigned a packet data channel.

- Network operation mode III: the network sends a CS paging message for a GPRS-attached MS on the CCCH paging channel, and sends a GPRS paging message on either the packet paging channel (if allocated in the cell) or on the CCCH paging channel. This means that an MS that wants to receive pages for both circuit-switched and packet-switched services shall monitor both paging channels if the packet paging channel is allocated in the cell. No paging co-ordination is performed by the network.

Table 2: Network Operation Modes for GPRS

Mode	Circuit Paging Channel	GPRS Paging Channel	Paging co-ordination
I	Packet Paging Channel	Packet Paging Channel	Yes
	CCCH Paging Channel	CCCH Paging Channel	
	Packet Data Channel	Not Applicable	
II	CCCH Paging Channel	CCCH Paging Channel	No
III	CCCH Paging Channel	Packet Paging Channel	No
	CCCH Paging Channel	CCCH Paging Channel	

When the Gs interface is present, all MSC-originated paging of GPRS-attached MSs shall go via the SGSN, thus allowing network co-ordination of paging. Paging co-ordination shall be made by the SGSN based on the IMSI, and is provided independently of whether the MS is in STANDBY or in READY state. The network operates in mode I.

When the Gs interface is not present, all MSC-originated paging of GPRS-attached MSs shall go via the A interface, and co-ordination of paging cannot be performed. The network shall then either:

- operate in mode II, meaning that the packet common control channel shall not be allocated in the cell; or
- operate in mode III, meaning that the packet common control channel shall be used for GPRS paging when the packet paging channel is allocated in the cell.

The network operation mode (mode I, II, or III) shall be indicated as system information to MSs. For proper operation, the mode of operation should be the same in each cell of a routing area.

Based on the mode of operation provided by the network, the MS can then choose, according to its capabilities, whether it can attach to GPRS services, to non-GPRS services, or to both.

6.3.4 CS Paging for UMTS

When an MS is both CS- and PS-attached in a network that operates in mode I, then the MSC/VLR executes paging for circuit-switched services via the SGSN. Paging is defined in subclause "Paging Initiated by CN".

6.3.4.1 Network Operation Modes for UMTS

The network operation mode is used to indicate whether the Gs interface is installed or not. When the Gs interface is present, MT can initiate combine procedures.

Table 3: Network Operation Modes for UMTS

Mode	Network configuration	Combined procedure by MT
I	Gs interface is present	Yes
II	Gs interface is not present	No

The network operation mode (mode I or II) shall be indicated as system information to the MSs. For proper operation, the mode of operation should be the same in each cell of a routing area.

Based on the mode of operation provided by the network, the MS can then choose, according to its capabilities, whether it can attach to CS domain services, to PS domain services, or to both. Furthermore, based on the mode of operation, the MS can choose whether it can initiate combine update procedures or separate update procedures, according to its capabilities.

NOTE: Network operation modes I and II for UMTS correspond to modes I and II, respectively, for GPRS. Mode III applies to GPRS and not to UMTS.

6.3.5 Non-PS Alert

The MSC/VLR may request an SGSN to report activity from a specific MS. In this case, the MSC/VLR shall send a BSSAP+ Alert Request (IMSI) message to the SGSN where the MS is currently GPRS-attached.

Upon reception of the Alert Request (IMSI) message, the SGSN shall set NGAF. If NGAF is set for an MS, the SGSN shall inform the MSC/VLR when the next activity from that MS (and the MS is both IMSI- and GPRS-attached) is detected, and shall clear NGAF.

If the activity detected by the SGSN leads to a procedure towards the MSC/VLR, the SGSN shall just follow this procedure. If the activity detected by the SGSN does not lead to any procedure towards the MSC/VLR, the SGSN shall send an MS Activity Indication (IMSI) message towards the MSC/VLR.

6.3.6 MS Information Procedure

When the MS is marked at the VLR as both CS and PS attached, the VLR may perform the MS Information procedure via the SGSN. If the information requested by the VLR in the MS Information procedure is known by the SGSN, then the SGSN shall return this information to the VLR without interrogating the MS.

If the information requested is MS identity information (e.g., IMEI) that is not known by the SGSN but is known by the MS, then the SGSN shall interrogate the MS in a similar manner to that described in subclause "Identity Check Procedures".

The MS Information procedure is illustrated in Figure 19. Each step is explained in the following list.

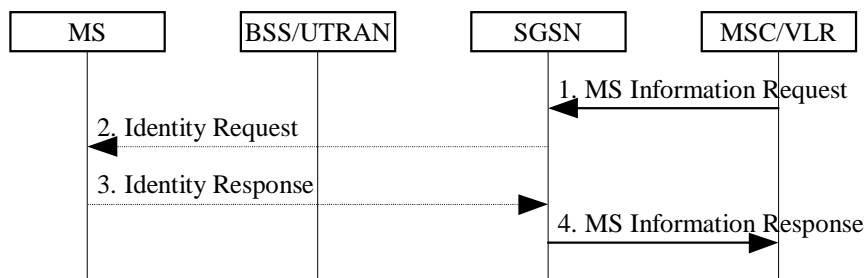


Figure 19: MS Information Procedure

- 1) The MSC/VLR sends an MS Information Request (IMSI, Information Type) message to the SGSN. Information Type indicates the information that the MSC/VLR is requesting for that IMSI.
- 2) If the information requested is not known by the SGSN but should be known by the MS, then the SGSN interrogates the MS in a similar manner to that described in the subclause "Identity Check Procedures". The SGSN sends an Identity Request (Identity Type) message to the MS.
- 3) The MS responds with an Identity Response (Mobile Identity) message to the SGSN.
- 4) The SGSN sends an MS Information Response (IMSI, Information) message to the MSC/VLR. Information contains the information requested by the MSC/VLR.

6.3.7 MM Information Procedure

When the MS is marked at the VLR as both CS and PS attached, the VLR may perform the MM Information procedure via the SGSN. The MM Information procedure is typically used to inform the MS about such things as the network name and the local timezone of the mobile.

The MM Information procedure is illustrated in Figure 20. Each step is explained in the following list.

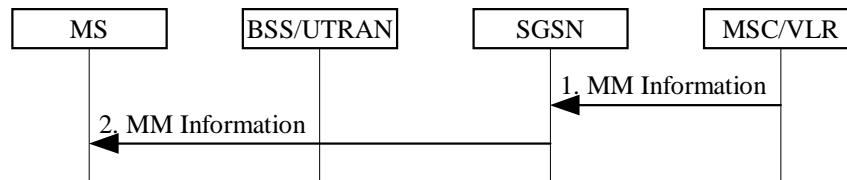


Figure 20: MM Information Procedure

- 1) The SGSN receives an MM Information (IMSI, Information) message from the MSC/VLR. Information is the information that the MSC/VLR is sending to the MS.
- 2) The SGSN sends an MM Information (Information) message to the MS including the information received by the MSC/VLR.

6.4 MM Procedures

For GPRS, the MM procedures shall use the LLC and RLC/MAC protocols for message transmission across the Gb and Um interfaces. The MM procedures shall provide information to the underlying layers to enable reliable transmission of MM messages on the Um interface. GSM 03.64 defines the mapping between LLC and the radio channels used.

For UMTS, the MM procedures shall use the RANAP and RRC protocols for message transmission across the Iu and Uu interfaces, respectively.

Furthermore, the MM procedures use MAP interfaces between SGSN and HLR (Gr), and between SGSN and EIR (Gf), and a BSSAP+ interface between SGSN and MSC/VLR (Gs).

User data can in general be transmitted during MM signalling procedures. User data transmitted during attach, authentication, and routing area update procedures may be lost and may therefore have to be retransmitted. In order to minimise the need for retransmission, the MS and SGSN should not transmit user data during the attach, authentication, and routing area update procedures.

6.5 PS Attach Function

An MS shall perform a PS Attach to the SGSN in order to obtain access to the PS services. If the MS is connected via a GPRS radio, it shall perform a GPRS Attach procedure. If the MS is connected via a UMTS radio access network, it shall perform a UMTS PS Attach procedure.

6.5.1 GPRS Attach Function

A GPRS attach is made to the SGSN. A GPRS-attached MS makes IMSI attach via the SGSN with the combined RA / LA update procedure if the network operation mode is I. In network operation modes II and III, or if the MS is not GPRS-attached, then the MS makes IMSI attach as already defined in GSM. An IMSI-attached MS in class-A mode of operation engaged in a CS connection shall use the (non-combined) GPRS Attach procedure when it performs a GPRS attach.

In the attach procedure, the MS shall provide its identity and an indication of which type of attach that is to be executed. The identity provided to the network shall be the MS's Packet TMSI (P-TMSI) or IMSI. P-TMSI and the RAI associated with the P-TMSI shall be provided if the MS has a valid P-TMSI. If the MS does not have a valid P-TMSI, then the MS shall provide its IMSI. The different types of attach are GPRS attach and combined GPRS / IMSI attach.

At the RLC/MAC layer, the MS shall identify itself with a Local or Foreign TLLI if the MS is already GPRS-attached and is performing an IMSI attach. Otherwise, the MS shall identify itself with a Foreign TLLI, or a Random TLLI if a valid P-TMSI is not available. The Foreign or Random TLLI is used as an identifier during the attach procedure until a new P-TMSI is allocated.

After having executed the GPRS attach, the MS is in READY state and MM contexts are established in the MS and the SGSN. The MS may then activate PDP contexts as described in subclause "Activation Procedures".

An IMSI-attached MS that can only operate in class-C mode of operation shall follow the normal IMSI detach procedure before it makes a GPRS attach. A GPRS-attached MS in class-C mode of operation shall always perform a GPRS detach before it makes an IMSI attach.

If the network operates in mode I (see subclause "Paging Co-ordination"), then an MS that is both GPRS-attached and IMSI-attached shall perform the Combined RA / LA Update procedures.

If the network operates in mode II or III, then a GPRS-attached MS that has the capability to be simultaneously GPRS-attached and IMSI-attached shall perform the (non-combined) Routeing Area Update procedures, and either:

- access the non-GPRS common control channels for CS operation (the way that CS operation is performed in parallel with GPRS operation is an MS implementation issue outside the scope of the present document); or
- if CS operation is not desired, depending on system information that defines whether or not explicit detach shall be used, either:
 - avoid all CS signalling (in which case the MS may be implicitly IMSI detached after a while); or
 - perform an explicit IMSI detach via the non-GPRS common control channels (if the MS was already IMSI-attached).

The Combined GPRS / IMSI Attach procedure is illustrated in Figure 21. Each step is explained in the following list.

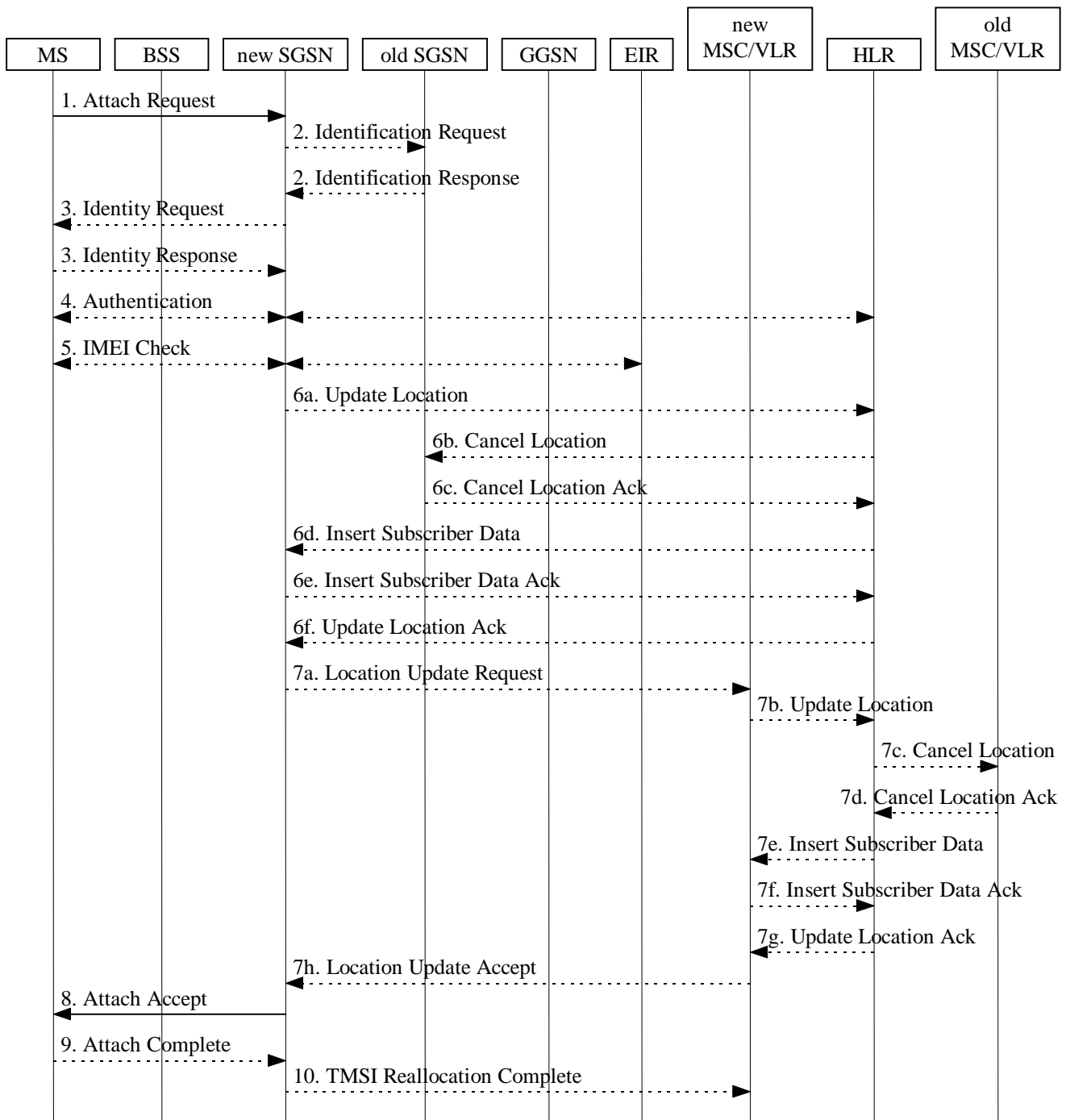


Figure 21: Combined GPRS / IMSI Attach Procedure

- 1) The MS initiates the attach procedure by the transmission of an Attach Request (IMSI or P-TMSI and old RAI, Classmark, CKSN, Attach Type, DRX Parameters, old P-TMSI Signature) message to the SGSN. IMSI shall be included if the MS does not have a valid P-TMSI available. If the MS has a valid P-TMSI, then P-TMSI and the old RAI associated with P-TMSI shall be included. Classmark contains the MS's GPRS multislot capabilities and supported GPRS ciphering algorithms in addition to the existing classmark parameters defined in GSM 04.08. Attach Type indicates which type of attach that is to be performed, i.e., GPRS attach only, GPRS Attach while already IMSI attached, or combined GPRS / IMSI attach. DRX Parameters indicates whether the MS uses discontinuous reception or not. If the MS uses discontinuous reception, then DRX Parameters also indicate when the MS is in a non-sleep mode able to receive paging requests and channel assignments. If the MS uses P-TMSI for identifying itself and if it has also stored its old P-TMSI Signature, then the MS shall include the old P-TMSI Signature in the Attach Request message.

- 2) If the MS identifies itself with P-TMSI and the SGSN has changed since detach, the new SGSN sends an Identification Request (P-TMSI, old RAI, old P-TMSI Signature) to the old SGSN to request the IMSI. The old SGSN responds with Identification Response (IMSI, Authentication Triplets). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN also validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN.
- 3) If the MS is unknown in both the old and new SGSN, the SGSN sends an Identity Request (Identity Type = IMSI) to the MS. The MS responds with Identity Response (IMSI).
- 4) The authentication functions are defined in the subclause "Security Function". If no MM context for the MS exists anywhere in the network, then authentication is mandatory. Ciphering procedures are described in subclause "Security Function". If P-TMSI allocation is going to be done, and if ciphering is supported by the network, ciphering mode shall be set.
- 5) The equipment checking functions are defined in the subclause "Identity Check Procedures". Equipment checking is optional.
- 6) If the SGSN number has changed since the GPRS detach, or if it is the very first attach, then the SGSN informs the HLR:
 - a) The SGSN sends an Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.
 - b) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure.
 - c) The old SGSN acknowledges with Cancel Location Ack (IMSI). If there are any ongoing procedures for that MS, the old SGSN shall wait until these procedures are finished before removing the MM and PDP contexts.
 - d) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new SGSN.
 - e) The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to attach in the RA, the SGSN rejects the Attach Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If subscription checking fails for other reasons, the SGSN rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack (IMSI, Cause) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
 - f) The HLR acknowledges the Update Location message by sending an Update Location Ack to the SGSN after the cancelling of old MM context and insertion of new MM context are finished. If the Update Location is rejected by the HLR, the SGSN rejects the Attach Request from the MS with an appropriate cause.
- 7) If Attach Type in step 1 indicated GPRS Attach while already IMSI attached, or combined GPRS / IMSI attach, then the VLR shall be updated if the Gs interface is installed. The VLR number is derived from the RA information. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 6 d). This operation marks the MS as GPRS-attached in the VLR.
 - a) The SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) message to the VLR. Location Update Type shall indicate IMSI attach if Attach Type indicated combined GPRS / IMSI attach. Otherwise, Location Update Type shall indicate normal location update. The VLR creates an association with the SGSN by storing SGSN Number.
 - b) If the LA update is inter-MSC, the new VLR sends Update Location (IMSI, new VLR) to the HLR.
 - c) If the LA update is inter-MSC, the HLR sends a Cancel Location (IMSI) to the old VLR.
 - d) The old VLR acknowledges with Cancel Location Ack (IMSI).
 - e) If the LA update is inter-MSC, the HLR sends Insert Subscriber Data (IMSI, GSM subscriber data) to the new VLR.
 - f) The VLR acknowledges with Insert Subscriber Data Ack (IMSI).

- g) After finishing the inter-MSC location update procedures, the HLR responds with Update Location Ack (IMSI) to the new VLR.
- h) The VLR responds with Location Update Accept (VLR TMSI) to the SGSN.
- 8) The SGSN selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS. P-TMSI is included if the SGSN allocates a new P-TMSI.
- 9) If P-TMSI or VLR TMSI was changed, the MS acknowledges the received TMSI(s) with Attach Complete (P-TMSI, VLR TMSI).
- 10) If VLR TMSI was changed, the SGSN confirms the VLR TMSI re-allocation by sending TMSI Reallocation Complete (VLR TMSI) to the VLR.

If the Attach Request cannot be accepted, the SGSN returns an Attach Reject (IMSI, Cause) message to the MS.

6.5.2 UMTS PS Attach Function

[It is an outstanding task to merge this subclause with "GPRS Attach Function".]

A PS-attached MS makes a CS attach via the SGSN with the combined RA / LA update procedure if the network operates in mode I. In network operates in mode II, or if the MS is not PS-attached, then the MS makes a normal CS attach. A CS-attached MS engaged in a CS connection shall use the (non-combined) PS Attach procedure when it performs a PS attach.

In the attach procedure, the MS shall provide its identity and an indication of which type of attach that is to be executed. The identity provided to the network shall be the MS's Packet TMSI (P-TMSI) or IMSI. P-TMSI and the RAI associated with the P-TMSI shall be provided if the MS has a valid P-TMSI. If the MS does not have a valid P-TMSI, then the MS shall provide its IMSI. The different types of attach are PS attach and combined PS / CS attach.

After having executed the PS attach, the MS is in the PMM-CONNECTED state and MM contexts are established in the MS and the SGSN. The MS may then activate PDP contexts as described in subclause "Activation Procedures".

An CS-attached MS that cannot operate in CS/PS mode of operation shall follow the normal CS detach procedure before it makes a PS attach. A PS-attached MS that cannot operate in CS/PS mode of operation shall perform a PS detach before it makes a CS attach.

The Combined PS / CS Attach procedure is illustrated in Figure 21. Each step is explained in the following list.

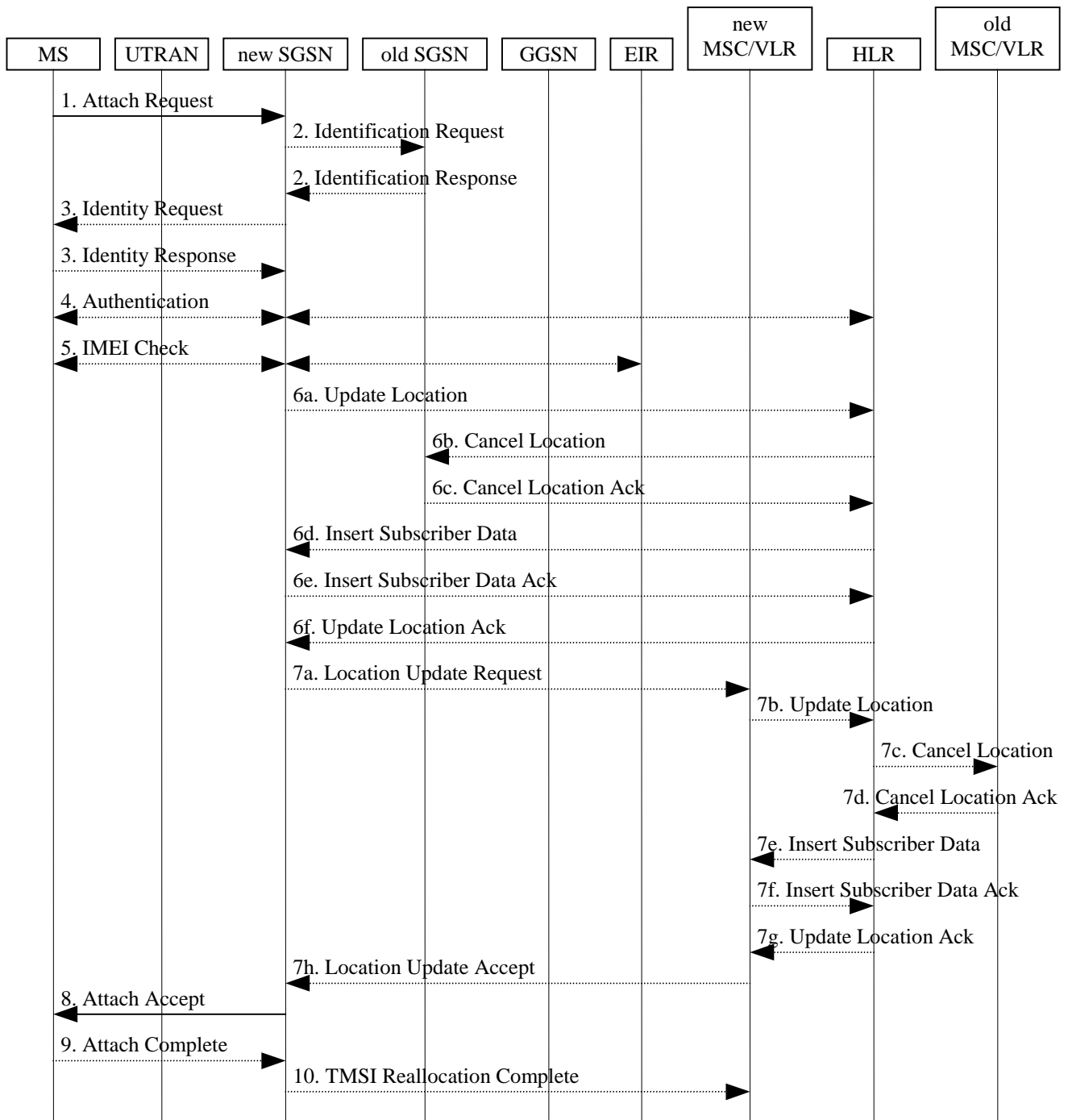


Figure 22: Combined PS / CS Attach Procedure

- 1) The MS initiates the attach procedure by the transmission of an Attach Request (IMSI or P-TMSI and old RAI, Core Network Classmark, KSI, Attach Type, old P-TMSI Signature, Follow on request) message to the SGSN. IMSI shall be included if the MS does not have a valid P-TMSI available. If the MS uses P-TMSI for identifying itself and if it has also stored its old P-TMSI Signature, then the MS shall include the old P-TMSI Signature in the Attach Request message. If the MS has a valid P-TMSI, then P-TMSI and the old RAI associated with P-TMSI shall be included. KSI shall be included if the MS has valid security parameters. Core Network Classmark is describe in subclause "Core Network Classmark". Follow on request shall be set by MS if there is pending uplink traffic (signaling or user data). The SGSN may use, as an implementation option, the follow on request indication to release or keep the Iu connection after the completion of the PS Attach procedure. Attach Type indicates which type of attach that is to be performed, i.e., PS attach only, PS Attach while already CS attached, or combined PS / CS attach.

If the MS identifies itself with P-TMSI and the SGSN has changed since detach, the new SGSN sends an Identification Request (P-TMSI, old RAI, old P-TMSI Signature) to the old SGSN to request the IMSI. The old SGSN responds with Identification Response (IMSI, Authentication vector). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN also validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN.

- 3) If the MS is unknown in both the old and new SGSN, the SGSN sends an Identity Request (Identity Type = IMSI) to the MS. The MS responds with Identity Response (IMSI).
- 4) The authentication functions are defined in the subclause "Security Function". If no MM context for the MS exists anywhere in the network, then authentication is mandatory. Ciphering procedures are described in subclause "Security Function". If P-TMSI allocation is going to be done, and if ciphering is supported by the network, ciphering mode shall be set.
- 5) The equipment checking functions are defined in the subclause "Identity Check Procedures". Equipment checking is optional.
- 6) If the SGSN number has changed since the GPRS detach, or if it is the very first attach, then the SGSN informs the HLR:
 - a) The SGSN sends an Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.
 - b) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure.
 - c) The old SGSN acknowledges with Cancel Location Ack (IMSI). If there are any ongoing procedures for that MS, the old SGSN shall wait until these procedures are finished before removing the MM and PDP contexts.
 - d) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new SGSN.
 - e) The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to attach in the RA, the SGSN rejects the Attach Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If subscription checking fails for other reasons, the SGSN rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack (IMSI, Cause) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
 - f) The HLR acknowledges the Update Location message by sending an Update Location Ack to the SGSN after the cancelling of old MM context and insertion of new MM context are finished. If the Update Location is rejected by the HLR, the SGSN rejects the Attach Request from the MS with an appropriate cause.
- 7) If Attach Type in step 1 indicated PS Attach while already CS attached, or combined PS / CS attach, then the VLR shall be updated if the Gs interface is installed. The VLR number is derived from the RA information. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 6 d). This operation marks the MS as GPRS-attached in the VLR.
 - a) The SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) message to the VLR. Location Update Type shall indicate CS attach if Attach Type indicated combined PS / CS attach. Otherwise, Location Update Type shall indicate normal location update. The VLR creates an association with the SGSN by storing SGSN Number.
 - b) If the LA update is inter-MSC, the new VLR sends Update Location (IMSI, new VLR) to the HLR.
 - c) If the LA update is inter-MSC, the HLR sends a Cancel Location (IMSI) to the old VLR.
 - d) The old VLR acknowledges with Cancel Location Ack (IMSI).
 - e) If the LA update is inter-MSC, the HLR sends Insert Subscriber Data (IMSI, GSM subscriber data) to the new VLR.
 - f) The VLR acknowledges with Insert Subscriber Data Ack (IMSI).
 - g) After finishing the inter-MSC location update procedures, the HLR responds with Update Location Ack (IMSI) to the new VLR.

- h) The VLR responds with Location Update Accept (VLR TMSI) to the SGSN.
- 8) The SGSN selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS. P-TMSI is included if the SGSN allocates a new P-TMSI.
- 9) If P-TMSI or VLR TMSI was changed, the MS acknowledges the received TMSI(s) with Attach Complete (P-TMSI, VLR TMSI).
- 10) If VLR TMSI was changed, the SGSN confirms the VLR TMSI re-allocation by sending TMSI Reallocation Complete (VLR TMSI) to the VLR.

If the Attach Request cannot be accepted, the SGSN returns an Attach Reject (IMSI, Cause) message to the MS.

6.6 Detach Function

The PS Detach procedure allows:

- an MS to inform the network that it does not want access the SGSN-based services any longer; and
- the network to inform an MS that it does not have access to the SGSN-based services any more.

The Detach function allows an MS to inform the network that it wants to make a PS and/or CS detach, and it allows the network to inform an MS that it has been PS-detached or CS-detached by the network.

The different types of detach are:

- CS detach;
- PS detach; and
- combined PS / CS detach (MS-initiated only).

The MS is detached either explicitly or implicitly:

- Explicit detach: The network or the MS explicitly requests detach.
- Implicit detach: The network detaches the MS, without notifying the MS, a configuration-dependent time after the mobile reachable timer expired, or after an irrecoverable radio error causes disconnection of the logical link.

In the explicit detach case, a Detach Request (Cause) is sent by the SGSN to the MS, or by the MS to the SGSN.

The MS can make a CS detach in one of two ways depending on if it is PS-attached or not:

- A PS-attached MS sends a Detach Request message to the SGSN, indicating a CS detach. This can be made in combination with PS detach.
- An MS that is not PS-attached makes the CS detach as already defined in GSM or UMTS.

In the MO Detach Request message there is an indication to tell if the detach is due to switch off or not. The indication is needed to know whether a Detach Accept message should be returned or not.

In the network-originated Detach Request message there may be an indication to tell the MS that it is requested to initiate PS Attach and PDP Context Activation procedures for the previously activated PDP contexts.

6.6.1 MS-Initiated Detach Procedure

The MS-Initiated Detach procedure when initiated by the MS is illustrated in Figure 23. Each step is explained in the following list.

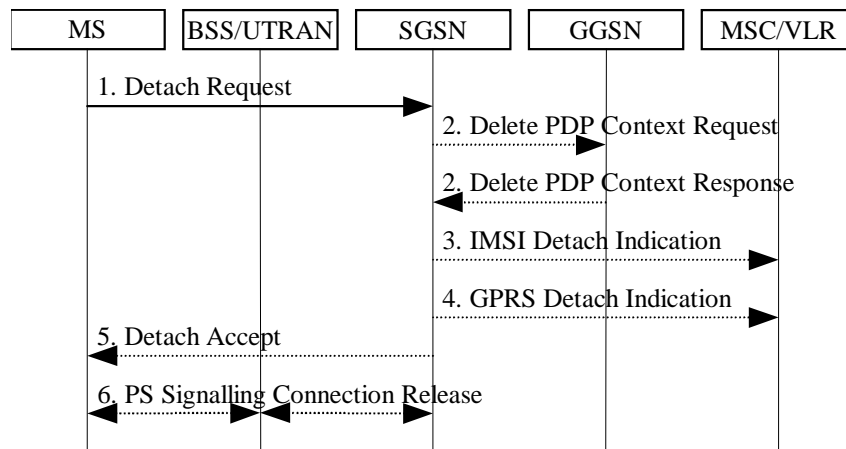


Figure 23: MS-Initiated Combined PS / CS Detach Procedure

- 1) The MS detaches by sending Detach Request (Detach Type, P-TMSI, P-TMSI Signature, Switch Off) to the SGSN. Detach Type indicates which type of detach that is to be performed, i.e., PS Detach only, CS Detach only or combined PS and CS Detach. Switch Off indicates whether the detach is due to a switch off situation or not. For UMTS, the Detach Request message includes P-TMSI and P-TMSI Signature. P-TMSI Signature is used to check the validity of the Detach Request message. If P-TMSI Signature is not valid or is not included, then authentication procedure should be performed.
- 2) If PS detach, the active PDP contexts in the GGSNs regarding this particular MS are deactivated by the SGSN sending Delete PDP Context Request (TEID) to the GGSNs. The GGSNs acknowledge with Delete PDP Context Response (TEID).
- 3) If CS detach, the SGSN sends CS Detach Indication (IMSI) to the VLR.
- 4) If the MS wants to remain CS-attached and is doing a PS detach, the SGSN sends a PS Detach Indication (IMSI) message to the VLR. The VLR removes the association with the SGSN and handles paging and location update without going via the SGSN.
- 5) If Switch Off indicates that the detach is not due to a switch off situation, the SGSN sends a Detach Accept to the MS.
- 6) If the MS was PS detached, then the 3G-SGSN releases the PS signalling connection.

6.6.2 Network-Initiated Detach Procedure

6.6.2.1 SGSN-Initiated Detach Procedure

The SGSN-Initiated Detach procedure when initiated by the SGSN is illustrated in Figure 24. Each step is explained in the following list.

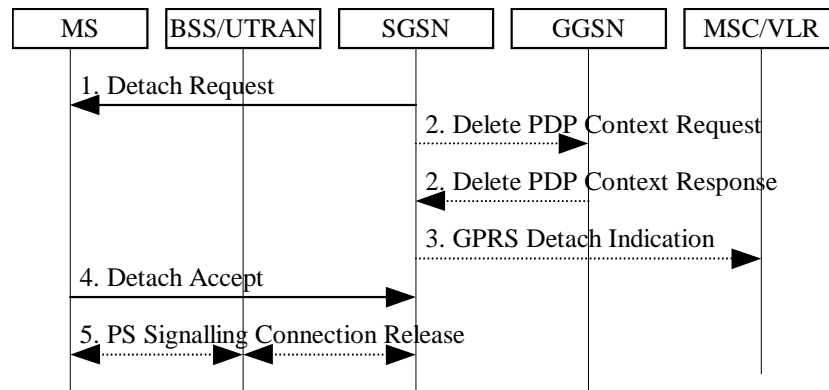


Figure 24: SGSN-Initiated PS Detach Procedure

- 1) The SGSN informs the MS that it has been detached by sending Detach Request (Detach Type) to the MS. Detach Type indicates if the MS is requested to make a new attach and PDP context activation for the previously activated PDP contexts. If so, the attach procedure shall be initiated when the detach procedure is completed.
- 2) The active PDP contexts in the GGSNs regarding this particular MS are deactivated by the SGSN sending Delete PDP Context Request (TEID) messages to the GGSNs. The GGSNs acknowledge with Delete PDP Context Response (TEID) messages.
- 3) If the MS was both CS- and PS-attached, the SGSN sends a PS Detach Indication (IMSI) message to the VLR. The VLR removes the association with the SGSN and handles paging and location update without going via the SGSN.
- 4) The MS sends a Detach Accept message to the SGSN any time after step 1.
- 5) After receiving the Detach Accept message, if Detach Type did not request the MS to make a new attach, then the 3G-SGSN releases the PS signalling connection.

6.6.2.2 HLR-Initiated Detach Procedure

The HLR-Initiated Detach procedure is initiated by the HLR. The HLR uses this procedure for operator-determined purposes to request the removal of a subscriber's MM and PDP contexts at the SGSN. The HLR-Initiated Detach Procedure is illustrated in Figure 25. Each step is explained in the following list.

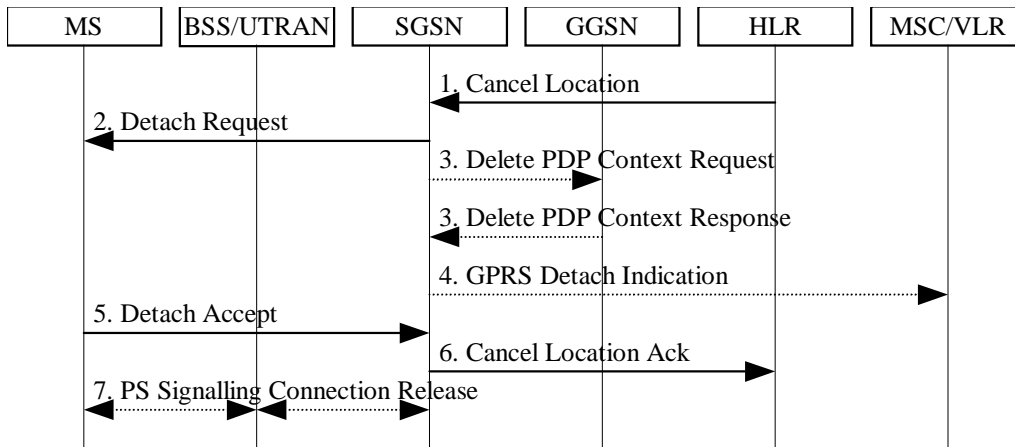


Figure 25: HLR-Initiated PS Detach Procedure

- 1) If the HLR wants to request the immediate deletion of a subscriber's MM and PDP contexts from the SGSN, the HLR shall send a Cancel Location (IMSI, Cancellation Type) message to the SGSN with Cancellation Type set to Subscription Withdrawn.
- 2) The SGSN informs the MS that it has been detached by sending Detach Request (Detach Type) to the MS. Detach Type shall indicate that the MS is not requested to make a new attach and PDP context activation.
- 3) The active PDP contexts in the GGSNs regarding this particular MS are deactivated by the SGSN sending Delete PDP Context Request (TEID) messages to the GGSNs. The GGSNs acknowledge with Delete PDP Context Response (TEID) messages.
- 4) If the MS was both CS- and PS-attached, the SGSN sends a PS Detach Indication (IMSI) message to the VLR. The VLR removes the association with the SGSN and handles paging and location update without going via the SGSN.
- 5) The MS sends a Detach Accept message to the SGSN any time after step 2.
- 6) The SGSN shall confirm the deletion of the MM and PDP contexts with a Cancel Location Ack (IMSI) message.
- 7) After receiving the Detach Accept message, if Detach Type did not request the MS to make a new attach, then the 3G-SGSN releases the PS signalling connection.

6.7 Purge Function

The Purge function allows an SGSN to inform the HLR that it has deleted the MM and PDP contexts of a detached MS. The SGSN may, as an implementation option, delete the MM and PDP contexts of an MS immediately after the implicit or explicit detach of the MS. Alternatively, the SGSN may keep for some time the MM and PDP contexts and the authentication triplets of the detached MS, so that the contexts can be reused at a later PS attach without accessing the HLR.

When the SGSN deletes the MM and PDP contexts, it shall initiate the Purge procedure as illustrated in Figure 26. Each step is explained in the following list.

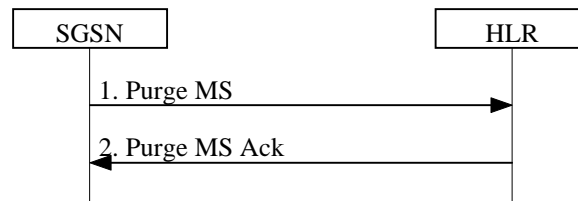


Figure 26: Purge Procedure

- 1) After deleting the MM and PDP contexts of a detached MS, the SGSN sends a Purge MS (IMSI) message to the HLR.
- 2) The HLR sets the MS Purged for GPRS flag and acknowledges with a Purge MS Ack message.

6.8 Security Function

The Security function:

- Guards against unauthorised packet-domain service usage (authentication and service request validation).
- Provides user identity confidentiality (temporary identification and ciphering).
- Provides user data and signalling confidentiality (ciphering).
- Provides, for UMTS only, data integrity and origin authentication of signalling data (integrity protection).
- Provides, for UMTS only, authentication of the network by the MS.

Security-related network functions are described in GSM 03.20 for GPRS and in UMTS 33.102 for UMTS.

6.8.1 Authentication

6.8.1.1 Authentication of GSM Subscriber in GSM

Authentication procedures already defined in GSM shall be used, with the distinction that the procedures are executed from the SGSN. The GPRS Authentication procedure performs subscriber authentication, or selection of the ciphering algorithm and the synchronisation of the start of ciphering, or both. Authentication triplets are stored in the SGSN. The MSC/VLR shall not authenticate the MS via the SGSN upon IMSI attach, nor location update, but may authenticate the MS during CS connection establishment. Security-related network functions are described in GSM 03.20 [6].

The Authentication of GSM Subscriber in GSM procedure (GSM SIM) is illustrated in Figure 27. Each step is explained in the following list.

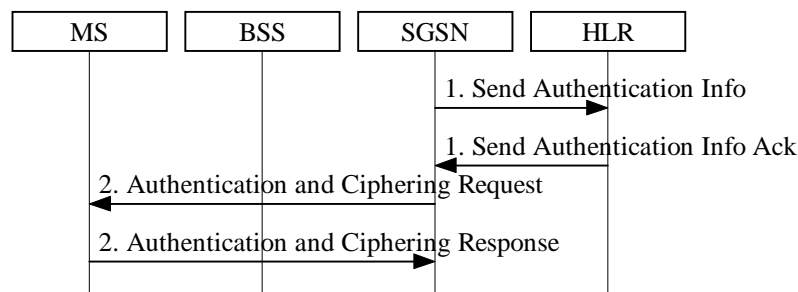


Figure 27: Authentication of GSM Subscriber in GSM Procedure

- 1) If the SGSN does not have previously stored authentication triplets, a Send Authentication Info (IMSI) message is sent to the HLR. The HLR responds with a Send Authentication Info Ack (Authentication Triplets) message. Each Authentication Triplet includes RAND, SRES, and Kc.
- 2) The SGSN sends an Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) message to the MS. The MS responds with an Authentication and Ciphering Response (SRES) message.

The MS starts ciphering after sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response is received from the MS. In the routing area update case, if ciphering was used before the routing area update, and if the Authentication procedure is omitted, then the SGSN shall resume ciphering with the same algorithm when a ciphered Routing Area Update Accept message is sent, and the MS shall resume ciphering when a ciphered Routing Area Update Accept message is received.

When changing to a UMTS system the MS and the 3G-SGSN shall generate the UMTS security keys IK and CK from the GSM Kc by using the conversion functions specified for this purpose in UMTS 33.102.

[Conversion functions to be defined by TSG SA3.]

6.8.1.2 Authentication of UMTS Subscriber in UMTS

The UMTS authentication procedure is described in UMTS 33.102. The UMTS authentication procedure executed from the SGSN performs both the mutual authentication and security keys agreement. Authentication quintuplets are stored in the SGSN. The MSC/VLR shall not authenticate the MS via the SGSN upon CS attach nor upon location update, but may authenticate the MS during CS connection establishment.

The Authentication of UMTS Subscriber in UMTS procedure (USIM) is illustrated in Figure 28. Each step is explained in the following list.

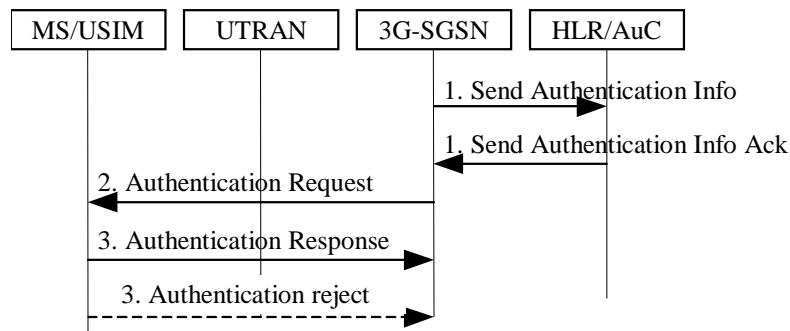


Figure 28: Authentication of UMTS Subscriber in UMTS Procedure

- 1) If the 3G-SGSN does not have previously stored UMTS Authentication Vectors (quintuplets), a Send Authentication Info (IMSI) message is sent to the HLR. Upon receipt of this message for a UMTS user, the HLR/AuC responds with a Send Authentication Info Ack message including an ordered array of quintuplets to the 3G-SGSN. Each quintuplet contains RAND, XRES, AUTN, CK, and IK. The generation of quintuplets in HLR/AuC for a UMTS user is performed as specified in UMTS 33.102.
- 2) At authentication of a UMTS user, the 3G-SGSN selects the next in-order quintuplet and transmits the RAND and AUTN, that belong to this quintuplet, to the MS in the Authentication Request (RAND, AUTN, KSN) message. The 3G-SGSN also selects a key sequence number, KSN, and includes this in the message.
- 3) At reception of this message, the USIM in the MS verifies AUTN and, if accepted, the USIM computes the signature of RAND, RES, in accordance with UMTS 33.102. If the USIM considers the authentication being successful the MS returns an Authentication Response (RES) message to the 3G-SGSN. The USIM in the MS computes then also a new Ciphering Key, CK, and a new Integrity Key, IK. These keys are stored together with the KSN until KSN is updated at the next authentication.

If the USIM considers the authentication being unsuccessful, i.e., in case of an authentication synchronisation failure, the MS returns the Authentication Reject message to the 3G-SGSN. The actions then taken are described in UMTS 33.102.

When changing to an SGSN that supports the UMTS authentication procedure, the used IK and CK are sent from the old SGSN to the new SGSN. The unused quintuplets, if any, are then also transferred to the new SGSN.

When changing to a UMTS system the MS and the 3G-SGSN shall generate the UMTS security keys IK and CK from the GSM Kc by using the conversion functions specified for this purpose in UMTS 33.102.

When changing to a GSM system the USIM and the SGSN shall generate from the UMTS security keys IK and CK the GSM Kc by using the standardised conversion function specified for this purpose in UMTS 33.102.

When changing to an SGSN that does not support the UMTS authentication procedure, the old 3G-SGSN should generate the GSM Kc as described above and transfer this to the new SGSN. This will then give support for a change of SGSN without the need for a new authentication. No quintuplets are transferred in this case.

6.8.1.3 Authentication of GSM Subscriber in UMTS

GSM users roaming in a UMTS network are authenticated with the GSM authentication procedure.

The UMTS Authentication of GSM Subscriber in UMTS procedure (GSM SIM) is illustrated in Figure 29. Each step is explained in the following list.

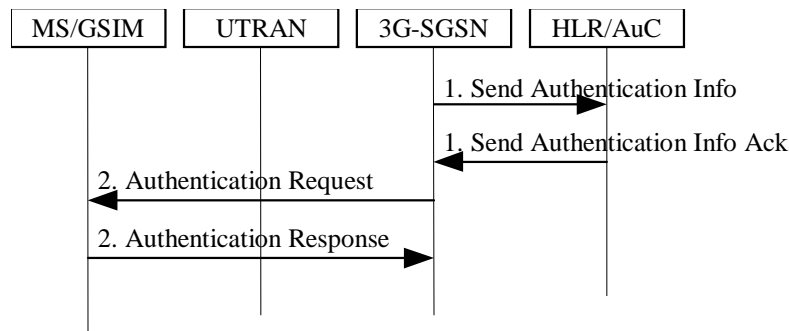


Figure 29: Authentication of GSM Subscriber in UMTS Procedure

- 1) If the 3G-SGSN does not contain previously stored authentication parameters, then a Send Authentication Info (IMSI) message is sent to the HLR. The HLR responds with a Send Authentication Info Ack (Authentication Triplets) message. Each Authentication Triplet includes RAND, SRES, and Kc.
- 2) At authentication in UMTS mode the 3G-SGSN selects an unused triplet and sends an Authentication Request (RAND) message to the MS. The GSM SIM then calculates the SRES and the GSM Kc. The MS returns an Authentication Response (SRES) message to the 3G-SGSN.

The 3G-SGSN shall generate the UMTS CK and IK from the GSM Kc using the standardised conversion functions specified for this purpose in UMTS 33.102.

The MS shall generate the UMTS CK and IK from the GSM Kc using the standardised conversion functions specified for this purpose in UMTS 33.102, i.e., the same algorithm as in the 3G-SGSN.

When changing SGSN the used Kc (i.e., the Kc of last used authentication triplet) is sent from the old 3G-SGSN to the new SGSN. The unused triplets, if any, are then also transferred to the new SGSN.

6.8.1.4 Authentication of UMTS Subscriber in GSM

For authentication of a UMTS subscriber (USIM) in a GSM system three cases are possible:

- a) The SGSN supports the GSM authentication procedure but not the UMTS authentication procedure.
- b) The SGSN supports both the GSM and UMTS authentication procedures but the MS supports only the GSM authentication procedure.
- c) Both the SGSN and the MS support the UMTS authentication procedure.

[It is an open issue whether it shall be possible to make a UMTS authentication also in GSM release 99.]

Case a)

When the SGSN supports only the GSM authentication procedure, then the authentication of a UMTS subscriber is performed using an authentication triplet produced by the HLR/AuC. The authentication of a UMTS subscriber by using a GSM authentication triplet is performed in the same way as authentication of a GSM subscriber in GSM, see subclause "Authentication of GSM Subscriber in GSM". The conversion functions that apply for HLR/AuC and USIM in this case are described in UMTS 33.102.

When changing to a UMTS system a new authentication using a UMTS authentication quintuplet is required.

[The requirements for this system change case need to be clarified.]

Case b)

When the SGSN supports both the GSM and UMTS authentication procedures but the MS supports only the GSM authentication procedure, then the authentication of a UMTS subscriber shall be performed using an authentication quintuplet produced by HLR/AuC. In this case the SGSN derives a GSM triplet from a UMTS quintuplet originally produced by HLR/AuC. The authentication procedure of the UMTS subscriber will then be performed in the same way as authentication of a GSM subscriber in GSM, see subclause "Authentication of GSM Subscriber in GSM". The conversion functions that apply for SGSN and USIM in this case are described in UMTS 33.102.

When changing to an SGSN that supports the UMTS authentication procedure, the IK and CK of the last used quintuplet are sent from the old SGSN to the new SGSN. The unused quintuplets, if any, are then also transferred to the new SGSN.

When changing to a UMTS system the UMTS CK and IK from the last used authentication quintuplet shall be used.

When changing to an SGSN that does not support the UMTS authentication procedure, the used GSM Kc is transferred from the old SGSN to the new SGSN. This supports SGSN change without the need for a new authentication. No quintuplet is transferred in this case.

Case c)

FFS.

6.8.2 User Identity Confidentiality

6.8.2.1 User Identity Confidentiality for GPRS

A Temporary Logical Link Identity (TLLI) identifies a GPRS user. The relationship between TLLI and IMSI is known only in the MS and in the SGSN. TLLI is derived from the P-TMSI allocated by the SGSN or built by the MS as described in subclause "NSAPI and TLLI".

6.8.2.2 User Identity Confidentiality for UMTS

A Radio Network Temporary Identity (RNTI) identifies a UMTS user between the MS and the UTRAN. The relationship between RNTI and IMSI is known only in the MS and in the UTRAN. A P-TMSI identifies a UMTS user between the MS and the SGSN. The relationship between P-TMSI and IMSI is known only in the MS and in the SGSN.

6.8.2.3 P-TMSI Signature

P-TMSI Signature is optionally sent by the SGSN to the MS in Attach Accept and Routeing Area Update Accept messages. If the P-TMSI Signature has been sent by the SGSN to the MS since the current P-TMSI was allocated, then the MS shall include the P-TMSI Signature in the next Routeing Area Update Request, Detach Request, Service Request, and Attach Request for identification checking purposes. If the P-TMSI Signature was sent, then the SGSN shall compare the P-TMSI Signature sent by the MS with the signature stored in the SGSN. If the values do not match, the SGSN should use the security functions to authenticate the MS. If the values match or if the P-TMSI Signature is missing, the SGSN may use the security functions to authenticate the MS. The P-TMSI Signature parameter has only local significance in the SGSN that allocated the signature.

If ciphering is supported by the network, the SGSN shall send the P-TMSI Signature ciphered to the MS. Routeing Area Update Request and Attach Request, into which the MS includes the P-TMSI Signature, are not ciphered.

6.8.2.4 P-TMSI Reallocation Procedure

The SGSN may reallocate the P-TMSI at any time. The reallocation procedure can be performed by the P-TMSI Reallocation procedure, or it can be included in the Attach or Routeing Area Update procedures.

The P-TMSI Reallocation procedure is illustrated in Figure 30. Each step is explained in the following list.

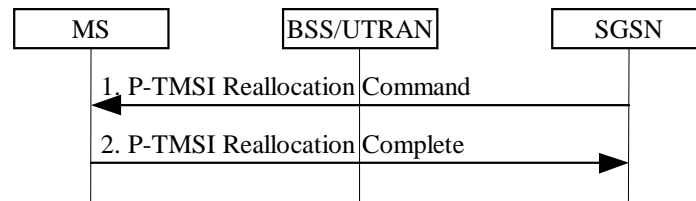


Figure 30: P-TMSI Reallocation Procedure

- 1) The SGSN sends a P-TMSI Reallocation Command (new P-TMSI, P-TMSI Signature, RAI) message to the MS. P-TMSI Signature is an optional parameter that the MS, if received, shall return to the SGSN in the next Attach and Routing Area Update procedures.
- 2) The MS returns a P-TMSI Reallocation Complete message to the SGSN.

6.8.3 User Data and GMM/SM Signalling Confidentiality

6.8.3.1 Scope of Ciphering

The scope of GPRS ciphering is from the ciphering function in the SGSN to the ciphering function in the MS. Ciphering is done in the LLC layer, and from the perspective of the existing GSM MS-BTS radio path, an LLC PDU is transmitted as plain text.

The scope of UMTS ciphering is from the ciphering function in the UTRAN to the ciphering function in the MS.

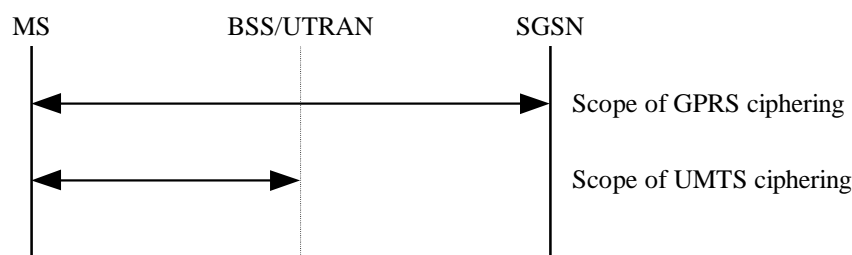


Figure 31: Scope of Ciphering

6.8.3.2 Ciphering Algorithm

GSM 01.61 [2] contains the requirements for the GPRS Encryption Algorithm (GEA). The GPRS ciphering key K_c is an input to the algorithm. The standard key management procedures for the K_c shall be used.

UMTS ciphering is performed with the UMTS Encryption Algorithm (UEA). The UMTS Ciphering Key CK is an input to the algorithm.

6.8.3.3 Start of Ciphering

In GPRS, the MS starts ciphering after sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response message is received from the MS. In the routing area update case, if ciphering was used before the routing area update, and if the authentication procedure is omitted, then the SGSN shall resume ciphering with the same algorithm when a ciphered Routing Area Update Accept message is sent, and the MS shall resume ciphering when a ciphered Routing Area Update Accept message is received.

In UMTS, the start of ciphering is controlled by the security mode procedure described in UMTS 33.102.

6.8.4 Identity Check Procedures

The Identity Check procedure is illustrated in Figure 32. Each step is explained in the following list.

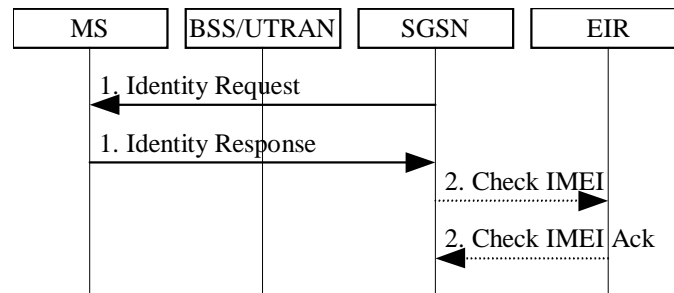


Figure 32: Identity Check Procedure

- 1) The SGSN sends Identity Request (Identity Type) to the MS. The MS responds with Identity Response (Mobile Identity). In UMTS, the MS may choose to send its IMSI encrypted (FFS).
- 2) If the SGSN decides to check the IMEI against the EIR, it sends Check IMEI (IMEI) to EIR. The EIR responds with Check IMEI Ack (IMEI).

6.8.5 Data Integrity Procedure for UMTS

The Data Integrity procedure is performed between the MS and the UTRAN. It is applicable only to radio signalling. The UMTS integrity check is made with the UMTS Integrity Algorithm (UIA). The UMTS Integrity Key IK is an input to the algorithm. The start of the data integrity procedure is controlled by the security mode procedure as described in UMTS 33.102.

6.9 Location Management Function

The Location Management function:

- provides mechanisms for cell and PLMN selection;
- provides a mechanism for the network to know the Routeing Area for MSs in STANDBY, PMM-IDLE, READY, and PMM-CONNECTED states;
- provides a mechanism for the 2G-SGSN to know the cell identity for MSs in READY state;
- provides a mechanism for the UTRAN to know the URA identity or cell identity for MSs in PMM-CONNECTED state;
- provides a mechanism for the UTRAN to indicate to an MS in RRC Connected mode when a Routeing Area Update procedure shall be performed by providing the RAI; and
- provides a mechanism for the network to know the address of the Serving RNC handling a MS in PMM-CONNECTED state. This mechanism is the Serving RNC relocation procedure.

NOTE: The SGSN may not know the Routing Area where the UMTS MS is physically located for an MS is in RRC Connected mode. An MS in PMM-CONNECTED state is necessarily in RRC Connected mode. An MS in PMM-IDLE state is in RRC Connected mode only if the MS is in CS MM-CONNECTED state.

In UMTS, the tracking of the location of the MS is on three levels (cell, URA, or RA), see UMTS 23.121.

In GPRS, the tracking of the location of the MS is on two levels (cell or RA).

Routeing Area (RA) is defined in subclause "Routeing Area Identity".

6.9.1 Location Management Procedures for GPRS

The PLMN shall provide information for the MS to be able to:

- detect when it has entered a new cell or a new RA; and
- determine when to perform periodic RA updates.

The MS detects that a new cell has been entered by comparing the cell's identity with the cell identity stored in the MS's MM context. The MS detects that a new RA has been entered by periodically comparing the RAI stored in its MM context with that received from the new cell. The MS shall consider hysteresis in signal strength measurements.

When the MS camps on a new cell, possibly in a new RA, this indicates one of three possible scenarios:

- a cell update is required;
- a routeing area update is required; or
- a combined routeing area and location area update is required.

In all three scenarios the MS stores the cell identity in its MM context.

If the MS enters a new PLMN, the MS shall either perform a routeing area update, or enter IDLE state.

In network mode of operation II and III, whenever an MS determines that it shall perform both an LA update and an RA update, the MS shall perform the LA update first.

Routeing Area Update Request messages shall be sent unciphered, since in the inter SGSN routeing area update case the new SGSN shall be able to process the request.

6.9.1.1 Cell Update Procedure

A cell update takes place when the MS enters a new cell inside the current RA and the MS is in READY state. If the RA has changed, a routeing area update is executed instead of a cell update.

The MS performs the cell update procedure by sending an uplink LLC frame of any type containing the MS's identity to the SGSN. In the direction towards the SGSN, the BSS shall add the Cell Global Identity including RAC and LAC to all BSSGP frames, see GSM 08.18. A cell update is any correctly received and valid LLC PDU carried inside a BSSGP PDU containing a new identifier of the cell.

The SGSN records this MS's change of cell, and further traffic directed towards the MS is conveyed over the new cell.

6.9.1.2 Routeing Area Update Procedure

A routeing area update takes place when a PS-attached MS detects that it has entered a new RA, when the periodic RA update timer has expired, or, for GPRS, when a suspended MS is not resumed by the BSS (see subclause "Suspension of GPRS Services"). The SGSN detects that it is an intra SGSN routeing area update by noticing that it also handles the old RA. In this case, the SGSN has the necessary information about the MS and there is no need to inform the GGSNs or the HLR about the new MS location. A periodic RA update is always an intra SGSN routeing area update.

An MS in READY state due to anonymous access shall not perform routeing area updates for the AA MM context. If the MS has entered a new routeing area, a new Anonymous Access PDP Context Activation procedure shall be initiated. The old context is implicitly deleted upon expiry of the READY timer.

6.9.1.2.1 Intra SGSN Routing Area Update

The Intra SGSN Routing Area Update procedure is illustrated in Figure 33. Each step is explained in the following list.

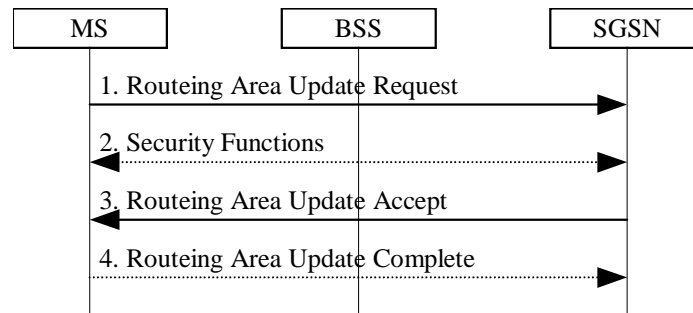


Figure 33: Intra SGSN Routing Area Update Procedure

- 1) The MS sends a Routing Area Update Request (P-TMSI, old RAI, old P-TMSI Signature, Update Type) to the SGSN. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN, see GSM 08.18.
- 2) Security functions may be executed. These procedures are defined in subclause "Security Function".
- 3) The SGSN validates the MS's presence in the new RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, then the SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the SGSN updates the MM context for the MS. A new P-TMSI may be allocated. A Routing Area Update Accept (P-TMSI, P-TMSI Signature) is returned to the MS.
- 4) If P-TMSI was reallocated, the MS acknowledges the new P-TMSI with Routing Area Update Complete (P-TMSI).

If the routing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routing Area Update Reject (Cause) message, the MS shall enter IDLE state.

6.9.1.2.2 Inter SGSN Routing Area Update

The Inter SGSN Routing Area Update procedure is illustrated in Figure 34. Each step is explained in the following list.

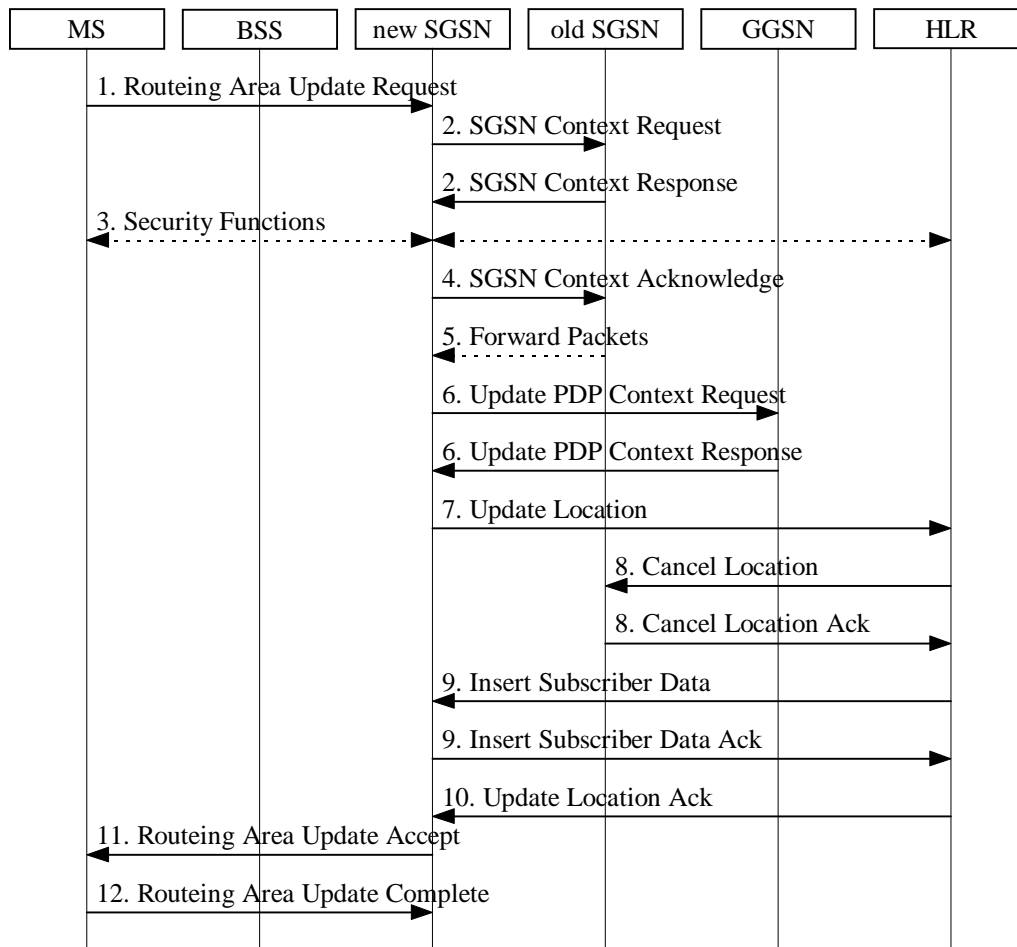


Figure 34: Inter SGSN Routing Area Update Procedure

- 1) The MS sends a Routing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the new SGSN. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN.
- 2) The new SGSN sends SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) to the old SGSN to get the MM and PDP contexts for the MS. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (old RAI, TLLI, MS Validated, New SGSN Address) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN stops assigning SMDCP N-PDU numbers to downlink N-PDUs received, and responds with SGSN Context Response (MM Context, PDP Contexts). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN stores New SGSN Address, to allow the old SGSN to forward data packets to the new SGSN. Each PDP Context includes the SMDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode to the MS, the SMDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode from the MS, the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled to the GGSN. The old SGSN starts a timer and stops the transmission of N-PDUs to the MS.
- 3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.

- 4) The new SGSN sends an SGSN Context Acknowledge message to the old SGSN. This informs the old SGSN that the new SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routing area update procedure back to the old SGSN before completing the ongoing routing area update procedure. If the security functions do not authenticate the MS correctly, then the routing area update shall be rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received.
- 5) The old SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new SGSN. Additional N-PDUs received from the GGSN before the timer described in step 2 expires are also duplicated and tunnelled to the new SGSN. N-PDUs that were already sent to the MS in acknowledged mode and that are not yet acknowledged by the MS are tunnelled together with the SMDCP N-PDU number. No N-PDUs shall be forwarded to the new SGSN after expiry of the timer described in step 2.
- 6) The new SGSN sends Update PDP Context Request (new SGSN Address, TID, QoS Negotiated) to the GGSNs concerned. The GGSNs update their PDP context fields and return Update PDP Context Response (TID).
- 7) The new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.
- 8) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, then the old SGSN removes the MM and PDP contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old SGSN to complete the forwarding of N-PDUs. It also ensures that the MM and PDP contexts are kept in the old SGSN in case the MS initiates another inter SGSN routing area update before completing the ongoing routing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).
- 9) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, the SGSN rejects the Routing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
- 10) The HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.
- 11) The new SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the SGSN, or if subscription checking fails, then the new SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the new SGSN constructs MM and PDP contexts for the MS. A logical link is established between the new SGSN and the MS. The new SGSN responds to the MS with Routing Area Update Accept (P-TMSI, P-TMSI Signature, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure.
- 12) The MS acknowledges the new P-TMSI with a Routing Area Update Complete (P-TMSI, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure. If Receive N-PDU Number confirms reception of N-PDUs that were forwarded from the old SGSN, then these N-PDUs shall be discarded by the new SGSN. LLC and SMDCP in the MS are reset.

In the case of a rejected routing area update operation, due to regional subscription or roaming restrictions, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

If the SGSN is unable to update the PDP context in one or more GGSNs, then the SGSN shall deactivate the corresponding PDP contexts as described in subclause "PDP Context Deactivation Initiated by SGSN Procedure". This shall not cause the SGSN to reject the routing area update.

If the timer described in step 2 expires and no Cancel Location (IMSI) was received from the HLR, then the old SGSN shall stop forwarding N-PDUs to the new SGSN.

If the routing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routing Area Update Reject (Cause) message, the MS shall enter IDLE state.

6.9.1.3 Combined RA / LA Update Procedure

A combined RA / LA update takes place in network operation mode I when the MS enters a new RA or when a GPRS-attached MS performs IMSI attach. The MS sends a Routing Area Update Request indicating that an LA update may also need to be performed, in which case the SGSN forwards the LA update to the VLR. This concerns only idle mode (see GSM 03.22), as no combined RA / LA updates are performed during a CS connection.

6.9.1.3.1 Combined Intra SGSN RA / LA Update

The Combined RA / LA Update (intra SGSN) procedure is illustrated in Figure 35. Each step is explained in the following list.

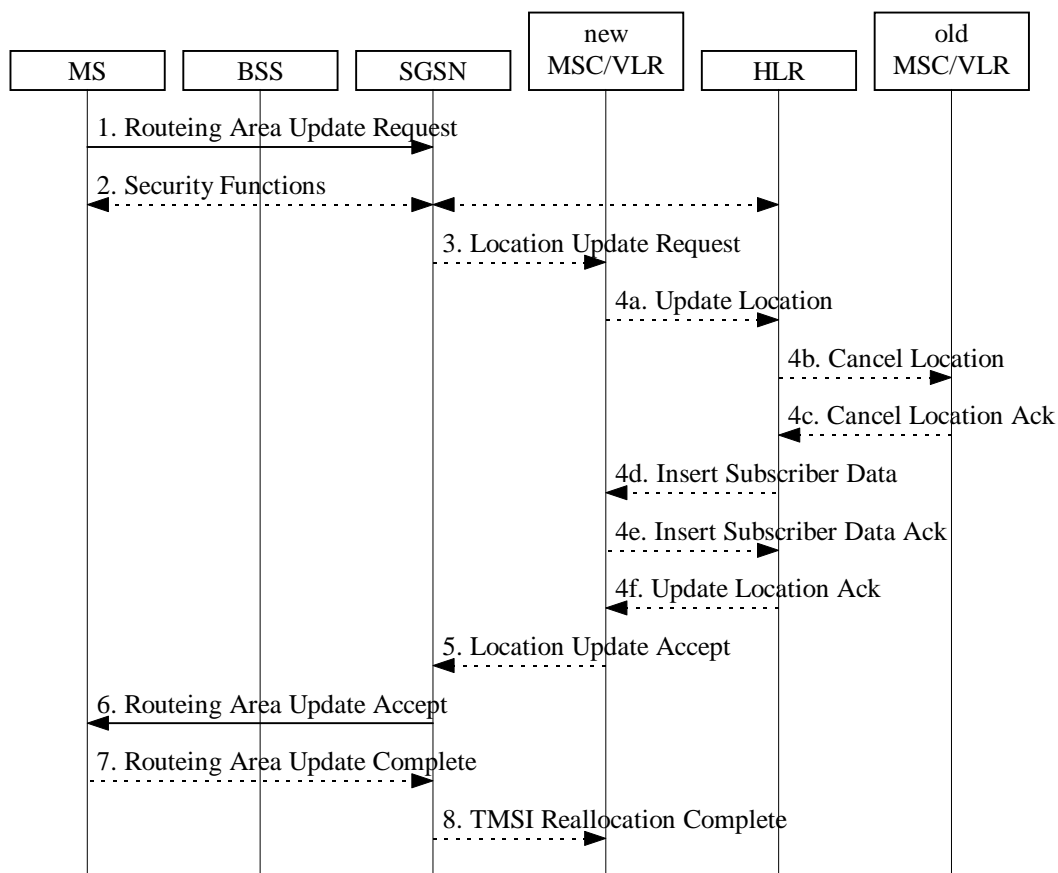


Figure 35: Combined RA / LA Update in the Case of Intra SGSN RA Update Procedure

- 1) The MS sends a Routing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the SGSN. Update Type shall indicate combined RA / LA update, or, if the MS wants to perform an IMSI attach, combined RA / LA update with IMSI attach requested. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN.
- 2) Security functions may be executed. This procedure is defined in subclause "Security Function".
- 3) If the association has to be established, if Update Type indicates combined RA / LA update with IMSI attach requested, or if the LA changed with the routing area update, then the SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA / LA update with IMSI attach requested. Otherwise, Location Update Type shall indicate normal location update. The VLR number is translated from the RAI via a table in the SGSN. The VLR creates or updates the association with the SGSN by storing SGSN Number.

- 4) If the subscriber data in the VLR is marked as not confirmed by the HLR, then the new VLR informs the HLR. The HLR cancels the data in the old VLR and inserts subscriber data in the new VLR (this signalling is not modified from existing GSM signalling and is included here for illustrative purposes):
 - a) The new VLR sends an Update Location (new VLR) to the HLR.
 - b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.
 - c) The old VLR acknowledges with Cancel Location Ack (IMSI).
 - d) The HLR sends Insert Subscriber Data (IMSI, GSM subscriber data) to the new VLR.
 - e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).
 - f) The HLR responds with Update Location Ack (IMSI) to the new VLR.
- 5) The new VLR allocates a new VLR TMSI and responds with Location Update Accept (VLR TMSI) to the SGSN. VLR TMSI is optional if the VLR has not changed.
- 6) The SGSN validates the MS's presence in the new RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, then the SGSN rejects the routeing area update with an appropriate cause. If all checks are successful then the SGSN updates the MM context for the MS. A new P-TMSI may be allocated. The SGSN responds to the MS with Routeing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI Signature).
- 7) If a new P-TMSI or VLR TMSI was received, then the MS confirms the reallocation of the TMSIs by sending Routeing Area Update Complete (P-TMSI, VLR TMSI) message to the SGSN.
- 8) The SGSN sends TMSI Reallocation Complete (VLR TMSI) to the VLR if the VLR TMSI is confirmed by the MS.

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

If the Location Update Accept message indicates a reject, then this should be indicated to the MS, and the MS shall not access non-GPRS services until a successful Location Update is performed.

6.9.1.3.2 Combined Inter SGSN RA / LA Update

The Combined RA / LA Update (inter SGSN) procedure is illustrated in Figure 36. Each step is explained in the following list.

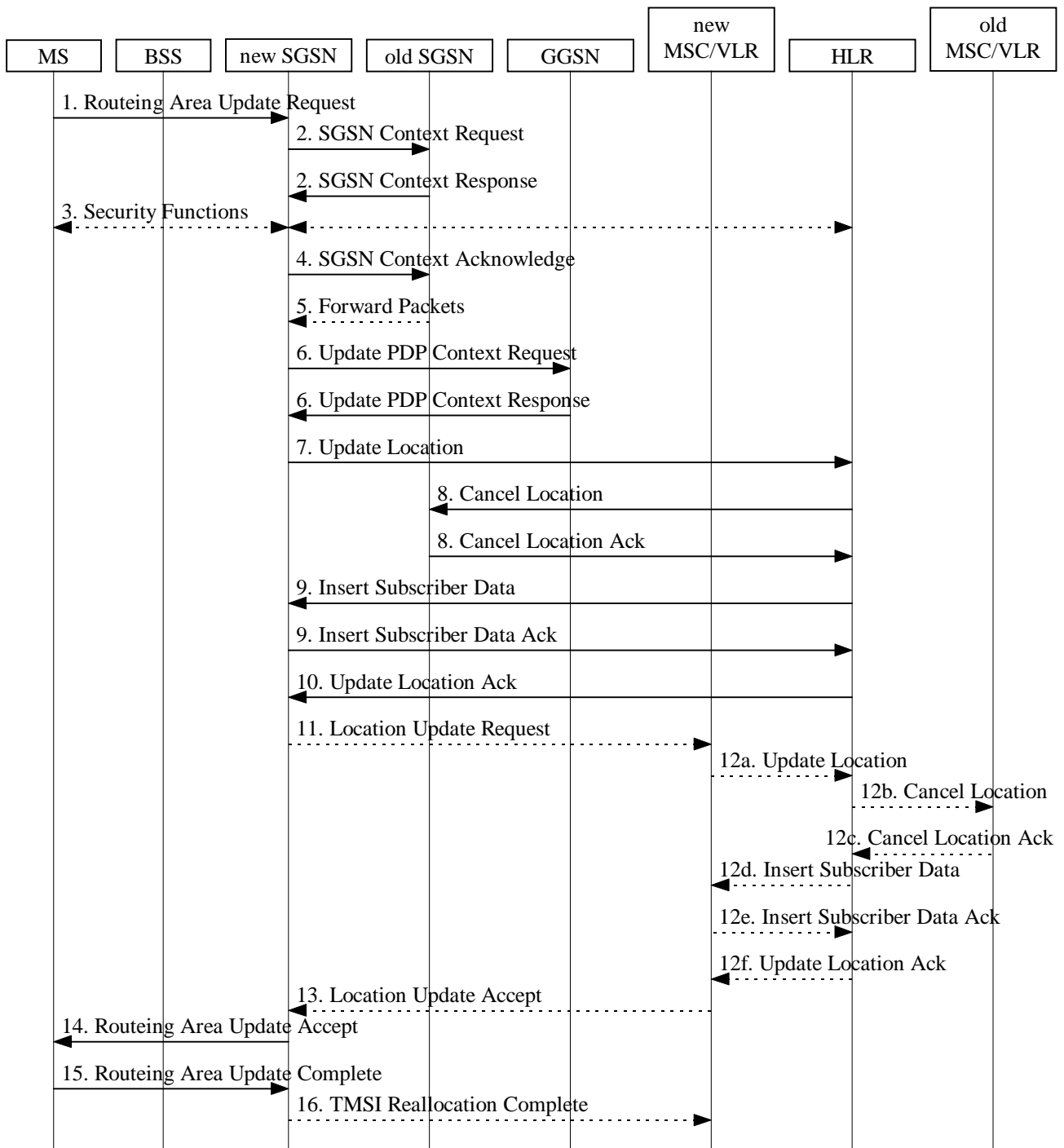


Figure 36: Combined RA / LA Update in the Case of Inter SGSN RA Update Procedure

- 1) The MS sends a Routing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the new SGSN. Update Type shall indicate combined RA / LA update, or, if the MS wants to perform an IMSI attach, combined RA / LA update with IMSI attach requested. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN.

- 2) The new SGSN sends SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) to the old SGSN to get the MM and PDP contexts for the MS. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (old RAI, TLLI, MS Validated, New SGSN Address) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN stops assigning SNDCP N-PDU numbers to downlink N-PDUs received, and responds with SGSN Context Response (MM Context, PDP Contexts). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN stores New SGSN Address until the old MM context is cancelled, to allow the old SGSN to forward data packets to the new SGSN. Each PDP Context includes the SNDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode to the MS, the SNDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode from the MS, the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled to the GGSN. The old SGSN starts a timer and stops the downlink transfer.
- 3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
- 4) The new SGSN sends an SGSN Context Acknowledge message to the old SGSN. This informs the old SGSN that the new SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure. If the security functions do not authenticate the MS correctly, then the routeing area update shall be rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received.
- 5) The old SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new SGSN. Additional N-PDUs received from the GGSN before the timer described in step 2 expires are also duplicated and tunnelled to the new SGSN. N-PDUs that were already sent to the MS in acknowledged mode and that are not yet acknowledged by the MS are tunnelled together with the SNDCP N-PDU number. No N-PDUs shall be forwarded to the new SGSN after expiry of the timer described in step 2.
- 6) The new SGSN sends Update PDP Context Request (new SGSN Address, TID, QoS Negotiated) to the GGSNs concerned. The GGSNs update their PDP context fields and return an Update PDP Context Response (TID).
- 7) The new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.
- 8) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, then the old SGSN removes the MM and PDP contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old SGSN to complete the forwarding of N-PDUs. It also ensures that the MM and PDP contexts are kept in the old SGSN in case the MS initiates another inter SGSN routeing area update before completing the ongoing routeing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).
- 9) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, the SGSN rejects the Routeing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
- 10) The HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.
- 11) If the association has to be established, if Update Type indicates combined RA / LA update with IMSI attach requested, or if the LA changed with the routeing area update, then the new SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA / LA update with IMSI attach requested. Otherwise, Location Update Type shall indicate normal location update. The VLR number is translated from the RAI via a table in the SGSN. The SGSN starts the location update procedure towards the new MSC/VLR upon

receipt of the first Insert Subscriber Data message from the HLR in step 9). The VLR creates or updates the association with the SGSN by storing SGSN Number.

- 12) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the old VLR and inserts subscriber data in the new VLR (this signalling is not modified from existing GSM signalling and is included here for illustrative purposes):
 - a) The new VLR sends an Update Location (new VLR) to the HLR.
 - b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.
 - c) The old VLR acknowledges with Cancel Location Ack (IMSI).
 - d) The HLR sends Insert Subscriber Data (IMSI, GSM subscriber data) to the new VLR.
 - e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).
 - f) The HLR responds with Update Location Ack (IMSI) to the new VLR.
- 13) The new VLR allocates a new TMSI and responds with Location Update Accept (VLR TMSI) to the SGSN. VLR TMSI is optional if the VLR has not changed.
- 14) The new SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the SGSN, or if subscription checking fails, then the SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the new SGSN establishes MM and PDP contexts for the MS. A logical link is established between the new SGSN and the MS. The new SGSN responds to the MS with Routing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure.
- 15) The MS confirms the reallocation of the TMSIs by sending Routing Area Update Complete (P-TMSI, VLR TMSI, Receive N-PDU Number) to the SGSN. Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure. If Receive N-PDU Number confirms reception of N-PDUs that were forwarded from the old SGSN, then these N-PDUs shall be discarded by the new SGSN. LLC and SNDCP in the MS are reset.
- 16) The new SGSN sends TMSI Reallocation Complete (VLR TMSI) to the new VLR if the VLR TMSI is confirmed by the MS.

In the case of a rejected routing area update operation, due to regional subscription or roaming restrictions, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

If the SGSN is unable to update the PDP context in one or more GGSNs, then the SGSN shall deactivate the corresponding PDP contexts as described in subclause "PDP Context Deactivation Initiated by SGSN Procedure". This shall not cause the SGSN to reject the routing area update.

If the routing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routing Area Update Reject (Cause) message, the MS shall enter IDLE state.

If the timer described in step 2 expires and no Cancel Location (IMSI) was received from the HLR, then the old SGSN shall stop forwarding N-PDUs to the new SGSN.

If the Location Update Accept message indicates a reject, then this should be indicated to the MS, and the MS shall not access non-GPRS services until a successful location update is performed.

6.9.2 Location Management Procedures for UMTS

Refer to UMTS 25.301 for further information on the location management procedures for the UMTS radio.

The PLMN shall provide information for the MS to be able to:

- detect when it has entered a new cell or a new RA; and

- determine when to perform periodic RA updates.

In this specification, only the Location Management procedures related to the CN are described. These procedures are:

- a routeing area update procedure; and
- SERVING RNC relocation procedure.

An MS detects that a new cell has been entered by comparing the cell's identity with the cell identity stored in the MS. The MS detects that a RA Update shall be performed by comparing the RAI stored in its MM context with the RAI received from the network. In RRC-CONNECTED mode (PMM-CONNECTED state or CS MM CONNECTED state), the MS is informed of RAI and Cell Identity by the Serving RNC via an "MM information" message at the RRC layer. In RRC-IDLE state, the MS is informed of RAI and Cell Identity by the broadcasted system information at the RRC layer.

In network mode of operation II, whenever an MS determines that it shall perform both an LA update and an RA update, the MS shall start the LA update first. The MS should start RA Update procedure before the LA update is completed.

6.9.2.1 Routeing Area Update Procedure

A routeing area update takes place when an attached MS detects that it has entered a new RA or when the periodic RA update timer has expired. The SGSN detects that it is an intra SGSN routeing area update by noticing that it also handles the old RA. In this case, the SGSN has the necessary information about the MS and there is no need to inform the GGSNs or the HLR about the new MS location. A periodic RA update is always an intra SGSN routeing area update. If the network operates in mode I, then an MS that is both PS-attached and CS-attached shall perform the Combined RA / LA Update procedures.

In UMTS, a RA Update is either intra-SGSN or inter-SGSN RA Update, either combined RA/LA update or only RA update, either initiated by an MS in PMM-CONNECTED or in PMM-IDLE state. All the RA Update cases are contained in the procedure illustrated in Figure 37. Each step is explained in the following list.

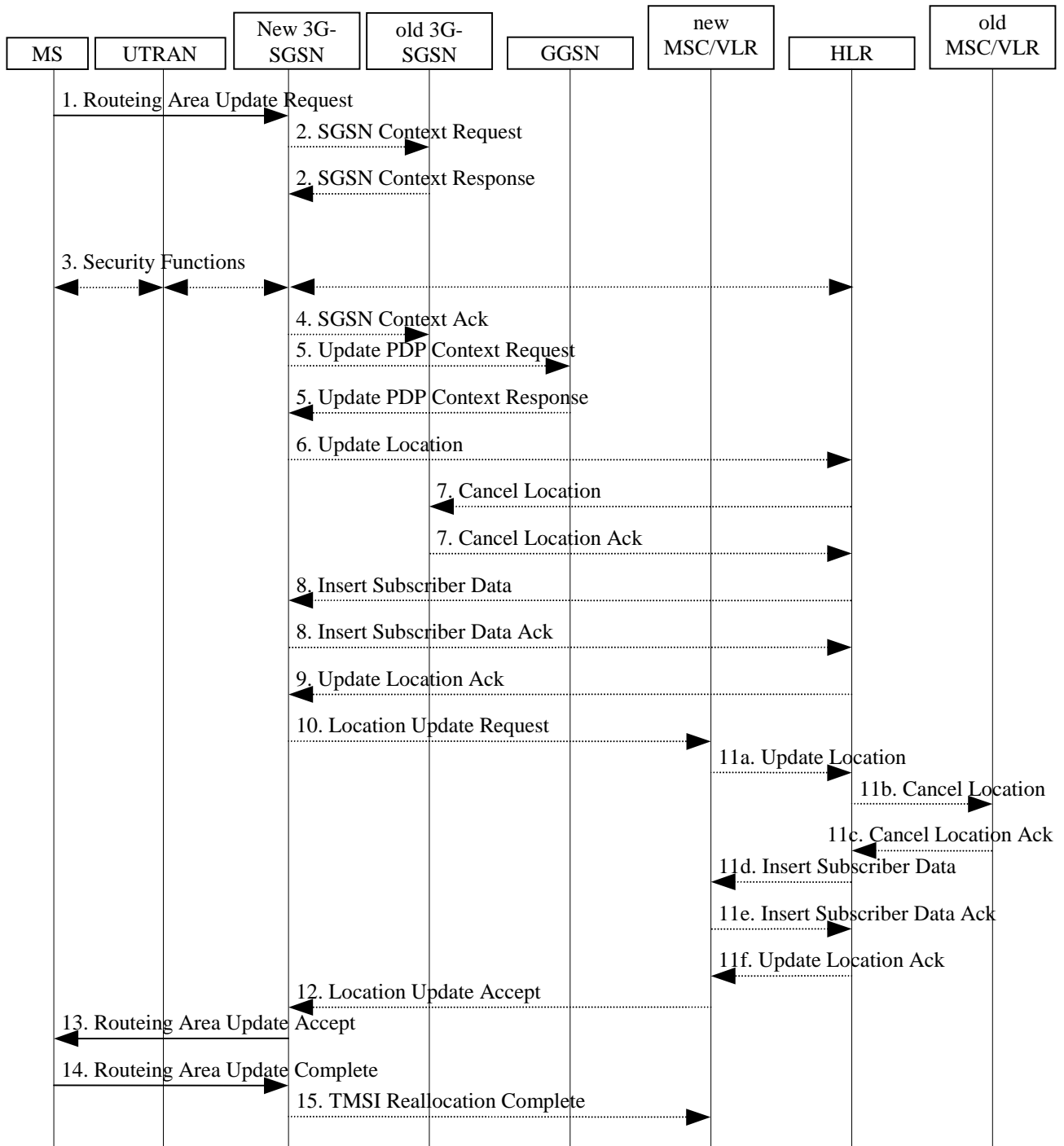


Figure 37: UMTS RA Update Procedure

- 1) The RRC connection is established, if not already done. The MS sends a Routing Area Update Request message (P-TMSI, old RAI, old P-TMSI Signature, Update Type, follow on request) to the new SGSN. Follow on request shall be set by MS if there is pending uplink traffic (signaling or user data). The SGSN may use, as an implementation option, the follow on request indication to release or keep the Iu connection after the completion of the RA update procedure. Update Type shall indicate:
 - RA Update if the RA Update is triggered by a change of RA;

- Periodic RA Update if the RA update is triggered by the expiry of the Periodic RA Update timer;
- Combined RA / LA Update if the MS is also CS attached and the LA update shall be performed in network operation mode I (see subclause "Interactions Between SGSN and MSC/VLR"); or
- Combined RA / LA Update with CS attach requested if the MS wants to perform an CS attach in network operation mode I.

The UTRAN shall add the Routing Area Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN. (FFS)

NOTE: Sending the Routeing Area Update Request message to the SGSN triggers the establishment of a signalling connection between UTRAN and SGSN for the concerned MS.

- 2) If the RA Update is an Inter-SGSN Routing area update and if the MS was in PMM-IDLE state, the new SGSN sends SGSN Context Request message (old PTMSI, old RAI, old P-TMSI Signature) to the old SGSN to get the MM and PDP contexts for the MS. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (IMSI, old RAI, MS Validated) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN responds with SGSN Context Response (Cause, IMSI, MM Context, PDP contexts). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN starts a timer.
- 3) Security functions may be executed. These procedures are defined in subclause "Security Function". If the security functions do not authenticate the MS correctly, then the routeing area update shall be rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received.
- 4) If the RA Update is an Inter-SGSN Routing area update, the new SGSN sends an SGSN Context Acknowledge message to the old SGSN. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure.
- 5) If the RA Update is an Inter-SGSN RA Update and if the MS was in PMM-IDLE state, the new SGSN sends Update PDP Context Request (new SGSN Address, QoS Negotiated, SGSN Tunnel Endpoint Identifier, GGSN Tunnel Endpoint Identifier) to the GGSNs concerned. GGSN Tunnel Endpoint Identifier is used by GGSN to identify the PDP context. The GGSNs update their PDP context fields and return an Update PDP Context Response (GGSN Tunnel Endpoint Identifier). Note: If the RA Update is an Inter-SGSN Routing area update initiated by an MS is in PMM-CONNECTED state, the update PDP Context Request is sent as described in subclause "SRNC relocation".
- 6) If the RA Update is an Inter-SGSN RA Update, the new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.
- 7) If the RA Update is an Inter-SGSN RA Update, the HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, then the old SGSN removes the MM context. Otherwise, the contexts are removed only when the timer expires. It also ensures that the MM context is kept in the old SGSN in case the MS initiates another inter SGSN routeing area update before completing the ongoing routeing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).
- 8) If the RA Update is an Inter-SGSN RA Update, the HLR sends Insert Subscriber Data (IMSI, subscription data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, the SGSN rejects the Routeing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
- 9) If the RA Update is an Inter-SGSN RA Update, the HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.

- 10) If Update Type indicates combined RA / LA update with CS attach requested, or if the LA changed with the routing area update, then the association has to be established, and the new SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate CS attach if Update Type in step 1 indicated combined RA / LA update with CS attach requested. Otherwise, Location Update Type shall indicate normal location update. The VLR number is translated from the RAI via a table in the SGSN. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 8). The VLR creates or updates the association with the SGSN by storing SGSN Number.
- 11) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the old VLR and inserts subscriber data in the new VLR (this signalling is not modified from existing GSM signalling and is included here for illustrative purposes):
- a) The new VLR sends an Update Location (new VLR) to the HLR.
 - b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.
 - c) The old VLR acknowledges with Cancel Location Ack (IMSI).
 - d) The HLR sends Insert Subscriber Data (IMSI, GSM subscriber data) to the new VLR.
 - e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).
 - f) The HLR responds with Update Location Ack (IMSI) to the new VLR.
- 12) The new VLR allocates a new TMSI and responds with Location Update Accept (VLR TMSI) to the SGSN. VLR TMSI is optional if the VLR has not changed.
- 13) The new SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the SGSN, or if subscription checking fails, then the SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the new SGSN establishes MM context for the MS. The new SGSN responds to the MS with Routing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI Signature).
- 14) The MS confirms the reallocation of the TMSIs by sending Routing Area Update Complete (P-TMSI, VLR TMSI) to the SGSN.
- 15) The new SGSN sends TMSI Reallocation Complete (VLR TMSI) to the new VLR if the VLR TMSI is confirmed by the MS.

NOTE: Steps 11, 12, and 15, are performed only if step 9 is performed.

In the case of a rejected routing area update operation, due to regional subscription or roaming restrictions, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routing area update to that RA. The RAI value shall be deleted when the MS is powered up.

If the routing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routing Area Update Reject (Cause) message, the MS shall enter PMM-DETACHED state.

If the Location Update Accept message indicates a reject, then this should be indicated to the MS, and the MS shall not access non-PS services until a successful location update is performed.

6.9.2.2 Serving RNC Relocation procedure

This procedure is only performed for MS in PMM-CONNECTED state.

The Serving RNC relocation procedure is used to move the UTRAN-CORE NETWORK connection point at UTRAN side from the Serving RNC to the target RNC. In the procedure, the Iu links are relocated. If the Target RNC is connected to the same SGSN as the Serving RNC, an intra-SGSN SERVING RNC Relocation procedure is performed. This procedure is followed by an Intra-SGSN RA Update procedure. If the Target RNC is connected to a different SGSN than the Serving RNC, an inter-SGSN SERVING RNC Relocation procedure is performed. This procedure is followed by an Inter-SGSN RA Update procedure.

Figure 38 shows SRNS relocation when source RNC and target RNC are connected to different 3G-SGSN. Figure 39 shows the situation after the procedure has been completed.

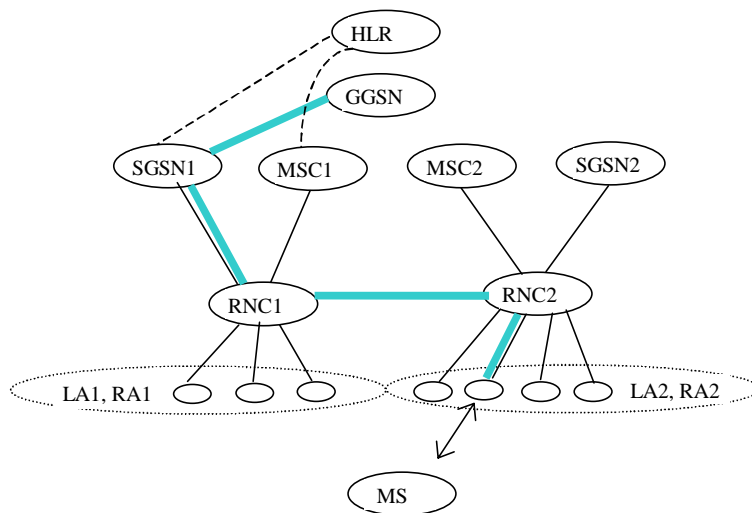


Figure 38: Before SRNS Relocation and Location Registration

Before the SRNS relocation and location registration the MS is registered in SGSN1 and in MSC1. The RNC1 is acting as SERVING RNC and the RNC2 is acting as Drift RNC.

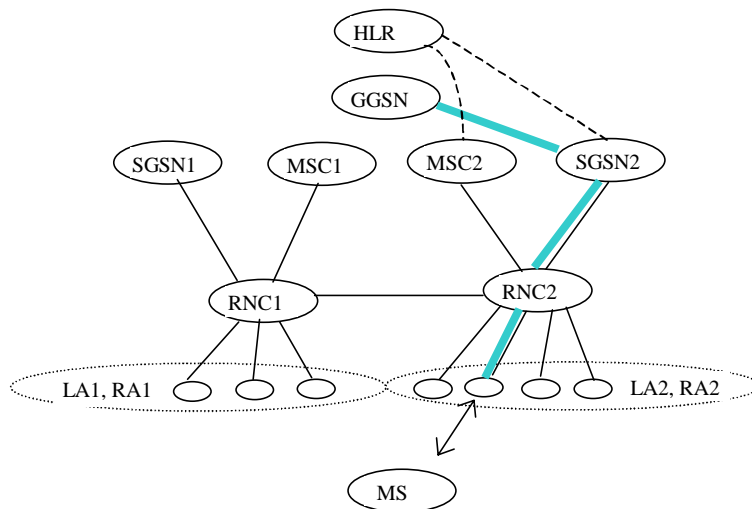


Figure 39: After SRNS Relocation and RA Update

After the SRNS relocation and RA Update, the MS is registered in MSC2 and in SGSN2. The MS is in state PMM-CONNECTED towards the SGSN2 and in state CMM-IDLE towards the MSC2. The RNC2 is acting as SERVING RNC.

The SRNS relocation procedure can be divided into 3 stages:

- 1) Resource Reservation: The path of the data traffic is not changed.
- 2) Actual handover of Serving RNC Phase: The UTRAN connection point is moved to the target RNC (new Serving RNS) and downlink traffic is forwarded from (old) Serving RNC to the Target RNC
- 3) Routing Area Update initiated by an MS is in PMM-CONNECTED state, which is described in the RA update subclause.

The SRNS relocation procedure is described in the procedure illustrated in Figure 40. Each step is explained in the following list.

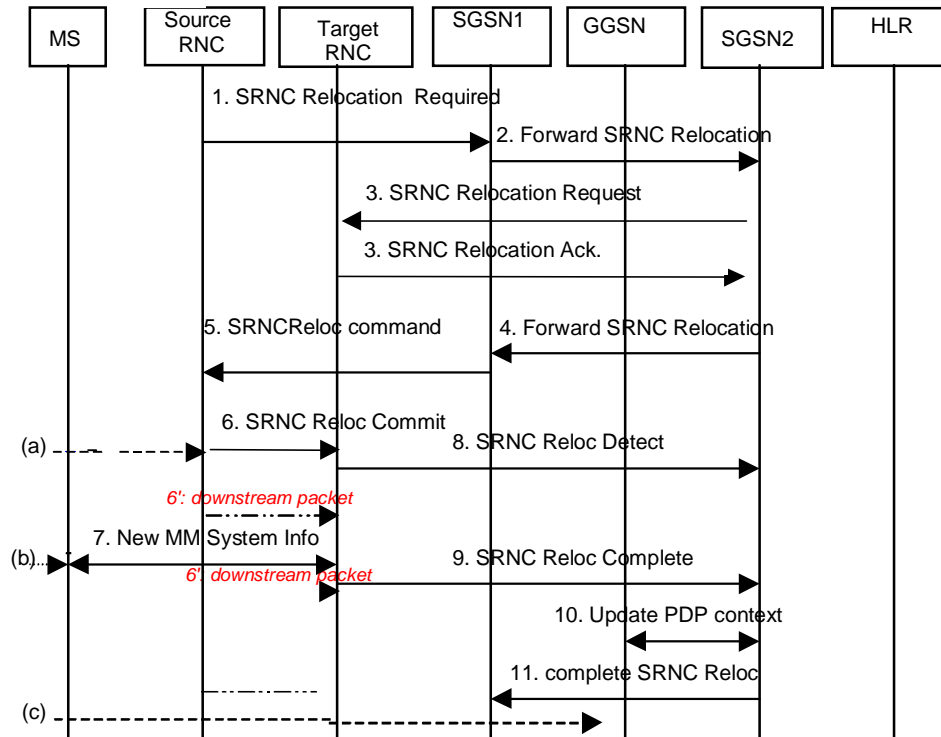


Figure 40: Phases 1 and 2 of Serving RNC Relocation

1. "Resource reservation" phase:

During this phase, the transmission of packets between GGSN and MS through the source SRNC continues.

- 1) UTRAN (source SRNC) makes the decision to perform the Serving RNC relocation procedure. This includes decision on into which RNC (Target RNC) the Serving RNC functionality is to be relocated. The source SRNC sends SRNC Relocation required message (target RNC identifier, transparent information field) to the SGSN1. Transparent information field shall be passed transparently to the target RNC.
- 2) If the SGSN1 determines from target RNC Identifier that the SRNC relocation is an inter-SGSN SERVING RNC Relocation, then SGSN1 sends a Forward SRNC relocation request to SGSN2 (target RNC identifier, transparent information field, IMSI, MM context, PDP contexts).

NOTE: Forward SRNC relocation request does not contain any information linked with packet transmission (sequence numbers) because such information is under the responsibility of the UTRAN.

- 3) The SGSN2 sends a SRNC Relocation Request message (target RNC identifier, transparent information field, IMSI) to the target RNC. When the Iu user plane transport bearers have been established, and target RNC completed its preparation phase, SRNC Relocation Acknowledge message (RNC IP address(es), and Tunnel End Point Identifier(s)) is sent to the SGSN2. The RNC IP address(es) (possibly one address per PDP context) on which the target RNC is willing to receive these packets. Tunnel End Point Identifier(s) are the Identifiers to be used in GTP level when sending packets to this RNC.
- 4) When the traffic resources between target RNC and SGSN2 has been allocated and the SGSN2 is ready for the SRNC move, then the Forward SRNC Relocation Response message (RNC IP address(es), and Tunnel End Point Identifier(s)) is sent from SGSN2 to SGSN1. This message indicates that SGSN2 / target RNC are ready to receive from source SRNC the downstream packets not yet acknowledged by MS.
- 5) When the Forward SRNC Relocation Response has been received in the SGSN1, the SGSN1 indicates the completion of preparation phase at the CN PS domain side for the SRNC relocation by sending the SRNC

Relocation Command message (RNC IP address(es), and Tunnel End Point Identifier(s)) to the Source RNC. The RNC IP address(es), and Tunnel End Point Identifier(s) are used by SRNC to send the downstream packets not yet acknowledged by MS to the target RNC.

2. "Actual handover of Serving RNC" phase:

- 6) When the source RNC has received the SRNC Relocation Proceeding 2 message, the source RNC sends a SRNC Relocation Commit message to the target RNC(list of (SNU, UP-RLC-ack, SND)). SND is the GTP sequence number for the next downlink packet received from the GGSN. SNU is the GTP sequence number for the next uplink packet to be tunnelled to the GGSN. UP-RLC-Ack contains the acknowledgements for upstream PDU received by the source SRNC on each RLC connection used by the MS (i.e. the Receive State Variable V(R) for all RLC SAPI in acknowledged mode). The source SRNC starts a timer T3-TUNNEL , stops the exchange of the packets with the MS (point (a)), and starts tunnelling the buffered and incoming downstream packets towards the target SRNC using RNC IP address(es), and Tunnel End Point Identifier(s). The target RNC executes switch for all bearers at the earliest suitable time instance.
 - 7) The target RNC starts acting as SRNC. The target SRNC:
 - Restarts the RLC connections. This includes the exchange between the target SRNC and the MS of the UP-RLC-Ack and DOWN-RLC-ACK. DOWN-RLC-ACK confirms all mobile-terminated packets successfully transferred before the start of the relocation procedure. If DOWN-RLC-ACK confirms reception of packets that were forwarded from the source SRNC, then these packets shall be discarded by the target SRNC. UP-RLC Ack confirms all mobile-originated packets successfully transferred before the start of the relocation procedure. From now on the exchange of the packets with the MS can restart (point (b)).
 - Sends New MM System Information to the MS indicating e.g. relevant Routing Area and Location Area. Additional RRC information may then also be sent to the MS, e.g. new RNTI identity. The new RAI triggers a RA Update procedure (case initiated by MS in PMM-CONNECTED state). This is point (c). The uplink traffic shall not be stopped due to the new MM System Information or the RA Update procedure.
- NOTE: The new SGSN may send uplink packets to the GGSN before the update PDP context is performed.
- 8) Immediately after a successful switch at RNC, target RNC (=SRNC) sends SRNC Relocation Detect message to the SGSN2.
 - 9) After sending out the New MM System Information, the target RNC sends an SRNC relocation complete to SGSN2. In case of intra-SGSN SERVING RNC Relocation, the SGSN use this indication to send an Iu release message to old SRNC.
 - 10) If the SRNC relocation is an Inter-SGSN SRNC relocation, the new SGSN sends Update PDP Context Request (new SGSN Address, QoS Negotiated, SGSN Tunnel Endpoint Identifier, GGSN Tunnel Endpoint Identifier) to the GGSNs concerned. GGSN Tunnel Endpoint Identifier is used by GGSN to identify the PDP context. The GGSNs update their PDP context fields and return an Update PDP Context Response (GGSN Tunnel Endpoint Identifier).
 - 11) If the SRNC relocation is an Inter-SGSN SRNC relocation, the new SGSN sends Complete SERVING RNC relocation message (IMSI) to the old SGSN when all GGSNs have been updated.

6.9.3 Periodic RA and LA Updates

All PS-attached MSs, except GPRS MSs in class-B mode of operation engaged in CS communication, shall perform periodic RA updates. MSs that are CS-attached and not PS-attached shall perform periodic LA updates. Periodic RA updates are equivalent to intra SGSN routing area updates as described in subclause "Intra SGSN Routing Area Update", with Update Type indicating periodic RA update. For MSs that are both CS-attached and PS-attached, the periodic updates depend on the mode of operation of the network:

- If the network operates in mode I, periodic RA updates shall be performed, and periodic LA updates shall not be performed. In this case, the MSC/VLR shall disable implicit detach for PS-attached MSs and instead rely on the SGSN to receive periodic RA updates. If periodic RA updates are not received in the SGSN and the SGSN detaches the MS, the SGSN shall notify the MSC/VLR by sending an IMSI Detach Indication message.
- If the network operates in mode II or mode III, both periodic RA updates and periodic LA updates shall be performed independently. RA updates are performed towards the SGSN, and LA updates are performed towards the MSC/VLR.

For GPRS, the periodic RA update timer in the MS is stopped when an LLC PDU is sent since all sent LLC PDUs set the MM context state to READY. The periodic RA update timer is reset and started when the state returns to STANDBY.

For UMTS, the periodic RA update timer in the MS is stopped when the MM context enters the PMM-CONNECTED state. The periodic RA update timer is reset and started when the state returns to PMM-IDLE state.

If the MS could not successfully complete the periodic RA update procedure after a retry scheme while the MS was in PS coverage, then the MS shall wait a backoff time equal to the periodic LA update timer broadcast by the network before re-starting the periodic RA update procedure.

6.10 Tunnelling of non-GSM Signalling Messages Function

This subclause applies to GPRS only.

Tunnelling of Messages (TOM) is an optional protocol layer that uses the LLC unacknowledged mode procedures to tunnel messages between the MS and the SGSN (see GSM 04.64). TOM uses two LLC SAPs for communication between the MS and the SGSN; one for high-priority messages and one for low-priority messages. A network that supports TIA/EIA-136 [49] shall support the TOM protocol and the Gs interface.

Upon receiving a non-GSM signalling message from an MS via the TOM protocol, the SGSN forwards the message to a non-GSM MSC/VLR using the BSSAP+ protocol (see GSM 09.18). The specific Gs interface used by the SGSN is determined by the:

- RAI associated with the current location of the MS; and
- information in the TOM protocol header.

Upon receiving a non-GSM signalling message from a non-GSM MSC/VLR via the BSSAP+ protocol, the SGSN forwards the message to a specific MS using the TOM protocol. The specific MS is determined by the SGSN based on the content of the BSSAP+ header.

The control plane between an MS and a non-GSM MSC/VLR that uses tunnelling procedures for non-GSM signalling is shown in Figure 41:

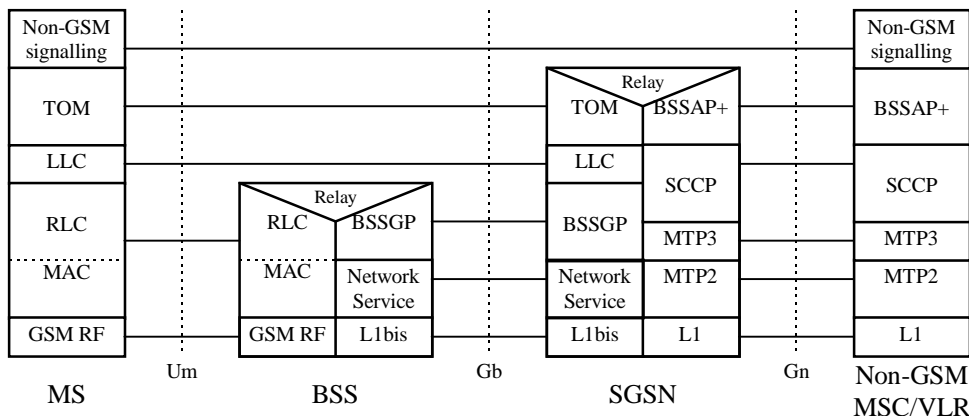


Figure 41: Control Plane MS - Non-GSM MSC/VLR

6.10.1 Uplink Tunnelling of non-GSM Signalling Messages Procedure

The Uplink Tunnelling of non-GSM Signalling Messages procedure is illustrated in Figure 42. Each step is explained in the following list.

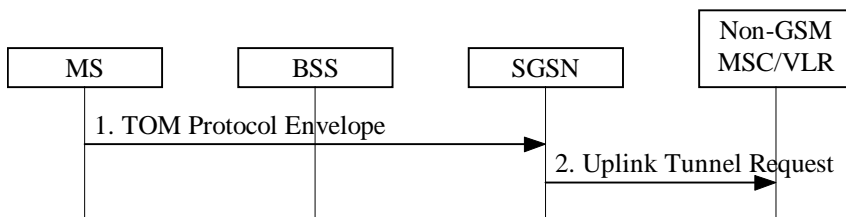


Figure 42: Uplink Tunnelling of non-GSM Signalling Messages Procedure

- 1) The MS sends a TOM Protocol Envelope (Non-GSM Signalling Message) to the SGSN either in ciphered or clear mode. The TOM protocol header contains information about the application using the TOM facility and any other TOM Protocol Discriminator-specific information. The TOM Protocol Envelope is received on one of the two LLC SAPs used for tunnelling of messages.
- 2) The SGSN identifies the non-GSM MSC/VLR to which to forward the non-GSM signalling message. It then sends a BSSAP+ Uplink Tunnel Request (IMSI, SGSN Address, TOM Priority, Cipher, Non-GSM Signalling Message) message to the identified non-GSM MSC/VLR. The Cipher parameter is set to cipher if the TOM Protocol Envelope was received by the LLC layer in ciphered form, otherwise it is set to not cipher. TOM Priority is set to high priority if the TOM Protocol Envelope was received on the high-priority LLC SAP, otherwise it is set to low priority.

6.10.2 Downlink Tunnelling of non-GSM Signalling Messages Procedure

The Downlink Tunnelling of non-GSM Signalling Messages procedure is illustrated in Figure 43. Each step is explained in the following list.

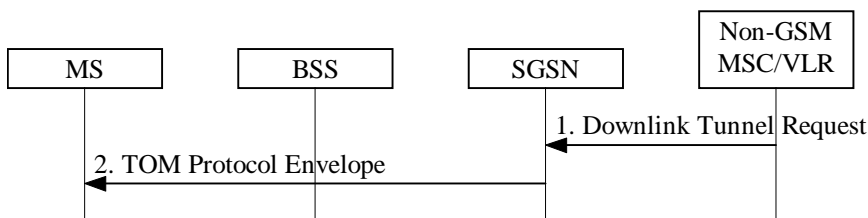


Figure 43: Downlink Tunnelling of non-GSM Signalling Messages Procedure

- 1) The non-GSM MSC/VLR sends a BSSAP+ Downlink Tunnel Request (IMSI, VLR Address, TOM Priority, Cipher, Non-GSM Signalling Message) message to the SGSN associated with the MS. TOM Priority indicates whether the SGSN shall select the high-priority or low-priority LLC SAP when forwarding the non-GSM signalling message to the MS. Cipher indicates whether or not the SGSN shall cipher the non-GSM signalling message before forwarding it to the MS.
- 2) The SGSN sends a TOM Protocol Envelope (Non-GSM Signalling Message) to the MS using the selected LLC SAP.

6.11 Subscriber Management Function

The Subscriber Management function provides a mechanism to inform the nodes about changes of the PS subscription data for a specific PS subscriber.

6.11.1 Subscriber Management Procedures

Whenever the PS subscription data is changed for a PS subscriber in the HLR, and the changes affect the PS subscription data stored in the SGSN, then the SGSN node shall be informed about these changes by means of the following procedures:

- Insert Subscriber Data procedure, used to add or modify PS subscription data in the SGSN; or
- Delete Subscriber Data procedure, used to remove PS subscription data in the SGSN.

6.11.1.1 Insert Subscriber Data Procedure

In addition to the insertion and modification of general PS subscription data for a PS subscriber, see GSM 09.02, the HLR may request the insertion or modification of one or several new or existing PDP contexts in the SGSN. It should be noted that the modification may trigger a PDP Context Modification procedure as described in subclause "Modification Procedures". In particular, the following PDP context parameters may be modified by the HLR:

- QoS Profile Subscribed; and
- VPLMN Address Allowed.

The Insert Subscriber Data procedure is illustrated in Figure 44. Each step is explained in the following list.

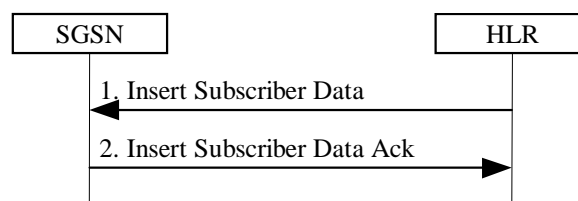


Figure 44: Insert Subscriber Data Procedure

- 1) The HLR sends an Insert Subscriber Data (IMSI, PS Subscription Data) message to the SGSN.
- 2) The SGSN updates its PS subscription data and acknowledges the Insert Subscriber Data message by returning an Insert Subscriber Data Ack (IMSI) message. For each PDP context that is included in PS Subscription Data the SGSN shall check whether it is a new, an active, or an inactive PDP context:
 - For a new or inactive PDP context, no further action is required except storage in the SGSN.
 - For an active PDP context, the SGSN shall in addition compare the new QoS Subscribed with QoS Negotiated and shall, if necessary, initiate a PDP Context Modification procedure as described in subclause "Modification Procedures". Furthermore, if VPLMN Address Allowed is changed, the SGSN shall, if necessary (e.g., if the PDP context is currently routed via a GGSN in the VPLMN and VPLMN Address Allowed is changed to not allowed), initiate a PDP Context Deactivation procedure as explained in subclause "Deactivation Procedures".

6.11.1.2 Delete Subscriber Data Procedure

In addition to the deletion of general GPRS subscription data for a GPRS subscriber, see GSM 09.02, the HLR may request the deletion of one or several PDP contexts from the SGSN.

The Delete Subscriber Data procedure is illustrated in Figure 45. Each step is explained in the following list.

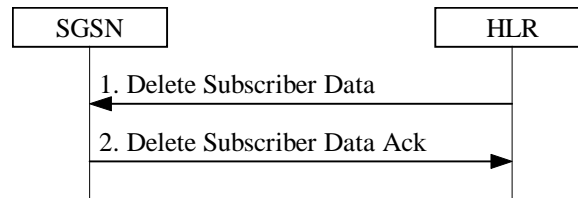


Figure 45: Delete Subscriber Data Procedure

- 1) The HLR sends a Delete Subscriber Data (IMSI, PDP Context Identifiers List) message to the SGSN.
- 2) The SGSN acknowledges the Delete Subscriber Data message by returning a Delete Subscriber Data Ack (IMSI) message. For each PDP context identifier included in PDP Context Identifiers List, the SGSN shall check whether it belongs to an active or an inactive PDP context:
 - For an inactive PDP context no further action is required except deletion of the PDP context.
 - For an active PDP context, the SGSN shall initiate the PDP Context Deactivation Initiated by SGSN procedure as explained in subclause "Deactivation Procedures" before the PDP context is deleted.

6.12 Service Request Procedure for UMTS

The Service Request procedure is used by a 3G-MS in PMM-IDLE state to request the establishment of a secure connection to a 3G-SGSN. The MS in PMM-IDLE state initiates this procedure in order to send uplink signalling messages (e.g., Activate PDP Context Request) or user data. This procedure is also used by an MS in PMM-CONNECTED state to request resource reservation for active PDP contexts.

6.12.1 Service Request Initiated by MS Procedure

The MS in PMM-IDLE state sends the Service Request message to the 3G-SGSN in order to establish the PS signalling connection for the upper layer signalling or for the resource reservation for active PDP contexts. After receiving the Service Request message the 3G-SGSN may perform authentication and it shall perform the security mode procedure. After the establishment of the secure PS signalling connection to a 3G-SGSN the MS may send signalling messages, e.g., Activate PDP Context Request, to the 3G-SGSN, or the 3G-SGSN may start the resource reservation for the active PDP contexts depending on the requested service in the Service Request message. This procedure is also used by an MS in PMM-CONNECTED state to request the resource reservation for the active PDP contexts.

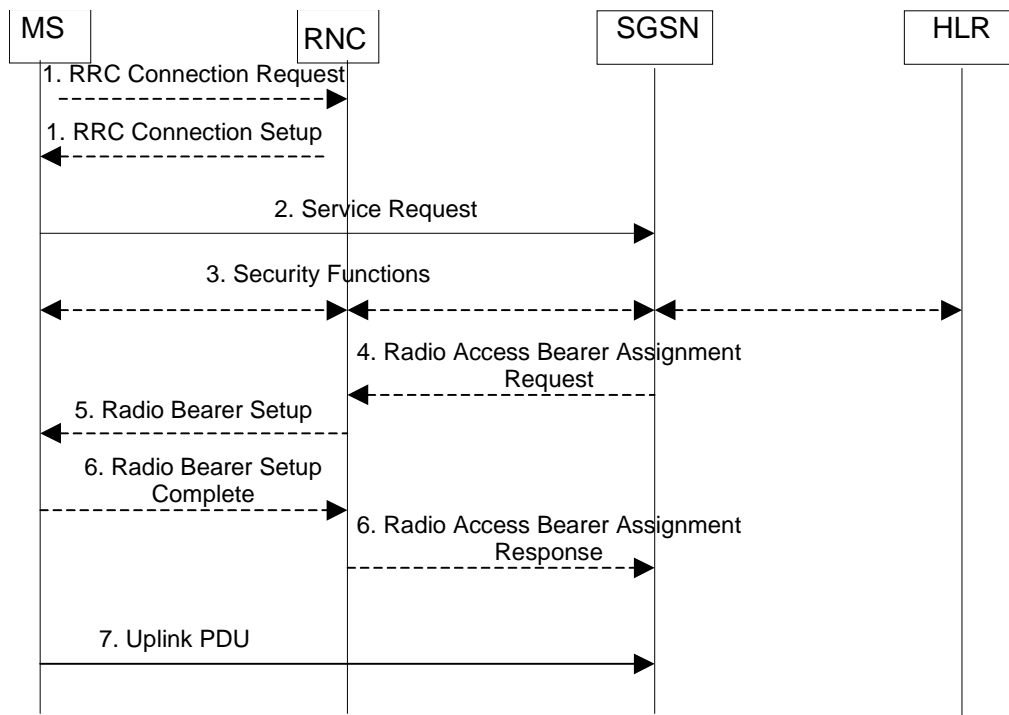


Figure 46: Service Request Initiated by MS Procedure

- 1) The MS establishes an RRC connection, if none exists for CS traffic.
- 2) The MS sends a Service Request (P-TMSI, P-TMSI Signature, RAI, CKSN, Service Type) message to the SGSN. Service Type specifies the requested service. Service Type shall indicate one of the following: Data or Signalling. At this point, the SGSN may perform the authentication procedure.

If Service Type indicates Data then a signalling connection is requested established between the MS and the SGSN, and resources for active PDP context(s) are requested allocated, i.e., RAB establishment for the activated PDP context(s).

If Service Type indicates Signalling then the signalling connection is requested established between the MS and the SGSN for sending upper-layer signalling messages, e.g., Activate PDP Context Request. The resources for active PDP context(s) are not requested allocated.

- 3) The SGSN shall perform the security functions if the service request was initiated by an MS in PMM-IDLE state.
- 4) In case Service Type indicates Data, the SGSN sends a Radio Access Bearer Assignment Request (NSAPI(s), Tunnel Identity(ies), QoS Profile(s), SGSN IP Address(es)) message to re-establish radio access bearer for every activated PDP context.
- 5) The RNC indicates to the MS the new Radio Bearer Identity established and the corresponding NSAPI with the RRC radio bearer set up procedure.
- 6) SRNC responds with the Radio Access Bearer Assignment Response (NSAPI(s), Tunnel Identity(ies), QoS Profile(s), RNC IP Address(es)) message. The GTP tunnel(s) are established on the Iu interface.
- 7) The MS sends the uplink packet.

The MS knows that the Service Request message was successfully received in the SGSN when the MS receives the RRC Security Mode Control Command message. It is, however, possible that the security mode procedure is not performed, e.g., if the Service Request message indicating Service Type = Data is sent after an RA update procedure via the same PS signalling connection. For such cases, the Service Accept message may be needed and it should be treated by the MS as a service acceptance indication.

If the service request cannot be accepted, the network returns a Service Reject message to the mobile station.

6.12.2 Service Request Initiated by Network Procedure

When the 3G-SGSN receives a downlink packet (e.g., Request PDP Context Activation, MT SMS, user data) for an MS in PMM-IDLE state, the 3G-SGSN sends a paging request to UTRAN. The paging request triggers the Service Request procedure in the UMS

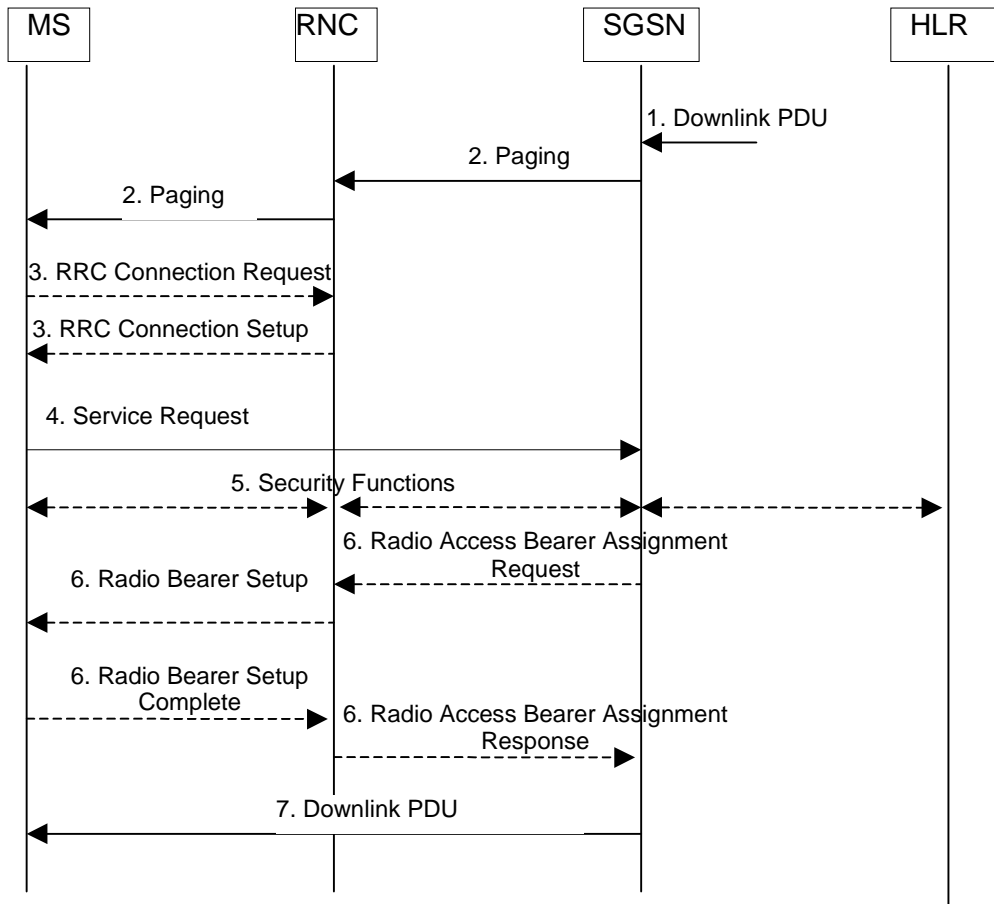


Figure 47: Service Request Initiated by Network Procedure

- 1) The SGSN receives a downlink PDP PDU for an MS in PMM-IDLE state.
- 2) The SGSN sends a Paging (IMSI, P-TMSI, RAI, Paging Cause) message to the RNC. The RNC pages the MS by sending a Paging (P-TMSI or IMSI, Paging Cause) message to the MS.
- 3) The MS establishes an RRC connection if none exists for CS traffic.
- 4) The MS sends a Service Request (P-TMSI, P-TMSI Signature, RAI, CKSN, Service Type) message to the SGSN. Service Type specifies Paging Response. The Service Request is carried over the radio in an RRC Direct Transfer message and over the Iu interface in the RANAP Initial MS message. At this point, the SGSN may perform the authentication procedure. The SGSN knows whether the downlink packet requires RAB establishment (e.g., downlink PDU) or not (e.g., Request PDP Context Activation or MT SMS).
- 5) The SGSN shall perform the security mode procedure.
- 6) If resources for the PDP contexts are re-established, the SGSN sends a Radio Access Bearer Assignment Request (NSAPI(s), Tunnel Identity(ies), QoS Profile(s), SGSN IP Address(es)) message to the RNC. The RNC sends a Radio Access Bearer Setup (RAB Identity, NSAPI) to the MS. The MS responds by returning a Radio Access Bearer Complete message to the RNC. The RNC sends a Radio Access Bearer Assignment Response (NSAPI(s), Tunnel Identity(ies), QoS Profile(s), RNC IP Address(es)) message to the SGSN in order to indicate that GTP tunnels are established on the Iu interface and radio access bearers are established between the RNC and the MS.

7) The SGSN sends the downlink packet.

6.13 UMTS-GPRS Intersystem Handover

The UMTS-GPRS inter system handover procedures may be supported for network elements supporting GSM Releases 97, 99 and UMTS Release 99. At intersystem handover the release 99 network elements shall use on the Gn interface the GTP version 97 when interworking with release 97 network elements.

[It appears the above forgets release 98]

An intersystem handover from UMTS to GPRS or GPRS to UMTS takes place when an MS supporting both UMTS and GPRS moves to a cell where the radio technology which the MS was using is not any longer supported. Prerequisite for an inter system handover is that the MS is PS-attached in the UMTS PS domain or PS-attached for GPRS. The transition of the mobility management states is as specified for the corresponding mobility management procedures.

There is no transition of the session management states at an intersystem handover.

6.13.1 Intersystem Handover within an RA between Cells in Different Systems

Inter-system handover without performing a RA update is supported only in case the SGSN is a combined 2G/3G-SGSN supporting both the Gb and Iu PS interfaces within the same physical node.

6.13.1.1 UMTS to GPRS Handover

An Inter System handover from UMTS to GPRS takes place when the MS in PMM-CONNECTED state enters a new GSM/GPRS cell inside the current RA. In this case the MS shall perform a Routing Area Update procedure with the Update Type set to 'Inter System Cell Change'.

The SGSN records this MS's change of cell, and further traffic directed towards the MS is conveyed over the Gb interface to the new cell.

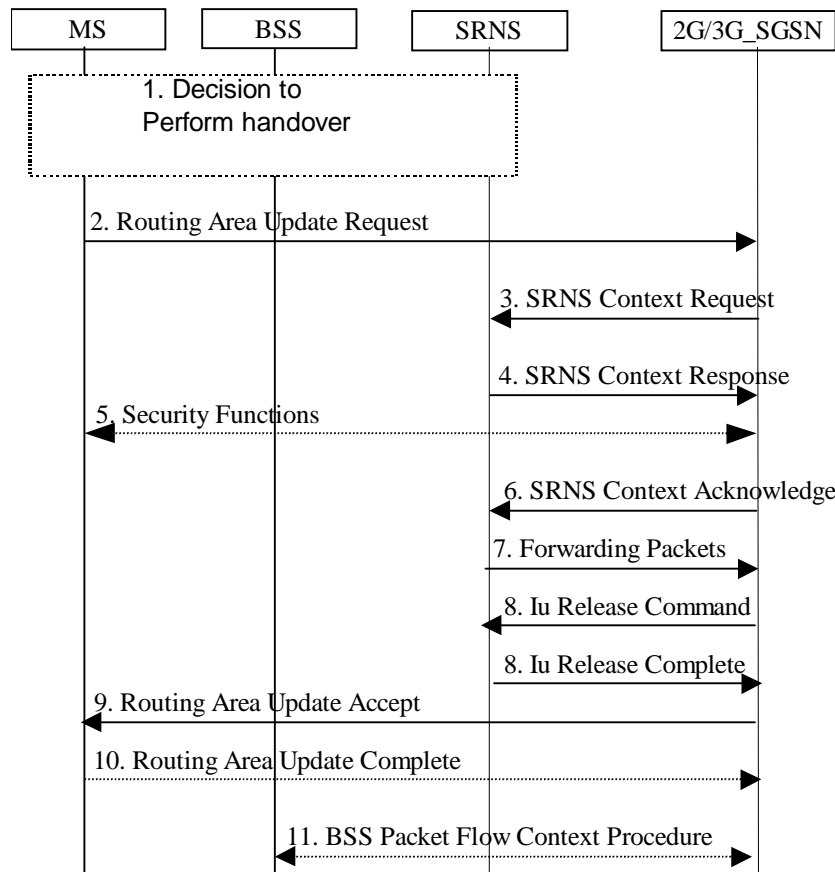


Figure 48: UMTS to GPRS Handover Between Cells in same RA

- 1) The MS and/or BSS/UTRAN decides to perform handover which leads to that the MS switches to the new cell supporting GPRS radio technology and suspends PDU transmission to the network
- 2) The MS sends a Routing Area Update Request (old RAI, old P-TMSI Signature, Update type) to the 2G/3G-SGSN. Update Type shall indicate 'Inter system cell change'. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the 2G/3G-SGSN.
- 3) The 2G/3G-SGSN sends SRNS Context Request (IMSI) to the SRNS, starts a timer on the MM and PDP Context and stops the transmission of GTP PDUs to the SRNS.
- 4) The SRNS responds with SRNS Context Response (IMSI, GTP SNDs, GTP SNU, RLC counters). The GTP sequence numbers are included for each PDP context indicating the next downlink PDU to be sent to the MS (i.e. the last GTP PDU in the buffer of the SRNS, which is not sent to the MS) and the next GTP PDU to be tunnelled to the GGSN. For each active PDP context the SRNS also includes the uplink and downlink RLC counters for PDP contexts using acknowledged mode.
- 5) Security functions may be executed.
- 6) The 2G/3G-SGSN sends SRNS Context Acknowledge to the SRNS. This informs the SRNS that the 2G/3G-SGSN is ready to receive data packets.
- 7) The buffered downlink GTP PDUs are tunnelled back to the 2G/3G-SGSN.
- 8) When the timer described under 3 has expired, the 2G/3G-SGSN sends an Iu Release Command to the SRNS. The SRNS responds with Iu Release Complete.
- 9) The 2G/3G-SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, then the 2G/3G-SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the 2G/3G-SGSN updates MM and PDP contexts for the MS. A new P-TMSI may be allocated. A Routing Area Update Accept (P-TMSI, P-TMSI Signature, Receive N-PDU Number) is returned to the MS. Receive N-PDU Number contains the

acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure. The 2G/3G-SGSN deduces the N-PDU Numbers from the RLC numbers received from the SRNS (FFS).

10) The MS acknowledges the new P-TMSI with a Routing Area Update Complete (P-TMSI, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure.

11) The 2G/3G-SGSN and the BSS may execute the BSS Packet Flow Context Procedure.

6.13.1.2 GPRS to UMTS Handover

An Inter System handover from GPRS to UMTS takes place when a PS-attached MS enters a new UMTS cell inside the current RA. In this case the MS shall perform a UMTS Inter System Cell Change procedure by performing a RRC connection establishment and an Intra SGSN Routing Area Update procedure with the Update Type set to 'Inter System Cell Change'.

The SGSN records this MS's change of cell, and further traffic directed towards the MS is conveyed over the Iu interface to the new cell.

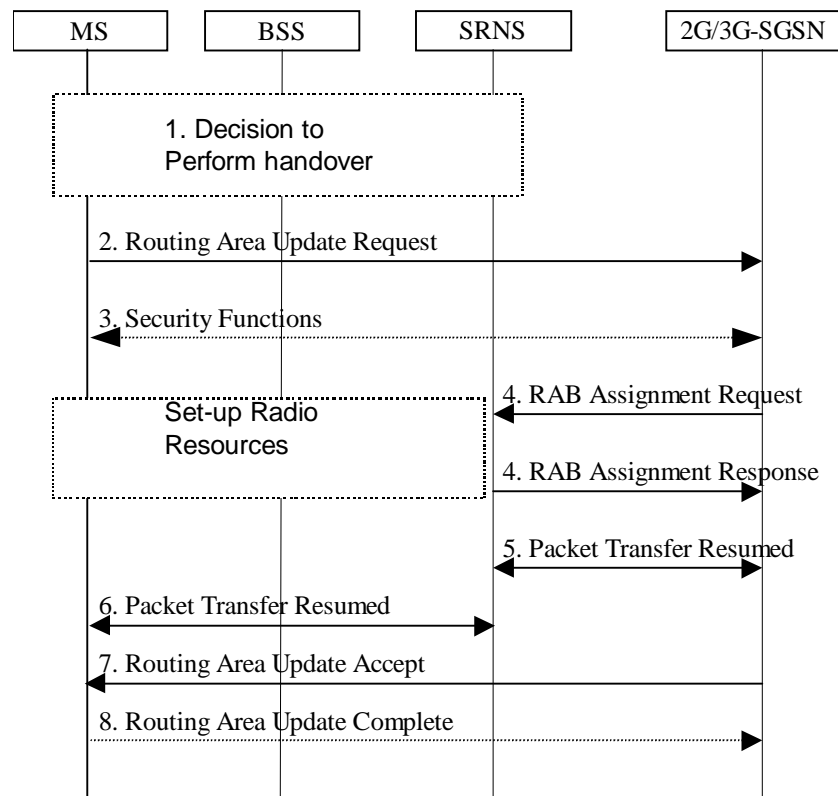


Figure 49: GPRS to UMTS Handover Between Cells in same RA

- 1) The MS and/or BSS/UTRAN decides to perform handover which leads to that the MS switches to the new cell supporting UMTS radio technology and Suspend PDU Transmission to the Network.
- 2) The MS initiate a RRC connection establishment and sends Routing Area Update Request (Old RA, Old P-TMSI Signature, Update Type, CM) to the combined 2G/3G-SGSN. The SRNS shall add an identifier of the area where the message was received before passing the message to the 2G/3G-SGSN. The 2G/3G-SGSN stops the transmission of N-PDUs to the MS.
- 3) Security functions may be executed.
- 4) The 2G/3G-SGSN request the SRNS to establish of a radio access bearer by sending RAB Assignment Request to the SRNS. The SRNS responds with RAB Assignment Response.

- 5) The traffic flow is resumed between the 2G/3G-SGSN and the SRNS
- 6) The traffic flow is resumed between the SRNS and the MS.
- 7) The 2G/3G-SGSN updates the MM context for the MS. A new P-TMSI may be allocated. A Routing Area Update Accept (P-TMSI, P-TMSI Signature, Receive N-PDU Number (FFS)) is returned to the MS.
- 8) The MS acknowledges the new P-TMSI with a Routing Area Update Complete (P-TMSI, Receive N-PDU Number (FFS)).

6.13.2 Intersystem Handover at RA Change

6.13.2.1 UMTS to GPRS Handover

An inter system handover from UMTS to GPRS takes place when the MS in PMM-IDLE or PMM-CONNECTED state moves to a new GSM/GPRS cell in a new RA. In this case the MS shall initiate a GPRS RA update procedure. The sequence applied for the inter SGSN RA update case is shown in the following figure:

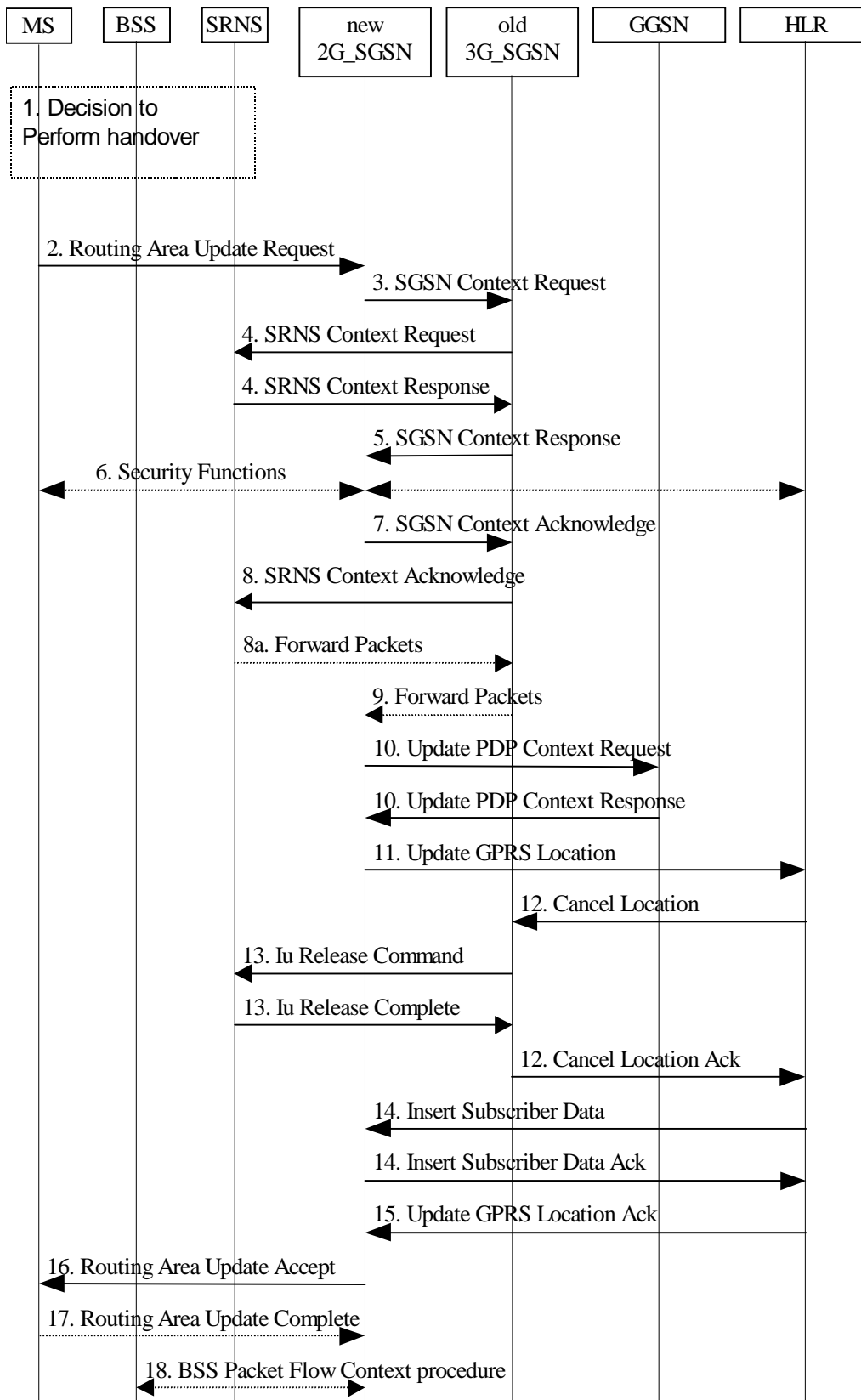


Figure 50: UMTS to GPRS Inter SGSN Routing Area Update Procedure

- 1) The MS and/or BSS/UTRAN decides to perform handover, which leads to that the MS switch to the new cell supporting GPRS radio technology and that the PDU transmission is suspended.
- 2) The MS sends a Routing Area Update Request (old RAI, old P-TMSI Signature, Update type) to the new 2G-SGSN. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global

- Identity including the RAC and LAC of the cell where the message was received before passing the message to the new 2G-SGSN.
- 3) The new 2G-SGSN sends SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) to the old 3G-SGSN to get the MM and PDP contexts for the MS. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old 3G-SGSN. The old 3G-SGSN starts a timer for supervision of the MS's context. If the MS is not known in the old 3G-SGSN, the old 3G-SGSN responds with an appropriate error cause.
 - 4) The old 3G-SGSN sends SRNS Context Request (IMSI) to the SRNS. Upon reception of this message the SRNS buffers and stops sending downlink PDUs to the MS and answers with SRNS Context Response (IMSI, GTP SNDs, GTP SNUs, RLC counters). The SRNS shall include for each PDP context the GTP sequence number of the next GTP sequence number to be sent in downlink to the MS (i.e. the last not yet transferred N-PDU) and the GTP sequence number of the next uplink PDU to be tunnelled to the GGSN. For each active PDP context the SRNS also includes the uplink and downlink RLC transmission counters for PDP contexts using acknowledged mode (FFS).
 - 5) The old 3G-SGSN responds with SGSN Context Response (MM Context, e.g. IMSI, PDP Contexts, e.g. APN). For each PDP context the old 3G-SGSN shall include the GTP sequence number for the next uplink GTP-U PDU to be tunnelled to the GGSN and the next downlink GTP sequence number for the next N-PDU to be sent to the MS. Each PDP Context also includes the SNDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode to the MS, the SNDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode from the MS. The SNDCP N-PDU numbers are derived from the RLC counters received from the SRNS (FFS).
 - 6) Security functions may be executed.
 - 7) The new 2G-SGSN sends an SGSN Context Acknowledge message to the old 3G-SGSN. This informs the old 3G-SGSN that the new 2G-SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a RA update procedure back to the old SGSN before completing the ongoing RA update procedure.
 - 8) The old 3G-SGSN sends SRNS Context Acknowledge (IMSI) to the SRNS.
 - 8a) The SRNS shall start duplicating and tunnelling the buffered GTP-U PDUs to the old 3G-SGSN.
 - 9) The old 3G-SGSN tunnels the GTP-U PDUs to the new 2G-SGSN. No SNDCP sequence numbers shall be included in the GTP header of the tunnelled PDUs.
 - 10) The new 2G-SGSN sends Update PDP Context Request (new SGSN Address, TID, QoS Negotiated) to the GGSN(s) concerned. The GGSN (s) updates its PDP context fields and returns Update PDP Context Response (TID).
 - 11) The new 2G-SGSN informs the HLR of the change of SGSN by sending Update GPRS Location (SGSN Number, SGSN Address, IMSI) to the HLR.
 - 12) The HLR sends Cancel Location (IMSI) to the old 3G-SGSN. The old 3G-SGSN acknowledges with Cancel Location Ack (IMSI). The old 3G-SGSN removes the MM and PDP contexts if the timer described in step 3 is not running. When the timer is running the MM and PDP contexts are removed when the timer expires.
 - 13) When the timer described in step 3 expires the old 3G-SGSN sends an Iu Release Command to the SRNS. The SRNS responds with Iu Release Complete.
 - 14) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new 2G-SGSN. The 2G-SGSN constructs a MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
 - 15) The HLR acknowledges the Update Location by sending Update GPRS Location Ack (IMSI) to the new 2G-SGSN.
 - 16) The new 2G-SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the 2G-SGSN, or if subscription checking fails, then the new 2G-SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the new 2G-SGSN constructs MM and PDP contexts for the MS. A logical link is established between the new 2G-SGSN and the MS. The new

2G-SGSN responds to the MS with Routing Area Update Accept (P-TMSI, P-TMSI Signature Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure.

17) The MS acknowledges the new P-TMSI with a Routing Area Update Complete (P-TMSI, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure.

18) The 2G-SGSN and the BSS may execute the BSS Packet Flow Context Procedure

The sequence applied for the intra SGSN RA update case is identical to the cell change case within the same RA as shown in subclause "Intersystem Handover within an RA between Cells in Different Systems" used with a different update type.

6.13.2.2 GPRS to UMTS Handover

An intersystem handover from GPRS to UMTS takes place when the PS-attached MS moves to a new UMTS cell of a new RA. In this case the MS shall initiate a UMTS RA update procedure by establishing a RRC connection and initiating the RA update procedure. The sequence applied for the inter SGSN RA update case is shown in the following figure:

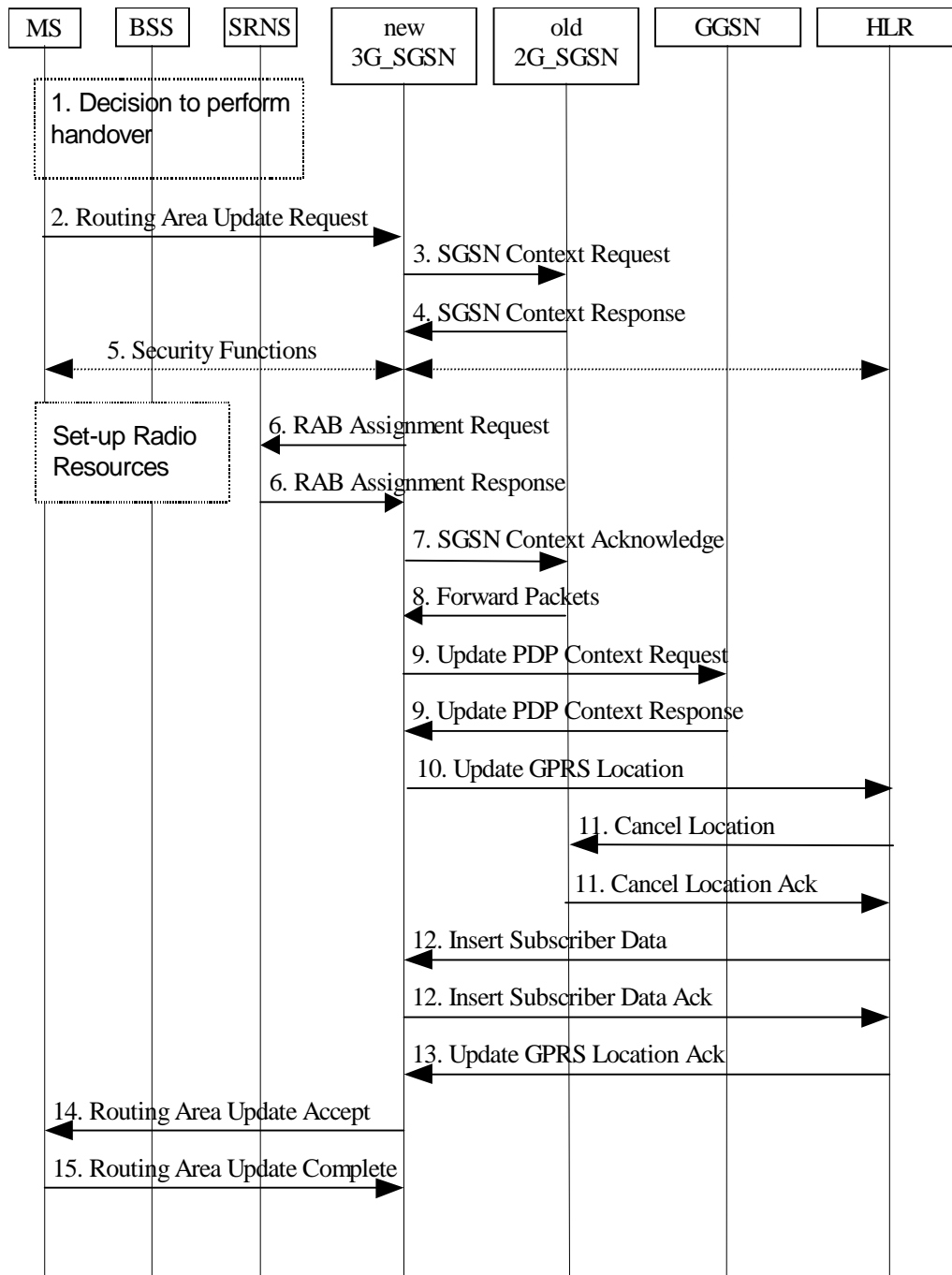


Figure 51: GPRS to UMTS Inter SGSN Routing Area Update Procedure

- 1) The MS and/or BSS/UTRAN decides to perform handover which leads to that the MS switches to the new cell supporting UMTS radio technology
- 2) The MS sends a Routing Area Update Request (old RAI, old P-TMSI Signature, Update Type, CM) to the new 3G-SGSN. The SRNS shall add an identifier of the area where the message was received before passing the message to the 3G-SGSN.
- 3) The new 3G-SGSN sends SGSN Context Request (old RAI, old P-TMSI, New SGSN Address) to the old 2G-SGSN to get the MM and PDP contexts for the MS (The old RAI received from the MS is used to derive the old 2G-SGSN address). The old 2G-SGSN starts a timer for supervision of the MS's context and stops the transmission of N-PDUs to the MS.
- 4) The old 2G-SGSN responds with SGSN Context Response (MM Context, e.g. IMSI, PDP Contexts, e.g. APN). Each PDP Context includes the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled to the GGSN. Each PDP Context also

includes the SNDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode to the MS, the SNDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode from the MS. The new 3G-SGSN shall use the GTP sequence numbers for in-sequence delivery over the Iu interface.

The new 3G-SGSN uses the received SNDCP N-PDU sequence number for reliable data transmission (FFS).

- 5) Security functions may be executed.
- 6) The new 3G-SGSN requests the SRNS to establish a radio access bearer by sending RAB Assignment Request to the SRNS. The SRNS responds with RAB Assignment Response.
- 7) The new 3G-SGSN sends a SGSN Context Acknowledge message to the old 2G-SGSN. This informs the old 2G-SGSN that the new 3G-SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routing area update procedure back to the old SGSN before completing the ongoing routing area update procedure.
- 8) The old 2G-SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new 3G-SGSN. The 3G-SGSN shall ignore any SNDCP sequence numbers received with the tunneled N-PDUs. Additional N-PDUs received from the GGSN before the timer described in step 3 expires are also duplicated and tunneled to the new 3G-SGSN. No N-PDUs shall be forwarded to the new 3G-SGSN after expiry of the timer described in step 3.
- 9) The new 3G-SGSN sends a Update PDP Context Request (new SGSN Address, TID, QoS Negotiated) to the GGSN (s) concerned. The GGSN (s) updates its PDP context fields and returns Update PDP Context Response (TID).
- 10) The new 3G-SGSN informs the HLR of the change of SGSN by sending Update GPRS Location (SGSN Number, SGSN Address, IMSI) to the HLR.
- 11) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old 2G-SGSN. The old 2G-SGSN removes the MM and PDP contexts if the timer described in step 3 is not running. When the timer is running the MM and PDP contexts are removed when the timer expires. The old 2G-SGSN acknowledges with Cancel Location Ack (IMSI).
- 12) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new 3G-SGSN. The 3G-SGSN constructs a MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.
- 13) The HLR acknowledges the Update GPRS Location by sending Update Location Ack (IMSI) to the new 3G-SGSN.
- 14) The new 3G-SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the 3G-SGSN, or if subscription checking fails, then the new 3G-SGSN rejects the routing area update with an appropriate cause. If all checks are successful then the new 3G-SGSN constructs MM and PDP contexts for the MS. A logical link is established between the new 3G-SGSN and the MS. The new 3G-SGSN responds to the MS with Routing Area Update Accept (P-TMSI, P-TMSI signature Receive N-PDU Number (FFS)).
- 15) The MS acknowledges the new P-TMSI with a Routing Area Update Complete (P-TMSI, Receive N-PDU Number (FFS)).

The sequence applied for the intra SGSN RA update case is identical to the cell change within the same RA case as shown in subclause "Intersystem Handover within an RA between Cells in Different Systems" used with a different update type.

6.14 Classmark Handling

To support efficient radio interface usage in GPRS, the MS classmark is handled differently for SGSN-based services than for MSC-based services. In particular, the classmark is sent in MM messages to the network and stored in the network as long as the MS is GPRS-attached, avoiding redundant classmark retransmissions over the radio interface. This is sometimes called the "idle-mode classmark" principle.

[By using Routing area update in order to perform the PS Attach procedure, the SGSN classmark may have to be transmitted at every RAU. The principle above may therefore change if the idea is accepted. This subclause needs further updates.]

In order to allow introduction of new radio access technologies in the future, the MS classmark is split into two distinct and independent information elements, the radio access classmark, and the SGSN classmark.

6.14.1 Radio Access Classmark

The radio access classmark contains the radio capabilities of the MS (e.g., multislot capability, power class), and more generally all the information that should be known by the BSS in order to handle radio resources for that MS.

The radio access classmark is a container for a multiplicity of radio access technology-dependent information, i.e., within the radio access classmark there are independent sub-fields for various technologies such as GSM 900, GSM 1800, Satellite, UMTS, etc. The coding shall allow a BSS to extract only the sub-fields relevant to it without interpreting the other sub-fields. This ensures that the radio classmark does not need to be interpreted by the NSS, and the full radio classmark is always sent by the MS to the SGSN, and thereafter provided to the BSS irrespective of the actual BSS capabilities.

The SGSN shall provide the radio access classmark as an information element on the Gb interface. It is the responsibility of the SGSN to provide the BSS with the most recent classmark received from the MS. The classmark information element can be included in a downlink transfer request, or be sent in a specific message that updates the radio classmark information in the BSS. The BSS may at any time request the radio classmark for a given MS to be transmitted from the SGSN to the BSS.

A specific optimisation allows the BSS to receive a reduced radio access classmark at initial access directly from the MS. This enables the BSS not to wait for the full radio access classmark to be provided by the SGSN, and is therefore quicker for the initial MS-originated transmission. The reduced classmark can be carried in several RR messages depending on the access method, e.g., in the initial random access message, or in the first uplink radio block. Details are provided in GSM 04.08 and GSM 04.60.

6.14.2 SGSN Classmark

The SGSN classmark contains non radio-related capabilities, e.g., the ciphering capability. The SGSN stores the SGSN classmark which is used both locally by the SGSN and for transfer to the new SGSN at all types of inter SGSN RA update.

7 Network Management Functionality

The Network Management function provides mechanisms to support O&M functions related to the packet domain.

8 Radio Resource Functionality

8.1 Radio Resource Functionality for GPRS

8.1.1 Cell Selection and Reselection

An MS (in any mode of operation (A, B, or C)) cannot camp on more than one cell. This means that the cell selection and reselection procedure should choose cells that support services the user has subscribed to.

If the MS is in idle mode, see UMTS 23.022, then it shall behave as described below:

When the MS is in GPRS IDLE state and wishes to initiate the GPRS Attach procedure, the following applies:

- If the currently camped-on cell supports GPRS then no cell reselection is required.

- If the currently camped-on cell does not support GPRS, then reselection of a cell supporting GPRS is required before execution of the attach procedure.

If the MS is in GPRS STANDBY or READY state, cell selection and reselection procedures specific to GPRS shall be used, see UMTS 23.022.

The cell reselection procedure used in READY state shall minimise the cell changes.

If the MS is in dedicated mode, see UMTS 24.008, then the changes from one cell to another is performed according to the network-controlled handover procedures.

There may be co-ordination of the idle and dedicated mode procedures used for circuit-switched services with the READY state procedure for MSs that are both IMSI-attached and GPRS-attached.

8.1.2 Discontinuous Reception

A GPRS MS may be able to choose if it wants to use discontinuous reception (DRX) or not. If using DRX, the MS shall also be able to specify other DRX parameters that indicate the delay for the network to send a page request or a channel assignment to the MS (see GSM 03.64).

The DRX parameters shall be indicated by the MS in the attach procedure. The SGSN shall then in each page request send these parameters to the BSS that uses this information and the IMSI to calculate the correct paging group.

DRX usage is independent of the MM states IDLE, STANDBY and READY. As DRX can be used by a GPRS MS in READY state, DRX has to be considered also when assigning a packet data channel for downlink transfer. The SGSN shall therefore indicate the DRX parameters for the MS in all packet transmission requests to the BSS.

A GPRS MS shall not apply DRX in READY state during the GPRS attach and routing area update procedures.

8.1.3 Radio Resource Management

GSM Radio Resource Management functions are defined in GSM 04.07 [12]. The radio interface layer 3 protocol is specified in UMTS 24.008.

8.1.3.1 Layer Functions

GPRS radio resource management procedures are required for the following functions:

- allocation and release of physical resources (i.e., timeslots) associated with a GPRS channel;
- monitoring GPRS channel utilisation to detect under-utilised or congested GPRS channels;
- initiating congestion control procedures; and
- distribution of GPRS channel configuration information for broadcasting to the MSs.

8.1.3.2 Model of Operation

8.1.3.2.1 Dynamic Allocation of Radio Resources

A cell may or may not support GPRS.

A cell supporting GPRS may have GPRS radio resources allocated at a given instance. If no GPRS radio resources are allocated, an MS can request allocation of such resources. MSs may then use these radio resources. The PLMN may dynamically increase, to a PLMN operator-defined maximum, or, decrease to an operator-defined minimum, the radio resources allocated.

The network broadcasts GPRS system information on the common control channels.

GSM radio resources are dynamically shared between GPRS and other GSM services.

8.1.4 Paging for GPRS Downlink Transfer

An MS in STANDBY state is paged by the SGSN before a downlink transfer to that MS. The paging procedure shall move the MM state to READY to allow the SGSN to forward downlink data to the radio resource. Therefore, any uplink data from the MS that moves the MM context at the SGSN to READY state is a valid response to paging.

The SGSN supervises the paging procedure with a timer. If the SGSN receives no response from the MS to the Paging Request message, it shall repeat the paging. The repetition strategy is implementation dependent.

The MS shall accept pages also in READY state if no radio resource is assigned. This supports recovery from inconsistent MM states in MS and SGSN.

The GPRS Paging procedure is illustrated in Figure 52. Each step is explained in the following list.

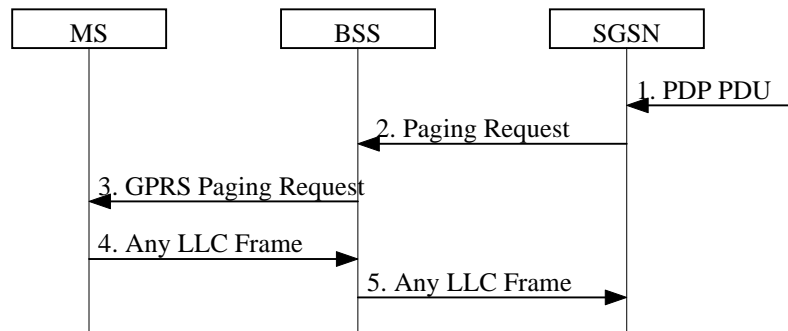


Figure 52: GPRS Paging Procedure

- 1) The SGSN receives a downlink PDP PDU for an MS in STANDBY state. Downlink signalling to a STANDBY state MS initiates paging as well.
- 2) The SGSN sends a BSSGP Paging Request (IMSI, P-TMSI, Area, Channel Needed, QoS, DRX Parameters) message to the BSS serving the MS. IMSI is needed by the BSS in order to calculate the MS paging group. P-TMSI is the identifier by which the MS is paged. Area indicates the routing area in which the MS is paged. Channel Needed indicates GPRS paging. QoS is the negotiated QoS for the PDP context that initiates the paging procedure, and indicates the priority of this Paging Request relative to other Paging Request messages buffered in the BSS. DRX Parameters indicates whether the MS uses discontinuous reception or not. If the MS uses discontinuous reception, then DRX Parameters also indicate when the MS is in a non-sleep mode able to receive paging requests.
- 3) The BSS pages the MS with one Paging Request (P-TMSI, Channel Needed) message in each cell belonging to the addressed routing area. This is described in GSM 03.64.
- 4) Upon receipt of a GPRS Paging Request message, the MS shall respond with either any single valid LLC frame (e.g., a Receive Ready or Information frame) that implicitly is interpreted as a page response message by the SGSN. When responding, the MS changes MM state to READY. The response is preceded by the Packet Channel Request and Packet Immediate Assignment procedures as described in GSM 03.64.
- 5) Upon reception of the LLC frame, the BSS adds the Cell Global Identity including the RAC and LAC of the cell and sends the LLC frame to the SGSN. The SGSN shall then consider the LLC frame to be an implicit paging response message and stop the paging response timer.

8.2 Radio Resource Functionality for UMTS

8.2.1 Radio Resource Management

UTRAN functions are defined in UMTS 25.401. The radio interface protocol architecture is specified in UMTS 25.301, and the Radio Resource Control protocol is specified in UMTS 25.331.

8.2.2 RRC State Machine

The RRC state machine is a description model of how the MS and the UTRAN co-operate regarding RRC functionality. The RRC state describes the MS state in the UTRAN. This subclause contains a brief description of the RRC state machine, for more information see UMTS 25.303.

The RRC state machine exists as two peer entities, one in the MS and one in UTRAN. Apart from transient situations and error cases the two peer entities are synchronised. Figure 53 illustrates the main modes and states of the RRC state machine.

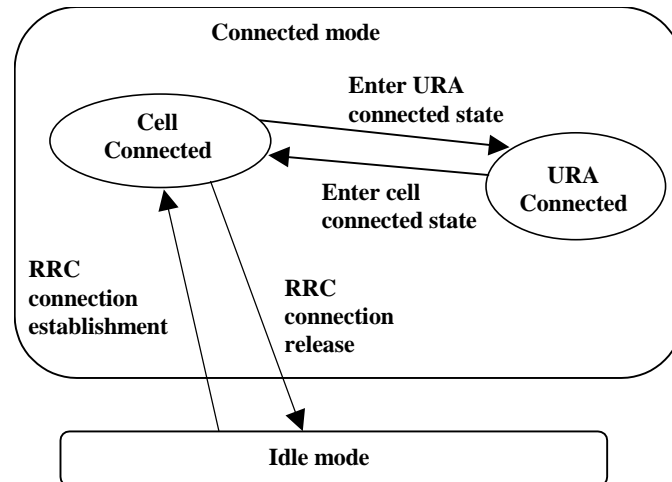


Figure 53: RRC Modes, Main RRC States and Main Mode and State Transition

RRC Idle mode: In the Idle mode there is no connection established between the MS and UTRAN. There is no signalling between UTRAN and the MS except for system information that is sent from UTRAN on a broadcast channel to the MS. The MS can also receive paging messages with a CN identity on the PCH. There is no information of the MS stored in UTRAN in this mode.

RRC Connected mode: In the Connected mode the main states are Cell Connected state and URA Connected state. In this mode there is one RNC that is acting as Serving RNC (SRNC), and an RRC connection is established between the MS and this SRNC.

- When the MS position is known at the cell level, the MS is in the Cell Connected state. When in Cell Connected state, the RRC connection mobility is handled by handover and cell update procedures.
- When the MS position is known at the URA level, the MS is in the URA Connected state. URA updating procedures provides the mobility functionality in this state. No dedicated radio resources are used in the URA Connected state.

8.2.3 Paging Initiated by CN

A CN node requests paging only for MSs in CMM-IDLE state or PMM-IDLE state. In the separate CN architecture, paging from a CN node is done independently from the state of the MS in the other CN service domain.

In this alternative with paging co-ordination in the UTRAN, the MS does not need to listen to the PCH (Paging Channel) in the RRC Connected mode, at least not when MS is allocated a dedicated channel.

For each paging request received from a CN node, the RNC determines whether the MS has an established RRC connection or not. In order to achieve this, the context that is prepared within the SRNC for MS in RRC Connected mode must contain the IMSI, which is the common MS identity for the two CN domains.

If no context is found for the MS, "normal PCH paging" is performed. The paging message is transferred on the paging channel, and it includes the MS paging identity received from the CN and a CN service domain type indication.

If a context is found, a "CN paging message" is transferred using the existing RRC connection. This message includes a CN service domain type indication.

8.2.3.1 PS Paging Initiated by 3G-SGSN Without RRC Connection for CS

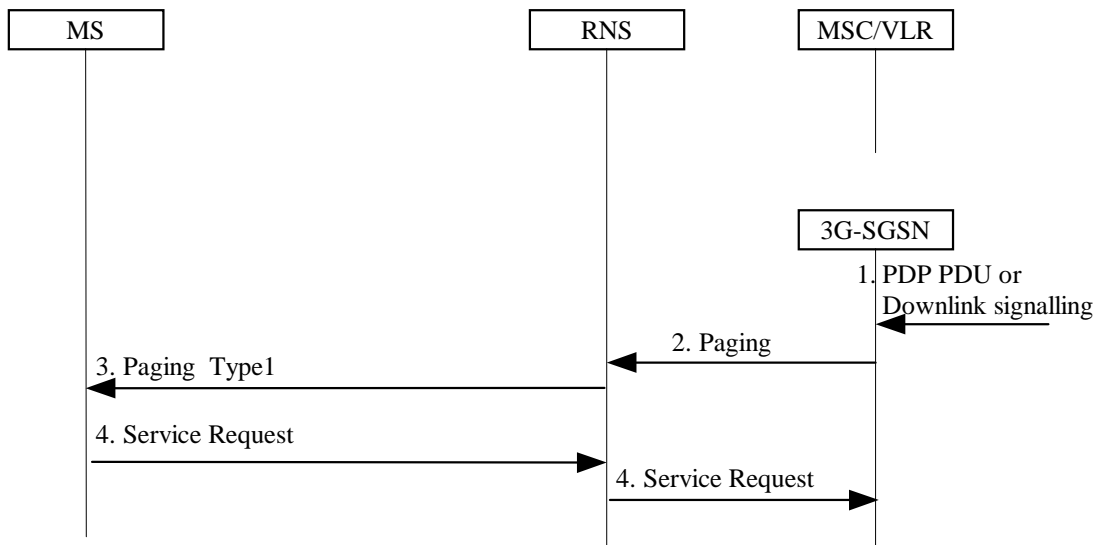


Figure 54: PS Paging Without RRC Connection for CS

- 1) The 3G-SGSN receives a PDP PDU or downlink signalling for an MS in PMM Idle state.
- 2) The 3G-SGSN sends a RANAP Paging (IMSI, P-TMSI, Area, CN Domain Indicator) message to each RNS belonging to the routeing area in which the MS located. IMSI is needed by the RNS in order to calculate the MS paging group, and to identify the paged MS. If 3G-SGSN assigned the P-TMSI to the MS, P-TMSI is also included. Area indicates the routeing area in which the MS is paged. CN Domain Indicator indicates which domain (MSC or 3G-SGSN) initiated the paging message, and it represents "SGSN" in this case.
- 3) The RNS controls whether the MS has an established RRC connection or not. In this case, MS has no RRC connection, so a "normal PCH paging" is performed. Paging Type 1 (IMSI or P-TMSI, Paging originator, CN domain ID) is transferred on the Paging channel, IMSI or P-TMSI identifies the MS. Paging originator indicates whether this is core network originated paging or UTRAN originated paging, so it represents "CN" in this case. And CN domain ID indicates whether this paging message is for CS-service or PS-service, so it represents "PS" in this case.
- 4) The paging request triggers the Service Request procedures in the MS. The service request procedures are described in subclause "Service Request Procedure for UMTS".

Optionally, 3G-SGSN may include "Non Searching Indication" in RANAP Paging message in this case. If a "Non Searching Indication" parameter is present, the RNC will not search the established RRC connection, and just initiate "normal PCH paging".

8.2.3.2 PS Paging Initiated by 3G-SGSN With RRC Connection for CS

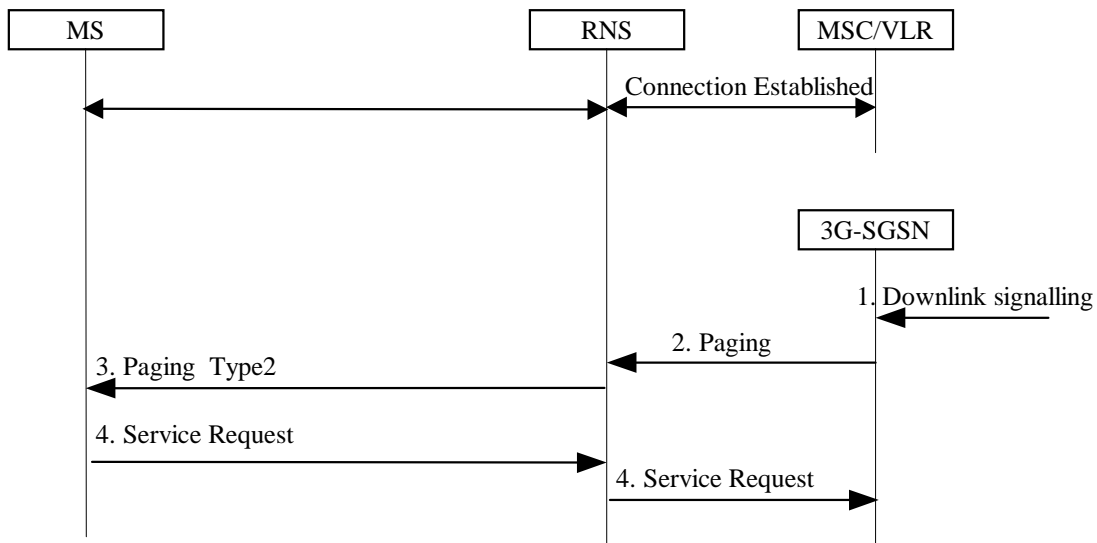


Figure 55: PS Paging With RRC Connection for CS

- 1) The 3G-SGSN receives a downlink signalling for an MS in PMM Idle state.
- 2) The 3G-SGSN sends a RANAP Paging (IMSI, P-TMSI, Area, CN Domain Indicator) message to each RNS belonging to the routing area in which the MS is located. IMSI is needed by the RNS in order to calculate the MS paging group. If 3G-SGSN assigned the P-TMSI to the MS, P-TMSI is included, and it identifies the MS is paged. Area indicates the routing area in which the MS is paged. CN Domain Indicator indicates to which domain (MSC or 3G-SGSN) the paging was initiated, and it represents "3G-SGSN" in this case.
- 3) The RNS controls whether the MS has an established RRC connection or not. In this case, MS has an established RRC connection for CS service, so RNS sends a RRC Paging Type 2(CN domain ID) message to the MS on established RRC connection. CN Domain ID indicates to which domain (CS or PS) the paging shall be directed, so it represents "PS" in this case.
- 4) The paging request triggers the Service Request procedures in the MS. The service request procedures are described in subclause "Service Request Procedure for UMTS".

8.2.4 Paging Initiated by UTRAN

An MS in RRC URA connected state is paged by the RNC before a downlink transfer to that MS. The URA paging procedure shall move the RRC state to Cell Connected to allow the RNC to forward downlink data or signalling message to the radio resource. Therefore, RRC: Cell Update message from the MS that moves the RRC State at the RNC to Cell Connected state is a valid response to URA paging.

The RNC supervises the paging procedure with a timer. If the RNC receives no response from the MS to the URA Paging Request message, it shall repeat the paging. The repetition strategy is implementation dependent. For more information see TS 25.303.

The Paging procedure is illustrated in Figure 42. Each step is explained in the following list.

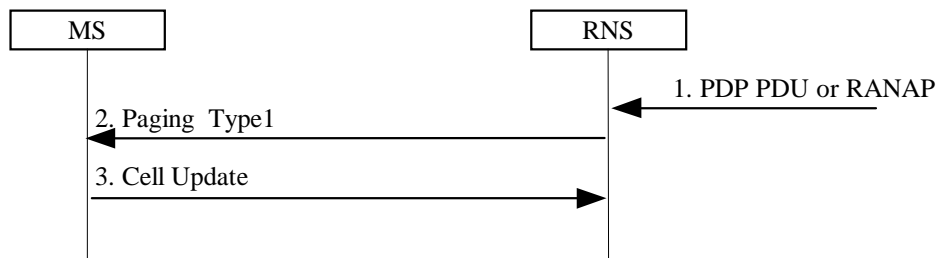


Figure 56: URA Paging Procedure

- 1) The RNS receives a downlink PDP PDU for an MS in RRC URA connected state. Downlink signalling to a MS in RRC URA connected state initiates URA paging as well.
- 2) The RNS pages the MS with one Paging Type 1 (RNTI, Paging originator) message in each cell belonging to the UTRAN routing area where the MS exists. RNTI is the identifier by which the MS is paged. Paging originator indicates whether this is the core network originated paging or UTRAN originated paging, so it represents "UTRAN" in this case.
- 3) The paging request triggers the Cell Update procedures in the MS. The Cell Update procedures are described in TS 25.331.

9 Packet Routing and Transfer Functionality

9.1 Definition of Packet Data Protocol States

A GPRS subscription contains the subscription of one or more PDP addresses. Each PDP address is described by one or more PDP contexts in the MS, the SGSN, and the GGSN. Each PDP context may be associated with a TFT. At most one PDP context associated with the same PDP address may exist at any time with no TFT assigned to it. Every PDP context exists independently in one of two PDP states. The PDP state indicates whether data transfer is enabled for that PDP address and TFT or not. In case all PDP contexts associated with the same PDP address are deactivated, data transfer for that PDP address is disabled. Activation and deactivation are described in subclause "PDP Context Activation, Modification, and Deactivation Functions". All PDP contexts of a subscriber are associated with the same MM context for the IMSI of that subscriber.

9.1.1 INACTIVE State

The INACTIVE state characterises the data service for a certain PDP address of the subscriber as not activated. The PDP context contains no routing or mapping information to process PDP PDUs related to that PDP address. No data can be transferred. A changing location of a subscriber causes no update for the PDP context in INACTIVE state even if the subscriber is PS-attached.

Mobile-terminated PDP PDUs received in INACTIVE state by the GGSN may initiate the Network-Requested PDP Context Activation procedure if the GGSN is allowed to initiate the activation of the PDP context for that PDP address. Otherwise, mobile-terminated PDP PDUs received in INACTIVE state invoke error procedures in the GGSN relevant to the external network protocol, for example, an IP packet is discarded and an ICMP (see RFC 792 [41]) packet (error notification) is returned to the source of the received packet. Other error procedures may be introduced on the application level, but this is outside the scope of the present document.

The MS initiates the movement from INACTIVE to ACTIVE state by initiating the PDP Context Activation procedure.

9.1.2 ACTIVE State

In ACTIVE state, the PDP context for the PDP address in use is activated in MS, SGSN and GGSN. The PDP context contains mapping and routing information for transferring PDP PDUs for that particular PDP address between MS and GGSN. The PDP state ACTIVE is permitted only when the mobility management state of the subscriber is STANDBY,

READY, PMM-IDLE, or PMM-CONNECTED. The Iu interface radio access bearer may or may not be established for an active PDP context.

An active PDP context for an MS is moved to INACTIVE state when the deactivation procedure is initiated.

All active PDP contexts for an MS are moved to INACTIVE state when the MM state changes to IDLE or PMM-DETACHED.

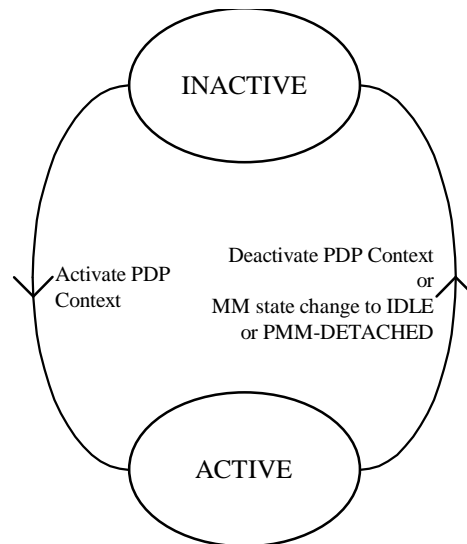


Figure 57: Functional PDP State Model

9.2 PDP Context Activation, Modification, and Deactivation Functions

A PS-attached MS can initiate these functions at any time in order to activate, modify, or deactivate a PDP context in the MS, the SGSN, and the GGSN. A GGSN may request the activation of a PDP context to a PS-attached subscriber. A GGSN may initiate the deactivation of a PDP context.

NOTE: If the MS is in PMM-IDLE state, it needs to perform a service request procedure to enter the PMM-CONNECTED state before initiating these procedure.

Upon receiving an Activate PDP Context Request message or an Activate Secondary PDP Context Request message, the SGSN shall initiate procedures to set up PDP contexts. The first procedure includes subscription checking, APN selection, and host configuration, while the latter procedure excludes these functions and reuses PDP context parameters including the PDP address but except the QoS parameters. Once activated, all PDP contexts are managed equally. At least one PDP context shall be activated for a PDP address before a Secondary PDP Context Activation procedure may be initiated.

Upon receiving a Deactivate PDP Context Request message, the SGSN shall initiate procedures to deactivate the PDP context. When the last PDP context associated with a PDP address is deactivated, then N-PDU transfer for this PDP address is disabled.

An MS does not have to receive the (De-)Activate PDP Context Accept message before issuing another (De-)Activate PDP Context Request. However, only one request can be outstanding for every NSAPI.

9.2.1 Static and Dynamic PDP Addresses

PDP addresses can be allocated to an MS in four different ways:

- the HPLMN operator assigns a PDP address permanently to the MS (static PDP address);
- the HPLMN operator assigns a PDP address to the MS when a PDP context is activated (dynamic HPLMN PDP address);

- the VPLMN operator assigns a PDP address to the MS when a PDP context is activated (dynamic VPLMN PDP address); or
- the PDN operator or administrator assigns an IP address to the MS after a PDP context has been activated (External PDN Address Allocation).

It is the HPLMN operator that defines in the subscription whether a dynamic HPLMN or VPLMN PDP address can be used.

For every IMSI, zero, one, or more dynamic PDP address per PDP type can be assigned. For every IMSI, zero, one, or more static PDP addresses per PDP type can be subscribed to.

When dynamic addressing from the HPLMN or the VPLMN is used, it is the responsibility of the GGSN to allocate and release the dynamic PDP address. When External PDN Address Allocation is used, it is the responsibility of the MS and the PDN to allocate and release the dynamic PDP address by means of protocols such as DHCP or MIP. In case of DHCP, the GGSN provides the function of a DHCP Relay Agent as defined in RFC 2131 [47] and RFC 1542 [45]. In case of MIP, the GGSN provides the function of a Foreign Agent as defined in RFC 2002 [46].

Only static PDP addressing is applicable in the network-requested PDP context activation case.

9.2.2 Activation Procedures

9.2.2.1 PDP Context Activation Procedure

The PDP Context Activation procedure is illustrated in Figure 58. Each step is explained in the following list.

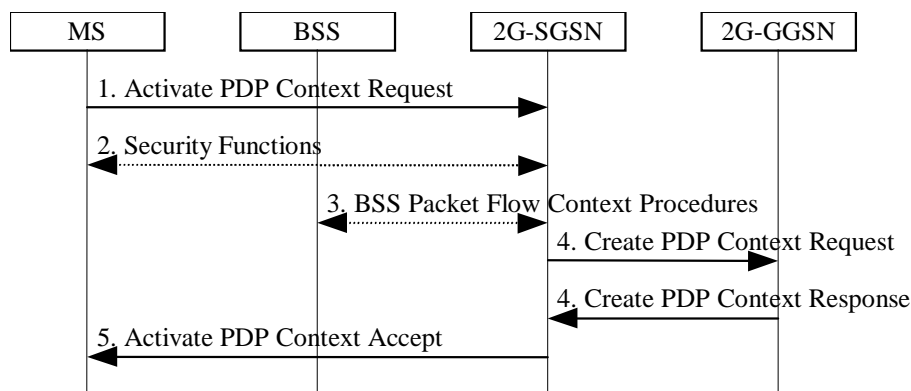


Figure 58: PDP Context Activation Procedure for GPRS

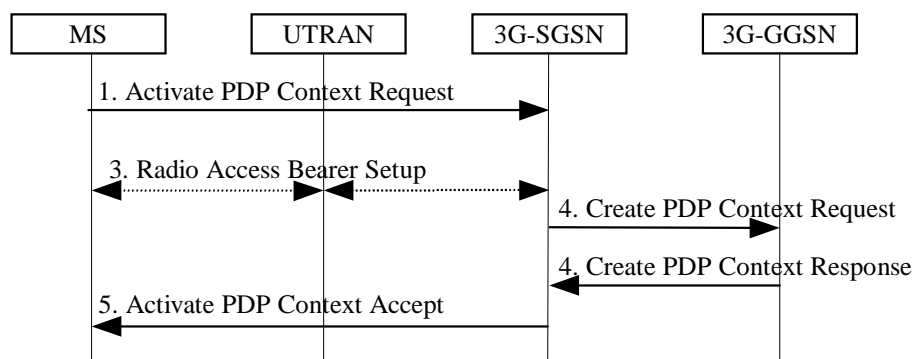


Figure 59: PDP Context Activation Procedure for UMTS

- 1) The MS sends an Activate PDP Context Request (NSAPI, TI, PDP Type, PDP Address, Access Point Name, QoS Requested, PDP Configuration Options) message to the SGSN. The MS shall use PDP Address to indicate whether it requires the use of a static PDP address or whether it requires the use of a dynamic PDP address. The MS shall leave PDP Address empty to request a dynamic PDP address. The MS may use Access Point Name to select a reference point to a certain external network and/or to select a service. Access Point Name is a logical

name referring to the external packet data network and/or to a service that the subscriber wishes to connect to. QoS Requested indicates the desired QoS profile. PDP Configuration Options may be used to request optional PDP parameters from the GGSN (see GSM 09.60). PDP Configuration Options is sent transparently through the SGSN.

- 2) For GPRS, security functions may be executed. These procedures are defined in subclause "Security Function".
- 3) For GPRS, BSS packet flow context procedures may be executed. These procedures are defined in subclause "BSS Context".

For UMTS, the RAB setup procedure is performed. The 3G-SGSN sends a Radio Access Bearer Setup Request message to UTRAN. The UTRAN then initiates the radio access bearer setup procedure.

- 4) The SGSN validates the Activate PDP Context Request using PDP Type (optional), PDP Address (optional), and Access Point Name (optional) provided by the MS and the PDP context subscription records. The validation criteria, the APN selection criteria, and the mapping from APN to a GGSN are described in annex A.

If no GGSN address can be derived or if the SGSN has determined that the Activate PDP Context Request is not valid according to the rules described in annex A, then the SGSN rejects the PDP context activation request.

If a GGSN address can be derived, the SGSN creates a TID for the requested PDP context by combining the IMSI stored in the MM context with the NSAPI received from the MS. If the MS requests a dynamic address, then the SGSN lets a GGSN allocate the dynamic address. The SGSN may restrict the requested QoS attributes given its capabilities, the current load, and the subscribed QoS profile.

[TEID is studied under N2. The impact should be clarified in 23.060.]

The SGSN sends a Create PDP Context Request (PDP Type, PDP Address, Access Point Name, QoS Negotiated, TID, MSISDN, Selection Mode, PDP Configuration Options) message to the affected GGSN. Access Point Name shall be the APN Network Identifier of the APN selected according to the procedure described in annex A. PDP Address shall be empty if a dynamic address is requested. The GGSN may use Access Point Name to find an external network and optionally to activate a service for this APN. Selection Mode indicates whether a subscribed APN was selected, or whether a non-subscribed APN sent by MS or a non-subscribed APN chosen by SGSN was selected. Selection Mode is set according to annex A. The GGSN may use Selection Mode when deciding whether to accept or reject the PDP context activation. For example, if an APN requires subscription, then the GGSN is configured to accept only the PDP context activation that requests a subscribed APN as indicated by the SGSN with Selection Mode.

The GGSN creates a new entry in its PDP context table and generates a Charging Id. The new entry allows the GGSN to route PDP PDUs between the SGSN and the external PDP network, and to start charging. The GGSN may further restrict QoS Negotiated given its capabilities and the current load. The GGSN then returns a Create PDP Context Response (TID, PDP Address, BB Protocol, Reordering Required, PDP Configuration Options, QoS Negotiated, Charging Id, Cause) message to the SGSN. PDP Address is included if the GGSN allocated a PDP address. If the GGSN has been configured by the operator to use External PDN Address Allocation for the requested APN, then PDP Address shall be set to 0.0.0.0, indicating that the PDP address shall be negotiated by the MS with the external PDN after completion of the PDP Context Activation procedure. The GGSN shall relay, modify, and monitor these negotiations as long as the PDP context is in ACTIVE state and use the GGSN-Initiated PDP Context Modification procedure to transfer the currently-used PDP address to the SGSN and the MS. BB Protocol indicates whether TCP or UDP shall be used to transport user data on the backbone network between the SGSN and GGSN. Reordering Required indicates whether the SGSN shall reorder N-PDUs before delivering the N-PDUs to the MS. PDP Configuration Options contain optional PDP parameters that the GGSN may transfer to the MS. These optional PDP parameters may be requested by the MS in the Activate PDP Context Request message, or may be sent unsolicited by the GGSN. PDP Configuration Options is sent transparently through the SGSN. The Create PDP Context messages are sent over the backbone network.

If QoS Negotiated received from the SGSN is incompatible with the PDP context being activated (e.g., the reliability class is insufficient to support the PDP type), then the GGSN rejects the Create PDP Context Request message. The compatible QoS profiles are configured by the GGSN operator.

- 5) The SGSN inserts the NSAPI along with the GGSN address in its PDP context. If the MS has requested a dynamic address, the PDP address received from the GGSN is inserted in the PDP context. The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns an Activate PDP Context Accept (PDP

Type, PDP Address, TI, QoS Negotiated, Radio Priority, Packet Flow Id, PDP Configuration Options) message to the MS. The SGSN is now able to route PDP PDUs between the GGSN and the MS, and to start charging.

For each PDP Address a different quality of service (QoS) profile may be requested. For example, some PDP addresses may be associated with E-mail that can tolerate lengthy response times. Other applications cannot tolerate delay and demand a very high level of throughput, interactive applications being one example. These different requirements are reflected in the QoS profile. The QoS profile is defined in subclause "Quality of Service Profile". If a QoS requirement is beyond the capabilities of a PLMN, the PLMN negotiates the QoS profile as close as possible to the requested QoS profile. The MS either accepts the negotiated QoS profile, or deactivates the PDP context.

After an SGSN has successfully updated the GGSN, the PDP contexts associated with an MS is distributed as shown in clause "Information Storage".

If the PDP Context Activation Procedure fails or if the SGSN returns an Activate PDP Context Reject (Cause, PDP Configuration Options) message, then the MS may attempt another activation to the same APN up to a maximum number of attempts.

9.2.2.1.1 Secondary PDP Context Activation Procedure

The Secondary PDP Context Activation procedure may be used to activate a PDP context while reusing the PDP address and other PDP context information from an already active PDP context, but with a different QoS profile. Procedures for APN selection and PDP address negotiation are not executed. All PDP contexts sharing the same PDP address are identified by one and the same TI but a unique NSAPI value.

The Secondary PDP Context Activation procedure associates a Traffic Flow Template (TFT) to the newly activated PDP context. The TFT contains attributes that specify an IP header filter that is used to direct data packets received from the interconnected external packet data network to the newly activated PDP context.

The Secondary PDP Context Activation procedure may only be initiated after a PDP context is already activated for the same PDP address. The procedure is illustrated in Figure 60. Each step is explained in the following list.

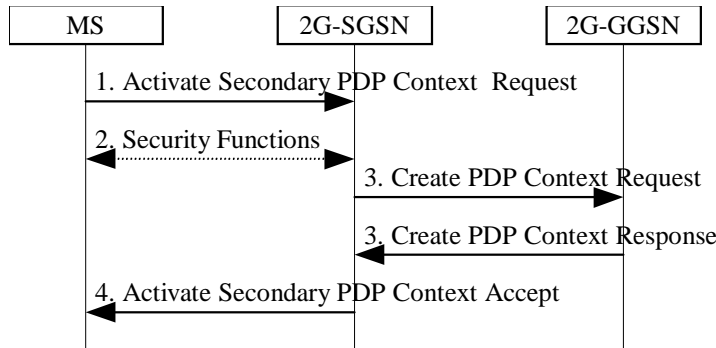


Figure 60: Secondary PDP Context Activation Procedure for GPRS

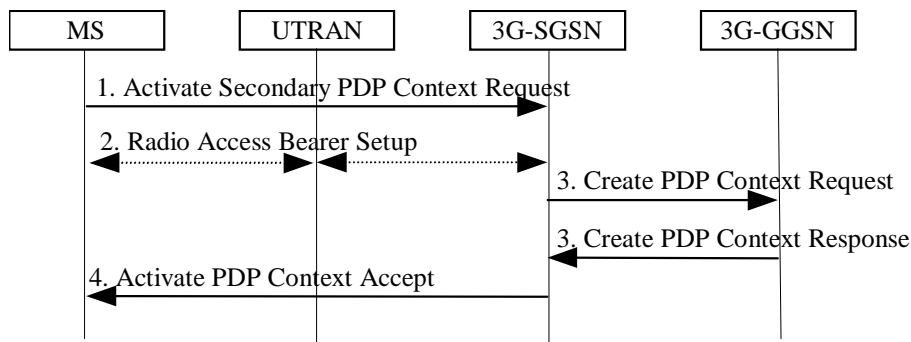


Figure 61: Secondary PDP Context Activation Procedure for UMTS

- 1) The MS sends an Activate Secondary PDP Context Request (NSAPI, TI, QoS Requested, TFT) message to the SGSN. QoS Requested indicates the desired QoS profile. TFT is sent transparently through the SGSN to the

GGSN to enable packet classification for downlink data transfer. TI is the same TI used by the already-activated PDP context(s) for that PDP address, and NSAPI contains a value not used by any other activated PDP context.

- 2) For GPRS, security functions may be executed. These procedures are defined in subclause "Security Function".

For UMTS, , the RAB setup procedure is performed. The 3G-SGSN sends a Radio Access Bearer Setup Request message to the UTRAN. The UTRAN then initiates the radio access bearer setup procedure.

- 3) The SGSN validates the Activate Secondary PDP Context Request using the TI. The same GGSN address is used by the SGSN as for the already-activated PDP context(s) for that TI and PDP address.

The SGSN and GGSN may restrict and negotiate the requested QoS as specified in subclause "PDP Context Activation Procedure". The SGSN sends a Create PDP Context Request (QoS Negotiated, TID, TFT) message to the affected GGSN. The GGSN uses the same external network as used by the already-activated PDP context(s) for that PDP address, generates a new entry in its PDP context table, and stores the TFT. The new entry allows the GGSN to route PDP PDUs via different GTP tunnels between the SGSN and the external PDP network. The GGSN returns a Create PDP Context Response (TID, BB Protocol, Reordering Required, QoS Negotiated, Cause) message to the SGSN.

- 4) The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns an Activate Secondary PDP Context Accept (TI, NSAPI, QoS Negotiated, Radio Priority, Packet Flow Id) message to the MS. The SGSN is now able to route PDP PDUs between the GGSN and the MS via different GTP tunnels and possibly different LLC links.

For each additionally activated PDP context a QoS profile and TFT may be requested.

If the secondary PDP context activation procedure fails or if the SGSN returns an Activate Secondary PDP Context Reject (Cause) message, then the MS may attempt another activation with a different TFT, depending on the cause.

9.2.2.2 Network-Requested PDP Context Activation Procedure

The Network-Requested PDP Context Activation procedure allows the GGSN to initiate the activation of a PDP context. When receiving a PDP PDU the GGSN checks if a PDP context is established for that PDP address. If no PDP context has been previously established the GGSN may try to deliver the PDP PDU by initiating the Network-Requested PDP Context Activation procedure. The criteria used by the GGSN to determine whether trying to deliver the PDP PDU to the MS may be based on subscription information and are outside the scope of GPRS standardisation.

To support Network-Requested PDP Context Activation the GGSN has to have static PDP information about the PDP address. To determine whether Network-Requested PDP Context Activation is supported for a PDP address the GGSN checks if there is static PDP information for that PDP address.

Once these checks have been performed the GGSN may initiate the Network-Requested PDP Context Activation procedure.

The network operator may implement the following techniques to prevent unnecessary enquires to the HLR:

- Implementation of the Mobile station Not Reachable for GPRS flag (MNRG) technique in GGSN, SGSN, and HLR (see subclause "Unsuccessful Network-Requested PDP Context Activation Procedure").
- The GGSN may reject or discard PDP PDUs after a previous unsuccessful delivery attempt. This systematic rejection of PDP PDUs would be performed during a certain time after the unsuccessful delivery.
- The GGSN may store the address of the SGSN with which the GGSN established the last PDP context. This would prevent an enquiry to the HLR. This SGSN address would be considered as valid during a certain time.

9.2.2.2.1 Successful Network-Requested PDP Context Activation Procedure

The Successful Network-Requested PDP Context Activation procedure is illustrated in Figure 62. Each step is explained in the following list.

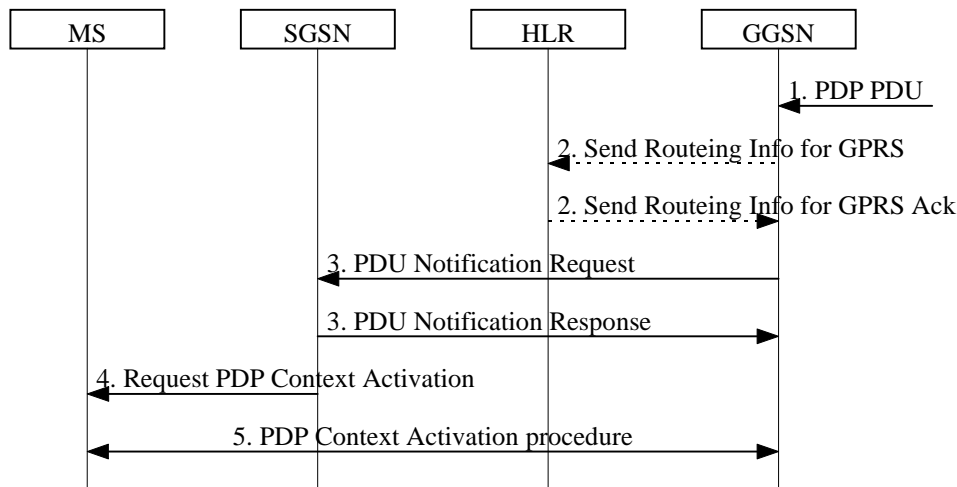


Figure 62: Successful Network-Requested PDP Context Activation Procedure

- 1) When receiving a PDP PDU the GGSN determines if the Network-Requested PDP Context Activation procedure has to be initiated. The GGSN may store subsequent PDP PDUs received for the same PDP address.
- 2) The GGSN may send a Send Routing Information for GPRS (IMSI) message to the HLR. If the HLR determines that the request can be served, it returns a Send Routing Information for GPRS Ack (IMSI, SGSN Address, Mobile Station Not Reachable Reason) message to the GGSN. The Mobile Station Not Reachable Reason parameter is included if the MNRG flag is set in the HLR. The Mobile Station Not Reachable Reason parameter indicates the reason for the setting of the MNRG flag as stored in the MNRR record (see GSM 03.40). If the MNRR record indicates a reason other than 'No Paging Response', the HLR shall include the GGSN number in the GGSN-list of the subscriber.

If the HLR determines that the request cannot be served (e.g., IMSI unknown in HLR), the HLR shall send a Send Routing Information for GPRS Ack (IMSI, MAP Error Cause) message. Map Error Cause indicates the reason for the negative response.

- 3) If the SGSN address is present and either Mobile Station Not Reachable Reason is not present or Mobile Station Not Reachable Reason indicates 'No Paging Response', the GGSN shall send a PDU Notification Request (IMSI, PDP Type, PDP Address, APN) message to the SGSN indicated by the HLR. Otherwise, the GGSN shall set the MNRG flag for that MS. The SGSN returns a PDU Notification Response (Cause) message to the GGSN in order to acknowledge that it shall request the MS to activate the PDP context indicated with PDP Address.
- 4) The SGSN sends a Request PDP Context Activation (TI, PDP Type, PDP Address, APN) message to request the MS to activate the indicated PDP context.
- 5) The PDP context is activated with the PDP Context Activation procedure (see subclause "PDP Context Activation Procedure").

9.2.2.2.2 Unsuccessful Network-Requested PDP Context Activation Procedure

If the PDP context requested by the GGSN cannot be established, the SGSN sends a PDU Notification Response (Cause) or a PDU Notification Reject Request (IMSI, PDP Type, PDP Address, Cause) message to the GGSN depending on if the context activation fails before or after the SGSN has sent a Request PDP Context Activation message to the MS. Cause indicates the reason why the PDP context could not be established:

- 'IMSI Not Known'. The SGSN has no MM context for that IMSI (Cause in PDU Notification Response).
- 'MS GPRS Detached'. The MM state of the MS is IDLE (Cause in PDU Notification Response).

- 'MS Not GPRS Responding'. The MS is GPRS-attached to the SGSN but the MS does not respond. This may be due to the lack of a response to a GPRS Paging Request, due to an Abnormal RLC condition, or due to no Activate PDP Context Request message received within a certain time after the Request PDP Context Activation message was delivered to the MS (Cause in PDU Notification Reject Request).
- 'MS Refuses'. The MS refuses explicitly the network-requested PDP context (Cause in PDU Notification Reject Request).

When receiving the PDU Notification Response or the PDU Notification Reject Request message the GGSN may reject or discard the PDP PDU depending on the PDP type.

After an unsuccessful Network-Requested PDP Context Activation procedure the network may perform some actions to prevent unnecessary enquires to the HLR. The actions taken depend on the cause of the delivery failure.

- If the MS is not reachable or if the MS refuses the PDP PDU (Cause value 'MS Not GPRS Responding' or 'MS Refuses'), then the SGSN shall not change the setting of MNRG for this MS. The GGSN may refuse any PDP PDU for that PDP address during a certain period. The GGSN may store the SGSN address during a certain period and send subsequent PDU Notification Request messages to that SGSN.
- If the MS is GPRS-detached or if the IMSI is not known in the SGSN (Cause value 'MS GPRS Detached' or 'IMSI Not Known'), then the SGSN, the GGSN, and the HLR may perform the Protection and Mobile User Activity procedures.

The Protection procedure is illustrated in Figure 63. Each step is explained in the following list.

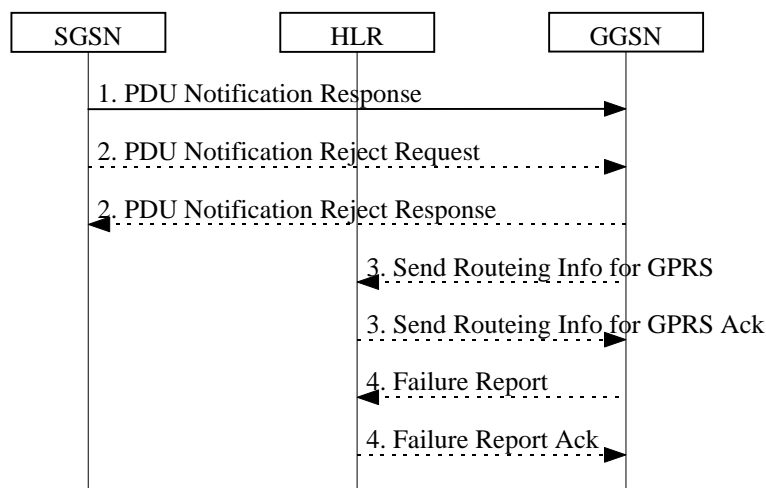


Figure 63: Protection Procedure

- 1) If the MM context of the mobile is IDLE or if the SGSN has no information about that user, the SGSN returns a PDU Notification Response (Cause) message to the GGSN with Cause equal to 'MS GPRS Detached' or 'IMSI Not Known', otherwise the Cause shall be 'Activation Proceeds'. If the Cause is 'MS GPRS Detached' or 'IMSI Not Known' and if the SGSN has an MM context for that user, the SGSN sets MNRG to indicate the need to report to the HLR when the next contact with that MS is performed.
- 2) If the MS does not respond or refuses the activation request, the SGSN sends a PDU Notification Reject Request (IMSI, PDP Type, PDP Address, Cause) message to the GGSN with Cause equal to 'MS Not GPRS Responding' or 'MS Refuses'. The GGSN returns a PDU Notification Reject Response message to the SGSN.
- 3) If Cause equals 'IMSI Not Known' the GGSN may send a Send Routeing Information for GPRS (IMSI) message to the HLR. The HLR returns a Send Routeing Information for GPRS Ack (IMSI, SGSN Address, Cause) message to the GGSN indicating the address of the SGSN that currently serves the MS. If SGSN Address is different from the one previously stored by the GGSN, then steps 3, 4, and 5 in Figure 62 are followed.
- 4) If SGSN Address is the same as the one previously stored in the GGSN, or if the Cause value returned in step 1 equals 'MS GPRS Detached', then the GGSN sets MNRG for that PDP address and sends a Failure Report (IMSI, GGSN Number, GGSN Address) message to the HLR to request MNRG to be set in the HLR. The HLR sets (if not already set) MNRG for the IMSI and adds GGSN Number and GGSN Address to the list of GGSNs to report

to when activity from that IMSI is detected. GGSN Number is either the number of the GGSN, or, if a protocol-converting GSN is used as an intermediate node, the number of the protocol-converting GSN. GGSN Address is an optional parameter that shall be included if a protocol-converting GSN is used.

The Mobile User Activity procedure is illustrated in Figure 64. Each step is explained in the following list.

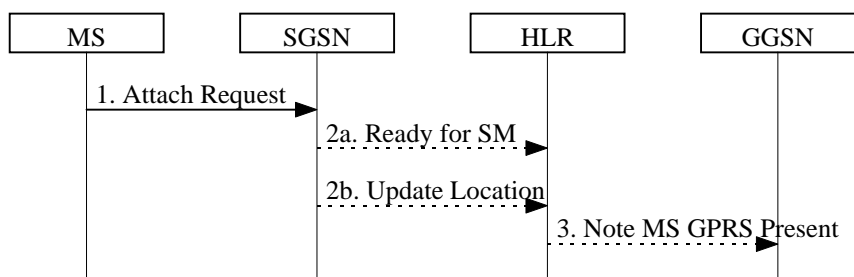


Figure 64: Mobile User Activity Procedure

- 1) The SGSN receives an indication that an MS is reachable, e.g., an Attach Request message from the MS.
- 2a) If the SGSN contains an MM context of the MS and MNRG for that MS is set, the SGSN shall send a Ready for SM (IMSI, MS Reachable) message to the HLR and clears MNRG for that MS.
- 2b) If the SGSN does not keep the MM context of the MS, the SGSN shall send an Update Location message (see subclause "Attach Function") to the HLR.
- 3) When the HLR receives the Ready for SM message or the Update Location message for an MS that has MNRG set, it clears MNRG for that MS and sends a Note MS GPRS Present (IMSI, SGSN Address) message to all the GGSNs in the list of the subscriber. (The Ready for SM message also triggers the SMS alert procedure as described in subclause "Unsuccessful Mobile-terminated SMS Transfer".) SGSN Address contains the address of the SGSN that currently serves the MS. Upon reception of Note MS Present, each GGSN shall clear MNRG.

9.2.2.3 Anonymous Access PDP Context Activation Procedure

The MS can anonymously initiate PDP Context Activation in IDLE, STANDBY, and READY states. An existing MM context in the SGSN is neither required nor used in this case. Only dynamic PDP addressing is applicable.

The Anonymous Access PDP Context Activation procedure is illustrated in Figure 65. Each step is explained in the following list.

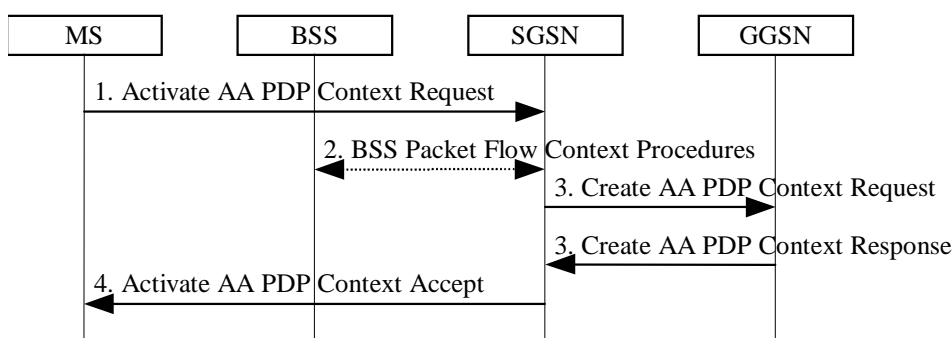


Figure 65: Anonymous Access PDP Context Activation Procedure

- 1) The MS sends an Activate AA PDP Context Request (NSAPI, TI, PDP Type, PDP Address, Access Point Name, QoS Requested, PDP Configuration Options) message to the SGSN. The MS shall use a Random TLLI at the RLC/MAC layer for identification purposes. The MS shall use PDP Address to indicate that it requires the use of a dynamic PDP address. The MS shall use Access Point Name to select a reference point to a certain external network that provides anonymous services. QoS Requested indicates the desired QoS profile. PDP Configuration Options may be used to request optional PDP parameters from the GGSN (see GSM 09.60). PDP Configuration Options is sent transparently through the SGSN.
- 2) BSS packet flow context procedures may be executed. These procedures are defined in subclause "BSS Context".

- 3) The SGSN may restrict the requested QoS value given its capabilities and the current load. The SGSN assigns an Auxiliary TLLI and creates an AA-TID for the PDP-Context. The SGSN sends a Create AA PDP Context Request (PDP Type, PDP Address, Access Point Name, QoS Negotiated, AA-TID, Selection Mode, PDP Configuration Options) message to the GGSN indicated by Access Point Name in the Activate AA PDP Context Request message. Selection Mode indicates how the APN was selected. The GGSN creates a new entry in its PDP context table and generates a Charging Id. The new entry allows the GGSN to route PDP PDUs between the SGSN and the server(s) that provide services for anonymous MSs, and to start charging. The GGSN may use Access Point Name to find an external network that provides anonymous services. The GGSN may further restrict QoS Negotiated given its capabilities and the current load. The GGSN then allocates a dynamic PDP Address and returns a Create AA PDP Context Response (AA-TID, PDP Address, BB Protocol, Reordering Required, PDP Configuration Options, QoS Negotiated, Charging Id, Cause) message to the SGSN. BB Protocol indicates whether TCP or UDP shall be used to transport user data on the backbone network between the SGSN and GGSN. Reordering Required indicates whether the SGSN shall reorder N-PDUs before delivering the N-PDUs to the MS. PDP Configuration Options contain optional PDP parameters that the GGSN may transfer to the MS. These optional PDP parameters may be requested by the MS in the Activate PDP Context Request, or may be sent unsolicited by the GGSN. PDP Configuration Options is sent transparently through the SGSN. The GGSN shall check the source and destination address in all subsequent anonymous MO PDP PDUs received from the SGSN. If the GGSN detects a not allowed address in an MO PDP PDU, then the PDP PDU shall be discarded and the MM and PDP contexts shall be deleted in the GGSN, SGSN, and MS, as defined in subclause "Anonymous Access PDP Context Deactivation Initiated by GGSN Procedure".

If QoS Negotiated received from the SGSN is incompatible with the PDP context being activated (e.g., the reliability class is insufficient to support the PDP type), then the GGSN rejects the Create AA PDP Context Request message. The compatible QoS profiles are configured by the GGSN operator.

- 4) The SGSN inserts the NSAPI along with the PDP address received from the GGSN in its PDP context. The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated and returns an Activate AA PDP Context Accept (A-TLLI, PDP Type, PDP Address, TI, QoS Negotiated, Radio Priority, Packet Flow Id, PDP Configuration Options) message to the MS. The SGSN is now able to route anonymous PDP PDUs between the GGSN and the MS and to start charging.

After an SGSN has successfully updated the GGSN, the MM and PDP contexts associated with an MS is distributed as shown in clause "Information Storage".

If the AA PDP Context Activation procedure fails or if the SGSN returns an Activate AA PDP Context Reject (Cause, PDP Configuration Options) message, then the MS may attempt another activation to the same GGSN up to a maximum number of attempts.

9.2.3 Modification Procedures

An MS or GGSN can request, or an SGSN can decide, possibly triggered by the HLR as explained in subclause "Insert Subscriber Data Procedure", to modify parameters that were negotiated during an activation procedure for one or several PDP contexts. The following parameters can be modified:

- QoS Negotiated;
- Radio Priority;
- Packet Flow Id; and
- PDP Address (in case of the GGSN-initiated modification procedure).

The SGSN can request the modification of parameters by sending a Modify PDP Context Request message to the MS.

A GGSN can request the modification of parameters by sending an Update PDP Context Request message to the SGSN.

An MS can request the modification of parameters by sending a Modify PDP Context Request message to the SGSN.

9.2.3.1 SGSN-Initiated PDP Context Modification Procedure

The SGSN-Initiated PDP Context Modification procedure is illustrated in Figure 66. Each step is explained in the following list.

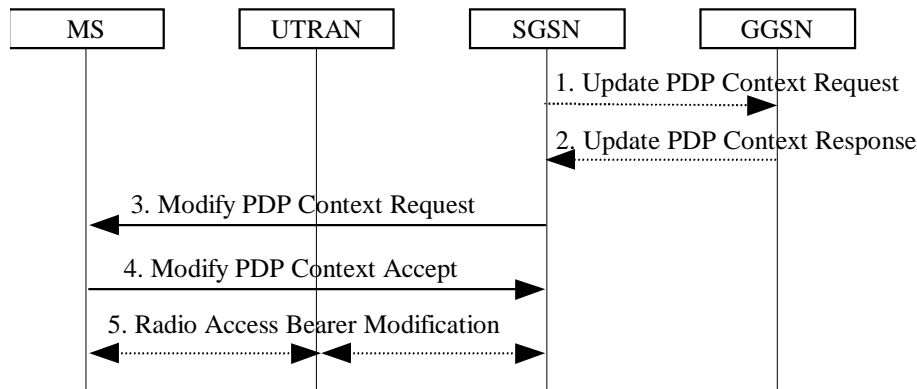


Figure 66: SGSN-Initiated PDP Context Modification Procedure

- 1) The SGSN may send an Update PDP Context Request (TID, QoS Negotiated) message to the GGSN. If QoS Negotiated received from the SGSN is incompatible with the PDP context being modified (e.g., the reliability class is insufficient to support the PDP type), then the GGSN rejects the Update PDP Context Request. The compatible QoS profiles are configured by the GGSN operator.
- 2) The GGSN may restrict QoS Negotiated given its capabilities and the current load. The GGSN stores QoS Negotiated and returns an Update PDP Context Response (TID, QoS Negotiated) message.
- 3) The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and sends a Modify PDP Context Request (TI, NSAPI, QoS Negotiated, Radio Priority, Packet Flow Id) message to the MS.
- 4) The MS acknowledges by returning a Modify PDP Context Accept message. If the MS does not accept the new QoS Negotiated it shall instead de-activate the PDP context with the PDP Context Deactivation Initiated by MS procedure.
- 5) The radio access bearer modification procedure may be executed.

9.2.3.2 GGSN-Initiated PDP Context Modification Procedure

The GGSN-Initiated PDP Context Modification procedure is illustrated in Figure 67. Each step is explained in the following list.

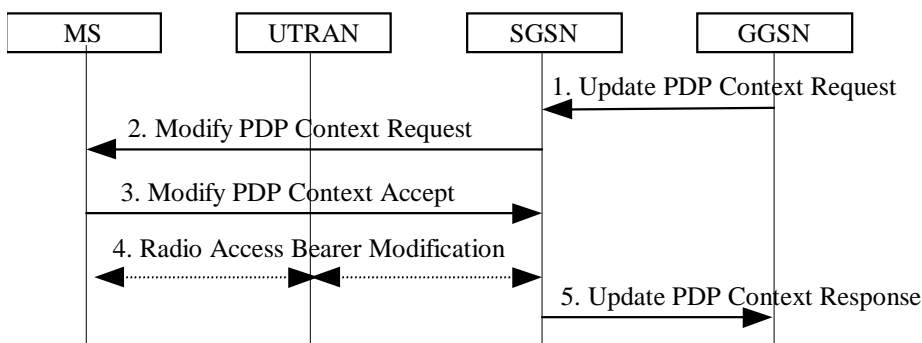


Figure 67: GGSN-Initiated PDP Context Modification Procedure

- 1) The GGSN sends an Update PDP Context Request (TID, PDP Address, QoS Requested) message to the SGSN. QoS Requested indicates the desired QoS profile. PDP Address is optional.
- 2) The SGSN may restrict the desired QoS profile given its capabilities, the current load, the current QoS profile, and the subscribed QoS profile. The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated,

and sends a Modify PDP Context Request (TI, NSAPI, PDP Address, QoS Negotiated, Radio Priority, Packet Flow Id) message to the MS. PDP Address is optional.

- 3) The MS acknowledges by returning a Modify PDP Context Accept message. If the MS does not accept the new QoS Negotiated it shall instead de-activate the PDP context with the PDP Context Deactivation Initiated by MS procedure.
- 4) For UMTS, the radio access bearer modification procedure may be executed.
- 5) Upon receipt of the Modify PDP Context Accept message, or upon completion of the RAB modification procedure, the SGSN returns an Update PDP Context Response (TID, QoS Negotiated) message to the GGSN. If the SGSN receives a Deactivate PDP Context Request message, it shall instead follow the PDP Context Deactivation Initiated by MS procedure.

9.2.3.3 MS-Initiated PDP Context Modification Procedure

The MS-Initiated PDP Context Modification procedure is illustrated in Figure 68. Each step is explained in the following list.

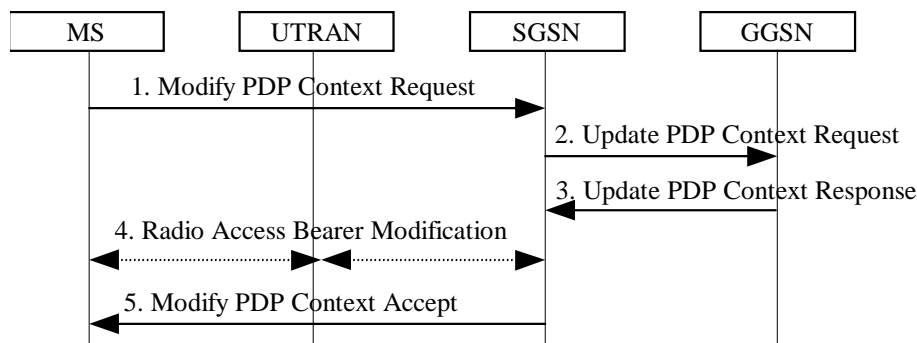


Figure 68: MS-Initiated PDP Context Modification Procedure

- 1) The MS sends a Modify PDP Context Request (TI, NSAPI, QoS Requested) message to the SGSN. QoS Requested indicates the desired QoS profile.
- 2) The SGSN may restrict the desired QoS profile given its capabilities, the current load, and the subscribed QoS profile. The SGSN sends an Update PDP Context Request (TID, QoS Negotiated) message to the GGSN. If QoS Negotiated received from the SGSN is incompatible with the PDP context being modified (e.g., the reliability class is insufficient to support the PDP type), then the GGSN rejects the Update PDP Context Request. The compatible QoS profiles are configured by the GGSN operator.
- 3) The GGSN may further restrict QoS Negotiated given its capabilities and the current load. The GGSN stores QoS Negotiated and returns an Update PDP Context Response (TID, QoS Negotiated) message.
- 4) For UMTS, the radio access bearer modification procedure may be executed.
- 5) The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns a Modify PDP Context Accept (TI, NSAPI, QoS Negotiated, Radio Priority, Packet Flow Id) message to the MS.

NOTE: If the SGSN does not accept QoS Requested, then steps 2 and 3 of this procedure are skipped, and the existing QoS Negotiated is returned to the MS in step 4.

9.2.4 Deactivation Procedures

9.2.4.1 PDP Context Deactivation Initiated by MS Procedure

The PDP Context Deactivation Initiated by MS procedure is illustrated in Figure 69. Each step is explained in the following list.

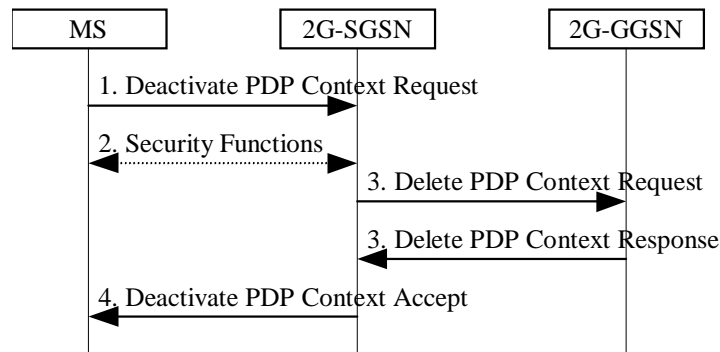


Figure 69: PDP Context Deactivation Initiated by MS Procedure for GPRS

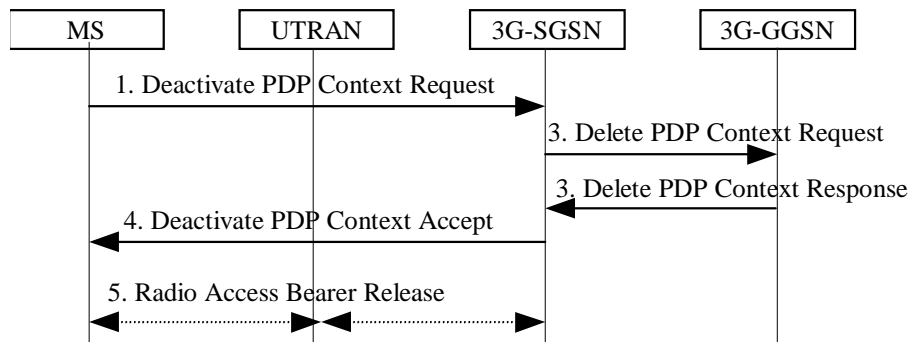


Figure 70: PDP Context Deactivation Initiated by MS Procedure for UMTS

- 1) The MS sends a Deactivate PDP Context Request (TI, NSAPI) message to the SGSN.
- 2) For GPRS security functions may be executed. These procedures are defined in subclause "Security Function".
- 3) The SGSN sends a Delete PDP Context Request (TID, Teardown Ind) message to the GGSN. If NSAPI was not included by the MS in the Deactivate PDP Context Request message, then the SGSN deactivates all PDP contexts associated with this TI and PDP address by including Teardown Ind in the Delete PDP Context Request message. The GGSN removes the PDP context(s) and returns a Delete PDP Context Response (TID) message to the SGSN. If the MS was using a dynamic PDP address allocated by the GGSN, and if the context being deactivated is the last PDP context associated with this PDP address, then the GGSN releases this PDP address and makes it available for subsequent activation by other MSs. The Delete PDP Context messages are sent over the backbone network.
- 4) The SGSN returns a Deactivate PDP Context Accept (TI, NSAPI) message to the MS.
- 5) For UMTS, the radio access bearer release procedure is executed.

At GPRS detach, all PDP contexts for the MS are implicitly deactivated.

If the SGSN receives a Deactivate PDP Context Request (TI) message for a PDP context that is currently being activated, then the SGSN shall stop the PDP Context Activation procedure without responding to the MS, and continue with the PDP Context Deactivation initiated by MS procedure.

9.2.4.2 PDP Context Deactivation Initiated by SGSN Procedure

The PDP Context Deactivation Initiated by SGSN procedure is illustrated in Figure 71. Each step is explained in the following list.

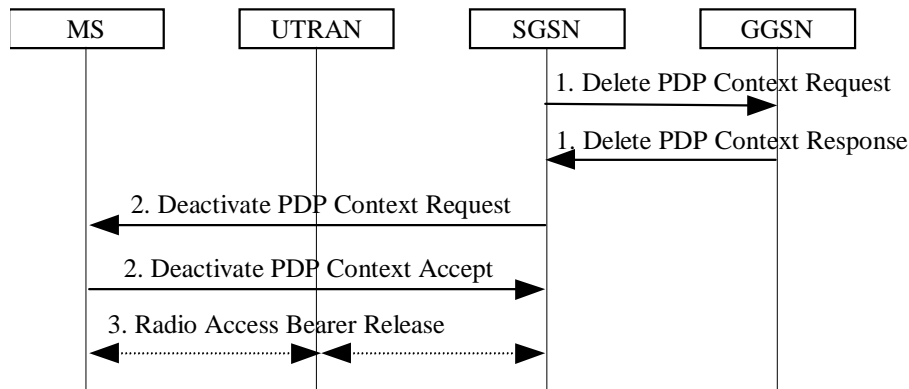


Figure 71: PDP Context Deactivation Initiated by SGSN Procedure

- 1) The SGSN sends a Delete PDP Context Request (TID, Teardown Ind) message to the GGSN. If Teardown Ind is included by the SGSN, then the GGSN deactivates all PDP contexts associated with this PDP address. The GGSN removes the PDP context and returns a Delete PDP Context Response (TID) message to the SGSN. If the MS was using a dynamic PDP address allocated by the GGSN, and if the context being deactivated is the last PDP context associated with this PDP address, then the GGSN releases this PDP address and makes it available for subsequent activation by other MSs. The Delete PDP Context messages are sent over the backbone network. The SGSN may not wait for the response from the GGSN before sending the Deactivate PDP Context Request message.
- 2) The SGSN sends a Deactivate PDP Context Request (TI, NSAPI) message to the MS. If NSAPI is not included, then all PDP contexts associated with this TI and PDP address are deactivated. The MS removes the PDP context(s) and returns a Deactivate PDP Context Accept (TI, NSAPI) message to the SGSN. NSAPI is included if received from the SGSN.
- 3) For UMTS, the radio access bearer release procedure is executed.

9.2.4.3 PDP Context Deactivation Initiated by GGSN Procedure

The PDP Context Deactivation Initiated by GGSN procedure is illustrated in Figure 72. Each step is explained in the following list.

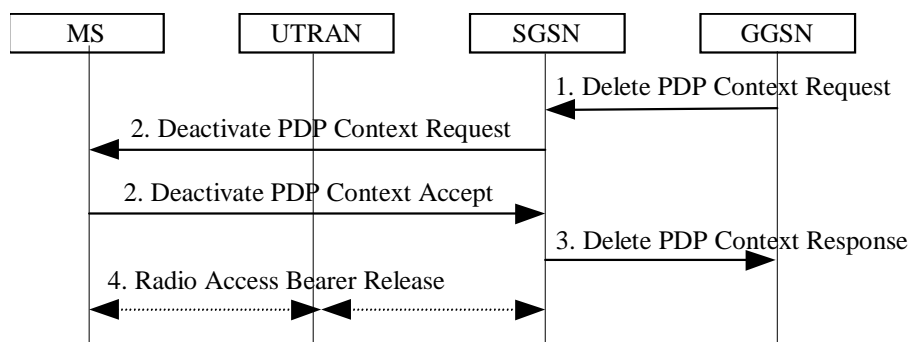


Figure 72: PDP Context Deactivation Initiated by GGSN Procedure

- 1) The GGSN sends a Delete PDP Context Request (TID, Teardown Ind) message to the SGSN. Teardown Ind indicates whether or not all PDP contexts associated with this PDP address shall be deactivated.
- 2) The SGSN sends a Deactivate PDP Context Request (TI, NSAPI) message to the MS. If NSAPI was not included by the SGSN, then all PDP contexts associated with this TI and PDP address are deactivated. The MS removes

the PDP context(s) and returns a Deactivate PDP Context Accept (TI, NSAPI) message to the SGSN. NSAPI is included if received from the SGSN.

- 3) The SGSN returns a Delete PDP Context Response (TID, Teardown Ind) message to the GGSN. If the MS was using a dynamic PDP address allocated by the GGSN, and if the context being deactivated is the last PDP context associated with this PDP address, then the GGSN releases this PDP address and makes it available for subsequent activation by other MSs. The Delete PDP Context messages are sent over the backbone network. The SGSN may not wait for the response from the MS before sending the Delete PDP Context Response message.
- 3) For UMTS, the radio access bearer release procedure is executed.

9.2.4.4 Anonymous Access PDP Context Deactivation Initiated by MS Procedure

The MS shall not issue explicit deactivation request messages to delete anonymous contexts in the network. Instead, the READY timer shall be used as an implicit deactivation timer to save signalling traffic on the radio interface.

The Anonymous Access PDP Context Deactivation Initiated by MS procedure is illustrated in Figure 73. Each step is explained in the following list.

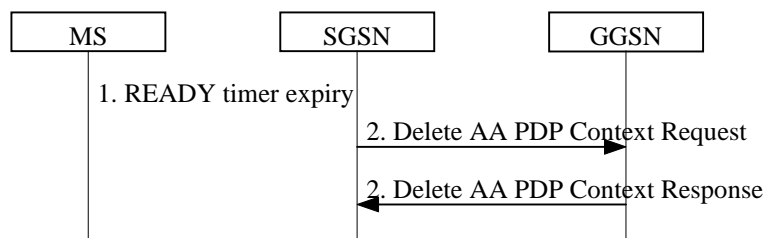


Figure 73: Anonymous Access PDP Context Deactivation Initiated by MS Procedure

- 1) The READY timer expires in the MS and SGSN.
- 2) The SGSN sends a Delete AA PDP Context Request (AA-TID) message. The GGSN removes the PDP context and returns a Delete AA PDP Context Response (AA-TID) message to the SGSN. The GGSN releases this PDP address and makes it available for subsequent anonymous activation by other MSs.

9.2.4.5 Anonymous Access PDP Context Deactivation Initiated by GGSN Procedure

If the GGSN detects a misuse or fraud of the anonymous context as described in subclause "Anonymous Access PDP Context Activation Procedure", step 2, it shall initiate the deactivation independently of the READY timer expiry.

If the anonymous server detects a misuse or fraud, it may request the GGSN to deactivate the AA context. The method that the anonymous server uses to inform the GGSN is outside the scope of the GSM specifications.

The Anonymous Access PDP Context Deactivation Initiated by GGSN procedure is illustrated in Figure 74. Each step is explained in the following list.

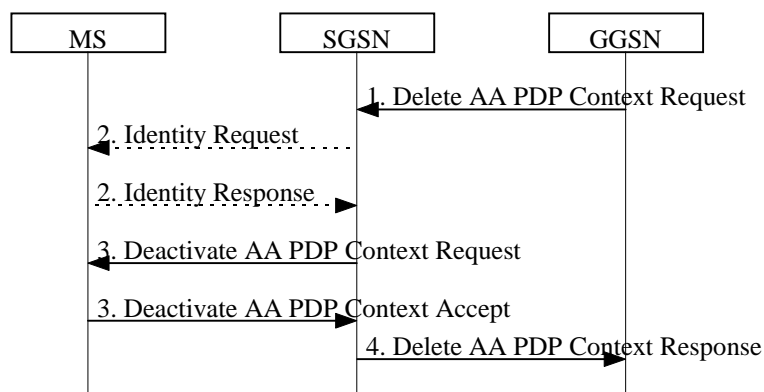


Figure 74: Anonymous Access PDP Context Deactivation Initiated by GGSN Procedure

- 1) The GGSN sends a Delete AA PDP Context Request (AA-TID) message to the SGSN.
- 2) The SGSN may send an Identity Request (Identity Type = IMSI or IMEI) message to the MS. The MS shall respond with an Identity Response (IMSI or IMEI) message.
- 3) The SGSN sends a Deactivate AA PDP Context Request (TI) message to the MS. The MS removes the PDP context and returns a Deactivate AA PDP Context Accept (TI) message to the SGSN.
- 4) The SGSN returns a Delete AA PDP Context Response (AA-TID) message to the GGSN. The GGSN releases this PDP address and makes it available for subsequent activation by other MSs. The Delete AA PDP Context messages are sent over the backbone network. The SGSN may not wait for the accept from the MS before sending the Delete AA PDP Context Response message.

9.3 Packet Routeing and Transfer Function

The packet routeing and transfer function:

- routes and transfers packets between a mobile TE and an external network, i.e., between reference point R and reference point Gi;
- routes and transfers packets between mobile TE and other GPRS PLMN, i.e., between reference point R and reference point Gi via interface Gp; and
- routes and transfers packets between TEs, i.e., between the R reference point in different MSs.

The PDP PDUs shall be routed and transferred between the MS and the GGSN as N-PDUs. The maximum size of each N-PDU shall be 1 500 octets [FFS]. When the MS or the GGSN receives a PDP PDU that is not larger than the maximum N-PDU size, then the PDP PDU shall be routed and transferred as one N-PDU. When the MS or the GGSN receives a PDP PDU that is larger than the maximum N-PDU size, then the PDP PDU shall be segmented, discarded or rejected, depending on the PDP type and the implementation. The packet data protocol in the MS may limit the maximum size of the PDP PDUs that are routed and transferred, e.g., due to MS memory limitations.

Between the 2G-SGSN and the MS, PDP PDUs are transferred with SNDSCP. Between the 3G-SGSN and the MS, PDP PDUs are transferred with GTP-U and PDCP.

Between the SGSN and the GGSN, PDP PDUs are routed and transferred with either the TCP/IP or the UDP/IP protocols. The GPRS Tunnelling Protocol transfers data through tunnels. A tunnel is identified by a tunnel identifier (TID) and a GSN address.

To support roaming subscribers, and for forward compatibility, the SGSN is not required to know the tunnelled PDP. Every SGSN shall have the capability to transfer PDUs belonging to PDPs not supported in the PLMN of the SGSN.

9.4 Relay Function

The relay function of a network node transfers the PDP PDUs received from the incoming link to the appropriate outgoing link. At the RNC, the SGSN, and the GGSN the relay function stores all valid PDP PDUs until they are forwarded to the next network node or until the maximum holding time of the PDP PDUs is reached. The PDP PDUs are discarded when buffering is longer than their maximum holding time. This maximum holding time is implementation dependent and can be influenced by the PDP type, the QoS of the PDP PDU, the resource load status, and by buffer conditions. The discarding protects resources from useless transfer attempts, especially the radio resource. Impacts on user protocol operation by too short holding time shall be avoided.

In GPRS, the SGSN and GGSN relay functions add sequence numbers to PDP PDUs received from SNDSCP and from the Gi reference point, respectively. In UMTS, the RNC and GGSN relay functions add sequence numbers to PDP PDUs received from PDCP and from the Gi reference point, respectively. The SGSN relay function may perform re-sequencing of PDP PDUs before passing the PDP PDUs to SNDSCP for GPRS. The GGSN relay function may perform re-sequencing of PDP PDUs before passing the PDP PDUs to the Gi reference point. The RNC may perform re-sequencing of PDP PDUs before passing the PDP PDUs to PDCP.

9.5 Packet Terminal Adaptation Function

The Packet Terminal Adaptation function adapts packets received from and transmitted to the Terminal Equipment to a form suitable for transmission within the PLMN.

A range of MT versions providing different standard interfaces towards the TE can be used, e.g.:

- MT with asynchronous serial interface and PAD (Packet Assembly / Disassembly) support (e.g., AT command set PAD, X.28 [35] / X.29 [36] / X.3 [33] PAD). In the case when the PAD function does not exist in the MT, it exists in the TE.
- "Embedded MT" integrated with the TE, possibly via an industry-standard application program interface.
- MT with synchronous serial interface.

9.6 Encapsulation Function

The packet domain transparently transports PDP PDUs between external networks and MSs. All PDP PDUs are encapsulated and decapsulated for routing purposes. Encapsulation functionality exists at the MS, at the RNC, at the SGSN, and at the GGSN. Encapsulation allows PDP PDUs to be delivered to and associated with the correct PDP context in the MS, the SGSN, or the GGSN. Two different encapsulation schemes are used; one for the backbone network between two GSNs and between an SGSN and an RNC, and one for the GPRS connection between the SGSN and the MS or for the UMTS RRC connection between the RNC and the MS.

Encapsulation requires that the MS is attached to GPRS, and that the PDP Context Activation procedure has been executed. If the PS Attach or PDP Context Activation procedures cannot be successfully executed, then uplink PDP PDUs are discarded in the MS. If these procedures have not been executed when a downlink PDP PDU arrives in the GGSN, then the downlink PDP PDU shall be discarded, rejected, or the Network-Requested PDP Context Activation procedure shall be initiated.

9.6.1 Encapsulation Between GSNs

The packet domain PLMN backbone network encapsulates a PDP PDU with a GPRS Tunnelling Protocol header, and inserts this GTP PDU in a TCP PDU or UDP PDU that again is inserted in an IP PDU. The IP and GTP PDU headers contain the GSN addresses and tunnel endpoint identifier necessary to uniquely address a GSN PDP context.

9.6.2 Encapsulation Between 3G-SGSN and RNC

On the Iu interface, a PDP PDU is encapsulated with a GPRS Tunnelling Protocol header.

9.6.2 Encapsulation Between 2G-SGSN and MS

Between a 2G-SGSN and an MS, an SGSN or MS PDP context is uniquely addressed with a temporary logical link identity and a network layer service access point identifier pair. TLLI is derived from the P-TMSI. An NSAPI is assigned when the MS initiates the PDP Context Activation function. The relationship between TLLI / NSAPI and LLC / SMDCP is illustrated in Figure 75. TLLI and NSAPI are described in subclause "NSAPI and TLLI".

9.6.3 Encapsulation Between RNC and MS

On the Uu interface, a PDP PDU is encapsulated with PDCP.

10 Message Screening Functionality

This screening mechanism may be performed by routers and firewalls, and performs the selection of which packets to allow and which to deny.

Only network-controlled message screening shall be supported. Network-controlled screening is used to protect the packet domain PLMN from known security problems, and the screening provided by a certain PLMN is applied independently of the MS user. Network-controlled screening is outside the scope of this specification.

11 Compatibility Issues

Non-GPRS MSs in GSM PLMNs that support GPRS shall, without changes, be able to continue operation.

GSM PLMNs that do not support GPRS shall, without changes, be able to continue interworking with GSM PLMNs that do support GPRS.

A GPRS ME shall be able to access GPRS services with GPRS-aware SIMs, and with SIMs that are not GPRS-aware. A GPRS-aware SIM is able to store information in the elementary files EF_{KcGPRS} and EF_{LOCIGPRS}, as defined in GSM 11.11 [28].

The compatibility of SIMs and USIMs with GPRS MEs or UMTS MEs is defined in UMTS 22.102.

12 Transmission

12.1 Transmission Modes

For GPRS, the GTP-U, LLC, and RLC protocols offer various transmission modes. The combinations of the GTP-U, LLC, and RLC transmission modes define the QoS reliability classes (see subclause "Reliability Class").

For UMTS, the GTP-U and RLC protocols provide various transmission modes to support user data transmission with different QoS.

The RLC protocol for GPRS and the RLC protocol for UMTS are distinct protocols of different Radio Access Networks.

12.1.1 GTP-U Transmission Modes

Two modes of operation of the GTP-U layer are supported for information transfer between the GGSN and SGSN; unacknowledged (UDP/IP) and acknowledged (TCP/IP). The GTP-U layer shall support both modes simultaneously. In UMTS, GTP-U is also used on the Iu interface for user data transport. Only the unacknowledged mode (UDP/IP) is supported on the Iu interface.

[Check the Gn TCP support in UMTS.]

12.1.2 LLC Transmission Modes for GPRS

Two modes of operation of the LLC layer are defined for information transfer; unacknowledged and acknowledged. The LLC layer shall support both modes simultaneously.

- In acknowledged mode, the receipt of LL-PDUs are confirmed. The LLC layer retransmits LL-PDUs if confirmation has not been received within a timeout period.
- In unacknowledged mode, there is no confirmation required for LL-PDUs.

Signalling and SMS shall be transferred in unacknowledged mode.

In unacknowledged mode, the LLC layer shall offer the following two options:

- transport of "protected" information, such that errors within the LLC information field result in the frame being discarded; and
- transport of "unprotected" information, such that errors within the LLC information field do not result in the frame being discarded.

The LLC layer shall support several different QoS delay classes with different transfer delay characteristics.

12.1.3 RLC Transmission Modes

Two modes of operation of the RLC layer are defined for information transfer; unacknowledged and acknowledged. The RLC layer shall support both modes simultaneously.

The RLC for GPRS is described in GSM 04.60, and for UMTS in UMTS 25.322.

12.2 Logical Link Control Functionality for GPRS

The Logical Link Control (LLC) protocol provides a reliable logical link between the MS and its SGSN. As shown in subclause "User and Control Planes", the LLC layer is situated below the SNDC layer.

12.2.1 Addressing

TLLI is used for addressing at the LLC layer. TLLI is described in subclause "NSAPI and TLLI".

12.2.2 Services

LLC provides the services necessary to maintain a ciphered data link between an MS and an SGSN. The LLC layer does not support direct communication between two MSs.

The LLC connection is maintained as the MS moves between cells served by the same SGSN. When the MS moves to a cell being served by a different SGSN, the existing connection is released and a new logical connection is established with the new SGSN.

LLC shall be independent of the underlying radio interface protocols. In order to allow LLC to operate with a variety of different radio interface protocols, and to ensure optimum performance, it may be necessary to adjust e.g., the maximum LLC PDU length and the LLC protocol timer values. Such adjustments can be made through negotiation between the MS and the SGSN. The maximum length of an LLC PDU shall not be greater than 1 600 octets minus the BSSGP protocol control information.

12.2.3 Functions

The Logical Link Control layer supports:

- service primitives allowing the transfer of SNDCP Protocol Data Units (SN-PDUs) between the Subnetwork Dependent Convergence layer and the Logical Link Control layer;
- procedures for transferring LL-PDUs between the MS and SGSN, including:
 - procedures for unacknowledged delivery of LL-PDUs between the MS and the SGSN; and
 - procedures for acknowledged, reliable delivery of LL-PDUs between the MS and SGSN;
- procedures for detecting and recovering from lost or corrupted LL-PDUs;
- procedures for flow control of LL-PDUs between the MS and the SGSN; and
- procedures for ciphering of LL-PDUs. The procedures are applicable to both unacknowledged and acknowledged LL-PDU delivery.

The layer functions are organised in such a way that ciphering resides immediately above the RLC/MAC layer in the MS, and immediately above the BSSGP layer in the SGSN.

12.3 Subnetwork Dependent Convergence Functionality for GPRS

The Subnetwork Dependent Convergence (SNDC) protocol is situated below the network layer and above the Logical Link Control layer in the MS and the SGSN, as shown in subclause "User and Control Planes". A variety of network layers are supported, e.g., IP and X.25. The network-layer packet data protocols share the same SNDCP, that then performs multiplexing of data coming from the different sources to be sent across LLC. This is illustrated in Figure 75.

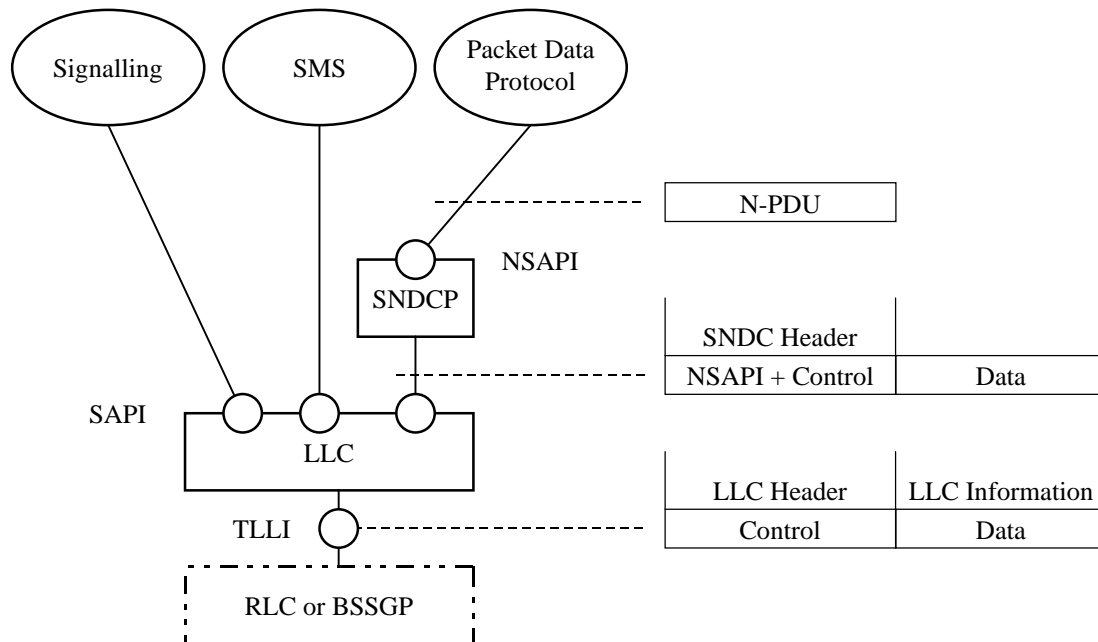


Figure 75: Multiplexing of Network Protocols

The following identities and control information is needed:

- NSAPI identifies the network layer. The SNDCP control part contains compression information.
- TLLI identifies the MS. The LLC control part contains the rest of the LLC protocol header including ciphering information.

The Subnetwork Dependent Convergence function is defined in terms of offered services and sub-functions.

12.3.1 Services

The SNDC function provides the following services to the network layer:

- Transmission and reception of N-PDUs in acknowledged and unacknowledged LLC mode. In acknowledged mode, the receipt of data shall be confirmed at the LLC layer, and the data shall be transmitted and received in order per NSAPI. In unacknowledged mode, the receipt of data shall not be confirmed at the SNDCP layer nor at the LLC layer.
- Transmission and reception between the MS and SGSN of variable-length N-PDUs.
- Transmission and reception of N-PDUs between the SGSN and MS according to the negotiated QoS profile.
- Transfer of the minimum amount of data possible between the SGSN and MS through compression techniques.

The SNDC function requires the following services from the LLC layer:

- Acknowledged and unacknowledged data transfer.
- Ciphered transmission of SN-PDUs.

- In-order delivery of SN-PDUs per LLC SAPI.
- Support for variable-length SN-PDUs.

12.3.2 Subfunctions

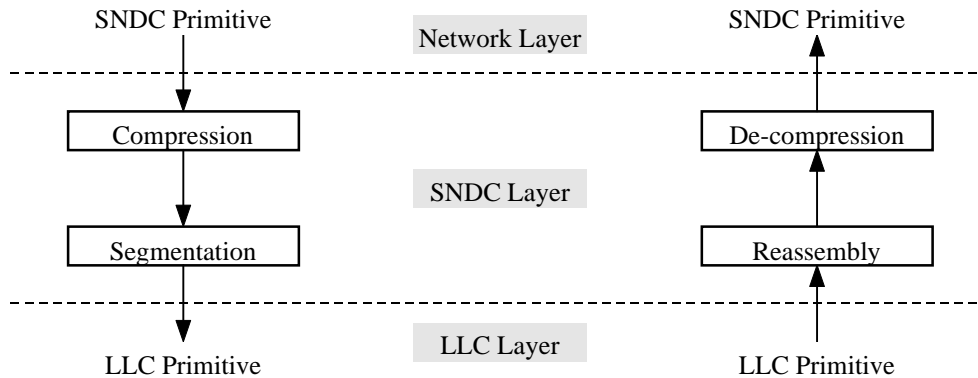


Figure 76: Sequential Invocation of SNDC Functionality

SNDCP performs the following subfunctions:

- Mapping of SNDC primitives received from the network layer into corresponding LLC primitives to be passed to the LLC layer, and vice versa.
- Multiplexing of N-PDUs from one or several NSAPIs onto one LLC SAPI. NSAPIs that are multiplexed onto the same SAPI shall use the same radio priority level, QoS delay class, and precedence class.
- Compression of redundant protocol control information and user data. This may include e.g., TCP/IP header compression and V.42 bis [32] data compression. Compression may be performed independently for each QoS delay class and precedence class. If several network layers use the same QoS delay class and precedence class, then one common compressor may be used for these network layers. The relationship between NSAPIs, compressors, and SAPIs is defined in GSM 04.65. Compression parameters are negotiated between the MS and the SGSN. Compression is an optional SNDC function.
- Segmentation and reassembly. The output of the compression subfunctions are segmented to maximum-length LLC frames.

12.4 PDCP for UMTS

The Packet Data Compatibility Protocol (PDCP) transmission functionality maps network-level characteristics onto the characteristics of the underlying network. PDCP can support several network layer protocols by providing protocol transparency for the users of the service. PDCP provides protocol control information compression. PDCP is located in the MS and the UTRAN and described in UMTS 25.323.

12.5 Octet Stream Protocol Functionality

The Octet Stream Protocol (OSP) is used to carry an unstructured octet (character) stream between the MS and GGSN. It is used to provide a character pipe to allow an MS to communicate (via the GGSN) with an arbitrary Internet host, or other character-based service. PDP type shall be selected as OSP for this purpose. Unlike PDP types IP and X.25, OSP has no existence outside the PLMN. In the MS there is a character stream at the R reference point together with some optional control signals. In the GGSN there is a relay function, carrying the same character stream and control signals between OSP and a fixed-network protocol stack.

OSP has two modes of operation. In octet mode, it uses a Packet Assembly function to assemble a number of user octets into a single packet for more efficient transport by the underlying protocols. A complementary Packet Disassembly function performs the reverse operation in the peer OSP. In block mode, the Packet Assembly / Disassembly (PAD) function is bypassed. In this case, data is transferred between the OSP user and OSP in blocks of octets. Each block of

octets is delivered as a single OSP PDU to the underlying protocol. The selection of octet or block mode is made independently for each OSP connection as an implementation or configuration decision before the connection is established, and remains fixed for the duration of the connection. An example of the use of the block mode is when OSP is used for interworking with a fixed network where the octets are also carried in packets. This avoids the use of back-to-back PADs. It could also be used in an embedded MT where the application transfers data in blocks of octets.

The quality of service is determined mainly by that provided by the underlying layers. However, the end-to-end delay may be affected by the presence of the PAD function. A reliable (acknowledged) service shall be provided by the layers below SNDCP and GTP.

The main functions of OSP are:

- transport of an unstructured octet stream;
- packet assembly and disassembly to make efficient use of network resources; and
- end-to-end flow control.

OSP may additionally provide:

- transport of a "break" signal;
- transport of control information blocks between the OSP users;
- user control of packet assembly buffer forwarding; and
- direct OSP user access to the underlying packet service, bypassing the PAD.

Figure 77 illustrates the OSP user plane for GPRS, and Figure 78 for UMTS.

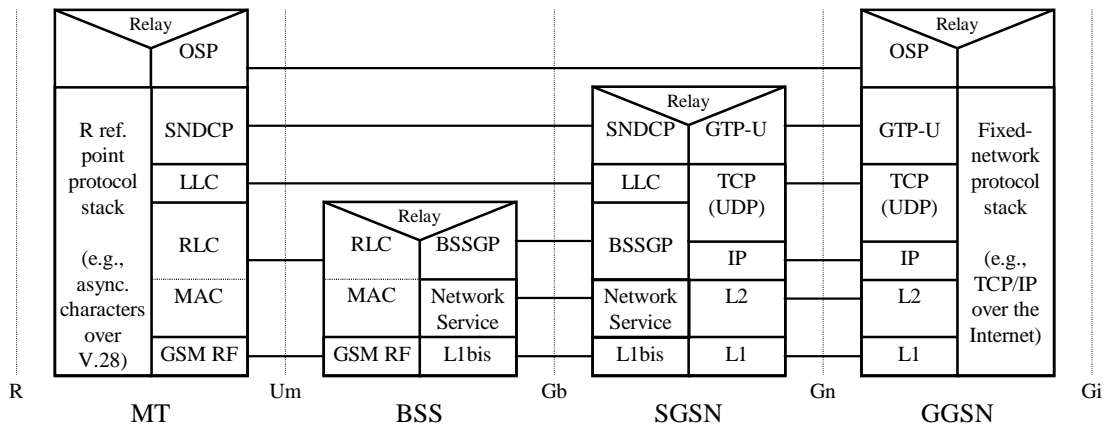


Figure 77: GPRS User Plane for PDP Type OSP

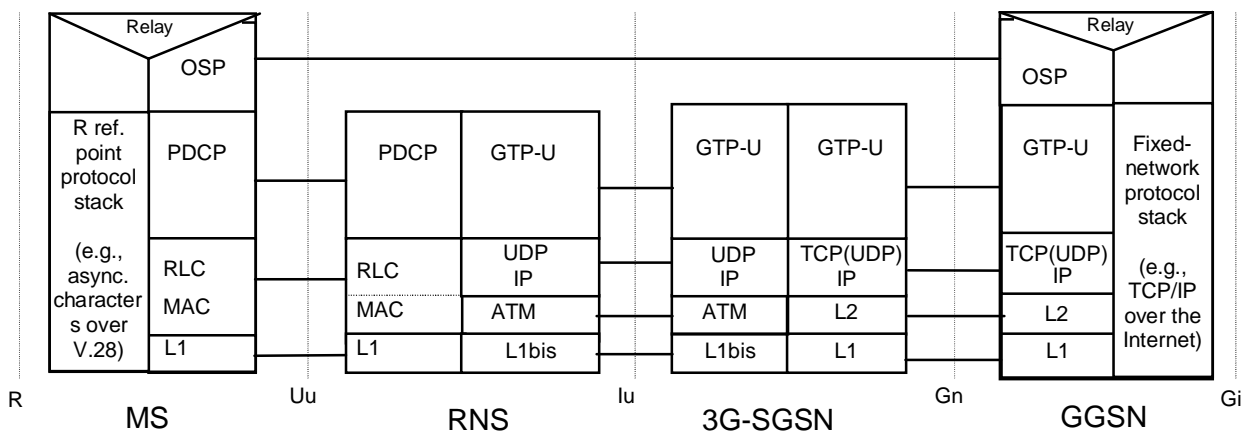


Figure 78: UMTS User Plane for PDP Type OSP

12.5.1 PAD Function

In order to make efficient use of the network resources, particularly the radio resource, octets received from the OSP user are not forwarded immediately but are placed in a buffer. When some forwarding criterion is satisfied, the contents of the buffer are forwarded in the payload of an N-PDU to the underlying layer. At the receiving end, the payload of an N-PDU received from the underlying layer is placed in a buffer and the octets are delivered to the OSP user as an octet stream.

The PAD is used only when OSP operates in octet mode. It is not used when OSP operates in block mode.

12.5.1.1 Packet Assembler

The packet assembler shall be able to detect the following forwarding criteria. When any one criterion is satisfied, the contents of the buffer shall be forwarded in an N-PDU to the underlying layer, subject to any flow control condition.

12.5.1.1.1 Buffer Full

The buffer contents are forwarded when the number of octets in the buffer reaches the value of the maximum buffer size parameter.

12.5.1.1.2 Inactivity Timer Expiry

The inactivity timer shall be started whenever an octet is placed in the buffer. When the timer expires, the buffer contents shall be forwarded. The inactivity timer shall be stopped whenever a buffer is forwarded.

12.5.1.1.3 Maximum Buffer Delay Timer Expiry

A maximum buffer delay timer may be started when the first octet is placed in the (empty) buffer. When the timer expires, the buffer contents shall be forwarded. This optional timer ensures that no octet is delayed in the buffer for longer than the specified time. The maximum buffer delay timer shall be stopped whenever a buffer is forwarded.

12.5.1.1.4 Special Character

Whenever an octet has been placed in the buffer, its least significant 7 bits shall be compared with a list of 7-bit special characters. If the bits match, the buffer shall be forwarded. The possible characters and combinations of characters shall be the same as specified for the X.3 PAD access to X.25.

12.5.1.1.5 Change in Flow Control State

The buffer may be forwarded when there is a need to signal a change in the ready to receive condition.

12.5.1.1.6 Immediate Forwarding Request

When the OSP receives an immediate forward request from its user, it shall immediately forward the buffer unless it is empty.

12.5.1.2 Packet Disassembler

The packet disassembler shall forward the contents of the N-PDU payload to the OSP user, subject to any local flow control condition.

12.5.2 Quality of Service

The QoS provided by the OSP layer is determined by that provided by the underlying protocol layers. However, the PAD functions introduce an additional variable delay into the transmission path. This delay can be limited at the risk of making less efficient use of network resources, in particular the radio resources.

12.6 Point-to-Point Protocol Functionality

[This subclause has not been checked against UMTS.]

The PPP protocol is specified in RFC 1661 [44].

12.6.1 User Plane for PDP Type PPP

The user plane for the PDP type PPP consists of a PPP protocol stack above SNDCP for GPRS or above PDCP for UMTS in the MS, and above GTP in the GGSN. The GGSN may either terminate the PPP protocol and access the packet data network at the IP level, or further tunnel PPP PDUs via e.g., L2TP.

In case the application above PPP uses a different protocol than IP (e.g., IPX or AppleTalk), the interconnection to the packet data network is outside the scope of this specification.

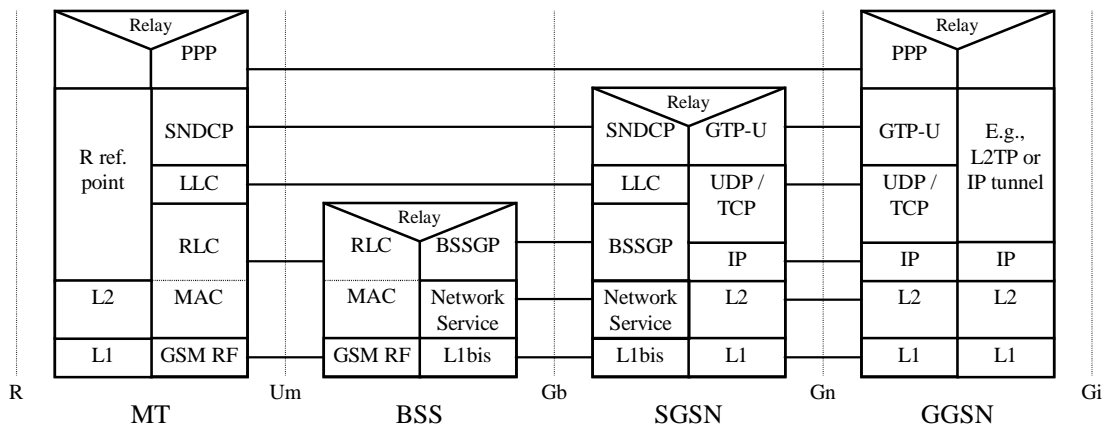


Figure 79: GPRS User Plane for PDP Type PPP

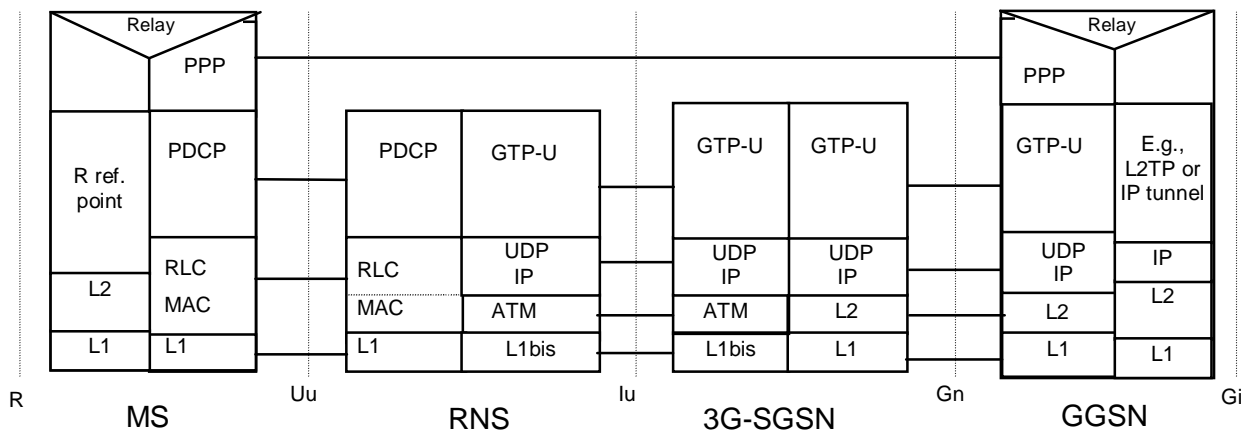


Figure 80: UMTS User Plane for PDP Type PPP

12.6.2 Functions

The PPP peers at the MS and GGSN handle the PPP protocol as specified in RFC 1661. PPP requires in-sequence packet delivery by the underlying protocols. Concerning GTP, this shall be achieved by enabling Reordering Required upon GTP tunnel establishment. For GPRS, concerning SNDCP, out-of-sequence packets, that may be present if LLC operates in unacknowledged mode, shall be discarded. SNDCP for GPRS, and PDCP for UMTS, shall not use TCP/IP header compression because PPP may not carry IP packets at all, or because PPP may carry IP packets with already compressed TCP/IP headers. These PPP options are negotiated during the RFC 1661 Network Control Protocol establishment phase.

12.7 Gb Interface for GPRS

The Gb interface connects the BSS and the SGSN, allowing the exchange of signalling information and user data. The Gb interface shall allow many users to be multiplexed over the same physical resource. Resources are given to a user upon activity (when data is sent or received) and are reallocated immediately thereafter. This is in contrast to the A interface where a single user has the sole use of a dedicated physical resource throughout the lifetime of a call irrespective of activity.

GPRS signalling and user data are sent in the same user plane. No dedicated physical resources are required to be allocated for signalling purposes.

Access rates per user may vary without restriction from zero data to the maximum possible line rate (e.g., 1 984 kbit/s for the available bitrate of an E1 trunk).

12.7.1 Physical Layer Protocol

Several physical layer configurations and protocols are possible, as defined in GSM 08.14 [19].

The physical resources shall be allocated by O&M procedures.

12.7.2 Link Layer Protocols

The Gb interface link layer is based on Frame Relay, as defined in GSM 08.16. Frame Relay virtual circuits are established between SGSN and BSS. LLC PDUs from many users are multiplexed on these virtual circuits. The virtual circuits may be multi-hop and traverse a network of Frame Relay switching nodes. Frame Relay shall be used for signalling and data transmission.

The following characteristics apply for the Frame Relay connection:

- The maximum Frame Relay information field size shall be 1 600 octets.
- The Frame Relay address length shall be 2 octets.
- The BSS and the SGSN shall both implement Frame Relay DTE functionality. The SGSN may optionally also implement DCE functionality.
- Frame Relay PVCs shall be used.
- The Frame Relay layer offers detection of but no recovery from transmission errors.
- One or more Frame Relay PVCs shall be used between one SGSN and one BSS to transport BSSGP PDUs.

12.7.3 BSS GPRS Protocol

The primary function of BSSGP is to provide the radio-related, QoS, and routing information that is required to transmit user data between a BSS and an SGSN. In the BSS, it acts as an interface between LLC frames and RLC/MAC blocks. In the SGSN, it forms an interface between RLC/MAC-derived information and LLC frames. A secondary function is to enable two physically distinct nodes, the SGSN and BSS, to operate node management control functions.

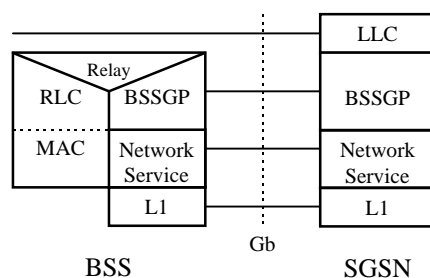


Figure 81: BSSGP Protocol Position

There is a one-to-one relationship between the BSSGP protocol in the SGSN and in the BSS. If one SGSN handles multiple BSSs, the SGSN has to have one BSSGP protocol machine for each BSS.

The main functions for the BSSGP protocol are to:

- provide a connection-less link between the SGSN and the BSS;
- transfer data unconfirmed between the SGSN and the BSS;
- provide tools for bi-directional control of the flow of data between the SGSN and the BSS;
- handle paging requests from the SGSN to the BSS;
- give support for flushing of old messages in the BSS e.g., when an MS changes BSS; and
- support multiple layer 2 links between the SGSN and one BSS.

BSSGP is defined in GSM 08.18.

12.7.3.1 Inter-dependency of the BSSGP and LLC Functions

The functions of the BSSGP shall be defined in the context of the LLC function in order to avoid duplication of functions and information flows. The following functional model indicates each layer's functional responsibilities.

Table 4: Mapping of High-level Functions Across the Gb Architecture

Network Node and Function	MS	BSS	SGSN
LLC: GSM 04.64	Same as for the SGSN.		Provides transfer of frames between the SGSN and MS.
BSSGP: GSM 08.18		<p>MS←PLMN: Using BSSGP information, RLC/MAC operations are invoked.</p> <p>MS→PLMN: Using RLC/MAC-derived information, a BSSGP PDU is constructed. An identifier of the cell including RAC and LAC in which an LLC frame was received is inserted into the BSSGP PDU.</p> <p>Same as for SGSN.</p>	<p>Individual MS radio-related information is used by the BSS to transfer LLC frames across the Gb and Um.</p> <p>Provides flow control and unconfirmed data delivery services across the Gb interface (not the Um – this is the function of the LLC and RLC/MAC function).</p> <p>Provides SGSN-BSS node management functions.</p>
Network Service: GSM 08.16		Same as for SGSN	Provides a multiplexing, variable-bandwidth, frame-based, link layer transport mechanism across the Gb interface, and load balancing.

12.7.3.2 BSSGP Addressing

For information transfer between the SGSN and the BSS the BSSGP is using a BSSGP Virtual Connection Identifier (BVCI) for addressing. Additionally, QoS profile, and the MS identification, e.g., TLLI, may be used to create queues and contexts in both the SGSN and the BSS. The flow control mechanism is then based on these queues and contexts.

12.7.3.3 BVC I Contexts in BSS and in SGSN

A BVC I context in the BSS consists of at least one queue for LLC PDUs and of the available radio resource capacity.

The BVC I context in the BSS is allocated for each cell supporting GPRS. For each new GPRS cell introduced in the BSS area, a new BVC I context shall be allocated.

In the SGSN the BVC I context consists of at least one queue for LLC PDUs and the allowed throughput on BSSGP. The allowed throughput is updated by BSSGP flow control messages.

12.7.3.4 Flow Control Between SGSN and BSS over the Gb Interface

The flow control mechanism controls the loading of the BSS LLC PDU queues per BVC I and per MS between the SGSN and the BSS in the downlink direction. No flow control is performed in the uplink direction. Buffers and link capacity shall be dimensioned to avoid loss of uplink data.

The downlink flow control mechanism is based on the following principles:

- In the SGSN, queues for LLC PDUs are provided per BVC I. These queues may be split further, e.g., per MS or per QoS delay class or precedence class. The SGSN shall pass LLC PDUs to LLC via BSSGP to the BSS as long as the allowed BSSGP throughput is not exceeded. The allowed BSSGP throughput is given per BVC I and for a single MS on that BVC I. The SGSN schedules the BSSGP downlink traffic of all MSs of a BVC I according to both throughput parameters and to the QoS profile related to each LLC PDU. The scheduling algorithm is implementation dependent.
- In the BSS, queues per BVC I are provided at the BSSGP level. These queues may be split further, e.g., per MS or per QoS delay class or precedence class. Depending on the queuing conditions and the available radio resource capacity in the cell the BSS indicates the allowed BSSGP throughput per BVC I and the default allowed BSSGP throughput for each individual MS of that BVC I by BSSGP flow control messages to the SGSN. Additionally, the BSS may change the allowed BSSGP throughput for an individual MS by a BSSGP flow control message.

12.7.3.5 BSS Context

The SGSN can provide a BSS with information related to ongoing user data transmission. The information related to one MS is stored in a BSS context. The BSS may contain BSS contexts for several MSs. A BSS context contains a number of BSS packet flow contexts. Each BSS packet flow context is identified by a packet flow identifier assigned by the SGSN. A BSS packet flow context is shared by one or more activated PDP contexts with identical or similar negotiated QoS profiles. The data transmission related to PDP contexts that share the same BSS packet flow context constitute one packet flow.

Two packet flows are pre-defined, and identified by two reserved packet flow identifier values. The BSS shall not negotiate BSS packet flow contexts for these pre-defined packet flows with the SGSN. One pre-defined packet flow is used for best-effort service, and one is used for SMS. The SGSN can assign the SMS packet flow identifier to any PDP context, and the BSS shall in this case handle the packet flow for this PDP context with the same QoS that it handles SMS with.

The combined BSS QoS profile for the PDP contexts that share the same packet flow is called the aggregate BSS QoS profile. The aggregate BSS QoS profile is considered to be a single parameter with multiple data transfer attributes as defined in subclause "Quality of Service Profile". It defines the QoS that must be provided by the BSS for a given packet flow between the MS and the SGSN, i.e., for the Um and Gb interfaces combined. The aggregate BSS QoS profile is negotiated between the SGSN and the BSS.

A BSS packet flow timer indicates the maximum time that the BSS may store the BSS packet flow context. The BSS packet flow timer shall not exceed the value of the READY timer for this MS. The BSS packet flow timer is started when the BSS packet flow context is stored in the BSS and when an LLC frame is received from the MS. When the BSS packet flow timer expires the BSS shall delete the BSS packet flow context.

When a PDP context is activated, modified, or deactivated, the SGSN may create, modify, or delete BSS packet flow contexts.

12.7.3.5.1 BSS Packet Flow Context Creation Procedure

On receiving a request to transmit an uplink or downlink LLC PDU for which no BSS packet flow context exists in the BSS, the BSS may request the download of the BSS packet flow context from the SGSN.

The SGSN may at any time request the creation of a BSS packet flow context, e.g., due to the activation of a PDP context.

The BSS Packet Flow Context Creation procedure is illustrated in Figure 82. Each step is explained in the following list.

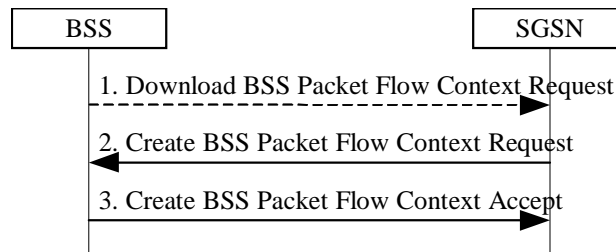


Figure 82: BSS Packet Flow Context Creation Procedure

- 1) The BSS receives a request to transfer an uplink or downlink user data LLC PDU for which it currently does not have a BSS packet flow context. In the uplink case, TLLI, Radio Priority, and Packet Flow Id are received from the MS as defined in GSM 04.60. In the downlink case, TLLI and Packet Flow Id are received from the SGSN as defined in GSM 08.18. If Packet Flow Id does not indicate best-effort service nor SMS, then the BSS sends a Download BSS Packet Flow Context Request (RAI, TLLI, Packet Flow Id) message to the SGSN. Until the BSS receives the BSS packet flow context, the BSS shall handle uplink and downlink transfers according to a default aggregate BSS QoS profile. For uplink transfers, the default profile is specific to the radio priority level.
- 2) The SGSN sends a Create BSS Packet Flow Context Request (IMSI, TLLI, Packet Flow Id, Aggregate BSS QoS Profile Requested, BSS Packet Flow Timer) message to the associated BSS.
- 3) The BSS may restrict the requested aggregate BSS QoS profile given its capabilities and the current load. The BSS creates a BSS packet flow context and inserts the parameters in its BSS context. The BSS returns a Create BSS Packet Flow Context Accept (IMSI, Packet Flow Id, Aggregate BSS QoS Profile Negotiated) message to the SGSN. The BSS uses the negotiated aggregate BSS QoS profile when allocating radio resources and other resources such as buffer capacity.

12.7.3.5.2 SGSN-Initiated BSS Packet Flow Context Modification Procedure

The SGSN may at any time request the modification of the contents of an existing BSS packet flow context, e.g., due to the activation, modification, or deactivation of a PDP context.

The SGSN-Initiated BSS Packet Flow Context Modification procedure is illustrated in Figure 83. Each step is explained in the following list.

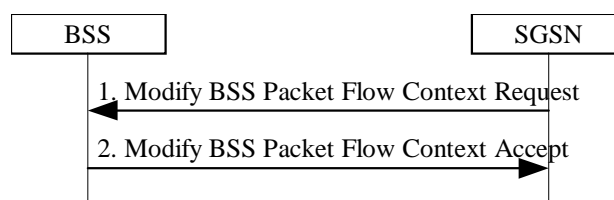


Figure 83: SGSN-Initiated BSS Packet Flow Context Modification Procedure

- 1) The SGSN sends a Modify BSS Packet Flow Context Request (IMSI, TLLI, Packet Flow Id, Aggregate BSS QoS Profile Requested, BSS Packet Flow Timer) message to the BSS.
- 2) The BSS may restrict the requested aggregate BSS QoS profile given its capabilities and the current load. The BSS inserts the modified parameters in its BSS context. The BSS returns a Modify BSS Packet Flow Context Accept (IMSI, Packet Flow Id, Aggregate BSS QoS Profile Negotiated) message to the SGSN.

12.7.3.5.3 BSS-Initiated BSS Packet Flow Context Modification Procedure

The BSS can at any time request modification of the contents of an existing BSS packet flow context, e.g., due to a change in the resource availability at the BSS.

The BSS-Initiated BSS Packet Flow Context Modification procedure is illustrated in Figure 84. Each step is explained in the following list.

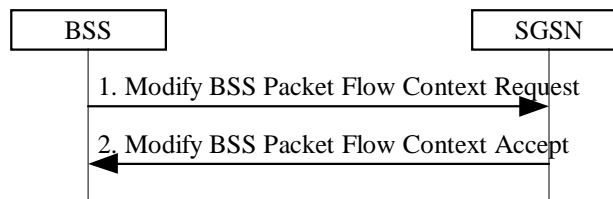


Figure 84: BSS-Initiated BSS Packet Flow Context Modification Procedure

- 1) The BSS sends a Modify BSS Packet Flow Context Request (IMSI, Packet Flow Id, Aggregate BSS QoS Profile Requested) message to the SGSN.
- 2) The SGSN may restrict the requested aggregate BSS QoS profile given its capabilities and the current load. The SGSN returns a Modify BSS Packet Flow Context Accept (IMSI, TLLI, Packet Flow Id, Aggregate BSS QoS Profile Negotiated, BSS Packet Flow Timer) message to the BSS. The BSS inserts the modified parameters in its BSS context.

12.7.3.5.4 BSS Packet Flow Context Deletion Procedures

The BSS can, due to e.g., memory restrictions, at any time delete a BSS packet flow context without notifying the SGSN.

The SGSN may request the deletion of a BSS packet flow context with the SGSN-Initiated BSS Packet Flow Context Deletion procedure, as illustrated in Figure 85. Each step is explained in the following list.

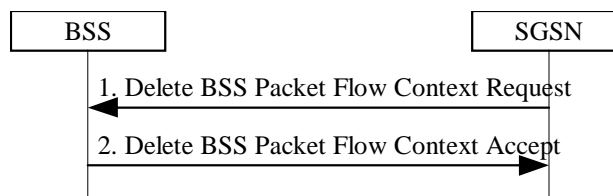


Figure 85: SGSN-Initiated BSS Packet Flow Context Deletion Procedure

- 1) The SGSN sends a Delete BSS Packet Flow Context Request (IMSI, Packet Flow Id) message to the BSS. The BSS deletes the corresponding BSS packet flow context from its BSS context.
- 2) The BSS returns a Delete BSS Packet Flow Context Accept (TLLI, Packet Flow Id) message to the SGSN.

12.8 Iu Interface for UMTS

[The level of detail of this Iu description chapter is still under discussion.]

The Iu interface connects the UTRAN and the Core Network packet domain, allowing the exchange of signalling information and user data. The user plane of Iu interface shall allow user data from many users to be multiplexed over the same physical resource. Resources are given to a user upon activity (when data is sent or received) and are reallocated immediately thereafter.

In UMTS only user data is transmitted on this shared physical medium. Signalling data is transferred via an SCCP connection. A reference configuration for Iu interface user plane is given in Figure 86.

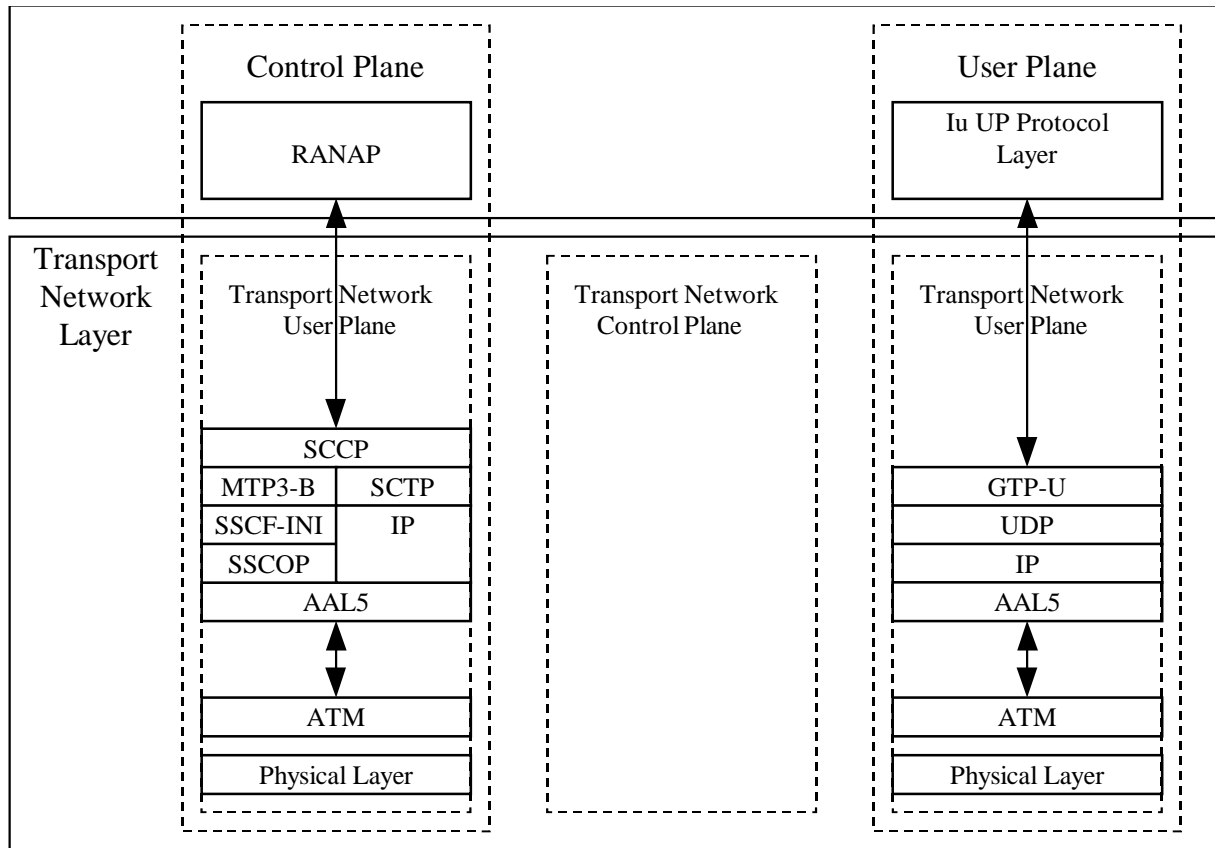


Figure 86: Iu User Plane Protocol Configuration for Packet-Switched Traffic

12.8.1 Physical Layer Protocols

The physical layer shall comply with one of a wide range of standards, according to UMTS 25.411. Services provided to the upper layer shall be independent from the used underlying technology.

12.8.2 Higher-Layer Protocols

12.8.2.1 Higher-Layer Protocols for User Data Transport

The GTP-U protocol shall be used over the Iu interface between the packet switched domain and the RNS.

The path protocol used shall be UDP, as specified in RFC 768. Both the IPv4 (RFC 791) and IPv6 (RFC 2460) IP protocols shall be supported, IPv6 support is FFS.

AAL5 shall be used according to I.363.5.

AAL5 permanent or switched virtual circuits are used to transport the IP packets across the Iu interface between RNS and the packet switched core network domain. Multiple VCs can be used over the Iu interface.

IP over ATM protocols are used to carry the IP packets over the ATM transport network. IP over ATM is specified in RFC 2225. Multiprotocol Encapsulation over AAL5 is specified in RFC 1483.

The Iu interface protocol stack is described in more detailed in UMTS 25.414.

12.8.2.1.1 Consistent Sequence Numbering of PDUs on Iu and Gn Interfaces

The GTP-U PDU sequence numbers allocated by the GGSN (downlink) and SRNS (uplink) are kept unchanged irrespective of the number of GTP tunnels the PDU is transferred over. Therefore, SGSN shall use on the Iu interface for downlink PDUs the GTP-U sequence number received from the GGSN, and shall use on the Gn interface for uplink

PDU's the GTP-U sequence number received from the SRNS. In case of SRNS relocation and intersystem handover, the SRNS and SGSN shall tunnel PDU's without changing the GTP-U sequence numbers.

12.8.2.2 Higher-Layer Protocols for Signalling Transport

The protocol stack for signalling transport is based on ATM/AAL5. Two AAL5 signalling transport services options are available to provide services for the SCCP layer.

The first option for the SCCP signalling protocol stack uses SSCOP for reliability reasons. SSCOP provides the adaptation to upper layers. MTP3-B is the network layer protocol.

The second option for the SCCP signalling protocol stack uses IP as the network layer. SCTP performs the adaptation of the IP layer and provides services to the SCCP layer.

12.8.3 Iu Release Procedure

This procedure is used to release the Iu interface. This procedure also triggers the release of all the Iu connections and changes the 3G-SGSN PMM state to PMM-IDLE. Both RNC-initiated and SGSN-initiated Iu release procedures are showed in the figure below.

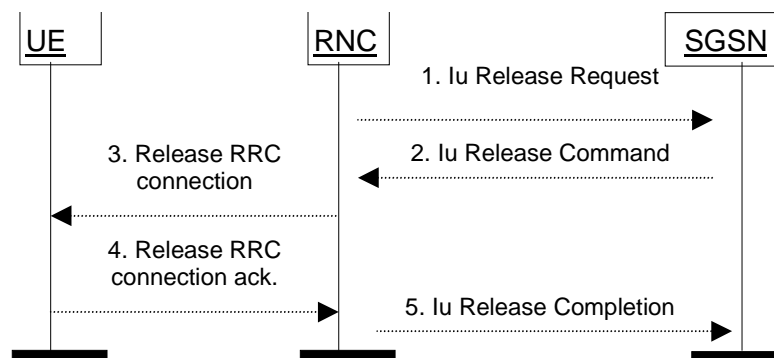


Figure 87: Iu Release Procedure

NOTE 1: Message 1 is only sent when the RNC-initiated Iu release procedure is considered.

NOTE 2: Message 1 is not sent but message 2 is sent when the SGSN-initiated Iu release procedure is considered.

- 1) The RNC notices that the RRC connection has been released or detects a need to release the radio resources. It sends an Iu Release Request (Cause) message to the SGSN. Cause indicates the reason for the release (O&M Intervention, Equipment Failure, Implicit Release, or Resource Optimisation). Implicit Release means that the periodic URA update timer expired. Resource Optimisation means that RNC decided to release an MS with only a non real-time bearer established to optimise the radio usage after the RRC-Connection-Release timer expired.
- 2) The SGSN releases the Iu by sending the Iu Release Command (Cause) message to the RNC. This message may be triggered either by an Iu Release Request message, or by another SGSN event (e.g., authentication failure or detach). It is optional for the SGSN to send the Iu Release Command message after an Iu Release Request message with Cause set to Resource Optimisation is received from the RNC.
- 3) If the RRC connection is not already released (Cause = Resource Optimisation), then the RNC sends a Release RRC Connection message to the MS. [Cause "Detach" or "Authentication failure are FFS]
- 4) The MS returns a Release RRC Connection Acknowledge message to the RNC.
- 5) The RNC confirms the Iu release by returning an Iu Release Completion message to the SGSN.

If the RNC does not receive the Release RRC Connection Acknowledge message and if Cause is different from Authentication Failure or Detach, then it should send a failure message to the SGSN, and the SGSN should stay in the MM-CONNECTED state.

12.8.4 Location Reporting Procedure

This procedure is used by a 3G-SGSN to request the SRNC to report where the MS is currently located, or to report when the MS moves into or out of a given service area. This procedure relates to location services (LCS) and other services (e.g., CAMEL and emergency calls) in UMTS. The overall LCS procedure is to be described in LCS stage 2 specification (add reference FFS).

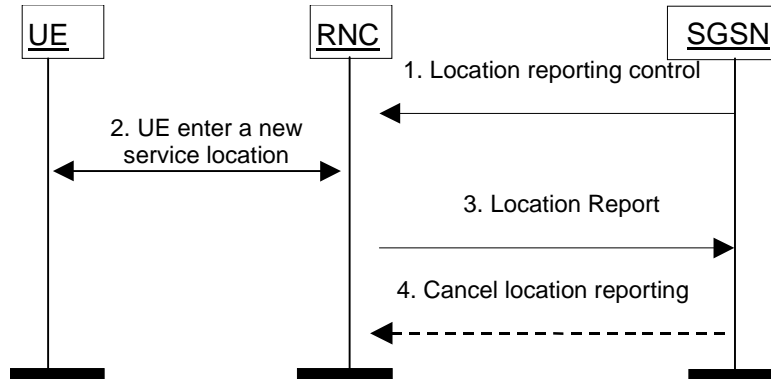


Figure 88: Location Reporting Procedure

- 1) The SGSN detects from the subscriber data the need to monitor in which service area an MS in the MM-CONNECTED state with an Iu interface connection is located. The SGSN sends a Location Reporting Control (Service Area Code(s), Reporting Type) message to the SRNC. The SRNC stores the Service Area Code(s) as reporting area(s) for this MS. For example, a service area may be a location area with restricted access. Reporting Type indicates whether the message is intended to start a reporting period or trigger a stand-alone report about the current location of the MS.
- 2) The SRNC detects that the MS moves into or out of a reporting area. Alternatively, the SRNC derives the current location of the MS if this was requested by the SGSN.
- 3) The SRNC sends a Location Report (Service Area Code) message informing the 3G-SGSN about where the MS is now located. If no Service Area Code is included, it indicates that the MS is outside the requested service area. When the SGSN has requested the current location of the MS, then SRNC shall include the requested location information in the Location Report message, e.g., in the format of a cell id. The SGSN may then perform specific actions (e.g., detach a MS entering a forbidden location area or route an emergency call to the nearest local emergency number).
- 4) The SGSN can send a Cancel Location Reporting message to inform the SRNC that it should terminate location reporting for a given MS. This message is needed only when the reporting was requested for a reporting period.

The procedure is implicitly cancelled at SRNC relocation. If the service is still required in the new SRNC or new SGSN then a new Location Reporting Control message shall be sent.

12.9 Abis Interface for GPRS

When the GPRS MAC and RLC layer functions are positioned remote to the BTS the information between the Channel Codec Unit (CCU) and the remote GPRS Packet Control Unit (PCU) is transferred in frames with a fixed length of 320 bits (20 ms). In the present document these frames are denoted "PCU Frames" and are an extension to the "TRAU frames" defined in GSM 08.60 [22]. Within these frames both GPRS data and the GPRS RLC/MAC associated control signals are transferred.

The Abis interface should be the same if the PCU is positioned at the BSC site (option B in Figure 89) or at the SGSN site (option C in Figure 89). In option B, the PCU could be implemented as an adjunct unit to the BSC. In option C, the BSC should be considered as transparent for 16 kbit/s channels. In configurations B and C the PCU is referred to as being a remote PCU.

The remote PCU is considered a part of the BSC, and the signalling between the BSC and the PCU may be performed by using BSC internal signals. The inband signalling between the CCU and the PCU functions, using PCU frames is required when the Abis interface is applied (options B and C in Figure 89).

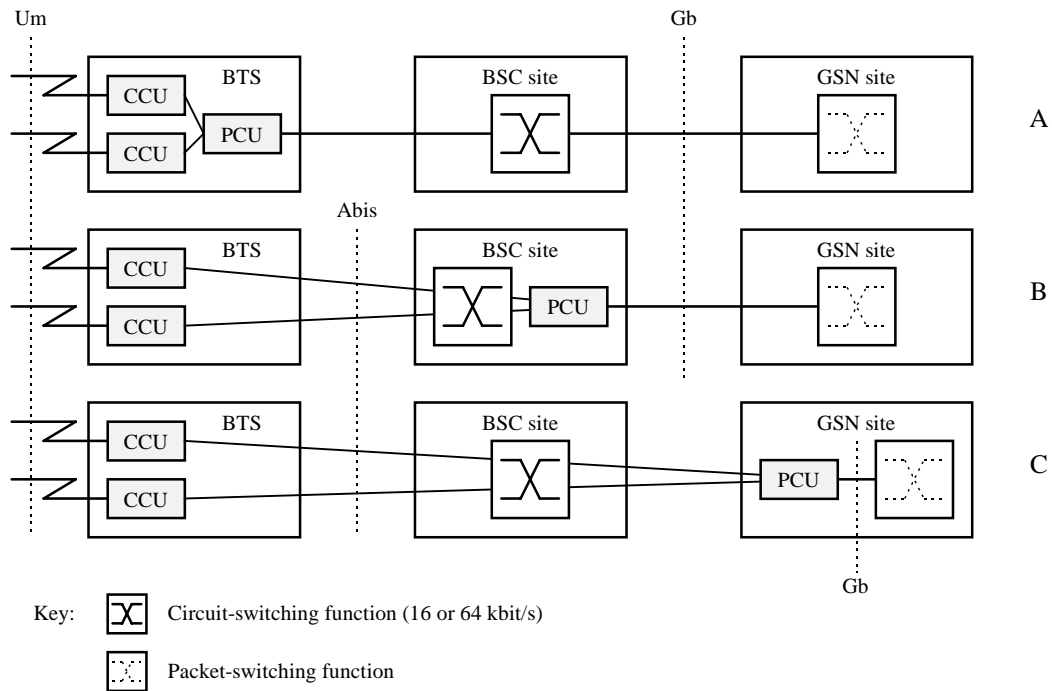


Figure 89: Remote Packet Control Unit (PCU) Positions

The PCU is responsible for the following GPRS MAC and RLC layer functions as defined in GSM 03.64:

- LLC layer PDU segmentation into RLC blocks for downlink transmission;
- LLC layer PDU reassembly from RLC blocks for uplink transmissions;
- PDCH scheduling functions for the uplink and downlink data transfers;
- PDCH uplink ARQ functions, including RLC block ack / nak;
- PDCH downlink ARQ function, including buffering and retransmission of RLC blocks;
- channel access control functions, e.g., access requests and grants; and
- radio channel management functions, e.g., power control, congestion control, broadcast control information, etc.

The functions inside the Channel Codec Unit (CCU) are:

- the channel coding functions, including FEC and interleaving;
- radio channel measurement functions, including received quality level, received signal level and information related to timing advance measurements; and
- for EGPRS, in case of incremental redundancy mode of operation, enhanced channel coding functions.

The BSS is responsible for allocation and de-allocation of radio resources. A PCU frame shall be transferred between the PCU and the CCU every 20 ms.

12.9.1 Remote Packet Control Unit

When the Packet Control Unit (PCU) is remote to the BTS, the Channel Codec Unit (CCU) in the BTS may control some of the functions in the remote PCU in the BSC. As well, the PCU may control some of the functions of the CCU. This remote control is performed by inband signalling carried by the control bits (C-bits) in each PCU frame.

13 Information Storage

This clause describes information storage structures required for the packet domain, and the recovery and restoration procedures needed to maintain service if inconsistencies in databases occur and at lost or invalid database information.

13.1 HLR

IMSI is the prime key to the packet domain subscription data stored in the HLR. There may be several sets of packet domain subscription data per IMSI. This is illustrated in Figure 90.

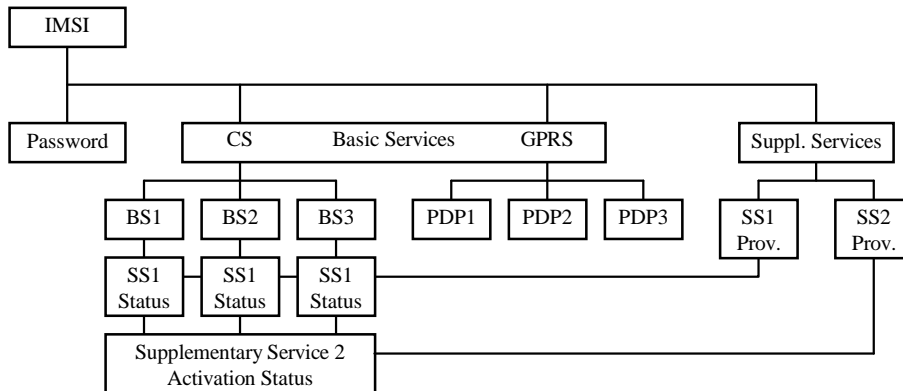


Figure 90: Packet Domain Subscription Data

As Figure 90 indicates, the packet domain subscription data is at the same level as basic services. Each PDP subscription is seen as a basic service. Supplementary services are provisioned as part of the overall subscription. Activation of SSs is either at the basic service level (SS1) or at the overall subscription level (SS2).

Table 5 shows the packet domain subscription data contained in the HLR.

Table 5: HLR Packet Domain Subscription Data

Field	Description	GPRS	UMTS
IMSI	IMSI is the main reference key.	X	X
MSISDN	The basic MSISDN of the MS.	X	X
SGSN Number	The SS7 number of the SGSN currently serving this MS.	X	X
SGSN Address	The IP address of the SGSN currently serving this MS.	X	X
SMS Parameters	SMS-related parameters, e.g., operator-determined barring.	X	X
MS PS Purged for	Indicates that the MM and PDP contexts of the MS are deleted from the SGSN.	X	X
MNRG	Indicates that the MS is not reachable through an SGSN, and that the MS is marked as not reachable at the SGSN and possibly at the GGSN.	X	X
GGSN-list	The GSN number and optional IP address pair related to the GGSN that shall be contacted when activity from the MS is detected and MNRG is set. The GSN number shall be either the number of the GGSN or the protocol-converting GSN as described in the subclauses "MAP-based GGSN - HLR Signalling" and "GTP and MAP-based GGSN - HLR Signalling".	X	X
Each IMSI contains zero or more of the following PDP context subscription records:			
PDP Context Identifier	Index of the PDP context.	X	X
PDP Type	PDP type, e.g., X.25, PPP, or IP.	X	X
PDP Address	PDP address, e.g., an X.121 address. This field shall be empty if dynamic addressing is allowed.	X	X
Access Point Name	A label according to DNS naming conventions describing the access point to the external packet data network.	X	X
QoS Profile Subscribed	The quality of service profile subscribed. QoS Profile Subscribed is the default level if a particular QoS profile is not requested.	X	X
VPLMN Address Allowed	Specifies whether the MS is allowed to use the APN in the domain of the HPLMN only, or additionally the APN in the domain of the VPLMN.	X	X

13.2 SGSN

SGSN maintains MM context and PDP context information for MSs in the STANDBY, READY, PMM-IDLE, and PMM-CONNECTED states. Table 6 shows the context fields for one MS.

Table 6: SGSN MM and PDP Contexts

Field	Description	GPRS	UMTS
IMSI	IMSI is the main reference key.	X	X
MM State	Mobility management state, IDLE, STANDBY, READY, PMM-DETACHED, PMM-IDLE, or PMM-CONNECTED.	X	X
P-TMSI	Packet Temporary Mobile Subscriber Identity.	X	X
P-TMSI Signature	A signature used for identification checking purposes.	X	X
IMEI	International Mobile Equipment Identity	X	X
MSISDN	The basic MSISDN of the MS.	X	X
Routeing Area	Current routeing area.	X	X
Cell Identity	Current cell in READY state, last known cell in STANDBY or IDLE state.	X	[FFS]
Cell Identity Age	Time elapsed since the last LLC PDU was received from the MS at the SGSN.	X	[FFS]
VLR Number	The VLR number of the MSC/VLR currently serving this MS.	X	X
New SGSN Address	The IP address of the new SGSN where buffered and not sent N-PDUs should be forwarded to.	X	X
Authentication Triplets	Authentication and ciphering parameters.	X	X
Authentication Vectors	Authentication and ciphering parameters for UMTS.		X
Kc	Currently used ciphering key.	X	
CKSN	Ciphering key sequence number of Kc.	X	
Ciphering algorithm	Selected ciphering algorithm.	X	
CK	Currently used ciphering key.		X
IK	Currently used integrity key.		X
KSI	Key Set Identifier.		X
Radio Access Classmark	MS radio access capabilities.	X	
SGSN Classmark	MS network capabilities.	X	X
DRX Parameters	Discontinuous reception parameters.	X	
MNRG	Indicates whether activity from the MS shall be reported to the HLR.	X	X
NGAF	Indicates whether activity from the MS shall be reported to the MSC/VLR.	X	X
PPF	Indicates whether paging for PS and CS services can be initiated.	X	X
SMS Parameters	SMS-related parameters, e.g., operator-determined barring.	X	X
Recovery	Indicates if HLR or VLR is performing database recovery.	X	X
Radio Priority SMS	The RLC/MAC radio priority level for uplink SMS transmission.	X	
Each MM context contains zero or more of the following PDP contexts:			
PDP Context Identifier	Index of the PDP context.	X	X
PDP State	Packet data protocol state, INACTIVE or ACTIVE.	X	X
PDP Type	PDP type, e.g., X.25, PPP, or IP.	X	X
PDP Address	PDP address, e.g., an X.121 address.	X	X
APN Subscribed	The APN received from the HLR.	X	X
APN in Use	The APN currently used.	X	X
NSAPI	Network layer Service Access Point Identifier.	X	X
TI	Transaction Identifier.	X	X
TEID	Tunnel Endpoint Identifier.	X	X
GGSN Address in Use	The IP address of the GGSN currently used.	X	X
VPLMN Address Allowed	Specifies whether the MS is allowed to use the APN in the domain of the HPLMN only, or additionally the APN in the domain of the VPLMN.	X	X
QoS Profile Subscribed	The quality of service profile subscribed.	X	X
QoS Profile Requested	The quality of service profile requested.	X	X
QoS Profile Negotiated	The quality of service profile negotiated.	X	X
TFT [FFS]	Traffic flow template.	X	X
Radio Priority	The RLC/MAC radio priority level for uplink user data transmission.	X	
Packet Flow Id	Packet flow identifier.	X	
Send N-PDU Number	SNDSCP sequence number of the next downlink N-PDU to be sent	X	

	to the MS.		
Receive N-PDU Number	SNDCP sequence number of the next uplink N-PDU expected from the MS.	X	
SND	GTP-U sequence number of the next downlink N-PDU to be sent to the MS.	X	X
SNU	GTP-U sequence number of the next uplink N-PDU to be sent to the GGSN.	X	X
Charging Id	Charging identifier, identifies charging records generated by SGSN and GGSN.	X	X
Reordering Required [FFS]	Specifies whether the SGSN shall reorder N-PDUs before delivering the N-PDUs to the MS.	X	X
RNC Address in Use	The IP address of the RNC currently used.		X

In case of anonymous access (GPRS only) the SGSN maintains the MM context and PDP context information for MSs in READY state. Table 7 shows the context fields for one MS.

Table 7: SGSN MM and PDP Contexts for Anonymous Access

Field	Description
A-TLLI	Auxiliary Temporary Logical Link Identity.
AA-TID	Anonymous Access Tunnel Identifier.
Routeing Area	Current routeing area.
Cell Identity	Current cell.
PDP Type	PDP type, e.g., X.25, PPP, or IP.
PDP Address	PDP address, e.g., an X.121 address.
APN in Use	The APN currently used.
NSAPI	Network layer Service Access Point Identifier.
TI	Transaction Identifier.
GGSN Address in Use	The IP address of the GGSN currently used.
QoS Profile Requested	The quality of service profile requested.
QoS Profile Negotiated	The quality of service profile negotiated.
Radio Priority	The RLC/MAC radio priority level for uplink user data transmission.
Packet Flow Id	Packet flow identifier.
Send N-PDU Number	SNDCP sequence number of the next downlink N-PDU to be sent to the MS.
Receive N-PDU Number	SNDCP sequence number of the next uplink N-PDU expected from the MS.
SND	GTP sequence number of the next downlink N-PDU to be sent to the MS.
SNU	GTP sequence number of the next uplink N-PDU to be sent to the GGSN.
Charging Id	Charging identifier, identifies charging records generated by SGSN and GGSN.
Reordering Required	Specifies whether the SGSN shall reorder N-PDUs before delivering the N-PDUs to the MS.

13.3 GGSN

GGSN maintains activated PDP contexts. Table 8 shows the PDP context fields for one PDP Address.

Table 8: GGSN PDP Context

Field	Description	GPRS	UMTS
IMSI	International Mobile Subscriber Identity.	X	X
NSAPI	Network layer Service Access Point Identifier.	X	X
MSISDN	The basic MSISDN of the MS.	X	X
PDP Type	PDP type, e.g., X.25, PPP, or IP.	X	X
PDP Address	PDP address, e.g., an X.121 address.	X	X
Dynamic Address	Indicates whether PDP Address is static or dynamic.	X	X
APN in Use	The APN Network Identifier currently used.	X	X
TFT	Traffic flow template.	X	X
QoS Profile Negotiated	The quality of service profile negotiated.	X	X
SGSN Address	The IP address of the SGSN currently serving this MS.	X	X
MNRG	Indicates whether the MS is marked as not reachable for PS at the HLR.	X	X
Recovery	Indicates if the SGSN is performing database recovery.	X	X
SND	GTP-U sequence number of the next downlink N-PDU to be sent to the MS.	X	X
SNU	GTP-U sequence number of the next uplink N-PDU to be received from the SGSN.	X	X
Charging Id	Charging identifier, identifies charging records generated by SGSN and GGSN.	X	X
Reordering Required [FFS]	Specifies whether the GGSN shall reorder N-PDUs received from the SGSN.	X	X

If a PDP context is enabled for network-requested PDP context activation, then IMSI, PDP Type, PDP Address, SGSN Address and MNRG contain valid information also when the PDP context is inactive and when the MS is GPRS-detached.

In case of anonymous access (GPRS only) the GGSN maintains activated PDP contexts. Table 9 shows the PDP context fields for one MS.

Table 9: GGSN PDP Context for Anonymous Access

Field	Description
AA-TID	Anonymous Access Tunnel Identifier.
PDP Type	PDP type, e.g., X.25, PPP, or IP.
PDP Address	PDP address, e.g., an X.121 address.
APN in Use	The APN Network Identifier currently used.
QoS Profile Negotiated	The quality of service profile negotiated.
SGSN Address	The IP address of the SGSN serving this MS.
SND	GTP-U sequence number of the next downlink N-PDU to be sent to the MS.
SNU	GTP-U sequence number of the next uplink N-PDU to be sent to the GGSN.
Charging Id	Charging identifier, identifies charging records generated by SGSN and GGSN.
Reordering Required	Specifies whether the GGSN shall reorder N-PDUs received from the SGSN.

A GGSN that supports anonymous access shall have a list of server addresses that are allowed to be accessed by anonymous MSs. The method to maintain the list of the servers is outside the scope of the present document.

13.4 MS

Each packet domain MS maintains MM and PDP context information in IDLE, STANDBY, READY, PMM-DETACHED, PMM-IDLE, and PMM-CONNECTED states. The information may be contained in the MS and the TE. Table 10 shows the MS context fields.

Table 10: MS MM and PDP Contexts

Field	SIM	Description	GPRS	UMTS
IMSI	V	International Mobile Subscriber Identity.	X	X
MM State		Mobility management state, IDLE, STANDBY, READY, PMM-DETACHED, PMM-IDLE, or PMM-CONNECTED.	X	X
P-TMSI	V	Packet Temporary Mobile Subscriber Identity.	X	X
P-TMSI Signature	V	A signature used for identification checking purposes.	X	X
Routeing Area	V	Current routeing area.	X	X
Cell Identity		Current cell.	X	
Kc	V	Currently used ciphering key.	X	
CKSN	V	Ciphering key sequence number of Kc.	X	
Ciphering algorithm		Selected ciphering algorithm.	X	X
CK	V	Currently used ciphering key.		X
CK Next	V	Ciphering key for the next authentication.		X
IK	V	Currently used integrity key.		X
IK Next	V	Integrity key for the next authentication.		X
KSI	V	Key Set Identifier.		X
Classmark		MS classmark.	X	X
DRX Parameters		Discontinuous reception parameters.	X	X
Radio Priority SMS		The RLC/MAC radio priority level for uplink SMS transmission.	X	
Each MM context contains zero or more of the following PDP contexts:				
PDP Type		PDP type, e.g., X.25, PPP, or IP.	X	X
PDP Address		PDP address, e.g., an X.121 address.	X	X
PDP State		Packet data protocol state, INACTIVE or ACTIVE.	X	X
Dynamic Address Allowed		Specifies whether the MS is allowed to use a dynamic address.	X	X
APN Requested		The APN requested.	X	X
NSAPI		Network layer Service Access Point Identifier.	X	X
TI		Transaction Identifier.	X	X
QoS Profile Requested		The quality of service profile requested.	X	X
QoS Profile Negotiated		The quality of service profile negotiated.	X	X
TFT		Traffic flow template.	X	X
Radio Priority		The RLC/MAC radio priority level for uplink user data transmission.	X	
Packet Flow Id		Packet flow identifier.	X	
Send N-PDU Number		SNDCP sequence number of the next uplink N-PDU to be sent to the SGSN.	X	X
Receive N-PDU Number		SNDCP sequence number of the next downlink N-PDU expected from the SGSN.	X	X

The information marked with an "V" in Table 10:

- shall be stored in the SIM if the connected SIM is GPRS-aware; and
- may be stored in the ME after PS detach if the connected SIM is not GPRS-aware.

If the SIM is packet domain service-aware, then the IMSI, P-TMSI, P-TMSI Signature, Routeing Area, Kc, CK, IK, and CKSN stored in the SIM shall be used when accessing the packet domain services.

[USIM is probably PS aware, and these paragraphs may need to be changed accordingly.]

If the SIM is not packet domain service-aware, then the P-TMSI, P-TMSI Signature, Routeing Area, Kc, CK, IK, CKSN, and KSI stored in the ME shall be used if and only if the IMSI stored in the SIM is identical to the IMSI image maintained in the ME. If the IMSI stored in the SIM is different from the IMSI image in the ME, then the IMSI image in the ME shall not be used, and the MS shall identify itself with the IMSI stored in the SIM when performing a PS attach. IMSI, P-TMSI, P-TMSI Signature, Routeing Area, Kc, CK, IK, CKSN, and KSI may be stored in the ME after the PS attach has been successfully performed.

For anonymous access (GPRS only) each GPRS MS maintains MM and PDP context information in READY state. The information may be contained in the ME and the TE. Table 11 shows the MS context fields.

Table 11: MS MM and PDP Contexts for Anonymous Access

Field	Description
A-TLLI	Auxiliary Temporary Logical Link Identity.
Routeing Area	Current routeing area.
Cell Identity	Current cell.
PDP Type	PDP type, e.g., X.25, PPP, or IP.
PDP Address	PDP address, e.g., an X.121 address.
NSAPI	Network layer Service Access Point Identifier.
TI	Transaction Identifier.
APN Requested	The APN requested.
QoS Profile Requested	The quality of service profile requested.
QoS Profile Negotiated	The quality of service profile negotiated.
Radio Priority	The RLC/MAC radio priority level for uplink user data transmission.
Packet Flow Id	Packet flow identifier.
Send N-PDU Number	SNDCP sequence number of the next uplink N-PDU to be sent to the SGSN.
Receive N-PDU Number	SNDCP sequence number of the next downlink N-PDU expected from the SGSN.

13.5 MSC/VLR

The MSC/VLR may store the SGSN number of PS-attached MSs that are also CS-attached. Table 12 shows the MSC/VLR association for one MS.

Table 12: MSC/VLR Association

Field	Description	GPRS	UMTS
IMSI	IMSI is the main reference key.	X	X
SGSN Number	The SGSN number of the SGSN currently serving this MS.	X	X

13.6 BSS for GPRS

Table 13 shows the BSS context fields for one MS.

Table 13: BSS Context

Field	Description
IMSI	IMSI is the main reference key.
TLLI	Temporary Logical Link Identity.
Each BSS context contains one or more BSS Packet Flow contexts:	
Packet Flow Id	Packet flow identifier.
Aggregate BSS QoS Profile Negotiated	The aggregate BSS quality of service profile negotiated for this packet flow.
BSS Packet Flow Timer	BSS packet flow context inactivity timer.

The BSS may store BSS contexts also in the anonymous access case. Table 14 shows the BSS context fields for one MS.

Table 14: BSS Context for Anonymous Access

Field	Description
A-TLLI	Auxiliary Temporary Logical Link Identity.
Packet Flow Id	Packet flow identifier.
Aggregate BSS QoS Profile Negotiated	The aggregate BSS quality of service profile negotiated for this packet flow.
BSS Packet Flow Timer	BSS packet flow context inactivity timer.

13.7 RNC for UMTS

RNC maintains RNC Context for CN-related information in PMM-CONNECTED state. RNC also contains RNC RAB contexts for activated RABs. Table 15: RNC Context shows the context fields for one MS.

Table 15: RNC Context

Field	Description
IMSI	IMSI is the main reference key.
Each RNC context contains one [FFS: zero or more?] or more RNC RAB contexts:	
NSAPI	Network layer Service Access Point Identifier.
TEID	Tunnel Endpoint Identifier
GGSN Address in Use	The IP address of the SGSN currently used.
QoS Profile Negotiated	The quality of service profile negotiated for this RAB.

13.8 Recovery and Restoration Procedures

The recovery and restoration procedures are intended to maintain service if inconsistencies in databases occur and at lost or invalid database information. "Invalid" in this context means that the database entry cannot be regarded as reliable.

13.8.1 HLR Failure

When an HLR restarts, it sends to each SGSN where one or more of its MSs are registered a Reset message. This causes the SGSN to mark the relevant MM contexts as invalid, and to set NGAF if an SGSN – MSC/VLR association exists. After receipt of the first valid LLC frame (for GPRS) or after receipt of the first valid GTP-U packet or uplink signalling message (for UMTS) from a marked MS, the SGSN performs an update location to the HLR as in the attach or inter SGSN RA update procedures, and, if NGAF is set, the procedure in subclause "Non-GPRS Alert" is followed. The update location procedure and the procedure towards the MSC/VLR may be delayed by the SGSN for a maximum operator configuration-depending time period to avoid high signalling load. The periodic back-up of HLR data to non-volatile storage is mandatory as described in UMTS 33.007 [5].

13.8.2 SGSN Failure

When an SGSN fails, it deletes all MM and PDP contexts affected by the failure. SGSN storage of subscriber data is volatile. Based on configuration data, the SGSN shall send a Reset message to each of its associated VLRs. The VLRs shall mark all associations containing the restarted SGSN as unreliable. See UMTS 23.007.

If data or signalling, except GPRS attach and RA update, is received in an SGSN from an MS for which no MM context exists in the SGSN, then the SGSN shall discard the data or signalling.

If an RA update request is received in an SGSN from an MS for which no MM context exists neither in the SGSN, nor in the old SGSN for the inter-SGSN RA update case, then the SGSN shall reject the RA update with an appropriate cause. In order to remain PS-attached, the MS shall then perform a new PS attach and should (re-)activate PDP contexts.

If a service request is received in a 3G-SGSN from an MS for which no MM context exists in the 3G-SGSN, then the 3G-SGSN shall reject the service request with an appropriate cause. In order to remain PS-attached, the MS shall then perform a new PS attach and should (re-)activate PDP contexts.

NOTE: In some cases, user interaction may be required, and then the MS cannot (re-)activate the PDP contexts automatically.

When the SGSN receives a GTP PDU for which no PDP context exists it discards the GTP PDU and sends an error indication to the originating GGSN. The GGSN marks the related PDP context as invalid. If there is no MM context for the MS, the SGSN may search the MS by paging with the IMSI in the SGSN area. An MS that is paged for PS services with IMSI as the identifier shall perform a new PS attach and should (re-)activate PDP contexts.

When the SGSN receives a mobile-terminated SM from the SMS-GMSC for an IMSI unknown in the SGSN, it rejects the request.

When the SGSN receives a paging request over the Gs interface for an IMSI unknown in the SGSN and the SGSN has not completed recovery, then the SGSN may page the MS for packet services with IMSI as identifier in the area specified by the location information provided by the MSC/VLR. If no such location information is provided, then the SGSN may page the MS in the routing areas corresponding to that MSC/VLR. After the MS performs a combined PS attach, the SGSN may continue serving the Gs interface paging request.

13.8.3 GGSN Failure

When a GGSN fails, all its PDP contexts affected by the failure become invalid and may be deleted. GGSN storage of subscriber data is volatile.

When the GGSN receives a GTP PDU for which no PDP context exists, it shall discard the GTP PDU and return an error indication to the originating SGSN. The SGSN shall mark the related PDP context as invalid and send a Deactivate PDP Context Request message to the MS. The MS may then reactivate the PDP context.

13.8.4 VLR Failure

When a VLR fails, all its associations with SGSNs affected by the failure become invalid and may be deleted. Based on configuration data, the MSC/VLR sends a BSSAP+ Reset message to each of its associated SGSNs. The SGSNs mark all associations containing the restarted VLR as invalid. After receipt of the first valid LLC frame (for GPRS) or after receipt of the first valid GTP-U packet or uplink signalling message (for UMTS) from an MS that is both PS-attached and CS-attached, the SGSN shall return a Detach Request (Detach Type) message in order to request the MS to perform a combined RA / LA update. Detach Type shall be set to CS Detach. The detach procedure may be delayed by the SGSN for a maximum operator-configuration depending time period to avoid high signalling load.

13.8.5 BSS Failure for GPRS

When a BSS fails, all its BSS contexts affected by the failure become invalid and shall be deleted. BSS storage of data is volatile.

13.8.6 RNC Failure for UMTS

When an RNC fails, all its RNC contexts affected by the failure become invalid and shall be deleted. RNC storage of data is volatile.

14 Identities

14.1 IMSI

A unique International Mobile Subscriber Identity (IMSI) shall be allocated to each packet-domain subscriber. This is also the case for PS-only subscribers, except for anonymous-only access subscribers. IMSI is defined in UMTS 23.003 [4].

14.2 Packet TMSI

A Packet Temporary Mobile Subscriber Identity shall be allocated to each PS-attached MS. P-TMSI is defined in UMTS 23.003.

14.3 NSAPI and TLLI for GPRS

The Network layer Service Access Point Identifier (NSAPI) and Temporary Logical Link Identity (TLLI) are used for network layer routing. An NSAPI / TLLI pair is unambiguous within a routing area.

In the MS, NSAPI identifies the PDP-SAP. In the SGSN and GGSN, NSAPI identifies the PDP context associated with a PDP address. Between the MS and SGSN, TLLI unambiguously identifies the logical link.

When the MS requests the activation of a PDP context, the MS selects one of its unused NSAPIs.

NSAPI is a part of the tunnel identifier (TID).

For example (shown figuratively below), an X.25 packet is received by the MS from a connected TE at the X.121 address SAP. The X.25 PDU is encapsulated and NSAPI is initialised to NSAPI-1. TLLI is set to the MS's TLLI before the encapsulated X.25 packet is passed to the SNDC function.

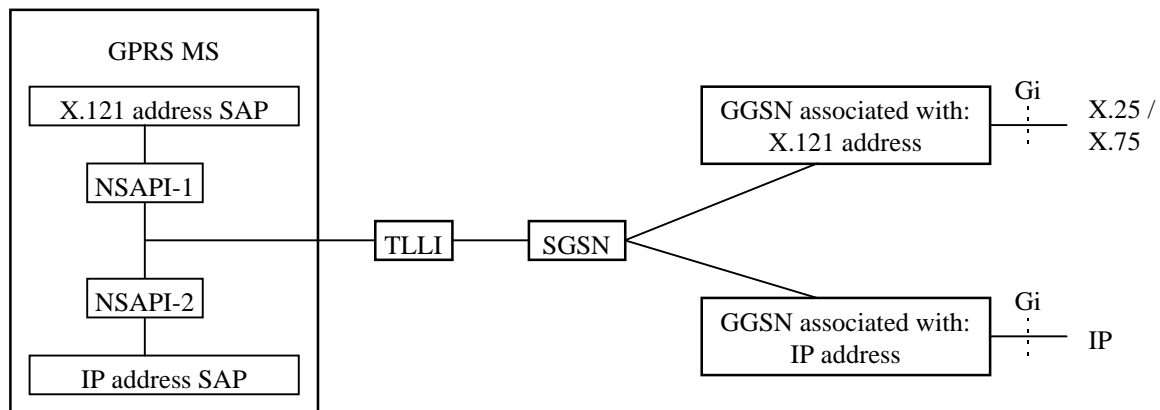


Figure 91: Use of NSAPI and TLLI

Within a routing area, there is a one-to-one correspondence between TLLI and IMSI that is only known in the MS and SGSN. If it is not clear from the context which routing area a TLLI belongs to, then TLLI is used together with RAI. TLLI is derived from a P-TMSI, and does then provide user identity confidentiality as described in subclause "User Identity Confidentiality".

The TLLI address range is divided into four ranges: Local, Foreign, Random, and Auxiliary. The TLLI structure allows the MS and SGSN to deduce the range that a TLLI belongs to. A Local TLLI is derived from the P-TMSI allocated by the SGSN, and is valid only in the RA associated with the P-TMSI. A Foreign TLLI is derived from a P-TMSI allocated in another RA. A Random TLLI is selected randomly by the MS, and is used when the MS does not have a valid P-TMSI available, or when the MS originates an anonymous access. An Auxiliary TLLI is selected by the SGSN and is used by the SGSN and MS to unambiguously identify an Anonymous Access MM and PDP Context.

If the MS has a valid P-TMSI associated with the RA where the MS is currently located, then the MS shall use a Local TLLI derived from its P-TMSI, unless the MS performs a GPRS attach.

If the MS does not have a valid P-TMSI associated with the current RA, or if the MS performs a GPRS attach, then it shall derive a Foreign TLLI from its P-TMSI, or allocate a Random TLLI if no valid P-TMSI is available.

When a TLLI is exchanged between the MS and an SGSN, then the TLLI is transmitted at the RLC/MAC layer within the Um protocol stack, and at the BSSGP layer within the Gb protocol stack. NSAPI is transmitted within the SNDCP layer in the user plane, and within the GMM/SM layer in the control plane. NSAPI is represented by a transaction identifier (TI) in some SM signalling messages. The TI is dynamically allocated by the MS for MS-requested (AA) PDP context activation, and by the network for network-requested PDP context activation. The TI is deallocated when a PDP context has been deactivated. TI usage is defined in UMTS 24.007 and UMTS 24.008.

By default, unless explicitly specified in the procedures, the TLLI transmitted at the RLC/MAC and BSSGP layers shall be used to identify the MS.

14.4 PDP Address

A packet-domain subscriber identified by an IMSI, shall have one or more network layer addresses, i.e., PDP addresses, temporarily and/or permanently associated with it that conforms to the standard addressing scheme of the respective network layer service used, e.g.:

- an IP version 4 address;
- an IP version 6 address; or
- an X.121 address.

PDP addresses are activated and deactivated through MM procedures described in subclause "PDP Context Activation, Modification, and Deactivation Functions".

14.5 TID

A Tunnel Identifier (TID) is used by the GPRS Tunnelling protocol between GSNs to identify a PDP context. A TID consists of an IMSI and an NSAPI. The combination of IMSI and NSAPI uniquely identifies a single PDP context.

The TID is forwarded to the GGSN upon PDP Context Activation and it is used in subsequent tunnelling of user data between the GGSN and the SGSN to identify the MS's PDP contexts in the SGSN and GGSN. The TID is also used to forward N-PDUs from the old SGSN to the new SGSN at and after an inter SGSN routing area update.

In the anonymous access case, AA-TID is allocated locally by the SGSN. An AA-TID consists of an A-TLLI and an NSAPI similar to TID. Since the IMSI is longer than A-TLLI, the unused digits shall be used to create a unique identity within one PLMN. The allocated AA-TID shall not collide with the TID address space.

[TID may be changed with GTP header modification, TID may become TEID]

14.6 Routing Area Identity

Routing Area Identity (RAI), defined by an operator, identifies one or several cells. In GPRS, RAI is broadcast as system information. In UMTS, RAI is broadcast to MSs in RRC Idle mode, and is notified to MSs in RRC Connected mode on established RRC connections as MM system information.

The location of an MS in STANDBY or PMM-IDLE state is known in the SGSN on an RA level. Cells that do not support packet-domain services within an LA are grouped into a null RA. The MS is paged for packet services in the RA where the MS is located when mobile-terminated traffic arrives in the SGSN. The MS is paged for circuit-switched services by the SGSN in the last known RA plus in the null RA.

NOTE: Cells not supporting GPRS and served by a BSC without a Gb interface should not be included in the same location area as cells not supporting GPRS and served by a BSC with a Gb interface.

A Routing Area is a subset of one, and only one, Location Area (LA), meaning that an RA cannot span more than one LA. An RA is served by only one SGSN.

The following rules apply for the Routing Area Identity:

- RAC is only unique when presented together with LAI.
- CI is only unique when presented together with LAI or RAI.
- LAI = MCC + MNC + LAC
- RAI = MCC + MNC + LAC + RAC
- CGI = LAI + CI

14.7 UTRAN Registration Area Identity for UMTS

Gives the identity of the UTRAN Registration Area.

[This definition does not seem useful, more text is needed.]

14.8 Cell Identity

Cell Identity (CI) identifies one cell. CI is defined in UMTS 23.003.

In UMTS, the cell identifier (C-Id) is used to uniquely identify a cell within an RNS. The C-Id together with the identifier of the controlling RNC (CRNC-Id) constitutes the UTRAN Cell Identity (UC-Id), and is used to uniquely identify the cell within UTRAN. UC-Id and C-Id is used to identify a cell on the UTRAN Iub, Iur, and Iu interfaces.

- UC-Id = RNC-Id + C-Id

14.9 GSN Addresses

14.9.1 GSN Address

Each SGSN and GGSN shall have an IP address, either of type IPv4 or IPv6, for inter-communication over the backbone network. The IP addresses of GSNs and other backbone nodes of all PLMNs build a private address space that is not accessible from the public Internet. For the GGSN and the SGSN, this IP address may also correspond to one or more DNS-type logical GSN names.

14.9.2 GSN Number

Each SGSN shall have an SGSN number for communication with e.g., HLR and EIR.

Each GGSN that supports the optional SS7-based Gc interface shall have a GGSN number for communication with HLRs.

14.10 RNC Addresses

[The Cell Identity subclause above uses CRNC-Id which needs to be defined here.]

14.10.1 RNC Address

Each RNC shall have one or more IP addresses, either of type IPv4 or IPv6, for inter-communication over the Iu interface.

14.10.2 RNC Number

Each RNC shall have an RNC number for inter-communication over the Iu interface.

14.11 Access Point Name

In the backbone, Access Point Name is a reference to the GGSN to be used. In addition, Access Point Name may, in the GGSN, identify the external network and optionally a service to be offered. Access Point Name is composed of two parts as defined in UMTS 23.003:

- The APN Network Identifier is mandatory and is a label (for example "corporation" or "service") or a set of labels separated by dots which is a fully qualified domain name according to the DNS naming conventions (for example "company.com" or "service.company.com"). In order to guarantee the uniqueness of the APN, the packet-domain PLMN should allocate, to an ISP or corporation, an APN Network Identifier identical to their domain name in the public Internet. The APN Network Identifier shall not end with ".gprs". An APN Network

Identifier that consists of 3 or more labels and that starts with a Reserved Service Label, or an APN Network Identifier that consists of a Reserved Service Label alone, shall indicate that for this APN the GGSN supports additional services such as external PDN address allocation or Mobile IP support. Reserved Service Labels, e.g., "dhcp" or "MIPv4FA", and the corresponding services that they stand for, e.g., external PDN address allocation via DHCP, or Mobile IP Foreign Agent support, are to be agreed among operators.

- The APN Operator Identifier is optional. It is a fully qualified domain name according to the DNS naming conventions, and consists of three labels. The APN Operator Identifier shall end in ".gprs". For example, it may be "MNCyyy.MCCzzz.gprs". The exact format is defined in UMTS 29.060.

The APN stored in the HLR shall not contain the APN Operator Identifier. A wild card may be stored in the HLR instead of the APN. This wild card indicates that the user may select an APN that is not stored in the HLR. The use of the wild card is described in annex A.

15 Operational Aspects

15.1 Charging

Charging information for the packet domain is collected for each MS by SGSNs and GGSNs that are serving the MS.

The information that the operator uses to generate a bill to a subscriber is operator-specific. Billing aspects, e.g., a regular fee for a fixed period, are outside the scope of the present document.

Every packet domain operator collects and processes their own charging information.

The SGSN collects charging information for each MS related with the radio network usage while the GGSN collects charging information for each MS related with the external data network usage. Both GSNs also collect charging information on usage of the network resources.

15.1.1 Charging Information

Charging information is collected for the PS subscriber.

As a minimum, the SGSN shall collect the following charging information:

- usage of the radio interface: the charging information shall describe the amount of data transmitted in MO and MT directions categorised with QoS and user protocols;
- usage of the packet data protocol addresses: the charging information shall describe how long the MS has used the packet data protocol addresses;
- usage of the general packet domain resources: the charging information shall describe the usage of other packet domain-related resources and the MS's network activity (e.g., mobility management); and
- location of MS: HPLMN, VPLMN, plus optional higher-accuracy location information.

As a minimum, the GGSN shall collect the following charging information:

- destination and source: the charging information shall describe the destination and source addresses with a level of accuracy as defined by the packet domain operator;
- usage of the external data networks: the charging information shall describe the amount of data sent and received to and from the external data network; and
- usage of the packet data protocol addresses: the charging information shall describe how long the MS has used the PDP addresses.

15.1.2 Reverse Charging

It shall be possible to provide reverse charging as a subscription option. However, reverse charging may not be applicable to certain external data network protocols.

15.1.3 Fair Charging for UMTS

FFS.

15.2 Quality of Service Profile

[Not yet updated for UMTS.]

A QoS profile is associated with each PDP context. The QoS profile is considered to be a single parameter with multiple data transfer attributes. It defines the quality of service expected in terms the following attributes:

- precedence class;
- delay class;
- reliability class;
- peak throughput class; and
- mean throughput class.

There are many possible QoS profiles defined by the combinations of the attributes. A PLMN may support only a limited subset of the possible QoS profiles.

During the QoS profile negotiation defined in subclause "Activation Procedures", it shall be possible for the MS to request a value for each of the QoS attributes, including the HLR-stored subscribed default values. The network shall negotiate each attribute to a level that is in accordance with the available GPRS resources. The network shall always attempt to provide adequate resources to support the negotiated QoS profiles.

The RLC/MAC layer supports four radio priority levels and an additional level for signalling messages as defined in GSM 03.64 and GSM 04.60. Upon uplink access the MS can indicate one of the four priority levels, and whether the cause for the uplink access is user data or signalling message transmission. This information is used by the BSS to determine the radio access precedence (i.e., access priority) and the service precedence (i.e., transfer priority under congested situation), see GSM 04.60. The radio priority levels to be used for transmission of MO SMS shall be determined by the SGSN and delivered to the MS in the Attach Accept message. The radio priority level to be used for user data transmission shall be determined by the SGSN based on the negotiated QoS profile and shall be delivered to the MS during the PDP Context Activation and PDP Context Modification procedures.

15.2.1 Precedence Class

Under normal operating conditions, the network shall attempt to meet the service commitments of all QoS profiles. The service precedence indicates the relative importance of maintaining the service commitments under abnormal conditions, for example which packets are discarded in the event of problems such as limited resources or network congestion. The precedence classes are defined in Table 16.

Table 16: Precedence Classes

Precedence	Precedence Name	Interpretation
1	High priority	Service commitments shall be maintained ahead of precedence classes 2 and 3.
2	Normal priority	Service commitments shall be maintained ahead of precedence class 3.
3	Low priority	Service commitments shall be maintained after precedence classes 1 and 2.

15.2.2 Delay Class

GSM 02.60 defines four delay classes (1 to 4). The network operator should provision adequate transmission resources on the radio and network communication channels in order to support the expected number of subscribers within each cell at a given delay class. A PLMN may support only a subset of the delay classes. As a minimum, the PLMN shall support the best effort delay class (4).

15.2.3 Reliability Class

Data reliability is defined in terms of the residual error rates for the following cases (see GSM 02.60):

- probability of data loss;
- probability of data delivered out of sequence;
- probability of duplicate data delivery; and
- probability of corrupted data.

The reliability class specifies the requirements of the various network protocol layers. The combinations of the GTP, LLC, and RLC transmission modes support the reliability class performance requirements. The reliability classes are summarised in Table 17.

Table 17: Reliability Classes

Reliability Class	GTP Mode	LLC Frame Mode	LLC Data Protection	RLC Block Mode	Traffic Type
1	Acknowledged	Acknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that cannot cope with data loss.
2	Unacknowledged	Acknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that can cope with infrequent data loss.
3	Unacknowledged	Unacknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that can cope with data loss, GMM/SM, TOM, and SMS.
4	Unacknowledged	Unacknowledged	Protected	Unacknowledged	Real-time traffic, error-sensitive application that can cope with data loss.
5	Unacknowledged	Unacknowledged	Unprotected	Unacknowledged	Real-time traffic, error non-sensitive application that can cope with data loss.
NOTE: For real-time traffic, the QoS profile also requires appropriate settings for delay and throughput.					

Each reliability class in combination with the Reordering Required information specifies the target residual error rates for a PDP context. The residual error rate targets are given in GSM 02.60. A PLMN may support only a subset of the reliability classes. Signalling and SMS shall be transferred with reliability class 3.

15.2.4 Throughput Classes

User data throughput is specified in terms of a set of throughput classes that characterise the expected bandwidth required for a PDP context. The throughput is defined by both peak and mean classes.

15.2.4.1 Peak Throughput Class

The peak throughput is measured at the Gi and R reference points in units of octets per second. It specifies the maximum rate at which data is expected to be transferred across the network for an individual PDP context. There is no guarantee that this peak rate can be achieved or sustained for any time period, this depends upon the MS capability and available radio resources. The network may limit the subscriber to the negotiated peak data rate, even if additional transmission

capacity is available. The peak throughput is independent of the delay class, that determines the per-packet GPRS network transit delay. The peak throughput classes are defined in Table 18.

Table 18: Peak Throughput Classes

Peak Throughput Class	Peak Throughput in octets per second
1	Up to 1 000 (8 kbit/s).
2	Up to 2 000 (16 kbit/s).
3	Up to 4 000 (32 kbit/s).
4	Up to 8 000 (64 kbit/s).
5	Up to 16 000 (128 kbit/s).
6	Up to 32 000 (256 kbit/s).
7	Up to 64 000 (512 kbit/s).
8	Up to 128 000 (1 024 kbit/s).
9	Up to 256 000 (2 048 kbit/s).

15.2.4.2 Mean Throughput Class

The mean throughput is measured at the Gi and R reference points in units of octets per hour. It specifies the average rate at which data is expected to be transferred across the GPRS network during the remaining lifetime of an activated PDP context. The network may limit the subscriber to the negotiated mean data rate (e.g., for flat-rate charging), even if additional transmission capacity is available. A "best effort" mean throughput class may be negotiated, and means that throughput shall be made available to the MS on a per need and availability basis.

The mean throughput classes are defined in Table 19.

Table 19: Mean Throughput Classes

Mean Throughput Class	Mean Throughput in octets per hour
1	100 (~0.22 bit/s).
2	200 (~0.44 bit/s).
3	500 (~1.11 bit/s).
4	1 000 (~2.2 bit/s).
5	2 000 (~4.4 bit/s).
6	5 000 (~11.1 bit/s).
7	10 000 (~22 bit/s).
8	20 000 (~44 bit/s).
9	50 000 (~111 bit/s).
10	100 000 (~0.22 kbit/s).
11	200 000 (~0.44 kbit/s).
12	500 000 (~1.11 kbit/s).
13	1 000 000 (~2.2 kbit/s).
14	2 000 000 (~4.4 kbit/s).
15	5 000 000 (~11.1 kbit/s).
16	10 000 000 (~22 kbit/s).
17	20 000 000 (~44 kbit/s).
18	50 000 000 (~111 kbit/s).
19	100 000 000 (~0.22 Mbit/s).
20	200 000 000 (~0.44 Mbit/s).
31	Best effort.

16 Interactions with Other GSM Services

This clause describes the interaction between GPRS and the following other GSM services:

- point-to-point Short Message Service (SMS);
- circuit-switched services; and

- supplementary services.

16.1 Point-to-point Short Message Service

[Not yet updated for UMTS, but SMS in UMTS packet should be very similar to GPRS SMS.]

It shall be possible for a GPRS-attached MS to send and receive short messages over GPRS radio channels. An MS that is GPRS-attached and not IMSI-attached shall transfer SMs over GPRS channels. MSs that are both GPRS-attached and IMSI-attached shall transfer SMs over GPRS channels or over non-GPRS control channels (if non-GPRS control channels are used, then paging for MT SMS may go through the SGSN).

The following two subclauses define the operation of mobile-terminated and mobile-originated SMS routing and transfer over GPRS radio channels. More detailed definitions are contained in GSM 03.40 [8].

16.1.1 Mobile-terminated SMS Transfer

Figure 92 and the description below show an example of a successful delivery of a SM to an MS over a GPRS radio channel.

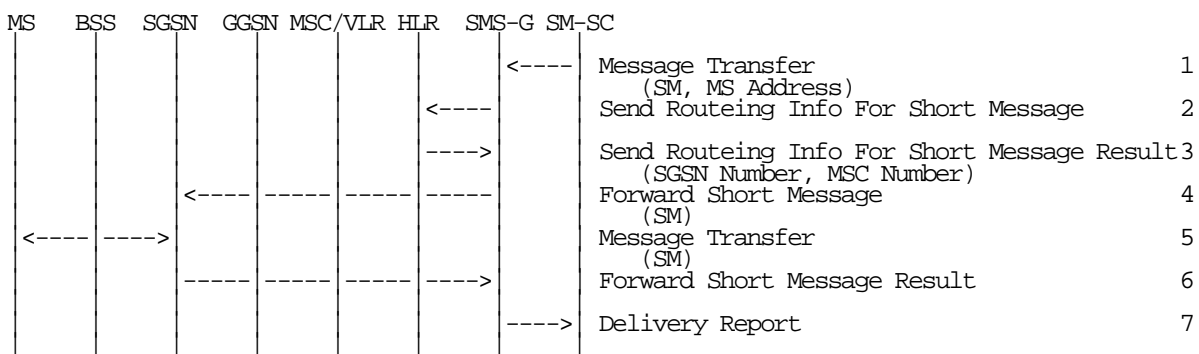


Figure 92: MT SMS Transfer, Successful

- 1) The short message service centre determines it shall send a SM to an MS. SM-SC forwards the SM to a SMS gateway MSC (SMS-GMSC).
- 2) SMS-GMSC examines the destination MS Address, and sends a Send Routeing Info For Short Message message to the relevant HLR.
- 3) HLR returns a Send Routeing Info For Short Message Result message to the SMS-GMSC. The result may contain the MS's current SGSN Number, the MSC Number, or both. If the result does not contain an SGSN Number (i.e., the HLR knows that the MS is not reachable via an SGSN), and if the result does contain an MSC Number, then non-GPRS SMS delivery procedures are followed. If the result contains an SGSN Number, the SMS transfer proceeds according to the following events.

NOTE: SMS delivery via the SGSN is normally more radio resource efficient than SMS delivery via the MSC/VLR. The preferred delivery path is selected by SMS-GMSC operator-specific action.

- 4) SMS-GMSC forwards the SM to the SGSN.
- 5) SGSN transfers the SM to the MS on the RP, CP, LLC layers, as defined in GSM 04.11 and GSM 04.64.
- 6) SGSN returns a Forward Short Message Result message to the SMS-GMSC indicating successful delivery of the SM.
- 7) SMS-GMSC returns a Delivery Report to the SM-SC indicating successful delivery of the SM.

16.1.1.1 Unsuccessful Mobile-terminated SMS Transfer

The SGSN may not be able to deliver the SM to the MS. This may for example happen when the MS is not attached to GPRS, or when the radio channel conditions are bad.

When the SGSN cannot deliver the SM to the MS, the SGSN sets the Mobile station Not Reachable for GPRS flag (MNRG), and returns a failure report to the SMS-GMSC. Based on the routing information received from the HLR, the SMS-GMSC shall do one of the following:

- If an MSC/VLR is available for the MS, the SM is forwarded to the MS via the MSC/VLR. A successful delivery report shall be returned to the SM-SC.
- If an MSC/VLR is not available for the MS, the Message Waiting Indication information in the HLR shall be updated and an unsuccessful delivery report shall be returned to the SM-SC.

Figure 93 illustrates one possible traffic scenario when neither the SGSN nor the MSC is able to deliver the SM.

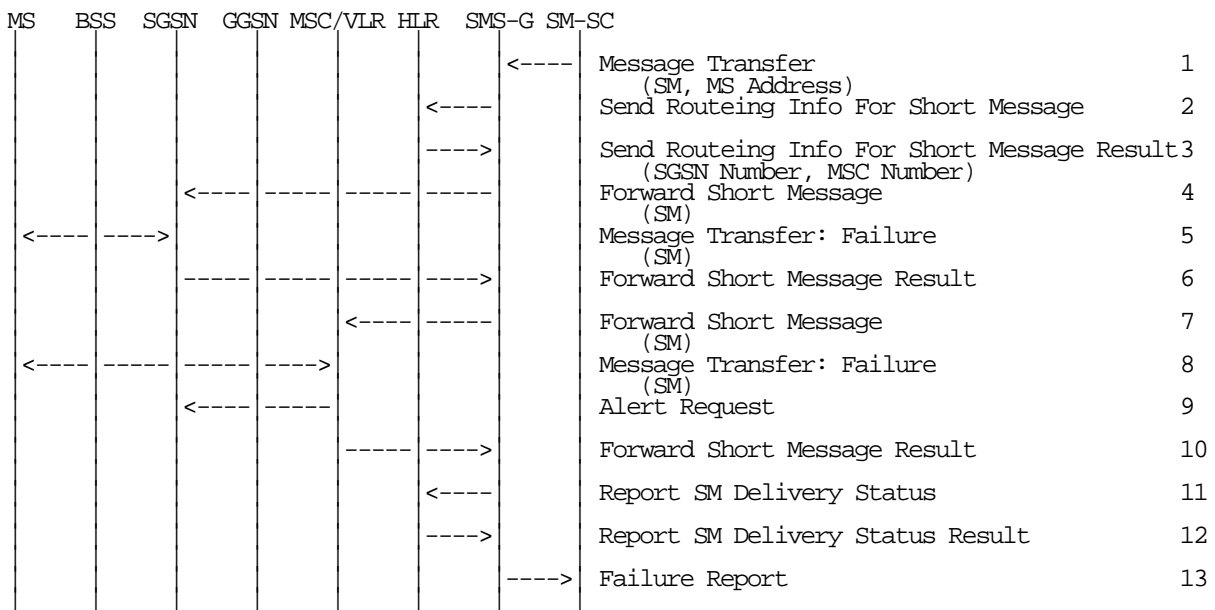


Figure 93: MT SMS Transfer, Unsuccessful

- 1) The short message service centre determines it shall send a SM to an MS. SM-SC forwards the SM to a SMS-GMSC.
- 2) SMS-GMSC examines the destination MS Address, and sends a Send Routeing Info For Short Message message to the relevant HLR.
- 3) HLR returns a Send Routeing Info For Short Message Result message to the SMS-GMSC. The Result contains an SGSN Number and an MSC Number.
- 4) SMS-GMSC forwards the SM to the SGSN.
- 5) SGSN attempts to transfer the SM to the MS, but fails.
- 6) SGSN sets MNRG and returns a Forward Short Message Result message to SMS-GMSC indicating unsuccessful delivery of the SM.
- 7) SMS-GMSC selects an alternative route for the SMS, and forwards the SM to the MSC/VLR.
- 8) MSC/VLR attempts to transfer the SM to the MS, but fails.
- 9) The MSC/VLR requests the setting of the NGAF at the SGSN.
- 10) VLR sets MNRG and returns a Forward Short Message Result message to the SMS-GMSC indicating unsuccessful delivery of the SM.
- 11) SMS-GMSC sends a Report SM Delivery message to the HLR.
- 12) HLR updates its Message Waiting Indication fields and returns a Report SM Delivery Result message to the SMS-GMSC.

13) SMS-GMSC returns a Failure Report to the SM-SC indicating unsuccessful delivery of the SM.

Figure 64 shows that the SGSN sends a Ready for SM (MS Reachable) message to the HLR when the MS becomes reachable and MNRG is set in the SGSN. The SGSN indicates also to the MSC/VLR when the MS becomes reachable and NGAF is set in the SGSN. If the MNRG is set at the MSC/VLR, the MSC/VLR sends a Ready for SM (MS Reachable) message to the HLR. Reception of a Ready for SM message or Update Location message when MNRG is set in the HLR shall trigger the SMS alert procedure as defined in GSM 03.40.

MNRG remains set in the SGSN independently of whether the MSC/VLR was successful in delivering the SM or not. This means that the SGSN in certain cases sends a Ready for SM message to the HLR when an MS becomes reachable via the SGSN, even if no SM is waiting. This causes a small amount of duplicate signalling between SGSN and HLR only.

16.1.2 Mobile-originated SMS Transfer

Figure 94 and the description below explain the steps involved in sending a SM from an MS over a GPRS radio channel.

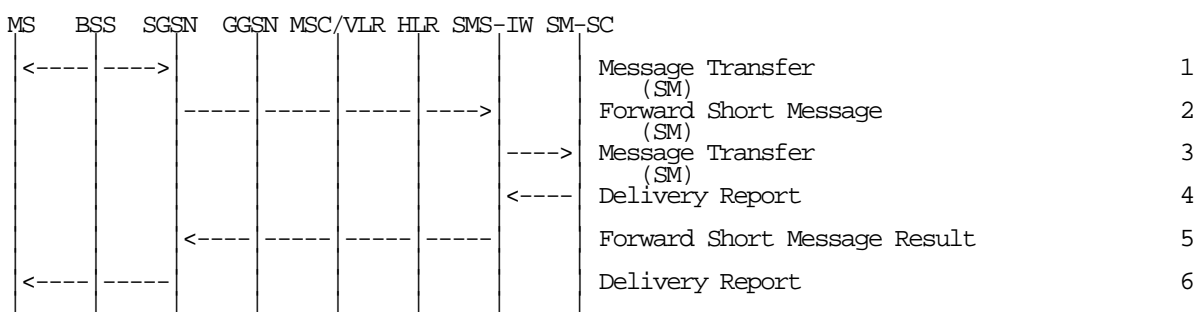


Figure 94: MO SMS Transfer, Successful

- 1) The MS has a SM to send, and transfers the SM to the SGSN via RP, CP, and LLC.
- 2) SGSN checks the MS subscription data, and determines that the MS is allowed to originate the SMS. SGSN forwards the SM to a SMS interworking MSC (SMS-IWMSC).
- 3) SMS-IWMSC passes the SM to the addressed SM-SC.
- 4) SM-SC returns a Delivery Report to the SMS-IWMSC indicating successful delivery of the SM.
- 5) SMS-IWMSC returns a Forward Short Message Result message to the SGSN indicating successful delivery of the SM.
- 6) SGSN returns a Delivery Report to the MS indicating successful delivery of the SM.

16.2 Circuit-switched Services for GPRS

The ability for a GPRS user to access circuit-switched services depends on the subscription held, the network capabilities, and the MS capabilities. Interaction between GPRS and circuit-switched services is described in subclause "Interactions Between SGSN and MSC/VLR".

16.2.1 Suspension of GPRS Services

When a GPRS-attached MS enters dedicated mode, and when the MS limitations make it unable to communicate on GPRS channels, the MS shall request the network for suspension of GPRS services. The Suspend and Resume procedure is illustrated in Figure 95. Each step is explained in the following list.

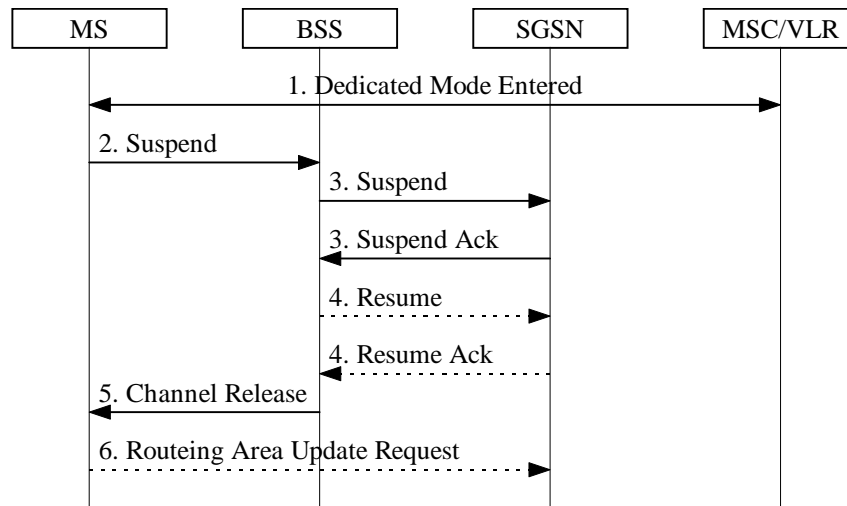


Figure 95: Suspend and Resume Procedure

- 1) The MS enters dedicated mode.
- 2) The MS sends an RR Suspend (TLLI, RAI) message to the BSS. The BSS may terminate any ongoing GPRS traffic for this TLLI.
- 3) The BSS sends a Suspend (TLLI, RAI) message to the SGSN, and the SGSN acknowledges by returning Suspend Ack. The BSS shall store TLLI and RAI in order to be able to request the SGSN to resume GPRS services when the MS leaves dedicated mode.
- 4) Eventually, the BSS determines that the circuit-switched radio channel shall be released. If the BSS is able to request the SGSN to resume GPRS services, the BSS shall send a Resume (TLLI, RAI) message to the SGSN. The SGSN acknowledges the successful outcome of the resume by returning Resume Ack.
- 5) The BSS sends an RR Channel Release (Resume) message to the MS. Resume indicates whether the BSS has successfully requested the SGSN to resume GPRS services for the MS, i.e., whether Resume Ack was received in the BSS before the RR Channel Release message was transmitted. The MS leaves dedicated mode.
- 6) If the BSS did not successfully request the SGSN to resume GPRS services, or if the RR Channel Release message was not received before the MS left dedicated mode, then the MS shall resume GPRS services by sending a Routing Area Update Request message to the SGSN, as described in subclause "Routing Area Update Procedure".

The full handling of suspended MSs in the BSS and the SGSN is implementation dependent. Typically, the SGSN should not page suspended MSs.

If the MS performs an inter-BSC handover while suspended, then TLLI and RAI should be transferred as BSC-to-BSC information in the Handover Required and Handover Request messages, see GSM 08.08. This allows the new BSC to initiate the Resume request procedure to the SGSN. In the case where the BSC-to-BSC information was not transferred or not understood, then the MS doesn't receive an indication that resumption has been successful, and the MS shall resume GPRS services by initiating a Routing Area Update Request procedure as described in step 6.

16.2.2 GPRS and Dedicated Mode Priority Handling

An MS in class-B mode of operation that communicates on GPRS radio channels when a dedicated channel is needed, shall immediately abort the GPRS communication and trigger the Suspend and Resume procedure.

[Response to circuit-switched paging,]non-emergency MO circuit-switched calls, MO SMS, and MO supplementary services are exceptions to the above rule. In these cases, it is an implementation choice whether to immediately abort GPRS communication or to delay the dedicated mode establishment.

16.3 Supplementary Services

No supplementary services are defined for the packet domain. Supplementary services may be available in the interworked-with networks (e.g., the X.25 Call Redirection user facility), but this is outside the scope of this specification.

Annex A (normative): APN and GGSN Selection

This annex contains the rules applied upon PDP context activation to determine the APN and the corresponding GGSN.

A.1 Definitions

The SGSN knows from the subscription data the parameters (S for Subscribed): PDP type (S), PDP address (S), APN (S), and VPLMN address allowed.

The SGSN may know from configuration the default APN supporting a given PDP type. This APN is called APN (SGSN) and does not include an APN Operator Identifier.

The SGSN knows the parameters requested by the MS (R for Requested): PDP type (R), PDP address (R), and APN (R). APN (R) is the APN Network Identifier requested by the MS.

In case of "an APN chosen by the SGSN" the activated PDP context is always linked with a dynamic PDP address.

An MS may have multiple subscription records for the same PDP type and the same PDP address, but with different APNs.

An MS may have one or two subscription records with the same PDP type and the same APN: one with a static PDP address, one with a dynamic PDP address.

When the MS is in its HPLMN, if the MS requests an APN that does not correspond to any GGSN of its HPLMN, the request shall be rejected by SGSN. When the MS is in a VPLMN, if the MS requests an APN that does not correspond to any GGSN of its HPLMN nor of this VPLMN, the request shall be rejected by SGSN.

If APN (S) = wild card (see GSM 03.03), it means either:

- that a default APN (a default PDN) has to be chosen by the SGSN (APN (SGSN)) if no APN (R) has been provided; or
- that a PDP context with dynamic PDP address may be activated towards any APN requested by the MS.

In order to derive APN (R) from the APN sent by the MS, the SGSN shall check if the APN sent by the user ends with ".gprs". If not, then APN (R) is equal to APN sent by the MS. If yes, then APN (R) is the APN sent by the MS without the three last labels.

A.2 Selection Rules

The SGSN shall select the APN to be used to derive the GGSN address, and set the selection mode parameter according to the rules in the SDL diagrams in this subclause. The following definitions apply to the SDL diagrams:

AddrMode: Addressing Mode.

APN-OI: APN Operator Identifier.

HPLMN-OI: HPLMN APN Operator Identifier.

Number <condition>: determines the PDP context subscription records that satisfy the given condition.

PDPaddr: PDP address.

SelMode := ChosenBySGSN: Network-provided APN, subscription not verified.

SelMode := SentByMS: MS-provided APN, subscription not verified.

SelMode := Subscribed: MS or Network-provided APN, subscription verified.

SelMode: Selection Mode.

VPLMN-OI: VPLMN APN Operator Identifier.

+: concatenation operation.

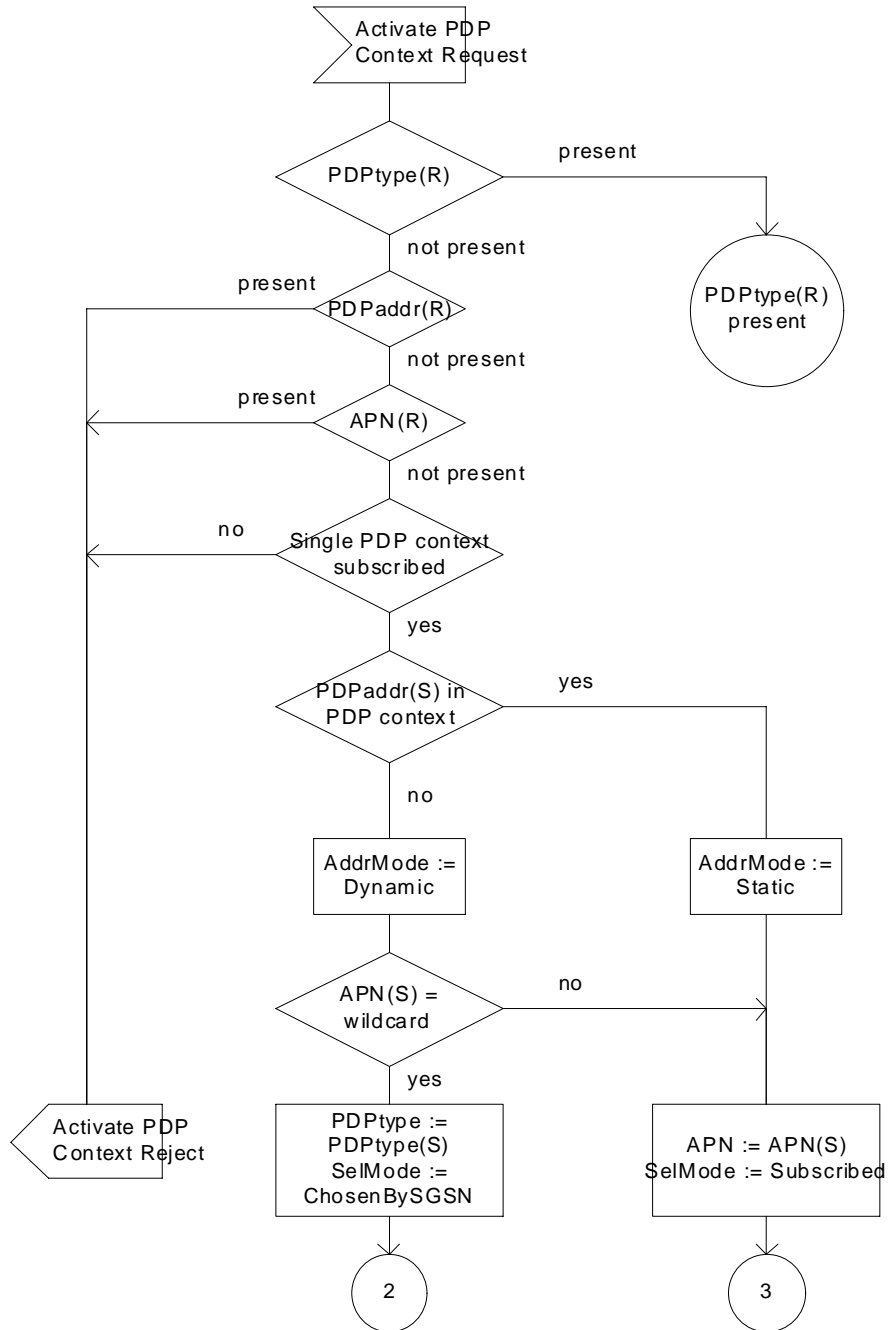


Figure A.1: SDL Diagram 1

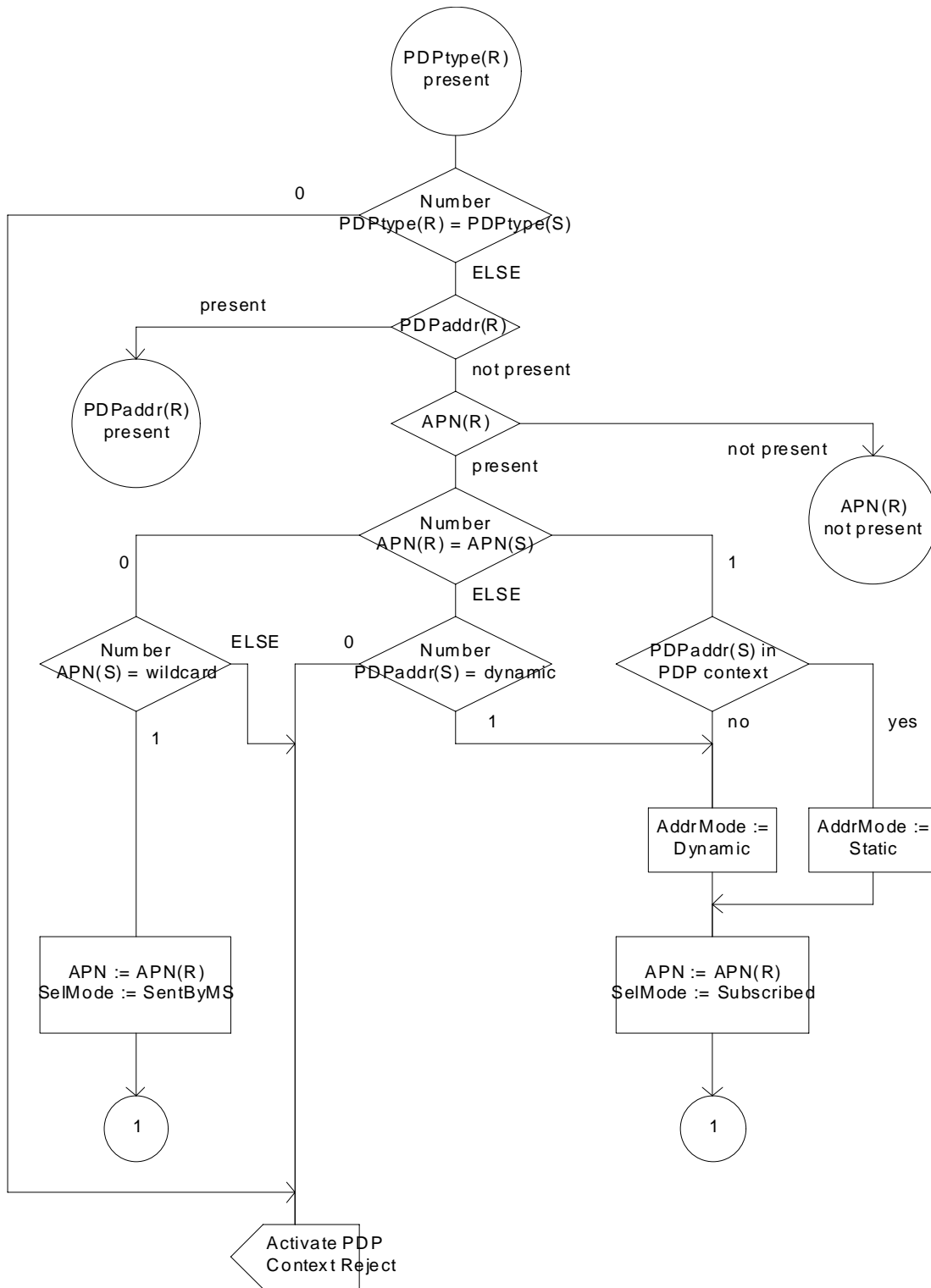


Figure A.2: SDL Diagram 2

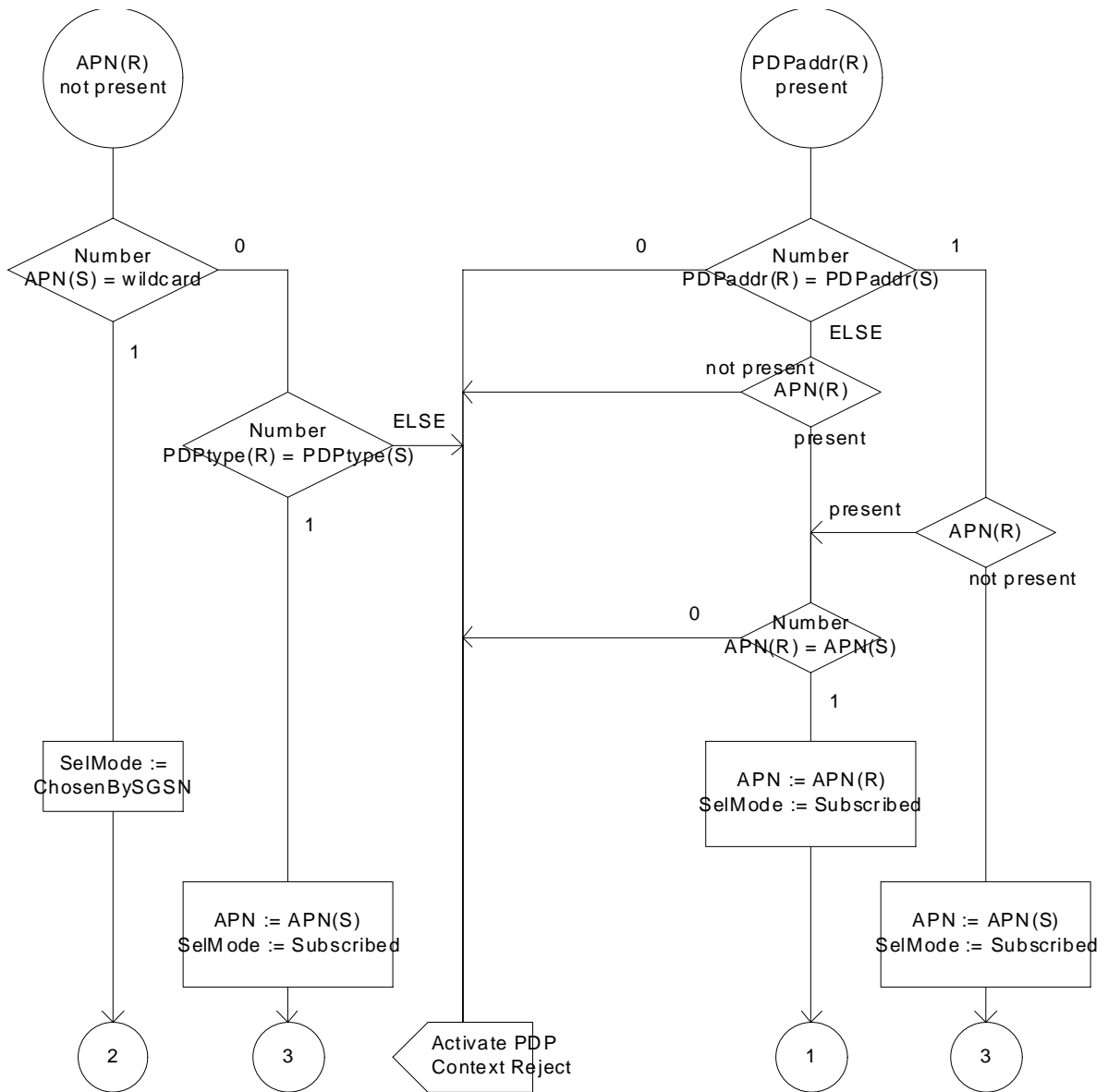


Figure A.3: SDL Diagram 3

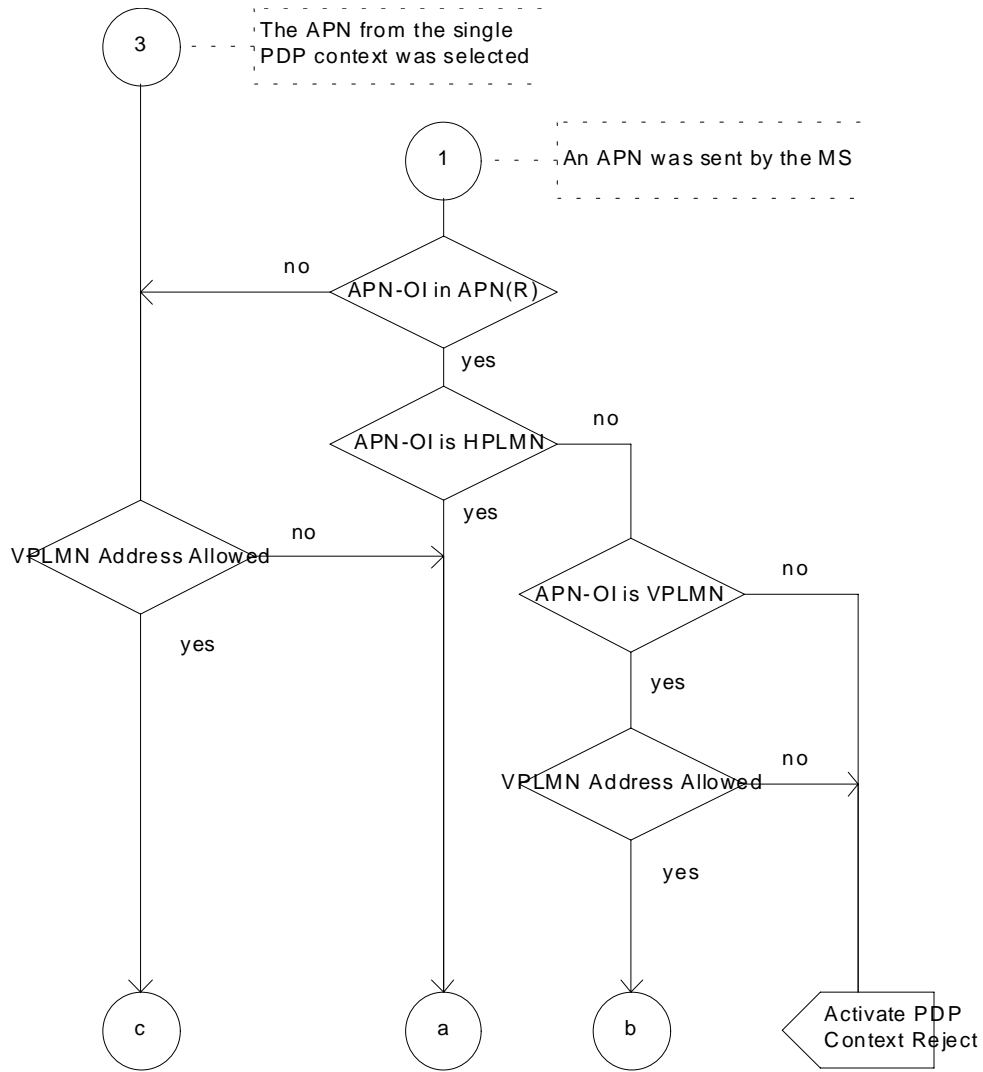


Figure A.4: SDL Diagram 4

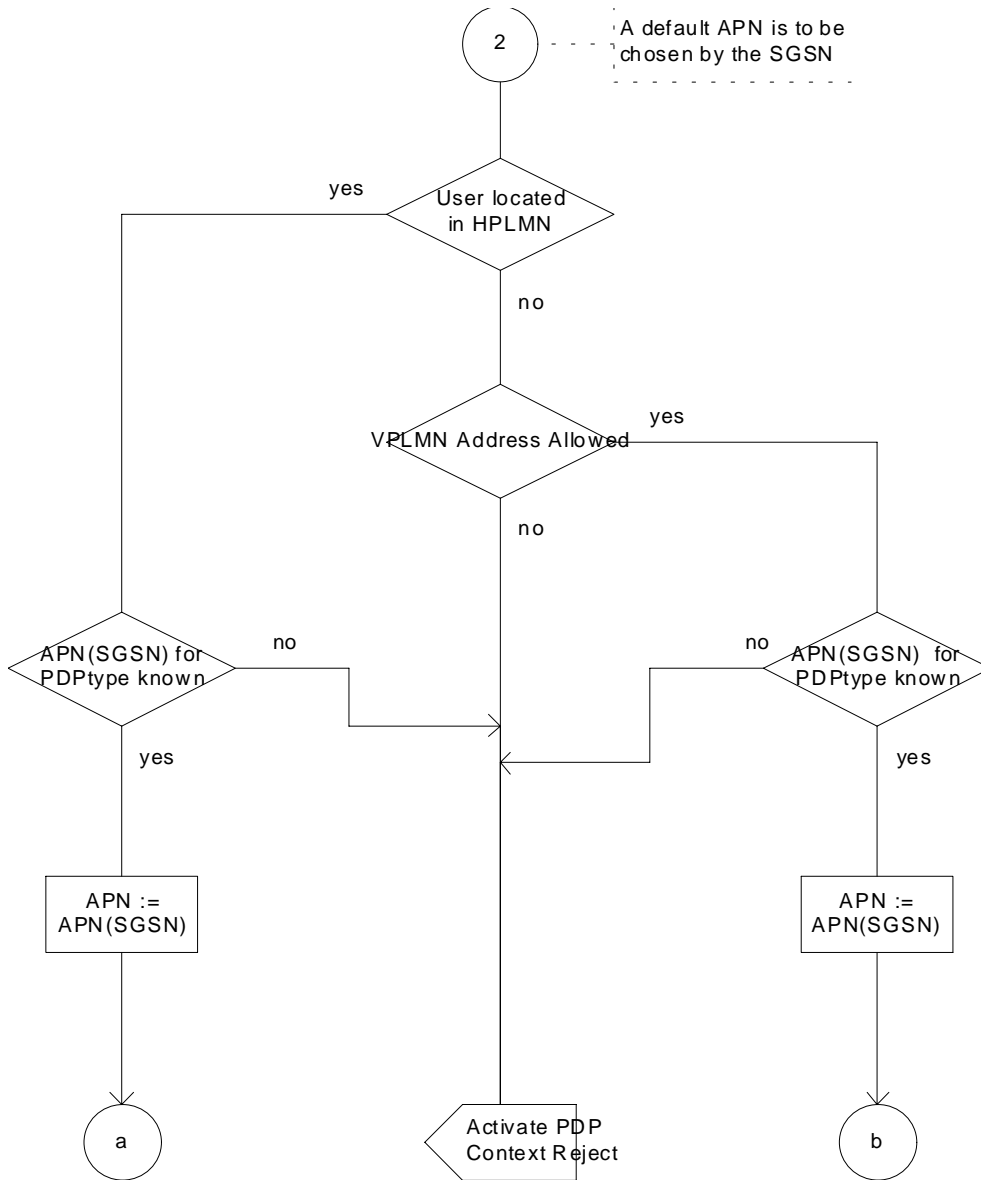


Figure A.5: SDL Diagram 5

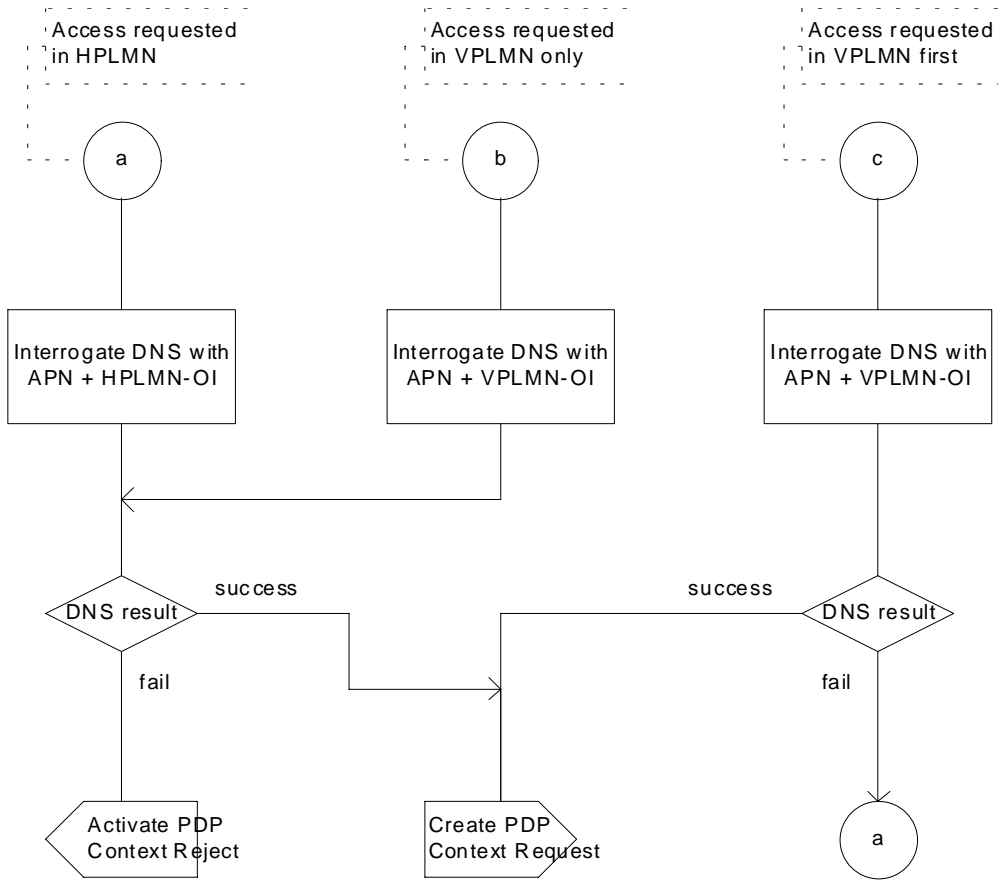


Figure A.6: SDL Diagram 6

Annex B (normative): Internet-Hosted Octet Stream Service

[Not yet updated for UMTS.]

The GPRS Internet-Hosted Octet Stream Service (IHOSS) is a connection-oriented service that can transport an unstructured octet (character) stream between a GPRS MS and an Internet host. The service uses the Octet Stream Protocol (OSP) PDP type to provide a 'character pipe' between the MS and the GGSN. In the GGSN there is an interworking function which provides a relay function between the OSP and the Internet host.

Figure B.1 shows the scope of IHOSS and OSP.

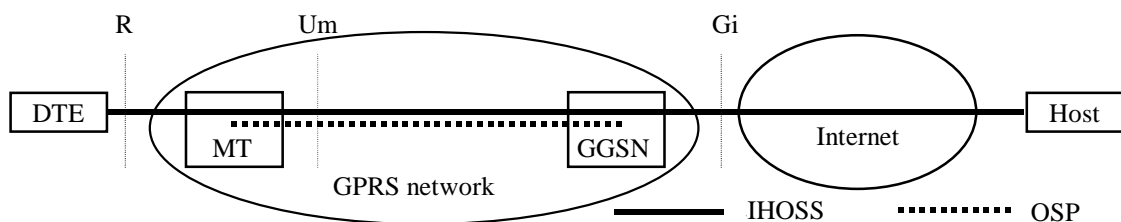


Figure B.1: Scope of IHOSS and OSP

IHOSS is analogous to a virtual serial cable between the MS and the Internet host.

This service is intended to provide a very simple connection for early implementation and for simple low-cost devices later on in the life cycle of GPRS.

B.1 Direction of Connection Setup

This service shall be mobile-originated only.

B.2 Bearer

The IHOSS shall use the unstructured Octet Stream Protocol as its bearer service.

The MT end of the IHOSS connection shall use the octet mode interface to the OSP as a Packet Assembler / Disassembler function is necessary.

The GGSN end of the IHOSS connection shall use the block mode interface to the OSP to remove the need for two back-to-back PAD functions.

B.3 Setup Data

The following data items are required before an octet stream can be initiated.

B.3.1 Protocol Type – TCP or UDP

This refers to the protocol used over IP on the GGSN to Internet host segment of the connection. The options available are TCP or UDP.

If no protocol is specified for a given context, TCP shall be used.

B.3.2 Host Name

This refers to the Internet host to which the connection is made. It shall be a fully formed domain name extended host name.

There shall be no default host name. If no host name is specified, the context activation shall fail.

B.3.3 Port Number

This refers to the TCP or UDP port on the host name, which forms the endpoint of the Internet side of the connection.

If no port number is specified for a given context, a default value of 23 decimal shall be used.

B.3.4 PAD Parameters

The Packet Assembler / Disassembler parameters determine how to fill the outgoing packets. If the user requires interactive terminal style behaviour then the PAD shall be able to act in this way. If the user requires a streaming data link then a different setup is necessary.

The default values for the PAD parameters are defined in GSM 07.60.

B.4 Flow Control

The service shall use the flow control features provided by the OSP to provide simple start / stop flow control.

B.5 Break Signal

The OSP break signals are mapped onto the appropriate break signals at the R and Gi interfaces.

B.6 Connection Establishment Procedure

Establishing an IHOSS connection involves setting up two segments, the PLMN segment (using the OSP) between the MS and the GGSN, and the fixed-network segment between the GGSN and the Internet host. Establishing the PLMN segment shall be as described in subclause "PDP Context Activation Procedure". Figure B.2 illustrates the overall procedure.

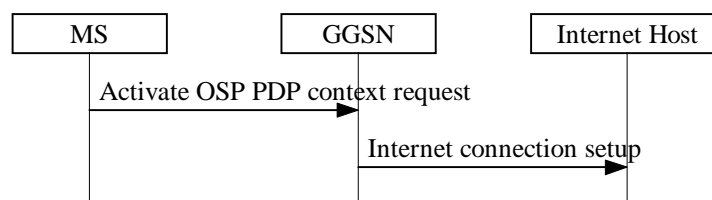


Figure B.2: IHOSS Connection Establishment

The MS requests that an OSP PDP context be activated by transmitting an Activate PDP Context Request (NSAPI, TI, PDP Type, PDP Address, Access Point Name, QoS Requested, PDP Configuration Options) message to the SGSN with the following parameter values:

- NSAPI is selected by the MS.
- TI is selected by the MS.

- PDP Type shall have a two-part value. The first part shall identify the protocol as OSP, and the second part shall identify the service being used and thereby allow the SGSN to select a GGSN that can provide this service. For IHOSS PDP Type shall be set to OSP:IHOSS.
- PDP Address shall be empty.
- APN is selected by the MS, may be empty.
- QoS Requested is selected by the MS.
- PDP Configuration Options may contain an Internet host name, a port number, a protocol type, and possibly other parameters in order to enable the GGSN to set up a connection to the Internet host, or it may be empty.

The Activate PDP Context Accept message shall be returned to the MS only after the connection to the Internet host has been established.

The activation parameters shall be provided as either interactive commands or via a system-default value. The following subclauses describe how these parameters shall be derived for a number of different scenarios.

B.6.1 Fully User-Specified Establishment

The MS shall request an OSP:IHOSS connection, specifying the PAD parameters, the host name, the port, and the protocol (UDP or TCP) in PDP Configuration Options.

The SGSN shall select an appropriate GGSN for the outgoing connection.

The GGSN shall attempt to establish a connection with the specified host. Connection failure shall be signalled back to the MS and the session terminated. A successful connection establishment enables data transmission over the connection.

B.6.2 Default Internet Endpoint Parameters Establishment

The MS shall request an OSP:IHOSS connection, specifying only PAD parameters that deviate from the system defaults.

The SGSN shall connect to the GGSN indicated by the APN in the HLR subscription record.

The GGSN shall use the APN to further select the host name, the port number, and the protocol. The method used to select these parameters is manufacturer specific and outside of the scope of the specifications.

B.7 Connection Termination

Either the MS or the Internet host may request that a connection be cleared.

B.7.1 MS-initiated TCP IHOSS Connection Termination

The MS clears the connection by sending a Deactivate PDP Context Request message to the SGSN. This shall result in the TCP session closure procedures being executed by the GGSN. Once this is complete, the GGSN shall deallocate any resources allocated for this session.

B.7.2 MS-initiated UDP IHOSS Connection Termination

No further action is required by the GGSN towards the Internet endpoint, as the User Datagram Protocol is connectionless. The GGSN shall deallocate any resources allocated for this session.

B.7.3 Internet Host Initiated TCP IHOS Connection Termination

When the GGSN receives a TCP clear request from the fixed network it shall follow the procedure described in subclause "PDP Context Deactivation Initiated by GGSN Procedure".

B.8 Quality of Service

The QoS profile shall be negotiated to the following QoS attribute values:

- Precedence: as required.
- Delay: as required, but consistent with PAD forwarding strategy.
- Reliability: Class 1 for TCP. Class 3 for UDP.
- Peak throughput: as required.
- Mean throughput: as required.

B.9 Security

B.9.1 Authentication of the GPRS User

Identification and authentication of the subscriber by the GPRS network is carried out as described elsewhere in this document. The GPRS network shall not provide any identification of the GPRS subscriber to the Internet host. End-to-end security is provided at the application layer and is outside of the scope of this document.

B.9.2 Malicious Reconfiguration of the GPRS Device

An MS that can not hold protocol, host name, and port information, would render it impossible to gain unauthorised access and subvert the system by providing alternative protocol, host name, or port information. This information would have to be provided by the GGSN, which is potentially more physically secure than the embedded MT, and it would make "man in the middle" type security breaches considerably more complex.

B.10 Maintenance

Configuring the Internet endpoint by accepting a mandatory default endpoint from the GGSN enables a GPRS user to effect system reconfiguration without the requirement for a site visit for each GPRS MS. The association between the APN and the host name, port number and protocol in the GGSN would be updated to give a new host name and/or port number and/or protocol.

Annex C (informative): Figures

Figure 1: Packet Domain Access Interfaces and Reference Points	18
Figure 2: Overview of the Packet Domain Logical Architecture	22
Figure 3: Intra- and Inter-PLMN Backbone Networks	23
Figure 4: User Plane for GPRS.....	26
Figure 5: User Plane GSN - GSN	27
Figure 6: User Plane for UMTS.....	27
Figure 7: Control Plane MS – 2G-SGSN.....	28
Figure 8: Control Plane MS - 3G-SGSN	29
Figure 9: Control Plane SGSN - HLR	29
Figure 10: Control Plane SGSN - MSC/VLR.....	30
Figure 11: Control Plane SGSN - SMS-GMSC and SGSN - SMS-IWMSC	30
Figure 12: Control Plane GSN - GSN.....	31
Figure 13: Control Plane GGSN - HLR Using MAP.....	31
Figure 14: Control Plane GGSN - HLR Using GTP and MAP.....	32
Figure 15: Functional Mobility Management State Model	34
Figure 16: Functional Anonymous Access Mobility Management State Model.....	35
Figure 17: PMM State Model.....	37
Figure 18: CS Paging Procedure.....	42
Figure 19: MS Information Procedure.....	44
Figure 20: MM Information Procedure.....	45
Figure 21: Combined GPRS / IMSI Attach Procedure	47
Figure 22: Combined PS / CS Attach Procedure	50
Figure 23: MS-Initiated Combined PS / CS Detach Procedure	53
Figure 24: SGSN-Initiated PS Detach Procedure	54
Figure 25: HLR-Initiated PS Detach Procedure	55
Figure 26: Purge Procedure	56
Figure 27: Authentication of GSM Subscriber in GSM Procedure.....	56
Figure 28: Authentication of UMTS Subscriber in UMTS Procedure.....	57
Figure 29: Authentication of GSM Subscriber in UMTS Procedure	58
Figure 30: P-TMSI Reallocation Procedure	60
Figure 31: Scope of Ciphering.....	60

Figure 32: Identity Check Procedure	61
Figure 33: Intra SGSN Routing Area Update Procedure	63
Figure 34: Inter SGSN Routing Area Update Procedure	64
Figure 35: Combined RA / LA Update in the Case of Intra SGSN RA Update Procedure.....	66
Figure 36: Combined RA / LA Update in the Case of Inter SGSN RA Update Procedure.....	68
Figure 37: UMTS RA Update Procedure	72
Figure 38: Before SRNS Relocation and Location Registration.....	75
Figure 39: After SRNS Relocation and RA Update.....	75
Figure 40: Phases 1 and 2 of Serving RNC Relocation	76
Figure 41: Control Plane MS - Non-GSM MSC/VLR.....	79
Figure 42: Uplink Tunnelling of non-GSM Signalling Messages Procedure.....	79
Figure 43: Downlink Tunnelling of non-GSM Signalling Messages Procedure	79
Figure 44: Insert Subscriber Data Procedure	80
Figure 45: Delete Subscriber Data Procedure.....	81
Figure 46: Service Request Initiated by MS Procedure	82
Figure 47: Service Request Initiated by Network Procedure	83
Figure 48: UMTS to GPRS Handover Between Cells in same RA.....	85
Figure 49: GPRS to UMTS Handover Between Cells in same RA.....	86
Figure 50: UMTS to GPRS Inter SGSN Routing Area Update Procedure	88
Figure 51: GPRS to UMTS Inter SGSN Routing Area Update Procedure	91
Figure 52: GPRS Paging Procedure.....	95
Figure 53: RRC Modes, Main RRC States and Main Mode and State Transition	96
Figure 54: PS Paging Without RRC Connection for CS.....	97
Figure 55: PS Paging With RRC Connection for CS.....	98
Figure 56: URA Paging Procedure	99
Figure 57: Functional PDP State Model	100
Figure 58: PDP Context Activation Procedure for GPRS	101
Figure 59: PDP Context Activation Procedure for UMTS	101
Figure 60: Secondary PDP Context Activation Procedure for GPRS.....	103
Figure 61: Secondary PDP Context Activation Procedure for UMTS.....	103
Figure 62: Successful Network-Requested PDP Context Activation Procedure.....	105
Figure 63: Protection Procedure	106
Figure 64: Mobile User Activity Procedure.....	107
Figure 65: Anonymous Access PDP Context Activation Procedure.....	107

Figure 66: SGSN-Initiated PDP Context Modification Procedure	109
Figure 67: GGSN-Initiated PDP Context Modification Procedure.....	109
Figure 68: MS-Initiated PDP Context Modification Procedure.....	110
Figure 69: PDP Context Deactivation Initiated by MS Procedure for GPRS	111
Figure 70: PDP Context Deactivation Initiated by MS Procedure for UMTS	111
Figure 71: PDP Context Deactivation Initiated by SGSN Procedure	112
Figure 72: PDP Context Deactivation Initiated by GGSN Procedure.....	112
Figure 73: Anonymous Access PDP Context Deactivation Initiated by MS Procedure	113
Figure 74: Anonymous Access PDP Context Deactivation Initiated by GGSN Procedure	113
Figure 75: Multiplexing of Network Protocols.....	118
Figure 76: Sequential Invocation of SNDC Functionality	119
Figure 77: GPRS User Plane for PDP Type OSP	120
Figure 78: UMTS User Plane for PDP Type OSP.....	120
Figure 79: GPRS User Plane for PDP Type PPP.....	122
Figure 80: UMTS User Plane for PDP Type PPP	122
Figure 81: BSSGP Protocol Position.....	123
Figure 82: BSS Packet Flow Context Creation Procedure.....	126
Figure 83: SGSN-Initiated BSS Packet Flow Context Modification Procedure	126
Figure 84: BSS-Initiated BSS Packet Flow Context Modification Procedure	127
Figure 85: SGSN-Initiated BSS Packet Flow Context Deletion Procedure	127
Figure 86: Iu User Plane Protocol Configuration for Packet-Switched Traffic	128
Figure 87: Iu Release Procedure	129
Figure 88: Location Reporting Procedure.....	130
Figure 89: Remote Packet Control Unit (PCU) Positions.....	131
Figure 90: Packet Domain Subscription Data.....	132
Figure 91: Use of NSAPI and TLLI	141
Figure 92: MT SMS Transfer, Successful	148
Figure 93: MT SMS Transfer, Unsuccessful	149
Figure 94: MO SMS Transfer, Successful.....	150
Figure 95: Suspend and Resume Procedure.....	151

Annex D (informative): Tables

Table 1: Mapping of Functions to Logical Architecture.....	25
Table 2: Network Operation Modes for GPRS.....	43
Table 3: Network Operation Modes for UMTS.....	43
Table 4: Mapping of High-level Functions Across the Gb Architecture.....	124
Table 5: HLR Packet Domain Subscription Data	133
Table 6: SGSN MM and PDP Contexts.....	134
Table 7: SGSN MM and PDP Contexts for Anonymous Access.....	135
Table 8: GGSN PDP Context	136
Table 9: GGSN PDP Context for Anonymous Access	136
Table 10: MS MM and PDP Contexts.....	137
Table 11: MS MM and PDP Contexts for Anonymous Access	138
Table 12: MSC/VLR Association.....	138
Table 13: BSS Context	138
Table 14: BSS Context for Anonymous Access	139
Table 15: RNC Context	139
Table 16: Precedence Classes.....	145
Table 17: Reliability Classes	146
Table 18: Peak Throughput Classes.....	147
Table 19: Mean Throughput Classes	147

Annex E: Change History

TSG CN#	Spec	Version	CR	<Phase>	New Version	Subject/Comment
Aug 1999	GSM 03.60	8.0.0				Transferred to 3GPP CN1
CN#04	23.060				3.0.0	Approved at CN#04
CN#05	03.60	7.1.0	A085r8	R99	3.1.0	Involvement of BSS in QoS provisioning
CN#05	03.60	7.1.0	A164r1	R99	3.1.0	Parallel handling of multiple user application flows
CN#05	23.060	3.0.0	001	R99	3.1.0	APN and GGSN selection SDL diagrams
CN#05	23.060	3.0.0	002	R99	3.1.0	Ga interface to the GPRS Logical Architecture diagram etc.
CN#05	23.060	3.0.0	003	R99	3.1.0	Modification information is not piggybacked
CN#05	23.060	3.0.0	004r1	R99	3.1.0	MM states in UMTS
CN#05	23.060	3.0.0	005r2	R99	3.1.0	Introduction of lu Release procedure
CN#05	23.060	3.0.0	006r1	R99	3.1.0	Addition of APN parameter in Network-requested PDP context activation procedures
CN#05	23.060	3.0.0	007r1	R99	3.1.0	Introduction of Service Request procedure
CN#05	23.060	3.0.0	008r2	R99	3.1.0	Introduction of LOCATION REPORTING procedure
CN#05	23.060	3.0.0	009	R99	3.1.0	MS and GSN-initiated PDP context modification
CN#05	23.060	3.0.0	010	R99	3.1.0	Introduction of EGPRS
CN#05	23.060	3.0.0	014r2	R99	3.1.0	Mobile terminated packet transfer to UE in PMM-Idle state
CN#05	23.060	3.0.0	015r2	R99	3.1.0	Clarification on multiplexing of several NSAPIS onto one LLC SAPI
CN#05	03.60	7.1.0	016	R98	3.1.0	PDP Context Deactivation during an activation
CN#05	23.060	3.0.0	018r2	R99	3.1.0	23.060 Section 1, 4
CN#05	23.060	3.0.0	019r1	R99	3.1.0	Change in chapter 2, 3 of 23.060
CN#05	23.060	3.0.0	020r1	R99	3.1.0	Changes in chapter 5 of 23.060
CN#05	23.060	3.0.0	021r1	R99	3.1.0	Updating of Section 9
CN#05	23.060	3.0.0	022r1	R99	3.1.0	Changes in chapter 7, 8 of 23.060
CN#05	23.060	3.0.0	023r1	R99	3.1.0	Adaptation to UMTS in chapter 13
CN#05	23.060	3.0.0	024r1	R99	3.1.0	Adaptation to UMTS in chapter 14
CN#05	23.060	3.0.0	025	R99	3.1.0	Extension of PDP type IP to support e.g. End-to-End DHCP or Mobile IP
CN#05	23.060	3.0.0	027r1	R99	3.1.0	Addition of Paging Co-ordination for UMTS
CN#05	23.060	3.0.0	028	R99	3.1.0	Modification of the definition and the usage of network operation mode
CN#05	23.060	3.0.0	029r1	R99	3.1.0	UMTS 23.060 v3.1.0 DRAFT 2
CN#05	23.060	3.0.0	030r1	R99	3.1.0	Authentication and security keys agreement for support of GSM-UMTS Interoperability
CN#05	23.060	3.0.0	031r1	R99	3.1.0	Introduction of UMTS security
CN#05	23.060	3.0.0	032	R99	3.1.0	Changes in chapter 11 of 23.060
CN#05	23.060	3.0.0	033r1	R99	3.1.0	Changes in chapter 12 of 23.060
CN#05	23.060	3.0.0	036r1	R99	3.1.0	CR to chapters 6.6
CN#05	23.060	3.0.0	037r1	R99	3.1.0	Interactions between 3G-SGSN and MSC/VLR for UMTS
CN#05	23.060	3.0.0	038r3	R99	3.1.0	Location Management and attach procedure for UMTS
CN#05	23.060	3.0.0	040	R99	3.1.0	Handling of lost of coverage for UMTS
CN#05	23.060	3.0.0	041r2	R99	3.1.0	Mobility Management states and state transitions for UMTS
CN#05	23.060	3.0.0	042r1	R99	3.1.0	Introduction of UMTS MS classes
CN#05	23.060	3.0.0	044r2	R99	3.1.0	UMTS-GPRS Intersystem Handover
CN#05	23.060	3.0.0	045r1	R99	3.1.0	Consistent Sequence Numbering of GTP-PDUs on lu and Gn interfaces

History

Document history		
V3.0.0	August 1999	Approved at TSGN #4. Under TSG CN Change Control.
DRAFT-1 V3.1.0	September 1999	For use at the 5-7 October 1999 23.060 drafting session in Helsinki.
DRAFT-2 V3.1.0	October 1999	Developed during the 5-7 October 1999 23.060 drafting session in Helsinki.
V3.1.0	October 1999	incorporation of all the CRs approved by SA2 and SA#5.