3GPP TR 29.803 V0.9.0 (2008-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System: CT WG4 Aspects (Stage3); Release 8

Select keywords from list provided in specs database.

Keywords
<keyword[, keyword]>

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

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

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 the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater 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 document.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The present document discusses and describes procedures and protocols from CT4 aspects of Evolved Packet System (EPS) towards a higher-data-rate, lower-latency, packet-optimized system that supports multiple access technologies.

These CT4 aspects include selection and study of protocols and procedures that will be used in the evolved system (e.g. within evolved packet core network, between EPC and current GPRS core network, between EPC and HSS/AAA, and between 3GPP and non-3GPP access), and describes impacts and required enhancements for related network protocols, including GTP and IETF protocols based on stage2 architecture requirements.

In addition, the present document also includes description of the new identities and addressing schemes required by Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet System (EPS), and in particular functional requirements and protocols for enhancing existing capabilities for EPS/E-UTRAN, e.g. MBMS and network sharing.

The present document is used as a place holder for CT4 EPS materials to be moved to appropriate 3GPP technical specifications when the TR is sufficiently stable.

2 References

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access ".

[3] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses".

[4] IETF, RFC 3344 (August, 2002), "Mobility Support for IPv4".

[5] IETF Draft, draft-ietf-netlmm-proxymip6-06.txt, "Proxy Mobile IPv6" work in progress.

[6] IETF Draft, draft-ietf-mip6-nemo-v4traversal-05.txt, "Dual Stack Mobile IPv6" work in progress.

[7] IETF RFC 4282 (December 2005): "The Network Access Identifier".

[8] 3GPP TS 29.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".

[9] 3GPP TS 23.003: "Numbering, addressing and identification".

[10] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[11] 3GPP TS 23.008: "Organization of subscriber data".

[12] IETF Draft, draft-muhanna-mip6-binding-revocation-01.txt, "Binding Revocation for IPv6 Mobility" work in progress.

[13] IETF RFC 4283: "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)".

[14] IETF RFC 3543: "Registration Revocation in Mobile IPv4".

[15] IETF Draft, draft-ietf-mip6-nemo-v4traversal-06.txt, "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", work in progress.

[16] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[17] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[18] IETF RFC 3588: "Diameter Base Protocol".

[19] IETF RFC 1034: "Domain Names – Concepts and facilities".

[20] IETF RFC 1035: "Domain Names – Implementation and Specification".

[21] GSMA PRD IR.67 – "DNS Guidelines for Operators" Version 2.1.0.

[22] IETF RFC 3401: "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS".

[23] IETF RFC 3402: "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm".

[24] IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".

[25] IETF RFC 3404: "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application".

[26] IETF RFC 3958: "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)".

[27] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Rel-8 HLR: a Rel-8 HLR is a HSS for GPRS/UMTS support only. It is used for a Rel-8 GRPS/UMTS network without EPS involved. A Rel-8 HLR only provides MAP based interfaces for a Rel-8 SGSN and a Rel-8 GGSN.

Editor's note: It is to be decided by SA2 whether this functional entity is a part of the Rel-8 network architecture.

Rel-8 HSS: a Rel-8 HSS is a PS domain functional entity. It serves the EPS, IMS and legacy systems. A Rel-8 HSS provides MAP based interfaces to a Rel-8 SGSN and Diameter based interface to an MME.

Rel-8 HSS-IMS: a Rel-8 HSS-IMS is a Rel-8 PS domain functional entity. It serves the EPS, IMS and legacy systems. A Rel-8 HSS-IMS provides MAP based interfaces to a Rel-8 SGSN and, via an IWF, to a Rel-8 MME or to a Rel-8 SGSN only. This HSS does support Diameter for IMS and/or I-WLAN although it does not support S6a.

Rel-8 HSS-EPS: a Rel-8 HSS-EPS is a Rel-8 PS domain functional entity. It serves only the EPS. The Rel-8 HSS-EPS without MAP based interfaces for EPS only provides Diameter based interfaces towards the MME.

Pre Rel-8 HLR: a pre Rel-8 HLR is a HSS for GPRS/UMTS support only. A pre Rel-8 HLR serves the pre Rel-8 GRPS/UMTS network. It only provides MAP based interfaces to a pre Rel-8 SGSN and a pre Rel-8 GGSN.

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HRPD	High Rate Packet Data
ISR	Idle-mode Signalling Reduction
GUMMEI	Globally Unique MME Identifier
GUTI	Globally Unique Temporary Identity
MMEC	MME Code
MMEGI	MME Group ID
MMEI	MME Identifier
M-TMSI	M-Temporary Mobile Subscriber Identity
S-TMSI	S-Temporary Mobile Subscriber Identity

4 Overview of CT4 Aspect of System Architecture Evolution

4.1 The aspect of "GPRS enhancements for E-UTRAN access"

4.1.1 Attach procedure

The Attach procedure is used for UE/users to register with the network to receive services that require registration. During Attachment, a default Bearer is established to enable the always-on IP connectivity for UE/users of the SAE system. The Attach procedure can also be used when a UE is already attached over GERAN/UTRAN, but has no PDP context established, and performs access change to E-UTRAN. The detailed information is in 3GPP TS 23.401 [2].

4.1.2 Dedicated Bearer Activation procedure

The Dedicated Bearer Activation procedure describes the scenario in which the network initiates a bearer establishment for an active mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.3 PDN GW initiated Bearer Deactivation procedure

The PDN GW initiated Bearer Deactivation procedure describes the scenario in which the PDN GW initiates a EPS bearer deactivation for an active mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.4 MME Initiated Dedicated Bearer Deactivation procedure

The MME Initiated Dedicated Bearer Deactivation procedure describes the scenario in which the MME initiates a bearer deactivation for an active mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.5 PDN GW Initiated Bearer Modification with Bearer QoS Update procedure

The PDN GW Initiated Bearer Modification with Bearer QoS Update procedure describes the scenario in which the PDN GW initiates a bearer modification with QoS of an EPS Bearer updated for an active mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.6 MME Initiated Bearer Modification with Bearer QoS Update procedure

The MME Initiated Bearer Modification with Bearer QoS Update procedure describes the scenario in which the MME initiates a bearer modification with QoS of an EPS Bearer updated for an active mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.7 Dedicated Bearer Modification without Bearer QoS Update procedure

The Dedicated Bearer Modification without Bearer QoS Update procedure describes the scenario in which the network initiates a bearer modification to update the Uplink TFT for an active dedicated Bearer of an active mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.8 E-UTRAN to UTRAN Iu Mode Inter RAT Handover Based on PS Handover procedure

The E-UTRAN to UTRAN Iu mode Inter RAT handover based on PS handover procedure describes the scenario in which an LTE_ACTIVE UE changes from an E-UTRAN cell to a UTRAN cell.. The detailed information is in 3GPP TS 23.401 [2].

4.1.9 Network Triggered Service Request procedure

The network Triggered Service Request procedure describes how the network can trigger the signalling procedure to send the downlink data to an idle mode UE. The detailed information is in 3GPP TS 23.401 [2].

4.1.10 Tracking Area Update procedure with MME and Serving Gateway change

The Tracking Area Update procedure with MME and Serving Gateway change describes the scenario in which an idle UE moves with tracking area and CN nodes change. The detailed information is in 3GPP TS 23.401 [2].

4.1.11 UE Triggered Service Request procedure

The UE Triggered Service Request procedure describes how an idle UE can trigger the signalling procedure to send the uplink data to the network. The detailed information is in 3GPP TS 23.401 [2].

4.1.12 UTRAN Iu Mode to E-UTRAN Inter RAT Handover Based on PS Handover procedure

The UTRAN Iu mode to E-UTRAN Inter RAT handover based on PS handover procedure describes the scenario in which a PMM_CONNECTED UE changes from a UTRAN cell to an E-UTRAN cell. The detailed information is in 3GPP TS 23.401 [2].

4.1.13 Detach procedures

There are four kinds of Detach procedures.

The UE-initiated Detach procedure describes the scenario in which the UE informs the network that it does not want to access to the EPS any longer. The detailed information is in 3GPP TS 23.401 [2].

The MME-initiated Detach procedure describes the scenario in which the MME informs the other network entities (for explicit detach scenario and implicit detach scenario) and the UE (for explicit detach scenario) that the UE does not have access to the EPS any longer. The detailed information is in 3GPP TS 23.401 [2].

The HSS-initiated Detach procedure describes the scenario in which the operator determines to remove the MM and EPS bearer of a subscriber. The detailed information is in 3GPP TS 23.401 [2].

The PDN GW-initiated Detach Procedure describes the scenario in which handovers without optimization occurs from 3GPP to non-3GPP. The detailed information is in 3GPP TS 23.401 [2].

4.1.14 Inter eNodeB Handover with MME Relocation procedure

The Inter eNodeB Handover with MME Relocation procedure describes the scenario in which an LTE_ACTIVE UE changes eNodeB accessed within E-UTRAN and the MME is or, the MME and the Serving Gateway are both relocated. The detailed information is in 3GPP TS 23.401 [2].

4.1.15 Inter eNodeB Handover without CN Node Relocation procedure

The Inter eNodeB Handover without CN Node Relocation procedure describes the scenario in which an LTE_ACTIVE UE changes eNodeB accessed within E-UTRAN with the MME and the Serving Gateway both unchanged. The detailed information is in 3GPP TS 36.300 [10] and 3GPP TS 23.401 [2].

4.1.16 Inter eNodeB Handover with only Serving GW Change procedure

The Inter eNodeB Handover with only Serving GW Change procedure describes the scenario in which an LTE_ACTIVE UE changes eNodeB accessed within E-UTRAN with MME unchanged and Serving GW changed. The detailed information is in 3GPP TS 23.401 [2].

4.1.17 E-UTRAN to GERAN A/Gb Mode Inter RAT Handover Based on PS Handover procedure

The E-UTRAN to GERAN A/Gb mode Inter RAT handover based on PS handover procedure describes the scenario in which an LTE_ACTIVE UE changes from an E-UTRAN cell to a GERAN cell. The detailed information is in 3GPP TS 23.401 [2].

4.1.18 GERAN A/Gb Mode to E-UTRAN Inter RAT Handover Based on PS Handover procedure

The GERAN A/Gb mode to E-UTRAN Inter RAT handover based on PS handover procedure describes the scenario in which a READY state UE changes from a GERAN cell to an E-UTRAN cell. The detailed information is in 3GPP TS 23.401 [2].

4.1.19 S1 Release procedure

The S1 Release procedure describes the scenario in which all S1 bearers for a UE are released and the UE state in MME is set to LTE_IDLE. The detailed information is in 3GPP TS 23.401 [2].

4.1.20 GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure

The GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure describes the scenario in which an idle state UE registered with a SGSN selects an E-UTRAN cell and changes to a Tracking Area in which it has not yet registered. The detailed information is in 3GPP TS 23.401 [2].

4.1.21 E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure

The E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure describes the scenario in which an idle state UE registered with an MME selects a GERAN cell and changes to a Routing Area in which it has not yet registered. The detailed information is in 3GPP TS 23.401 [2].

4.1.22 UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure

The UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure describes the scenario in which an idle state UE registered with a 3G-SGSN selects an E-UTRAN cell and changes to a Tracking Area in which it has not yet registered. The detailed information is in 3GPP TS 23.401 [2].

4.1.23 E-UTRAN to UTRAN Iu Mode Routing Area Update procedure

The E-UTRAN to UTRAN Iu Mode Routing Area Update procedure describes the scenario in which an idle state UE registered with an MME selects a UTRAN cell and changes to a Routing Area in which it has not yet registered. The detailed information is in 3GPP TS 23.401 [2].

4.1.24 Subscriber Profile Update procedure

The Subscriber Profile Update procedure describes the scenario in which the HSS informs the MME that it has added, modified, or deleted information in a subscriber's subscription data.

4.1.25 Purge procedure

The Purge procedure describes the scenario in which the MME inform the HSS that it has deleted the subscription data and MM context of a detached MS.

4.1.26 Reset procedure

The Reset procedure describes the scenario in which the HSS informs all MMEs to which its subscribers are attached that it has lost its subscribers mobility data.

4.1.27 UE requested bearer resource allocation procedure

The UE requested bearer resource allocation procedure describes the scenario in which the UE requests an allocation of bearer resources to a new Service Data Flow. If accepted by the network, the request invokes either the Dedicated Bearer Activation Procedure or the Dedicated Bearer Modification Procedure. The detailed information is in TS 23.401 [2].

4.1.28 UE Requested Bearer Resource Release procedure

The UE Requested Bearer Resource Release procedure describes the scenario in which the UE requests for release of bearer resources associated with a Service Data Flow. If accepted by the network, the request invokes either the Dedicated Bearer Deactivation Procedure or the Dedicated Bearer Modification Procedure. The detailed information is in 3GPP TS 23.401 [2].

4.1.29 UE Requested PDN Connectivity procedure

The UE Requested PDN Connectivity procedure describes the scenario in which an active mode UE requests for connectivity to a PDN including allocation of a default bearer through E-UTRAN. The detailed information is in 3GPP TS 23.401 [2].

4.1.30 Authentication Information Retrieval procedure

The Authentication Information Retrieval procedure describes the scenario in which the MME requests authentication information from the HSS.

4.2 The aspect of "Architecture enhancements for non-3GPP accesses"

4.2.1 Initial Attach procedure of Trusted non-3GPP IP accesses using S2a

The subclause describes the initial attach procedure of Trusted non-3GPP accesses which occurs when the UE powers-on in a trusted non-3GPP IP access and attaches to the EPS via S2a interface.

There are two kinds of procedures depending on the position of the anchor.

Initial Attach procedure with S2a and Anchor in PDN GW describes the procedure in which UE accesses EPS via S2a interface and the anchoring is in the PDN GW. In this procedure, the user plane on S8 interface is not established. The later user traffic will not go through the S8 interface. The PDN GW can be in the HPLMN (the non roaming scenario and the Home Routed roaming scenario in which the termination of S6b is PDN GW and AAA Server) or in the VPLMN (the Local Breakout roaming scenario in which the termination of S6b is PDN GW and AAA Proxy).

Initial Attach procedure with S2a and Anchor in Serving GW describes the procedure in which UE accesses EPS via S2a interface and the anchoring is in the Serving GW in VPLMN. In this procedure, the user plane on S8 interface is established. The later user traffic will go through the S8 interface. This procedure is used only for Home Routed roaming scenario in which PDN GW is in HPLMN and the termination of S6b is PDN GW and AAA Server.

The S2a interface shall support Client MIPv4 Foreign Agent (FA) Mode as defined in IETF RFC 3344 [4] and Proxy MIPv6 as defined in Internet-Draft, draft-ietf-netlmm-proxymip6-06 [5]. So two initial attach procedures of Trusted non-3GPP IP accesses are specified. For more information about initial attach procedures of Trusted non-3GPP IP accesses is in 3GPP TS 23.402 [3].

In the non-roaming case, S2a interface is between trusted non-3GPP IP accesses and PDN GW in home network; STa interface is between trusted non-3GPP IP accesses and 3GPP AAA Server.

4.2.2 Detach Procedures for Trusted Non-3GPP IP Accesses using S2a

4.2.2.1 General

The subclause describes the Detach procedures which occur when a UE previously accessing EPS over Trusted Non-3GPP IP Accesses does not have access to EPS any longer.

There are two kinds of procedures depending on the position of the anchor.

The Detach Procedures with S2a and Anchoring in PDN GW. These procedures describe the scenario in which a UE previously accessing the EPS via S2a interface with anchor in the PDN GW doesn't have access to EPS any longer. The S8 interfaces are not involved in these procedures. The PDN GW can be in the HPLMN (the non-roaming scenario and the Home Routed roaming scenario in which the termination of S6b is PDN GW and AAA Server) or in the VPLMN (the Local Breakout roaming scenario in which the termination of S6b is PDN GW and AAA Proxy).

The Detach Procedures with S2a and Anchoring in Serving GW. These procedures describe the scenario in which a UE previously accessing the EPS via S2a interface with anchor in the Serving GW doesn't have access to EPS any longer. The S8 interfaces are involved in these procedures. These procedures are used only for Home Routed roaming scenario in which PDN GW is in HPLMN and the termination of S6b is PDN GW and AAA Server.

4.2.2.2 Detach Procedures with S2a and Anchoring in PDN GW

The S2a interface shall support Client MIPv4 Foreign Agent (FA) Mode as defined in IETF RFC 3344 [4] and Proxy MIPv6 as defined in Internet-Draft, draft-ietf-netlmm-proxymip6 [5]. Under either mode of S2a, there are three kinds of detach procedures.

The UE-initiated Detach procedure describes the scenario in which the UE informs the network that it does not want to access to the EPS any longer, e.g. when the UE is power off. The detailed information is in 3GPP TS 23.402 [3].

The Trusted Non-3GPP Access Network-initiated Detach procedure describes the scenario in which the Trusted Non-3GPP Access Network informs the other network entities (for explicit detach scenario and implicit detach scenario) and the UE (for explicit detach scenario) that the UE does not have access to the EPS any longer due to administration reason or the detection of UE's leaving. The detailed information is in 3GPP TS 23.402 [3].

The HSS/AAA-initiated Detach procedure describes the scenario in which the network does not allow a UE to have access to the EPS any longer because, e.g. operator determines to remove a user's subscription (for HSS initiated procedure), received instruction from O&M (for AAA initiated procedure) or timer for re-authentication/re-authorization expired (for AAA initiated procedure). The detailed information is in 3GPP TS 23.402 [3].

Different de-registration messages shall be used on S2a interface, according to the mobility mode and the initiator of MIP de-registration:

In the case of the MIPv4 FA Mode:

- for the UE-initiated Detach procedures, MIPv4 De-registration procedures as defined in IETF RFC 3344 [4] are used
- for the NW-initiated Detach procedures, MIPv4 Revocation procedures as defined in IETF RFC 3543 [14] are used

In the case of the PMIPv6:

- for the UE-initiated/NW-initiated Detach procedures, PMIP De-registration procedures defined in Internet-Draft, draft-ietf-netlmm-proxymip6 [5] are used.

If there are multiple (P)MIP tunnels connecting towards multiple PDNs, all active (P)MIP bandings are released one by one.

The PDN GW information stored in the HSS shall be removed after corresponding (P)MIP banding to each PDN is released.

4.2.2.3 Detach Procedures with S2a and Anchoring in Serving GW

The Detach Procedures with S2a anchoring in Serving GW are FFS.

4.2.3 Initial Attach procedure of Untrusted non-3GPP IP accesses using S2b

The subclause describes the initial attach procedure of Untrusted non-3GPP accesses which occurs when the UE powers-on in a untrusted non-3GPP IP access and attaches to the EPS via S2b interface.

There are two kinds of procedures depending on the position of the anchor.

Initial Attach procedure with S2b and Anchor in PDN GW describes the procedure in which UE accesses EPS via S2b interface and the anchoring is in the PDN GW. In this procedure, the user plane on S8 interface is not established. The later user traffic will not go through the S8 interface. The PDN GW can be in the HPLMN (the non roaming scenario and the Home Routed roaming scenario in which the termination of S6b is PDN GW and AAA Server) or in the VPLMN (the Local Breakout roaming scenario in which the termination of S6b is PDN GW and AAA Proxy).

Initial Attach procedure with S2b and Anchor in Serving GW describes the procedure in which UE accesses EPS via S2b interface and the anchoring is in the Serving GW in VPLMN. In this procedure, the user plane on S8 interface is established. The later user traffic will go through the S8 interface. This procedure is used only for Home Routed roaming scenario in which PDN GW is in HPLMN and the termination of S6b is PDN GW and AAA Server.

The S2b interface shall Proxy MIPv6 as defined in Internet-Draft, draft-ietf-netlmm-proxymip6-06[5]. For more information about initial attach procedures of Untrusted non-3GPP IP accesses is in 3GPP TS 23.402 [3].

In the non-roaming case, S2b interface is between evolved Packet Data Gateway (ePDG) and the PDN GW; SWm interface is between ePDG and 3GPP AAA Server.

In the roaming case with home routed traffic anchored by visited Serving GW, S2b is between ePDG and Serving GW in visited network; PMIP-based S8 interface is between Serving GW in VPLMN and PDN GW in HPLMN; SWm interface is between ePDG and 3GPP AAA Proxy.

Editor's Note: It is FFS that in the roaming case whether the scenario of S2b between ePDG and PDN GW in home network exists.

4.2.4 Detach Procedure for Untrusted Non-3GPP IP Accesses using S2b

4.2.4.1 General

The subclause describes the Detach procedures which occur when a UE previously accessing EPS over Untrusted Non-3GPP IP Accesses dose not have access to EPS any longer.

There are two kinds of procedures depending on the position of the anchor.

The Detach Procedures with S2b and Anchoring in PDN GW. These procedures describe the scenario in which a UE previously accessing the EPS via S2b interface with anchor in the PDN GW doesn't have access to EPS any longer. The S8 interfaces are not involved in these procedures. The PDN GW can be in the HPLMN (the non-roaming scenario and the Home Routed roaming scenario in which the termination of S6b is PDN GW and AAA Server) or in the VPLMN (the Local Breakout roaming scenario in which the termination of S6b is PDN GW and AAA Proxy).

The Detach Procedures with S2b and Anchoring in Serving GW. These procedures describe the scenario in which a UE previously accessing the EPS via S2b interface with anchor in the Serving GW doesn't have access to EPS any longer. The S8 interfaces are involved in these procedures. These procedures are used only for Home Routed roaming scenario in which PDN GW is in HPLMN and the termination of S6b is PDN GW and AAA Server.

4.2.4.2 Detach Procedures with S2b and Anchoring in PDN GW

The S2b interface shall support Proxy MIPv6 as defined in Internet-Draft, draft-ietf-netlmm-proxymip6 [5]. There are three kinds of detach for S2b procedures.

The UE-initiated Detach procedure describes the scenario in which the UE informs the network that it does not want to access to the EPS any longer, e.g. when the UE is power off. The detailed information is in 3GPP TS 23.402 [3].

The ePDG-initiated Detach procedure describes the scenario in which the ePDG informs the other network entities (for explicit detach scenario and implicit detach scenario) and the UE (for explicit detach scenario) that the UE does not have access to the EPS any longer due to administration reason or the IKEv2 tunnel releasing. The detailed information is in 3GPP TS 23.402 [3].

The HSS/AAA-initiated Detach procedure describes the scenario in which the network does not allow a UE to have access to the EPS any longer because, e.g. operator determines to remove a user's subscription (for HSS initiated procedure), received instruction from O&M (for AAA initiated procedure) or timer for re-authentication/re-authorization expired (for AAA initiated procedure). The detailed information is in 3GPP TS 23.402 [3].

For the above Detach procedures, PMIP De-registration procedures defined in Internet-Draft, draft-ietf-netlmm-proxymip6 [5] are used.

If there are multiple PMIP tunnels connecting towards multiple PDNs, all active PMIP bindings are released one by one.

The PDN GW information stored in the HSS shall be removed after corresponding PMIP bindings to each PDN is released.

4.2.4.3 Detach Procedures with S2b and Anchoring in Serving GW

The Detach Procedures with S2b anchoring in Serving GW are FFS.

4.2.5 Initial Attach procedure of IP accesses using S2c

The subclause describes the initial attach procedure to trusted non-3GPP and untrusted non-3GPP accesses via the S2c reference point.

The S2c reference point shall support DSMIPv6 as defined in Internet-Draft, draft-ietf-mip6-nemo-v4traversal-06 [15]. More information about initial attach procedures to trusted non-3GPP and untrusted non-3GPP IP accesses using S2c is in 3GPP TS 23.402 [3].

In this procedure, the user plane on S8 interface is not established. The later user traffic will not go through the S8 interface.

In both, the roaming and non-roaming case, the S2c reference point is between the UE and the PDN gateway. The S6b reference point is between the PDN gateway and the 3GPP AAA server.

4.2.6 Detach procedure of IP accesses using S2c

The subclause describes the detach procedure for the S2c reference point.

More information about this procedure is in 3GPP TS 23.402 [3].

The detach can be initiated by the UE which is indicated to the PDN GW by a Binding Update with lifetime 0. Upon the receipt of the Binding Update with lifetime 0, the PDN GW sends an Update PDN GW address request to the 3GPP AAA server to remove the related PDN GW address information, e.g. a Session Termination Request (STR) message. The 3GPP AAA Server responds to the update PDN GW address acknowledgement message, e.g. a Session Termination Answer (STA) message.

The detach can also be initiated by the 3GPP AAA Server. In this case, the 3GPP AAA Server sends a Detach Indication message, e.g. an Abort Session Request (ASR) message, to the PDN GW. The PDN GW responds to the Detach Indication with a Detach Ack message, e.g. an Abort Session Answer (ASA) message.

4.2.7 Handover procedure from 3GPP access to non-3GPP access

The subclause describes the handover procedure from 3GPP access to non-3GPP access in which an UE changes radio access from a 3GPP access to non-3GPP access. The detailed information is in 3GPP TS 23.402 [3].

4.2.8 Handover procedure from non-3GPP access to 3GPP access

The subclause describes the handover procedure from non-3GPP access to 3GPP access in which an UE changes radio access from a non-3GPP access to 3GPP access. The detailed information is in 3GPP TS 23.402 [3].

4.2.9 Optimized Active Handover: E-UTRAN Access to cdma2000 HRPD Access

The subclause describes the Optimized Active Handover from E-UTRAN Access to cdma2000 HRPD Access procedure in which a UE changes radio access from 3GPP access to non-3GPP access. The detailed information is in 3GPP TS 23.402 [3].

In case where the UE is connected to the EUTRAN and conditions are such that a handover to HRPD may be required, the source system provides the UE with sufficient information to perform pre-registration with the target HRPD access and core network, over the S101 tunnelling interface. If conditions subsequently warrant that a handover should occur, the handover signalling will also be performed over the S101 tunnelling interface. Once the UE is ready to connect to the target system, it switches to the HRPD access

4.2.10 Optimized Active Handover: cdma2000 HRPD Access to E-UTRAN Access

The subclause describes the Optimized Active Handover from cdma2000 HRPD Access to E-UTRAN Access procedure in which a UE changes radio access from non-3GPP access to 3GPP access. The detailed information is in 3GPP TS 23.402 [3].

In case where the UE is connected to the HRPD and conditions are such that a handover to E-UTRAN may be required, the source system provides the UE with sufficient information to perform pre-registration with the target EPS. The pre-registration may be performed over the S101 tunnelling interface. If conditions subsequently warrant that a handover should occur, the handover signalling may also be performed over the S101 tunnelling interface. Once the UE is ready to connect to the target system, it switches to the E-UTRAN access

5 Functional Entities

<This section explains the role of the functional entity>

6 Description of Interfaces

6.1 General

The stage 2 parameters in the "Requirements" subsection are to describe the stage 2 functions. The stage 2 parameters are from the stage 2 requirements and will apply to all of the stage 3 protocol candidates. If the function of a stage 2 parameter is not described in stage 2 specification, it should be described in the related "Requirements" subsection.

The stage 3 parameters in the "Analysis" subsection are to describe the realization the related stage 2 functions based on some protocol candidate. The parameter name for the stage 3 parameter should be the same as that of the corresponding stage 2 parameter although in some cases they may have to be different because of the requirements of the protocol. Where they do have to be different, the stage 3 parameter should clearly state the mapping to the associated stage 2 parameter and the reason why they are different stated in the analysis section where the list of stage 3 parameter are.

6.2 Interface related to "GPRS enhancements for E-UTRAN access"

Editor's note: It needs to be investigated if GTP version upgrade is necessary.

6.2.1 Introduction

6.2.2 SGSN – MME (S3) Interface

6.2.2.1 Requirements

6.2.2.1.1 E-UTRAN to UTRAN Iu Mode Inter RAT Handover Based on PS Handover Procedure

6.2.2.1.1.1 Forward Relocation Request

The parameters for Forward Relocation Request message are, but not exclusively, listed as below:

- IMSI;
- Target Identification;
- MM Context;
- PDP Context;
- PDP Context Prioritization;
- MME Address for control plane on S3;
- MME S3 TEID for control plane;
- Source to Target Transparent Container;
- S1-AP Cause;
- Direct Forwarding Flag;

6.2.2.1.1.2 Forward Relocation Response

The parameters for Forward Relocation Response message are, but not exclusively, listed as below:

- Cause;
- SGSN Address for control plane;

- SGSN TEID for control plane;
- RANAP cause;
- SGSN Number;
- Target to Source Transparent Container;
- RAB Setup Information;
- Additional RAB Setup Information;
- Address for Data Forwarding (RNC address for direct forwarding, or Serving Gateway S1 address for indirect forwarding);
- TEID for Data Forwarding (RNC TEID for direct forwarding, or Serving Gateway S1 TEID for indirect forwarding);

6.2.2.1.1.3 Forward SRNS Context

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context message are, but not exclusively, listed as below:

- Delivery Order;

6.2.2.1.1.4 Forward SRNS Context Acknowledge

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context Acknowledge message are FFS.

6.2.1.1.1.5 Forward Relocation Complete

The parameters for Forward Relocation Complete message are FFS.

6.2.2.1.1.6 Forward Relocation Complete Acknowledge

The parameters for Forward Relocation Complete Acknowledge message are FFS.

6.2.2.1.2 UTRAN Iu Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.2.2.1.2.1 Forward Relocation Request

The parameters for Forward Relocation Request message are, but not exclusively, listed as below:

- IMSI;
- Target Identification;
- MM Context;
- PDP Context;
- PDP Context Prioritization;
- SGSN Address for control plane on S3;
- SGSN TEID for control plane on S3;
- Source to Target Transparent Container;
- Direct Forwarding Flag;

6.2.2.1.2.2 Forward Relocation Response

The parameters for Forward Relocation Response message are, but not exclusively, listed as below:

- Cause;
- List of Set Up RABs;
- MME Address for control plane on S3;
- MME TEID for control plane on S3;
- S1-AP cause;
- Target to Source Transparent Container;
- Address for Data Forwarding (eNodeB address for direct forwarding, or Serving Gateway S4 address for indirect forwarding);
- TEID for Data Forwarding (eNodeB TEID for direct forwarding, or Serving Gateway S4 TEID for indirect forwarding);

6.2.2.1.2.3 Forward SRNS Context

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context message are FFS

6.2.2.1.2.4 Forward SRNS Context Acknowledge

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context Acknowledge message are FFS.

6.2.1.1.2.5 Forward Relocation Complete

The parameters for Forward Relocation Complete message are FFS.

6.2.2.1.2.6 Forward Relocation Complete Acknowledge

The parameters for Forward Relocation Complete Acknowledge message are FFS.

6.2.2.1.3 E-UTRAN to GERAN A/Gb Mode Inter RAT Handover Based on PS Handover Procedure

6.2.2.1.3.1 Forward Relocation Request

The parameters for Forward Relocation Request message are, but not exclusively, listed as below:

- IMSI;
- Target Identification;
- MM Context;
- PDP Context;
- PDP Context Prioritization;
- MME Address for control plane on S3;
- MME S3 TEID for control plane;
- Source to Target Transparent Container;
- (Packet Flow ID is FFS);

- (XID Parameters is FFS);
- Direct Forwarding Flag.

Editor's note: It should be clarified if "Cell Identification IE" in Forward Relocation Request is needed or if The Target Identification IE may include: "Target CellId" (in case 2G), "Target RNCId" (in case 3G) or "Target eNodeB" (in case E-UTRAN).

6.2.2.1.3.2 Forward Relocation Response

The parameters for Forward Relocation Response message are, but not exclusively, listed as below:

- Cause;
- SGSN Address for control plane on S3;
- SGSN S3 TEID for control plane;
- BSSGP cause;
- (List of set-up PFIs is FFS);
- Target to Source Transparent Container;
- Address for Data Forwarding (SGSN address for direct forwarding, or Serving Gateway S1 address for indirect forwarding);
- TEID for Data Forwarding (SGSN TEID for direct forwarding, or Serving Gateway S1 TEID for indirect forwarding).

6.2.2.1.3.3 Forward SRNS Context

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context message are, but not exclusively, listed as below:

- Delivery Order;

6.2.2.1.3.4 Forward SRNS Context Acknowledge

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context Acknowledge message are FFS.

6.2.2.1.3.5 Forward Relocation Complete

The parameters for Forward Relocation Complete message are FFS.

6.2.2.1.3.6 Forward Relocation Complete Acknowledge

The parameters for Forward Relocation Complete Acknowledge message are FFS.

6.2.2.1.4 GERAN A/Gb Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.2.2.1.4.1 Forward Relocation Request

The parameters for Forward Relocation Request message are, but not exclusively, listed as below:

- IMSI;
- Target Identification;
- MM Context;
- PDP Context;

- PDP Context Prioritization;
- SGSN Address for control plane on S3;
- SGSN S3 TEID for control plane;
- Source to Target Transparent Container;
- (Packet Flow ID is FFS);
- (SNDCP XID Parameters is FFS);
- (LLC XID Parameters, is FFS);
- Direct Forwarding Flag.

6.2.2.1.4.2 Forward Relocation Response

The parameters for Forward Relocation Response message are, but not exclusively, listed as below:

- Cause;
- (List of Set Up PFCs, is FFS);
- MME Address for control plane on S3;
- MME S3 TEID for control plane;
- S1-AP cause;
- Target to Source Transparent Container;
- Address for Data Forwarding (eNodeB address for direct forwarding, or Serving Gateway S4 address for indirect forwarding);
- TEID for Data Forwarding (eNodeB TEID for direct forwarding, or Serving Gateway S4 TEID for indirect forwarding).

6.2.2.1.4.3 Forward SRNS Context

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context message are FFS.

6.2.2.1.4.4 Forward SRNS Context Acknowledge

Editor's note: Whether this message is needed is FFS.

The parameters for Forward SRNS Context Acknowledge message are FFS.

6.2.2.1.4.5 Forward Relocation Complete

The parameters for Forward Relocation Complete message are FFS.

6.2.2.1.4.6 Forward Relocation Complete Acknowledge

The parameters for Forward Relocation Complete Acknowledge message are FFS.

6.2.2.1.5 GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure

6.2.2.1.5.1 Context Request

The parameters for Context Request message are, but not exclusively, listed as below:

- Old RAI;
- Old P-TMSI;

- MME Address for control plane on S3;

6.2.1.1.5.2 Context Response

The parameters for Context Response message are, but not exclusively, listed as below:

- 2G-SGSN Context;

Editor's note: The detailed content of 2G-SGSN Context is FFS.

6.2.1.1.5.3 Context Acknowledge

The parameters for Context Acknowledge message are FFS.

6.2.2.1.6 E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure

6.2.2.1.6.1 Context Request

The parameters for Context Request message are, but not exclusively, listed as below:

- Old TAI;
- Old GUTI;
- SGSN Address for control plane on S3;

6.2.2.1.6.2 Context Response

The parameters for Context Response message are, but not exclusively, listed as below:

- MME Context;

6.2.2.1.6.3 Context Acknowledge

The parameters for Context Acknowledge message are FFS.

6.2.2.1.7 UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure

6.2.2.1.7.1 Context Request

The parameters for Context Request message are, but not exclusively, listed as below:

- Old RAI;
- Old P-TMSI;
- MME Address for control plane on S3;

6.2.2.1.7.2 Context Response

The parameters for Context Response message are, but not exclusively, listed as below:

- 3G-SGSN Context;

Editor's note: The detailed content of 3G-SGSN Context is FFS.

6.2.2.1.7.3 Context Acknowledge

The parameters for Context Acknowledge message are FFS.

6.2.2.1.8 E-UTRAN to UTRAN Iu Mode Routing Area Update procedure

6.2.2.1.8.1 Context Request

The parameters for Context Request message are, but not exclusively, listed as below:

- Old TAI;
- Old GUTI;
- SGSN Address for control plane on S3;

6.2.2.1.8.2 Context Response

The parameters for Context Response message are, but not exclusively, listed as below:

- MME Context;

6.2.2.1.8.3 Context Acknowledge

The parameters for Context Acknowledge message are FFS.

6.2.2.1.9 Attach Procedure

6.2.2.1.9.1 Identification Request

This message is sent from MME to old SGSN to request the IMSI.

The parameters for Identification Request message are, but not exclusively, listed as below:

- P-TMSI;
- Old Routeing Area Identity(RAI);
- It is FFS if P-TMSI signature is needed.

6.2.2.1.9.2 Identification Response

The parameters for Identification Response message are, but not exclusively, listed as below:

- IMSI;
- Authentication Quintets(FFS);
- Cause to indicate that the UE is not known in the old SGSN.

6.2.2.2 Candidates

6.2.2.2.1 GTP

This is the only candidate for S3.

6.2.2.3 Analysis

6.2.2.3.1 GTP

Editor's note: enhancements to the GTP protocol shall be studied in this section.

6.2.2.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.2.3 SGSN – Serving Gateway (S4) Interface

6.2.3.1 Requirements

6.2.3.1.1 E-UTRAN to UTRAN Iu Mode Inter RAT Handover Based on PS Handover Procedure

6.2.3.1.1.1 Create Bearer Request

Editor's note: Whether this message is needed is FFS.

The parameters for Create Bearer Request message are, but not exclusively, listed as below:

- Cause;
- RNC Address for user plane;
- RNC TEID for use plane;

6.2.3.1.1.2 Create Bearer Response

Editor's note: Whether this message is needed is FFS.

The parameters for Create Bearer Response message are, but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for user plane on S12;
- Serving Gateway S12 TEID for user plane;

6.2.3.1.1.3 Update Bearer Request

The parameters for Update Bearer Request message are , but not exclusively, listed as below:

- Cause;
- SGSN Address for control plane on S4;
- SGSN TEID for control plane on S4;
- NSAPI;
- RNC Address for user plane on S12 for Direct Tunnel case or SGSN Address for user plane on S4 for Non Direct Tunnel case;
- RNC TEID for user plane on S12 for Direct Tunnel case or SGSN Address for user plane on S4 for Non Direct Tunnel case;
- RAT Type;

6.2.3.1.1.4 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for control plane on S4;
- Serving Gateway TEID for control plane on S4;

6.2.3.1.2 E-UTRAN to GERAN A/Gb Mode Inter RAT Handover Based on PS Handover Procedure

6.2.3.1.2.1 Create Bearer Request

The parameters for Create Bearer Request message are FFS.

6.2.3.1.2.2 Create Bearer Response

The parameters for Create Bearer Response message are FFS.

6.2.3.1.2.3 Update Bearer Request (for preparation phase)

Editor's note: Whether this message is needed is FFS.

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Cause;
- SGSN Address for user plane on S4;
- SGSN S4 TEID for use plane;

6.2.3.1.2.4 Update Bearer Response (for preparation phase)

Editor's note: Whether this message is needed is FFS.

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for user plane on S4;
- Serving Gateway S4 TEID for user plane;

6.2.3.1.2.5 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Cause;
- SGSN Address for control plane on S4;
- SGSN S4 TEID for control plane;
- NSAPI;
- SGSN Address for user plane on S4;
- SGSN S4 TEID for user plane;
- RAT Type;

6.2.3.1.2.6 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for control plane on S4;
- Serving Gateway S4 TEID for control plane;

6.2.3.1.3 E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure

6.2.3.1.3.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- SGSN Address for user plane on S4;
- SGSN S4 TEID for user plane;
- QoS Negotiated;
- Serving Network Identity;
- RAT type;

6.2.3.1.3.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on S4;
- Serving Gateway S4 TEID for user plane;
- PDN Gateway Address for control plane on GTP-based S5/S8;
- PDN Gateway GTP-based S5/S8 TEID for control plane;

6.2.3.1.4 E-UTRAN to UTRAN Iu Mode Routing Area Update procedure

6.2.3.1.4.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- SGSN Address for user plane on S4;
- SGSN S4 TEID for user plane;
- QoS Negotiated;
- Serving Network Identity;
- RAT type;

6.2.3.1.4.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on S4;
- Serving Gateway S4 TEID for user plane;
- PDN Gateway Address for control plane on GTP-based S5/S8;
- PDN Gateway GTP-based S5/S8 TEID for control plane;

6.2.3.1.4.3 Update Bearer Request (for Direct Tunnel)

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- eNodeB Address for user plane on S1;
- eNodeB S1 TEID for user plane;

6.2.3.1.4.4 Update Bearer Response (for Direct Tunnel)

The parameters for Update Bearer Response message are FFS.

6.2.3.1.5 Attach Procedure

6.2.3.1.5.1 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- TEID(s)

6.2.3.1.5.2 Delete Bearer Response

The parameters for Delete Bearer Response message are, but not exclusively, listed as below:

- Cause;
- TEID(s).

6.2.3.2 Candidates

6.2.3.2.1 GTP

This is the only candidate for S4.

6.2.3.3 Analysis

6.2.3.3.1 GTP

Editor's note: enhancements to the GTP protocol shall be studied in this section.

6.2.3.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.2.4 Serving Gateway – PDN Gateway GTP-based S5 Interface

Editor's note: If the Serving Gateway and the PDN Gateway are combined, this interface is not needed for some function, such as bearer establishment.

6.2.4.1 Requirements

6.2.4.1.1 Attach Procedure

6.2.4.1.1.1 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.4.1.1.2 Delete Bearer Response

The parameters for Delete Bearer Response message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.4.1.1.3 Create Default Bearer Request

The parameters for Create Default Bearer Request message are, but not exclusively, listed as below:

- Serving GW Address for the user plane on GTP-based S5;
- Serving GW TEID for the user plane on GTP-based S5;
- Serving GW TEID for the control plane on GTP-based S5;
- EPS Bearer Identity;
- IMSI;
- APN;
- RAT type;
- Default Bearer QoS;
- PDN Address Allocation;
- AMBR;
- Protocol Configuration Options;
- ME Identity;
- User Location Information.

6.2.4.1.1.4 Create Default Bearer Response

The parameters for Create Default Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for the user plane on GTP-based S5;
- PDN Gateway TEID for the user plane on GTP-based S5;
- PDN Gateway TEID for the control plane on GTP-based S5;
- PDN Address Information;
- EPS Bearer Identity;
- Protocol Configuration Options.

6.2.4.1.2 Dedicated Bearer Activation Procedure

6.2.4.1.2.1 Create Dedicated Bearer Request

The parameters for Create Dedicated Bearer Request message are, but not exclusively, listed as below:

- Bearer QoS (the detailed description of Bearer QoS is FFS);
- Uplink TFT;
- PDN GW TEID of the user plane on GTP-based S5;
- Linked EPS Bearer Identity;
- Procedure Transaction Id.

6.2.4.1.2.2 Create Dedicated Bearer Response

The parameters for Create Dedicated Bearer Response message are, but not exclusively, listed as below:

- Serving GW TEID of the user plane on GTP-based S5;

- EPS Bearer Identity

6.2.4.1.3 PDN GW initiated Bearer Deactivation Procedure

6.2.4.1.3.1 Delete Bearer Request

The parameters for Delete Dedicated Bearer Request message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.4.1.3.2 Delete Bearer Response

The parameters for Delete Bearer Response message are but not exclusively, listed as below:

- EPS Bearer Identity;

Editor's note: Whether this parameter is needed is FFS.

6.2.4.1.4 MME Initiated Dedicated Bearer Deactivation Procedure

6.2.4.1.4.1 Request Dedicated Bearer Deactivation

The parameters for Request Dedicated Bearer Deactivation message are, but not exclusively, listed as below:

- EPS Bearer Identity;
- Procedure Transaction Id (this parameter is only needed for UE initiated procedures).

6.2.4.1.5 PDN GW Initiated Bearer Modification with Bearer QoS Update Procedure

6.2.4.1.5.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Bearer QoS (the detailed description of Bearer QoS is FFS);
- Uplink TFT;
- EPS Bearer Identity;
- Procedure Transaction Id (this parameter is only needed for UE initiated procedures).

6.2.4.1.5.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- EPS Bearer Identity.

Editor's note: Whether this parameter is needed is FFS..

6.2.4.1.6 MME Initiated Bearer Modification with Bearer QoS Update Procedure

6.2.4.1.6.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Bearer QoS (the detailed description of Bearer QoS is FFS);
- EPS Bearer Identity.

6.2.4.1.7 Dedicated Bearer Modification without Bearer QoS Update Procedure

6.2.4.1.7.1 Update Dedicated Bearer Request

The parameters for Update Dedicated Bearer Request message are, but not exclusively, listed as below:

- Uplink TFT;
- EPS Bearer Identity;
- Procedure Transaction Id.

6.2.4.1.7.2 Update Dedicated Bearer Response

The parameters for Update Dedicated Bearer Response message are, but not exclusively, listed as below:

- EPS Bearer Identity;

Editor's note: Whether this parameter is needed is FFS.

6.2.4.1.8 E-UTRAN to UTRAN Iu Mode Inter RAT Handover Based on PS Handover Procedure

6.2.4.1.8.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- RAT Type;
- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane.

6.2.4.1.8.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane.

6.2.4.1.9 Tracking Area Update Procedure with MME and Serving Gateway change

6.2.4.1.9.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane.

6.2.4.1.9.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane.

6.2.4.1.10 UTRAN Iu Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.2.4.1.10.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- RAT Type;
- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane;

6.2.4.1.10.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane;

6.2.4.1.11 Detach Procedures

6.2.4.1.11.1 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.4.1.11.2 Delete Bearer Response

The parameters for Delete Bearer Response message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.4.1.12 Inter eNodeB Handover with MME Relocation procedure

6.2.4.1.12.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane;

6.2.4.1.12.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane.

6.2.4.1.13 Inter eNodeB Handover with only Serving GW Change Procedure

6.2.4.1.13.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane.

6.2.4.1.13.2 Update Bearer Response

The parameters for Update Bearer Response message are FFS.

6.2.4.1.14 E-UTRAN to GERAN A/Gb Mode Inter RAT Handover Based on PS Handover Procedure

6.2.4.1.14.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- RAT Type;
- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane.

6.2.4.1.14.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane.

6.2.4.1.15 GERAN A/Gb Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.2.4.1.15.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- RAT Type;
- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane.

6.2.4.1.15.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane.

6.2.4.1.16 GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure

6.2.4.1.16.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane;
- RAT type;

6.2.4.1.16.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane;

6.2.4.1.17 E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure

6.2.4.1.17.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane;
- RAT type;

6.2.4.1.17.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane;

6.2.4.1.18 UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure

6.2.4.1.18.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane;
- RAT type;

6.2.4.1.18.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane;

6.2.4.1.19 E-UTRAN to UTRAN Iu Mode Routing Area Update procedure

6.2.4.1.19.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on GTP-based S5;
- Serving Gateway GTP-based S5 TEID for user plane;
- RAT type;

6.2.4.1.19.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for user plane on GTP-based S5;
- PDN Gateway GTP-based S5 TEID for user plane;

6.2.4.1.20 Handover procedure from non-3GPP access to 3GPP access

Editor's note: this section covers the requirements for handover procedures from non-3GPP access to 3GPP access.

Editor's note: The stage2 procedure is still under work on this procedure, and contents within this subclause may subject to change.

6.2.4.1.21 Handover procedure from 3GPP access to non-3GPP access

6.2.4.1.21.1 Delete Bearer Request

The parameters for Delete Bearer Request are, but not exclusively, listed as below:

- Teardown Ind;
- EPS Bearer ID.

6.2.4.1.21.2 Delete Bearer Response

The parameters for Delete Bearer Response are, but not exclusively, listed as below:

- Cause

6.2.4.1.22 UE requested bearer resource allocation procedure

6.2.4.1.22.1 Request Bearer Resource Allocation

The parameters for Request Bearer Resource Allocation message are, but not exclusively, listed as below:

- SDF QoS (the detailed description of SDF QoS is FFS);
- Uplink TFT;
- Downlink TFT;
- Linked EPS Bearer Identity;
- Procedure Transaction Identity.

6.2.4.1.22.2 Bearer Resource Allocation Response

The parameters for Bearer Resource Allocation Response message are, but not exclusively, listed as below:

- Procedure Transaction Identity
- Linked EPS Bearer Identity
- Cause

6.2.4.1.23 UE Requested Bearer Resource Release Procedure

6.2.4.1.23.1 Request Bearer Resource Release

The parameters for Request Bearer Resource Release message are, but not exclusively, listed as below:

- Uplink TFT;
- Downlink TFT;
- Procedure Transaction Id;
- Linked Bearer ID.

6.2.4.1.24 UE Requested PDN Connectivity Procedure

6.2.4.1.24.1 Create Default Bearer Request

The parameters for Create Default Bearer Request message are, but not exclusively, listed as below:

- Serving GW Address for the user plane on GTP-based S5;
- Serving GW TEID for the user plane on GTP-based S5;
- Serving GW TEID for the control plane on GTP-based S5;
- EPS Bearer Identity;
- RAT Type;
- Default Bearer QoS;
- PDN Address Allocation;
- AMBR;
- APN;
- Protocol Configuration Options;
- Single Address Bearer Flag.

6.2.4.1.24.2 Create Default Bearer Response

The parameters for Create Default Bearer Response message are, but not exclusively, listed as below:

- PDN GW Address for the user plane on GTP-based S5;
- PDN GW TEID for the user plane on GTP-based S5;
- PDN GW TEID for the control plane on GTP-based S5;
- EPS Bearer Identity;
- PDN Address Allocation;
- Protocol Configuration Options;
- Uplink TFT;

6.2.4.2 Candidates

6.2.4.2.1 GTP

This is the only candidate for GTP-based S5.

6.2.4.3 Analysis

6.2.4.3.1 GTP

Editor's note: enhancements to the GTP protocol shall be studied in this section.

6.2.4.3.1.1 Create Default Bearer Request

The Information Elements for Create Default Bearer Request message based on GTP-C protocol are listed as below:

- IMSI;

- Serving GW Address for User Plane;
- S5 TEID for User Plane;
- S5 TEID for Control Plane;
- Serving GW Address for Control Plane;
- Access Point Name;
- Quality of Service Profile for Default Bearer;
- RAT Type;
- EPS Bearer Identity;
- PDN Address Allocation;
- AMBR;
- Protocol Configuration Options;
- ME Identity;
- User Location Information;

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create Default Bearer Request message shall be sent from a Serving GW node to a PDN GW node as a part of the E-UTRAN Initial Attach procedure or UE Requested PDN Connectivity procedure.

The S5 TEID for Control Plane field specifies a downlink Tunnel Endpoint Identifier for control plane messages which is chosen by the Serving GW used on GTP-based S5 interface. The PDN GW shall include this Tunnel Endpoint Identifier in the GTP header of all downlink control plane messages which are related to the requested bearer context.

The Serving GW shall include a Serving GW address for Control Plane used on GTP-based S5 interface. The PDN GW shall store the Serving GW address and use it when sending control plane message on this GTP tunnel.

The S5 Tunnel Endpoint Identifier for user plane field specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the Serving GW used on GTP-based S5 interface. The PDN GW shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink G-PDUs which are related to the requested bearer context.

Serving GW Address for User Plane used on GTP-based S5 interface shall be included in Create Default Bearer Request message. The PDN GW shall store the Serving GW address and use it when sending downlink G-PDUs on this GTP tunnel.

The Access Point Name IE indicates the default APN for the UE which is a part of Subscription Data obtained from HSS. This default APN will be used to choose the PDN GW on which the default bearer will be established.

The Quality of Service Profile for Default Bearer information element should be included in Create Default Bearer Request message which is a part of Subscription Data obtained from HSS and relayed by MME to Serving GW.

Editor's notes: It is FFS what parameters are included in the Quality of Service Profile for default bearer IE.

The Serving GW shall include RAT Type IE in Create Default Bearer Request message if the MME transfers the IE to the Serving GW.

IMSI information element together with EPS Bearer Identity information element uniquely identifies the bearer context to be created.

The Serving GW shall include PDN Address Allocation information element in Create Default Bearer Request message. The PDN GW will choose the proper PDN address allocation mechanism according this IE.

The Serving GW shall include AMBR information element in Create Default Bearer Request message which is a part of Subscription Data obtained from HSS.

The Protocol Configuration Options (PCO) information element may be included in Create Default Bearer Request message when UE provides the PDG GW with some application specific parameters. If there is a Protocol Configuration Options IE in the Create Default Bearer Request message sent from MME, Serving GW shall includes PCO IE in Create Default Bearer Request message sent to PDN GW. Serving GW shall copy the content of this IE transparently from the PCO IE in the Create Default Bearer Request message sent from MME.

The ME Identity information element and User Location Information may be included in Create Default Bearer Request message if they are available.

6.2.4.3.1.2 Create Default Bearer Response

The Information Elements for Create Default Bearer Response message based on GTP-C protocol are listed as below:

- Cause;
- PDN Gateway Address for User Plane;
- S5 TEID for User Plane;
- S5 TEID for Control Plane;
- PDN Gateway Address for Control Plane
- PDN Address Information;
- EPS Bearer Identity:
- Protocol Configuration Options;

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create Default Bearer Response shall be sent from a PDN GW node to a Serving GW node as a response of a Create Default Bearer Request.

The PDN GW shall include Cause IE in the message. The parameter indicates if a Bearer context has been created in the PDN GW or not.

The S5 Tunnel Endpoint Identifier for Control Plane field specifies an uplink Tunnel Endpoint Identifier for control plane messages, which is chosen by the PDN GW used on GTP-based S5 interface. The Serving GW shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent uplink control plane messages which are related to the requested bearer context.

The S5 Tunnel Endpoint Identifier for user plane field specifies an uplink Tunnel Endpoint Identifier for G-PDUs that is chosen by the PDN GW used on GTP-based S5 interface. The Serving GW shall include this Tunnel Endpoint Identifier in the GTP header of all uplink G-PDUs which are related to the requested bearer context.

PDN GW Address for User Plane used on GTP-based S5 interface shall be included in Create Default Bearer Response message. The Serving GW shall store the PDN GW address and use it when sending uplink G-PDUs on this GTP tunnel.

PDN GW Address for Control Plane used on GTP-based S5 interface may be included in Create Default Bearer Response message. The Serving GW shall store the PDN GW address and use it when sending subsequent control plane message on this GTP tunnel.

Editor's note: It is FFS whether an IPv4/IPv6 capable PDN GW should include both IPv4 and IPv6 addresses for control plane and user plane in this message if IPv6 is also supported by the Serving GW.

If the UE requests dynamic PDP address(es) and an IPv4 and/or an IPv6 prefix dynamic PDP address(es) is/are allowed, then the PDN Address Information IE shall be included to contain the dynamic PDP Address(es) allocated by the PDN GW.

Editor's notes: It is FFS whether static PDN address for UE will be supported in EPS.

The network does not support PPP bearer type in this version of the specification. Pre-Release 8 PPP functionality of a GGSN may be implemented in the PDN GW.

The EPS Bearer Identity information element is optional, and the PDN GW may include the EPS Bearer Identity received from the Serving GW in the Create Default Bearer Request message, in order to facilitate error handling in Serving GW.

NOTE: If a Serving GW receives a Create Default Bearer Response with an EPS Bearer Identity IE included for which there is no corresponding outstanding request, the Serving GW may send a Delete Bearer Request towards the PDN GW that sent the Create Default Bearer Response with the EPS Bearer Identity included.

The Protocol Configuration Options (PCO) information element may be included in Create Default Bearer Response message when PDN GW provides the UE with some application specific parameters.

6.2.4.3.1.3 Create Dedicated Bearer Request

The Information Elements for Create Dedicated Bearer Request message based on GTP-C protocol are listed as below:

- S5 TEID for User Plane;
- Bearer QoS;
- Linked EPS Bearer Identity;
- Uplink TFT;
- Procedure Transaction Id.

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create Dedicated Bearer Request shall be sent from a PDN GW node to a Serving GW node as a part of the Dedicated Bearer Activation procedure.

The S5 Tunnel Endpoint Identifier for User Plane specifies an uplink Tunnel Endpoint Identifier for G-PDUs which is chosen by the PDN GW used on GTP-based S5 interface. The Serving GW shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent uplink G-PDUs which are related to the requested bearer context.

The Bearer QoS IE which specifies the QoS for the dedicated bearer to be activated shall be included.

Editor's notes: It is FFS what parameters are included in the Bearer QoS IE.

The Uplink TFT which specifies the uplink TFT for the dedicated bearer to be activated shall be included.

Linked EPS Bearer Identity shall be included in the Create Dedicated Bearer Request. This IE is the EPS bearer identity for the default bearer of that APN.

If the procedure is triggered by a UE Requested Bearer Resource Allocation procedure, the Procedure Transaction Id (PTI) ID which is allocated by the UE shall be included in the Create Dedicated Bearer Request.

6.2.4.3.1.4 Create Dedicated Bearer Response

The Information Elements for Create Dedicated Bearer Response message based on GTP-C protocol are listed as below:

- Cause;
- S5 TEID for User Plane;
- EPS Bearer Identity.

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create Dedicated Bearer Response shall be sent from a Serving GW node to a PDN GW node as a response of a Create Dedicated Bearer Request.

Cause IE shall be included in the message. The parameter indicates whether success or not the Serving GW handles Create Dedicated Bearer Request message and the failure cause.

The S5 Tunnel Endpoint Identifier for User Plane shall be included in the Create Dedicated Bearer Response. This IE specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the Serving GW used on GTP-based S5 interface. The PDN GW shall include this Tunnel Endpoint Identifier in the GTP header of all downlink G-PDUs which are related to the requested bearer context.

The EPS Bearer Identity information element together with the Tunnel Endpoint Identifier in the GTP header uniquely identifies a bearer context in the PDN GW.

6.2.4.3.1.5 Update Bearer Request

The Information Elements for Update Bearer Request message based on GTP-C protocol are listed as below:

- Serving GW Address for User Plane;
- Serving GW S5 TEID(S) for User Plane;
- RAT Type;
- Bearer QoS;
- EPS Bearer Identity;
- Uplink TFT;
- Procedure Transaction Id.

Editor's notes: It is FFS whether there is more Information Element for this message.

An Update Bearer Request shall be sent from a Serving GW node to a PDN GW node as a part of the Tracking Area Update procedure with MME and Serving Gateway change procedure or UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure or E-UTRAN to UTRAN Iu Mode Routing Area Update procedure or GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure or E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure or MME Initiated Bearer Modification with Bearer QoS Update procedure or Inter eNodeB Handover with only Serving GW Change procedure or E-UTRAN to UTRAN Iu mode Inter RAT handover based on PS handover procedure or UTRAN Iu mode to E-UTRAN Inter RAT handover based on PS handover procedure or E-UTRAN to GERAN A/Gb mode Inter RAT handover based on PS handover procedure or GERAN A/Gb mode to E-UTRAN Inter RAT handover based on PS handover procedure. In the Inter eNodeB Handover with MME Relocation procedure, if the Serving GW is relocated, the new Serving GW node shall send a Create Default Bearer Request to the PDN GW node.

An Update Bearer Request shall be sent from a PDN GW node to a Serving GW node as a part of the PDN GW Initiated Bearer Modification with Bearer QoS Update procedure.

If the Serving GW is relocated, the Serving GW S5 Tunnel Endpoint Identifier(S) for User Plane will be included. This IE specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the Serving GW used on GTP-based S5 interface. The PDN GW shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink G-PDUs which are related to the requested bearer context.

If the Serving GW is relocated, Serving GW Address for User Plane used on GTP-based S5 interface shall be included in Update Bearer Request message. The PDN GW shall store the Serving GW address and use it when sending downlink G-PDUs on this GTP tunnel.

For the procedures in which the RAT type is changed, the RAT Type IE shall be included in the Update Bearer Request message.

In the MME Initiated Bearer Modification with Bearer QoS Update procedure or the PDN GW Initiated Bearer Modification with Bearer QoS Update procedure, the Bearer QoS which specifies the updated QoS for the bearer shall be included.

Editor's notes: It is FFS what parameters are included in the Bearer QoS IE.

In PDN GW Initiated Bearer Modification with Bearer QoS Update procedure, if the uplink TFT for the EPS bearer is updated, the Uplink TFT which specifies the updated uplink TFT for the EPS bearer shall be included

The EPS Bearer Identity information element together with the Tunnel Endpoint Identifier in the GTP header uniquely identifies a bearer context in the PDN GW or Serving GW.

If the procedure is triggered by a UE Requested Bearer Resource Allocation procedure, the Procedure Transaction Id (PTI) ID which is allocated by the UE shall be included in the Update Bearer Request.

6.2.4.3.1.6 Update Bearer Response

The Information Elements for Update Bearer Response message based on GTP-C protocol are listed as below:

- Cause;
- PDN Gateway Address for User Plane;
- PDN Gateway S5 TEID(S) for User Plane;
- EPS Bearer Identity.

Editor's notes: It is FFS whether there is more Information Element for this message.

Except in the MME Initiated Bearer Modification with Bearer QoS Update procedure, an Update Bearer Response shall be sent from a PDN GW node to a Serving GW node or from a Serving GW node to a PDN GW node as a response of an Update Bearer Request.

Cause IE shall be included in the message. The parameter indicates whether success or not the PDN GW or the Serving GW handles Update Bearer Request message and the failure cause.

If the Serving GW Address for User Plane and the Serving GW S5 TEID(S) for User Plane is received in the Update Bearer Request and the Cause IE indicates the value of success, the PDN Gateway S5 Tunnel Endpoint Identifier(S) for User Plane shall be included in the Update Bearer Response. This IE specifies an uplink Tunnel Endpoint Identifier for G-PDUs which is chosen by the PDN GW used on GTP-based S5 interface. The Serving GW shall include this Tunnel Endpoint Identifier in the GTP header of all uplink G-PDUs which are related to the requested bearer context.

If the Serving GW Address for User Plane and the Serving GW S5 TEID(S) for User Plane is received in the Update Bearer Request and the Cause IE indicates the value of success, the PDN GW Address for User Plane used on GTP-based S5 interface shall be included in Create Default Bearer Response message. The Serving GW shall store the PDN GW address and use it when sending uplink G-PDUs on this GTP tunnel.

The EPS Bearer Identity information element is optional. The PDN GW or the Serving GW may include the EPS Bearer Identity received from the Update Bearer Request message, in order to facilitate error handling in Serving GW.

Editor's notes: If a Serving GW or a PDN GW receives an Update Bearer Response with an EPS Bearer Identity IE included for which there is no corresponding outstanding request, it is FFS what the Serving GW or the PDN GW will do.

6.2.4.3.1.7 Update Dedicated Bearer Request

The Information Elements for Update Dedicated Bearer Request message based on GTP-C protocol are listed as below:

- EPS Bearer Identity;
- Uplink TFT;
- Procedure Transaction Id.

Editor's notes: It is FFS whether there is more Information Element for this message.

An Update Dedicated Bearer Request shall be sent from a PDN GW node to a Serving GW node as a part of the Dedicated Bearer Modification without Bearer QoS Updated procedure.

The Uplink TFT which specifies the uplink TFT for the dedicated bearer to be activated shall be included.

The EPS Bearer Identity information element together with the Tunnel Endpoint Identifier in the GTP header uniquely identifies a bearer context in the Serving GW.

If the procedure is triggered by a UE Requested Bearer Resource Allocation procedure, the Procedure Transaction Id (PTI) ID which is allocated by the UE shall be included in the Update Dedicated Bearer Request.

6.2.4.3.1.8 Update Dedicated Bearer Response

The Information Elements for Update Dedicated Bearer Response message based on GTP-C protocol are listed as below:

- Cause;
- EPS Bearer Identity.

Editor's notes: It is FFS whether there is more Information Element for this message.

An Update Dedicated Bearer Response shall be sent from a Serving GW node to a PDN GW node as a response of a Update Dedicated Bearer Request.

Cause IE shall be included in the message. The parameter indicates whether success or not the Serving GW handles Update Dedicated Bearer Request message and the failure cause.

The EPS Bearer Identity information element is optional, and the Serving GW may include the EPS Bearer Identity received from the Serving GW in the Update Dedicated Bearer Request message, in order to facilitate error handling in PDN GW.

NOTE: If a PDN GW receives an Update Dedicated Bearer Response with an EPS Bearer Identity IE included for which there is no corresponding outstanding request, the PDN GW may send a Delete Bearer Request towards the Serving GW that sent the Update Dedicated Bearer Response with the EPS Bearer Identity included.

6.2.4.3.1.9 Request Bearer Resource Allocation

The Information Elements for Request Bearer Resource Allocation message based on GTP-C protocol are listed as below:

- SDF QoS;
- Uplink TFT;
- Downlink TFT;
- Linked EPS Bearer Identity;
- Procedure Transaction Id.

Editor's notes: It is FFS whether there is more Information Element for this message.

A Request Bearer Resource Allocation shall be sent from a Serving GW node to a PDN GW node as a part of the UE Requested Bearer Resource Allocation procedure.

The SDF QoS IE which is used to describe the QoS for a service data flow shall be included in the Request Bearer Resource Allocation.

Editor's notes: It is FFS what parameters are included in the SDF QoS IE.

The Uplink TFT IE and Downlink TFT IE identifying a service data flow in the PDN GW shall be included in the Request Bearer Resource Allocation.

Linked EPS Bearer Identity shall be included in the Request Bearer Resource Allocation. This IE is the EPS bearer identity for the default bearer of that APN.

The Procedure Transaction Id which is allocated by the UE shall be included in the Request Bearer Resource Allocation.

6.2.4.3.1.10 Request Bearer Resource Release

The Information Elements for Request Bearer Resource Release message based on GTP-C protocol are listed as below:

- Uplink TFT;
- Downlink TFT;

- Linked EPS Bearer Identity;
- Procedure Transaction Id.

Editor's notes: It is FFS whether there is more Information Element for this message.

Editor's notes: It is FFS whether Uplink TFT and Downlink TFT are both needed to update the bearer TFT.

A Request Bearer Resource Release shall be sent from a Serving GW node to a PDN GW node as a part of the UE Requested Bearer Resource Release procedure.

The Uplink TFT IE and Downlink TFT IE identifying a service data flow in the PDN GW shall be included in the Request Bearer Resource Release.

Editor's notes: It is FFS whether Uplink TFT and Downlink TFT are both needed to update the bearer TFT.

Linked EPS Bearer Identity shall be included in the Request Bearer Resource Release. This IE is the EPS bearer identity for the default bearer of that APN.

The Procedure Transaction Id which is allocated by the UE shall be included in the Request Bearer Resource Release.

6.2.4.3.1.11 Request Dedicated Bearer Deactivation

The Information Elements for Request Dedicated Bearer Deactivation message based on GTP-C protocol are listed as below:

- EPS Bearer Identity;

Editor's notes: It is FFS whether there is more Information Element for this message.

A Request Dedicated Bearer Deactivation shall be sent from a Serving GW node to a PDN GW node as a part of the MME Initiated Dedicated Bearer Deactivation procedure.

The EPS Bearer Identity information element together with the Tunnel Endpoint Identifier in the GTP header uniquely identifies a bearer context in the PDN GW.

6.2.4.3.1.12 Delete Bearer Request

The Information Elements for Delete Bearer Request message based on GTP-C protocol are listed as below:

- Teardown Ind;
- EPS Bearer Identity;

Editor's notes: It is FFS whether there is more Information Element for this message.

If there are active bearer contexts in MME for a particular UE at E-UTRAN Initial Attach procedure, the MME deletes all these bearer contexts by sending Delete Bearer Request messages to the Serving GW involved. The Serving GW sends Delete Bearer Request message to the PDN GW involved. At Detach procedures, the Serving GW shall send Delete Bearer Request message to the PDN GW involved to delete all the bearer contexts for a UE. At PDN GW Initiated Bearer Deactivation procedure, PDN GW shall send Delete Bearer Request message to the Serving GW involved to delete an EPS bearer for a UE.

If handovers without optimization occurs from 3GPP to non-3GPP, the PDN GW sends Delete Bearer Request message to the Serving GW involved to delete all bearers with the PDN address.

The Teardown Ind IE is used to indicate whether all bearer contexts that share the PDN address with the bearer context identified in the request should also be deleted. If the Teardown Ind information element value is set to '1', then all Bearer contexts that share the same PDN address with the bearer context identified by the EPS Bearer Identity included in the Delete bearer Context Request Message shall be torn down. Otherwise, only the bearer context identified by the EPS Bearer Identity included in the Delete bearer context Request shall be deleted if the value of this information element is '0' or this information is not included.

The EPS bearer Identity IE shall be included in Delete Bearer Request message to identify the bearer to be deleted.

6.2.4.3.1.13 Delete Bearer Response

The Information Elements for Delete Bearer Response message based on GTP-C protocol are listed as below:

- Cause;

A Delete Bearer Response message shall be sent from a PDN GW node to a Serving GW node or from a Serving GW node to a PDN GW node as a response of a Delete Bearer Request.

Cause parameter should be included in the message. The parameter indicates whether success or not the PDN GW handles Delete Bearer Request message from the Serving GW and failure cause.

The message shall also be sent from a Serving GW node to a PDN GW node as a response of a Delete Bearer Request.

Cause parameter should be included in the message. The parameter indicates whether success or not the Serving GW handles Delete Bearer Request message from the PDN GW and failure cause.

6.2.4.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.2.5 MME – HSS (S6a) Interface

6.2.5.1 Requirements

6.2.5.1.1 General

The following list of requirements applies to the S6a interface:

- generation and provision of user authentication, integrity and ciphering data;
- maintain and provide subscription profile (including updates);
- apply roaming restrictions;
- apply network access control;
- update user location information at inter-access level (serving MME, serving SGSN);
- supply a selected PDN GW address (at inter-access mobility);
- purging of subscription profile;
- reset procedure;
- the protocol for the S6a interface shall be designed in a way that easily allows an Interworking Function (see 6.2.5) to convert the S6a protocol onto the Gr protocol (MAP) and vice versa. The requirements for the S6a procedures, messages and parameters are therefore equally valid for Gr procedures, messages and parameters;
- the functions to support double registration;
- the functions to support ISR.

6.2.5.1.2 Attach Procedure

6.2.5.1.2.1 Update Location

The parameters for Update Location message are, but not exclusively, listed as below:

- MME Identity;
- IMSI;
- ME identity;

- Supported RAT Types Indicator;

NOTE: The MME shall indicate support of EUTRAN. It is FFS whether a possible signalling optimization should allow co-located MME/SGSN to also indicate support of other RAT types.

- ISR Information.

6.2.5.1.2.2 Update Location Acknowledge

The parameters for Update Location Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the attach request;
- HSS number.

6.2.5.1.2.3 Cancel Location

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.2.4 Cancel Location Acknowledge

The parameters for Cancel Location Acknowledge message are, but not exclusively, listed as below:

- cause for rejection

6.2.5.1.2.5 Insert Subscriber Data

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

NOTE: Subscription Data include subscriber status, ODB data, Regional Subscription Data, CSG Information (FFS), APN-OI Replacement, Roaming Restricted in MME due to unsupported feature, Subscribed Charging Characteristics (FFS), Access Restriction Data, Enhanced GPRS Subscription Data (context id, pdp address, eps-QoS-subscribed, apn, vplmn allowed, charging characteristics(FFS), pdn-gw-address, default apn indicator)

6.2.5.1.2.6 Insert Subscriber Data Acknowledge

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the Subscription Data;
- Regional Subscription Response;
- ODB data;

6.2.5.1.2.7 Update Location Request

The parameters for Update Location Request message are, but not exclusively, listed as below:

- PDN GW address;
- APN.

6.2.5.1.2.8 Update Location Response

The parameters for Update Location Response message are FFS.

Editor's note: It is FFS whether Update Location Request/Response messages can be realize with the same protocol messages as those of the Update Location/Update Location Acknowledge messages. When it comes to mapping onto MAP Gr, existing MAP message is used.

6.2.5.1.3 Tracking Area Update Procedure with MME and Serving Gateway change

6.2.5.1.3.1 Update Location

The parameters for Update Location message are, but not exclusively, listed as below:

- MME Identity;
- IMSI;
- ME IDENTITY;
- Supported RAT Type Indicator;
- ISR Information.

6.2.5.1.3.2 Update Location Acknowledge

The parameters for Update Location Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the TAU request;
- HSS number.

6.2.5.1.3.3 Cancel Location

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.3.4 Cancel Location Acknowledge

The parameters for Cancel Location Acknowledge message are, but not exclusively, listed as below:

- cause for rejection

6.2.5.1.3.5 Insert Subscriber Data

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

6.2.5.1.3.6 Insert Subscriber Data Acknowledge

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the Subscription Data;
- Regional Subscription Response;
- ODB data.

6.2.5.1.4 Detach Procedures

6.2.5.1.4.1 Cancel Location

This message is used for HSS-initiated Detach procedure.

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.4.2 Cancel Location Acknowledge

This message is only used for HSS-initiated Detach procedure.

The parameters for Cancel Location Acknowledge message are, but not exclusively, listed as below:

- cause for rejection

6.2.5.1.5 GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure

6.2.5.1.5.1 Update Location

The parameters for Update Location message are, but not exclusively, listed as below:

- MME Address;
- IMSI;
- ME IDENTITY;
- Supported RAT Type Indicator;
- ISR Information.

6.2.5.1.5.2 Update Location Acknowledge

The parameters for Update Location Acknowledge message are, but not exclusively, listed as below:

- Cause;
- HSS number.

6.2.5.1.5.3 Cancel Location

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.5.4 Cancel Location Acknowledge

The parameters for Cancel Location Acknowledge message are, but not exclusively, listed as below:

- cause for rejection

6.2.5.1.5.5 Insert Subscriber Data

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

6.2.5.1.5.6 Insert Subscriber Data Acknowledge

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the Subscription Data;
- Regional Subscription Response;

- ODB data.

6.2.5.1.6 E-UTRAN to GERAN A/Gb Mode Routing Area Update procedure

6.2.5.1.6.1 Update Location

The parameters for Update Location message are, but not exclusively, listed as below:

- MME Address;
- IMSI;
- ME IDENTITY;
- Supported RAT Type Indicator;
- ISR Information

6.2.5.1.6.2 Update Location Acknowledge

The parameters for Update Location Acknowledge message are, but not exclusively, listed as below:

- Cause;
- HSS number.

6.2.5.1.6.3 Cancel Location

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.6.4 Cancel Location Acknowledge

- cause for rejection

6.2.5.1.6.5 Insert Subscriber Data

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

6.2.5.1.6.6 Insert Subscriber Data Acknowledge

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the Subscription Data;
- Regional Subscription Response;
- ODB data.

6.2.5.1.7 UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure

6.2.5.1.7.1 Update Location

The parameters for Update Location message are, but not exclusively, listed as below:

- MME Id;
- IMSI;

- ME IDENTITY;
- Supported RAT Type Indicator;
- ISR Information.

6.2.5.1.7.2 Update Location Acknowledge

The parameters for Update Location Acknowledge message are, but not exclusively, listed as below:

- Cause;
- HSS number

6.2.5.1.7.3 Cancel Location

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.7.4 Cancel Location Acknowledge

- cause for rejection

6.2.5.1.7.5 Insert Subscriber Data

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

6.2.5.1.7.6 Insert Subscriber Data Acknowledge

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the Subscription Data;
- Regional Subscription Response;
- ODB data;

6.2.5.1.8 E-UTRAN to UTRAN Iu Mode Routing Area Update procedure

6.2.5.1.8.1 Update Location

The parameters for Update Location message are, but not exclusively, listed as below:

- MME Id;
- IMSI;
- ME IDENTITY;
- Supported RAT Type Indicator;
- ISR Information.

6.2.5.1.8.2 Update Location Acknowledge

The parameters for Update Location Acknowledge message are, but not exclusively, listed as below:

- Cause;

- HSS number.

6.2.5.1.8.3 Cancel Location

The parameters for Cancel Location message are, but not exclusively, listed as below:

- IMSI;
- Cancellation Type;

6.2.5.1.8.4 Cancel Location Acknowledge

- cause for rejection

6.2.5.1.8.5 Insert Subscriber Data

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

6.2.5.1.8.6 Insert Subscriber Data Acknowledge

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the Subscription Data;
- Regional Subscription Response;
- ODB data;

6.2.5.1.9 Subscriber Profile Update Procedure

6.2.5.1.9.1 Insert HSS User Profile

This message is sent from the HSS to the MME, whenever the HSS user profile is changed for a user in the HSS and the changes affect the HSS user profile stored in the MME.

The parameters for Insert Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

6.2.5.1.9.2 Insert HSS User Profile Acknowledge

This message is sent from the MME to the HSS to acknowledge Insert HSS User Profile message.

The parameters for Insert Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the insert request;
- Regional Subscription Response;
- ODB data;

6.2.5.1.9.3 Delete Subscriber Data

The parameters for Delete Subscriber Data message are, but not exclusively, listed as below:

- IMSI;
- Subscription Data;

NOTE: Subscription Data includes regional subscription identifier, gprs subscription withdraw, roaming restricted due to unsupported feature, CSG information withdraw (FFS), subscribed charging characteristics withdraw (FFS)

6.2.5.1.9.4 Delete Subscriber Data Acknowledge

The parameters for Delete Subscriber Data Acknowledge message are, but not exclusively, listed as below:

- Cause for reject the delete request;
- Regional Subscription Response

6.2.5.1.10 Purge Procedure

6.2.5.1.10.1 Purge MS

This message is sent from MME to HSS to indicate that a subscription profile has been purged e.g. due to long-lasting inactivity.

The parameters for the Purge MS message are, but not exclusively, listed as below:

- MME Identity;
- IMSI;

6.2.5.1.10.2 Purge MS Acknowledge

The parameters for the Purge MS Acknowledge message are, but not exclusively, listed as below:

- Freeze S-TMSI indicator;

6.2.5.1.10.3 Detailed Procedure

An MME may purge the subscriber data for an MS which has not established radio contact for a period determined by the network operator. Purging means to delete the subscriber data and to release or to freeze the S-TMSI that has been allocated to the purged MS. The MME shall inform the HSS of the purging.

When the HSS is informed of the purging, it shall check whether the stored MME address matches the MME Identity received in the Purge MS message. If so, the Freeze S-TMSI indicator is set in the Purge MS Acknowledge message sent to the MME and the IMSI record stored in the HSS is marked "MS purged in MME".

When MME receives the Purge MS Acknowledgement message, it shall check the Freeze S-TMSI indicator. If set the MME shall not release the S-TMSI but freeze it for a period determined by the network operator in order to avoid one TMSI being allocated to two MSs. Otherwise the S-TMSI shall be released.

In the HSS, the "MS purged in MME" flag is reset by the location updating procedure and after reload of data from the non-volatile back-up that is performed when the HSS restarts after a failure.

The HSS shall not send Insert Subscriber Data messages or Cancel Location messages to the MME for subscribers whose IMSI record is marked "MS purged in MME".

The MME shall release a frozen S-TMSI when an Identification Request message that contains the S-TMSI is received via S10.

When a purged MS attaches to the MME, the MME shall release the frozen S-TMSI and re-allocate it to the attaching MS. The MME shall initiate an Update Location procedure towards the HSS in order to retrieve the subscriber data and to reset the "MS purged in MME" flag set in the HSS.

Editor's note: should decide whether S-TMSI or GUTI to be used for purge procedure.

6.2.5.1.11 Reset Procedure

6.2.5.1.11.1 Reset

This message is sent from HSS to the MME to indicate that mobility data have been lost in the HSS e.g. due to a restart.

The parameters for the Reset message are, but not exclusively, listed as below:

- HSS Identity;
- HSS Id List.

6.2.5.1.11.2 Detailed procedure

The HSS stores and maintains in non-volatile memory addresses of MMEs and counters counting how many of its subscribers are attached to a specific MME. A counter in increased when an Update Location message is received (unless no MME address is stored against the subscriber's profile) and decreased when a Cancel Location message is sent or a Purge MS message is received. When a counter reaches a value of 0 the associated MME address and the counter may be deleted. When an Update Location Message is received from an MME for which no counter is yet maintained, the MME address is stored and an associated counter is creadted with a value set to 1.

When the HSS recovers from a restart it may have lost the information which subscriber is attached to which MME. Subsequent modification of the subscriber profile cannot be propagated to the MME immediately. The HSS shall send Reset messages to all MMEs for which addresses are stored with the associated couter values >0.

When receiving the Reset message the MME shall mark all subscription profiles which have been received from the HSS that sent the message as "not confirmed by HSS".

Before the MME reads data from a subscriber's profile it shall check the flag "not confirmed by HSS". If set, the MME shall performs Update Location towards the HSS which triggers download of the up to date service profile (which is then unmarked "not confirmed by HSS" in the MME). As a result of the Update Location Procedure the HSS stores the up-to date MME address against the subscriber's profile.

6.2.5.1.12 Authentication Information Retrieval Procedure

6.2.5.1.12.1 Send Authentication Info

This message is sent from MME to HSS to request authentication information. For details see 3GPP TR 33.821.

The parameters for the Send Authentication Info message are, but not exclusively, listed as below:

- IMSI;
- requesting PLMN-Id
- requesting Node Type
- Radio Access Technology

6.2.5.1.12.2 Send Authentication Info Acknowledge

The parameters for the Send Authentication Info Acknowledge message are, but not exclusively, listed as below:

- EPC AV (RAND, AUTN, XRES, KASME);

6.2.5.1.13 UE Requested PDN Connectivity Procedure

6.2.5.1.13.1 Update Location Request

The parameters for Update Location Request message are, but not exclusively, listed as below:

- PDN GW Address;
- APN.

6.2.5.1.13.2 Update Location Response

The parameters for Update Location Response message are FFS.

6.2.5.2 Candidates

6.2.5.2.1 Diameter

Diameter is a candidate protocol for S6a.

6.2.5.2.2 MAP

MAP is a candidate protocol for S6a.

6.2.5.3 Analysis

6.2.5.3.1 Diameter

Diameter was chosen in past 3GPP specifications as the most optimal protocol to transfer subscription and authentication data for authenticating/authorizing users accessing 3GPP networks and has since then been driven and improved to meet 3GPP requirements and development.

Basing S6a on Diameter will allow for efficient resource usage since the HSS currently makes use of the Diameter Base protocol over a number of reference points (Wx, Cx, Sh, Zh).

The Diameter protocol provides the following advantages:

- Reliable transport protocols (both TCP and SCTP are supported).
- Capability negotiation (includes selection of transport protocol).
- Security, based on IPsec and/or TLS
- Reliability and scalability.
- Connection and session management; Error notification.
- Easily extended with new commands and AVPs.
- Addressing and Routing is DNS based
- Less protocol layers, lighter processing.

The above advantages are already available over several reference points supported by the HSS: Wx, Cx, Sh, Zh. Hence, it only seems natural to continue in this same direction already taken by 3GPP by selecting Diameter for all new HSS-reference points related to an All-IP network scenario such as is the case of the S6a interface. Selection of heavier SS7-based addressing used by MAP with complex GTT configuration (compared to DNS) would result in network cost increase and not make use of Diameter's advantages listed above. SS7-based protocols should be avoided in all-IP networks in Release 8.

Given that pre-Release-8 HSS servers already support Diameter, the impact of supporting Diameter in the HSS can be considered null. If the Diameter Application chosen for the S6a reference point is based on Wx (or Cx) then implementation impacts can be considered small and deployment times reduced. The preferred Diameter Application for the S6a ref point is FFS.

The impact of supporting Diameter in the MME can also be considered null since the MME is a new Evolved Packet Core entity in Release 8.

The Diameter protocol is used over the Wd reference point between the AAA-proxy and the Home-AAA server in the I-WLAN roaming architecture. Despite this fact, it seems convenient to analyse specific issues concerning S6a roaming, i.e. MME in the VPLMN and the HSS in the HPLMN domain.

Diameter may run over SCTP or TCP at transport level. The case may be that SCTP connectivity is not available between all home and visited operator domains, in which case TCP can be used. It should be noted here that SCTP is

strongly recommended due to its advantages over TCP such as SCTP's support for multi-streaming (avoiding TCP's head-of-line blocking problems), multi-homing (which allows data to be automatically sent to alternate addresses when failures occur, and most importantly, without the application even knowing a lower level failure occurred) and its message orientation (vs. TCP being byte-oriented). The lack of SCTP support should not be considered a show-stopper to supporting Diameter over S6a.

Assuring S6a security with Diameter across operator boundaries is possible with IPsec which is required by the Diameter base protocol specification [18]. It is also possible to apply TLS instead of IPsec. In either case it is assumed that all Diameter nodes are trusted.

Establishing a hierarchy of Diameter relay agents between the MME in a VPLMN and a HSS in a HPLMN allows for efficient resource usage and deployment. It reduces the number of peers each Diameter node has to interact with, which provides the following benefits:

- Lighter peer tables, which requires fewer resources and are easier to maintain.
- Lower number of resources dedicated in each Diameter node to maintaining connections. This includes the resources needed in order to provide sufficient security to the connections.
- Higher chances that the established connections are used often, thus reducing the overhead associated to the creation and tear down of connections.

Moreover, routing tables are also minimized (which implies less resources needed and easier maintenance), and an efficient route from the Diameter client (i.e. the MME) to the appropriate Diameter server (i.e. the HSS) can always be found.

6.2.5.3.2 MAP

In networks that do not support IMS, the functionality of the HSS is basically restricted to the functionality of an HLR. In early deployments of SAE Diameter capable HSSs may not be available. MAP, however is supported in HLRs and may be easily enhanced to cover SAE's S6a requirements.

MAP over IP is also available to avoid SS7 links to terminate at the MME, and IP-transport is the only option for S6a.

Basing S6a on MAP will allow for early deployment especially in networks that do not need full HSS support, since the HLR currently makes use of the MAP protocol over a number of reference points (Gr, C, D, Gc, Lh,...)

Basing S6a on MAP will also allow combined MME/SGSN entities to efficiently communicate with the HSS (HLR) using a single dialogue.

Although the HLR is an integrated part of the HSS from the standards point of view it must be noted that in some deployment scenarios the HLR is a separated entity.

6.2.5.3.3 Comparison

The following table compares the two candidates with regard to relevant aspects:

Table 6.2.5.3.3.1: "Comparison Diameter vs. MAP"

aspect	Diameter	MAP	comment
availability in HSS	Diameter may already be available in the HSS on various optional interfaces and will be used on SWx	MAP is already available in the HSS on various mandatory interfaces	SA2 confirmed that a pre Rel-8 HSS without Diameter based interface exists (so called stand alone HLR).
availability in MME		MAP may be available if MME implementations are based on SGSN implementations or combined MME/SGSNs are deployed	.

protocol specification and implementation	A new Diameter application is required. Re-use of existing command codes and AVP codes used in other applications is ffs.	Some operations (Reset, PurgeMS, CancelLocation) can be re-used without any modification. Other operations need to be extended with extension mechanisms already available.	
interworking with earlier releases	An IWF has to convert Diameter S6a application to MAP Gr and vice versa. In order to make S6a convertable to Gr, dialogue structure and message content of the S6a Diameter application needs to be tightly aligned with Gr.	MAP has in-built inter-release interoperability. An IWF is not needed at all.	Conversion of the security parameters and subscriber data is ffs
lower layer	Diameter runs over IP. SS7 addressing is not needed	MAP runs over IP and over MTP. Signaling gateways performing the conversion are available.	Stand alone HLRs that do not support IP can use existing MTP layer for EPC functionality if MAP is chosen for S6a. In this case a signalling gateway is required. If MAP is chosen for S6a SS7 infrastructure needs to be maintained within the EPC for this purpose.
combined MME/SGSN	A combined MME/SGSN entity needs to run two protocols for one purpose: Diameter on S6a and MAP on Gr.	A combined MME/SGSN entity runs MAP on S6a and on Gr. E.g. a single MAP dialogue could download SAE subscription data and GPRS subscription data.	
Future evolution towards DIAMETER only HSS	supports "DIAMETER only" HSS even for EPC only networks.		SA2's long term vision is to have a "DIAMETER only HSS". Backward compatibility is ensured with the IWF (see C4-071515)

6.2.5.4 Conclusions

Diameter is the chosen protocol for S6a.

To address the inter-operator roaming scenario where only SS7 based roaming agreements are in place, two IWFs need to be placed in the path between MME and HSS. The chosen protocol between the two IWFs is MAP. Messages already defined for MAP Gr shall be extended to allow a one to one back and forth mapping between DIAMETER (S6a) and MAP. MAP shall also be used between IWF and a Rel-8 HSS without any Diameter supported interfaces ("stand alone Rel-8 HLR").

Editor's note: should SA3 finally decide that interworking to pre Rel-8 HSSs is needed the IWF needs to reflect this, i.e. MAP (Gr) is used between IWF and pre Rel-8 HSS. If the outcome of the IWF study deems that the IWF is not a viable solution for the scenarios, CT4 might need to revisit the decision of the protocol selection.

6.2.6 S6a – Gr Interworking Function (IWF)

6.2.6.1 General

The IWF is located between MME and Rel-8 Stand Alone HLR. It is also located between MME and pre Rel-8 HSS/HLR. Two IWFs may be located between MME and HSS.

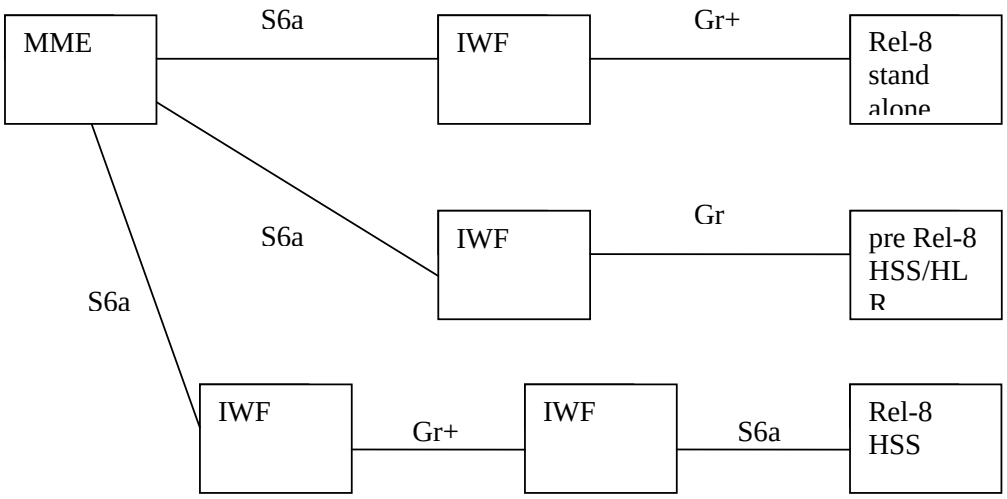

Figure 6.2.6.1.1: "S6a - Gr Interworking scenarios"

Note that some messages on the MAP based interface between IWF and Rel-8 stand alone HLR and on the MAP based interface between IWF and IWF need to be extended (Gr+) to fully meet Rel-8 EPC requirements, e.g. send EPC-Authentication vectors, send EPC-subscription data.

6.2.6.2 Requirements

The IWF shall be able to convert the following Gr/Gr+ messages to equivalent S6a messages:

MAP-CancelLocation (invoke) v3
MAP-CancelLocation (result/error) v3
MAP-Reset (invoke) v1
MAP-Reset (invoke) v2
MAP-SendParameters (result/error) v1
MAP-SendAuthenticationInfo (result/error) v2
MAP-SendAuthenticationInfo (invoke) v3
MAO-SendAuthenticationInfo (result/error) v3
MAP-InsertSubscriberData (invoke) v3
MAP-InsertSubscriberData (result/error) v3
MAP-DeleteSubscriberData (invoke) v3
MAP-DeleteSubscriberData (result/error) v3
MAP-PurgeMS (invoke) v3
MAP-PurgeMS (result/error) v3
MAP-UpdateGprsLocation (invoke) v3
MAP-UpdateGprsLocation (result/error) v3

The IWF shall be able to reject the following Gr messages:

MAP-ActivateTraceMode (invoke) v1
MAP-ActivateTraceMode (invoke) v2
MAP-ActivateTraceMode (invoke) v3
MAP-ProvideSubscriberInfo (invoke) v3

The IWF shall be able to perform MAP version negotiation for the InfoRetrievalContext (SendAuthenticationInfoV3/SendAuthenticationInfoV2/SendParametersV1).

The IWF shall be able to convert the following S6a messages to equivalent Gr/Gr+ messages:

Cancel Location Request
Cancel Location Answer
Send AuthenticationInfo Request
Send AuthenticationInfo Answer
Insert SubscriberData Request
Insert SubscriberData Answer
DeleteSubscriberData Request
Delete SubscriberData Answer
Purge MS Request
Purge MS Answer
Update Location Request
Update Location Answer
Reset Request

6.2.7 hPDN Gateway – vServing Gateway (GTP-based S8) Interface

6.2.7.1 Requirements for 3GPP accesses

The requirements for 3GPP accesses on GTP-based S8 are basically the same as those on GTP-based S5 which is described in chapter 6.2.4.1. The only difference currently can be seen is the TEID and the user plane/control plane addresses are for GTP-based S8 here instead of GTP-based S5.

6.2.7.2 Requirements for non-3GPP accesses

6.2.7.2.1 Initial Attach Procedure with S2a and Anchoring in Serving GW

6.2.7.2.1.1 Create Default Bearer Request

The parameters for Create Default Bearer Request message are, but not exclusively, listed as below:

- Serving GW Address for the user plane on GTP-based S8;
- Serving GW TEID for the user plane on GTP-based S8;
- Serving GW TEID for the control plane on GTP-based S8;
- RAT type;
- Default Bearer QoS;
- PDN Address Allocation;
- AMBR;
- Protocol Configuration Options;
- ME Identity;
- User Location Information.

6.2.7.2.1.2 Create Default Bearer Response

The parameters for Create Default Bearer Response message are, but not exclusively, listed as below:

- PDN Gateway Address for the user plane on GTP-based S8;
- PDN Gateway TEID for the user plane on GTP-based S8;

- PDN Gateway TEID for the control plane on GTP-based S8;
- PDN Address Information;
- Default Bearer QoS.

6.2.7.3 Candidates

6.2.7.3.1 GTP

This is the only candidate for GTP-based S8.

6.2.7.4 Analysis

6.2.7.4.1 GTP

The analysis for 3GPP accesses on GTP-based S8 are basically the same as those on GTP-based S5 which is described in chapter 6.2.4.3.1. The only difference currently can be seen is 1) the TEID and the user plane/control plane addresses are for GTP-based S8 here instead of GTP-based S5; 2) some messages on GTP-based S8 will also be used for some Non-3GPP related procedures.

Editor's note: The difference on applied procedures for the message will be clarified based on each message in each subsection below.

6.2.7.5 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.2.8 MME –MME (S10) Interface

6.2.8.1 Requirements

6.2.8.1.1 Attach Procedure

6.2.8.1.1.1 Identification Request

The parameters for Identification Request message are, but not exclusively, listed as below:

- Old GUTI

6.2.8.1.1.2 Identification Response

The parameters for Identification Response message are, but not exclusively, listed as below:

- IMSI;
- Authentication Quintets;
- Cause to indicate that the UE is not known in the old MME;

6.2.8.1.2 Tracking Area Update Procedure with MME and Serving Gateway change

6.2.8.1.2.1 MME Context Request

The parameters for MME Context Request message are, but not exclusively, listed as below:

- Old GUTI

6.2.8.1.2.2 MME Context Response

The parameters for MME Context Response message are, but not exclusively, listed as below:

- MME Context;
- Cause to indicate that the UE is not known in the old MME;

6.2.8.1.2.3 MME Context Acknowledge

The parameters for MME Context Acknowledge Response message are, but not exclusively, listed as below:

- reject indication;

6.2.8.1.3 Inter eNodeB Handover with MME Relocation Procedure

6.2.8.1.3.1 Forward Relocation Request

The parameters for Forward Relocation Request message are, but not exclusively, listed as below:

- MME UE Context;

6.2.8.1.3.2 Forward Relocation Response

The parameters for Forward Relocation Response message are FFS.

6.2.8.1.3.3 Forward Relocation Complete

The parameters for Forward Relocation Complete message are FFS.

6.2.8.1.3.4 Forward Relocation Complete Acknowledge

The parameters for Forward Relocation Complete Acknowledge message are FFS.

6.2.8.2 Candidates

6.2.8.2.1 GTP-C

This is the only candidate for S10.

6.2.8.3 Analysis

6.2.8.3.1 GTP-C

6.2.8.3.1.1 Identification Request

The parameters for Identification Request message are listed as below:

- Old GUTI;
- MME Address for Control Plane;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

If the UE, at E-UTRAN Initial Attach, identifies itself with GUTI and it has changed MME since detach, the new MME shall send an Identification Request message to the old MME to request the IMSI.

The new MME should include the old GUTI which is allocated to UE by the old MME.

When the old MME belongs to an MME pool, the new MME can in the general case determine the old MME. The new MME shall send the Identification Request message to an MME based on the old GUTI.

The parameter 'MME Address for Control Plane' is optional in the Identification Request message.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.2 Identification Response

The parameters for Identification Response message are listed as below:

- Cause;
- IMSI;
- Authentication Quintets;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

The old MME shall send an Identification Response to the new MME as a response to a previous Identification Request.

If an old MME within an MME pool receives an Identification Request message that contains the optional parameter MME Address for Control Plane, the old MME shall use this address as destination IP address of the Identification Response message.

The IMSI information element is mandatory if the UE is known in the old MME.

Only the Cause information element shall be included in the response if the UE is not known in the old MME.

The Authentication Quintuplet information elements may be included in the message if the UE is known in the old MME.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.3 MME Context Request

The parameters for MME Context Request message are listed as below:

- Old GUTI;
- Tunnel Endpoint Identifier Control Plane ;
- MME Address for Control Plane;
- Alternative MME Address for Control Plane;
- MME Number;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

The new MME shall send an MME Context Request to the old MME to get the MME Context for the UE.

When the old MME belongs to an MME pool, the new MME can in the general case determine the old MME. The new MME shall send the MME Context Request message to an MME based on the old GUTI.

The new MME should include the old GUTI which is allocated to UE by the old MME. The UE is identified in the old MME by its old GUTI values.

The old MME responds with an MME Context Response.

The new MME shall include a MME Address for control plane. If the new MME is IPv4/ IPv6 capable, it shall include IPv4 address in the field of MME Address for Control Plane and IPv6 address in the field of Alternative MME Address for Control Plane. If the old MME is IPv6 capable, it shall store and use the IPv6 MME address when sending control plane messages for the UE to the new MME in the MME context transfer procedure. Otherwise if the old MME is only IPv4 capable, it shall store and use the IPv4 MME address in the MME context transfer procedure. The old MME shall

store this MME Address and use it when sending control plane messages for the UE to the new MME in the MME context transfer procedure.

The new MME may include its MME number. If the old MME receives the MME number of the new MME it shall include this number when informing interworking core network nodes that there is a need to re-route previously sent requests against the new MME.

The Tunnel Endpoint Identifier Control Plane field specifies a Tunnel Endpoint Identifier for control plane messages, which is chosen by the new MME. The old MME shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent control plane messages that are sent from the old MME to the new MME and related to the Bearer context(s) requested.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.4 MME Context Response

The parameters for MME Context Response message are listed as below:

- Cause;
- IMSI;
- MM Context;
- Bearer Context;
- Tunnel Endpoint Identifier Control Plane;
- MME Address for Control Plane;
- Bearer Context Prioritization;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

The old MME shall send an MME Context Response to the new MME as a response to a previous MME Context Request.

The old MME shall include a MME Address for control plane. If the MME Context Request received from the new MME includes an IPv6 MME address, an IPv4/IPv6 capable old MME shall include IPv6 address in the field of MME address for control plane; Otherwise it shall include IPv4 address in this field. The new MME shall store this MME Address and use it when sending control plane messages for the UE to the old MME in the MME context transfer procedure.

The Tunnel Endpoint Identifier Control Plane field specifies a Tunnel Endpoint Identifier, which is chosen by the old MME. The new MME shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent control plane messages, which are sent from the new MME to the old MME and related to the Bearer context(s) requested.

The IMSI information element contains the IMSI matching the old GUTI in the MME Context Request and is mandatory if the UE is known in the old MME.

The MM Context contains necessary mobility management and security parameters.

All active Bearer contexts in the old MME shall be included as Bearer Context information elements. The Bearer contexts are included in an implementation dependant prioritized order, and the most important Bearer context is placed first. When the Bearer Context Prioritization IE is included, it informs the new MME that the Bearer contexts are sent prioritized. If the new MME is not able to maintain active all the Bearer contexts received from the old MME when it is indicated that prioritization of the Bearer contexts is applied, the new MME should use the prioritisation sent by old MME as input when deciding which Bearer contexts to maintain active and which ones to delete.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.5 MME Context Acknowledge

The parameters for MME Context Acknowledge message are listed as below:

- Cause;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

The new MME shall send an MME Context Acknowledge message to the old MME as a response to the MME Context Response message. MME Context Acknowledge indicates to the old MME that the new MME has correctly received MME Context information. This message shall not be sent if the MME Context Request was rejected.

Only the Cause information element shall be included in the acknowledgement if the new MME has not correctly received MME Context information.

The optional Private Extension contains vendor or operator specific information.

Editor's note: It is FFS whether there are more Information Elements for this message and whether date forwarding needs to be considered in TAU procedure, if the Handover procedure was not executed properly before TAU procedure occurs.

6.2.8.3.1.6 Forward Relocation Request

The parameters for Forward Relocation Request message are listed as below:

- IMSI;
- MM Context;
- Bearer Context;
- Bearer Context Prioritization;
- Direct Forwarding Flag;
- Target ID;
- S1-AP cause;
- Source to Target Transparent Container;
- Tunnel Endpoint Identifier Control Plane;
- MME Address for Control Plane;
- Selected PLMN ID;
- Private Extension;

Editor's notes: It is FFS whether there is more Information Element for this message.

The old MME shall send a Forward Relocation Request to the new MME to convey necessary information to perform the Inter eNodeB Handover procedure.

The IMSI information element contains the IMSI of the target UE for the Handover procedure.

The old MME shall include a MME Address for control plane. The new MME shall store this MME Address and use it when sending control plane messages for the UE to the old MME in the Handover procedure. If the new MME is IPv6 capable, an IPv4/IPv6 capable old MME shall include an IPv6 address in the field MME Address for Control Plane, otherwise it shall include an IPv4 address in this field.

The Tunnel Endpoint Identifier Control Plane field specifies a tunnel endpoint identifier, which is chosen by the old MME. The new MME shall include this Tunnel Endpoint Identifier Control Plane in the GTP header of all subsequent control plane messages, which are sent from the new MME to the old MME.

The MM Context contains necessary mobility management and security parameters.

All active Bearer contexts in the old MME shall be included as Bearer Context information elements. The Bearer contexts are included in an implementation dependant prioritized order, and the most important Bearer context is placed

first. When the Bearer Context Prioritization IE is included, it informs the new MME that the Bearer contexts are sent prioritized. If the new MME is not able to maintain active all the Bearer contexts received from the old MME when it is indicated that prioritization of the Bearer contexts is applied, the new MME should use the prioritisation sent by old MME as input when deciding which Bearer contexts to maintain active and which ones to delete.

Direct Forwarding Flag indicates if direct forwarding is applied from the source eNodeB to the target eNodeB, or if indirect forwarding is going to be set up by the source side.

Source to Target Transparent Container, Target Identification and S1-AP cause are information from the source eNodeB in the old MME. The old MME shall include in the Forward Relocation Request message the S1-AP Cause IE, Source to Target Transparent Container IE and Target Identification IE when this message is used for the Handover procedure.

The Selected PLMN ID IE indicates the core network operator selected for the UE in a shared network. The old MME shall include this IE if the selected PLMN identity is available.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.7 Forward Relocation Response

The parameters for Forward Relocation Response message are listed as below:

- Cause ;
- S1-AP cause;
- Tunnel Endpoint Identifier Control Plane;
- MME Address for Control Plane;
- MME Number;
- Address(es) and TEID(s) for User Traffic Data Forwarding;
- Target to Source Transparent Container;
- List of Set Up RABs;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

The new MME shall send a Forward Relocation Response to the old MME as a response to a previous Forward Relocation Request.

The Cause IE is Mandatory.

S1-AP Cause is mandatory if cause value is contained in S1-AP message.

List of Set Up RABs, Target to Source Transparent Container and S1-AP Cause are information from the target eNodeB in the new MME.

The new MME shall include a MME Address for control plane. The old MME shall store this MME Address and use it when sending control plane messages for the UE to the new MME in the Handover Procedure. If the Forward Relocation Request received from the old MME includes an IPv6 MME address, an IPv4/IPv6 capable MME shall include an IPv6 address in the field MME Address for Control Plane, otherwise, it shall include an IPv4 address in this field.

The Tunnel Endpoint Identifier Control Plane field specifies a Tunnel Endpoint Identifier that is chosen by the new MME. The old MME shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent signalling messages that are sent from the old MME to the new MME.

If 'Direct Forwarding' is applicable, then the IEs 'Address(es) and TEID(s) for Data Forwarding' contains the GTP-U tunnel endpoint parameters to the Target eNodeB. Otherwise the IEs 'Address(es) and TEID(s) for Data Forwarding' may contain the GTP-U tunnel endpoint parameters to the Serving GW (or to the Target Serving GW for S-GW re-location).

The new MME may include its MME number. If the old MME receives the MME number of the new MME it shall include this number when informing interworking core network nodes that there is a need to re-route previously sent requests against the new MME.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.8 Forward Relocation Complete

The parameters for Forward Relocation Complete message are listed as below:

- Private Extension

Editor's notes: It is FFS whether there is more Information Element for this message.

The new MME shall send a Forward Relocation Complete to the old MME to indicate that the Handover procedure has been successfully finished.

The optional Private Extension contains vendor or operator specific information.

6.2.8.3.1.9 Forward Relocation Complete Acknowledge

The parameters for Forward Relocation Complete Acknowledge message are listed as below:

- Cause;
- Private Extension.

Editor's notes: It is FFS whether there is more Information Element for this message.

The old MME sends a Forward Relocation Complete Acknowledge message to the new MME as a response to Forward Relocation Complete.

The Cause IE is mandatory.

The optional Private Extension contains vendor or operator specific information.

6.2.8.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.2.9 MME – Serving Gateway (S11) Interface

6.2.9.1 Requirements

6.2.9.1.1 Attach Procedure

6.2.9.1.1.1 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.9.1.1.2 Delete Bearer Response

The parameters for Delete Bearer Response message are FFS.

6.2.9.1.1.3 Create Default Bearer Request

The parameters for Create Default Bearer Request message are, but not exclusively, listed as below:

- IMSI;
- MME Context ID;

- EPS Bearer Identity

6.2.9.1.1.4 Create Default Bearer Response

The parameters for Create Default Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for the user plane;
- Serving Gateway TEID for the user plane;
- PDN Address for the UE;
- Serving SAE GW Context ID;
- EPS Bearer Identity

6.2.9.1.1.5 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- eNodeB address for the user plane;
- eNodeB TEID for the user plane;
- EPS Bearer Identity

6.2.9.1.1.6 Update Bearer Response

The parameters for Update Bearer Response message are FFS.

6.2.9.1.2 Dedicated Bearer Activation Procedure

6.2.9.1.2.1 Create Dedicated Bearer Request

The parameters for Create Dedicated Bearer Request message are, but not exclusively, listed as below:

- Bearer QoS (the detailed description of Bearer QoS is FFS);
- Uplink TFT;
- S1 TEID for uplink user plan;
- Linked EPS Bearer Identity

6.2.9.1.2.2 Create Dedicated Bearer Response

The parameters for Create Dedicated Bearer Response message are, but not exclusively, listed as below:

- S1 TEID for downlink user plan;
- EPS Bearer Identity

6.2.9.1.3 PDN GW initiated Bearer Deactivation Procedure

6.2.9.1.3.1 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.9.1.3.2 Delete Bearer Response

The parameters for Delete Bearer Response message are but not exclusively, listed as below:

- EPS Bearer Identity;

Editor's note: Whether this parameter is needed is FFS.

6.2.9.1.4 MME Initiated Dedicated Bearer Deactivation Procedure

6.2.9.1.4.1 Request Dedicated Bearer Deactivation

The parameters for Request Dedicated Bearer Deactivation message are, but not exclusively, listed as below:

- EPS Bearer Identity.

6.2.9.1.5 PDN GW Initiated Bearer Modification with Bearer QoS Update Procedure

6.2.9.1.5.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Bearer QoS (the detailed description of Bearer QoS is FFS);
- Uplink TFT;
- EPS Bearer Identity;
- Procedure Transaction Id (this parameter is only needed for UE initiated procedures);

6.2.9.1.5.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- EPS Bearer Identity.

Editor's note: Whether this parameter is needed is FFS.

6.2.9.1.6 MME Initiated Bearer Modification with Bearer QoS Update Procedure

6.2.9.1.6.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Bearer QoS (the detailed description of Bearer QoS is FFS);
- EPS Bearer Identity.

Editor's notes: Whether to need and how to correlate this message to corresponding downlink message is FFS.

6.2.9.1.7 MME Initiated Dedicated Bearer Deactivation

6.2.9.1.7.1 Request Dedicated Bearer Deactivation

The parameters for Request Dedicated Bearer Deactivation message are, but not exclusively, listed as below:

Editor's notes: Whether to need and how to correlate this message to corresponding downlink message is FFS.

6.2.9.1.8 Dedicated Bearer Modification without Bearer QoS Update Procedure

6.2.9.1.8.1 Update Dedicated Bearer Request

The parameters for Update Dedicated Bearer Request message are, but not exclusively, listed as below:

- Uplink TFT;
- EPS Bearer Identity

6.2.9.1.8.2 Update Dedicated Bearer Response

The parameters for Update Dedicated Bearer Response message are FFS.

6.2.9.1.9 Network Triggered Service Request Procedure

6.2.9.1.9.1 Downlink Data Notification

The parameters for Downlink Data Notification message are FFS.

6.2.9.1.10 Tracking Area Update Procedure with MME and Serving Gateway change

6.2.9.1.10.1 Create Bearer Request

The parameters for Create Bearer Request message are, but not exclusively, listed as below:

- IMSI;
- Bearer Contexts;
- MME Context ID;
- EPS Bearer Identity

6.2.9.1.10.2 Create Bearer Response

The parameters for Create Bearer Response message are, but not exclusively, listed as below:

- MME Context ID;
- Serving Gateway Address for the user plane;
- Serving Gateway TEID of the user plane;
- Serving SAE GW Context ID;
- EPS Bearer Identity

6.2.9.1.10.3 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- TEID for user plane
- EPS Bearer Identity

6.2.9.1.10.4 Delete Bearer Response

The parameters for Delete Bearer Response message are, but not exclusively, listed as below:

- TEID for user plane

6.2.9.1.11 UE Triggered Service Request Procedure

6.2.9.1.11.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- eNodeB address for the user plane;
- downlink eNodeB TEID for the user plane;

6.2.9.1.11.2 Update Bearer Response

The parameters for Update Bearer Response message are FFS.

6.2.9.1.12 UTRAN Iu Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.2.9.1. 12.1 Create Context Request

Editor's note: Whether this message is needed is FFS.

The parameters for Create Context Request message are, but not exclusively, listed as below:

- Cause;
- eNodeB Address for user plane on S1;
- eNodeB S1 TEID for user plane.

6.2.9.1.12.2 Create Context Response

Editor's note: Whether this message is needed is FFS.

The parameters for Create Context Response message are , but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for user plane on S12;
- Serving Gateway S12 TEID for user plane.

6.2.9.1.12.3 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Cause;
- MME Address for control plane on S11;
- MME S11 TEID for control plane;
- NSAPI;
- eNodeB Address for user plane on S1;
- eNodeB S1 TEID for user plane;
- RAT Type.

Editor's note: Whether MME will be aware of the type of bearer, i.e. default bearer or dedicated bearer, and how MME will identify or re-establish a bearer as default bearer of UE in UMTS/GPRS to E-UTRAN Inter RAT handover procedure, is FFS.

6.2.9.1.12.4 Update Bearer Response

The parameters for Update Bearer Response message are , but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for control plane on S11;
- Serving Gateway S1 TEID for control plane;

6.2.9.1.13 Detach Procedures

6.2.9.1.13.1 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- Teardown Ind;

- EPS Bearer ID.

6.2.9.1.13.2 Delete Bearer Response

The parameters for Delete Bearer Response message are, but not exclusively, listed as below:

- Cause;

6.2.9.1.14 Inter eNodeB Handover with MME Relocation Procedure

6.2.9.1.14.1 Create Bearer Request

The parameters for Create Bearer Request message are, but not exclusively, listed as below:

- Bearer Context;
- EPS Bearer Identity

6.2.9.1.14.2 Create Bearer Response

The parameters for Create Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on S1;
- Serving Gateway S1 TEID for user plane;
- EPS Bearer Identity

6.2.9.1.14.3 Update Bearer Request (on target side, for indirect forwarding)

Editor's note: Whether this message is needed is FFS.

The parameters for Update Bearer Request message are FFS.

6.2.9.1.14.4 Update Bearer Response (on target side, for indirect forwarding)

Editor's note: Whether this message is needed is FFS.

The parameters for Update Bearer Response message are FFS.

6.2.9.1.14.5 Update Bearer Request (on source side, for indirect forwarding)

Editor's note: Whether this message is needed is FFS.

The parameters for Update Bearer Request message are FFS.

6.2.9.1.14.6 Update Bearer Response (on source side, for indirect forwarding)

Editor's note: Whether this message is needed is FFS.

The parameters for Update Bearer Response message are FFS.

6.2.9.1.14.7 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- eNodeB Address for user plane on S1;
- eNodeB S1 TEID for user plane;
- EPS Bearer Identity.

6.2.9.1.14.8 Update Bearer Response

The parameters for Update Bearer Response message are FFS.

6.2.9.1.14.9 Delete Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- EPS Bearer Identity

6.2.9.1.14.10 Delete Bearer Response

The parameters for Delete Bearer Response message are FFS.

6.2.9.1.15 Inter eNodeB Handover without CN Node Relocation Procedure

6.2.9.1.15.1 User Plane Update Request

The parameters for User Plane Update Request message are FFS.

6.2.9.1.15.2 User Plane Update Response

The parameters for Create Bearer Response message are FFS.

6.2.9.1.16 Inter eNodeB Handover with only Serving GW Change Procedure

6.2.9.1.16.1 Create Bearer Request

The parameters for Create Bearer Request message are, but not exclusively, listed as below:

- Bearer Context;

6.2.9.1.16.2 Create Bearer Response

The parameters for Create Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for user plane on S1;
- Serving Gateway S1 TEID for user plane.

6.2.9.1.16.3 Delete Bearer Request

The parameters for Delete Bearer Request message are FFS.

6.2.9.1.16.4 Delete Bearer Request

The parameters for Delete Bearer Response message are FFS.

6.2.9.1.17 GERAN A/Gb Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.2.9.1.17.1 Create Context Request

Editor's note: Whether this message is needed is FFS.

The parameters for Create Context Request message are, but not exclusively, listed as below:

- Cause;
- eNodeB Address for user plane on S1;
- eNodeB S1 TEID for user plane.

6.2.9.1.17.2 Create Context Response

Editor's note: Whether this message is needed is FFS.

The parameters for Create Context Response message are, but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for user plane on S4;
- Serving Gateway S4 TEID for user plane.

6.2.9.1.17.3 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- Cause;
- MME Address for control plane on S11;
- MME S11 TEID for control plane;
- NSAPI;
- eNodeB Address for user plane on S1;
- eNodeB S1 TEID for user plane.
- RAT Type;

6.2.9.1.17.4 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Cause;
- Serving Gateway Address for control plane on S11;
- Serving Gateway TEID for control plane on S11.

6.2.9.1.18 S1 Release Procedure

6.2.9.1.18.1 Update Bearer Request

The parameters for Update Bearer Request message are FFS.

6.2.9.1.18.2 Update Bearer Response

The parameters for Update Bearer Response message are FFS.

6.2.9.1.19 GERAN A/Gb Mode to E-UTRAN Tracking Area Update procedure

6.2.9.1.19.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- MME Address for control plane on S11;
- MME S11 TEID for control plane;
- QoS Negotiated;
- Serving Network Identity;

6.2.9.1.19.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for control plane on S11;
- Serving Gateway TEID for control plane on S11;

- PDN Gateway Address for control plane on GTP-based S5/S8;
- PDN Gateway GTP-based S5/S8 TEID for control plane;

6.2.9.1.20 UTRAN Iu Mode to E-UTRAN Tracking Area Update procedure

6.2.9.1.20.1 Update Bearer Request

The parameters for Update Bearer Request message are, but not exclusively, listed as below:

- MME Address for control plane on S11;
- MME S11 TEID for control plane;
- QoS Negotiated;
- Serving Network Identity;

6.2.9.1.20.2 Update Bearer Response

The parameters for Update Bearer Response message are, but not exclusively, listed as below:

- Serving Gateway Address for control plane on S11;
- Serving Gateway S11 TEID for control plane;
- PDN Gateway Address for control plane on GTP-based S5/S8;
- PDN Gateway GTP-based S5/S8 TEID for control plane;

6.2.9.1.21 UE requested bearer resource allocation procedure

6.2.9.1.21.1 Bearer Resource Allocation Request

The parameters for Bearer Resource Allocation Request message are, but not exclusively, listed as below:

- Uplink TFT;
- Downlink TFT
- SDF QoS (the detailed description of SDF QoS is FFS)
- Linked EPS Bearer Identity
- Procedure Transaction Identity

6.2.9.1.21.2 Bearer Resource Allocation Response

The parameters for Response Indication message are, but not exclusively, listed as below:

- Procedure Transaction Identity
- Linked EPS Bearer Identity
- Cause

6.2.9.1.22 UE Requested Bearer Resource Release Procedure

6.2.9.1.22.1 Request Bearer Resource Release

The parameters for Request Bearer Resource Release message are, but not exclusively, listed as below:

- Uplink TFT;
- Downlink TFT;

- Procedure Transaction Id;
- Linked Bearer ID.

6.2.9.1.23 UE Requested PDN Connectivity Procedure

6.2.9.1.23.1 Create Default Bearer Request

The parameters for Create Default Bearer Request message are, but not exclusively, listed as below:

- IMSI;
- MME Context ID;
- EPS Bearer Identity;
- RAT Type;
- Default Bearer QoS;
- PDN Address Allocation;
- AMBR;
- APN;
- Protocol Configuration Options;
- Single Address Bearer Flag.

6.2.9.1.23.2 Create Default Bearer Response

The parameters for Create Default Bearer Response message are, but not exclusively, listed as below:

- Serving GW Address for the user plane on S1;
- Serving GW TEID for the user plane on S1;
- Serving GW Context ID;
- EPS Bearer Identity;
- PDN Address Information;
- Protocol Configuration Options;
- Uplink TFT.

6.2.9.1.23.3 Update Bearer Request

The parameters for Delete Bearer Request message are, but not exclusively, listed as below:

- eNodeB Address for the user plane on S1;
- eNodeB TEID for the user plane on S1;
- EPS Bearer Identity.

6.2.9.1.23.4 Update Bearer Response

The parameters for Update Bearer Response message are FFS.

6.2.9.1.24 Optimized Active Handover from E-UTRAN Access to cdma2000 HRPD Access Procedure

6.2.9.1.24.1 Create forwarding tunnels Request

The Information Elements for Create forwarding tunnels Request message are listed as below:

- PDSN Address;
- PDSN GRE Keys;

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create forwarding tunnels Request message shall be sent by MME to a SGW as a part of the MME configures resources for Indirect data forwarding.

The MME includes the PDSN data forwarding parameters in the message, which includes PDSN Address and PDSN GRE Keys. The Serving GW will forwards downlink data to the PDSN via the PDSN Address and PDSN GRE Keys when the Serving GW receives downlink data forwarded from the eNodeB.

6.2.9.1.24.2 Create forwarding tunnel Response

The Information Elements for Create forwarding tunnels Response message are listed as below:

- Serving GW Address;
- Serving GW TEID(s).

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create forwarding tunnels Response message shall be sent by a Serving GW to MME as a response to a Create forwarding tunnels Request message.

The Serving GW includes the Serving GW data forwarding parameters in the message, which includes Serving GW Address and Serving GW TEID(s). The eNodeB will forward received downlink data to the Serving GW via the Serving GW Address and Serving GW TEID(s).

6.2.9.1.25 Handover procedure from 3GPP access to non-3GPP access

6.2.9.1.25.1 Delete Bearer Request

The parameters for Delete Bearer Request are, but not exclusively, listed as below:

- Teardown Ind;
- EPS Bearer ID

6.2.9.1.25.2 Delete Bearer Response

The parameters for Delete Bearer Response are, but not exclusively, listed as below:

- Cause

6.2.9.2 Candidates

6.2.9.2.1 GTP-C

GTPv2 Control Plane is the only candidate for S11.

6.2.9.3 Analysis

6.2.9.3.1 GTP-C

6.2.9.3.1.1 Create Default Bearer Request

The Information Elements for Create Default Bearer Request message are listed as below:

- IMSI;
- EPS Bearer ID;
- MME S11 Address for Control Plane;
- MME S11 TEID for Control Plane;
- PGW GTP-based S5/S8 Address for Control Plane;
- End User Address;
- Access Point Name;
- Default QoS Profile;
- RAT Type;
- PDN Address Allocation;
- AMBR;
- EPS Bearer Identity

Editor's note: It should be clarified with SA2 if "MME Context ID" in TS 23.401 means "MME S11 TEID for Control Plane" for TS 29.803.

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create Default Bearer Request message shall be sent from a MME to a SGW as a part of the default bearer establishment procedure.

Editor's note: Current assumption is that this procedure is used for all default bearer activations.

The MME shall include IMSI IE in Create Default Bearer Request message.

Editor's note: Emergency call related matters (e.g. availability of IMSI) are FFS.

The MME shall include EPS Bearer ID IE in Create Default Bearer Request message.

The MME shall include MME S11 Address for Control Plane IE and MME S11 TEID for Control Plane IE in Create Default Bearer Request message. These IEs specify the downlink tunnel for control plane messages which is chosen by the MME. The SGW shall include this Tunnel Endpoint Identifier in the GTP header of all downlink control plane messages which are related to the requested bearer.

Editor's note: It is FFS if this tunnel will also be used for the associated dedicated bearers.

The MME shall include selected PGW GTP-based S5/S8 Address for Control Plane IE in Create Default Bearer Request message. The SGW needs this address for sending Create Default Bearer Request message to PGW.

The MME shall conditionally include End User Address IE in Create Default Bearer Request message. If the UE requests the network to allocate a dynamic address then the End User Address IE shall be empty. If the UE requests a static Address then the End User Address IE shall contain the static Address. If UE does not request neither dynamic, not static address, then MME shall not include the End User Address IE into the message.

The MME shall include APN IE in Create Default Bearer Request message, if available.

Editor's note: APN matter is till not completely clear at stage 2.

The MME shall include Default Quality of Service (QoS) Profile IE in Create Default Bearer Request message. The QoS Profile IE is included in Create Default Bearer Request message to contain the Default Bearer QoS derived from subscription data of UE. The Default bearer QoS may be upgraded or downgraded by PGW in corresponding response message. It is FFS what parameters are included in the IE.

The MME may include RAT Type IE in Create Default Bearer Request message for following RAT based charging and PCC decision.

Editor's note: IF MME is unaware of the actual RAT type, then MME either sets the RAT type value to 'unknown' or does not send the IE altogether.

The MME shall include PDN Address Allocation IE, if available in Create Default Bearer Request message. PDN Address Allocation IE contains UE's IP version capability.

The MME shall include Aggregate Maximum Bit Rate (AMBR) IE in Create Default Bearer Request message. AMBR IE is used for bearer level rate enforcement.

6.2.9.3.1.2 Create Default Bearer Response

The Information Elements for Create Default Bearer Response message based on GTP-C protocol are listed as below:

- Cause;
- SGW S11 Address for Control Plane;
- SGW S11 TEID for Control Plane;
- SGW S1-U Address for User Plane;
- SGW S1-U TEID for User Plane;
- PGW GTP-based S5/S8 Address for Control Plane;
- PGW GTP-based S5/S8 TEID for Control Plane;
- PGW GTP-based S5/S8 Address for User Plane;
- PGW GTP-based S5/S8 TEID for User Plane;
- End User Address;
- Default QoS Profile
- EPS Bearer Identity

Editor's note: It should be clarified with SA2 if "SGW Context ID" in TS 23.401 means "SGW S11 TEID for Control Plane" for TS 29.803.

Editor's note: It is FFS if AMBR and EPS Bearer ID are needed.

Editor's notes: It is FFS whether there is more Information Element for this message.

A Create Default Bearer Response shall be sent from a SGW to a MME as a response to a Create Default Bearer Request message.

The SGW shall include Cause IE in the Create Default Bearer Response message. This IE indicates if bearers context have been created in the SGW and PGW or not.

The SGW may include SGW S11 Address for Control Plane IE in Create Default Bearer Response message, if SGW decides to use different IP address for the subsequent communication. The MME shall replace the old SGW address and use the new address when sending subsequent control plane messages to this GTP-C tunnel.

The SGW shall include SGW S11 Tunnel Endpoint Identifier for Control Plane IE in Create Default Bearer Response message. The MME shall include this TEID-C in the GTP-C header of all subsequent uplink control plane messages which are related to the default bearer.

The SGW shall include SGW S1-U Address for User Plane IE and SGW S1-U Tunnel Endpoint Identifier for User Plane IE in Create Default Bearer Response message. The MME forwards these IE to eNB. The eNB uses these IE when sending uplink data to this GTP-U tunnel. The eNB shall include this TEID-U into the GTP-U header of all uplink G-PDUs which are related to the default bearer.

The SGW may include PGW GTP-based S5/S8 Address for Control Plane IE in Create Default Bearer Response message, if PGW returns different IP address to the SGW. The MME shall replace the old PGW GTP-based S5/S8 Address for Control Plane with the new value.

The SGW shall include PGW GTP-based S5/S8 Tunnel Endpoint Identifier for Control Plane IE in Create Default Bearer Response message. The MME shall store the IE.

NOTE: MME needs to forward PGW GTP-based S5/S8 Address for Control Plane IE and respective TEID-C to the new MME/SGSN during the subsequent TAU procedure.

The SGW shall include PGW GTP-based S5/S8 Address for User Plane IE and PGW GTP-based S5/S8 Tunnel Endpoint Identifier for User Plane IE in Create Default Bearer Response message.

Editor's notes: It is FFS whether an IPv4/IPv6 capable SGW should include both IPv4 and IPv6 addresses for control plane and user plane in this message.

The SGW shall include the End User Address IE, if available in Create Default Bearer Response message.

Editor's notes: It is FFS whether static PDN address for UE will be supported in EPS.

The network does not support PPP bearer type in this version of the specification. Pre-Release 8 PPP functionality of a GGSN may be implemented in the PDN GW.

The SGW shall include Default Quality of Service Profile (QoS) IE in Create Default Bearer Response message, if it was included in corresponding Create Default Bearer Response message from PGW to SGW. It is FFS what parameters are included in the IE.

The EPS Bearer ID information element is optional, and the Serving GW may include the EPS Bearer ID received from the MME in the Create Default Bearer Request message, in order to facilitate error handling in MME.

NOTE: If an MME receives a Create Default Bearer Response with an EPS Bearer ID IE included for which there is no corresponding outstanding request, an MME may send a Delete Bearer Request towards the Serving GW that sent the Create Default Bearer Response with the EPS Bearer ID included.

6.2.9.3.1.3 Create Bearer Request

- Operation indication (used to inform the S-GW whether it should continue forwarding the message to the P-GW or not);

Editor's note: The Create Bearer Request message is used during the TAU. The content of the message is FFS.

6.2.9.3.1.4 Create Bearer Response

Editor's note: The Create Bearer Response message is used during the TAU. The content of the message is FFS.

6.2.9.3.1.5 Delete Bearer Request

The Information Elements for Delete Bearer Request message are listed as below:

- Teardown Ind;
- EPS Bearer ID;
- Operation indication;

Editor's notes: It is FFS whether there is more Information Element for this message.

A Delete Bearer Request message shall be sent by MME to a SGW, or by SGW to MME as a part of the default bearer deactivation procedure.

If handovers without optimization occurs from 3GPP to non-3GPP, the PDN GW sends Delete Bearer Request message to the Serving GW involved to delete all bearers with the PDN address. The Serving GW sends Delete Bearer Request message to the MME involved to delete all bearers with the PDN address.

If there are active bearer contexts in MME for a particular UE at attach procedure, the MME deletes all these bearer contexts by sending Delete Bearer Request messages to the Serving GW involved.

The Teardown Ind is used to indicate whether all bearer contexts that share the PDN address with the bearer context identified in the request should also be deleted. If the Teardown Ind information element value is set to '1', then all Bearer contexts that share the same PDN address with the bearer context identified by the EPS Bearer ID included in the Delete bearer Context Request Message shall be torn down. Otherwise, only the bearer context identified by the EPS Bearer ID included in the Delete bearer context Request shall be deleted if the value of this information element is '0' or this information is not included.

The MME allocates the EPS bearer ID during the default or dedicated bearer establishment procedure to identify the bearer in following bearer modification and deactivation procedures.

If all bearers for a UE are deleted, the MME shall detach the UE.

A Delete Bearer Request message may include an operation indication which is used to inform S-GW whether the S-GW should continue forwarding the message to the P-GW or not when it receives this message.

Editor's note: It is FFS whether the Teardown Ind may be used to indicate that all bearers for a particular UE shall be deleted, regardless whether these bearers share the same Paddress. In EPS, only one Serving GW is used for a particular UE. Therefore, the MME may indicate the Serving GW delete all bearer contexts of a particular UE in one Delete Bearer Request message to reduce message interaction between MME and Serving GW. If so, the presence requirement of EPS bearer ID in Delete Bearer Request message should be changed from mandatory to conditional

6.2.9.3.1.6 Delete Bearer Response

The Information Elements for Delete Bearer Response message are listed as below:

- Cause

Editor's note: It is FFS whether there is more Information Element for this message.

A Delete Bearer Response message shall be sent by a SGW to MME, or by MME to SGW as a response to a Delete Bearer Request message.

The MME or the SGW shall include Cause IE in Delete Bearer Response message. The IE indicates if the peer has deleted the bearer, or not.

6.2.9.3.1.7 MME initiated Update Bearer Request

Editor's note: This subclause is confined only to the cases when a default bearer modification is executed either right after the default bearer establishment.

The Information Elements for Update Bearer Request message are listed as below:

- EPS Bearer ID;
- MME S11 Address for Control Plane;
- MME S11 TEID for Control Plane;
- eNB S1-U Address for User Plane;
- eNB S1-U TEID for User Plane;
- Operation indication.

Editor's notes: It is FFS whether there is more Information Element for this message.

An Update Bearer Request message shall be sent by MME to a SGW as a part of an attach procedure.

The MME shall include EPS Bearer ID IE in Update Bearer Request message.

The MME shall conditionally include MME S11 Address for Control Plane IE and MME S11 TEID for Control Plane IE in Update Bearer Request message. The new MME includes these IEs after the TAU procedure. The MME does not include these IE in Update Bearer Request message, which immediately follows Create Default Bearer Request / Response messages.

The MME shall include one eNB S1-U Address for User Plane IE and eNB S1-U TEID for User Plane IE pair in Update Bearer Request message.

A MME initiated Update Bearer Request message may include an operation indication which is used to inform S-GW whether the S-GW should continue forwarding the message to the P-GW or not when it receives this message.

Editor's note: The case of shared eNB is FFS.

6.2.9.3.1.8 Update Bearer Response sent to MME

Editor's note: This subclause is confined only to the cases when a default bearer modification is executed either right after the default bearer establishment.

The Information Elements for Update Bearer Request message are listed as below:

- Cause;
- EPS Bearer ID;

Editor's notes: It is FFS whether there is more Information Element for this message.

An Update Bearer Response message shall be sent by SGW to a MME as part of an attach procedure.

The SGW shall include Cause IE in Update Bearer Response message.

The SGW shall include EPS Bearer ID IE in Update Bearer Response message.

6.2.9.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.2.10 UTRAN – Serving Gateway (S12) Interface

6.2.10.1 Requirements

6.2.10.2 Candidates

6.2.10.2.1 GTP-U

This is the only candidate for S12.

6.2.10.3 Analysis

6.2.10.3.1 GTP

Editor's note: enhancements to the GTP protocol shall be studied in this section.

6.2.10.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3 Interface related to "Architecture enhancements for non-3GPP accesses"

Editor's Note: the impact on IETF based protocols may be described in certain related sections.

6.3.1 Introduction

6.3.2 Gateway – Trusted Non-3GPP IP Access (S2a) Interface

6.3.2.1 Requirements

6.3.2.1.1 Initial Attach Procedure for non-roaming with S2a and Anchoring in PDN GW

6.3.2.1.1.1 MIPv4 Registration Request (RRQ)

The parameters for MIPv4 Registration Request message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of NAI (as specified in IETF RFC 4282 [7]);
- Reverse Tunnel Request indication;
- An indication that FA mode is used;
- An indication that simultaneous binding is not used

6.3.2.1.1.2 MIPv4 Registration Reply (RRP)

The parameters for MIPv4 Registration Reply message are, but not exclusively, listed as below:

- IP address allocated for the UE;
- IP address of the HA allocated to the UE;
- A value indicating the result of the Registration Request;
- A value indicating the lifetime of the registration

6.3.2.1.1.3 Proxy Binding Update Request

The parameters for Proxy Binding Update Request message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7]);
- IP Address Request Indication;
- Access Point Name when available;

Editor's note: the Access Point Name could be conveyed in Proxy Binding Update using the Service Selection option defined in IETF draft-korhonen-mip6-service-04. Other mechanisms for conveying the Access Point Name information are FFS.

6.3.2.1.1.4 Proxy Binding Update Acknowledgement

The parameters for Proxy Binding Update Acknowledgement message are, but not exclusively, listed as below:

- IP Address(es) or Home Network Prefix Allocated for the UE based on the selected PDN;

6.3.2.1.2 Initial Attach Procedure with S2a and Anchoring in Serving GW

6.3.2.1.2.1 Proxy Binding Update Request

The parameters for Proxy Binding Update Request message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7]);

NOTE: The value of Mobile Node (MN-ID) includes IMSI.

6.3.2.1.2.2 Proxy Binding Update Acknowledgement

The parameters for Proxy Binding Update Acknowledgement message are, but not exclusively, listed as below:

- PDN Address Information;
- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7]);

NOTE: The value of Mobile Node (MN-ID) includes IMSI.

6.3.2.1.3 Detach Procedures with S2a and Anchoring in PDN GW

6.3.2.1.3.1 Proxy Binding Update

This message is used in Detach Procedures with PMIPv6.

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9]);
- Lifetime (which shall be set to zero).

6.3.2.1.3.2 Proxy Binding Acknowledgement

This message is used in Detach Procedures with PMIPv6.

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- A value indicating the result of the Proxy Binding Update

6.3.2.1.3.3 MIPv4 Registration Request

This message is only used in UE-initiated Detach Procedure with MIPv4 FACoA.

The parameters for Registration Request message are, but not exclusively, listed as below:

- Lifetime (which shall be set to zero);

6.3.2.1.3.4 MIPv4 Registration Reply

This message is only used in UE-initiated Detach Procedure with MIPv4 FACoA.

The parameters for MIPv4 Registration Reply message are, but not exclusively, listed as below:

- A value indicating the result of the Registration Request

6.3.3.1.3.5 Registration Revocation

This message is used in Network-initiated Detach Procedures with MIPv4 FACoA.

The parameters for Registration Revocation message are, but not exclusively, listed as below:

- An indication (A bit) identifying the role of the agent sending the revocation is FA;
- An indication (I bit) identifying whether the UE should be informed of the revocation;
- The HoA of the mobile node whose registration is being revoked;
- The CoA in the foreign domain to identify which binding is being revoked;
- The IP address of the home agent;
- Timestamp.

6.3.2.1.3.6 Registration Revocation Acknowledgement

This message is used in Network-initiated Detach Procedures with MIPv4 FA CoA.

The parameters for Registration Revocation Acknowledgement message are, but not exclusively, listed as below:

- An indication identifying (I bit) whether the UE should be informed of the revocation;
- The HoA of the mobile node copied from Registration Revocation message.

6.3.2.1.4 Handover procedure from 3GPP access to non-3GPP access

Editor's note: this section covers the requirements for handover procedures from 3GPP access to non-3GPP access.

Editor's note: The stage2 procedure is still under work on this procedure, and contents within this subclause may subject to change.

6.3.2.2 Candidates

The S2a interface shall support following protocols:

- Client MIPv4 Foreign Agent (FA) mode as specified in IETF RFC 3344 [4].
- Proxy MIPv6 as specified in Internet-Draft, draft-ietf-netlmm-proxymip6-00[5].

Editor's note: Whether more protocols will be selected for the S2a interface is FFS.

6.3.2.2.1 Client MIPv4 FA mode

6.3.2.2.2 Proxy MIPv6

6.3.2.3 Analysis

6.3.2.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.3 Gateway – ePDG (S2b) Interface

6.3.3.1 Requirements

6.3.3.1.1 Initial Attach Procedure with S2b and Anchoring in PDN GW

6.3.3.1.1.1 Proxy Binding Update Request

In the case of PMIPv6, the parameters for Proxy Binding Update Request message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IP Address Request Indication
- Access Point Name when available in ePDG;

Editor's note: the Access Point Name could be conveyed in Proxy Binding Update using the Service Selection option defined in IETF draft-korhonen-mip6-service-04. Other mechanisms for conveying the Access Point Name information are FFS.

6.3.3.1.1.2 Proxy Binding Update Acknowledgement

In the case of PMIPv6, the parameters for Proxy Binding Update Acknowledgement message are, but not exclusively, listed as below:

- IP Address(es) or Home Network Prefix Allocated for the UE based on the selected PDN;

6.3.3.1.2 Detach Procedure with S2b and Anchoring in PDN GW

6.3.3.1.2.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9]);
- Lifetime (which shall be set to zero).

6.3.3.1.2.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- A value indicating the result of the Proxy Binding Update

6.3.3.1.3 Handover procedure from 3GPP access to non-3GPP access

Editor's note: this section covers the requirements for handover procedures from 3GPP access to non-3GPP access.

Editor's note: The stage2 procedure is still under work on this procedure, and contents within this subclause may subject to change.

6.3.3.1.3.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IP Address Request Indication
- Access Point Name when available in ePDG;

Editor's note: the Access Point Name could be conveyed in Proxy Binding Update using the Service Selection option defined in IETF draft-korhonen-mip6-service-04. Other mechanisms for conveying the Access Point Name information are FFS.

6.3.3.1.3.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- IP Address(es) or Home Network Prefix Allocated for the UE based on the selected PDN;

6.3.3.2 Candidates

6.3.3.2.1 Proxy MIPv6

This is the only candidate for S2b.

6.3.3.3 Analysis

6.3.3.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.4 Serving Gateway – PDN Gateway (PMIP-based S5) Interface

Editor's note: If the Serving Gateway and the PDN Gateway are combined, this interface is not needed for some function, such as bearer establishment.

6.3.4.1 Requirements

6.3.4.1.1 General

Differences between PMIP-based S5 and GTP-based S5 should be minimized.

The following capabilities need to be considered for the support on the PMIP-based S5 interface.

a) Path Management

- Health check, i.e. find out whether if the opponent is alive
- Indication of the latest supported GTP version
- Indication of the supported Extension headers for GTP

Editor's note: It is FFS whether if the capabilities provided by GTP messages "Version Not Supported" used for the indication of the latest supported GTP version, and "Supported Extension Headers Notification" used for the indication of the supported Extension headers for GTP, needs to be supported on IETF based S5 Interface.

b) Tunnel Management

- Tunnel establishment
- Tunnel update at the time of Serving GW relocation
- Delete Tunnel
- Error Indication
- NW initiated tunnel setup request for terminating the packets
- NW initiated tunnel setup reject for terminating the packets
- Initial tunnel establishment

Editor's note: These lists above are not exclusive.

6.3.4.1.2 Attach Procedure

6.3.4.1.2.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name
- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

Editor's note: the Access Point Name could be conveyed in Proxy Binding Update using the Service Selection option defined in IETF draft-korhonen-mip6-service-04. Other mechanisms for conveying the Access Point Name information are FFS.

6.3.4.1.2.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix Allocated for the UE based on the selected PDN;
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options).

6.3.4.1.3 E-UTRAN to UTRAN Iu Mode Inter RAT Handover Based on PS Handover Procedure

6.3.4.1.4 Tracking Area Update Procedure with MME and Serving Gateway change

6.3.4.1.4.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])
- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name
- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.4.1.4.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix Allocated for the UE based on the selected PDN
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.4.1.5 UTRAN Iu Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

Editor's note: The stage2 procedure is still under work on this procedure, and contents within this subclause may subject to change.

6.3.4.1.6 Handover procedure from non-3GPP access to 3GPP access

6.3.4.1.6.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name
- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.4.1.6.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix allocated for the UE based on the selected PDN
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.4.1.7 Inter eNodeB Handover with MME Relocation procedure

6.3.4.1.7.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])
- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name
- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.4.1.7.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix Allocated for the UE based on the selected PDN
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.4.1.8 Detach procedure

6.3.4.1.8.1 Proxy Binding Update

The lifetime field of the Proxy Binding Update message is set to zero. The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix allocated to the UE based on the selected PDN
- Access Point Name
- Lifetime, set to zero
- Access Technology Type, set to 3GPP

6.3.4.1.8.2 Proxy Binding Acknowledgement

The lifetime field of the Proxy Binding Update message is set to zero. The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix allocated to the UE based on the selected PDN

- Lifetime, set to zero
- Access Technology Type, set to 3GPP

Editor's Note: It is FFS whether MIPv6 binding revocation (see IETF draft, draft-muhanna-mip6-binding-revocation [12]) can be another alternative for the detach procedure over IETF-based S5 interface.

6.3.4.1.9 Inter eNodeB Handover with only Serving GW Change Procedure

6.3.4.1.10 UE Requested PDN Connectivity Procedure

6.3.4.2 Candidates

The only candidate protocol provided over PMIP-based S5 interface is PMIPv6.

6.3.4.3 Analysis

Editor's note: This section will cover the analysis for the candidate protocols and for the possible enhancement to the protocols that may be applied for the PMIP-based S5 interface.

6.3.4.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.5 hPDN Gateway – 3GPP AAA Server/Proxy (S6b) Interface

6.3.5.1 Requirements

6.3.5.1.1 General

The following list of requirements applies to the S6b interface:

- Authentication of the UE in order to set up the Security Association to protect MIPv4 FA mode or DS-MIPv6 signalling;
- Authorization of the UE to use client-based mobility;
- The selected PDN GW informs the 3GPP AAA Server of its address.

Editor's note: It is FFS whether this step can be avoided, e.g. if the PDN GW address is already known by the AAA/HSS by other means

Editor's note: This requirement applies to DS-MIPv6. It is FFS if this requirement applies also to MIPv4 FA mode.

Editor's note: This list is not exhaustive as some requirements depend on the security model agreed for DS-MIPv6 and MIPv4 FA Mode.

6.3.5.1.2 Initial Attach Procedure with S2a and Anchoring in PDN GW

6.3.5.1.2.1 Update PDN GW Address Request

The parameters for Update PDN GW Address Request message are, but not exclusively, listed as below:

- user-id matching the MN ID value in the format of the user ID NAI value supplied during user authentication.

NOTE: Mobile node must link to IMSI

- PDN GW address
- EAP payload
- Visited Network Identifier
- Indication of mobility protocol (value = DSMIPv6)

Editor's notes: The actual content and format of the PDN GW address parameter is FFS.

6.3.5.1.2.2 Update PDN GW Address Acknowledgement

- EAP payload
- Result

6.3.5.1.3 Detach Procedures

6.3.5.1.3.1 Update PDN GW Address Request

The parameters for Update PDN GW Address Request message are, but not exclusively, listed as below:

- user-id;
- PDN GW address;
- An indication to distinguish removing the PDN GW address from registering the PDN GW address.

Editor's notes: It is FFS whether the user-id will match the MN-ID value in the format of a NAI supplied in the MIP signaling or the user-id NAI value supplied during user authentication or other.

Editor's notes: The actual content and format of the PDN GW address parameter is FFS.

6.3.5.1.3.2 Update PDN GW Address Acknowledgement

The parameters for Update PDN GW Address Acknowledgement message are, but not exclusively, listed as below:

- Result

6.3.5.1.3.3 Detach Indication

This message is used in HSS/AAA-initiated Detach Procedures.

The parameters for Detach Indication message are, but not exclusively, listed as below:

- user-id;
- Cause.

6.3.5.1.3.4 Detach Ack

This message is used in HSS/AAA-initiated Detach Procedures.

The parameters for Detach Ack message are, but not exclusively, listed as below:

- Result

6.3.5.2 Candidates

6.3.5.2.1 Diameter

Diameter is a candidate protocol for S6b.

6.3.5.3 Analysis

The Diameter protocol provides a number of advantages that make it the most eligible candidate for the S6b reference point. Diameter provides a good framework for performing authentication and authorisation operations. The advantages of Diameter are listed in already under chapter 6.2.4.3.1. The same reasons apply in a general manner to the S6b.

In addition to proposing Diameter as candidate protocol for S6b, this analysis section provides some reasons as to why Diameter should be selected as the final protocol for S6b without other protocols also being defined for S6b, namely Radius.

Diameter provides a set of basic advantages over Radius such as:

- Greater scalability
- End-to-end confidentiality
- Greater AVP space than in Radius
- Support of vendor specific commands via base protocol extensibility
- Ability to run over SCTP which provides re-transmission detection

In addition to the previous list of Diameter advantages, the actual systems implementing the S6b reference point (i.e. PDN GW and AAA) would greatly benefit if only one protocol is needed in order to support this functionality. It is proposed that these aspects be taken into account when selecting the S6b reference point protocol.

6.3.5.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

Diameter is the chosen protocol for S6b.

6.3.6 vServing Gateway – 3GPP AAA Proxy (S6c) Interface

6.3.6.1 Requirements

6.3.6.1.1 Initial Attach Procedure with S2a and Anchoring in Serving GW

6.3.6.1.1.1 QoS Request

The parameters for QoS Request message are FFS.

6.3.6.1.1.2 QoS Response

The parameters for QoS Response message are FFS.

6.3.6.2 Candidates

6.3.6.3 Analysis

6.3.6.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.7 hPDN Gateway – vServing Gateway (PMIP-based S8) Interface

6.3.7.1 Requirements

6.3.7.1.1 General

Differences between PMIP-based S8 and GTP-based S8 should be minimized.

6.3.7.1.2 Initial Attach Procedure with S2b and Anchoring in Serving GW

6.3.7.1.2.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name
- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

Editor's note: the Access Point Name could be conveyed in Proxy Binding Update using the Service Selection option defined in IETF draft-korhonen-mip6-service-04. Other mechanisms for conveying the Access Point Name information are FFS.

6.3.7.1.2.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix Allocated for the UE based on the selected PDN
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.7.1.3 E-UTRAN to UTRAN Iu Mode Inter RAT Handover Based on PS Handover Procedure

6.3.7.1.4 Tracking Area Update Procedure with MME and Serving Gateway change

6.3.7.1.4.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])

- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name
- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.7.1.4.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IP v4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix Allocated for the UE based on the selected PDN
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.7.1.5 UTRAN Iu Mode to E-UTRAN Inter RAT Handover Based on PS Handover Procedure

6.3.7.1.6 Inter eNodeB Handover with MME Relocation procedure

6.3.7.1.6.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])
- IP Address Request Indication

6.3.7.1.6.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- IP Address(es) Allocated for the UE

6.3.7.1.7 Handover procedure from non-3GPP access to 3GPP access

6.3.7.1.7.1 Proxy Binding Update

The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address, set to 0.0.0.0
- IPv6 Home Network Prefix, set to 0::/0
- Access Point Name

- Lifetime, set to the requested binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.7.1.7.2 Proxy Binding Acknowledgement

The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID as specified in IETF RFC 4283 [13]) in the format of NAI (as specified in IETF RFC 4282 [7])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix allocated for the UE based on the selected PDN
- Lifetime, set to the binding validity duration
- Access Technology Type, set to 3GPP
- Additional Parameters (e.g., protocol configuration options)

6.3.7.1.8 Detach procedure

6.3.7.1.8.1 Proxy Binding Update

The lifetime field of the Proxy Binding Update message is set to zero. The parameters for Proxy Binding Update message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix allocated to the UE based on the selected PDN
- Access Point Name
- Lifetime, set to zero
- Access Technology Type, set to 3GPP

6.3.7.1.8.2 Proxy Binding Acknowledgement

The lifetime field of the Proxy Binding Update message is set to zero. The parameters for Proxy Binding Acknowledgement message are, but not exclusively, listed as below:

- Mobile Node (MN-ID) in the format of IMSI-based NAI (as specified in IETF RFC 4282 [7] and 3GPP TS 23.003 [9])
- IPv4 Home Address allocated for the UE based on the selected PDN
- IPv6 Home Network Prefix allocated to the UE based on the selected PDN
- Lifetime, set to zero
- Access Technology Type, set to 3GPP

Editor's Note: It is FFS whether MIPv6 binding revocation (see IETF draft, draft-muhanna-mip6-binding-revocation [12]) can be another alternative for the detach procedure over PMIP-based S8 interface.

6.3.7.1.9 Inter eNodeB Handover with only Serving GW Change Procedure

6.3.7.1.10 UE Requested PDN Connectivity Procedure

6.3.7.2 Candidates

The only candidate protocol provided over PMIP-based S8 interface is PMIPv6.

6.3.7.3 Analysis

6.3.7.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.8 Trusted Non-3GPP IP Access - 3GPP AAA Server/Proxy (STa) Interface

6.3.8.1 Requirements

6.3.8.1.1 Initial Attach Procedure with S2a and Anchoring in PDN GW

6.3.8.1.1.1 Authentication Request

The parameters for Authentication Request message are FFS.

6.3.8.1.1.2 Authentication Response

The parameters for Authentication Response message are FFS.

6.3.8.1.1.3 Authorization Request

The parameters for Authorization Request message are FFS.

The Authorization Request message may contain Access Point Name information, if such information is available in non-3GPP access.

6.3.8.1.1.4 Authorization Response

The parameters for Authorization Response message are FFS. Charging-related parameters can be parts of parameters contained in Authorization Response message.

The Authorization Response message may include a subscription default Access Point Name information or an address of a PDN-GW in a case the Authorization Request message did not include any specific Access Point Name. The default Access Point Name information and/or the returned PDN-GW address may then be used for subsequent PDN selection and Proxy Mobile IPv6 signalling. The message is expected to include an indication of the decision on the mobility management mechanism, i.e. whether DSMIPv6 or PMIP or MIPv4FA mode should be used. The indication may then be used for subsequent IP connection establishment.

6.3.8.1.2 Detach Procedures with S2a and Anchoring in PDN GW

6.3.8.1.2.1 Detach Indication

This message is used in HSS/AAA-initiated Detach Procedures.

The parameters for Detach Indication message are, but not exclusively, listed as below:

- user-id;
- Cause.

6.3.8.1.2.2 Detach Ack

This message is used in HSS/AAA-initiated Detach Procedures.

The parameters for Detach Ack message are, but not exclusively, listed as below:

- Result

6.3.8.2 Candidates

6.3.8.2.1 RADIUS

Editor's note: The equivalent interface of STa in current 3GPP system is Wa interface in I-WLAN (see 3GPP TS 29.234 [8]). Wa interface can be based on RADIUS. So RADIUS is listed as a candidate protocol for STa interface.

6.3.8.2.2 Diameter

Editor's note: The equivalent interface of STa in current 3GPP system is Wa interface in I-WLAN (see 3GPP TS 29.234 [8]). Wa interface can be based on Diameter. So Diameter is listed as a candidate protocol for STa interface.

6.3.8.3 Analysis

6.3.8.3.1 RADIUS

Editor's Note: the usage of RADIUS to support the requirements in subclause 6.3.7.1 shall be studied in this section.

6.3.8.3.2 Diameter

Editor's Note: the usage of Diameter to support the requirements in subclause 6.3.7.1 shall be studied in this section.

6.3.8.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.9 Untrusted non-3GPP IP Access - 3GPP AAA Server/Proxy (SWa) Interface

6.3.9.1 Requirements

6.3.9.2 Candidates

6.3.9.3 Analysis

6.3.9.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.10 3GPP AAA Server/Proxy – ePDG (SWm) Interface

6.3.10.1 Requirements

The SWm reference point is defined between the 3GPP AAA Server/Proxy and the ePDG. The SWm reference point is an evolution of the existing Wm and respects backwards compatibility. The SWm reference point inherits existing Wm procedures, message descriptions and information elements specified in 3GPP TS 29.234 [8] for users accessing SAE via an Untrusted Non-3GPP IP Access.

6.3.10.1.1 Initial Attach Procedure with S2b and Anchoring in PDN GW

6.3.10.1.1.1 Authentication Request

The parameters for Authentication Request message are, but not exclusively, listed as below:

- User Identity in the format of NAI;
- EAP payload;
- Visited PLMN Identifier for roaming case;
- Access Type;

6.3.10.1.1.2 Authentication Response

The parameters for Authentication Response message are, but not exclusively, listed as below:

- EAP payload;

6.3.10.1.1.3 Authorization Request

The parameters for Authorization Request message are, but not exclusively, listed as below:

- User Identity in the format of NAI;
- W-APN;
- Visited PLMN Identifier for roaming case;

6.3.10.1.1.4 Authorization Response

The parameters for Authorization Response message are, but not exclusively, listed as below:

- PDN GW Selection Information;
- IP mobility management selection Information.

Editor's note: The content of PDN GW Selection Information is FFS.

The parameters for Authorization Request message are FFS. Charging-related parameters can be parts of parameters contained in Authorization Response message.

6.3.10.1.2 Detach Procedure with S2b and Anchoring in PDN GW

6.3.10.1.2.1 Detach Indication

This message is used in HSS/AAA-initiated Detach Procedure.

The parameters for Detach Indication message are, but not exclusively, listed as below:

- user-id;
- Cause.

6.3.10.1.2.2 Detach Ack

This message is used in HSS/AAA-initiated Detach Procedure.

The parameters for Detach Ack message are, but not exclusively, listed as below:

- Result

6.3.10.2 Candidates

6.3.10.2.1 Diameter

Editor's note: The equivalent interface of SWm in current 3GPP system is Wm interface in I-WLAN (see 3GPP TS 29.234 [8]). Wm interface can be based on Diameter. So Diameter is listed as a candidate for SWm interface.

6.3.10.3 Analysis

6.3.10.3.1 Diameter

Editor's Note: the usage of Diameter to support the requirements in subclause 6.3.9.1 shall be studied in this section.

6.3.10.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.11 Untrusted Non-3GPP IP Access – ePDG (SWn) Interface

6.3.11.1 Requirements

6.3.11.2 Candidates

6.3.11.3 Analysis

6.3.11.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.12 3GPP AAA Server – HSS (SWx) Interface

6.3.12.1 Requirements

6.3.12.1.1 General

The SWx reference point is an evolution of the existing Wx and respects backwards compatibility. The SWx reference point inherits existing Wx procedures, message descriptions and information elements specified in 3GPP TS 29.234 [8] for users accessing EPS via an un-trusted non-3GPP IP accesses since the latter are assumed to follow procedures defined for I-WLAN.

The SWx supports the following procedures irrespective of whether a user is accessing via a trusted non-3GPP IP accesses or un-trusted non-3GPP IP accesses: authentication procedures, location management procedures and user data handling.

These procedures should be as similar as possible although variations may exist regarding information elements depending on the non-3GPP IP accesses.

6.3.12.1.2 Initial Attach Procedure with S2a and Anchoring in PDN GW

6.3.12.1.2.1 Authentication Request

The parameters for Authentication Request message are FFS.

6.3.12.1.2.2 Authentication Response

The parameters for Authentication Response message are FFS.

6.3.12.1.2.3 Authorization Request

The parameters for Authorization Request message are FFS.

6.3.12.1.2.4 Authorization Response

The parameters for Authorization Request message are FFS. Charging-related parameters can be parts of parameters contained in Authorization Response message.

6.3.12.1.2.5 UE Registration Request

The parameters for UE Registration Request message are, but not exclusively, listed as below:

- Permanent user identity
- Server Assignment Type (note: this parameter refers to the Type of procedure the 3GPP AAA Server requests in the HSS e.g. REGISTRATION, USER_DEREGISTRATION, etc).

6.3.12.1.2.6 UE Registration Response

The parameters for UE Registration Request message are, but not exclusively, listed as below:

- Permanent user identity
- Registration Result
- User profile

6.3.12.1.3 Initial Attach Procedure with S2a and Anchoring in Serving GW

6.3.12.1.3.1 QoS Profile Request

The parameters for QoS Profile Request message are FFS.

6.3.12.1.3.2 QoS Profile Response

The parameters for QoS Profile Response message are FFS.

6.3.12.1.4 Detach Procedures

6.3.12.1.4.1 UE De-Registration Request

This message will be sent from HSS or from 3GPP AAA Server in this procedure.

The parameters for UE De-Registration Request message are, but not exclusively, listed as below:

- User Identity;
- Cause.

6.3.12.1.4.2 UE De-Registration Ack

This message will be sent from HSS or from 3GPP AAA Server in this procedure.

The parameters for UE De-Registration Ack message are, but not exclusively, listed as below:

- Result

Editor's note: it is FFS whether 3GPP AAA Server initiated UE De-Registration performs overlapped functions with Update PDN GW Address (remove PDN GW Address) operations during the detach procedures. If yes, how to solve the problem is FFS.

6.3.12.1.5 Network Initiated Deregistration by HSS

6.3.12.1.5.1 Network Initiated Deregistration by HSS Request

The parameters for Network Initiated Deregistration by HSS Request message are, but not exclusively, listed as below:

- Permanent user identity
- Reason for de-registration;

6.3.12.1.5.2 Network Initiated Deregistration by HSS Response

6.3.12.1.6 User Profile Update

6.3.12.1.6.1 User Profile Update Request

The parameters for User Profile Update request message are, but not exclusively, listed as below:

- Permanent user identity;
- user profile;

6.3.12.1.6.2 User Profile Update Response

The parameters for User Profile Update response message are, but not exclusively, listed as below:

- Result;

6.3.12.2 Candidates

6.3.12.2.1 Diameter

Diameter is a candidate protocol for SWx interface.

6.3.12.3 Analysis

6.3.12.3.1 Diameter

Editor's Note: the usage of Diameter to support the requirements in subclause 6.3.11.1 shall be studied in this section.

Basing SWx on Diameter will enable a smooth evolution from Wx to SWx. A Diameter-based SWx will minimise impacts on both HSS and 3GPP AAA Server and allow for swifter accomplishment of SAE specifications given the large competence acquired by 3GPP regarding Diameter.

The procedures defined for the Wx interface can be re-used to support SWx functions without or with some appropriate extensions of parameters and behaviours of the 3GPP AAA Server and/or the HSS:

- Authentication information retrieval
- Location management:
  - WLAN Registration procedure;
  - 3GPP AAA Server initiated De-Registration procedure;
  - HSS initiated De-Registration procedure.
- User profile management:
  - 3GPP AAA Server-initiated provide user profile;
  - HSS-initiated user profile update.

New procedures for SWx needs to be specified to support SAE functions include:

- As a part of Location management, the PDN GW address notification which is used to register/de-register the current PDN GW address in the HSS for a given user.

From parameter point of view, most of parameters defined for Wx can be re-used. The parameter user profile needs to be extended to contain more sub-parameters including:

- PDN GW Address information which is stored in the HSS and used for inter-system mobility.

The PDN GW related information can be considered location management related data and also subscriber related data. Hence it seems natural to include the following new information elements:

Table 6.3.12.3.1-1: New information elements related to PDN GW

VPLMN PDN GW ALLOWED	Indicates whether a VPLMN may allocate PDN GW or not to a user.
PDN GW NAME	PDN GW identity returned as part of subscriber data on initial attach or registration.
PDN GW IP ADDRESS	The IP address of already allocated PDN GW to be used in inter-system mobility. If this value is returned then no new PDN GW is selected. If this value is NULL then the PDN GW NAME is used. In the case of multiple PDN support, APN information shall be returned together with corresponding PDN GW NAME or PDN GW IP ADDRESS. NOTE: The APN information defined in the Wx interface in 3GPP TS 29.234 [8] is mainly used for authorization of a user. And the APN information here is used together with PDN GW NAME or PDN GW IP ADDRESS to support inter-system mobility in the case of multiple PDN feature. From parameter point of view, only one parameter, e.g. 3GPP-WLAN-APN-Id AVP, is sufficient to support both cases in different scenarios.

The above data can be exchanged between HSS and 3GPP AAA Server. Note that the prefix WLAN has been dropped in order to cover both trusted and un-trusted non-3GPP accesses.

6.3.12.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.13 3GPP AAA Server - 3GPP AAA Proxy (SWd) Interface

6.3.13.1 Requirements

The SWd reference point is defined between the 3GPP AAA Proxy and the 3GPP AAA Server. The SWd reference point is an evolution of the existing Wd and respects backwards compatibility. The SWd reference point inherits existing Wd procedures, message descriptions and information elements specified in 3GPP TS 29.234[8] for users accessing SAE via an Untrusted Non-3GPP IP Access or Trusted Non-3GPP IP Access in roaming case.

6.3.13.1.1 Initial Attach Procedure with S2b and Anchoring in Serving GW

6.3.13.1.1.1 Authentication Request

The parameters for Authentication Request message are FFS.

6.3.13.1.1.2 Authentication Response

The parameters for Authentication Response message are FFS.

6.3.13.1.1.3 Authorization Request

The parameters for Authorization Request message are FFS.

6.3.13.1.1.4 Authorization Response

The parameters for Authorization Response message are, but not exclusively, listed as below:

- PDN GW Selection information, which is:

An IP address of a PDN GW and an APN, or an APN and an indication whether the allocation of a PDN GW from the visited PLMN is allowed or a PDN GW from the home PLMN shall be allocated.

The parameters for Authorization Request message are FFS. Charging-related parameters can be parts of parameters contained in Authorization Response message.

6.3.13.1.2 Initial Attach Procedure with S2a and Anchoring in Serving GW

6.3.12.1.2.1 Provide User Profile

The parameters for Provide User Profile message are, but not exclusively, listed as below:

- User Identity

6.3.13.1.2.2 Provide User Profile Acknowledge

The parameters for Provide User Profile Acknowledge message are, but not exclusively, listed as below:

- User Identity;
- Subscription Data.

6.3.13.1.3 Detach Procedures

6.3.13.1.3.1 Update PDN GW Address Request

The parameters for Update PDN GW Address Request message are, but not exclusively, listed as below:

- user-id;
- PDN GW address;
- An indication to distinguish removing the PDN GW address from registering the PDN GW address.

Editor's notes: It is FFS whether the user-id will match the MN-ID value in the format of a NAI supplied in the MIP signaling or the user-id NAI value supplied during user authentication or other.

Editor's notes: The actual content and format of the PDN GW address parameter is FFS.

6.3.13.1.3.2 Update PDN GW Address Acknowledgement

The parameters for Update PDN GW Address Acknowledgement message are, but not exclusively, listed as below:

- Result

6.3.13.1.3.3 Detach Indication

This message is used in HSS/AAA-initiated Detach Procedures.

The parameters for Detach Indication message are, but not exclusively, listed as below:

- user-id;
- Cause.

6.3.13.1.3.4 Detach Ack

This message is used in HSS/AAA-initiated Detach Procedures.

The parameters for Detach Ack message are, but not exclusively, listed as below:

- Result

6.3.13.2 Candidates

6.3.13.2.1 RADIUS

Editor's note: The equivalent interface of SWd in current 3GPP system is Wd interface in I-WLAN (see 3GPP TS 29.234 [8]). Wm interface can be based on RADIUS. So RADIUS is listed as a candidate for SWd interface.

6.3.13.2.2 Diameter

Editor's note: The equivalent interface of SWd in current 3GPP system is Wd interface in I-WLAN (see 3GPP TS 29.234 [8]). Wd interface can be based on Diameter. So Diameter is listed as a candidate for SWd interface.

6.3.13.3 Analysis

6.3.13.3.1 RADIUS

Editor's Note: the usage of RADIUS to support the requirements in subclause 6.3.12.1 shall be studied in this section.

6.3.13.3.2 Diameter

Editor's Note: the usage of Diameter to support the requirements in subclause 6.3.12.1 shall be studied in this section.

6.3.13.4 Conclusions

Editor’s note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.14 Gateway - UE (S2c) Interface

Editor’s note: S2c interface mentioned here is just for possible effect, it will be specified in TR 24.801.

6.3.14.1 Requirements

6.3.14.2 Candidates

The S2c interface shall support following protocol(s):

- Dual Stack MIPv6 as specified in Internet-Draft, draft-ietf-mip6-nemo-v4traversal-04 [6].

Editor’s note: Whether more protocols will be selected for the S2c interface is FFS.

6.3.14.2.1 Dual Stack MIPv6

6.3.14.3 Analysis

6.3.14.4 Conclusions

Editor's note: this section covers the conclusion for protocol selection and possible enhancement.

6.3.15 MME – HRPD (S101) Interface

This interface is required to perform procedures related to optimise HO between EPS and HRPD access to allow for pre-registration and handover signalling with the target system as described in TS 23.402 [3].

6.3.15.1 Requirements

The S101 reference point is defined between the MME and the trusted non-3GPP access network, enabling interactions between EPS and HRPD access to allow for pre-registration and handover signalling with the target system.

Requirements for this interface are detailed in TS 23.402 [3].

6.3.15.1.1 Optimized Active Handover from E-UTRAN Access to cdma2000 HRPD Access Procedure

Editor's note: These messages and parameters are shown here as described in TS 23.402; however, the details of how these messages are manifest into the S101 application protocol are FFS.

The following messages are used on the S101 interface for handover from E-UTRA to cdma2000 HRPD access:

- Direct Transfer Request
- Direct Transfer Response
- Notification Request
- Notification Response

All S101 messages shall include the following parameter(s):

- S101 Session ID – The S101 Session ID is a scalar value that uniquely identifies an instance of the S101 interface between an HRPD AN and an MME.

Editor's note: The details of additional protocol functions, such as path management and protocol error detection and recovery are FFS.

Editor's note: The list of parameters in this section is intended to satisfy the requirements as specified in TS 23.402. Additional parameters that may be required for protocol operation are FFS.

6.3.15.1.1.1 Pre-registration Procedure

Pre-registration, as described in TS 23.402, allows a UE to register with the cdma2000 HRPD access network while still attached to E-UTRA access.

The UE initiates pre-registration with the HRPD access network by encapsulating an HRPD registration message into the payload of an RRC message. This message is forwarded to the MME via the S1 interface. When the MME receives an HRPD registration message, the MME will decapsulate the HRPD registration request, and then reencapsulate into an S101 Direct Transfer message to be sent to the HRPD RNC. The MME determines the IP address of the HRPD RNC based on the sector ID, which will be statically configured on the eNB and sent as a parameter along with the HRPD registration payload from the UE.

Responses from the HRPD access network are also carried via the Direct Transfer message from the HRPD RNC to the MME, which then forwards via S1-AP to the eNB to be sent to the UE. Signalling between the UE and the HRPD access network continue in this fashion until pre-registration is complete.

The signalling itself is carried as payload in the Direct Transfer message and is opaque to the MME, and hence, the details of the pre-registration procedure itself are largely transparent to the S101 protocol itself.

6.3.15.1.1.1.1 Direct Transfer Message

This message is sent from the MME to HRPD access.

In order to be able to distinguish S101 signalling transactions belonging to different UEs, the MME shall use the selected S101 Session ID to identify signalling related to that UE on S101. The MME shall select the correct HRPD access node address based on the Sector ID.

If the MME finds an entry in the MME context for that UE indicating the same HRPD access node address associated with the Sector ID, then the same S101 Session ID will be used.

If the MME finds an entry in the MME context for that UE indicating a different HRPD access node address associated with the Sector ID, then the MME shall select the correct HRPD access node address based on the received Sector ID and shall select a new S101 Session ID to identify signalling related to that UE on S101.

The MME shall include the HRPD PDU transparently as received from the UE via the eNodeB.

Editor's Note: the Direct Transfer message name could be changed in SA2.

Editor's Note: MME procedure to select S101 Session ID is FFS.

Editor's Note: The usage of a separate S101 Session ID that is local to the specific S101 instance or another existing UE specific identifier is FFS in SA2.

The parameters for Direct Transfer message are, but not exclusively, listed as below:

- S101 Session ID; (to identify signalling related to that UE on S101, the format is FFS);
- Sector ID;
- HRPD PDU (sent from the UE - transparent to EPS);

6.3.15.1.1.2 Handover Procedure

6.3.15.1.1.2.1 Direct Transfer Message

This message is described in 6.3.14.1.1.1.1.

6.3.15.1.1.2.2 S101 HO Command Message

This message is sent from the HRPD access to MME.

The S101 HO Command message is sent form the HRPD access to the MME providing the HO status in HRPD in HO Result information element and the HRPD PDU which shall be passed transparently via the eNodeB to the UE.

If data forwarding is required the HRPD access shall provide data forwarding target information (comparable to target IP address and TEID) to the MME, where the MME shall configure data forwarding resources for indirect data forwarding on Serving GW.

Editor's Note: The details of the parameters for data forwarding are FFS, also if the end point of data forwarding on the EUTRAN side is eNB or Serving GW is FFS.

Editor's Note: the S101 HO Command message name could be changed in SA2

The parameters for Direct Transfer message are, but not exclusively, listed as below:

- S101 Session ID;
- Data Forwarding target information (details FFS);
- A value indicating the result of the ongoing HO preparation within the other system;

- HRPD PDU (sent to the UE - transparent to EPS);

6.3.15.1.2 Optimized Active Handover from cdma2000 HRPD Access to E-UTRAN Access Procedure

Editor's note: FFS- List of messages and parameters on S101

6.3.15.2 Candidates

6.3.15.2.1 UDP Based Application Protocol

The only candidate at this time is a UDP based application protocol as proposed in TS.23.402 [3]. The detailed messages and message formats are FFS.

6.3.15.3 Analysis

As described in 23.402 [3], the interface between the MME and HRPD RNC is a signalling interface, and need not inherently provide signalling reliability on transport level. In this case, the choice of UDP, as opposed to TCP or SCTP, as a transport protocol is appropriate. Reliable transport for signalling messages shall be provided by the S101-AP protocol.

All other protocol requirements dictated by 23.402 [3] can also be satisfied by an application run over UDP, making a UDP based application the appropriate choice for this interface.

6.3.15.4 Conclusions

UDP/IP is the chosen protocol for S101 transport.

7 Numbering addressing and identification for EPS

7.1 General

This chapter will describe the identities for each new introduced access, the identities used in EPC and the identities used through EPS. This chapter will also describe the identities that are newly added or updated for the existing accesses because of the introduction of EPS.

Editor's Note: Radio accesses related identities are defined in the specifications from RAN groups or CT1 and referred here to be merged to 3GPP TS 23.003 [9] in the future.

Editor's Note: The existing identities that are related to EPS are referred to 3GPP TS 23.003[9], e.g. I-WLAN, MBMS. It is FFS whether these identities are needed to be changed or new identities will be added.

7.2 Identifications of E-UTRAN

<This section is for the identifications of only E-UTRAN related>

7.3 Identifications of Non-3GPP Accesses

<This section is for the identifications of only non-3GPP accesses related and subsections are needed if necessary>

7.4 Identifications of EPC

<This section is for the identifications of only EPC related>

7.4.1 EPS bearer Identity

An EPS bearer identity uniquely identifies an EPS bearer for one UE accessing via E-UTRAN. The EPS Bearer Identity is allocated by the MME.

Editor's Note: The encoding of EPS bearer identity is FFS. The relationship between the NSAPI/RAB ID used in UMTS and EPS bearer identity is FFS.

7.4.2 Globally Unique Temporary UE Identity (GUTI) and S-Temporary Mobile Subscriber Identity (S-TMSI)

The GUTI is used to support subscriber identity confidentiality, and, in the shortened S-TMSI form, to enable more efficient radio signalling procedures (e.g. paging and Service Request).

The GUTI is allocated by the MME and has two main components:

- one that uniquely identifies the MME which allocated the GUTI; and
- one that uniquely identifies the UE within the MME that allocated the GUTI.

Within the MME, the mobile is identified by the M-TMSI.

The Globally Unique MME Identifier (GUMMEI) is constructed from MCC, MNC and MME Identifier (MMEI).

In turn the MMEI is constructed from an MME Group ID (MMEGI) and an MME Code (MMEC).

The GUTI is constructed from the GUMMEI and the M-TMSI.

For paging and Service Request, the mobile is identified with the S-TMSI. The S-TMSI is constructed from the MMEC and the M-TMSI.

In EPS,

<GUTI> = <GUMMEI><M-TMSI>,

where <GUMMEI> = <MCC><MNC><MME Identifier>

and <MME Identifier> = <MME Group ID><MME Code>

It is assumed that MCC and MNC have the same field size (3 BCD digits) and the meaning as in pre release 8 3GPP systems.

M-TMSI is used to uniquely identify the UE within the MME that allocates the GUTI. It is assumed to have 32 bits.

MME Code is used to uniquely identify the MME within a MME pool. It is assumed to have 8 bits.

MME Group ID is used to uniquely identify the MME pool within a PLMN. It is assumed to have 16 bits.

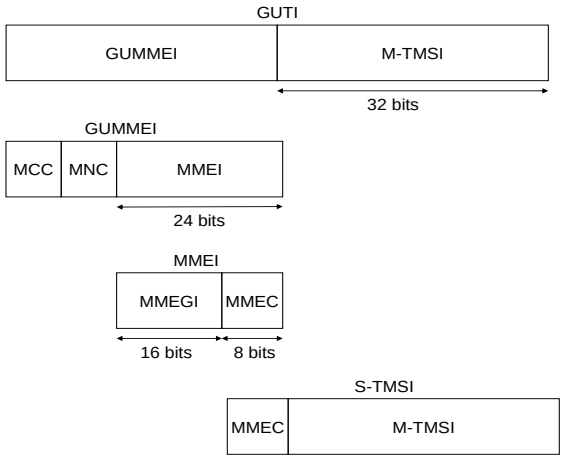

Figure 7.4.2.1-1 Structure of GUTI/S-TMSI

When mapping of EPS identities to legacy identities is done, the following mapping rules shall be followed:

- MCC maps to MCC of the legacy system;
- MNC maps to MNC of the legacy system;
- MMEGI maps to LAC of the legacy system;
- FFS: MMEC maps to RAC or also copied to 8 bits of P-TMSI of the legacy system;
- FFS: M-TMSI maps to P-TMSI or 24 bits of P-TMSI and 8 bits of P-TMSI Signature of the legacy system.

7.4.3 Tracking Area Identity

This is the identity used to identify tracking areas. Tracking Area Identity is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code) and TAC (Tracking Area Code).

Editor's Notes: The encoding of TAC is FFS.

7.4.4 EPC QoS profile

An EPC QoS profile is a parameter with multiple data transfer attributes for a particular bearer.

Editor's Notes: The encoding of EPC QoS profile is FFS. The relationship between EPC QoS Profile and UMTS QoS profile is FFS.

7.4.5 Linked EPS bearer Identity

The Linked EPS Bearer Identity (LBI) is the EPS bearer identity of the default bearer which is used to associate the corresponding PDN connection in the dedicated bearer management procedures

7.4.6 Access Point Name

In the EPC of the EPS, an Access Point Name (APN) is ultimately a reference to a PGW, LMA or HA. To support inter-PLMN roaming, the EPC internal DNS functionality is used to translate the APN into the IP address of the PGW.

The following clauses describe proposals on the mechanisms used to select a PDN-GW, LMA or HA using DNS and the APN parameter.

7.4.6.1 Alternative 1

The APN is composed of two parts as follows:

- The APN Network Identifier; this defines to which external network the PGW is connected. This part of the APN is mandatory.

- The APN Operator Identifier; this defines in which PLMN the PGW is located. This part of the APN is optional, but is required when resolving PWG addresses belonging to other PLMNs using DNS.

Editor's note: it is FFS if APN Operator Identifier should also become mandatory.

The APN Operator Identifier is placed after the APN Network Identifier. An APN consisting of both the Network Identifier and Operator Identifier corresponds to a DNS name of a PGW; the APN has, after encoding as defined in the paragraph below, a maximum length of 100 octets.

The encoding of the APN shall follow the Name Syntax defined in RFC 2181, RFC 1035 and RFC 1123. The APN consists of one or more labels. Each label is coded as a one octet length field followed by that number of octets coded as 8 bit ASCII characters. Following RFC 1035 the labels shall consist only of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-). Following RFC 1123, the label shall begin and end with either an alphabetic character or a digit. The case of alphabetic characters is not significant. The APN is not terminated by a length byte of zero.

NOTE: A length byte of zero is added by the MME or R8 SGSN at the end of the APN before sending a DNS query.

The labels in the EPS APN shall be separated by dots (e.g. "Label1.Label2.Label3").

7.4.6.1.1 Format of APN Network Identifier

The APN Network Identifier shall contain at least one label and shall have, after encoding a maximum length of 63 octets. An APN Network Identifier shall not start with any of the strings "rac", "lac", "sgsn", "rnc", "w-apn", "pub" or "eps-apn-", and it shall not end in "gprs" or in "3gppnetwork.org". Further, it shall not take the value "*".

In order to guarantee uniqueness of APN Network Identifiers within or between PLMNs, an APN Network Identifier containing more than one label shall correspond to an Internet domain name. This name should only be allocated by the PLMN if that PLMN belongs to an organisation which has officially reserved this name in the Internet domain. Other types of APN Network Identifiers are not guaranteed to be unique within or between PLMNs.

Editor's note: it is FFS if APN Network Identifier optionally indicates also MS requested service. Depending on the decision the following paragraph would be either kept, or removed.

An APN Network Identifier may be used to access a service associated with a PGW. This may be achieved by defining:

- an APN which corresponds to a FQDN of a PGW, and which is locally interpreted by the PGW as a request for a specific service; or

- an APN Network Identifier consisting of 3 or more labels and starting with a Reserved Service Label, or an APN Network Identifier consisting of a Reserved Service Label alone, which indicates a PGW by the nature of the requested service. Reserved Service Labels and the corresponding services they stand for shall be agreed between operators who have roaming agreements.

7.4.6.1.2 Format of APN Operator Identifier in DNS

In DNS the APN Operator Identifier is composed of five or six labels. The first label shall be "eps-apn-<NodeName>". The second and the third labels together shall uniquely identify the PLMN. Last two labels shall be "3gppnetwork.org".

For each operator, there is a default APN Operator Identifier (i.e. domain name). The MME and R8 SGSN derive the default APN Operator Identifier from the IMSI as follows:

"eps-apn-<NodeName>.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

And the EPS UE shall derive the default APN Operator Identifier from the IMSI as follows:

"eps-apn-<NodeName>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where:

"mnc" and "mcc" serve as constant identifiers for the following digits.

<MNC> and <MCC> are derived from the components of the IMSI defined in 3GPP TS 23.003 [9].

"eps-apn-" indicates the EPS access type

<NodeName> indicates the IP address of the function in question (PGW, HA, LMA, etc.).

Editor's note: it is FFS (a) how pre-R8 SGSN constructs APN for the UE, which is trying to access EPC, (b) in what format does pre-R8 receive EPS APN from MME or R8 SGSN, (c) how MME and R8 SGSN handle APN that was received from pre-R8 SGSN. Besides, it is also FFS if DNS should support also "eps-apn-xxx.mnc<MNC>.mcc<MCC>.gprs" format for the migration period.

The default APN Operator Identifier is used in inter-PLMN roaming situations when attempting to translate an APN consisting only of a Network Identifier into the IP address of e.g. the PGW in the HPLMN. The PLMN may provide DNS translations for other, more human-readable, APN Operator Identifiers in addition to the default Operator Identifier described above.

In DNS the APN Operator Identifier shall be coded as specified above. In addition to that, in order to guarantee inter-PLMN DNS translation, the <MNC>, <MCC> and <NodeName> coding used in the APN OI shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits
- If there are only 2 significant digits in the MNC, one "0" digit is inserted at the left side to fill the 3 digits coding of MNC in the APN OI.
- <NodeName> = 3 characters. When GTP tunnel termination point is requested, the value shall be "pgw". When HA address is requested, the default value shall be "ha0". When PMIP tunnel termination point (LMA) is requested, the value shall be "lma".

Editor's note: It is FFS if values like "ha1", "ha2", etc. would be useful.

Below are two examples of the EPS APN OI for MCC = 345 and MNC = 12.

If APN was provided by HSS for 3GPP access and if MME requests PGW's IP address (i.e. the GTP tunnel termination point), then this will be coded in the DNS as:

"eps-apn-pgw.mnc012.mcc345.3gppntwork.org"

7.4.6.1.3 Usage of EPS APN in DNS queries

Editor's note: the usage of EPS APN will be specified in respective technical specifications (GTPv2, DSMIPv6, MIPv4, NAS signalling, etc.). Therefore, the above subclauses 7.4.6.1 and 7.4.6.2 should only specify the APN format and encoding rules. The rest of the text will be moved here.

7.4.6.2 Alternative 2

This is a placeholder for an alternative mechanism using DNS and the APN parameter for PGW, LMA and HA selection.

This alternative intends to address the issue that may be a number of problems related to the PGW selection function which could be solved by a different usage of the DNS queries on the APN. (See S2-080074 from the SA2#62 meeting for details)

These problems are among other:

- The dependencies between the PGW selection function and the SGW selection function. According to 23.401 [2] v8.0.0, section 4.3.8 "If combined Serving and PDN GWs are configured in the network the Serving GW Selection Function preferably derives a Serving GW that is also a PDN GW for the UE."
- The existence of different protocol options for PDN-GW interfaces S5/S8. The PDN-GW might define different IP addresses for the different protocols. (This problem is addressed by Alternative 1 above)

This alternative proposes a two step mechanism where a first DNS query is used to resolve the APN into a logical name identifying a GW, and a second step is used to resolve that logical name into the information required for the PDN GW addressing the problems described above.

In order to allow this first step, the APN name shall not be decorated. It is FFS if the logical GW name to be used in the second step could use decoration.

7.4.7 Procedure Transaction Identity

An identity which is dynamically allocated by the UE for the UE requested bearer resource allocation and release procedures. The procedure transaction identity is released when the procedure is completed.

7.4.8 ME Identity

The ME identity is used to uniquely identify a Mobile Equipment.

Editor's note: The relationship between ME Identity and IMEISV is FFS. The detailed format of ME Identity is FFS.

The ME Identity can be checked at MME at initial Attach procedure when Attach Type does not indicate handover and, at TAU from UTRAN/GERAN if the old SGSN does not provide the ME Identity.

Editor's note: It is FFS whether the MME should obtain the ME Identity during the EPC Authentication and Ciphering procedure.

Editor's note: It is FFS whether HSS and/or PDN GW can also check the ME Identity.

7.5 Identifications of EPS

<This section is for the identifications used through EPS but not included in the above sections>

8 EPS impacts on existing capabilities and interfaces

8.1 MBMS

8.2 Network Sharing

8.3 Enhancement on Rel8 Gr interface

8.3.1 General

This section is to collect all the new requirements on Rel8 Gr introduced by EPS as the basic for future work on TS 29.002. In each subsection below, the stage 2 requirements and the related effect on Rel8 Gr should be given.

9 General issues

9.1 Protocol version of R8 GTP for EPS (eGTP)

9.1.1 General

This key issue is to discuss the protocol version of Rel8 GTP for EPS. It is to be decided how to extend the current GTP to realize the new features introduced by EPS. It can be foreseen that this issue would not only affect the vendors when developing the equipment but also affect the operators when deploying their networks.

CT4 has identified the following requirements for R8 GTP for EPS (eGTP):

- There is a need for specifying R8 GTP version for EPS (eGTP). Both control plane and user plane flavours shall be defined.
- eGTP shall be backward compatible to pre-R8 GTPv1.
- eGTP shall not support interworking with GTPv0.
- FFS: eGTP shall be used by both R8 EPS (as defined in R8 TS 23.401) and by R8 UMTS (as defined in R8 TS 23.060).
- eGTP shall use the same port numbers, which were assigned to GTPv1. This is necessary for more efficient interworking with legacy GTPv1 entities.

The EPS architecture for GTP based interfaces is shown as below.

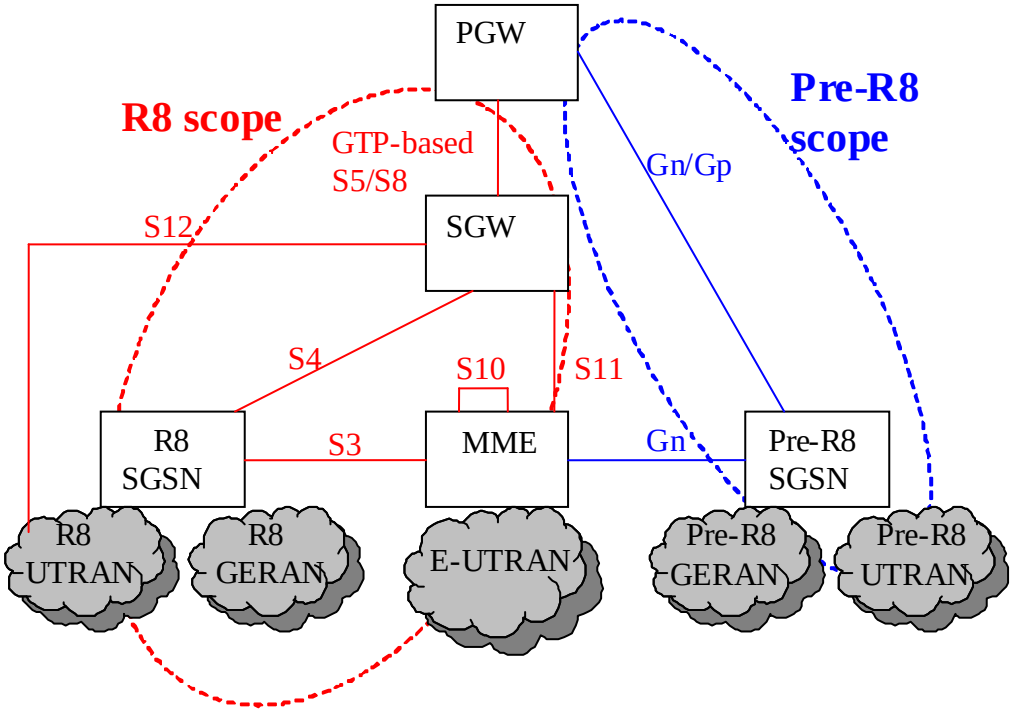

Figure 9.1.1-1 EPS architecture for GTP based interfaces

The scope of R8 GTP for EPS based interfaces is S3, S4, GTP-based S5, GTP-based S8, S10, S11, S12.

9.1.2 Alternatives for eGTP

Currently, there are two alternatives for the R8 GTP-C for EPS: one is extending the GTP version 1, and the other is to specify new version of GTP, GTPv2.

Editor's note: How to deal with GTP-U for EPS is FFS.

9.1.2.1 Extended GTP-C version 1

With the extended GTP-C version 1 alternative the existing GTPv1 message types and information element types will be reused by eGTP-C. Also eGTP-C message format will be the same as it is in GTPv1. GTPv1 however will be extended by adding necessary new messages and information elements for the new features introduced by EPS.

The sending or responding eGTP-C entity would need to insert a new flag or a new IE indicating to the peer that the extended GTPv1 message was sent.

9.1.2.2 GTP-C version 2

With the GTPv2 alternative all messages and the Information Elements will be defined new. The eGTP message format may also newly defined to better fit the requirements for the affected interfaces.

GTPv2 shall use the same port numbers, which were assigned to GTPv1. This is necessary for more efficient interworking with legacy GTPv1 entities.

9.1.3 Requirements for eGTP

Before making a decision on which GTP version to use for eGTP, there are several key factors which should be studied. The final decision should take these factors into account.

Editor's notes: It should be noted that the key factors in this paper may be not integrated and some other key factors may also be needed.

9.1.3.1 New features to be supported by the protocol

This subsection lists new features that should be supported by eGTP and which are not supported by the current GTP version 1. It should be noted that the list is not exhaustive other new features may also be needed.

- New QoS mechanism
- New UE Context because of, e.g. separation of control plane entity and user plane entity
- New bearer ID
- New function entity ID
- Idle mode signalling reduction
- Inter 3GPP mobility
- eMBMS
- End marker packet

For the method of extending GTP version 1, it should be evaluated whether it is sufficiently extensible for accommodation all new features.

For the method of GTP version 2, GTP version 2 does not have such limitation.

9.1.3.2 Backward compatibility issue

EPC network elements (MME, SGW and PGW) and R8 SGSN should be able to communicate with pre-R8 UMTS network elements (SGSN, RNC, GGSN). Therefore, MME, PGW and R8 SGSN should also support GTPv1 based Gn/Gp interfaces. When UE moves between E-UTRAN and pre-R8 UTRAN/GERAN, the compatibility issue needs to be handled.

For the method of extending GTP version 1, the compatibility issue is FFS.

For the method of GTP version 2, the compatibility issue is to be evaluated, such as message mapping, Information Element mapping, and GTP version handling.

9.1.3.3 Extendibility issue

Extensibility is very important protocol feature for supporting future requirements. The protocol should be designed in the way that to adding new messages and information elements should not cause any problems.

For the method of extending GTP version 1, it is to be evaluated whether there is enough available messages type code and Information Element type code for the current new features the possible future requirement of EPS. Or some other mechanism is needed, e.g. extending the message type and/or the Information Element type code.

For the method of GTP version 2, currently there is no effect foreseen.

9.1.3.4 Requirements of different interfaces

Below table lists the GTP version support status of the reference points of EPC:

Table 9.1.3.4.1: "Requirements of different GTP based interfaces"

Interfaces	GTPv1 feature support required	GTPv1 parameter required	extension to eGTP required	legacy entity connected
S3	Yes	Yes	Yes*	R8 SGSN
S4	Yes	Yes	FFS*	R8 SGSN
GTP-based S5	No	FFS	Yes	No
GTP-based S8	No	FFS	Yes	No
S10	No	No	Yes	No
S11	No	Yes	Yes	No

(*) S3 interface shall be involved in ISR feature and possibly other new EPS features, but it is still FFS how it is involved.

It is FFS whether S4 interface would be extended to support ISR or other EPS features.

9.1.3.5 Comparison of the alternatives

Table 9.1.3.5.1: "Comparison between GTPv2 and extended GTPv1"

Point of relevance	GTPv2	Extended GTPv1	Summary
Backward compatibility when GTPv1 entity receives R8 message.	Receiving entity responds with "Version not supported" message. Sending entity will fallback to GTPv1.	Receiving entity silently discards the message. Sending entity will retransmit the message x times.	GTPv2 will use less time
Fallback to the legacy GTPv1 mechanism	To be defined.	To be defined.	Both capable of being enhanced with the feature.
CT4 efforts required for upgrading to R8.	Starting from GTPv1 e.g. re-use of GTPv1IEs where feasible	Has a ready foundation.	GTPv2 require more efforts.
Available range of type values for R8 messages.	At least 255.	8-15, 24-25, 38-47, 61-69, 71-95, 101-106, 122-127,130-239, 242-254. Altogether 68.	Equally sufficient space.
Available range of type values for R8 TV IEs.	At least 127.	29-117 (usage is limited on new Rel-8 messages)	Equally sufficient space.
Available range of type values for R8 TLV IEs.	At least 127.	184-239	Equally sufficient space.
Deficiencies that cannot be corrected, without becoming backward incompatible.	None.	Some. E.g. it is not possible to remove mandatory or conditional IE even if it becomes obsolete for Rel-8; it is not possible to extend some useful TLV coded IE if the respective table shows the length of non-variable number, etc.	GTPv1 has a certain drawback.
Restoration and recovery	Possible to define an efficient mechanism.	CT4 tried to improve the existing recovery and restoration mechanism, but it did not prove efficient. The problem is that if a message that carries such info is lost, then bringing the GTP entities back to sync seems impossible.	GTPv1 has a an inefficiency.
SUMMARY			GTPv2 has a clear advantage

9.1.3.6 The charging related GTP' protocol

Support of GTP' in EPC is decoupled from GTP v2 protocol development. An EPC node may support the GTP' protocol but will base this on legacy GTP' protocol.

Messages of GTP' and GTP v2 may be distinguished by the receiving node by different registered UDP ports (3386 for GTP' and 2123/2152 for GTP v2). In GTP v2 it is not necessary to reserve protocol resources for message types, Cause values and IE type codes for GTP'.

9.1.3.7 eGTP control procedure requirements

The eGTP Bearer Management transactions handle a group of bearers for one end-user and one APN. This group of bearers consists of a number of EPS bearers that are linked for one user and one APN. A group of linked bearers always has a Default bearer and possibly in addition a number of Dedicated bearers.

- eGTP Control messages may operate on a number of bearers in one control message, e.g. at S-GW relocation (see 3GPP TS 23.401 [2], section 5.5.1, Inter eNodeB handover with CN node relocation);
- whether at any time, there may be more than one outstanding eGTP Bearer Control Request (creation or modification) in a group of linked bearers for one end-user and one APN, is FFS.

If certain IP interface of an EPC network element fails, the network element may notify the peer with one message. Depending on the nature of failure, EPC network element may send appropriate control plane message to the peer and identify the affected EPC bearers by the failed IP address and/or APN.

9.1.3.8 eGTP Path Management

The eGTP Path Management functionality shall be mandatory to use for all EPC nodes implementing eGTP. Both eGTP-C and eGTP-U shall be supervised.

9.1.3.9 GTPv2 header

The following are the requirements for the GTPv2 header:

1. In order to simplify the fall back to GTP v1, the Version field in the header shall indicate GTP version 2 (i.e. bits 6-8 of the Octet 1);

2. For GTPv2 – GTPv1 interworking at e.g. PGW, it is important that TEID identifies EPS bearer (SGW) / PDP context (pre-R8 SGSN). But TEID length shall be the same to make the handover seamless: when MME sends TEID to pre-R8 SGSN, the SGSN has to be able to read it right and send the Update message with TEID-C, and/or uplink G-PDU with TEID-U to PGW.

3. For the reliable delivery of GTP-C messages, GTPv2 messages for the control plane shall contain Sequence Number field. SN may be also put into the message body. CT4 should decide which way to go.

4. G-PDU across GTP-based S5/S8, S1-U and X2 interfaces have different requirements.

5. Control plane messages under GTP-U header (Echo, Error indication, End Marker, etc.) may have different requirements.

6. RAN3 required that G-PDU across X2 interface should contain PDCP Sequence Numbers. Need to send an LS to RAN3 how long the parameter should be.

7. RAN3 required that G-PDU across S1-U and X2 interfaces should support End Marker feature. CT4 has to select one out of two alternatives and inform RAN3 about it.

8. For the MBMS G-PDU RAN3 is discussing two alternatives. SYNC protocol is considered for single cell operation, which means at least putting a timestamp into GTP-U header. Need to send an LS to RAN3 about the format (length, etc.) and precision of the timestamp.

9. For harmonizing the optimized EPS-cdma2000 interworking with GTPv2, it should be considered if GTP-C header may also contain "S101 Transaction Identifier" (S101-TI). This IE however may be also put into the message body. Note: it is still open if cdma2000 IW will be based on GTPv2 based, or not.

10. GTPv2 should maintain useful GTPv1 header fields: Version (is a must), Message Type (most probably), Length (most probably), TEID (is a must).

11. Current assumption is that GTPv2 header shall be aligned to multiples of 4 octets. This is true at least for S1-U, GTP-based S5/S8, S10 and S11 interfaces.

12. CT4 has to decide if GTPv2 header can be 9 or 10 octets long across X2 interface.

13. CT4 has to decide if it would become possible to multiplex multiple T-PDU's of the same session under one GTP-U header?

14. GTPv2 should provide for the extension headers if in future the extension headers become necessary.

15. Below is a list of considerations for determining how many different lengths would be necessary for GTPv2 headers:

    a) G-PDU across GTP-based S5/S8: 8 or 5 or 7

    b) G-PDU across S1-U: 8 or 5 or 7

    c) G-PDU across X2 (PDCP SN): 9, 10 or 12. Another alternative without Length field would be 8 octets.

d) GTP-C: 8 octets if SN goes into body. Otherwise, it should be either 10 (if 4 octet alignment is not necessary in GTPv2) or 12 octets long.

e) GTP-U signalling (Echo and Error): 8 octets

f) GTP-U signalling (End Marker): 8 octets in case of new message type and same as G-PDU in ordinary case (see bullet point 14a).

g) MBMS G-PDU (SYNC protocol): for the timestamp at least 4 octets (12+ octets). We can't know if more IEs are coming from RAN3. All of them must be in the header. Anyway for MBMS packet size will typically be quite large and the header overhead is not critical.

h) GTP-C across S101: 9 octets or put TI into the body (8 octets). Perhaps more IEs are coming.

Summary:

- GTP-C including S101: 8 or 12. Fixed. But the semantics for 12 may be different.
- G-PDU: 8 octets and across X2 either 10 or 12 (if 4 octet alignment).
- MBMS G-PDU: either 8 or longer (FFS).

Octets	Bits 8	7	6	5	4	3	2	1
1	Version = 2			FFS				
2	Message Type							
3	Length (1st Octet)							
4	Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (4th Octet)							
9-n	The length and Content is determined by the value in bits 4-1							

Figure 9.1.3.9.1:" Generic format of GTPv2 header**"**

The following can be considered for specifying the usage of the Octet 1:

- Bit 5: Bit 5 is FFS.
- Bits 4 – 1: the value range 0 – 15 are used to specify 16 different flavours of the header (it is expected that the final decision on the usage of these bits will be reached by the next CT4 meeting):
  - Binary value 0 0 0 0, which means that GTP header is 8 octets long.
  - Binary value 0 0 0 1, which means that GTP header is 9 octets long. Octet 9 contains S101-TI.
  - Binary value 0 0 1 0, which means that GTP header is 9 octets long. Octet 9 contains PDCP SN.
  - Binary value 0 0 1 1, which means that GTP header is 12 octets long. Octet 9 contains S101-TI. Octets 10-12 are spare.
  - Binary value 0 1 0 0, which means that GTP header is 12 octets long. Octets 9-10 contain SN. Octets 11-12 are spare.
  - Binary value 0 1 0 1, which means that GTP header is 12 octets long. Octet 9 contains PDCP SN. Octets 10-12 are spare.
  - Binary value 0 1 1 0, which means that GTP header is 12 octets long. Reserved for FFS.
  - Binary value 0 1 1 1, which means that GTP header is n octets long. Octets 9-n contain one or more extension headers.

- Binary value 1 0 0 0, which means that GTP header is n octets long. Octets 9-n contain MBMS SYNC protocol IEs.
- Binary values 1 0 0 1 – 1 1 1 1 are spare and for future use.

Alternatively the octet 1 can reserve:

- A two bits field to encode the header length. One value meaning 8 octets, another 12 octets, and the other two to be defined based on the requirements above (possibly an additional size for X2 and or MBMS).
- A two or three bits field (depending on the need to keep the PT bit from GTPv1) encoding the meaning of the 9 to n octets for header sizes bigger than 8.

9.1.3.10 GTPv2 Message Types

Table 9.1.3.10.1: Messages types for GTPv2

Message Type value (Decimal)	Message	Reference	GTP-C	GTP-U
0	Reserved and shall not be sent. If received, shall be treated as an Unknown message.			
1	Echo Request		X	X
2	Echo Response		X	X
3	Version Not Supported		X	
4-30	Reserved for other protocols (e.g. S101, etc.)		X	
31	Create Default Bearer Request			
32	Create Default Bearer Response		X	
33	Delete Bearer Request		X	
34	Delete Bearer Response		X	
35	MME initiated Update Bearer Request		X	
36	Update Bearer Response sent to MME		X	
37-70	FFS		X	
71	Create Bearer Request			
72	Create Bearer Response		X	
73-254	FFS			
255	User plane data (payload). G-PDU			X

9.1.3.11 Information Element Types and Formats for GTPv2

9.1.3.11.1 Information Elements Type values for GTPv2

In order to have forward compatible type definitions for the GTPv2 information elements, all of them should be TLV coded.

Table 9.1.3.11.1.1: Information Elements Type values for GTPv2

IE Type Value	Format	Information Element	Reference
1-70	TLV	Reserved for other protocols (e.g. S101, etc.)	
71	TLV	AMBR	
72	TLV	Cause	
73	TLV	QoS Profile for EPS	
74	TLV	IMSI	

IE Type Value	Format	Information Element	Reference
75	TLV	PDN Address Allocation	
76	TLV	TEID-C	

9.1.3.11.2 AMBR

Aggregate Maximum Bit Rate (AMBR) is defined in 3GPP TS 23.003 [9]. For GTPv2 the value part of the AMBR is transparently copied to the Value field of the AMBR IE.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 71 (decimal)							
2-3	Length = n (decimal)							
4-(n-3)	Aggregate Maximum Bit Rate (AMBR)							

Figure 9.1.3.11.2.1: Aggregate Maximum Bit Rate (AMBR)

9.1.3.11.3 Cause

Cause IE coding is specified in Figure 9.9.1.3.11.3-1.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 72 (decimal)							
2-3	Length = 1 (decimal)							
4	Cause							

Figure 9.1.3.11.3.1: Cause

9.1.3.11.4 QoS Profile for EPS

The QoS Profile for EPS is defined in 3GPP TS 23.003 [9]. When GTP entity sends this IE, the value part of the QoS Profile is copied to the Value field of the GTP IE.

NOTE: QoS IE may contain Default QoS value.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 73 (decimal)							
2-3	Length = n (decimal)							
4-(n-3)	QoS Profile for EPS							

Figure 9.1.3.11.4.1: QoS Profile for EPS

9.1.3.11.5 IMSI

IMSI is defined in 3GPP TS 23.003 [9] and its coding is specified in 3GPP TS 24.008 [16] and in 3GPP TS 29.002 [17]. When GTP entity sends this IE, the value part of the received IMSI is transparently copied to the Value field of the GTP IE.

NOTE: Because of the historical reasons, the nibbles in each octet of the IMSI are swapped.

Example: IMSI = 01 23 45 67 89 12 34 5 is coded as:

10 32 54 76 98 21 43 F5.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 74 (decimal)							
2-3	Length = 8 (decimal)							
4-11	IMSI							

Figure 9.1.3.11.5.1: IMSI

9.1.3.11.6 PDN Address Allocation

The PDN Address Allocation is defined in 3GPP TS 23.003 [9]. When GTP entity sends this IE, the value part of the PDN Address Allocation is copied to the Value field of the GTP IE.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 75 (decimal)							
2-3	Length = n (decimal)							
4-(n-3)	PDN Address Allocation							

Figure 9.1.3.11.6.1: PDN Address Allocation

9.1.3.11.7 Tunnel Endpoint Identifier for Control Plane

The coding of the Tunnel Endpoint Identifier is specified in Figure 9.1.3.11.7-1.

Editor's note: It is FFS if TEID-C is used also for User plane.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 76 (decimal)							
2-3	Length = 4 (decimal)							
4-7	Tunnel Endpoint Identifier							

Figure 9.1.3.11.7.1: TEID-C

9.1.3.12 End Marker Packet

During the inter eNodeB handover the Serving GW shall send one or more "end marker" packets on the old path to the source eNodeB immediately after switching the path.

9.1.3.12.1 Alternative Solutions

9.1.3.12.1.1 Empty G-PDU

GTP-U packet with the same message type as G-PDU (which is 255 in GTP v1) and no payload is used to indicate the ‘’end marker" packet.

9.1.3.12.1.2 New Message Type

New and dedicated GTP-U message type is introduced for "end marker" packet.

9.1.3.12.2 Conclusions

New and dedicated GTP-U message type is introduced to indicate “end marker”. The "End Marker" message shall be sent for each GTPv2-U tunnel (multiple messages).

9.1.3.13 Reliable Delivery of Signaling Messages

As GTPv2 header is proposed to have sequence number the same way as GTPv1 header, the sequence number can be used to match requests with response messages as well as help the receiving end to differentiate between new requests and retransmitted ones.

In EPC, a node running GTPv2 may serve multiple sessions of a UE simultaneously. Even GTPv2 tunnel management messages could be operated on a per APN session base, signaling request can still be initiated from different directions and from different network nodes. This makes it possible for GTPv2 node to process several outstanding requests or responses from a same UE.

For the similarity of GTPv1 and GTPv2 transportation mechanism, the requirement of GTPv2 and GTPv1 of message confirmation and retransmission could be similar. The principles for reliable signaling delivery of GTPv1 shall also apply to GTPv2. However, there is no procedure that contains recursive GTP messages in legacy system. That is, no sending of GTPv1 response message depends on reception of any other GTP response message. As different from GTPv1, GTPv2 can be running over more network elements in EPC. GTP-C tunnel management message could be sent from MME to S-GW and then after processing on S-GW from S-GW to P-GW, or on a reverse path. The Serving GW shall only send signaling response message over S11/S4 interface after it receives the corresponding response message over S5-GTP/S8-GTP interface.

This is could be a problem if there is only one timer per procedure for GTP request messages in different nodes. Take "Create default bearer request" message in Attach procedure as an example. The message is sent from MME to S-GW, and then from S-GW to P-GW. In case network congestion occurs in the tunnel between S-GW and P-GW, and P-GW doesn't receive the request message within the timer defined, then S-GW would retransmit the request message. Yet as the timers of current GTP protocol are all the same, the MME GTP-C timer shall also be timeout for waiting the "Create default bearer response". This would cause message retransmission behavior even on a link without any problem. In case of a retransmission fails after the S-GW tried maximum times, the link between S-GW and P-GW shall be regarded as down. In this situation, the timer of retransmission between MME and S-GW would also timeout for the maximum times, a good link between S-GW and MME may also be treated as down. This is not reasonable for the MME as there may be bearers on this S-GW and the MME for other PDN GW(s). Moreover, the reason of the failure of connecting a PDN GW shall be reported to the MME. The MME, in Attach procedure for instance, may select another Serving GW or PDN GW for the UE based on the failure reason. Hence, the retransmission timer of the tunnel management message on MME shall be at least longer than that of S-GW to avoid a false deletion of bearer context in the MME.

This is also the case for Handover procedure with MME change. As illustrated in the following figure the inter eNodeB handover procedure with MME change, there are create bearer request/response pairs within the loop of a Forward relocation request/response message. Actually, there could be the case of a MME selected SGW is temporarily unreachable and another SGW would be selected. The timeout of a Create bearer request message in this case shall not affect the handover procedure to be continued. In such case, different timers shall be defined for retransmission of Forward relocation request message and Create Bearer request message to avoid the procedure is interrupted by the timeout of connecting to one SGW.

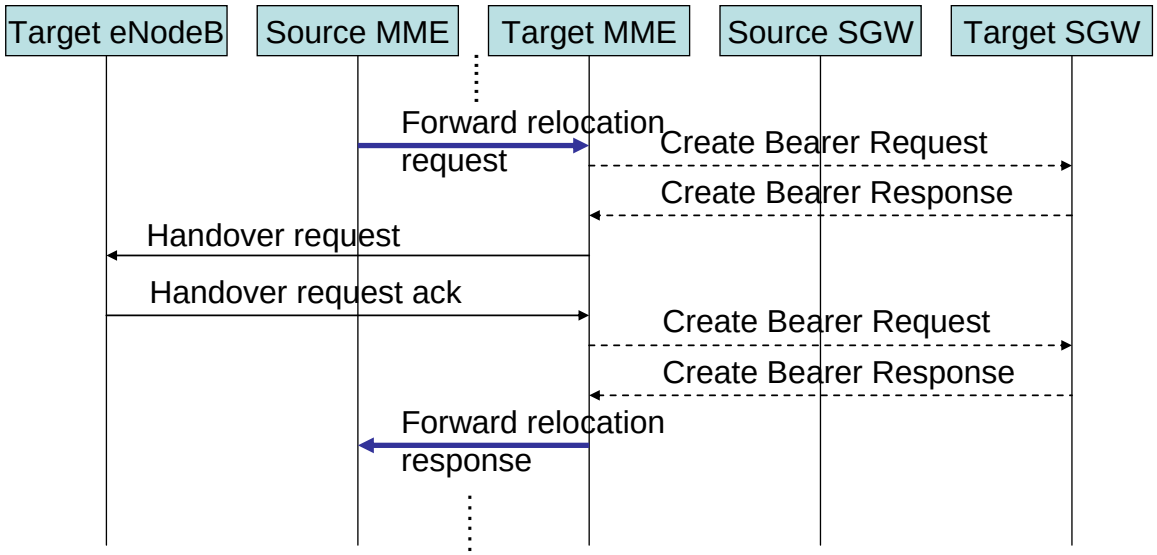

Figure 9.1.3.13-1: Inter eNodeB handover procedure with MME change

It is then necessary to have different timers for different GTPv2 message even in one procedure. There shall be at least 3 Timers for GTPv2, T301-RESPONSE for GTP-C tunnel management message on MME and PDN GW, T302-RESPONSE for GTP-C tunnel management message on Serving GW, T303-RESPONSE for GTP-C mobility management message like Forward relocation request.

For uplink signaling request, if the tunnel management message is sent over S4/S11 interface and then S5-GTP/S8-GTP interface, the timer of MME (SGSN) uplink GTP-C tunnel management message T301-RESPONSE shall be longer than the timer of Serving GW's uplink GTP-C tunnel management message T302-RESPONSE; while for downlink signaling request, the timer of PDN GW GTP-C tunnel management message shall be longer than the timer of Serving GW's downlink GTP-C tunnel management message T302-RESPONSE. Furthermore, the timer for mobility management message like Forward relocation request T303-RESPONSE shall be longer than the total wait time of the downlink tunnel management messages.

9.1.4 Conclusions

GTPv2 shall be used across S3, S4, GTP-based S5, GTP-based S8, S10 and S11 interfaces.

Editor's note: GTP version for Rel-8 Gn/Gp interfaces are FFS.

9.2 IP Fragmentation

Editor's notes: the background information and the detailed mechanism are to be clarified.

9.3 PDN GW address registration

9.3.1 General

Currently for inter-access handover, it is possible that the mobility management protocol is also changed, e.g. an UE uses GTP-S5 interface for non-roaming LTE access, and then moves to a non-3GPP access network and uses PMIP-S2 interface for access. From the view of PDN GW, the logic anchor is also changed, one is the GTP anchor, and the other is LMA.

For a PDN GW supporting both GTP and PMIPv6/DSMIPv6 protocol stack, to provide it with the same flexibility level of implementation as legacy GPRS architecture, the case should be allowed that the PDN GW's GTP-C address and its LMA/HA address can be different.

This clause is to discuss PDN GW address registration issue to meet the requirement above.

9.3.2 Candidates

9.3.2.1 Usage extended PDN GW's name

For PDN GW address retrieval, the target access network will get the PDN GW's logic name from the HSS/AAA. This name can be extended to include the mobility protocol information selected in the target side, e.g. Constructing the FQDN of the PDN GW to include the selected mobility protocol information in the suffix. And then the target access network can resolve the anchor's IP address via DNS service according to this FQDN with the mobility protocol suffix.

9.3.2.2 Providing protocol related anchor address(es)

For PDN GW address retrieval, the target access network can get the anchor's IP address according to the selected mobility protocol in the target side. And for PDN GW address registration, the PDN GW/MME should provide the anchor address (es) for each kind of supported mobility management protocols of the PDN GW to the HSS/AAA.

9.3.3 Conclusions

Editor's note: this section covers the conclusion for PDN GW address retrieve.

10 Subscriber Data related to EPC

10.1 General

This chapter will list and describe subscriber data stored in EPC.

NOTE: Subscriber data related to EUTRAN and PCC will be specified by RAN WGx and CT WG3 respectively.

10.2 Subscriber data stored in MME

The subscriber data stored in MME for a UE contains the UE's MM context and EPS bearer context information. Table 10.2-1 shows the context fields for one UE with the differences from TS23.401 highlighted.

Table 10.2-1: Subscriber data stored in MME

Field	Description	Descriptions on differences with TS23.401
IMSI	IMSI (International Mobile Subscriber Identity) is the subscriber's permanent identity.	
MM State	Mobility management state of a UE in MME, it could be ECM-IDLE, ECM-CONNECTED, EMM-DEREGISTERED.	
S-TMSI	Packet Temporary Mobile Subscriber Identity.	
IMEISV	Mobile Equipment Identity – (e.g. IMEI/IMEISV) Software Version Number	
Tracking Area Identity List	Current Tracking area Identity list	
Cell Global Identity	Last known cell	
Cell Identity Age	Time elapsed since the last Cell Global Identity was acquired	
Authentication Vector	Temporary authentication and key agreement data that enables an MME to engage in AKA with a particular user. An authentication vector consists of following elements: a) network challenge RAND, b) an expected response XRES, c) K_{ASME}, d) a network authentication token AUTN.	Original description of the authentication vector in 23.401 is " Temporary authentication and key agreement data that enables an MME to engage in AKA with a particular user. A quintet consists of five elements: a) network challenge RAND, b) an expected response XRES, c) a ciphering key CK', d) an integrity key IK', e) a network authentication token AUTN. (relation of K_ASME with CK' and IK' FFS)"
UE Radio Access Capability	UE radio access capabilities.	
UE Network Capability	UE network capabilities including security algorithms and key derivation functions supported by the UE	
Selected NAS Algorithm	Selected NAS security algorithm	
Selected AS Algorithm	Selected AS security algorithms.	
KSI_{ASME}	Key Set Identifier for the main key K_{ASME}	
K_{ASME}	Main key for E-UTRAN key hierarchy based on CK, IK and SN identity	Original description of this authentication is "Main key for E-UTRAN key hierarchy based on (CK' and IK' (FFS))"
NAS Keys and COUNT	K_{NASint}, K_{NASenc}, and NAS COUNT parameter.	
Selected CN operator id	Selected core network operator identity (to support network sharing).	
Recovery	Indicates if the HSS is performing database recovery.	
Access Restriction	The access restriction subscription information.	
ODB for PS parameters	Indicates that the status of the operator determined barring for packet oriented services.	
MME IP address for S11	MME IP address for the S11 interface (used by S-GW)	
MME TEID for S11	MME Tunnel Endpoint Identifier for S11 interface.	
S-GW IP address for S11	S-GW IP address for the S11 interface (used by MME)	
S-GW TEID for S11	S-GW Tunnel Endpoint Identifier for the S11 interface.	
eNodeB Address in Use	The IP address of the eNodeB currently used.	
eNodeB UE S1AP ID	Unique identity of the UE over the S1 interface within eNodeB.	
MME UE S1AP ID	Unique identity of the UE over the S1 interface within MME.	
QoS Profile Subscribed	Subscribed UE QoS Profile	
APN Restriction	Denotes the restriction on the combination of types of APN for the APN associated with this EPS bearer Context.	If this field shall be stored in HSS is FFS
Subscribed Charging	e.g. Normal, prepaid, flat rate and/or hot billing.	

Field	Description	Descriptions on differences with TS23.401
Characteristics		
For each active PDN connection:		
APN in Use	The APN currently used. This APN shall be composed of the APN Network Identifier and the APN Operator Identifier.	
APN Subscribed	The subscribed APN received from the HSS.	
IP Address and prefix	IPv4 address and IPv6 prefix	Update the IPv6 address to IPv6 prefix
VPLMN Address Allowed	Specifies whether the UE is allowed to use the APN in the domain of the HPLMN only, or additionally the APN in the domain of the VPLMN.	
PDN GW Address in Use (control plane)	The IP address of the PDN GW currently used for sending control plane signalling.	
Location Change Report Required	Need to communicate Cell or TAI to the PDN GW with this EPS bearer Context.	
For each EPS Bearer within the PDN connection		
EPS Bearer ID	An EPS bearer identity uniquely identifies an EP S bearer for one UE accessing via E-UTRAN	
S-GW IP address for S1-u	IP address of the S-GW for the S1-u interfaces.	
EPS Bearer QoS Profile	ARP, GBR, MBR, QCI	
EPS Bearer Charging Characteristics (Removed)		It is FFS if this field shall be removed as MME is no longer responsible for charging
Charging Id (Removed)		It is FFS if this field shall be removed as MME is no longer responsible for charging

Editor's Notes: the Removed mark is to indicate the parameters which are listed in TS23.401 but shall be removed from the subscriber data according to the up-to-date study of CT4

NOTE: The details of above subscriber data need to be further investigated and other subscriber data stored in MME is FFS.

10.3 Subscriber data stored in HSS

IMSI is the prime key to the data stored in the HSS. The data held in the HSS is defined in Table 10.3-1 here below with the differences from TS23.401/TS23.402 highlighted

Table 10.3-1: Subscriber data stored in HSS

Field	Description	Descriptions on differences with TS23.401/TS23.402
IMSI	IMSI is the main reference key.	
MSISDN	The basic MSISDN of the MS.	It is FFS whether it shall be applied in EPS 3GPP access.
IMEI / IMEISV	International Mobile Equipment Identity - Software Version Number	
Serving node ID(s)	The IP address of the MME and/or the SS7 number of SGSN currently serving this UE in 3GPP system or the IP address of the node serving the UE in non 3GPP system.	Original field for this parameter in TS23.401 is MME address. Original field for this parameter in TS23.402 is Serving node IP address
MS PS Purged from EPS	Indicates that the EMM and ESM contexts of the UE are deleted from the MME.	
ODB parameters	Indicates that the status of the operator determined barring	
Access Restriction	Indicates the access restriction subscription information.	remove the FFS in 23.401
APN-OI Replacement	Indicates the domain name to replace the APN OI when constructing the PDN GW FQDN upon which to perform a DNS resolution. This replacement applies for all the APNs in the subscriber's profile.	
Each subscription profile contains one or more APN configurations:		
Context Identifier	Context Identifier	
UE IP Address and prefix	Subscribed UE IPv4 Address and- IPv6 prefix	IPv6 address shall be updated to IPv6 prefix
Access Point Name	A label according to DNS naming conventions describing the access point to the packet data network.	
QoS Profile Subscribed	EPS subscribed QoS profile	
VPLMN Address Allowed	VPLMN Address Allowed	
Subscribed Charging Characteristics	e.g. Normal, prepaid, flat rate and/or hot billing.	The subscribed Charging Characteristics is listed for MME but not for HSS in 23.401. This is to add it into HSS data.
PDN GW address(es)	The IPv4 address and/or IPv6 address currently used for the PDN GW supporting this APN. It is FFS how to indicate whether the PDN GW address is subscribed as well as whether the subscribed PDN GW address is the same with the PDN GW address in use.	Original field name for this parameter in TS23.401 is "PDN GW address"

NOTE: The details of above subscriber data need to be further investigated and other subscriber data stored in HSS is FFS.

10.4 Subscriber data stored in S-GW

The Serving GW maintains the following EPS bearer context information for UEs. Table 10.4-1 shows the context fields for one UE with the differences from TS23.401/TS23.402 highlighted.

Table 10.4-1: Subscriber data stored in Serving Gateway

Field	Description	Descriptions on differences with TS23.401/TS23.402
IMSI	IMSI (International Mobile Subscriber Identity) is the subscriber permanent identity.	
Selected CN operator id	Selected core network operator identity (to support network sharing).	
MME TEID for S11	MME Tunnel Endpoint Identifier for the S11 interface	
MME IP address for S11	MME IP address the S11 interface.	
SGW TEID for S11	SGW Tunnel Endpoint Identifier for the S11 Interface.	
SGW IP address for S11	SGW IP address for the S11 interface	
For each PDN Connection:		
APN in Use	The APN currently used. This APN shall be composed of the APN Network Identifier and the APN Operator Identifier.	
UE IP Address and prefix	UE IPv4 address and IPv6 prefix	Change the IPv6 address to prefix
P-GW Address in Use (control plane)	The IP address of the P-GW currently used for sending control plane signalling.	
P-GW TEID for S5/S8 (control plane)	P-GW Tunnel Endpoint Identifier for the S5/S8 interface for the control plane.	
S-GW IP address for GTP-based S5/S8 (control plane)	S-GW IP address for the GTP-based S5/S8 for the control plane signalling.	
S-GW TEID for GTP-based S5/S8 (control plane)	S-GW Tunnel Endpoint Identifier for the GTP-based S5/S8 control plane interface.	
APN Restriction	Denotes the restriction on the combination of types of APN for the APN associated with this EPS bearer Context.	If this field shall be stored in HSS is FFS
For each EPS Bearer within the PDN Connection:		
EPS Bearer Id	An EPS bearer identity uniquely identifies an EPS bearer for one UE accessing via E-UTRAN	
UL TFT	Uplink Traffic Flow Template	
DL TFT	Downlink Traffic Flow Template	
PDN GW Address (user plane)	The IP address of the P-GW currently used for sending user plane traffic.	
PDN GW TEID for S5/S8 (user plane)	P-GW Tunnel Endpoint Identifier for the S5/S8 interface for the user plane.	
S-GW IP address for GTP-based S5/S8 (user plane)	S-GW IP address for user plane data received from PDN GW.	
S-GW TEID for GTP-based S5/S8 (user plane)	S-GW Tunnel Endpoint Identifier for the GTP-based S5/S8 interface for user plane.	
S-GW IP address for S1-u	S-GW IP address for the S1-u interface (Used by the eNodeB)	
S-GW TEID for S1-u	S-GW Tunnel Endpoint Identifier for the S1-u interface.	
eNodeB IP address for S1-u	eNodeB IP address for the S1-u interface (Used by the S-GW).	
eNodeB TEID for S1-u	eNodeB Tunnel Endpoint Identifier for the S1-u interface.	
QoS Profile in use	ARP, GBR, MBR, QCI.	
Charging Id	Charging identifier, identifies charging records generated by S-GW and PDN GW.	Remove the FFS from Charging Id
Charging Characteristics	Normal, prepaid, flat rate and/or hot billing	

Editor's Notes: the Removed mark is to indicate the parameters which are listed in TS23.401 but shall be removed from the subscriber data according to the up-to-date study of CT4

NOTE: The details of above subscriber data need to be further investigated and other subscriber data stored in HSS is FFS.

10.5 Subscriber data stored in P-GW

10.6 Subscriber data stored in ePDG

10.7 Subscriber data stored in 3GPP AAA Server

10.8 Subscriber data storage for EPC

Table 10.8.1: Overview of data used for EPC

PARAMETER	MME	HSS	S-GW	P-GW	ePDG	3GPP AAA Server	TYPE
IMSI	M	M	FFS	FFS	FFS	FFS	P
TA list	M	-	-	-	-	-	T
GUTI	C	-	-	-	-	-	T
Authentication Vector	C	M	FFS	-	FFS	FFS	T
Serving Node IP Address	-	M	-	-	-	FFS	T
MM State	M	-	-	FFS	FFS	FFS	T
IMEISV	C	C	-	FFS	FFS	FFS	T
Cell Global Identity	C	-	-	-	-	-	T
Cell Identity Age	C	-	-	-	-	-	T
UE Radio Access Capability	C	-	-	FFS	FFS	FFS	P
UE Network Capability	C	-	-	FFS	FFS	FFS	P
Selected NAS Algorithm	M	-	-	-	FFS	-	T
Selected AS Algorithm	M	-	-	-	FFS	-	T
KSI_{ASME}	M	-	-	-	FFS	-	T
K_{ASME}	M	-	-	-	FFS	-	T
NAS Keys and COUNT	M	-	-	-	FFS	-	T
Selected CN operator id	C	-	C	FFS	FFS	FFS	T
Recovery	C	-	-	FFS	FFS	FFS	T
Access Restriction	C	C	-	FFS	FFS	FFS	P
ODB for PS parameters	C	C	-	FFS	FFS	FFS	P
MS PS Purged from EPS	-	C	-	FFS	FFS	FFS	T
MME IP address for S11	C	-	C	-	-	-	T
MME TEID for S11	C	-	C	-	-	-	T
MME UE S1AP ID	C	-	-	-	-	-	T
S-GW IP address for S11	C	-	C	-	-	-	T
S-GW TEID for S11	C	-	C	-	-	-	T
S-GW IP address for GTP-based S5/S8 (control plane)	C	-	C	FFS	-	-	T
S-GW TEID for GTP-based S5/S8 (control plane)	C	-	C	FFS	-	-	T
S-GW IP address for S1-u	C	-	C	FFS	-	-	T
S-GW TEID for S1-u	C	-	C	FFS	-	-	T
S-GW IP address for GTP-based S5/S8 (user plane)	-	-	C	FFS	-	-	T
S-GW TEID for GTP-based S5/S8 (user plane)	-	-	C	FFS	-	-	T
eNodeB Address S1-MME	C	-	-	-	-		T
eNodeB UE S1AP ID	C	-	-	-	-	--	T
eNodeB IP address for S1-u	-	-	C	-	-	-	T
eNodeB TEID for S1-u	-	-	C	-	-	-	T
QoS Profile Subscribed	M	M	-	-	FFS	FFS	P
QoS Profile in use	C	-	C	FFS	FFS	FFS	T
APN Restriction	FFS	-	FFS	FFS	FFS	FFS	T
Subscribed APN	M	M	-	-	-	FFS	P
APN in use	C	C	-	FFS	FFS	FFS	T
APN-OI Replacement	-	C	-	FFS	FFS	FFS	P
Context Identifier	-	M	-	FFS	FFS	FFS	P
UE IPv4 Address and IPv6 prefix	C	C	C	FFS	FFS	FFS	T

PARAMETER	MME	HSS	S-GW	P-GW	ePDG	3GPP AAA Server	TYPE
Location Change Report Required	C	-	-	FFS	FFS	FFS	T
VPLMN Address Allowed	C	C	-	FFS	FFS	FFS	P
PDN GW Address Subscribed	-	C	-	FFS	FFS	FFS	P
PDN GW Addess (control plane)	C	C	-	FFS	FFS	FFS	T
PDN GW Address (user plane)	C	-	C	FFS	FFS	FFS	T
PDN GW TEID for S5/S8 (user plane)	C	-	C	FFS	FFS	FFS	T
PDN GW TEID for S5/S8 (control plane)	-	-	C	FFS	FFS	FFS	T
EPS Bearer ID	C	-	C	FFS	-	-	T
UL TFT	-	-	-	FFS	-	-	T
DL TFT	-	-	C	FFS	-	-	T
Charging Id	-	-	C	FFS	FFS	FFS	T
Charging Characteristics	-	M	C	FFS	FFS	FFS	P

NOTE: For the definition of M (=mandatory), C (=conditional), P (=permanent) and T (=temporary) in the table, refer to TS 23.008 [11] section 4 and whether the subscriber data attributes in TS 23.008 should be reused or new definition of attributes should be introduced is FFS.

11 Conclusion

Annex A: Network scenarios for all kinds of PS related HSS/HLR

The following section is to describe all kinds of PS related HSS/HLR and their corresponding implementation scenarios.

Rel-8 HLR:

This scenario is related to operators which only launch Rel-8 UTRAN/GERAN and do not use EPS. The scenario for a Rel-8 HSS for GPRS/UMTS only is described as below.

Editor's note: It is to be decided by SA2 whether this network scenario is a part of the Rel-8 network architecture and whether Rel-8 GGSN will exist.

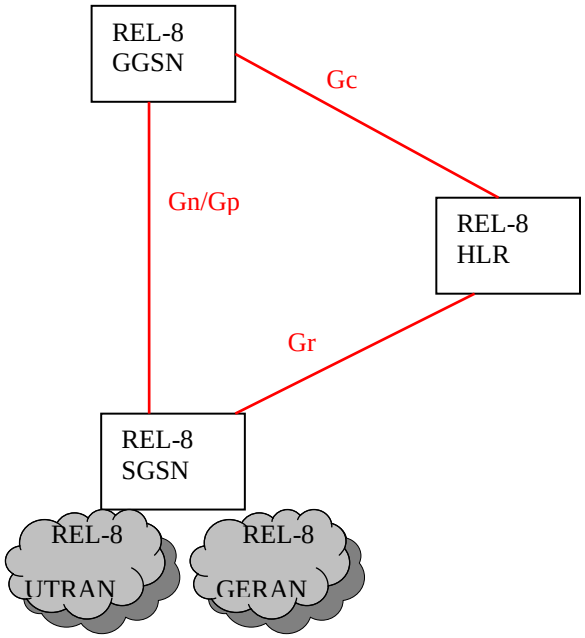

Figure A.1: Scenario for Rel-8 HLR

Rel-8 HSS:

This scenario is related to operators which launch both Rel-8 UTRAN/GERAN and E-UTRAN. The scenario for a Rel-8 HSS for EPS is described as below.

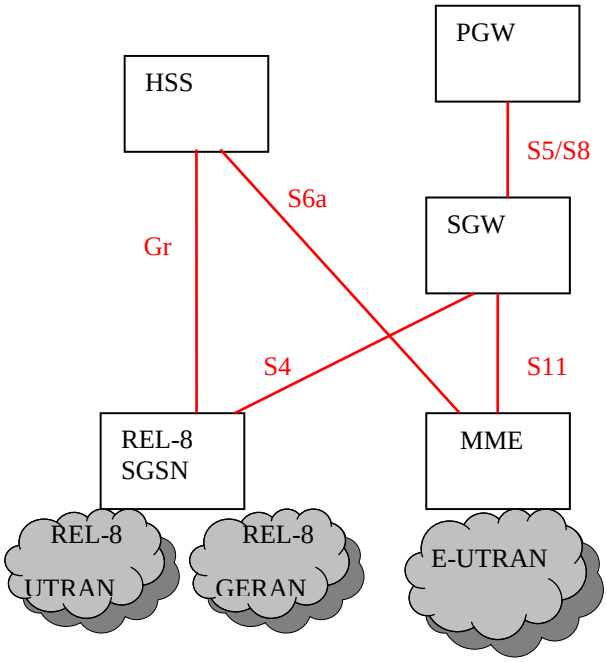

Figure A.2: Scenario for Rel-8 HSS

Rel-8 HSS-IMS:

This scenario is related to operators which launch both Rel-8 UTRAN/GERAN and E-UTRAN upgrading existing HSS functionalities or launch only REL-8 UTRAN/GERAN and like to use EPS as the core network. The scenarios for a Rel-8 HSS without supporting S6a for EPS are described as below.

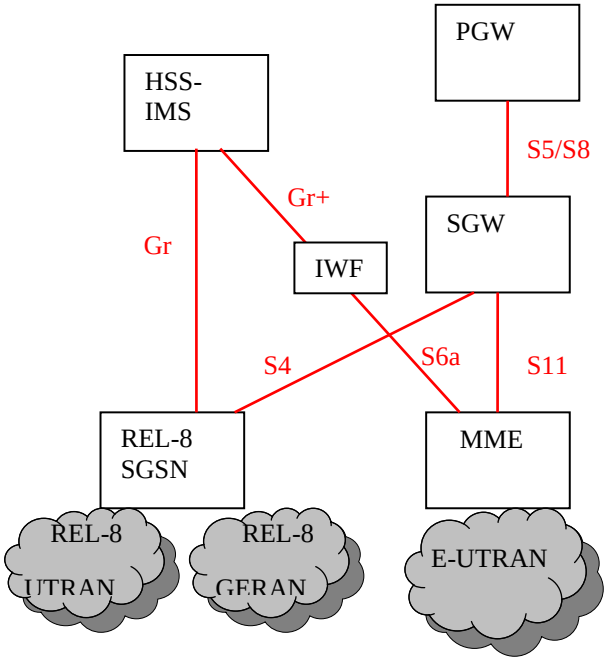

Figure A.3-1: Scenario for Rel-8 HSS-IMS for both Rel-8 UTRAN/GERAN and E-UTRAN

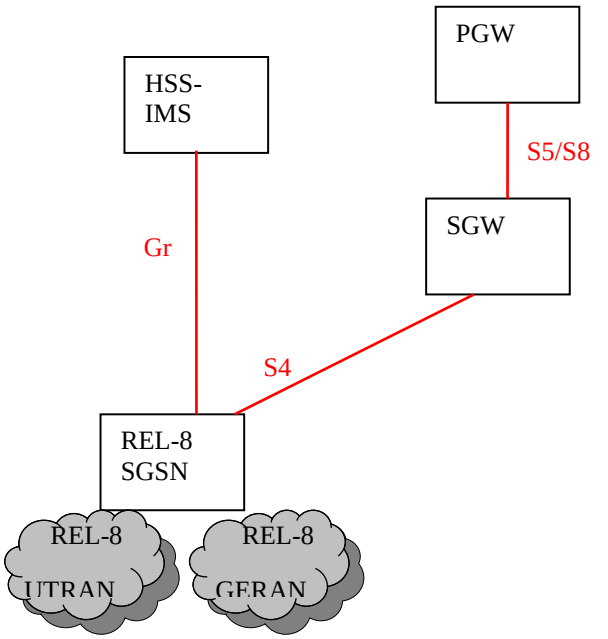

Figure A.3-2: Scenario for Rel-8 HSS-IMS for EPS, for Rel-8 UTRAN/GERAN only

Rel-8 HSS-EPS

This scenario is related to operators which directly launch E-UTRAN at some new market and use EPS as the core network. The scenario for a Rel-8 HSS-EPS (without MAP based interfaces for EPS) is described as below.

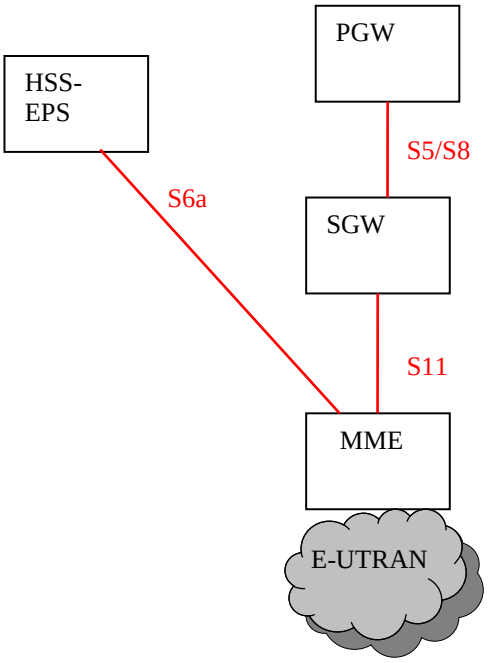

Figure A.4: Scenario for Rel-8 HSS-EPS

Pre Rel-8 HLR:

This scenario is related to operators which launch pre Rel-8 UTRAN/GERAN. The scenario for a pre Rel-8 HLR is described as below.

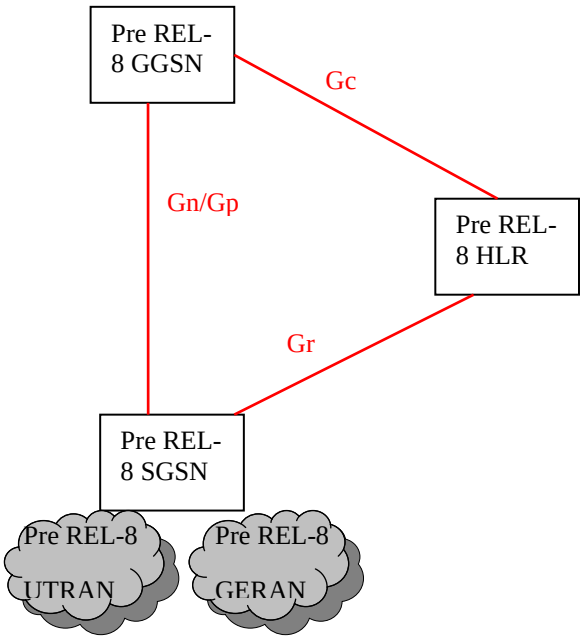

Figure A.5: Scenario for Pre REL-8 HLR

Annex B: Effect from ISR

The following section is to describe ISR principles and its effect from CT4 point of view.

Editor's note: There are still some little open issues about ISR in SA2, so the analysis below may be updated. But when ISR is stable in CT4, this annex will be removed.

ISR principles

ISR has the following principles:

- UE registers to the MME and SGSN separately; MME and SGSN register to the HSS and the HSS maintain two PS registrations; HSS keeps double registration for MME and SGSN

When ISR is activated, UE registers to the MME and SGSN and HSS keeps two PS registrations. When ISR is not activated, UE is either registers to MME or to SGSN (attached in one node while detached in the other node), but HSS also keeps double registrations in order to reuse the security context information in MME or SGSN, and the frequency of security information retrieval from HSS on S6a will be decreased .

If double registration principle applies, whether ISR is activated or not, when MME or SGSN sends update location message to HSS, HSS only initiates the Cancel Location procedure to the old entity of the same RAT. Otherwise, if single registration principle applies, when MME or SGSN sends update location message to HSS with Update Type setting to "single registration", HSS shall initiate the Cancel Location procedure to the both of the old entities.

Note: When a UE moves from a R8 SGSN with ISR activated into an area served by a pre REl-8 SGSN, the HSS will keep the MME registration.

- UE needs to be informed by the CN nodes (SGSN and MME) if the ISR functionality is activated or deactivated for that UE; The Serving GW needs to be informed if the ISR functionality is activated or deactivated for a UE;

ISR status is decided by the negotiation between SGSN and MME and the result needs to be informed to the UE and S-GW. So that UE, SGSN, MME and S-GW all know the ISR status (activated or deactivated).

- There is no "signaling free reselection" of an E-UTRAN cell by a UE in URA_PCH state (e.g. URA_PCH is treated as active mode by the UE/EPC when moving to E-UTRAN);

When URA_PCH state UE selects an E-UTRAN cell, the UE shall initiate TAU procedure immediately and the Iu connection in UTRAN is required to be released by the context request/response/ACK message from MME or Cancel Location message from HSS (the cancel location is related to principle 6). With this mechanism, the Iu connection in UTRAN can be released correctly.

- When ISR is activated for 2G and/or 3G, Idle Mode UP Termination is in S-GW for that RAT;

When ISR is activated, idle mode user plane termination is in S-GW and S-GW shall initiate the paging notification to both MME and SGSN simultaneously. With this method, the paging coordination with ISR active will be unified and simplified (such as user plane handling).

- Two periodic update timers, running separately in the UE for updating SGSN and MME separately; Functionality is needed (FFS) in SGSN and MME to avoid the deletion of the PDP context/EPS Bearers because of missing periodic updates.

There are two separate Periodic Update Timers in UE and SGSN/MME if ISR is activated, so when the Timer in one RAT is expired, it is not necessary to inform the other RAT. And special mechanism is required to avoid MME or SGSN implicitly detach the UE due to the expiration of Timer while the UE camps in the other RAT.

- When a UE moves from a Pre-8 SGSN to MME, the SGSN registration at HSS is cancelled.

It is just an exception to the double registration principle because when P-R8 URA_PCH state UE selects an E-UTRAN cell, the Iu connection in UTRAN will not be released unless the SGSN receives the cancel location message from HSS. R7-SGSN will not support extended context request/response/Ack to release Iu connection, so the SGSN registration at HSS shall be cancelled.

- The UE shall maintain an internal update type status and provide TIN (Temporary Identity used in Next update) in the TAU/RAU request according to the internal update type status. If the UE holds valid TMSI information of

the access system, the UE indicates it as additional TMSI information, regardless whether the TIN is identical with the additional TMSI.

Effect on CT4

Based on the above principles, what will ISR feature bring to the protocol definition in CT4:

- For GTP related interfaces:
  * ISR activation and deactivation is realized by GTP message on S3, e.g. "Context Request/Response/Ack". The TAU/RAU procedure may involve ISR activation/deactivation. "Context Response" message shall indicate whether support ISR or not and "Context Ack" message shall indicate whether ISR is activated or not. This is related to principle 2
  * S-GW is conscious of the ISR status also by GTP message on S11 or S4, e.g. the "Update Bearer Request" message from SGSN/MME to S-GW shall indicate ISR status (activated or deactivated). This is related to principle 2.
  * Some new GTP messages shall be added to support the ISR feature. New "Detach Indication" message on S3 is added to support the detach coordination between SGSN and MME when ISR is activated. New "Stop Paging" message on S4/S11 is added to support the paging coordination. This is related to principle 4.
  * During "Service Request" procedure if the RAT Type has changed compared to the last reported RAT Type, the Serving GW shall send the Update Bearer Request message (RAT Type) to the PDN GW.
- For S6a: When a UE that is registered with a Pre-Rel-8 SGSN selects an E-UTRAN cell, TAU will be performed and MME shall indicate "single registration" to HSS. Without this indication, HSS shall always keep double registrations. This is related to principle 1, 6.

Annex C: General DNS Based Node Selection Description

Editor's note: This clause will describe general principles of using various DNS resource records for EPC node discovery and selection based on desired service and protocol.

C.1 Domain Name Structure for EPC

Editor's note: The normative definitions of identifiers in this section could be placed in 3GPP TS 23.003 [9].

C.1.1 Upper level domain name

At least for the non-roaming case the sub-domain name to place new types of DNS records [19][20] should clearly be under

3gppnetwork.org

For "public" node usage or for UE usage the following would normally be used

pub.3gppnetwork.org

See 3GPP TS 23.003 [9] and GSMA IR 67 [21] for the conventions of these sub-domains.

For the roaming case "3gppnetwork.org" would also be desirable but requires discussion with GSMA

The records being provisioned are actually records that an operator would provision under their own authority. Hence, the domains employed here use pattern:

mnc<MNC>.mcc<MCC>.3gppnetwork.org

and for UE or other "public" usage

mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

following the format of 3GPP TS 23.003 [9] and GSMA IR 67 [21].

In order to avoid problems with name collisions with existing zone cuts under mnc<MNC>.mcc<MCC>.3gppnetwork.org and also to provide for cleanly adding future extensions a new zone cut under this is suggested for new Release 8 DNS usage for EPC node discovery and node naming.

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

and if needed

epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

The "epc" could be any label and this choice is subject to GSMA approval.

Note this is the same approach as used for the 3GPP IMS and WLAN zone cuts

ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org

wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org

as well as other existing usages (see more examples in GSMA IR 67 [21]).

Within this "epc" zone cut another cut will be added by 3GPP when a new function is added to give clear separation in the name spaces. At this time the next level zone cuts under "epc" proposed are

Table C.1-1: Zone cuts under epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

Zone cut	Usage
apn.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org	APN usage in release 8
tac.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org	TAI related records
mme.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org	MME node and MME pool
nodes.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org	Operators usage

Other zone cuts under epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org are reserved for future usage.

C.1.2 APN fully qualified domain name

The existing APN concept will still be used in release 8 networks based on TS 23.401 [2]. The current full APN format, from 3GPP TS 23.003 [9] is of form

<APN-NI>.mnc<MNC>.mcc<MCC>.gprs

and obeys the rules established in 3GPP TS 23.003 [9] and continues to be the normative authority for APN format. This APN string will continue to be used in charging, HSS data structures and many other records due to the need to have the APN usage be backwards compatible to pre-release 8 nodes.

Due to the need to support pre-release 8 the existing A/AAAA records will still need to be provisioned at <APN-NI>.mnc<MNC>.mcc<MCC>.gprs. These records are for the "Gn/Gp" interfaces. These A/AAAA records will not be used by release 8 nodes towards release 8 capable networks.

While it is technically possible to place the new DNS records at the APN string it has also been agreed with IETF not to have new usages of ".gprs" see 3GPP TS 23.003 [9] and GSMA IR 67 [21]. Hence, the existing APN string is transformed for actual DNS query usage to the following fully qualified domain name

<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The fully qualified domain name above using 3gppnetwork.org above is NOT stored in HSS or other locations other than DNS functions.

Again this choice is subject to approval with GSMA especially in regards to roaming interfaces.

C.1.3 Tracking Area Identity fully qualified domain name

The TAI is a critical identifier for mobility in the same manner as the NRI, RAC and LAC are critical in 3GPP U-TRAN and GPRS networks.

The Tracking Area Identity (TAI) consists of a TAC code, MNC and MCC from 3GPP TS 23.401 [2].

Domain name for the tracking area is

<tac-low-byte>.<tac-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The TAC is a 16 bit integer. <tac-high-byte> is the hexadecimal string of the most significant byte in the TAC and <tac-low-byte > is the hexadecimal string of the least significant byte.

NOTE: The two labels within TAC are employed to allow easier use of wild cards which may be desirable in a network with thousands of TAI.

C.1.4 MME node fully qualified domain name

The MME within an operators network is identified with the MME group ID (MMEGI) which identifies an MME pool area and the MMEC which identifies an MME within the MME pool. This information is encoded in the GUTI that is assigned to a UE and the old GUTI will be available in a target eNodeB/target MME during mobility procedures. Currently 3GPP has not defined that DNS will be used however when a target MME needs to contact a source MME in a different MME pool the target MME will have the old GUTI so the DNS records based on this FQDN is likely to be required.

The MME node fully qualified domain names are therefore

mmec<mmec>.mmegi<mmegi>.mme.epc.mnc<mnc>.mcc<mcc>.3gppnetwork.org

Where the <mmec> and <mmegi> are MMEC and MMEGI as hex.

The following fully qualified domain name is used for the MME pool itself

mmegi<mmegi>.mme.epc.mnc<mnc>.mcc<mcc>.3gppnetwork.org

C.1.5 Operator usage zone cut

The following zone cut is given back to the operator for their own usage

nodes.epc.mnc<mnc>.mcc<mcc>.3gppnetwork.org

This is simply to allow an operator to place any records they chose under this zone while still being under the authority of epc.mnc<mnc>.mcc<mcc>.3gppnetwork.org (i.e. may simplify security aspects)

C.2 Resource Records

Editor's note: This subclause will list and describe used DNS RRs [20] and their intended use.

C.3 Identifying Nodes, Services and Protocols

C.3.1 Introduction to RFC 3958

IETF RFC 3958 [26] is designed to find a set of servers for a particular service(s) at a domain name.

For more details see IETF RFC 3401 [22], IETF RFC 3402 [23], IETF RFC 3403 [24], IETF RFC 3404 [25] and IETF RFC 3958 [26]. Especially important is IETF RFC 3958 section 2.2 [26] and IETF RFC 3402 section 3.3 [23].

The input to the IETF RFC 3958 [26] procedure is a fully qualified domain name and a list of (Service, Protocol) name pairs.

The output of the IETF RFC 3958 [26] procedure is the "best" SRV or A/AAAA record set that matches one or more of the input "Service/Protocol" names. SRV is the preferred output for functional reasons but A/AAAA records are allowed if the goal is to reduce number of DNS queries. The "best" fit is based first on the "order" field in the NAPTR records and secondarily on the preference field as per RFC 3402 [23] (and RFC 3958 [26]). The procedure can continue to alternate choices as well if needed due to failure.

The procedure allows an operator to specify "priority/preferences" for service types as well as priority and weight for interfaces within the service. There are also well defined fallback nodes (assuming more than one node is provisioned in the record).

Once a node implements the IETF RFC 3958 [26] procedure it can be reused with different inputs to select different server types. The usages so far introduced are given in section **Error! Reference source not found.**. The "service" input is summarized in section 0 for easier reference.

Editor's Note: The NAPTR preference field is currently poorly utilized in RFC 3958 [26] and other NAPTR procedures and could be defined as a statistical weight to avoid the need to use SRV for statistical weights. I.e. weight = (65535-"NAPTR preference"). This is for FFS.

C.3.2 IETF RFC 3958 Service and Protocol service names for 3GPP

To identify a "service" in IETF RFC 3958 [26] we need to have a list of standardized "service-parms" names. See section 6.5 of IETF RFC 3958 [26].

The following tables is one possible assignment of those names

Table C-3.2-1 List of 'app-service' and 'app-protocol' names

Description	IETF RFC 3958 section 6.5 'app-service' name	IETF RFC 3958 section 6.5 'app-protocol' name
PGW and interface types supported by the PGW	x-3gpp-pgw	x-s5-gtp , x-s5-pmip, x-s8-gtp , x-s8-pmip
SGW and interface types supported by the SGW	x-3gpp-sgw	x-s5-gtp , x-s5-pmip, x-s8-gtp , x-s8-pmip, x-s11, x-s12, x-s4
GGSN	x-3gpp-ggsn	x-gn, x-gp
SGSN	x-3gpp-sgsn	x-gn, x-gp, x-s4,x-s3
MME and interface types supported by the MME	x-3gpp-mme	x-s10 , x-s11, x-s3, x-s6a, x-s1-mme

Table C-3.2-2 List of 'app-service' and 'app-protocol' names proposed to be used in the IETF RFC 3958 [26] procedures for 3GPP core network node selection. Note that greyed out names are not used yet in an EPC DNS procedure.

NOTE: The formats follows RFC 3958 [26] experimental format. 3GPP could use approved names under RFC 3958 [26] by publishing a new informational RFC defining the names. Above table assumes x-s5-gtp refers to udp based GTP control plane. If other transports are possible then names would include transport x-s5-gtp-tcp, x-s5-gtp-sctp etc.

For example, to find the S8 PMIP interfaces on a PGW the 'service parameter' of

3gpp-pgw:x-s8-pmip

would be used as input in the IETF RFC 3958 [26] procedure.

C.3.3 Identification of node names

There are many use cases where it is desirable to select a collocated node in preference to a non-collocated node. To easily do this action a "canonical" node name is to be employed so that the "canonical" node names from two or more sets of records can be compared to see if nodes are actually the same nodes.

In DNS neither A or AAAA record names, in general, represent a host name instead these are a set of "equivalent" interfaces. A node may need to have more than one host name for the simple reason that it can have different interfaces for different purposes. For example, a node can have a set of roaming interface on a completely different network than the internal network due to security needs. Hence, there are always situations where multiple A/AAAA record sets must exist, which implies multiple distinct host names. Therefore, host names, in general, cannot be used as node names.

Instead of creating new DNS records to map a host name to a node name (such as a NAPTR record with the "u" flag [27], or a "fake" PTR record) a restriction is placed on how host names will appear in the IETF RFC 3958 [26] procedure as used in 3GPP.

The host names shall have form

<single-label-interface-name> . <canonical-node-name>

For example the node names are in bold for the following examples.

Eth-0.**pgw32.company.com**

S8.**sgw32.company.com**

vip.**east33.company.com**

board3.**gw4.west.company.com**

Interface names and node names do NOT identify a function in the procedures here.

NOTE: The interface is part of the natural hierarchy within a node and the host name is already returned with the existing DNS records. The approach here is believed to be simpler and more logical to maintain than additional DNS records.

Specifically, the naming restriction shall be placed only on all targets pointing to A/AAAA record sets from the IETF RFC 3958 [26] procedure. This restriction does NOT apply to any other records the operator may be using.

NOTE: The NAPTR with flag "a" will have a target pointing to the A/AAAA record directly so the restriction is on the NAPTR record with flag "a". For the flag "s" case the restriction is on the targets in the SRV record not the NAPTR record. The operator is free to use PTR or CNAME records after this point so the actual A/AAAA record naming is actually unrestricted though the proposed naming format could be identical to what is normally used.

C.3.4 Services from node names

There are potential use cases where a node has a logical name of a peer but does not have the protocols it supports. The DNS NAPTR records for any of the services in the above table can be provisioned at the nodes logical name. This allows any peer to discover the available services of any other peer based on logical name.

C.4 Procedures for EPC Node Discovery and Selection

Editor's note: This clause will contain the description of the DNS procedures used for discovering and selection EPC nodes.

C.5 Procedures for Discovering and Selecting a PGW

Editor's note: This subclause will contain the DNS procedures for discovering and selecting a PGW under various scenarios.

C.5.1 Discovering a PGW for a 3GPP Access

C.5.1.1 General

The procedures here give a list of possible PGW and their interfaces that serve a particular APN. This is very similar to the existing function that gives the GGSN IP address based on an APN.

However, the release 8 behavior must include more functionally than pre-release 8 systems. Primarily, since the PDN-GW now can support more than one protocol and secondarily there is a desire to have the PGW and SGW collocated whenever possible. New DNS records are required to distinguish between different protocols and interfaces and assist in the more complicated selections needed.

C.5.1.2 Discovering a PGW for a 3GPP Access - S8/Gp roaming case

Assuming the SGW is in the visiting network and the APN to be selected is in the home network then the IETF RFC 3958 [26] procedure is started with "Service Parameters" of

"x-3gpp-pgw:x-s8-gtp", "x-3gpp-pgw:x-s8-pmip", "x-3gpp-ggsn:x-gp"

and the first NAPTR lookup starts at

<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The IETF RFC 3598 [26] NAPTR procedure then returns either an SRV record set or a A/AAAA record set. The records are then used to contact the node (using the statistical weights in the SRV record set as per IETF RFC 2782 [27] and random selection within the A/AAAA record sets).

The above procedure is used by the MME to select the PGW. Note that the GGSN records would be used in case there was no PGW for that APN.

The PGW and SGW cannot be collocated in this case since the SGW and PGW are in different operator networks. This makes the DNS procedure actually easier than the non-roaming case.

In the above procedure the selected PGW node name, port and selected type (GTP vs PMIP) must be stored in the MME on a PDN basis. It is for FFS if the IP address is also stored separately.

3GPP TS 23.401 [2] currently indicates only one of PMIP or GTP will be used based on roaming agreements so the above query would actually not require both gtp and pmip. The operator could use the order field in the NAPTR records to accomplish a optional fallback to the other protocol type.

C.5.1.3 Discovering a PGW for a 3GPP Access - S5/Gn intra-operator existing PDN

Assuming the SGW is already selected and fixed by having an existing PDN connection and a UE attempts to create a new PDN connection for a different APN in the users home network then the MME will perform the following procedure.

The IETF RFC 3958 [26] procedure is started with "Service Parameters" of

"x-3gpp-pgw:x-s5-gtp", "x-3gpp-pgw:x-s5-pmip", "x-3gpp-ggsn:x-gn"

and the first NAPTR lookup starts at

<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The IETF RFC 3598 [26] NAPTR procedure then returns either an SRV record set or a A/AAAA record set.

Before proceding the record set is inspected and the node names are extracted from the target names by removing the first label. Any PGW records that match the current SGW node name (the SGW node name was previously stored with the other PDN in the MME) are to be used first since those are PGW interfaces that are collocated with the current SGW.

The DNS records are then used to contact the PGW node (using the statistical weights in the SRV record set and random selection within the A/AAAA record sets but respecting the collocated records being first in the selection process and using the same protocols supported by the current SGW (gtp vs pmip)).

NOTE: The GGSN records would be used in case there was no PGW for that APN.

C.5.1.4 Discovering a PGW for a 3GPP Access - S5/Gn intra-operator initial attach

Assuming an initial attach with PDN creation in 3GPP access then the PGW and SGW are both to be selected.

The IETF RFC 3958 [26] procedure is started with "Service Parameters" of

"x-3gpp-pgw:x-s5-gtp", "x-3gpp-pgw:x-s5-pmip", "x-3gpp-ggsn:x-gn"

and the first NAPTR lookup starts at

<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The IETF RFC 3958 [26] NAPTR procedure then returns either an SRV record set or a A/AAAA record set.

The procedure here is only a pre-selection of PGW candidates. This is generally required since the possible SGW that can serve the cell the UE is in must be found before it is possible to see if any of the preferred combined PGW/SGW can serve both the cell the UE is in and the selected APN at the same time.

The DNS output data has to be "saved" here and the RFC 3958 [26] procedure is "frozen" for later use in case of failures. The procedure here will therefore be completed in the PGW/SGW node selection section after SGW selection has been covered.

There is the special case of one SGW service area where all SGW will serve every cell and it is in theory enough to see if the PGW has any SGW collocated. This could be handled as a separate case. However, this is covered with an optimization in the general SGW selection rather than here.

Editor's note: This section will be updated with the reference to the combined PGW/SGW selection procedure.

C.5.2 Discovering a PGW for a non-3GPP Access with Network Based Mobility Management

Editor's note: This subclause will contain the DNS procedures for discovering a PGW in case of S2a and S2b interfaces, if DNS interactions are needed.

C.6 Procedures for Discovering and Selecting a SGW

Editor's note: This subclause will contain the DNS procedures for discovering and selecting a SGW under various circumstances where a PGW is already selected including a roaming UE, TAU, creating a second PDN connection , etc.

C.7 Procedures for Discovering and Selecting a PGW and SGW Simultaneously

Editor's note: This subclause will contain the DNS procedures for discovering and selecting a SGW at the same time under various circumstances including the home UE initial attach.

C.8 Procedures for Discovering and Selecting a MME

Editor's note: This subclause will contain the DNS procedures for discovering and selecting a MME under various circumstances including when a source MME selects a target MME during Inter eNodeB handover with MME relocation.

C.9 DNS Examples (Informative)

Editor's note: This subclause will contain DNS record examples for illustration and elaboration.

Annex D:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2007-02					Draft skeleton	-	0.0.0
2007-02					Skeleton + scope	0.0.0	0.1.0
2007-05	CT4 #35		-	-	Inclusion of documents agreed at CT4 #35: C4-070842, C4-070843, C4-070844, C4-070845, C4-070846, C4-070847, C4-070848, C4-070849, C4-070850, C4-070853, C4-070880, C4-070881, C4-070882	0.1.0	0.2.0
2007-08	CT4#36		-	-	Inclusion of documents agreed at CT4#36: C4-(071346, 1208, 1201, 1204, 1205, 1207, 1002, 1209, 1210, 1211, 1212, 1213, 1214, 1216, 1154, 1155, 1200, 1331, 1199, 1332, 1350, 1239, 1334, 1242, 1325, 1335)	0.2.0	0.3.0
2007-10	CT4#36 bis		-	-	Inclusion of documents agreed at CT4#36bis: C4-07(1524, 1612, 1610, 1400, 1401, 1526, 1613, 1413, 1529, 1415, 1616, 1591, 1406, 1459, 1617, 1584, 1535, 1497, 1532)	0.3.0	0.4.0
2007-11	CT4#37		-	-	Inclusion of documents agreed at CT4 #37: C4-071749, C4-071851, C4-071872, C4-071900, C4-071904, C4-071905, C4-071906, C4-071908, C4-071909, C4-071916, C4-071924, C4-071925, C4-071926, C4-071929, C4-071930, C4-071998, C4-072016, C4-072029, C4-072047	0.4.0	0.5.0
2008-02	CT4#38		-	-	Inclusion of documents agreed at CT4 #38: C4-080072, C4-080089, C4-080090, C4-080092, C4-080094, C4-080095, C4-080099, C4-080100, C4-080101, C4-080102, C4-080104, C4-080106, C4-080108, C4-080109, C4-080110, C4-080117, C4-080118, C4-080120, C4-080229, C4-080230, C4-080285, C4-080289, C4-080327, C4-080342, C4-080365, C4-080366, C4-080367, C4-080371, C4-080372, C4-080373, C4-080376, C4-080392, C4-080397, C4-080398, C4-080399, C4-080400, C4-080401, C4-080402, C4-080403, C4-080404, C4-080408, C4-080411, C4-080412, C4-080413, C4-080414, C4-080415, C4-080416, C4-080417, C4-080418, C4-080419, C4-080421, C4-080439, C4-080538, C4-080540, C4-080541, C4-080543, C4-080545, C4-080551, C4-080561, C4-080562	0.5.0	0.6.0
2008-03					Editorial changes based on 3GPP drafting rules.	0.6.0	0.6.1
2008-03					Small editorial corrections by rapporteur	0.6.1	0.6.2
2008-04	CT4#38 bis				Inclusion of documents agreed at CT4 #38bis: C4-080694, C4-080861, C4-080862, C4-080867, C4-080890, C4-080952, C4-081005	0.6.2	0.7.0
2008-05	CT4#39				Inclusion of documents agreed at CT4 #39: C4-081100, C4-081295	0.7.0	0.8.0
2008-06	CT4#39 bis				Inclusion of documents agreed at CT4 #39bis: C4-081635	0.8.0	0.9.0