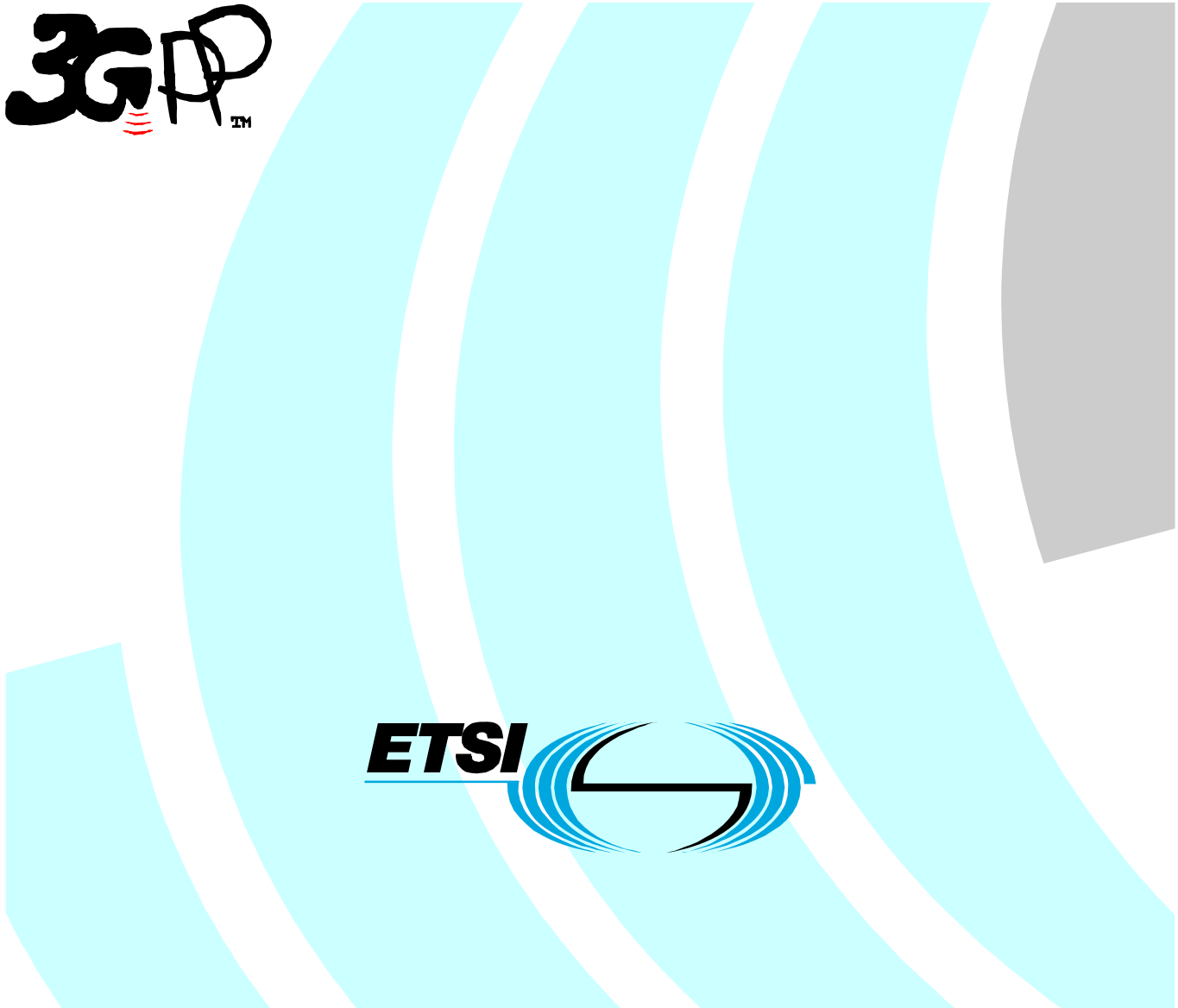
ETSI TS 123 402 V8.2.0 (2008-11)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Architecture enhancements for non-3GPP accesses
(3GPP TS 23.402 version 8.2.0 Release 8)



Reference
DTS/TSGS-0223402v820

Keywords
access, architecture, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification 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

Guidance to Readers of this Specification

In order to reduce the number of procedures in this specification certain editorial practices have been adopted. Though there are many independent factors, such as variants of S5/S8 and attachment cases, these are in essence quite similar. So, rather than presenting the permutations of these factors separately and thereby needlessly repeating normative text, conventions have been adopted to combine this information in single procedures.

The S5 and S8 reference points in the EPC architecture have been defined to have both a GTP and PMIP variant. The GTP variant is documented in TS 23.401 [4], while the PMIP variant is documented in this specification. Every effort has been made to eliminate duplication of normative text common to both specifications. Many figures in this specification refer to procedures in TS 23.401 [4] to achieve this end. Common procedures between TS 23.401 [4] and TS 23.402, are represented in this specification in figures by text in shaded box(es) that reference the appropriate figure and steps in TS 23.401 [4]. The details of the common steps are only captured in TS 23.401 [4].

Attachment cases (as discussed in section 6.2.1 and 7.2.1) have been combined in a single figure. The different attachment cases can be accommodated by including optional items in the flows, for instance, a vPCRF that is only employed during when a roaming case or LBO is specified.

Multiple APN interactions may occur for many of the procedures defined in this specification. These interactions complicate the flows by introducing certain operations that may occur multiple times. Rather than produce unique flows for this purpose, we indicate where this possibility may occur in text.

1 Scope

This document specifies the stage 2 service description for providing IP connectivity using non-3GPP accesses to the Evolved 3GPP Packet Switched domain. In addition, for E-UTRAN and non-3GPP accesses, the specification describes the Evolved 3GPP PS Domain where the protocols between its Core Network elements are IETF-based.

ITU-T Recommendation I.130 [2] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [3] defines stage 2 of the method.

The specification covers both roaming and non-roaming scenarios and covers all aspects, including mobility between 3GPP and non 3GPP accesses, policy control and charging, and authentication, related to the usage of non-3GPP accesses.

TS 23.401 [4] covers architecture aspects common to the Evolved 3GPP Packet Switched domain.

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] ITU-T Recommendations I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[3] ITU-T Recommendation Q.65: "The unified functional methodology for the characterization of services and network capabilities".

[4] 3GPP TS 23.401: "GPRS Enhancements for E-UTRAN Access".

[5] 3GPP TS 23.234: "3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description".

[6] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description Stage 2".

[7] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[8] IETF Internet-Draft, draft-ietf-netlmm-proxymip6-10.txt, "Proxy Mobile IPv6", work in progress.

[9] IETF RFC 4306, "Internet Key Exchange Protocol Version 2".

[10] IETF Internet-Draft, draft-ietf-mip6-nemo-v4traversal-03.txt, "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", work in progress.

[11] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[12] IETF RFC 3344, "Mobility Support for IPv4".

[13] IETF RFC 4285, "Authentication Protocol for Mobile IPv6".

[14] IETF RFC 3775, "Mobility Support in IPv6".

[15] IETF RFC 4282, "The Network Access Identifier".

[16] 3GPP TS 23.003: "Numbering, addressing and identification".

[17] IETF Internet-Draft, draft-ietf-netlmm-pmip6-ipv4-support-00.txt, "IPv4 Support for Proxy Mobile IPv6" work in progress.

[18] IETF RFC 4555, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)"

[19] 3GPP TS 23.203: "Policy and Charging Control Architecture".

[20] 3GPP TS 22.278: "Service requirements for evolution of the system architecture".

[21] 3GPP TS 23.060: "GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[22] IETF RFC 4877, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[23] IETF RFC 2784, "Generic Routing Encapsulation (GRE)".

[24] IETF RFC 2890, "Key and Sequence Number Extensions to GRE".

[25] IETF RFC 3543, "Registration Revocation in Mobile IPv4".

[26] 3GPP TS 29.212: "Policy and charging control over Gx reference point".

[27] 3GPP TS 29.214: "Policy and charging control over Rx reference point".

[28] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[29] IETF RFC 4039: "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[30] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[31] IETF RFC 3633: "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

[32] 3GPP2 C.S0024-A v2.0: "cdma2000 High Rate Packet Data Air Interface Specification".

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

[34] IETF RFC 2794: "Mobile IP Network Access Identifier Extension for IPv4".

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

[36] IETF Internet-Draft, draft-muhanna-netlmm-grekey-option-01.txt, "GRE Key Option for Proxy Mobile IPv6" work in progress.

[37] IETF Internet-Draft, draft-giaretta-netlmm-mip-interactions-01, "Interactions between PMIPv6 and MIPv6: scenarios and related issues", work in progress.

[38] IETF RFC 4861: "Neighbor Discovery for IP Version 6 (IPv6)".

[39] IETF Internet-Draft, draft-korhonen-mip4-service-02.txt, "Service Selection for Mobile IPv4", work in progress.

[40] IETF RFC 5026: "Mobile IPv6 bootstrapping in split scenario".

[41] IETF Internet-Draft, draft-ietf-mip6-bootstrapping-integrated-dhc-05: "MIP6-bootstrapping for the Integrated Scenario", work in Progress.

[42] IETF Internet-Draft, draft-ietf-mip6-ha-switch-06: "Mobility Header Home Agent Switch Message", work in progress.

[43] IETF Internet-Draft, draft-korhonen-dime-pmip6-02.txt: "Diameter Proxy Mobile IPv6: Support for Mobility Access Gateway and Local Mobility Anchor to Diameter Server Interaction", work in progress.

[44] IETF Internet-Draft, draft-ietf-dime-mip6-integrated-07.txt: "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", work in progress.

[45] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[46] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[47] 3GPP TS 22.011: "Service accessibility".

[48] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

[49] 3GPP2 C.S0087-0: "E-UTRAN - HRPD and CDMA2000 1x Connectivity and Interworking: Air Interface Aspects".

[50] IETF RFC 4739: " Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[51] 3GPP2 X.P0057-0 v0.6.0: "E-UTRAN - HRPD Connectivity and Interworking: Core Network Aspects", work in progress.

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].

SectorID or Sector Address Identifier: This identifier is defined in 3GPP2 C.S0024-A v2.0 [32] and is used to identify an HRPD AN. The Network operator shall set the value of the SectorID according to the rules specified in section 14.9 of 3GPP2 C.S0024-A v2.0 [32].

3.2 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].

CCoA	Collocated Care-of-address
DSMIPv6	Dual-Stack MIPv6
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
FACoA	Foreign Agent Care-of-Address
GW	Gateway
HRPD	High Rate Packet Data
HSGW	HRPD Serving Gateway
IPMS	IP Mobility management Selection
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MME	Mobility Management Entity
P-GW	PDN Gateway
PMIP/PMIPv6	Proxy Mobile IP version 6
SectorID	Sector Address Identifier
S-GW	Serving GW

4 Architecture Model and Concepts

4.1 Concepts

4.1.0 General Concepts

The EPS supports the use of non-3GPP IP access networks to access the EPC.

The EPS supports IETF-based network-based mobility management mechanism (e.g., PMIP) and host-based mobility management mechanism (e.g., MIP) over S2 reference points.

The EPS supports IETF-based network-based mobility management mechanism (e.g., PMIP) over S5, and S8 reference points.

When host-based mobility protocol (DSMIPv6 [10]) is used within the EPS and the UE camps on a 3GPP access network, in this specification the UE is considered to be on its home link.

NOTE A scenario where the UE in EPS uses a host based mobility protocol with a HA that is outside the EPS is out of the scope of 3GPP specification.

The mobility management procedures specified to handle mobility between 3GPP and non 3GPP accesses shall include mechanisms to minimize the handover latency due to authentication and authorization for network access. This applies to UEs either supporting simultaneous radio transmission capability or not supporting it.

For multiple PDN-GWs connecting to the same PDN, all the PDN GWs shall support the same mobility protocols.

The EPC supports local breakout of traffic whether a roaming subscriber is accessing the EPC via a 3GPP or a non 3GPP access network according to the design principles described in section 4.1 of TS 23.401 [4].

The full support for connecting an UE simultaneously to the EPC via more than one access network is out of the scope of this release of the specification.

NOTE: Even though not explicitly supported by this specification, the mechanisms specified in this specification can be used to connect a UE in parallel to the EPC via 3GPP access network and a Non-3GPP access network towards different PDNs.

4.1.1 General Concepts for Interworking Between E-UTRAN and CDMA2000

The mobility management procedures specified to handle mobility between E-UTRAN and CDMA2000 accesses (as required by TS 22.278 [20]) shall include mechanisms to minimize the service interruption during handover and where possible support bidirectional service continuity.

- This applies to UEs supporting either single or dual radio capability.
- The mobility management procedures should minimize any performance impacts to the UE and the respective accesses, for example, UE battery consumption and network throughput.
- The mobility management procedures should minimize the coupling between the different accesses allowing independent protocol evolution in each access.

4.1.2 General Concepts for Interworking Between 3GPP Accesses and WiMAX

The mobility management procedures specified to handle mobility between 3GPP Accesses and WiMAX (as required by TS 22.278 [20]) shall include mechanisms to minimize the service interruption during handover and where possible support bidirectional service continuity.

- This applies to UEs supporting either single or dual radio capability.

- The mobility management procedures should minimize any performance impacts to the UE and the respective accesses, for example, UE battery consumption and network throughput.

- The mobility management procedures should minimize the coupling between the different accesses allowing independent protocol evolution in each access.

Furthermore, the mobility management procedures specified to handle mobility between 3GPP accesses and WiMAX should minimize the impact on legacy systems (i.e. UTRAN and GERAN).

4.1.3 IP Mobility Management Selection Principles

The Mobility mechanisms supported between 3GPP and non-3GPP accesses within an operator and its roaming partner's network would depend upon operator choice.

4.1.3.1 Static Configuration of Inter-technology Mobility Mechanism

For networks deploying a single IP mobility management mechanism, the statically configured mobility mechanism can be access type and/or roaming agreement specific. The information about the mechanism to be used in such scenario is expected to be provisioned into the terminal (or the UICC) and the network. IP session continuity between 3GPP and non-3GPP access types may not be provided in this case if there is a mismatch between what the UE expects and what the network supports. For example service continuity may not be possible if the user switches to a terminal supporting a different IP mobility management mechanism than provisioned in the network.

NOTE: The mismatch case where a non-3GPP network only supports DSMIPv6 and the UE does not, may lead to a situation where the UE receives a local IP address in the non-3GPP access network, but gains no PDN connectivity in the EPS. Depending on operator policy and roaming agreements, IP connectivity may be provided using this local IP address to access services (e.g. internet access) in the non-3GPP network. However, any such use of the local IP address where the user traffic does not use the EPC is not described in this specification.

4.1.3.2 Networks Supporting Multiple IP Mobility Mechanisms

IP Mobility management Selection (IPMS) consist of two components:

- IP MM protocol selection between Network Based Mobility (NBM) and Host based mobility (HBM - MIPv4 orDSMIPv6).

- Decision on IP address preservation if NBM is selected.

IPMS does not relate to the selection between PMIP and GTP over S5/S8.

Upon initial attachment to a 3GPP access, no IPMS is necessary since connectivity to a PDN GW is always established with a network-based mobility mechanism.

Upon initial attachment to a non-3GPP access and upon handover from 3GPP to non-3GPP access, IPMS is performed before an IP address is allocated and provided to the UE.

The UE support for a specific IP Mobility Management protocol and/or IP address preservation mechanism for inter-access mobility may be known by the network-based on explicit indication from the UE.

Upon attachment to a non-3GPP access, if the access network (supporting at least PMIP6) is not aware of the UE capabilities and the home and access network's policies allow the usage of PMIP6, then PMIP6 is used for establishing connectivity for the UE to the EPC.

When a NBM mechanism is used for establishing connectivity in the target access upon inter-access mobility, IP address preservation for session continuity based on NBM may take place as per PMIP6 specification (draft-ietf-netlmm-proxymip6 [8]) and additionally based on the knowledge in the network of UE's capability (if available) to support NBM. Such knowledge may be based on an explicit indication from the UE upon handover that IP address preservation based on NBM management can be provided.

IP address preservation for session continuity based on HBM may take place if the network is aware of the UE capability to support DSMIPv6 or MIPv4. Such knowledge may be based on an indication to the target non-3GPP access from the HSS/AAA (e.g. in case of DSMIPv6, the UE performed S2c bootstrap before moving to the target non-

3GPP access). In such a case, the non-3GPP access network provides the UE with a new IP address, local to the access network if IP mobility management protocol selected is DSMIP6. In that case, in order to get IP address preservation for session continuity, the UE shall use DSMIP6 over S2c refernce point. This IP address shall be used as a care-of address for DSMIPv6, and any other use is out of scope of this specification. If the IP mobility management protocol selected is MIPv4, the address provided to the UE by the non-3GPP access network is a FACoA and IP address preservation is performed over S2a using MIPv4 FACoA procedures.

The final decision on the mobility management mechanism is made by the HSS/AAA upon UE authentication in the non-3GPP access system (both at initial attachment and handover), based on the information it has regarding the UE, local/home network capabilities and local/home network policies. If the UE provided an explicit indication of the supported mobility mechanisms, the network shall provide an indication to the UE identifying the selected mobility management mechanism.

Support of different IP mobility management protocols at local/home network is known by the AAA/HSS in one of the following ways:

- through static pre-configuration, or
- through indication of the supported IP mobility management protocols (PMIP6 and/or MIPv4 FA CoA mode) by the non-3GPP access system as part of the AAA exchange for network access authentication.

Upon selecting a mobility management mechanism, as part of the AAA exchange for UE authentication in the non-3GPP access system the HSS/AAA returns to the non-3GPP access system an indication on whether a local IP address shall be allocated to the UE, or the address of the MIPv4 Foreign Agent shall be provided, or if instead PMIP shall be used to establish the connectivity.

IPMS is performed in the following scenarios:

- Upon initial attach to a non-3GPP access, the IPMS is performed to decide how to establish IP connectivity for the UE.
- Upon handover without optimization from a 3GPP access to a non-3GPP access, the IPMS is performed to decide how to establish IP connectivity for the UE over non-3GPP access.
- Upon change of access between a non-3GPP access and a 3GPP access or between two non-3GPP accesses, if the IP MM protocol used to provide connectivity to the UE over non-3GPP access is a NBM protocol, then a decision is performed on whether IP address preservation is provided or not as per PMIP6 specification (draft-ietf-netlmm-proxymip6 [8]) and additionally based on the knowledge in the network of UE's capability (if available) to support NBM.

4.1.3.2.1 IP Mobility Management Selection During Initial Attach to a Non-3GPP Access

The IPMS decision is performed as described in the following:

- If the UE indicates DSMIPV6 support only, and the network supports and selects DSMIPV6, the access network provides a local IP address to the UE to be used as CoA for DSMIPv6/S2c.
- If the UE indicates MIPv4 support only, and the network supports and selects MIPv4, then the access network provides a FACoA to the UE.
- If the UE indicates DSMIPV6 or MIPv4 support only, and the network selects PMIP for providing connectivity, then PMIP is used for connectivity.
- If the UE does not indicate any capabilities, it is assumed that the UE is not able to support DSMIPv6 or MIPv4, and NBM is used for providing connectivity if the network supports NBM.

4.1.3.2.2 IPMS solutions

On handover to 3GPP access, UE shall request for IP address preservation by setting "attach type" flag to "handover" during the attach procedure.

NOTE: UE requests for address preservation if S2c is used over source access network or MIPv4 FACoA is used to connect over source access network or UE is capable of Network address preservation.

When the UE provides an indication of its supported mobility modes either during initial attach or on handover, the UE provides such information to the entity performing IPMS during network access authentication, for trusted non-3GPP accesses, or during authentication for tunnel establishment with ePDG, for untrusted non-3GPP accesses.

The network then makes the decision on what mobility protocol to be used for connectivity as described in further subsections depending on the scenario.

4.1.3.2.3 IP Mobility Management Selection on Handover between accesses

On handover to non-3GPP accesses, the IPMS decision is performed as described in the following:

a. If the UE only indicates NBM support between the two access technologies involved in the handover and the network supports NBM between those two access technologies involved in the handover, then PMIP is used for providing connectivity, and IP address preservation is provided with S2a procedures.

b. If the UE indicates DSMIPv6 support and the home network supports and selects DSMIPv6, the access network provides a local IP address to the UE to be used as CoA for DSMIPv6, and IP address preservation is provided with S2c procedures.

c. If the UE indicates DSMIPv6 support only and the home network does not support DSMIPv6, then PMIP is used for providing basic connectivity to the existing PDN GW if PMIP is supported by the access network. In this case, the decision for IP address preservation is made as per PMIP6 specification (draft-ietf-netlmm-proxymip6 [8]).

d. If the UE indicates support for both NBM and DSMIPv6, and the network based on policies selects PMIP to establish the connectivity, then PMIP is used to establish connectivity, and IP address preservation is provided with S2a procedures.

e. If the UE indicates support for both NBM and DSMIPv6, and the network based on policies selects DSMIPv6 to establish the connectivity, then the access network provides a local IP address to the UE to be used as CoA for DSMIPv6, and IP address preservation is provided with S2c procedures.

f. If the UE does not indicate any capabilities, then PMIP6 is used for establishing connectivity if PMIP6 is supported by the access network. In this case, the decision for IP address preservation is made as per PMIP6 specification (draft-ietf-netlmm-proxymip6 [8]).

NOTE 1: In case of bullet c and f, PMIP6 specification allows two options:

a) Preserve the IP address based on a timer; If the connection through the old access system is not torn down before the timer expires then a new prefix is assigned, or

b) Immediately assign a new prefix.

This decision can be based on operator's policies.

NOTE 2: If prior to the handover, the UE was attached to a non-3GPP access with DSMIPv6, bullets a. and c. are considered not to apply.

NOTE 3: The PDN GW capability of supporting NBM or DSMIPv6 or MIPv4 should be considered in IP Mobility Mode Selection.

The UE indication of DSMIPv6 support may be implicit, e.g. having bootstrapped a security association via the old access network. The same applies to NBM, since the network can collect information about NBM support from other sources.

On handover to 3GPP access, the only decision that needs to be made is whether IP address preservation needs to be provided or not.

4.1.4 Trusted/untrusted non-3GPP access network detection

During initial attach or handover attach a UE needs to discover the trust relationship (whether it is a Trusted or Untrusted Non-3GPP Access Network) of the non-3GPP access network in order to know which non-3GPP IP access procedure to initiate. The trust relationship of a non-3GPP access network is made known to the UE with one of the following options:

1) If the non-3GPP access supports 3GPP-based access authentication, the UE discovers the trust relationship during the 3GPP-based access authentication.

2) The UE operates on the basis of pre-configured policy in the UE.

4.2 Architecture Reference Model

4.2.1 Architecture for 3GPP Accesses with PMIP-based S5/S8

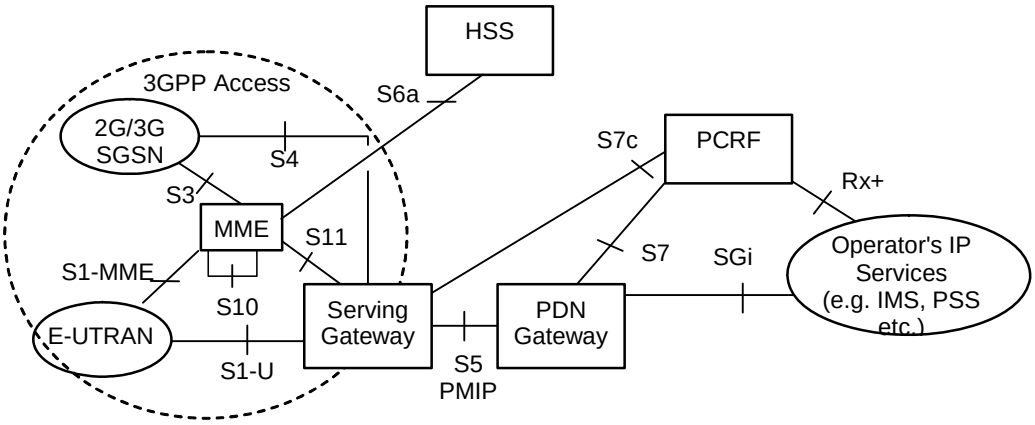


Figure 4.2.1-1: Non-Roaming Architecture for 3GPP Accesses within EPS using PMIP-based S5

NOTE: The "3GPP Access" bubble represents a collection of functional entities and interfaces for the purpose of pictorial simplification of the architectural models presented below.

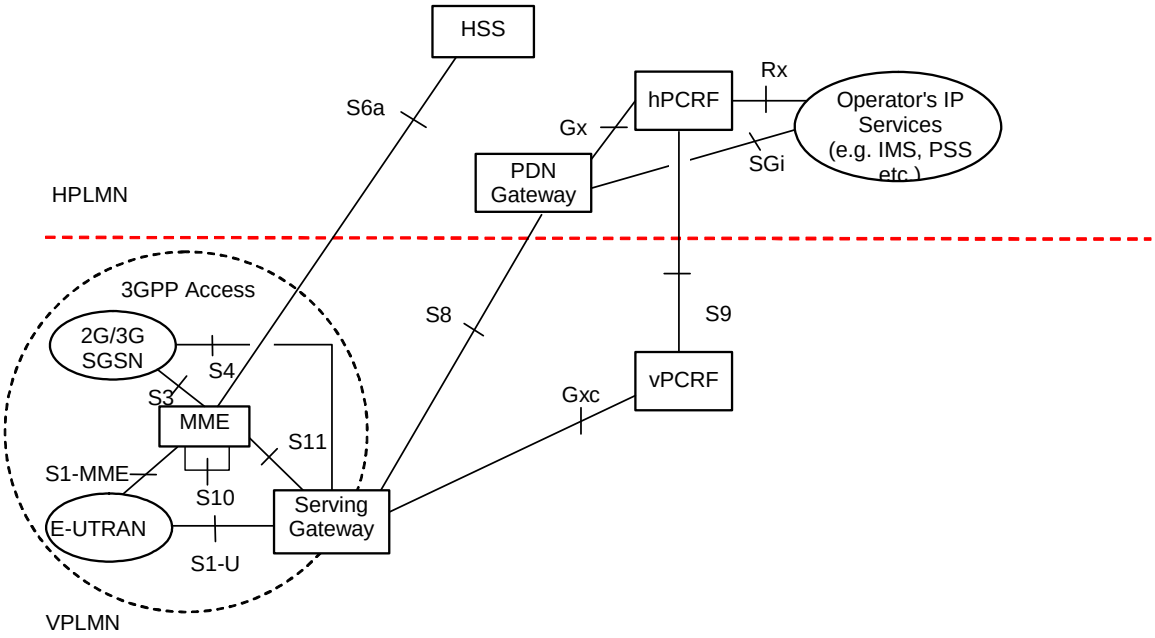


Figure 4.2.1-2: Roaming Architecture for 3GPP Accesses within EPS using PMIP-based S8

4.2.2 Non-roaming Architectures for EPS

The following considerations apply to interfaces where they occur in figures in this and the next section:

- S5 can be GTP-based or PMIP-based.
- Gxc is used only in the case of PMIP variant of S5 or S8.

- Gxa is used when the Trusted non-3GPP Access network is owned by the same operator.
- S9 is used instead of Gxa to the Trusted non-3GPP Access network not owned by the same operator.
- Gxa or S9 are terminated in the Trusted non-3GPP Accesses if supported.
- S2c is used only for DSMIPv6 bootstrapping and DSMIPv6 De-Registration (Binding Update with Lifetime equals zero) when the UE is connected via 3GPP access.

NOTE: SWu shown in Figure 4.2.2-1 also applies to architectural reference Figures 4.2.2-2 and 4.2.3-1 to 4.2.3-6, but is not shown for simplicity.

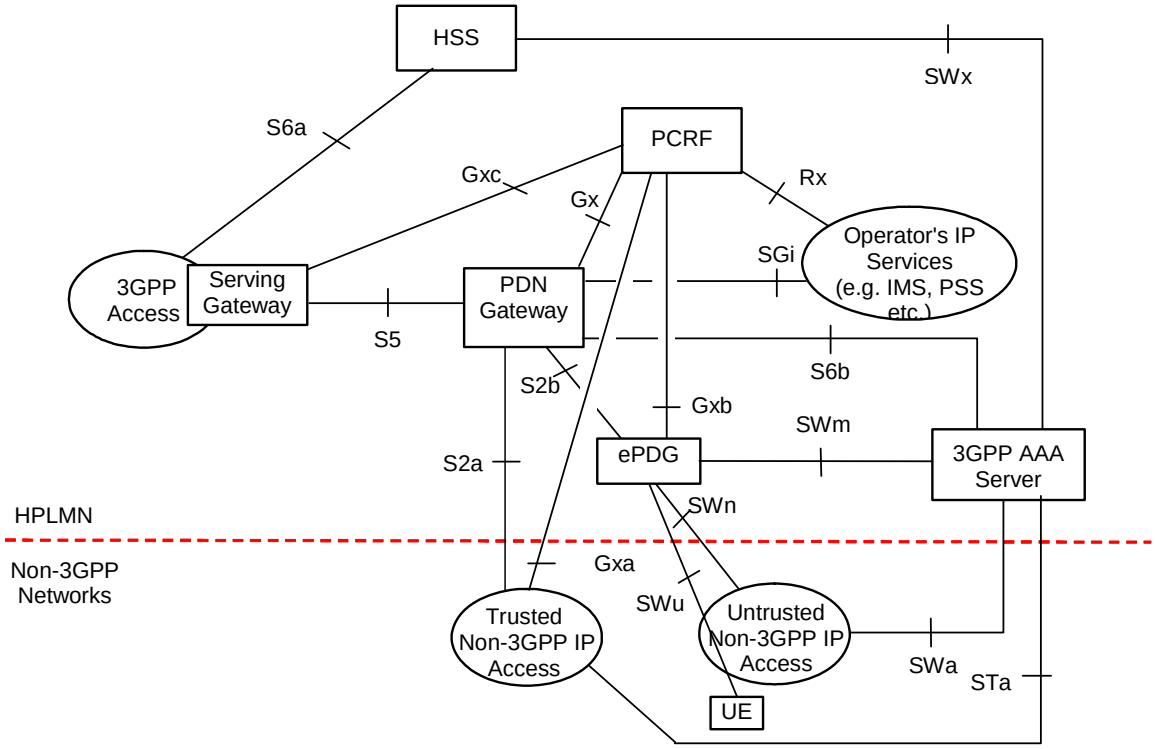


Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

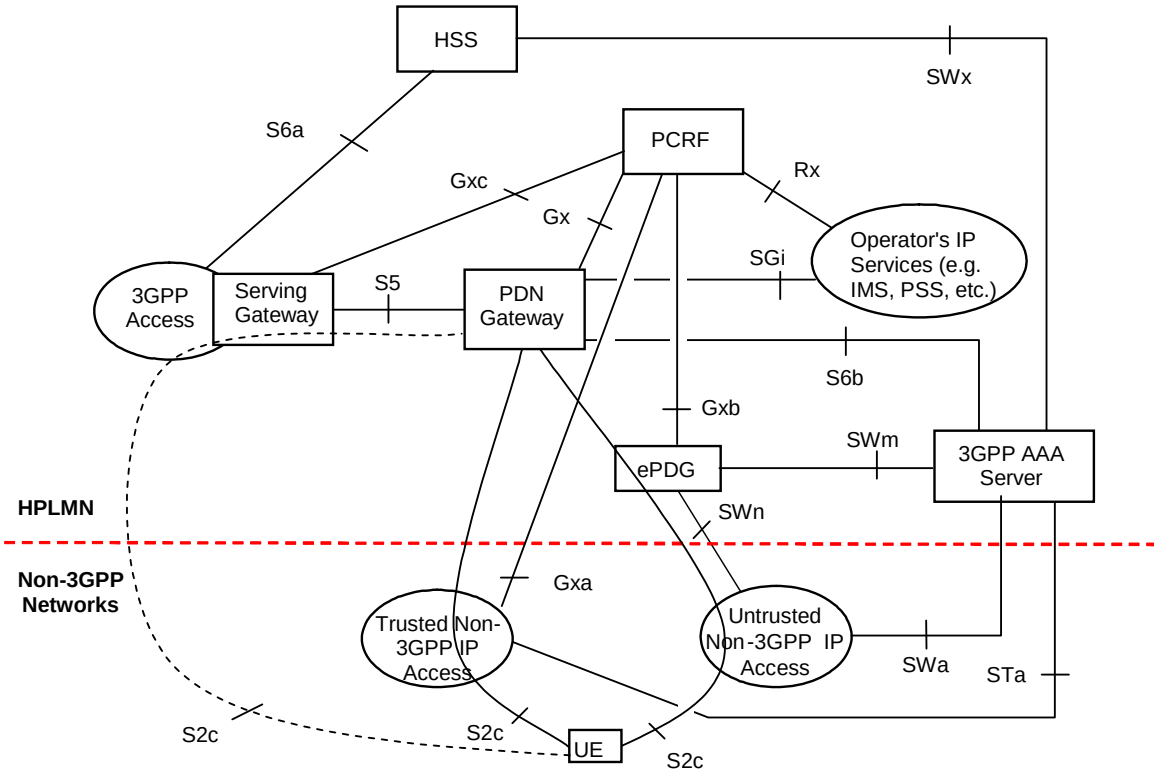


Figure 4.2.2-2: Non-Roaming Architecture within EPS using S5, S2c

4.2.3 Roaming Architectures for EPS

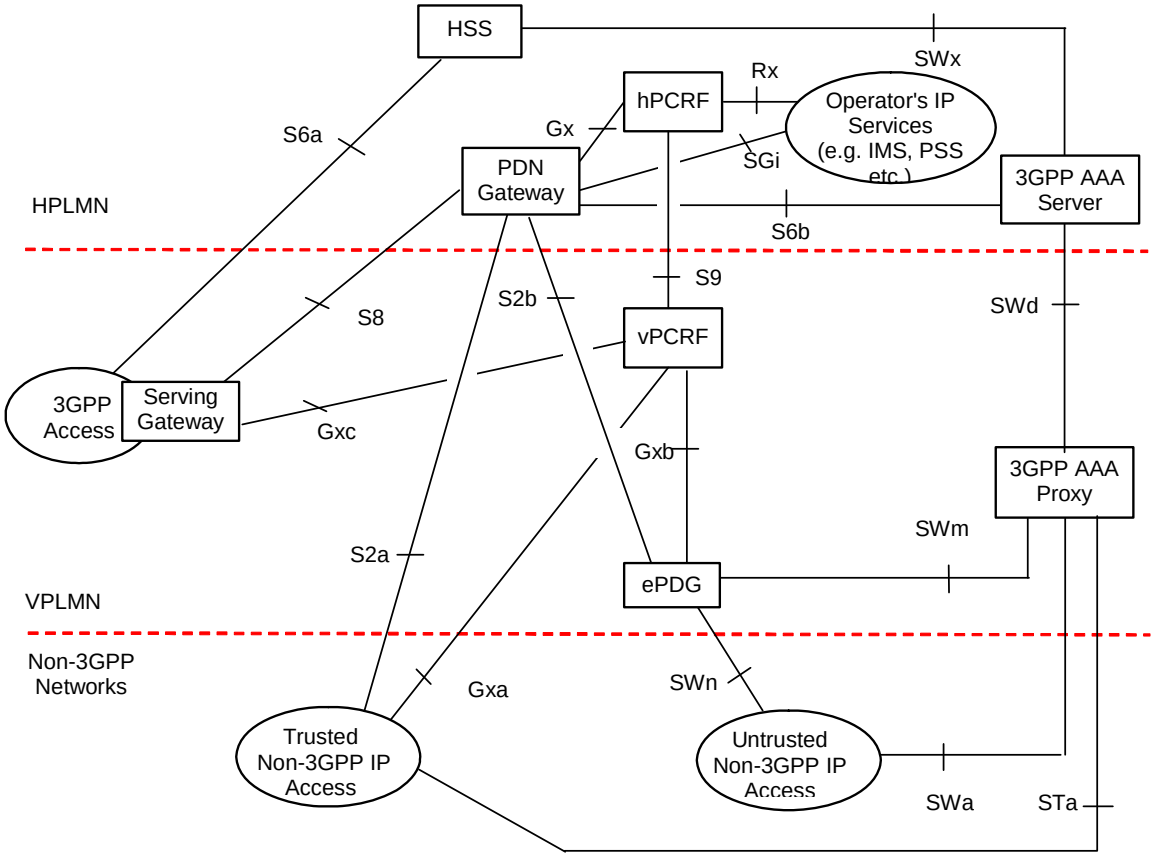


Figure 4.2.3-1: Roaming Architecture for EPS using S8, S2a– S2b - Home Routed

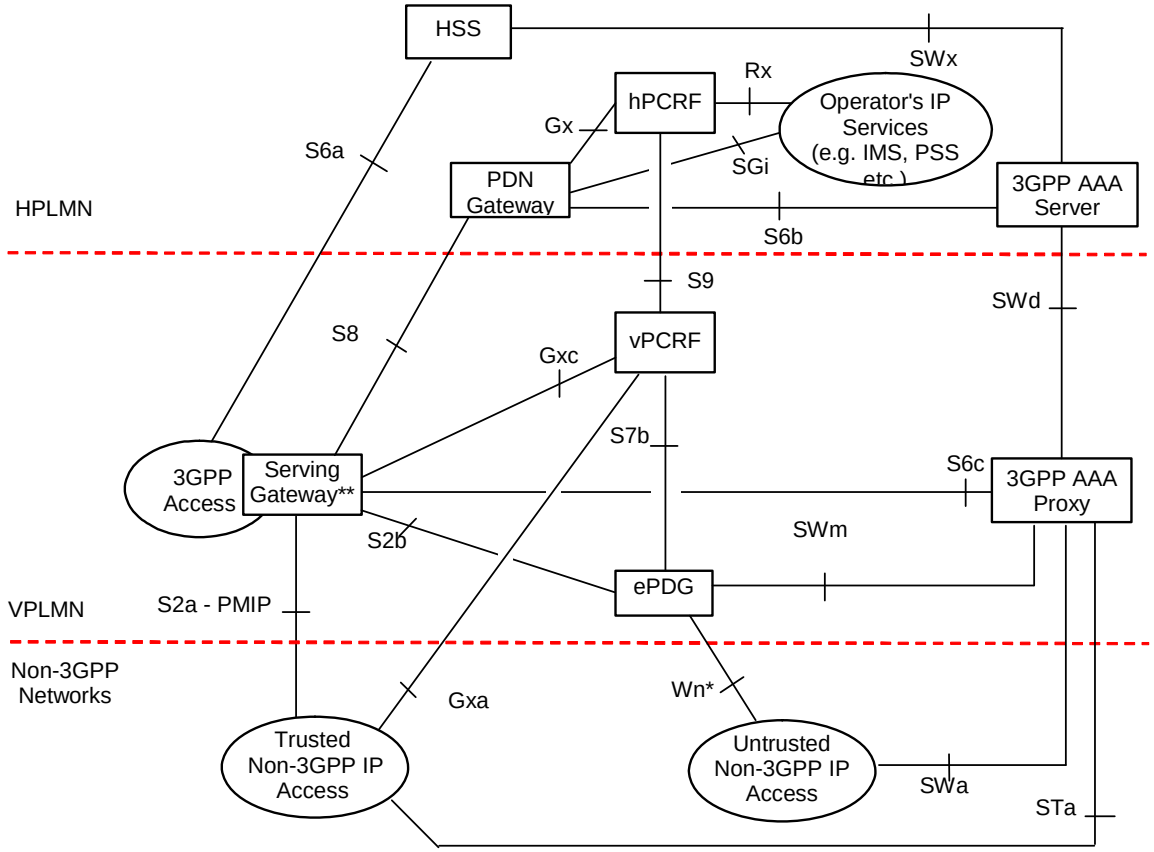


Figure 4.2.3-2: Roaming Architecture for EPS using PMIP-based S8, S2a, S2b (Chained PMIP-based S8-S2a/b) - Home Routed

** Chained S2a/S2b and S8a/b used when VPLMN has business relationship with Non-3GPP Networks and S-GW in VPLMN includes local non-3GPP Anchor.

NOTE 1: AAA, mobility, and QoS policy and event reporting related optimizations (e.g. signalling reduction and information hiding towards the HPLMN) for PMIP-based S8-S2a/b chainging are not specified within this release of the specification.

The following are some additional considerations in this case:

- Gxc is used only in the case of PMIP-based S8. Gxc is not required for Trusted Non-3GPP IP Access if the serving GW and the trusted non-3GPP access are in the control of the same operator; Gxais used instead to signal the QoS policy and event reporting.

Editor's Note: QoS policy may be required by the Serving GW for enforcing admission control to PMIP-based S8 as part of implementing GRX Roaming service level agreements. It is FFS whether or how Gxc to the Serving GW in the case of Trusted and Un-trusted Non-3GPP IP Access could be employed for this purpose.

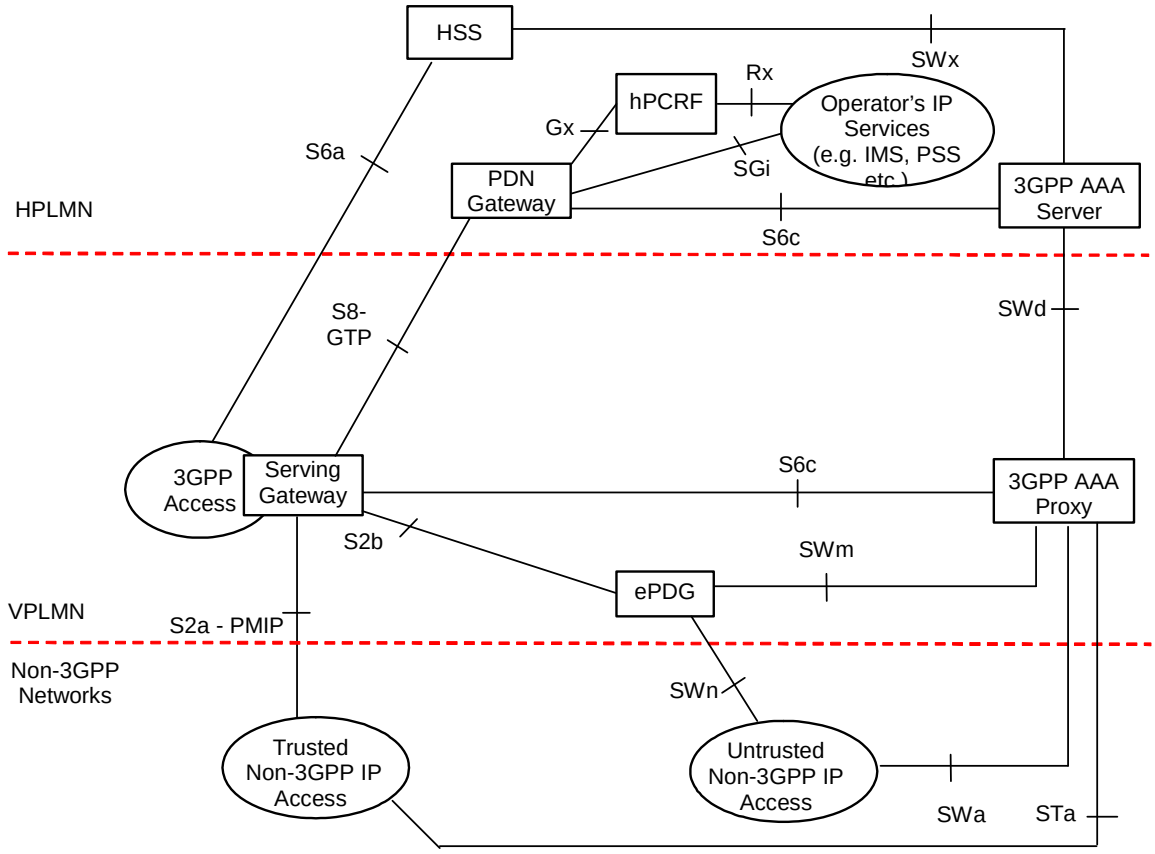


Figure 4.2.3-3: Roaming Architecture for EPS using GTP- based S8, S2a, S2b (Chained S8a + S2a–S2b) - Home Routed

** Chained S2a/S2b and S8a/b used when VPLMN has business relationship with Non-3GPP Networks and S-GW in VPLMN includes local non-3GPP Anchor

The above scenario supports QoS differentiation between subscribers on the default bearer (i.e. QoS subscription-based). In case multiple PDN's are supported QoS differentiation per PDN can apply (i.e. multiple default bearers). The principles for this scenario include:

- Does not require PCC in visited network
- Does not require S9 for roaming
- Default EPS bearer support over S8a
- The assumption is that MME is not involved when UE is attached in non-3GPP access
- Same S8a roaming interface is used as in TS 23.401 [4]
- No dynamic QoS policy control in non-3GPP access
- Subscriber-based QoS differentiation in the non-3GPP access
- The subscriber's QoS profile to create the default bearer on S8a may be transmitted to the S-GW through S6c from the AAA proxy which gets the profile from AAA Server

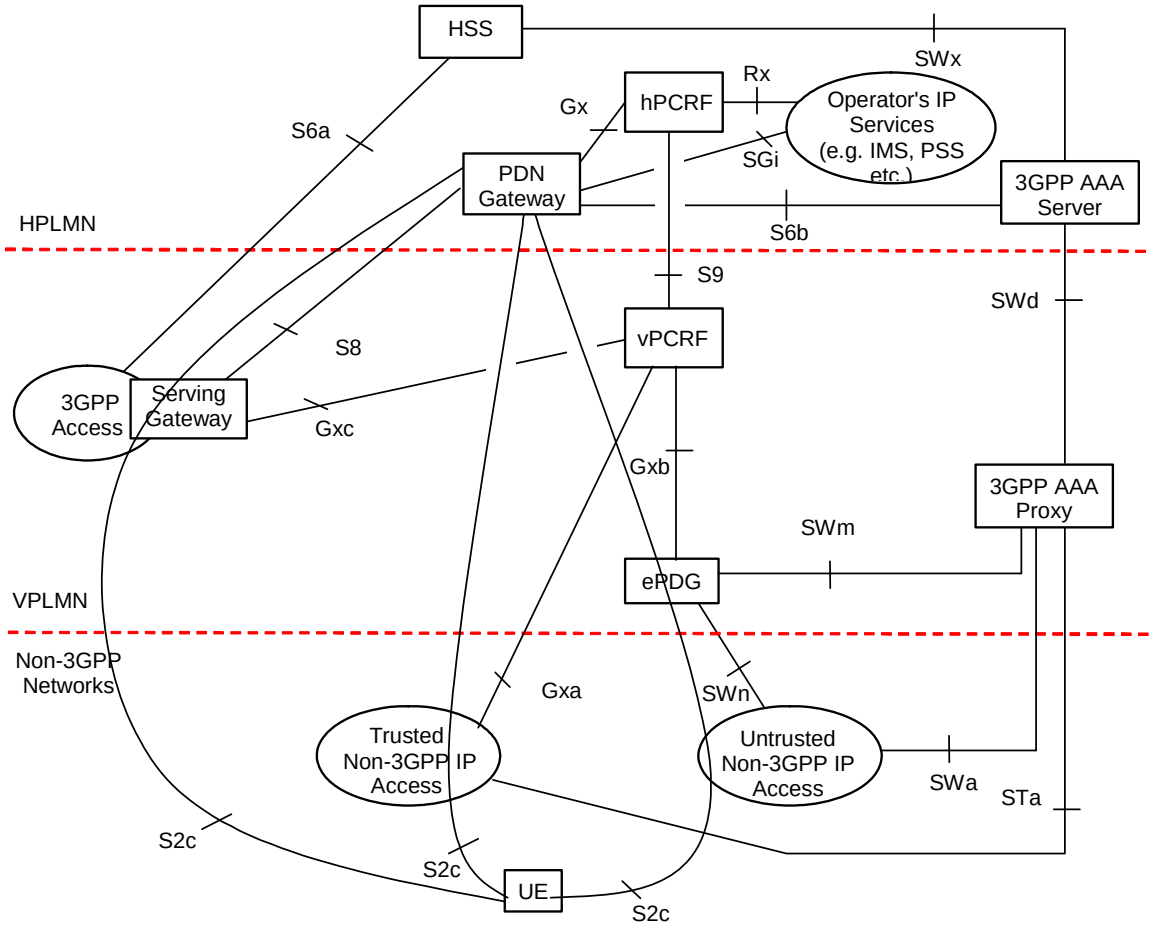


Figure 4.2.3-4: Roaming Architecture for EPS using S8 – S2c - Home Routed

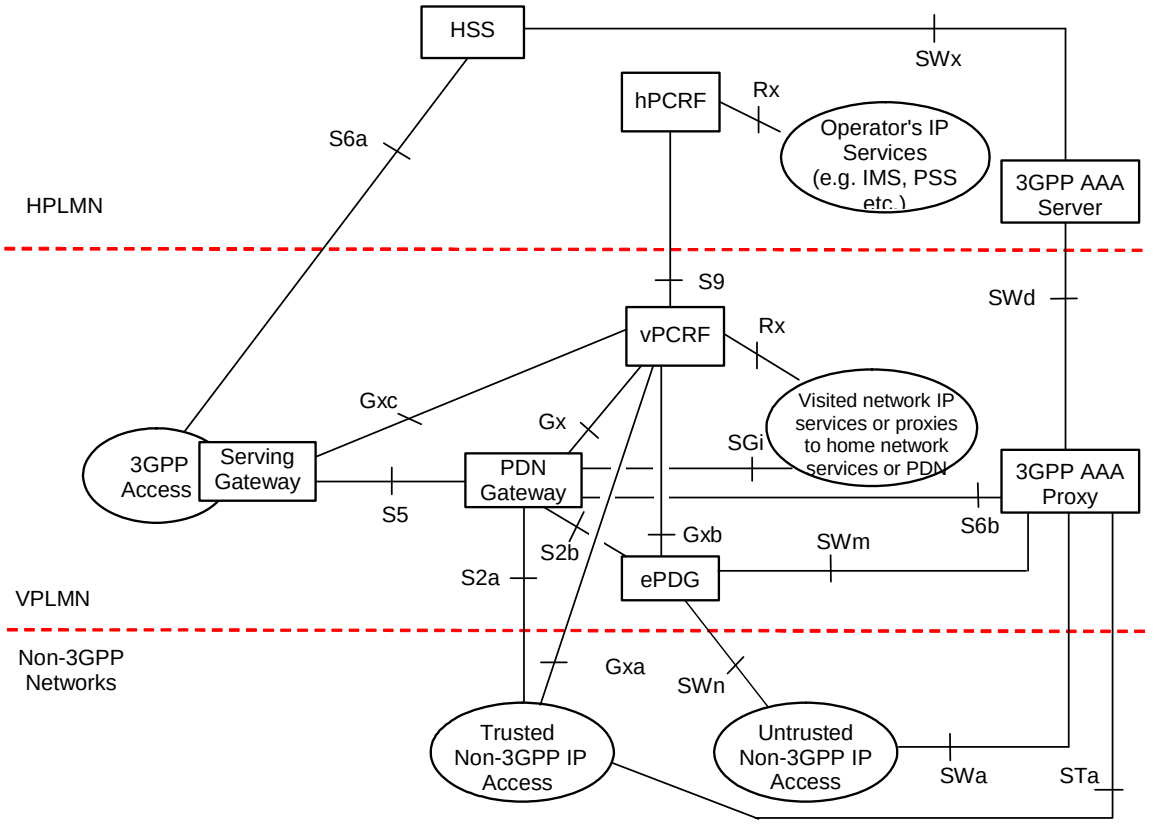


Figure 4.2.3-5: Roaming Architecture for EPS using S5, S2a, S2b – Local Breakout

NOTE 2: The two Rx instances in Figure 4.2.3-5 apply to different application functions in the HPLMN and VPLMN.

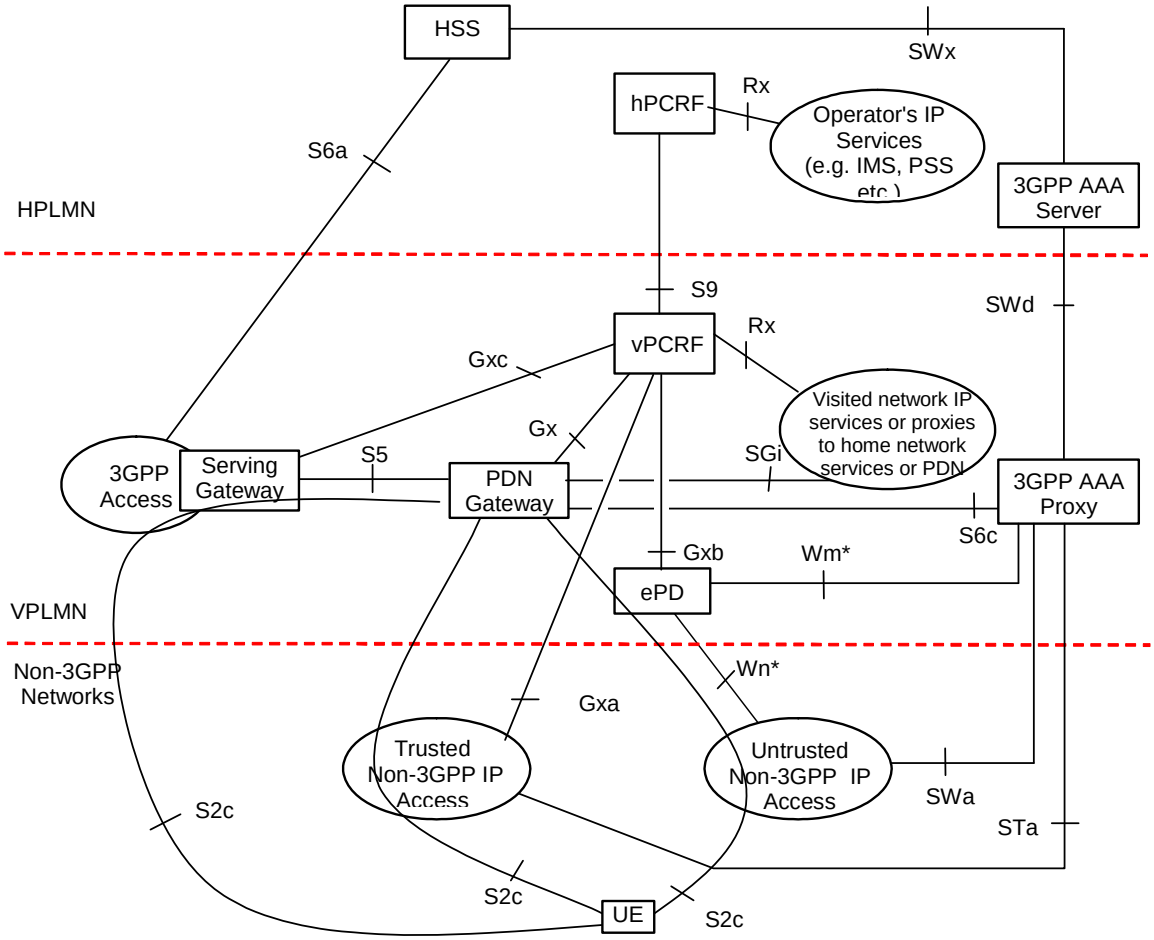


Figure 4.2.3-6: Roaming Architecture for EPS using S5, S2c – Local Breakout

NOTE 3: The two Rx instances in Figure 4.2.3-6 apply to different application functions in the HPLMN and VPLMN.

4.3 Network Elements

4.3.1 Access Networks

4.3.1.1 E-UTRAN

E-UTRAN is described in detail in TS 36.300 [6] with additional functions listed in TS 23.401 [4].

4.3.1.2 Trusted and Untrusted Non-3GPP Access Network

Trusted and Untrusted Non-3GPP Access Networks are IP access networks that use access technology whose specification is out of the scope of 3GPP.

Whether a Non-3GPP IP access network is Trusted or Untrusted is not a characteristic of the access network.

In non-roaming scenario it is the HPLMN's operator decision if a Non-3GPP IP access network is used as Trusted or Untrusted Non-3GPP Access Network.

Editor's note: It is FFS whether it is the HPLMN or VPLMN or both that decide if a Non-3GPP access is trusted or untrusted in roaming scenario.

4.3.2 MME

The details of functionality of MME are described TS 23.401 [4].

The following are additional MME functions:

- HRPD access node (terminating S101 reference point) selection and maintenance for handovers to HRPD;
- Transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access, as specified in the pre-registration and handover flows.
- Forwarding the GRE key for uplink traffic to the target S-GW in case of CN node relocation.

4.3.3 Gateway

4.3.3.1 General

Two logical Gateways exist:

- Serving GW (S-GW)
- PDN GW (P-GW)

The functional split of PDN GW and Serving GW is described in TS 23.401 [4].

4.3.3.2 Serving GW

The functionality of the Serving GW is described in TS 23.401 [4]. In addition to the functions described in TS 23.401 [4] the Serving GW includes the following functionality:

- A local non-3GPP anchor for the case of roaming when the non-3GPP IP accesses connected to the VPLMN.
- Event reporting (change of RAT, etc.) to the PCRF.
- Uplink and downlink bearer binding towards 3GPP accesses as defined in TS 23.203 [19].
- Uplink bearer binding verification with packet dropping of "misbehaving UL traffic".

NOTE 1: The term 'Uplink bearer binding verification' is defined in TS 23.401 [4].

- Mobile Access Gateway (MAG) according to draft-ietf-netlmm-proxymip6 [8] if PMIP-based S5 or S8 is used. The MAG function shall be able to send UL packets before sending the PBU or before receiving the PBA.
- DHCPv4 (relay agent) and DHCPv6 (relay agent) functions if PMIP-based S5 or S8 is used.
- Handling of Router Solicitation and Router Advertisement messages as defined in RFC 4861 [38], if PMIP based S5 and S8 is used.
- Allocation of GRE key, which is used by the PDN GW to encapsulate downlink traffic to the Serving GW on the PMIP-based S5/S8 interface.
- If GTP-based or PMIP-based S8-S2a/b chaining is used:
  - the Serving GW acts as a LMA towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG;
  - the Serving GW allocates GRE key, which is used to encapsulate uplink traffic on PMIP-based S2a/S2b interface.

NOTE 2: The Serving GW does not require full MAG and full LMA functionally.

- If GTP-based S8-S2a/b chaining is used:
  - the Serving GW includes functionality to interwork the control plane of GTP towards the PDN GW and PMIPv6 signalling towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG;

- the Serving GW includes functionality to link the user-plane of the GTP tunnel towards the PDN GW and the user-plane of the PMIPv6 tunnel towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG.

NOTE 3: There is no 1:1 mapping between GTP tunnels and PMIPv6 tunnels; several GTP tunnels can be mapped into a single PMIPv6 tunnel.

- If PMIP-based S8-S2a/b chaining is used:

  - the Serving GW includes functionality to interwork the PMIPv6 signalling towards the PDN GW and PMIPv6 signalling towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG. In this case the Serving GW also acts as a MAG towards the PDN GW;

  - the Serving GW includes functionality to link the user-plane of the PMIPv6 tunnel towards the PDN GW and the user-plane of the PMIPv6 tunnel towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG.

4.3.3.3 PDN GW

PDN GW functionality is described in TS 23.401 [4]. In addition to the functions described in TS 23.401 [4], the PDN GW functions includes user plane anchor for mobility between 3GPP access and non-3GPP access. The PDN GW includes the following functionality:

- A LMA according to draft-ietf-netlmm-proxymip6 [8], if PMIP-based S5 or S8, or if S2a or S2b is used. The LMA function shall be able to accept UL packets from any trusted S-GW MAGs without enforcing that the source IP address must match the CoA in the MN BCE.

- A DSMIPv6 Home Agent, as described in draft-ietf-mip6-nemo-v4traversal [10], if S2c is used.

- Allocation of GRE key, which is used to encapsulate uplink traffic to the PDN GW on the PMIP-based S5/S8, or S2a or S2b interface.

- A MIPV4 Home Agent, if S2a with MIPv4 FA CoA mode is used.

4.3.4 ePDG

The functionality of ePDG includes the following:

- Functionality defined for the PDG in TS 23.234 [7] for the allocation of a remote IP address as an IP address local to the ePDG which is used as CoA when S2c is used;

  - Functionality for transportation of a remote IP address as an IP address specific to a PDN when S2b is used;

- Routing of packets from/to PDN GW (and from/to Serving GW if it is used as local anchor in VPLMN) to/from UE;

- De-capsulation/Encapsulation of packets for IPSec and PMIP tunnels (the latter only if network based mobility (S2b) is used);

- Mobile Access Gateway (MAG) according to draft-ietf-netlmm-proxymip6 [8] if network based mobility (S2b) is used;

- Tunnel authentication and authorization (termination of IKEv2 signaling and relay via AAA messages);

- Local mobility anchor within untrusted non-3GPP access networks using MOBIKE (if needed);

- Transport level packet marking in the uplink;

- Enforcement of QoS policies based on information received via AAA infrastructure;

- Lawful Interception.

- Allocation of GRE key, which is used to encapsulate downlink traffic to the ePDG on the PMIP-based S2b interface.

4.3.5 PCRF

The functionality of PCRF is described in TS 23.203 [19] with additional functionality listed in TS 23.401 [4]. In the non-roaming scenario, additionally, the PCRF terminates the Gxa, Gxb and Gxc reference points with the appropriate IP-CANs.

In roaming scenarios, the difference from TS 23.401 [4], is that the vPCRF exists for the UE for the scenario of roaming with home-routed traffic in addition to the scenario in TS 23.401 [4] of roaming with local breakout.

4.3.5.1 Home PCRF

In addition to the h-PCRF functionality listed in TS 23.401 [4], in this document the Home PCRF

- Terminates the Gx reference point for roaming with home routed traffic;
- Terminates the Gxa, Gxb or Gxc/S9 reference points as appropriate for the IP-CAN type.

4.3.5.2 Visited PCRF

In addition to the v-PCRF functionality listed in TS 23.401 [4], in this document the Visited PCRF

- Terminates the Gxa, Gxb or Gxc reference points as appropriate for the IP-CAN type;
- Terminates the S9 reference point.

4.4 Reference Points

4.4.1 List of Reference Points

The description of the reference points:

S1-MME, S1-U, S3, S4, S10, S11: these are defined in TS 23.401 [4].

S2a It provides the user plane with related control and mobility support between trusted non 3GPP IP access and the Gateway.

S2b It provides the user plane with related control and mobility support between ePDG and the Gateway.

S2c It provides the user plane with related control and mobility support between UE and the Gateway. This reference point is implemented over trusted and/or untrusted non-3GPP Access and/or 3GPP access.

S5 It provides user plane tunneling and tunnel management between Serving GW and PDN GW. It is used for Serving GW relocation due to UE mobility and in case the Serving GW needs to connect to a non collocated PDN GW for the required PDN connectivity.

S6a This interface is defined between MME and HSS for authentication and authorization. It is defined in TS 23.401 [4].

S6b It is the reference point between PDN Gateway and 3GPP AAA server/proxy for mobility related authentication if needed. This reference point may also be used to retrieve and request storage of mobility parameters. This reference point may also be used to retrieve static QoS profile for a UE for non-3GPP access in case dynamic PCC is not supported.

S6c It is the reference point between Serving Gateway in VPLMN and 3GPP AAA Proxy for mobility related authentication if needed. This reference point may also be used to retrieve and request storage of mobility parameters.

S7 It provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Point (PCEF)) in the PDN GW.

Gxa It provides transfer of (QoS) policy information from PCRF to the Trusted Non-3GPP accesses.

Gxb This interface is not specified within this release of the specification.

Gxc It provides transfer of (QoS) policy information from PCRF to the Serving Gateway

PMIP-based S8 It is the roaming interface in case of roaming with home routed traffic. It provides the user plane with related control between Gateways in the VPLMN and HPLMN.

S9 It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function. In all other roaming scenarios, S9 has functionality to provide dynamic QoS control policies from the HPLMN.

SGi It is the reference point between the PDN Gateway and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services. This reference point corresponds to Gi and Wi functionalities and supports any 3GPP and non-3GPP access systems.

SWa It connects the Untrusted non-3GPP IP Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization and charging-related information in a secure manner.

STa It connects the Trusted non-3GPP IP Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner.

SWd It connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server.

SWm This reference point is located between 3GPP AAA Server/Proxy and ePDG and is used for AAA signaling (transport of mobility parameters, tunnel authentication and authorization data). This reference point also includes the MAG-AAA interface functionality, IETF Internet-Draft, draft-korhonen-dime-pmip6 [43] and Mobile IPv6 NAS-AAA interface functionality, IETF Internet-Draft, draft-ietf-dime-mip6-integrated [44].

SWn This is the reference point between the Untrusted Non-3GPP IP Access and the ePDG. Traffic on this interface for a UE-initiated tunnel has to be forced towards ePDG. This reference point has the same functionality as Wn which is defined in TS 23.234 [5].

SWu This is the reference point between the UE and the ePDG and supports handling of IPSec tunnels. The functionality of SWu includes UE-initiated tunnel establishment, user data packet transmission within the IPSec tunnel and tear down of the tunnel and support for fast update of IPSec tunnels during handover between two untrusted non-3GPP IP accesses.

SWx This reference point is located between 3GPP AAA Server and HSS and is used for transport of authentication data.

S1 interface for E-UTRAN is the same for both the architectures.

Protocol assumption:

- S2a interface and S2b interface are based on current or future IETF RFCs. S2a is based on Proxy Mobile IP. To enable access via Trusted Non 3GPP IP accesses that do not support PMIP, S2a also supports Client Mobile IPv4 FA mode. S2b is based on Proxy Mobile IP.

- S2c is based on DSMIPv6 [10].

- The PMIP-based S5, PMIP-based S8 and S2a/S2b interfaces are based on the same protocols and differences shall be minimized. The S5 interface is based on current or future IETF RFCs. The GTP variant of S5 interface is described in TS 23.401 [4].

- PMIP-based S8 interface is based on current or future IETF RFCs. The GTP variant interface is described in TS 23.401 [4].

- The PMIP-based interfaces (S5, S8, S2a, and S2b) shall support Generic Routing Encapsulation (GRE) RFC 2784 [23] including the Key field extension RFC 2890 [24]. The Key field value of each GRE packet header should enable the unique identification of the UE PDN connection that the GRE packet payload is associated with. These keys are exchanged using GRE Options extension to PMIP Proxy Binding Update and Proxy Binding Ack messages on PMIP-based interfaces, draft-giaretta-netlmm-mip-interactions [37].

- In case of CN node relocation, the GRE key for uplink traffic is forwarded to the target S-GW over S10/S11 reference point.

- SWu interface is based on IKEv2 [9] and MOBIKE [18].

The EPS shall allow the operator to configure a type of access (3GPP or non-3GPP) as the "home link" for Client Mobile IP purposes.

NOTE: Redundancy support on reference points PMIP-based S5 and PMIP-based S8 should be taken into account.

4.4.2 Reference Point Requirements

4.4.2.1 S5 Reference Point Requirements

Both the GTP and PMIP variants of the S5 reference point shall satisfy the following architectural principles:

- There shall be only one radio interface protocol stack defined, common for both S5 variants, including both radio layer and Non-Access Stratum protocols.
- There shall be only one S6a interface defined common to both S5 variants. There may be a need for different information elements specific to PMIP-based or GTP-based variants of S5 but differences due to the S5 variants should be minimized.
- In the non-roaming case, there shall be only one Gx interface defined for transfer of policy and charging rules, common to both S5 variants. There may be a need for different information elements specific to PMIP-based or GTP-based variants of S5 but differences due to the S5 variants should be minimized.
- Differences between S5 variants in terms of functional split between the endpoints should be minimized.

The S5 reference point shall fulfil the following requirements:

- S5 shall allow access to multiple PDNs. It shall be possible to allow an UE to connect to different packet data networks. It shall also be possible to support a UE with concurrent connections to several packet data networks.
- S5 shall be able to transport both IPv4 and IPv6 user plane traffic independent of IP version of the underlying IP transport network.
- S5 shall support fault handling. There should be mechanisms to identify and signal faults for groups of mobiles – e.g., if a large node handling millions of terminals goes down.

NOTE: As further development of the architecture takes place as well as when additional functionality such as MBMS, LCS etc. are addressed, further requirements will be needed.

4.4.2.2 Gx Reference Point Requirements

The Gx reference point shall satisfy the following architectural principles:

- Gx shall be based on an evolution of the Gx application specified in TS 29.212 [26];
- Gx shall support transfer of PCC information at the SDF (Service Data Flow) level;
- Gx shall support transfer of access network and location information.

4.4.2.3 Gxa/b/c Reference Point Requirements

The Gxa/b/c reference point shall satisfy the following architectural principles:

- Gxa/b/c shall be based on an evolution of the Gx application specified in TS 29.212 [26];
- Gxa/b/c shall support transfer of QoS parameters and related packet filters;
- Gxa/b/c shall support transfer of control information.

4.4.2.4 S9 Reference Point Requirements

The S9 reference point shall satisfy the following architectural principles:

- S9 shall be based on an evolution of the Rx/Gx application specified in TS 29.212 [26] and TS 29.214 [27];

Editor's note: It is FFS what components of Rx and Gx will be used by S9.

- S9 shall support transfer of PCC information at the SDF (Service Data Flow) level for the Local Breakout;
- S9 shall support transfer of QoS parameters and related packet filters for all other cases;
- S9 shall support transfer of control information;
- Gxa or S9 are terminated in the Trusted non-3GPP Accesses, if supported.

4.5 High Level Functions

4.5.1 PDN GW Selection Function for Non-3GPP Accesses

PDN Gateway selection for non-3GPP accesses uses similar mechanisms as defined in TS 23.401 [4], with the following modification:

- The PDN Gateway selection function interacts with the 3GPP AAA Server or 3GPP AAA Proxy and uses subscriber information provided by the HSS to the 3GPP AAA Server. To support separate PDN GW addresses at a PDN GW for different mobility protocols (PMIP, MIPv4 or GTP), the PDN GW Selection function takes mobility prototocol type into account when deriving PDN GW address by using the Domain Name Service function.

During the initial authorization, PDN Gateway selection information for each of the subscribed PDNs is returned to the non-3GPP access system. The PDN Gateway selection information includes:

- The identity of a PDN GW which is a logical name (FQDN) 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.

This enables the entity requiring the address of the gateway to proceed with selection. Once the selection has occurred, the PDN Gateway registers its association with a UE and the APN with the AAA/HSS. This permits the 3GPP AAA Server or Proxy to provide association of the PDN Gateway address and the related APN subsequently.

In the case that a UE already has assigned PDN Gateway(s), the IP identity(ies) of the already allocated PDN Gateway(s) are returned by the 3GPP AAA Server or Proxy during the authorization step. This eliminates the need to repeat PDN Gateway selection for the PDNs the UE is already connected with.

Upon mobility between 3GPP and non-3GPP accesses, PDN Gateway selection information for the subscribed PDNs the UE is not yet connected with is returned to the target access system as done during initial attachment. For the PDNs the UE is already connected with transfer of PDN GW information takes place as defined below:

- If a UE attaches to a non-3GPP access and it already has assigned PDN Gateway(s) due to a previous attach in a 3GPP access, the HSS provides the IP identity(ies) of the already allocated PDN Gateway(s) with the corresponding PDN information to the 3GPP AAA server over the SWx reference point. The PDN gateway's address(es) is derived from the PDN GW identity(ies) and the protocol type on S2 and S5/S8 using Domain Name Service function and sent during the attach procedure in the non-3GPP access.
- If a UE attaches to a 3GPP access and it already has an assigned PDN Gateway(s) due to a previous attach in a non-3GPP access, the HSS provides the IP identity(ies) of the already allocated PDN Gateway(s) with the corresponding PDN information to the MME over the S6a reference point. The PDN gateway address(es) is derived from the PDN GW identity(ies) and the protocol type on S5/S8 using Domain Name Service function and sent during the attach procedure in the 3GPP access.

The HSS receives the values of identity(ies) of all allocated PDN GWs and the corresponding PDN information for a given UE, from both the 3GPP AAA and also from the MME, depending on the currently in-use access. The HSS is responsible for the storage of PDN GW identity information.

Editor's Note: It is FFS whether the PDN Gateway selection mechanism defined in 23.401 can be used to determine the Serving Gateway.

The interaction between the 3GPP AAA Server and the HSS is not explicitly presented in several figures of this specification. Though these entities are depicted as "AAA/HSS" in these figures, these functions are distinct and interact over the SWx interface as described in this subclause.

NOTE: The location of the PDN GW selection function depends upon the type of S2 interface used for attachment and the IP mobility mechanism being used.

- For PMIPv6 on S2a/b, the entity requesting the PDN Gateway is the entity acting as Mobile Access Gateway (MAG).
- For the S8-S2a/b chained cases, the PDN GW information is sent together with the selected Serving GW address from the 3GPP AAA proxy to the entity acting as MAG in the non-3GPP access network during access authentication and authorization. The PDN GW selection mechanism is the same as in the unchained case. The MAG function of the non-3GPP access network conveys the PDN GW address to the Serving GW as part of the PMIPv6 PBU message.
- For MIPv4 FA mode on S2a, the entity requesting the PDN Gateway is the entity that plays the role of the FA.

4.5.2 PDN GW Selection Function for S2c

For the S2c reference point, the UE needs to know the IP address of the PDN Gateway for the PDN the UE wants to connect to. This address is made known to the UE using one of the following methods:

1) Via the attach procedure for 3GPP access (as defined in TS 23.401)
2) Via IKEv2 during tunnel setup to ePDG
3) If the IP address of the PDN GW is not received using options 1-2 above and if the UE knows that the HA is in the PDN where the UE is attached to then the UE shall request a PDN Gateway address via DHCP draft-ietf-mip6-bootstrapping-integrated-dhc [41].
4) If the IP address of the PDN GW is not delivered using options 1-3 above the UE can interact directly with the Domain Name Service function by composing a FQDN corresponding to the PDN.

For the S2c reference point, the network can force a reallocation of the PDN Gateway selected upon initial DSMIPv6 bootstrapping for the PDN the UE wants to connect to. This may happen if one of the following situations occurs:

- The UE has done initial network attachment on an access system supporting network-based mobility, but the PDN Gateway discovered by the UE for the S2c reference point is different from the PDN Gateway allocated at initial network attachment. In this case, to enable IP address preservation based on DSMIPv6 upon inter-system mobility, the network must trigger a PDN Gateway reallocation for the S2c reference point, to re-direct the UE to the PDN Gateway that was selected upon initial network attachment.
- The UE has done initial network attachment over S2c and, relying on DNS, has discovered a sub-optimal PDN Gateway. In this case, based on operator's policies, the network can optionally trigger a PDN Gateway reallocation to re-redirect the UE to a PDN Gateway that can provide better performance.

PDN Gateway reallocation for the S2c reference point is triggered by the AAA/HSS at the first BU/BA exchange following DSMIPv6 bootstrapping.

NOTE: This reallocation is initiated only if the UE has not yet successfully established a binding with the selected PDN GW.

4.5.3 Serving GW Selection Function for Non-3GPP Accesses

The S-GW selection function allocates an S-GW that acts as a local anchor for non-3GPP access in the case of S8-S2a/b chained roaming. Whether S8-S2a/b chaining should be used and which S8 variant to be used is decided by 3GPP AAA Proxy based on per-HPLMN configuration.

The Serving GW selection function is located in 3GPP AAA Proxy. If an S-GW is needed for non-3GPP access in the visited network, the 3GPP AAA proxy will select an S-GW for the UE during initial attach or handover attach. The 3GPP AAA proxy shall send the selected S-GW address and the protocol type over S8 (GTP or PMIP) to the MAG function of the Trusted non-3GPP IP access or ePDG in the chained S8-S2a/b scenarios.

There is no mechanism standardized for S-GW address preservation for handover between 3GPP and non-3GPP in S2/S8 chained case within this Release of the specification.

4.5.4 ePDG Selection

The UE may select the ePDG by static configuration.

Dynamic ePDG selection by the UE is performed after the UE attaches to the non 3GPP access which is untrusted.

If the ePDG needs to be dynamically selected when the UE roams in a VPLMN which VPLMN ID is known by the UE, the procedure is as follows:

- The UE constructs an FQDN using the VPLMN ID as the Operator Identifier and employs the DNS server function to obtain the IP address(es) of the ePDG(s) in the VPLMN.
- The UE selects an ePDG address from the list returned in the DNS response and initiates the IPsec tunnel establishment.

Otherwise if the ePDG needs to be dynamically selected the procedure is as follows:

- The UE constructs an FQDN using the HPLMN ID and employs the DNS server function to obtain the IP address(es) of the ePDG(s).
- The UE selects an ePDG address from the list returned in the DNS response and initiates the IPsec tunnel establishment.

A UE connected to one or multiple PDN GWs uses a single ePDG. In case of handover between ePDGs, the UE may be temporarily connected to two ePDGs.

4.5.5 PCRF Selection

In addition to the PDN-GW and AF being served by one or more PCRF nodes in a HPLMN and, where applicable , in VPLMN as in TS 23.401 [4], the following nodes in this specification also are served by PCRF:

- Serving GW;
- Elements in trusted non-3gpp access;
- ePDG.

Selection of a PCRF by nodes served by PCRF in this specification, is the same as that in specified in TS 23.203 [19].

4.5.6 DSMIPv6 Home Link Detection Function

The DSMIPv6 Home Link Detection Function is used by the UE to detect if, for a specific PDN, an access interface is the Home Link from a DSMIPv6 perspective.

It is up to the UE configuration to decide when to trigger the home link detection function for a specific PDN connection, except that homelink detection for an access interface shall be performed before sending any DSMIPv6 Binding Update via that access interface.

The home link detection function can be performed in one of the following ways:

~ If supported by the UE, the UE may be dynamically configured by the operator to know that when connected to a 3GPP access it is on the Home Link. In this case, this configuration information is delivered to the UE in the PCO during 3GPP attach.

~ The UE compares the IPv6 prefix associated with a specific access interface of the UE , and the Home Network Prefix (HNP) associated with the PDN connection. If there is a match, the UE detects it is in the home link for this specific PDN over the access interface. Otherwise, the UE detects it is not in the home link for this specific PDN over the access interface.

NOTE: The UE knows the IPv6 prefix associated with a specific access system interface via IP address allocation mechanisms applied in that access system.

The UE knows the HNP associated with a specific PDN from the IPsec security association bootstrap (see clause 6.3, step 4) or from PCO received in 3GPP attach.

4.6 Identities

4.6.1 User Identification

In order to access the 3GPP Evolved Packet Core from non-3GPP accesses, and get Authentication, Authorization and Accounting services from the Evolved Packet Core, the NAI RFC 4282 [15] based user identification defined in TS 23.003 [16] shall be used.

In order to support network-based and client-based mobility related services from the evolved packet core, the NAI RFC 4282 [15] based user identification as defined in TS 23.003 [16] shall be used by the network and mobility clients. The username part of NAI shall be based on IMSI. This applies to S2a, S2b and S2c reference points.

User identification in non-3GPP accesses may require additional identities that are out of the scope of 3GPP. These user identities, if not compliant to TS 23.003 [16], are however not sufficient to identify a user in the 3GPP Evolved Packet Core.

4.7 IP Address Allocation

4.7.1 IP Address Allocation with PMIP-based S5/S8

The IP address allocation mechanisms described in clause 5.3.1.1 of TS 23.401 [4] are also valid for the PMIP based S5/S8. This section is complementary to section 5.3.1 of TS 23.401 [4] and describes the differences in the IP Address when PMIP-S5 is used.

For IP address allocation with PMIP-based S5/S8, the following clarifications apply:

- IPv4 address allocation via default bearer activation. This case does not present any architecture differences from the GTP based S5/S8 described in clause 5.3.1.2.1 of TS 23.401 [4].
  - If External PDN Address Allocation is used then the PDN-GW follows the same procedures defined in TS 23.401 [4].
- IPv4 address allocation and IPv4 parameter configuration via DHCPv4 according to RFC 2131 [28] and RFC 4039 [29]: In this case the Serving GW shall have DHCPv4 relay agent functionality.

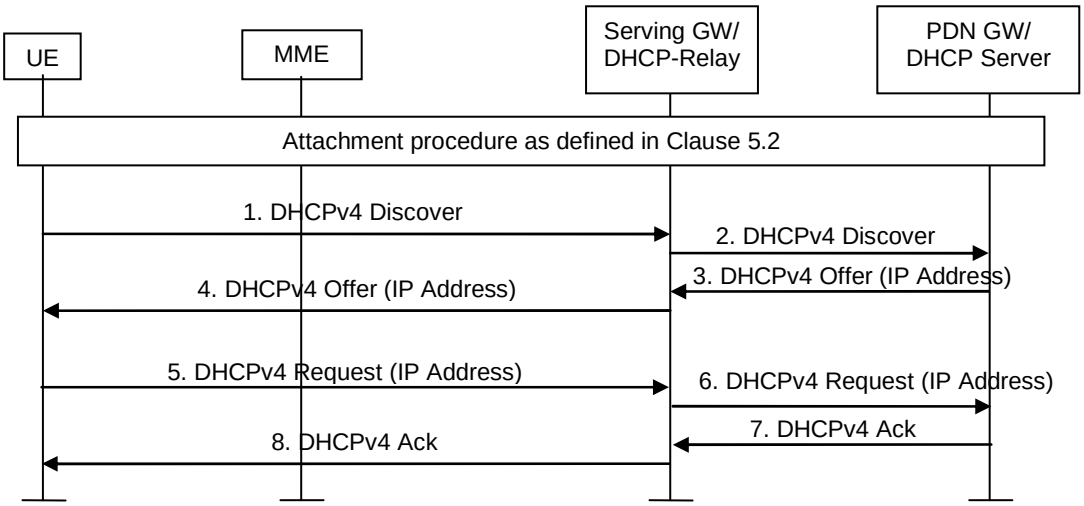


Figure 4.7.1-1: IPv4 Address Allocation using DHCP with DHCP Server Collocated with the PDN GW and DHCP Relay in the Serving GW

1. The UE IPv4 address received from the PDN GW in the PBA message shall not be delivered to the UE when the attachment is completed. After the default bearer is setup, the UE sends a DHCP Discovery message in broadcast to the network to find available servers.

2. Upon receiving the DHCP Discovery message, the Serving GW acting as a relay agent shall add its address in the GIADDR option and add the assigned UE IP address (received from PDN GW at the PBA message) in the "Address Request" option, and relay the message in unicast within the PMIP tunnel to PDN GW acting as a DHCPv4 server.

3. When receiving the DHCP Discovery message, the PDN GW should verify the GIADDR option. Then the PDN GW uses "Address Request" option to identify the UE binding and update it with the 'client identifier' and 'chaddr' combination for subsequent DHCP procedure. After that the PDN GW extends an IP lease offer and sending the DHCP Offer with the assigned UE IP address.

4. The Serving GW acting as DHCP relay agent relays the DHCP message to the UE.

5. When the UE receives the lease offer, it sends a DHCPREQUEST message containing the received IP address.

6. The Serving GW acting as DHCP relay agent relays the DHCP message to the PDN GW.

7. When the PDN GW receives the DHCPREQUEST message from the UE, it sends a DHCPACK packet to the UE. This message includes the lease duration and any other configuration information that the client might have requested.

8. The Serving GW acting as DHCP relay agent relays the DHCP message to the UE.

9. When receiving the DHCPACK message, the UE completes TCP/IP configuration process.

NOTE 1: The PDN GW shall discard the unicast DHCP Discovery or Request message with an empty or unknown GIADDR option, if the assigned UE IP address is not delivered to the UE yet.

NOTE 2: The DHCP client may skip DHCP Discovery phase, and send DHCP Request message in broadcast as the first message. In this case, the Serving GW acting as a relay agent shall add its address in the GIADDR option and add the assigned UE IP address (received from PDN GW at the PBA message) in the "Address Request" option, and relay the message in unicast within the PMIP tunnel to PDN GW acting as a DHCPv4 server.

- IPv6 prefix allocation via IPv6 Stateless Address auto-configuration: In this case the difference from the GTP based S5/S8 is that the Serving GW acts as the access router instead of the PDN GW. Note that the Serving GW shall advertise the same information as the PDN GW would advertise with GTP based S5/S8. In the case of PMIP-S5/S8 because any prefix that the Serving GW will advertise to the UE is unique, there is no need for the UE to perform Duplicate Address Detection for global uniqueness for any IPv6 address configured from the

allocated IPv6 prefix. However, the Serving GW shall respond with Neighbor Advertisement upon receiving Neighbor Solicitation messages from a given UE. For example, as the UE may perform Neighbor Unreachability Detection towards the Serving GW, similar to the DAD related functionality supported by PDN GW in the case of GTP-S5/S8 described in section 5.3.1.2.2. Otherwise the PDN GW has the same functions as it is defined in clause 5.3.1.2.2 in TS 23.401 [4].

- IPv6 parameter configuration via Stateless DHCPv6 according to RFC 3736 [30] and RFC 3633 [31]: In this case the Serving GW shall have DHCPv6 relay agent functionality.

- If shorter than /64 IPv6 prefix delegation via DHCPv6 is provided, the Serving GW should act as a DHCPv6 relay agent.

NOTE: Allocation of IP address from an external PDN using Radius or Diameter requires the "Proxy Binding Update" of PMIP to carry the relevant PCO that is transported by GTP.

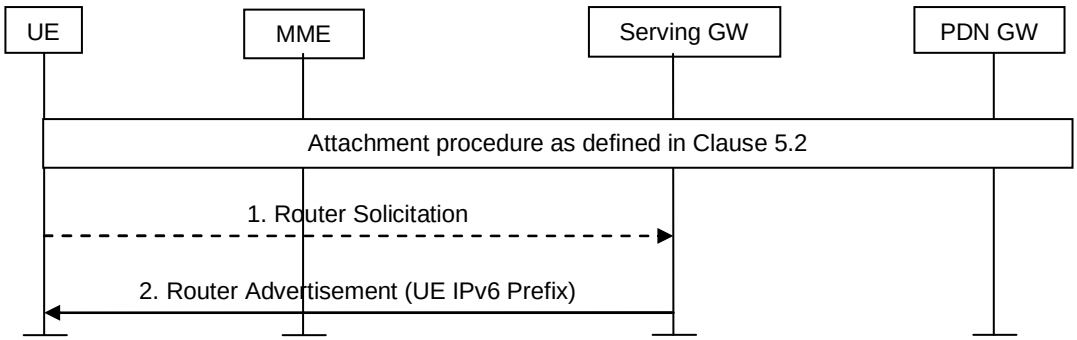


Figure 4.7.1-2: IPv6 Prefix allocation after the Attach procedure

4.7.2 IP Address Allocation in Trusted Non-3GPP IP Access using PMIPv6 on S2a

IP address is allocated to the UE when connectivity to new PDN is initiated. The IP address can be provided by either PDN GW or external PDN. Access GW in non-3GPP access system is responsible for delivering the IP address to the UE. The non-3GPP Access shall support at least one of the following functionalities in order to successfully allocate IP address to the UE in the EPC:

- Support of DHCPv4 relay agent functionality for IPv4 parameter configuration and IP address allocation as specified in RFC 2131 [28] and RFC 4039 [29] and in clause 4.7.1 for Serving GW.This functionality is required to support DHCPv4 based IP address allocation mechanism in the UE.

- Support of DHCPv4 server functionality for IPv4 parameter configuration and IP address allocation as specified in RFC 2131 [28] and RFC 4039 [29]. This functionality is required to support DHCPv4 based IP address allocation mechanism in the UE.

NOTE: The configuration parameters are received from the PDN GW by using DHCPv4 (the non-3GPP Access GW as DHCP client) or PMIP PCO at PBA message. When DHCP is used, the DHCP messages shall be sent within the PMIP tunnel.

- Support of DHCPv6 (relay agent or server) functionality for IPv6 parameter configuration as specified in RFC 3736 [30] and IP prefix delegation as specified in RFC 3663 [31]. This functionality is required to support DHCPv6 based IP prefix delegation and Configuration parameter configuration mechanism in the UE.

- Support of prefix advertisement for IP prefix received from PDN GW in PMIPv6 Proxy Binding Acknowledgement.

- Support for IPv4 Address allocation that is received from PDN GW from PMIPv6 Proxy Binding Acknowledgement using access specific mechanisms.

4.7.3 IP Address Allocation in Untrusted Non-3GPP IP Access using PMIPv6 on S2b

When an Untrusted Non-3GPP IP access is used two types of IP address are allocated to the UE:

- An IP address, which is used by the UE within the Untrusted Non-3GPP IP Access Network to get IP connectivity towards the ePDG.
- One or more IP address(es), which is used by the UE towards the external PDNs via the allocated PDN GW(s).

The IP address that is allocated by the Untrusted Non-3GPP IP Access Network is used as the end point of the IPSec SAs between the UE and the ePDG. The allocation of this IP address is out of the scope of this specification.

The IP address(es) that are allocated by the PDN GW(s) are allocated to the UE when connectivity to a new PDN is initiated. This IP address can be provided by either PDN GW or external PDN as it is specified in clause 5.3.1.1 of TS 23.401 [4]. The ePDG receives the allocated IP address(es) within the Proxy Binding Acknowledgement and the ePDG is responsible for delivering the IP address(es) to the UE.

4.7.4 IP Address Allocation using S2c

Prior the use of S2c an IP address which will be used as a care-of address shall be allocated to the UE.

When a Trusted Non-3GPP Access Network is used one or more IP addresses are allocated to the UE by the Trusted Non-3GPP Access Network. One of these IP addresses is used by the UE as care-of address within DSMIPv6. The allocation of these IP addresses is out of the scope this specification.

When an Untrusted Non-3GPP Access Network is used one or more IP addresses are allocated to the UE by the Untrusted Non-3GPP Access Network. The allocation of these IP addresses is out of the scope of 3GPP. One of these IP addresses is used by the UE as the IP address towards the ePDG when IPSec SAs are established. During the IPSec SA establishment the ePDG allocates and delivers an IP address to the UE, which IP address is used by the UE as care-of address within DSMIPv6. This IP addess is allocated by the ePDG either by using an internal address pool or using an external server, such as DHCP. The allocation of this IP address is implementation specific.

When a UE is connecting to a PDN via S2c, address allocation for that PDN takes place as follows.

During IKEv2 exchange for bootstrapping the DSMIPv6 security association (see clause 6.3) the following parameters can be negotiated between the UE and the PDN GW/HA:

- The IPv6 prefix to which the IPv6 Home Address belongs, also called the "Home Network Prefix";
- The UE's IPv6 Home Address;
- The UE's IPv4 Home Address;
- The DNS server address for that PDN.

The UE may also request additional configuration parameters by running stateless DHCP as defined in RFC 4039 [29] and RFC 3736 [30] over the DSMIPv6 tunnel.

The UE may also request an IPv4 home address using DSMIPv6 signaling, as defined in draft-ietf-mip6-nemo-v4traversal [10].

4.8 Network Discovery and Selection

4.8.0 General Principles

The following principles have been identified regarding multi-access network selection (between operators & RAT types) and discovery when both 3GPP and non-3GPP accesses are available or when multiple non-3GPP accesses are available:

- The EPS network may provide the UE with assistance data/policies about available accesses to allow the UE to scan for accesses and select an access.

- The EPS network allows the home and visited operator to influence the access that the UE shall handover to (when in active mode) or re-select (when in idle mode).
- Multi-access network discovery and selection works for both single-radio and multiple- radio terminals.
- No architectural impact is foreseen for network selection upon initial network attachment.
- The UE may provide information to the network for the retrieval of the assistance data/policies.

The multi-access network discovery and selection mechanism shall not interfere with either existing 3GPP PLMN selection mechanisms used for the 3GPP Access Technologies or existing 3GPP2 network selection mechanisms.

The ANDSF's policy and the UE implementation shall ensure that the UE does not change PLMN more often than the time stored in the USIM (in EF_{HPLMN}, see TS 31.102 [46]) for the "periodic network selection attempts" specified in TS 22.011 [47].

4.8.1 Architecture for Access Network Discovery Support Functions

The following architecture may be used for access network discovery and selection. The support and the use of these functions and interfaces are optional.

Figure 4.8.1.1-1: Architecture for Access Network Discovery Support Functions

4.8.2 Network Elements

4.8.2.1 Access Network Discovery and Selection Function (ANDSF)

The ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data as per operators' policy. The ANDSF is able to initiate data transfer to the UE, based on network triggers, and respond to requests from the UE.

NOTE: The usage of ANDSF capabilities is intended for scenarios where access-network level solutions are not sufficient for the UE to perform Network Discovery and Selection of non-3GPP technologies according to operator policies.

The ANDSF shall be able to provide the following information:

1) Inter-system mobility policy:

   - The inter-system mobility policy is a set of operator-defined rules and preferences that affect the inter-system mobility decisions taken by the UE. The UE uses the inter-system mobility policy to:

     (i) decide when inter-system mobility is allowed or restricted; and

     (ii) to select the most preferable access technology type or access network that should be used to access EPC.

     For example, an inter-system mobility policy may indicate that inter-system handover from E-UTRAN access to WLAN access is not allowed. It may also indicate e.g. that WiMAX access is more preferable to WLAN access.

   - The inter-system mobility policy may be provisioned in the UE and may be updated by the ANDSF based on network triggers or after receiving a UE request for network discovery and selection information.

   - The inter-system mobility policy identifies which access technology type or which specific access network is mostly preferable for EPC access. It shall be able to indicate:

- If a specific access technology type is preferable to another (e.g. WiMAX is preferable to WLAN).
- If a specific access network identifier is preferable to another (e.g. WLAN SSID-1 is preferable to WLAN SSID-2).

- The inter-system mobility policy identifies also when inter-system mobility is allowed or restricted. It shall be able to indicate:
  - If inter-system mobility is restricted from one access technology type to another (e.g. handover from WiMAX to WLAN is restricted).
  - If inter-system mobility is restricted when certain conditions are met.
  - Validity conditions, i.e. conditions indicating when a policy is valid (such conditions may include e.g. a time duration, a location area, etc.). The validity conditions may also indicate when the UE shall request for new policies.

2) Access network discovery information:

- Upon UE request, the ANDSF may provide a list of access networks available in the vicinity of the UE for all the access technology types requested by the UE (if requested any).
- The ANDSF provides information for access networks that are available to the UE including:
  - the access technology type (e.g. WLAN, WiMAX).
  - the access network identifier (e.g. the SSID of a WLAN).
- other technology specific information, e.g. one or more carrier frequencies.
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).
- The UE may retain and use the access network discovery information provided by the ANDSF until new/updated information is retrieved.
- The UE shall select the most preferable available access network for inter-system mobility based on the received / provisioned inter-system mobility policies.

The ANDSF shall be able to limit the amount of information provided to the UE based e.g. on the UE's current location, UE capabilities, operator's policies, etc.

The ANDSF shall be able to limit the frequency of UE initiated requests e.g. with a minimum time interval that shall elapse between two consequtive UE initiated requests towards the ANDSF.

There are two types of information provided by the ANDSF, i.e. the inter-system mobility policy and the access network discovery. The ANDSF may provide both types of information or only one of them, according to the operator requirements.

4.8.3 Reference Points

S14 This reference point is between UE and ANDSF for direct queries via pull. It enables dynamic provision of information to the UE for NW discovery and selection procedures related to non-3GPP accesses. Push and/or combination of Pull-Push may be supported as well".

Protocol assumption:

- S14 interface is realized above IP level.

4.8.4 ANDSF Discovery

The ANDSF in the HPLMN is discovered through interaction with the Domain Name Service function or the DHCP Server function. The ANDSF address may also be provisioned to the UE.

When the UE is roaming and supports ANDSF discovery, it shall try to discover an ANDSF in the HPLMN.

NOTE: The ANDSF may not be contactable in certain PDNs.

4.8.5 Inter-system Mobility Policies

Policies may be organized in a hierarchy, e.g. a priority order among multiple policies determines which policy is applied with the highest priority.

The inter system mobility policies delivered to UE may have different scopes:

- A generic inter-system mobility policy has an unrestricted scope.
- A UE activity level specific inter-system mobility policy applies to the UE depending on its activity level, e.g.. a certain policy may apply to the UE while it is "active" , while another policy (or no policy) may apply to the UE while it is "idle".

Editors Note: How "active" and "idle" are defined is FFS.

4.9 Authentication and Security

4.9.1 Access Authentication in non-3GPP Accesses

Non-3GPP access authentication defines the process that is used for Access Control i.e. to permit or deny a subscriber to attach to and use the resources of a non-3GPP IP access which is interworked with the EPC network. Non-3GPP access authentication signalling is executed between the UE and the 3GPP AAA server/HSS. The authentication signalling may pass through AAA proxies.

3GPP based access authentication is executed across a SWa/STa reference point as depicted in the EPS architecture diagram. Following principles shall apply in this case:

- Transport of authentication signalling shall be independent of the non-3GPP IP Access technology.
- The 3GPP based access authentication signalling shall be based on IETF protocols, for e.g., Extensible Authentication Protocol (EAP) as specified in RFC 3748 [11].

The details of the access authentication procedure are defined in TS 33.402 [45].

4.9.2 Tunnel Authentication

Tunnel authentication refers to the procedure by which the UE and the ePDG perform mutual authentication during the IPsec tunnel establishment between the UE and the ePDG (SWu reference point).

Tunnel authentication is used only in case of Untrusted Non-3GPP Access and is executed across a SWm reference point as depicted in the EPS architecture diagram.

The details of the tunnel authentication procedure are defined in TS 33.402 [45].

4.10 QoS Concepts

4.10.1 General

The QoS model that is applied in conjunction with PMIP-based reference points does not use bearer IDs in user plane packets. Instead it is based on packet filters and associated QoS parameters (QCI, ARP, MBR, GBR) provided to the access system through off-path signalling.

The PCRF signals the same packet filters and associated QoS parameters over Gxa, Gxb and Gxc as over S7; in other words the granularity of the QoS information that is passed over Gxa, Gxb and Gxc is the same as over S7.

4.10.2 PCC/QoS Principles

The following are the principles around PCC/QoS functionality:

1) Full PCEF with service-aware end-user charging is located only in PDN-GW.

2) Bearer binding for the S1 interface in case of S5/S8(PMIP) is to be performed in the SGW. This does not impact SGW relocation.

3) To enable S1 bearer binding in case of S5/S8(PMIP), off-path signalling is applied from the PCRF to SGW.

4) To enable bearer binding for non-3GPP accesses, off-path signalling is applied from the PCRF to the non-3GPP access if the non-3GPP access supports PCC. For the roaming case this interface can also terminate in the ePDG.

5) The visited network has the capability to reject the QoS authorized by the home network based on the visited network operator policies.

6) The signalling interface described in 3) and 4) is assumed to be the same.

4.10.3 The EPS Bearer with PMIP-based S5/S8 and E-UTRAN access

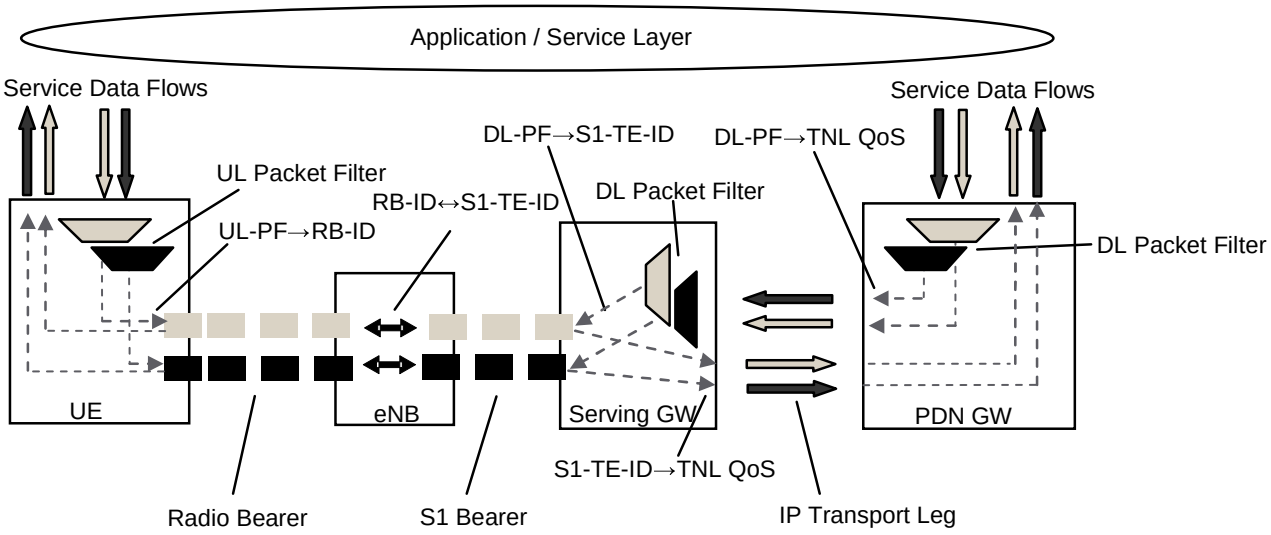


Figure 4.10.3-1: Two Unicast EPS bearers (PMIP-based S5/S8 and E-UTRAN access)

For PMIP-based S5/S8 and E-UTRAN access, an EPS bearer consists of the concatenation of one Radio Bearer and one S1 bearer. The PDN Connectivity Service between a UE and an external packet data network is supported through a concatenation of an EPS Bearer and IP connectivity between Serving GW and PDN GW. QoS control between a Serving GW and a PDN GW is provided at the Transport Network Layer (TNL).

The EPS bearer is realised by the following elements:

- An UL TFT in the UE binds an SDF to an EPS bearer in the uplink direction. Multiple SDFs can be multiplexed onto the same EPS bearer by including multiple uplink packet filters in the UL TFT.

- A DL TFT in the Serving GW binds an SDF to an EPS bearer in the downlink direction. Multiple SDFs can be multiplexed onto the same EPS bearer by including multiple downlink packet filters in the DL TFT.

- A radio bearer transports the packets of an EPS bearer between a UE and an eNodeB. There is a one-to-one mapping between an EPS bearer and a radio bearer.

- An S1 bearer transports the packets of an EPS bearer between an eNodeB and a Serving GW. There is a one-to-one mapping between an EPS bearer and a S1 bearer.

- A per UE per PDN tunnel transports the packets of an EPS bearer between a Serving GW and a PDN GW. There is a many-to-one mapping between an EPS bearer and this per UE, per PDN tunnel.

- A UE stores a mapping between an uplink packet filter and a radio bearer to create the binding between an SDF and a radio bearer in the uplink.

- An eNodeB stores a one-to-one mapping between a radio bearer and an S1 bearer to create the binding between a radio bearer and an S1 bearer in both the uplink and the downlink direction.

- A Serving GW stores a one-to-one mapping between a downlink packet filter and an S1 bearer to creating the binding between an SDF and an S1 bearer in the downlink.

4.10.4 Application of PCC in the Evolved Packet System

EPS supports both static and dynamic PCC deployment options as specified in TS 23.401 [4].

NOTE: The local configuration of PCEF static policy and charging control functionality is not subject to standardization and is not based on subscription information.

In case of non-3GPP access that does not support an Gxa/b or S9 interface, static QoS policies (e.g. based on subscription QoS parameters for default connectivity) may be provided to the non-3GPP access through the AAA infrastructure. To perform policy enforcement according to the subscription QoS parameters for default connectivity, additional information may be provided to the PDN GW in one of the following ways:

- from the PCRF, if present and if the PDN GW supports the Gx interface;

- from the 3GPP AAA Server through the S6b interface in the form of a static QoS profile.

NOTE: In the latter case the PCEF may change the provided values based on interaction with the PCRF or based on local configuration.

When dynamic policy provisioning is not deployed, the PDN GW in case of PMIP based signalling uses the access type information (RAT Type in 3GPP access) contained in Proxy Binding Update messages for, e.g. charging. When dynamic policy provisioning is deployed, the PDN GW relies on the PCRF for indication of the handling required due to the access technology.

The behaviour of the system when PCC is deployed only in VPLMN or only in HPLMN is described in TS 23.203 [19].

4.11 Charging for Non-3GPP Accesses

The following are related to Non-3GPP accesses:

- Accounting information, e.g. the amount of data transmitted in uplink and downlink direction categorized with the QCI per UE, could be collected by components, if any, in the Non-3GPP access networks for inter-operator settlements.

NOTE: Specification of the above functionality is outside the scope of this TS.

4.12 Multiple PDN Support

This section provides high level principles for the support of multiple-PDNs from Non-3GPP IP Accesses. When a UE attaches to the EPS via Trusted/Untrusted Non-3GPP IP Accesses, the following principles apply for multiple PDN support:

- Simultaneous exchange of IP traffic to multiple PDNs is supported in the EPS, when the network policies, non-3GPP access and user subscription allow it. UE Support for multiple overlapping IP address spaces is optional.

- It shall be possible to support in the EPS simultaneous exchange of IP traffic to multiple PDNs through the use of separate PDN GWs or single PDN GW.

- The EPS shall support UE-initiated connectivity establishment to separate PDN GWs or single PDN GW in order to allow parallel access to multiple PDNs.

- The request for additional PDN shall be triggered by the UE.
- It shall be possible for a UE to initiate disconnection from any PDN.

Once a specific IP mobility protocol is selected during initial attach for a specific non-3GPP access, it is not possible for the UE to use different mobility protocols for any of the PDNs that it obtains connectivity on the same non-3GPP access after initial attach. It is not possible for a UE that is connected to multiple PDNs over a 3GPP access to perform an handover to a non-3GPP access and then using different mobility protocols for the various PDNs that it connected with on the same non-3GPP access.

5 Functional Description and Procedures for 3GPP Accesses with PMIP-based S5/S8

5.1 Control and User Plane Protocol Stacks

5.1.2 General

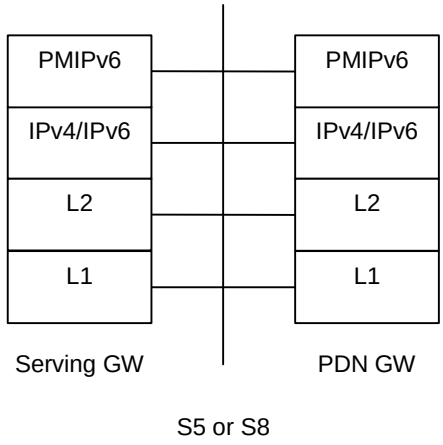
TS 23.401 [4] defines the protocol stack for both the control plane and user plane for 3GPP accesses using GTP-based S5/S8. This section defines the protocol stacks for 3GPP accesses using the PMIP-based S5/S8.

Editor's note: Protocol stacks between Serving Gateway and UE are the same as described in TS 23.401 [4]

Editor's note: According to terms defined in PMIPv6 (draft-ietf-netlmm-proxymip6 [8]), the functional entities terminating both the control and user planes are denoted MAG (Mobile Access Gateway) in the Serving Gateway and LMA (Local Mobility Anchor) in the PDN Gateway. LMA includes also the function of a Home Agent.

5.1.3 Control Plane

5.1.3.1 Serving GW - PDN GW



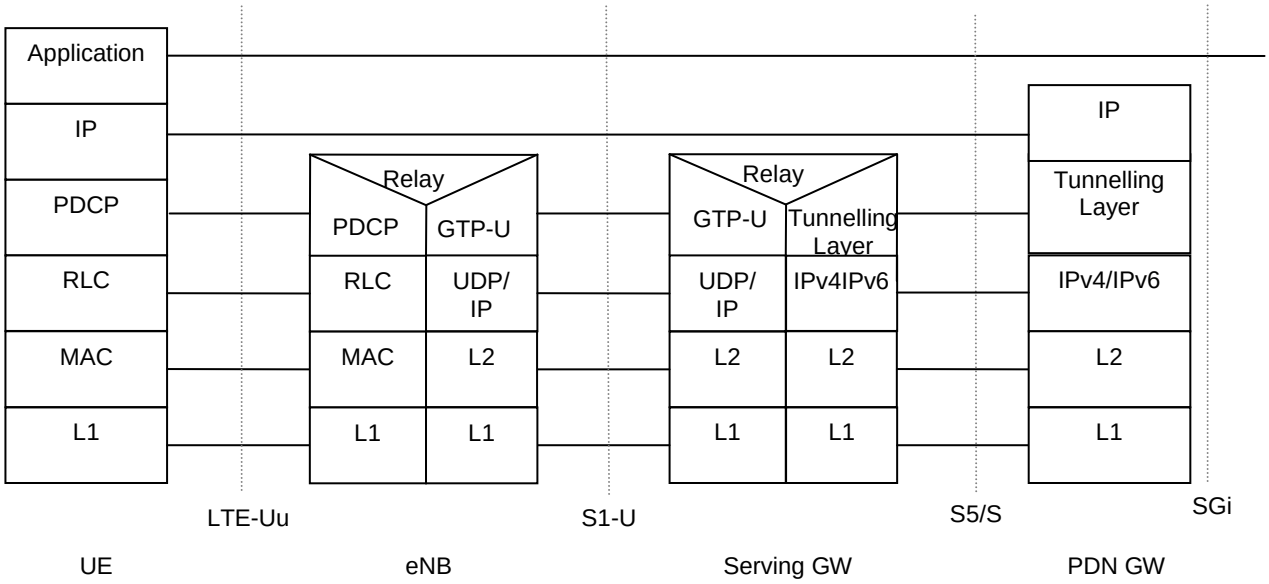
Legend:

- The control part of PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) protocol is used for signalling messages between Serving GW and PDN GW (S5 or S8).

Figure 5.1.3.1-1: Control Plane for PMIP-based S5 and PMIP-based S8 Interfaces

5.1.4 User Plane

5.1.4.1 UE – PDN GW User Plane with E-UTRAN

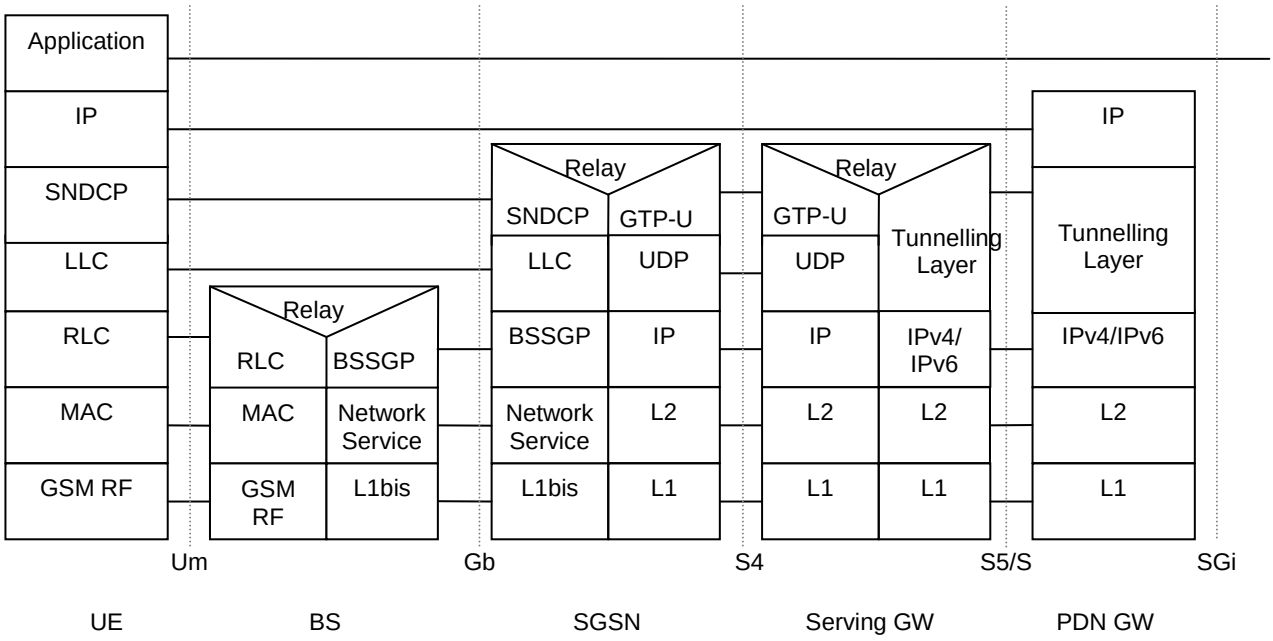


Legend:

- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6 [36].
- MME controls the user plane tunnel establishment and establishes User Plane Bearers between eNB and Serving GW.
- LTE-Uu: The radio protocols of E-UTRAN between the UE and the eNB are specified in TS 36.300 [6].

Figure 5.1.4.1-1: User Plane for E-UTRAN

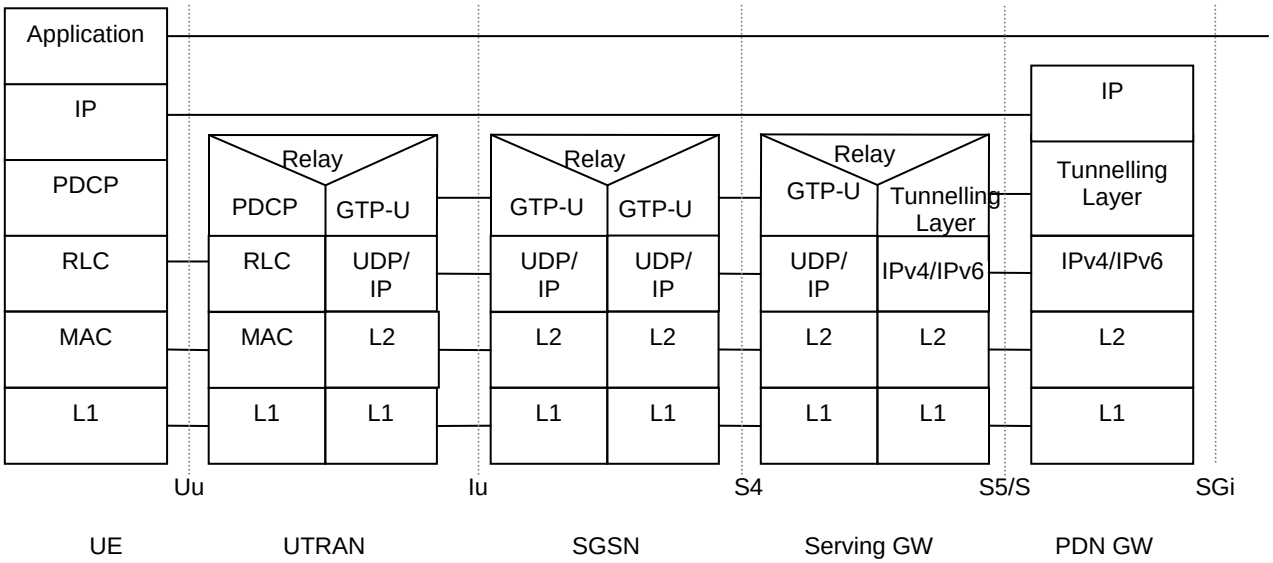
5.1.4.2 UE – PDN GW User Plane with 2G access via the S4 Interface



Legend:
- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6 [36].
- Protocols on the Um and the Gb interfaces are described in the TS 23.060 [21].

Figure 5.1.4.2-1: User Plane for A/Gb mode

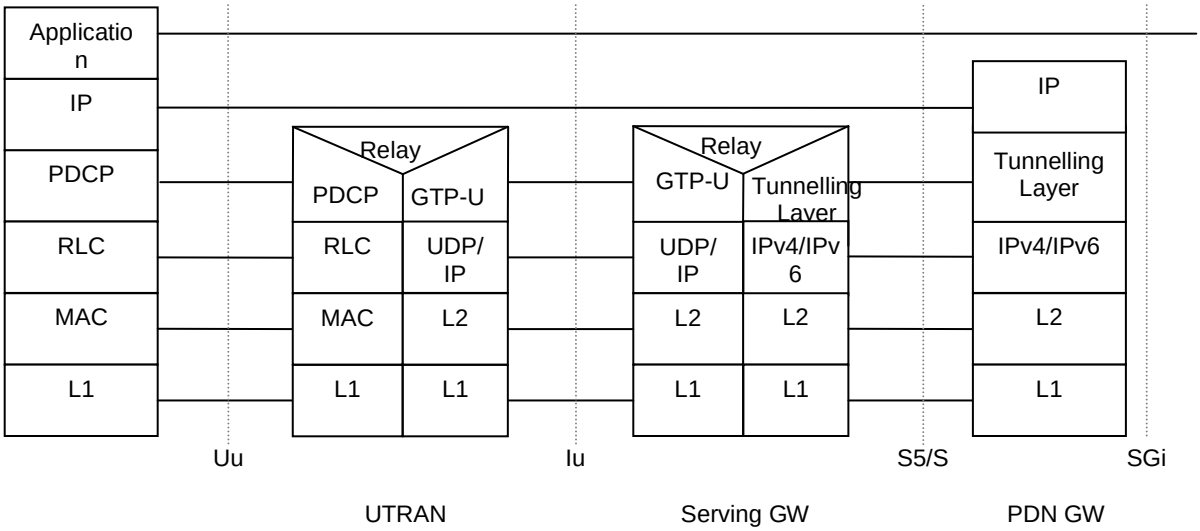
5.1.4.3 UE – PDN GW User Plane with 3G Access via the S4 Interface



Legend:
- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6 [36].
- Protocols on the Uu and the Iu interfaces are described in the TS 23.060 [21].

Figure 5.1.4.3-1: User Plane for Iu mode

5.1.4.4 UE – PDN-GW User Plane with 3G Access via the S12 Interface



Legend:

- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6 [36].
- Protocols on the Uu interface are described in the TS 23.060 [21].
- SGSN controls the user plane tunnel establishment and may establish a Direct Tunnel between UTRAN and Serving GW.

Figure 5.1.4.4-1: User Plane for UTRAN mode and Direct Tunnel on S12

5.2 Initial E-UTRAN Attach with PMIP-based S5 or S8

This section is related to the case when the UE powers-on in the LTE network with PMIP-based S5 or S8 interface and includes the case of roamers from a GTP network into a PMIP network when PMIP-based S5 is used to connect the Serving GW and the PDN GW of the visited PLMN. Proxy Mobile IP is used on S5 or S8 interface. It is assumed that the MAG is collocated with the Serving GW for the PMIPv6 procedure between the Serving GW and the PDN GW.

When only GTP-based S5 or S8 connections are established for roamers from a GTP network into a PMIP network the procedure as described in TS 23.401 [4] applies.

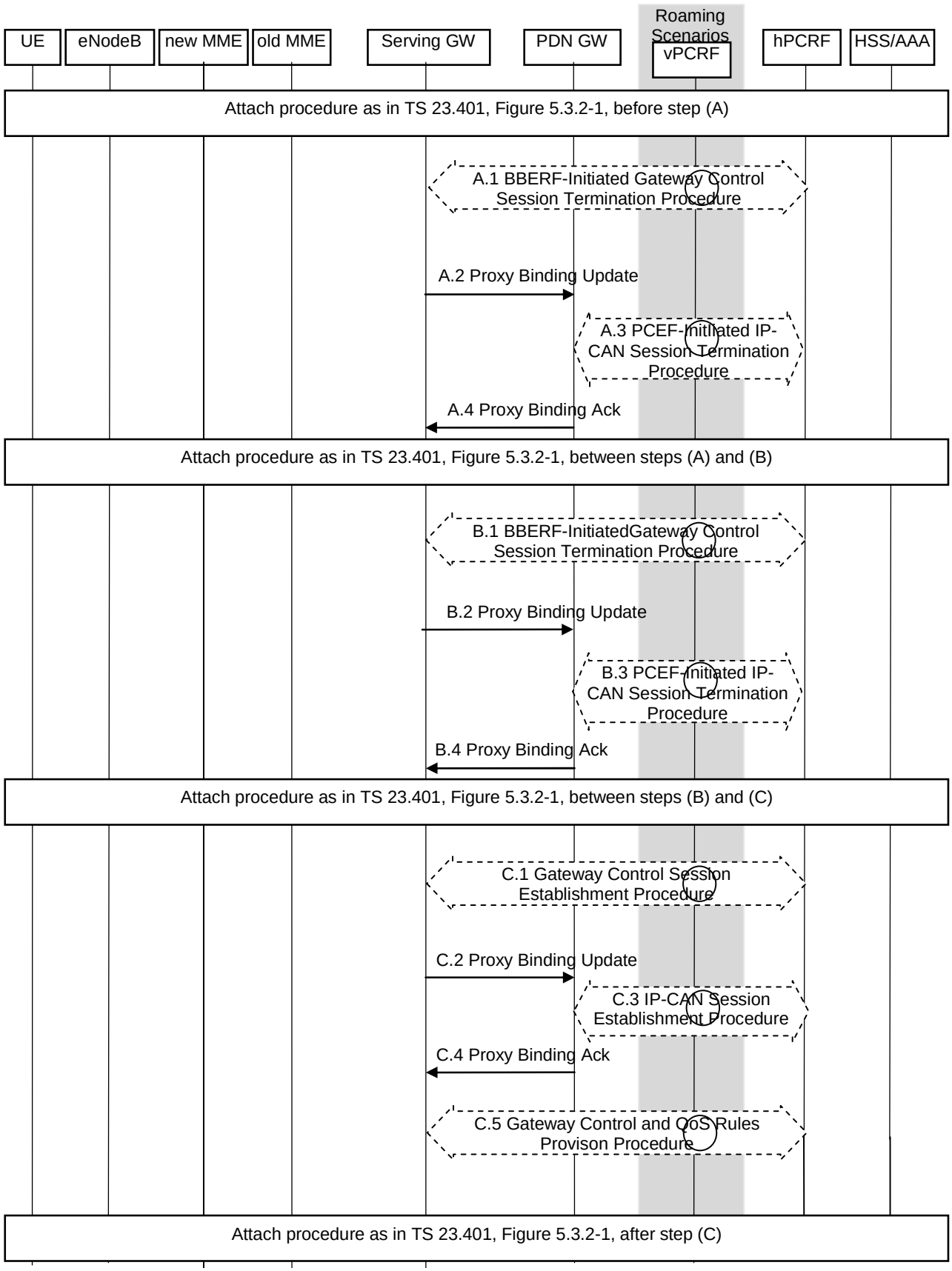


Figure 5.2-1: Initial E-UTRAN attach with PMIP-based S5 or S8

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-5) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF, as specified in TS 23.203 [19]. The S-GW provides information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of the Gateway Control session in S-GW.

A.2) The Serving GW sends a Proxy Binding Update (MN NAI, lifetime=0) message to the PDN GW. The MN NAI identifies the UE. The lifetime field indicates that the message is used to de-register the UE at the PDN-GW.

A.3) The PDN GW initiates the IP CAN session Termination Procedure with the PDN GW as specified in TS 23.203 [19]. The PDN GW provides information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of IP-CAN session related information in the PCRF and in the PDN-GW.

A.4) The PDN GW responds to the Serving GW with the result of the deregistration with Proxy Binding Update Acknowledgement message.

Steps between A.3 and B.1 are described in TS 23.401 [4], clause 5.3.2.

Steps B.1 through B.6 are the same as Steps A.1 through A.6.

C.1) The Serving GW initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The S-GW provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in step C.3 and also to convey subscription related parameters to the PCRF that have been received between steps (B) and (C) from the MME.

C.2) The Serving GW sends a Proxy Binding Update (MN NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, UE Address Info Additional Parameters) to the PDN GW in order to establish the new registration. The MN NAI identifies the UE for whom the message is being sent. The Lifetime field must be set to a nonzero value in the case of a registration. Access Technology Type is set to indicate the RAT type (E-UTRAN). Handover Indication option is set to indicate attachment over a new interface. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The optional Additional Parameters may contain information, for example, protocol configuration options. If both an IPv4 and an IPv6 address is requested for the UE, both IP addresses shall be requested in the same Proxy Binding Update. The UE Address Info IE is used to request an IPv6 address, IPv4 address, or IPv4/IPv6 addresses. Based on PDN Address Allocation received in the Create Default Bearer Request, Serving GW includes request for IPv4 Home Address and/or IPv6 Home Network Prefix in the PBU as specified in PMIPv6 (draft-ietf-netlmm-proxymip6 [8]). If both an IPv4 address and an IPv6 prefix is requested for the UE, IPv4 Home Address and IPv6 Home Network Prefix shall be present in the same Proxy Binding Update. In the case of a subscribed IP address(es) provided by the MME in the PDN Address Allocation IE, the UE Address Info IE is set to the subscribed address(es).

C.3) The PDN GW initiates the IP CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session and associate Gateway Control Sessions established in step C.1 correctly. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers.

C.4) The PDN GW responds with a PMIP Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The PDN GW takes into account the request from Serving GW and the policies of operator when the PDN GW allocates the UE Address Info. The UE address info returns the the newly assigned IPv4 Address(es) and/or IPv6 prefix assigned to the UE, if one was requested in the PMIP Proxy Binding Update message. Otherwise, the PDN GW validates the addresses and returns in the UE Address Info IE the IPv4 address and/or IPv6 prefix received in the Proxy Binding Update message.. The optional Additional Parameter information element may contain other information, including for example Protocol Configuration Options.

Editor's Note: It is FFS how to handle deferred IP Address Allocation when PMIP-based S5/S8 is employed.

C.5) In case the QoS rules have changed, the PCRF updates the QoS rules at the S-GW by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

NOTE: QoS rules may lead to establishment of new dedicated bearers along with the default bearer.

5.3 Detach for PMIP-based S5/S8

In case of detach, all the bearers at the Serving GW are terminated. Further, the IP CAN session for the UE in the PDN GW is also terminated.

The procedure described in this section applies equally to UE, MME and HSS initiated detach procedures.

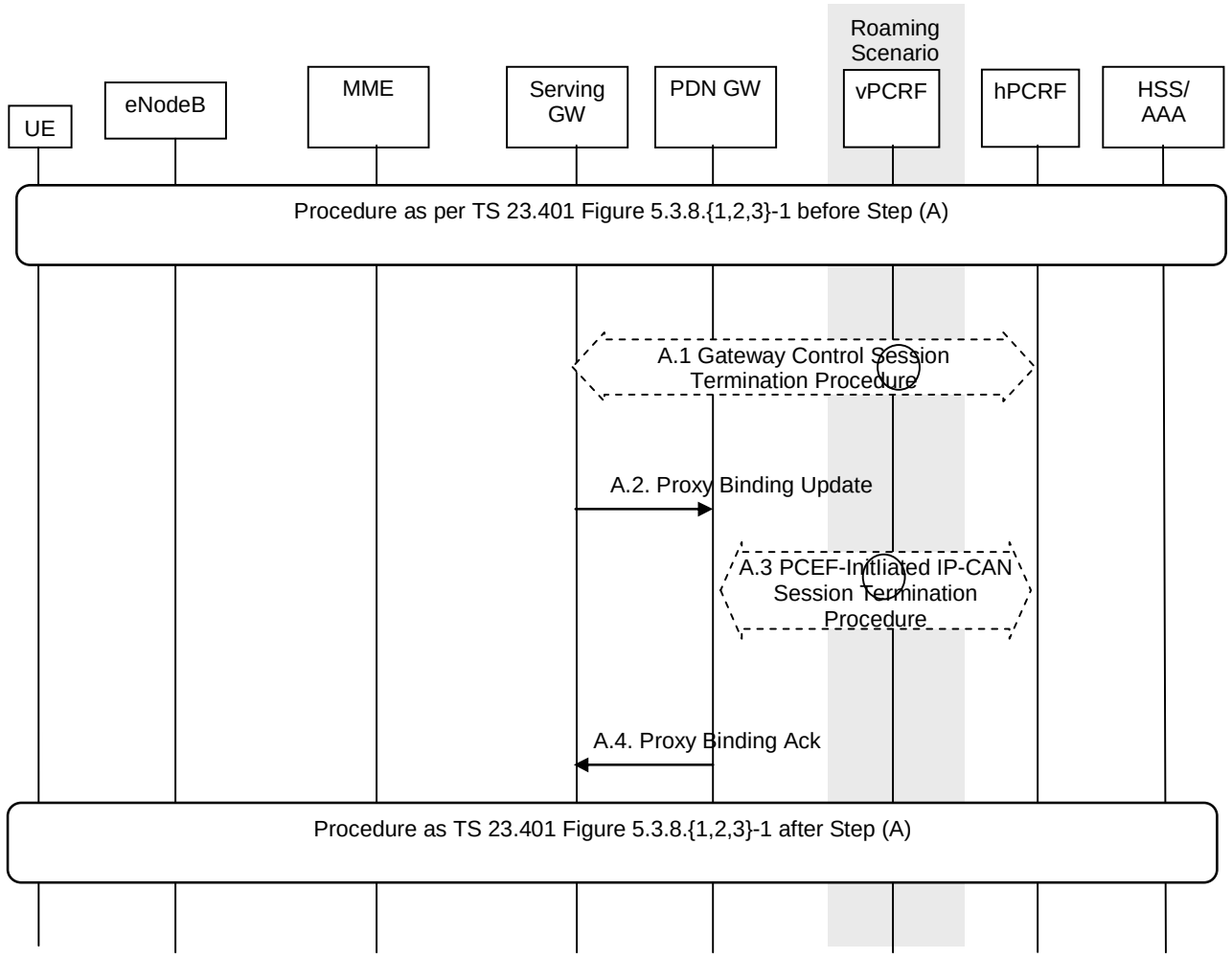


Figure 5.3-1: E-UTRAN Detach Procedure for PMIP-based S5/S8

The optional interaction steps between the gateways and the PCRF in Figure 5.3-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The figure covers both the non-roaming (S5) as per Figure 4.2.1-1 and roaming case (S8) as per Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN acts as an intermediary between the Serving GW and the hPCRF in the HPLMN. The vPCRF forwards messages in both directions. In the case of Local Breakout, the PDN GW exchanges messages with the hPCRF by way of the vPCRF. The vPCRF forwards messages between the PDN GW and the hPCRF in this case. In the non-roaming case, the vPCRF is not involved at all.

A.1) The Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The S-GW provides information to enable the PCRF to unambiguously identify the IP-CAN session corresponding to the Gateway Control Session. This results in the removal of the Gateway Control session in S-GW.

A.2) The Serving GW sends a Proxy Binding Update (MN NAI, lifetime=0) message to the PDN GW to de-register the UE at the PDN-GW. The MN NAI identifies the UE. The lifetime field indicates that the message is used to de-register the UE at the PDN-GW.

A.3) The PDN GW initiates the PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The PDN GW provides information to enable the PCRF to uniquely identify the

IP-CAN session. This results in the removal of IP-CAN session related information in the PCRF and in the PDN GW.

A.4) The PDN GW responds to the Serving GW with the result of the deregistration with Proxy Binding Update Acknowledgement

5.4 Dedicated Bearer Procedures for E-UTRAN Access with PMIP-based S5/S8

5.4.1 General

The procedure given in Figure 5.4.1-1 applies to all dedicated resource allocation operations for E-UTRAN which are triggered by PCRF, with the only exception of MME-initiated Dedicated Resource Allocation Deactivation procedure which is covered in Section 5.4.5.3 The procedure initiated by the S-GW in the E-UTRAN differ for each case.

The procedure described in Figure 5.4.1-1 shows only the steps, due to PMIP based S5/S8, that are different from the GTP variant of the procedure given in TS 23.401 [4].

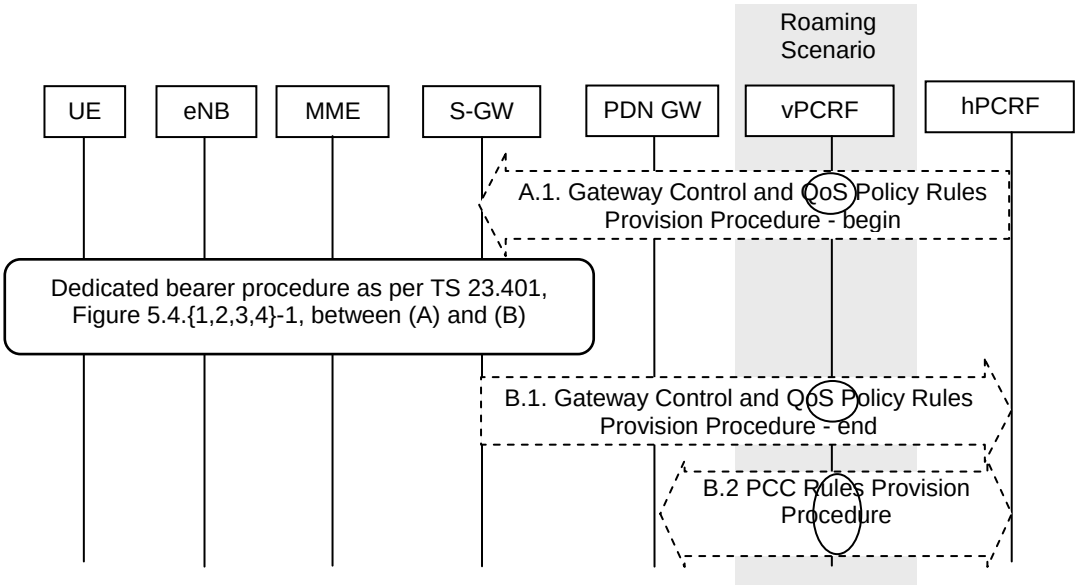


Figure 5.4.1-1: Dedicated Resource Allocation Procedure, UE in Active Mode

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

If dynamic policy provision is not deployed, the steps shown in the figure are not taken. Instead, a configured static policy may be applied.

A.1) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the QoS rules and Event Trigger information to the S-GW.

Steps between A.1 and B.1 are described in TS 23.401 [4], clause 5.4.1.

NOTE: For a PMIP-based S5/S8, after procedure steps (A.3 of TS 23.401 [4], clause 5.4.1), the PCRF sends a PCC decision provision (QoS policy) message to the S-GW and not to the P-GW as donefor GTP-based S5/S8. The S-GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active bearer. The S-GW generates the UL TFT and updates the Bearer QoS to match the aggregated set of service date flows. The S-GW then sends the Update Bearer Request (PTI, EPS Bearer Identity, Bearer QoS, UL TFT) message to the MME.

B.1) The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not nd thus completing the GW Control and QoS Rules Provision procedure started in step A.1.

B.2) The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [19]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of an PCC Rules Provision procedure specified in TS 23.203 [19].

NOTE: Step B.2 may occur before step A.1 or performed in parallel with steps A.1-B.1 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

5.4.2 Dedicated Bearer Activation

When the QoS Policy rules provided by the PCRF to the Serving Gateway in Step A.1 of figure 5.4.1-1 above results in the Serving Gateway to decide to activate a dedicated bearer, this procedure is applied.

The procedure depicted in Figure 5.4.1-1 apply for this case. On receiving message A.1, the Serving GW decides that a new bearer needs to be activated, the Serving GW uses this QoS policy to assign the bearer QoS, i.e., it assigns the values to the bearer level QoS parameters (excluding AMBR); see TS 23.401 [4] clause 4.6.2. The Serving GW follows the procedure shown in TS 23.401 [4], section 5.4.1 by sending a Create Dedicated Bearer Request message (Bearer QoS, UL and DL TFT, S1 TEID) to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this case as well. The steps between A.3 and B.1 are described in 3GPP TS 23.401, Section 5.4.1.

5.4.3 Bearer Modification with Bearer QoS Update

5.4.3.1 PCC Initiated Bearer Modification with Bearer QoS Update

When the QoS Policy rules provided by the PCRF to the Serving Gateway in step A.1 of Figure 5.4.1-1 above results in the Serving Gateway to decide to modify the QoS of an already existing bearer, this procedure is applied. QoS modification occurs this may result in a bearer modification in the E-UTRAN access.

The procedures depicted in Figures 5.4.1-1 apply to this case as well. On receiving message A.1, the Serving GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active bearer. The Serving GW generates the UL and DL TFT and updates the Bearer QoS to match the aggregated set of service date flows. The Serving GW then follows the procedure shown in TS 23.401 [4], section 5.4.2 by sending the Update Bearer Request (Bearer QoS, UL and DL TFT) message to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this procedure as well. The steps between A.3 and B.1 are described in 3GPP TS 23.401, clause 5.4.2.1.

5.4.3.2 HSS-Initiated Subscribed QoS Modification

The HSS Initiated Subscribed QoS Modification for a PMIP-based S5/S8 is depicted in Figure 5.4.3.2-1.

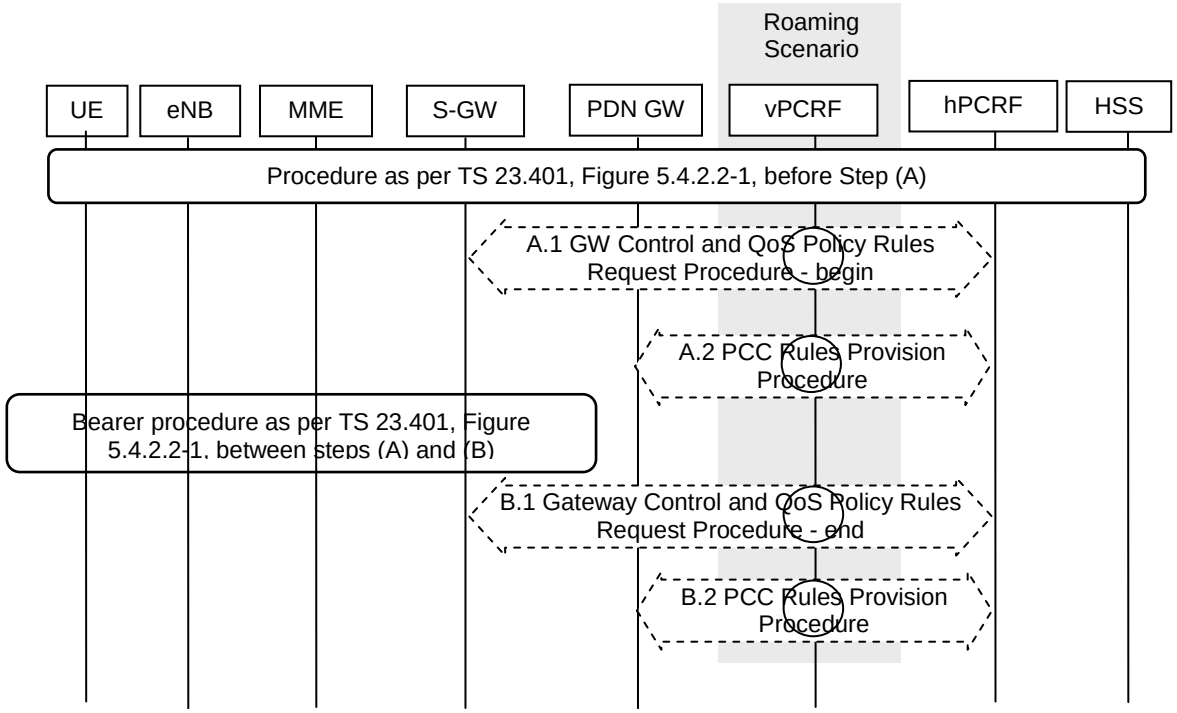


Figure 5.4.3.2-1: HSS-initiated Subscribed QoS Modification

A.1. The Serving GW initiates the Gateway Control and QoS Policy Rules Request Procedure with the PCRF as specified in TS 23.203 [19]. The S-GW provides the updated default bearer QoS for the default bearer to the PCRF and the PCRF responds with updated QoS rules. The PCRF makes a PCC decision as a result of the Gateway Control and QoS policy request and provides the updated QoS Rules to the Serving GW.

A.2. The PCRF initiates the PCC Rules Provision Procedure with the PDN GW as specified in TS 23.203 [19] to updates the rules in the PDN GW.

After Step A.1, the Serving GW follows the procedure shown in TS 23.401 [4], clause 5.4.2.1 by sending the Update Bearer Request message to the MME. The procedure is completed when the Serving GW receives a Update Bearer Response from the MME in Step 8 of TS 23.401 [4] clause 5.4.2.1.

B.1. The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not and thus completing the GW Control and QoS Rules Provision procedure started in step A.1.

B.2. The PCRF executes the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19] to update the PCC rules in the PDN GW.

NOTE: Step B.2 may be performed in parallel with steps A.1-B.1 if acknowledgement of resource allocation is not required at the PCRF to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

5.4.4 Dedicated Bearer Modification without Bearer QoS Update

When the QoS Policy rules provided by the PCRF to the Serving Gateway in step A.1 of figure 5.4.1-1 above results in the Serving Gateway to decide to only update the set of TFTs corresponding to an already existing dedicated bearer, this procedure is applied.

The procedures depicted in Figures 5.4.1-1 apply to this case as well. On receiving message A.1, the Serving GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active dedicated bearer. The Serving GW generates the UL TFT and determines that no update of the Bearer QoS is needed. The Serving GW then follows the procedure shown in TS 23.401 [4], section 5.4.3 by sending the Update Dedicated Bearer Request (UL and DL TFT) message to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this procedure as well. The steps between A.3 and B.1 are described in TS 23.401, Section 5.4.3.

5.4.5 Dedicated Bearer Deactivation

5.4.5.1 PCC-initiated Dedicated Bearer Deactivation

When the QoS Policy rules provided by the PCRF to the Serving Gateway in step A.1 of figure 5.4.1-1 above results in the Serving Gateway to decide to deactivate an existing dedicated bearer, this procedure is applied.

The procedures depicted in Figures 5.4.1-1 apply to this case as well. On receiving message A.1, the Serving GW uses this QoS policy to determine that a dedicated bearer needs to be deactivated, the Serving GW follows the procedure shown in TS 23.401 [4], section 5.4.3 by sending the Delete Dedicated Bearer Request message to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this procedure as well. The steps between A.3 and B.1 are described in TS 23.401, Section 5.4.4.1

5.4.5.2 PDN-GW-initiated PDN-disconnection Procedure

The default bearer and all the dedicated resource allocations associated with the PDN address are released in this procedure.

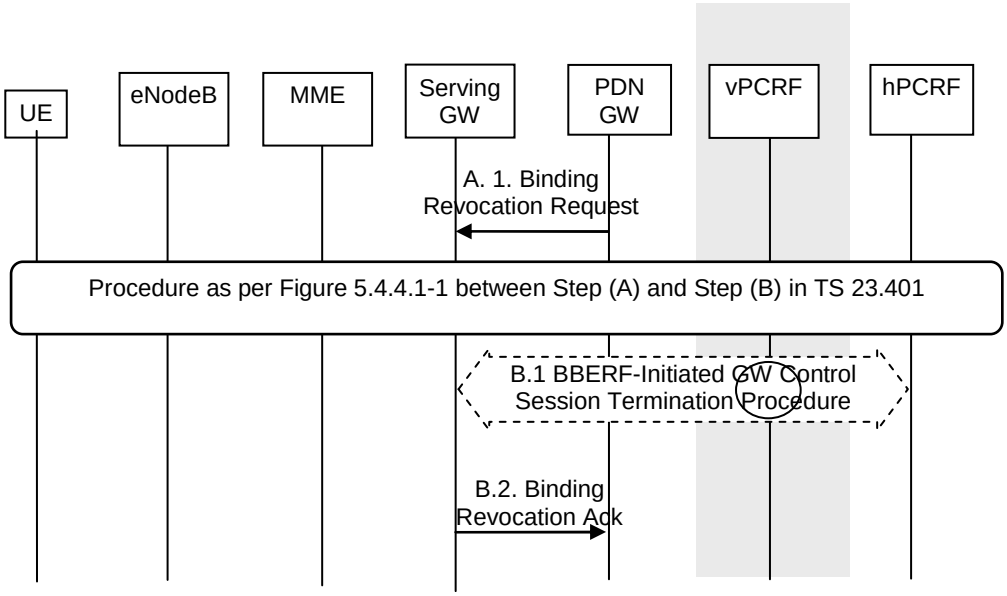


Figure 5.4.5.2-1: PDN-GW-initiated Bearer Deactivation

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the Gateway Control Session Termination message from the Serving GW in the VPLMN to the hPCRF in the HPLMN. The vPCRF receives the Acknowledgment from the hPCRF and forwards it to the Serving GW. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.4.5.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1. The PDN GW sends a Binding Revocation Indication (PDN address) message to the Serving GW as defined in draft-muhanna-mip6-binding-revocation [35].

Steps between A and B are described in Section 5.4.4.1 in TS 23.401 [4] using the indication that all bearers belonging to the given PDN address shall be released.

B.1. The Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The S-GW provides the information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of the Gateway Control session in S-GW.

B.2. The Serving GW returns a Binding Revocation Acknowledgement message to the PDN GW.

NOTE: Step B.2 may occur before steps B.1 since the Serving GW need not wait for terminating the GW Control Session with the PCRF before acknowledging the Binding Revocation.

5.4.5.3 MME-initiated Dedicated Resource Allocation Deactivation

This section contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the procedure defined in 23.401 Section 5.4.4.2 for -MME initiated dedicated bearer deactivation.

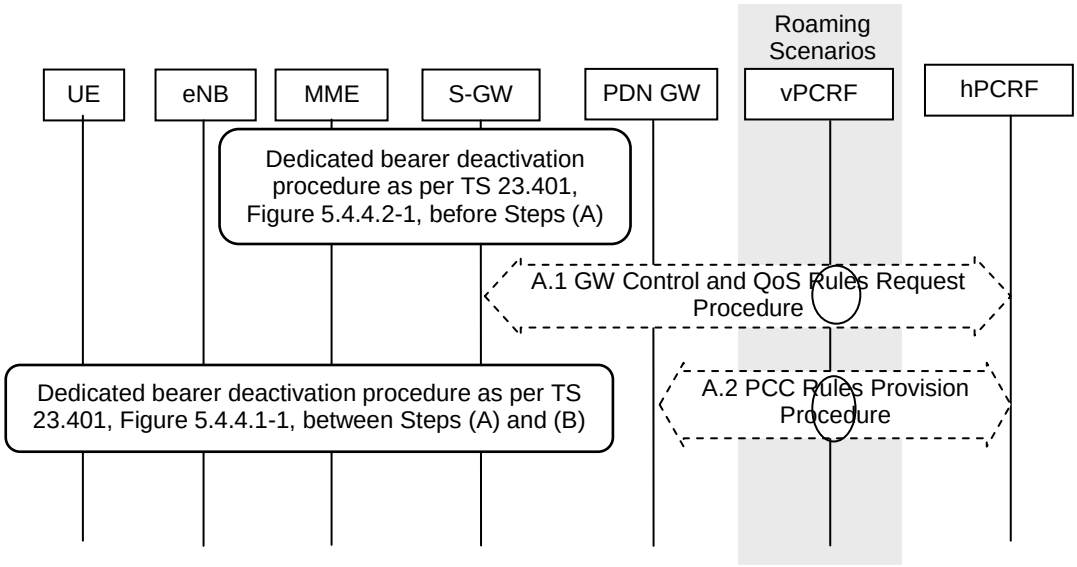


Figure 5.4.5.3-1: MME-initiated Dedicated Resource Allocation Deactivation

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout as in Figure 4.2.3-5, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.4.5.3-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Before Step A.1. the procedure shown in TS 23.401 [4] is followed and the Serving GW receives a Request Bearer Resource Release message from the MME.

A.1) The Serving GW decides to deactivate the bearers and initiates the Gateway Control and QoS Policy Rules Request Procedure with the PCRF as specified in TS 23.203 [19]. The Serving GW informs the PCRF about the deleted QoS Rules.

A.2) The PCRF initiates the PCC Rules Provision Procedure with the PDN GW as specified in TS 23.203 [19] to updates the rules in the PDN GW. The PCC rules provide the PDN GW with information required to enforce the remaining dedicated resource allocation policy, after removing PCC rules corresponding to the QoS rules deactivated by step A.1.

After step A.1, the Serving GW follows the procedure shown in TS 23.401 [4], clause 5.4.4.2 by sending the Delete Dedicated Bearer Request message to the MME. The Serving GW does not need to wait for step A.1 to complete to proceed with the deactivation of bearers with the MME. The procedure is completed when the Serving GW receives a Delete Dedicated Bearer Response from the MME in Step 8 of TS 23.401 [4], clause 5.4.4.2.

5.5 UE-initiated Resource Request and Release

This section is related to the case when UE-initiated resource request and release is supported, and it is utilized for the PMIP-based S5/S8 SDFs.

In the non-roaming case, vPCRF will not be involved.

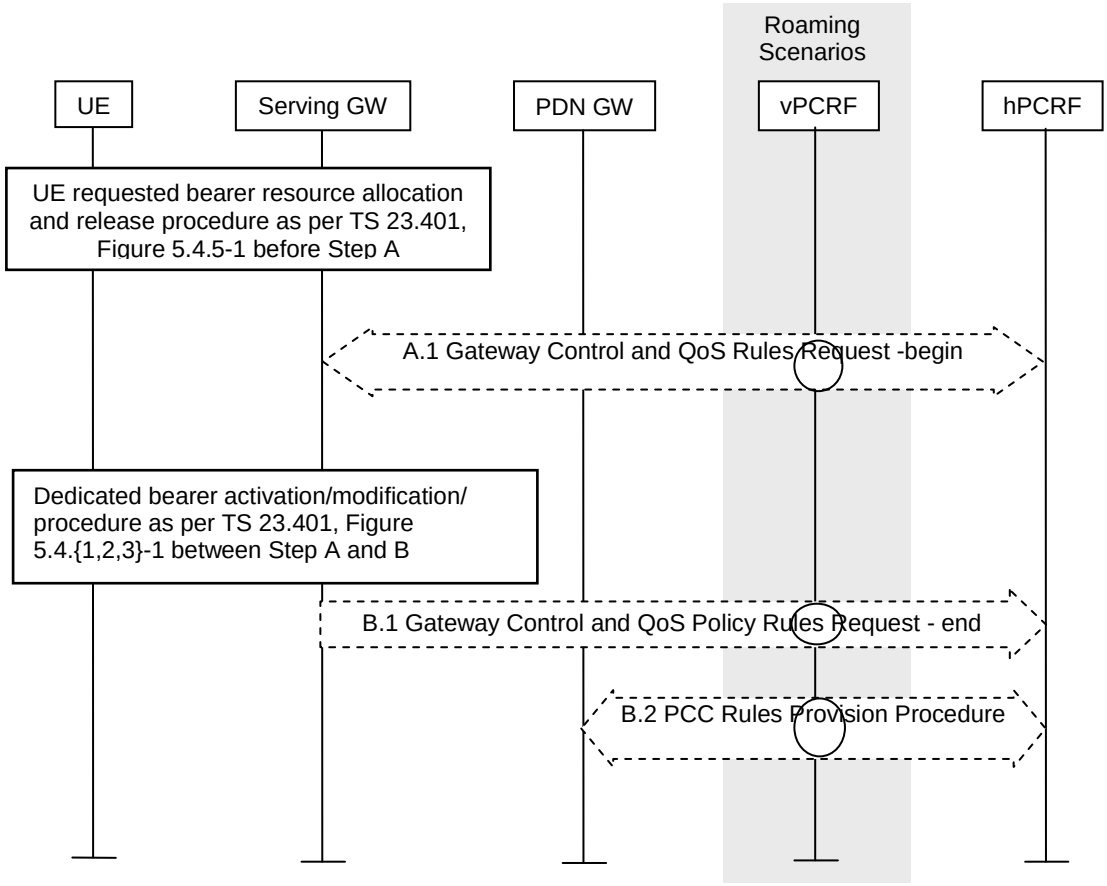


Figure 5.5-1: UE-initiated resource request/release with PMIP-based S5/S8

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout as in Figure 4.2.3-5, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.5-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1. The Serving GW initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19]. The Serving GW provides the UE request or release of resources as an Event Report. The PCRF makes a PCC decision as a result of the Gateway Control and QoS policy request and provides the updated QoS Rules to the Serving GW.

Steps between A.1 and B.1 are described in TS 23.401 [4], clauses 5.4.1, 5.4.2 and 5.4.3. Based on the QoS policy rules, the Serving GW decides whether to initiate a dedicated resource allocation activation or dedicated resource allocation modification (with or without QoS update).The Serving GW uses this QoS policy to assign the bearer QoS, i.e. it assigns the values to the bearer level QoS parameters (excluding AMBR); see clause 4.6.2 of TS 23.401 [4] and sends the appropriate message to the MME.

B.1. The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not and thus completing the GW Control and QoS Rules Provision procedure started in step A.1.

B.2. The PCRF initiates the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19] to update the PCC rules in the PDN GW.

NOTE: Step B.2 may be performed in parallel with Steps A.1-B1 if acknowledgement of resource allocation is not required at the PCRF to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

5.6 UE Initiated Connection to Additional PDN with PMIP-based S5/S8

5.6.1 UE requested PDN connectivity

The UE requested PDN connectivity procedure for an E-UTRAN is depicted in figure 5.6.1-1. The procedure allows the UE to request for connectivity to a PDN including allocation of a default bearer. In this procedure, the UE is assumed to be in active mode. Proxy Mobile IP is used on PMIP-based S5 or S8 interface. It is assumed that the MAG is collocated with the Serving GW for the PMIPv6 procedure between the Serving GW and the PDN GW.

When only GTP-based S5 or S8 connections are established for roamers from a GTP network into a PMIP network the procedure as described in clause 5.10.2 of TS 23.401 [4] applies.

The procedure is also used for the re-establishment of existing PDN connectivity after the UE performed the handover from non-3GPP accesses for the first PDN connection by the Attach procedure. The UE triggers the re-establishment of existing PDN connectivity after the handover by providing a Request Type indicating "Handover" as specified in TS 23.401 [4].

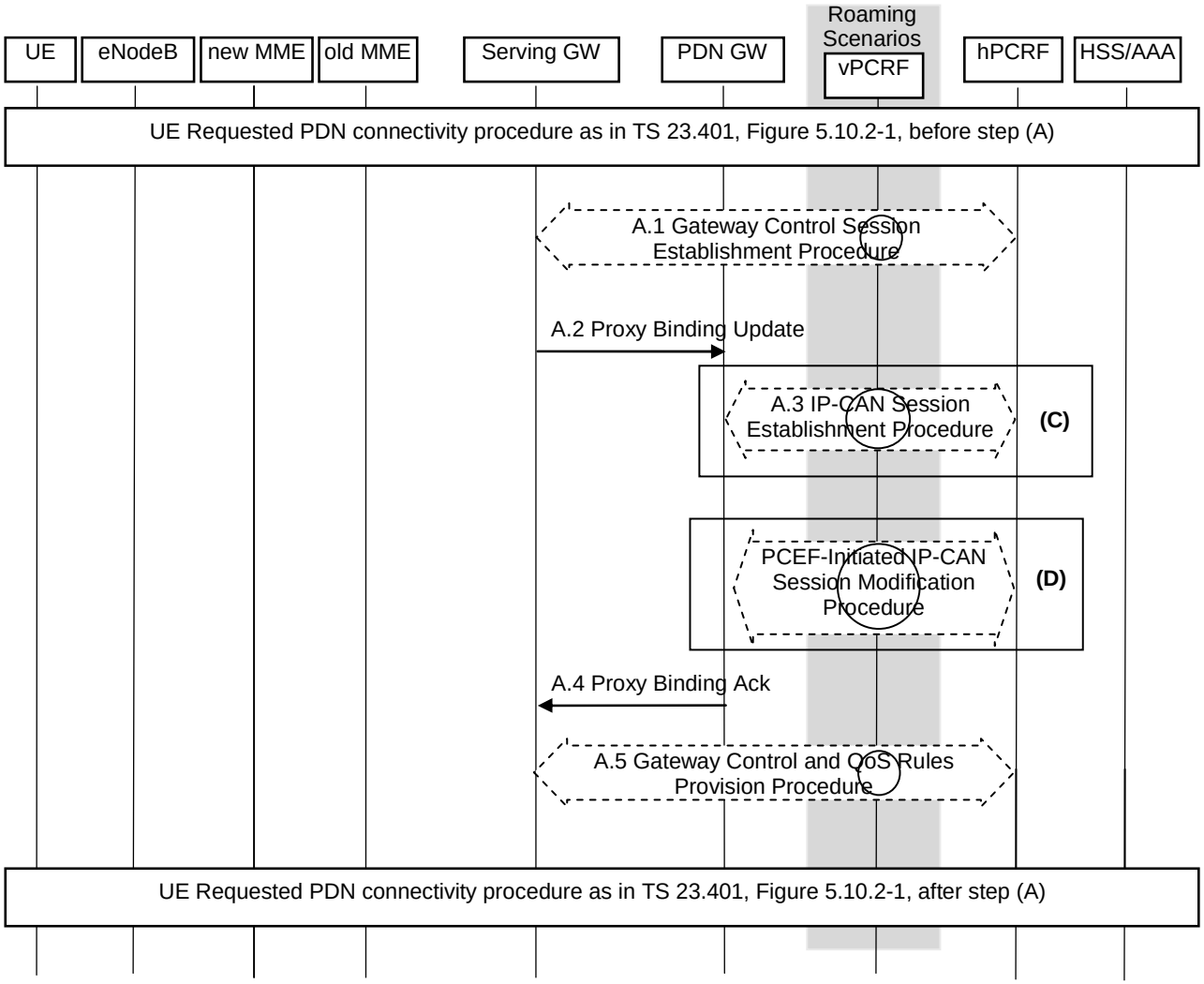


Figure 5.6.1-1: UE requested PDN connectivity with PMIP-based S5 or S8

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.6.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

For re-establishment of existing PDN connectivity after the UE performed the handover from non-3GPP accesses, the following applies:

- In step A.2 the Serving GW sets the Handover Indicator to "handover".
- The steps in (C) are performed only when the UE establishes additional PDN connectivity with a PDN it is not connected to.
- The steps in (D) are performed only when the UE re-establishes PDN connectivity after a handover. The steps in (D) correspond to the PCEF-Initiated IP-CAN Session Modification procedure specified in TS 23.203 [19].
- In step A.4, the UE Address Info shall contain the IP address the UE obtained during PDN connectivity establishment for this PDN over the non-3GPP access.

The steps A.1-A.5 correspond to steps C.1-C.5 in clause 5.2-1.

5.7 Handover and Tracking area Update Procedures for PMIP-based S5/S8 Interface

5.7.1 Intra-LTE TAU and Inter-eNodeB Handover with Serving GW Relocation

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the TAU with MME and Serving GW change procedure defined in 23.401 section 5.3.3.1 as well as Inter-eNodeB Handover with CN Node Relocation described in 23.401 section 5.5.1.2.

In case of a Serving GW relocation, the target Serving GW must establish a Gateway Control Session with the PCRF to perform policy controlled functions such as Bearer-Binding. The source Serving GW relinquishes its Gateway Control Session with the PCRF in step B.

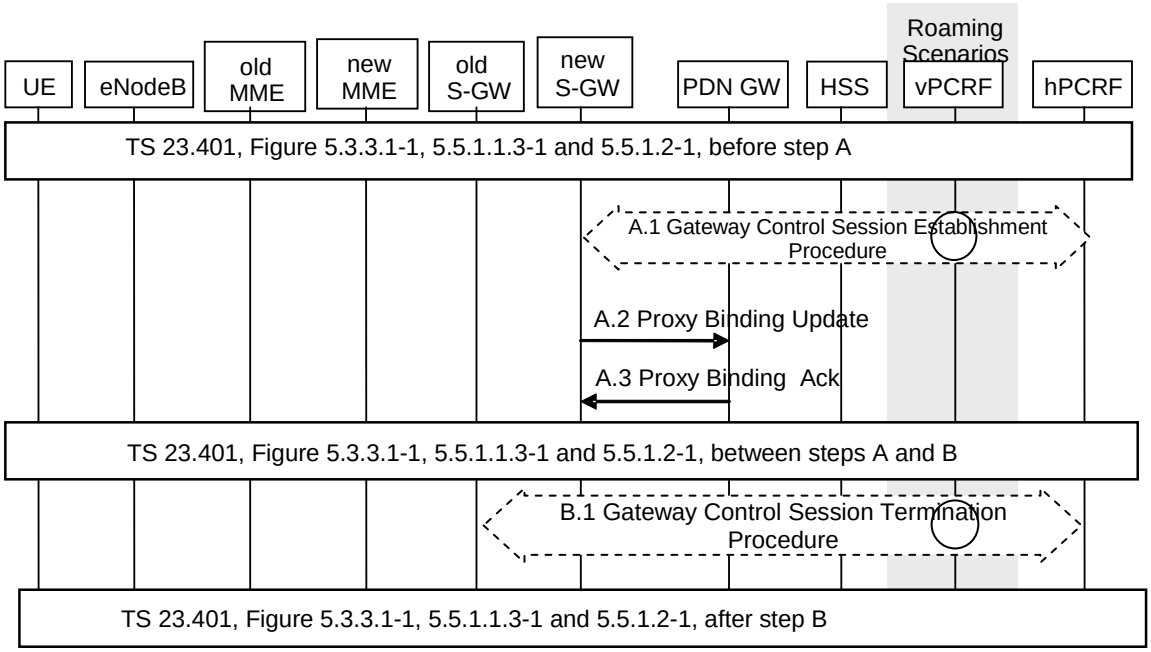


Figure 5.7.1-1: Intra-LTE and Inter-eNodeB Handover with Serving GW Relocation

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the

HPLMN. In the case of Local Breakout as in Figure 4.2.3-5, the vPCRF also forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.7.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Target Serving GW initiates the Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. As part of the procedure the Serving GW informs the PCRF of the new RAT type. The PCRF sends information to the Serving GW enabling bearer binding and other behavior.

NOTE: The Target Serving GW preserves the Bearer Binding that has already been established by the Source Serving GW to employ in order to support the existing bearer bindings. To enable this the EPS Bearer ID, UL TFT and DL TFT is transferred before Step A as follows: across S10 in Forward Relocation Request and across S11 in Create Bearer Request. The Event Triggers indicate to the Serving GW under what conditions to report events to the PCRF.

A.2) The new Serving GW performs a PMIPv6 Proxy Binding Update (MN NAI, Lifetime, Access Technology Type option, APN, GRE key for downlink traffic, *Additional Parameters*) message in order to re-establish the user plane as a result of the Serving GW relocation. The MN NAI identifies the UE for whom the message is being sent. Within Access Technology Type option an indication for RAT (E-UTRAN) type is set; an indication for handover between MAGs for the same interface is also set. The APN disambiguates which PDN this message refers to. The additional parameters may include protocol configuration options and other information.

A.3) The PDN GW acknowledges the Binding Update by sending a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, *Additional Parameters*) message to the Serving GW. A PMIP tunnel is established at this point between the PDN GW and the Serving GW. The UE Address Info includes one or more IP addresses. The Additional Parameters may contain protocol configuration options and other information.

Steps between A.3 and B.1 are described in TS 23.401, Section 5.3.3.1 and Section 5.5.1.

B.1) The old Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Serving GW ceases to perform Bearer Binding and associated policy controlled functions.

5.7.2 TAU/RAU or Handover between GERAN A/Gb Mode or UTRAN Iu Mode and E-UTRAN

In case of inter-RAT TAU/RAU or handovers, the Serving GW may or may not be relocated. The PMIP based S5/S8 variants procedure steps for inter-RAT TAU/RAU or handover without Serving GW relocation is shown in Figure 5.7.2-1 and those corresponding to a change of Serving GW is shown in Figure 5.7.2-2.

The procedures in this section correspond to the following Figures in TS 23.401 [4]:

- Figure 5.3.3.2-1 [UTRAN Iu mode to E-UTRAN] Tracking Area Update
- Figure 5.3.3.3-1E-UTRAN to UMTS RA Update,
- Figure 5.3.3.5-1 GERAN A/Gb mode to E-UTRAN Tracking Area Update
- Figure 5.3.3.6-1 E-UTRAN to GERAN A/Gb mode Routeing Area Update
- Figure 5.5.2.1.3-1: E-UTRAN to UTRAN Iu mode Inter RAT HO, execution phase
- Figure 5.5.2.2.3-1: UTRAN Iu mode to E-UTRAN Inter RAT HO, execution phase
- Figure 5.5.2.3.3-1: E-UTRAN to GERAN A/Gb mode Inter RAT HO, execution phase
- Figure 5.5.2.4.3-1: GERAN A/Gb mode to E-UTRAN Inter RAT HO, execution phase

In TS 23.401 [4], the clauses corresponding to the above figures cover both the case of Serving GW relocation and no Serving GW relocation. In case of no Serving GW relocation, Steps (A) in the above figures are between the un-changed Serving GW and the PCRF and the Steps (B) in those figures do not apply, as shown in Figure 5.7.2-1. In case of Serving GW relocation, Steps (A) in the above figure are between the target Serving GW and the PCRF and the Steps (B) is between the source Serving GW and the PCRF, as shown in Figure 5.7.2-2.

In case of no Serving GW relocation, the S-GW signals the change of RAT to the PCRF. If PCC rules provided to the PDN-GW have changed, the PCRF updates these rules at the PDN-GW.

The user plane already exists between the Serving GW and the PDN GW and remains unchanged. In case of RAU or handover to 2G/3G, user plane routing is assumed to proceed over the S4 interface towards the S2/S3 SGSN. When an inter-RAT TAU occurs, the enhanced packet core may signal this event to the PDN GW, for example to inform the PDN GW of a RAT type change. In the case of a PMIP-based S5 and S8, an Update Bearer Request is not sent from the Serving GW to the PDN GW. Instead, the PCRF in the HPLMN reports the change of event. The PCRF signals any change in the policy resulting from the event to the PDN GW, provisioning updated policy and charging rules.

In case dynamic PCC is not deployed, a change of RAT type will not be signalled to the PDN GW using PMIP based S5/S8 interfaces, if no change of Serving GW has occurred.

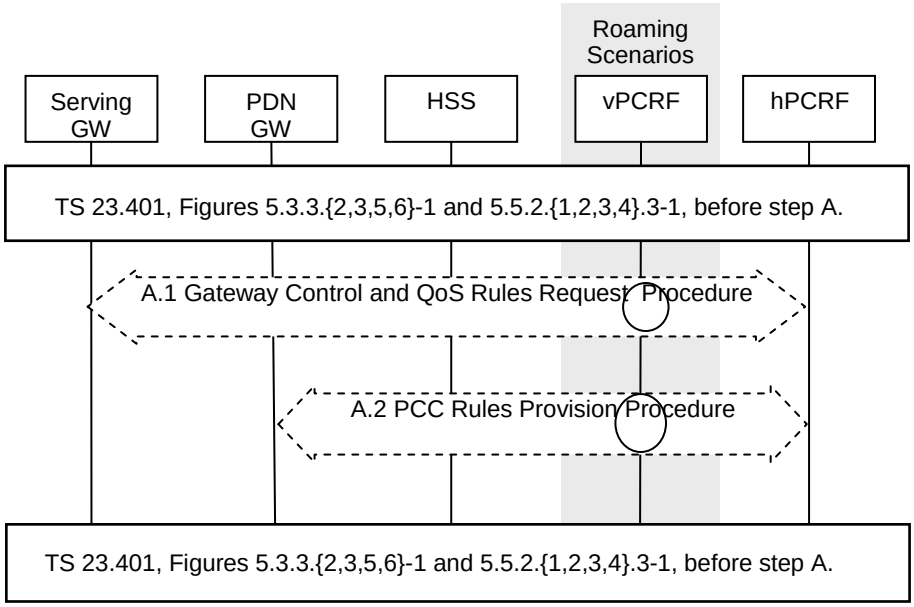


Figure 5.7.2-1: Inter-RAT TAU/RAU or Handover without Serving GW relocation

This procedure concerns both the non-roaming (S5) and roaming case (S8). In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.7.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Serving GW informs the PCRF about the change of RAT type by initiating the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19].

A.2) The PCRF updates the PCC rules at the PDN GW by initiating the PCC Rules Provision Procedure as specified in TS 23.203 [19] if the PCC rules have changed based on the RAT type reported by the Serving GW in step A.1. Further, the hPCRF notifies the PDN GW of the change in RAT.

Step A.2 may be initiated before A.1 completes.

The following procedure describes inter-RAT TAU/RAU or Handover in the case of Serving Gateway relocation for PMIP-based S5/S8.

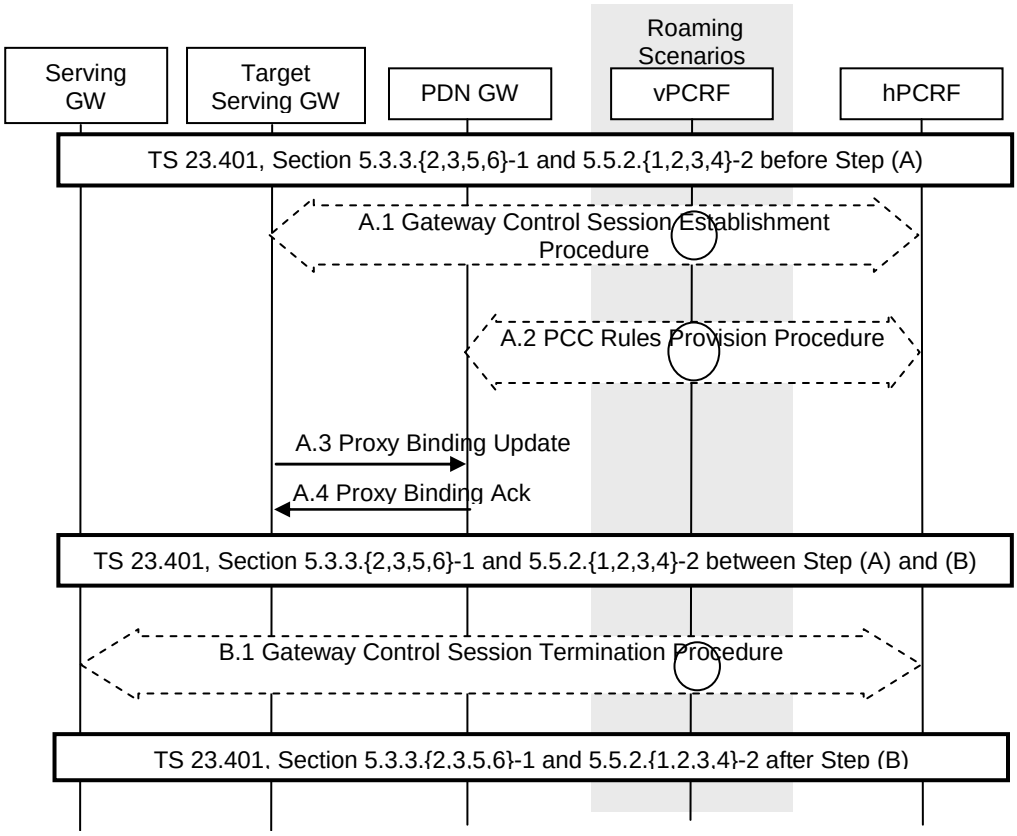


Figure 5.7.2-2: Inter-RAT TAU/RAU or Handover with Serving GW Relocation

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout as in Figure 4.2.3-5, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps in the procedure are not applied.

A.1) The Target Serving Gateway initiates a Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19] and informs the PCRF of the new RAT type.

A.2) The PCRF sends an updated policy to the PDN GW by initiating the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19]. This contains any effected PCC rules and Event Triggers resulting from the preceding step that may require enforcement or event reporting to be performed by the PDN GW.

A.3) The Target Serving GW sends a Proxy Binding Update (MN NAI, Lifetime, Access Technology Type option, APN, GRE key for downlink traffic, *Additional Parameters*) message in order to re-establish the user plane as a result of the Serving GW relocation. The MN NAI identifies the UE for whom the message is being sent. Within Access Technology Type option an indication for RAT type is set; an indication for handover between MAGs for the same interface is also set. The APN disambiguates which PDN this message refers to. The additional parameters may include protocol configuration options and other information.

A.4) The PDN GW acknowledges the Binding Update by sending a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, *Additional Parameters*) message to the Target Serving GW. A PMIP tunnel is established at this point between the PDN GW and the Target Serving GW. The UE Address Info includes one or more IP addresses. The Additional Parameters may contain protocol configuration options and other information.

Steps between A.4 and B.1 are described in the clauses of TS 23.401 [4], containing the figures referenced in Figure 5.7.2-1 above.

B.1) The old Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF, as specified in TS 23.203 [19]. The S-GW provides information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of the Gateway Control session in S-GW.

5.8 ME Identity Check Procedures for PMIP-based S5/S8

< This subclause will contain details on ME identity checking (e.g. IMEI checking)>

5.9 UE-triggered Service Request for PMIP-based S5/S8

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the UE-triggered Service Request procedure defined in TS 23.401 [4], clause 5.3.4.1, for the case where the RAT Type reported in the Service Request has changed compared to the last reported RAT Type.

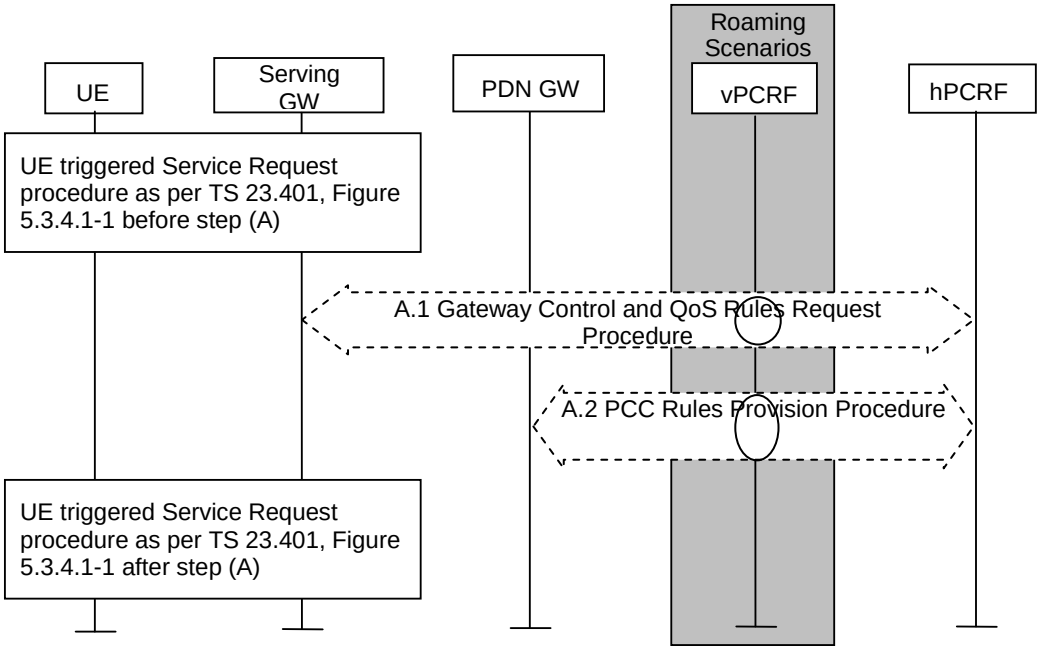


Figure 5.9-1: UE-triggered Service Request for PMIP-based S5/S8

This procedure concerns both the non-roaming (S5) and roaming case (S8). In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.9-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Serving GW informs the PCRF about the change of RAT type by initiating the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19].

A.2) The PCRF updates the PCC rules at the PDN GW by initiating the PCC Rules Provision Procedure as specified in TS 23.203 [19] if the PCC rules have changed based on the RAT type reported by the Serving GW in step A.1. Further, the hPCRF notifies the PDN GW of the change in RAT.

Step A.2 may be initiated before step A.1 completes: Once the hPCRF receives the event report from the Serving GW as part of step A.1, the hPCRF may complete step A.1 and initiate step A.2 in any order..

5.10 PMIP-based S5/S8 procedures for GERAN/UTRAN over S4

5.10.1 General

This section presents the PMIP-based S5/S8 procedures equivalent to the GTP-based procedures presented in TS 23.060 [21] for interworking. The differences required for interpretation of the PMIP-based S5/S8 procedures in other clauses of this specification are clarified below.

If PCC is not deployed, only default bearers may be provided for UE connection to a PDN. This is described fully in the PMIP-based S5/S8 procedures refered to in clause 5.10. Secondary PDP context requests are not supported in this case.

5.10.2 GPRS procedures that update the PDN GW

Several procedures employing GTP-based S5/S8 includes an "Update Bearer" exchange, initiated by the Serving GW, responded to by the PDN GW. The equivalent interaction for a PMIP-based S5/S8 is shown in figure 5.7.2-1.

The following procedures in TS 23.060 [21] will make use of the procedure shown in this specification, clause 5.7.2 to signal RAT change as determined by the SGSN. Aside from the new RAT type, no additional parameter must be sent as an event report by the Serving GW to the PDN GW by means of the PCRF (as described in TS 23.203 [19]).

The procedure in clause 5.7.2 refers directly to procedures in TS 23.401 [4], while the procedures described here in support of S4 refer to clauses in TS 23.060 [21]. The following clarifications to the procedure in clause 5.7.2 must be considered to interpret clause 5.7.2:

- **6.13.1.1.2: Iu mode to A/Gb mode Intra-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 6.13.1.1.2, figure 52-2.

- **6.13.1.2.2: A/Gb mode to Iu mode Intra-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 6.13.1.2.2, figure 53-2.

- **6.13.2.1.2: Iu mode to A/Gb mode Inter-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.13.2.1.2, figure 54-3.

- **6.13.2.2.2: A/Gb mode to Iu mode Inter-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.13.2.2.2, figure 55-3.

5.10.3 UE allocated resources

The UE (or the SGSN on behalf of the UE) requests resources in several procedures in TS 23.060 [21]. The procedure described in clause 5.5 of this specification provides the PMIP-based S5/S8 describes UE-initiated resource request and release. This procedure, with the additional clarification given below, will support the following procedures shown in TS 23.060 [21].

In each case, the SGSN provides a Bearer identifier (the LBI) over S4. The bearer binding performed by the Serving GW is in this case constrained to either reject or modify (increase or decrease the resource assigned to) the indicated bearer. The Serving GW shall not provide a different bearer as a result of the PDP Context Activation or Modification procedures.

There are two modes of operation, indicated to the Serving GW by the SGSN in the BCM parameter.

- For "mixed-mode", the procedures in GERAN/UTRAN are very similar to those in E-UTRAN. The only difference is constrained bearer binding behaviour as described in the previous paragraph.

- For "UE-only mode", additional support is required in the PCRF to calculate the effective total QoS allocation that applies to each bearer.

- **9.2.2.1: A PDP Context Activation using S4**

  Steps A.1, B.1 and B.2 of the procedure in clause 6.2.1 (from steps 4-10) occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.2.1A, figure 64a.

  The BCM parameter, received by the Serving GW from the SGSN, is sent to the PCRF and a BCM parameter is returned from the PCRF as an additional IE in step A.1.

- **9.2.2.1.1A, Figure 66a: Secondary PDP Context Activation Procedure, PDP Creation Part using S4**

  Step A.1 of the procedure in clause 5.5 corresponds to the steps described in the box (A1) in TS 23.060 [21], clause 9.2.2.1.1A, figure 66a.

  In step A.1, additional IEs are required by the PCRF and PDN GW in order properly assign QoS rules and prepare the dedicated bearer. The TFT and SDF QoS IEs received from the SGSN by the S-GW over S4. These parameters are then forward to the PCRF as described in clause 5.5.

- **9.2.2.1.1A, Figure 66b: Secondary PDP Context Activation Procedure, PDP Update Part, using S4**

  Steps B.1 and B.2 of the procedure in clause 5.5 corresponds to the steps described in the box (B1) in TS 23.060 [21], clause 9.2.2.1.1A, figure 66b.

  In step A.1, additional IEs are required by the PCRF and PDN GW in order properly assign QoS rules and prepare the dedicated bearer. These include the TFT and SDF QoS IEs received from the SGSN by the S-GW over S4.

- **9.2.3.1A: MS- and SGSN-Initiated EPS Bearer Modification Procedure**

Editor's Note: This clause remains incomplete in TS 23.060 [21], so the PMIP-based S5/S8 equivalent cannot be described.

The UE adds, modifies or removes an SDF from abearer. The SGSN sends a request, as is shown in TS 23.060 [21], clause 9.2.3.1A including information elements used for issuing a QoS Rules Request to the PCRF.

- In the case of "mixed-mode" the TFT is always present. The TFT and the requested SDF QoS are forwarded to the PCRF in step A.1.

- In the case of "UE-only" operation, the Serving GW fowards the requested QoS and TFT to the PCRF. The TFT may not be present. In this case, the Serving GW shall send the QoS rules currently associated with the bearer that is to be modified.

5.10.4 Network allocated resources

Network entities may request resources by means of off-path signalling to support PMIP-based S5/S8. This is defined in clause 5.4.1. The following procedures in TS 23.060 [21] employ this procedure:

- **9.2.2.3A: Network Requested PDP Context Activation Procedure using S4**

  Step A.1 of the procedure in clause 5.4.1 occurs instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.2.3A, Figure 69c. Steps B.1 and B.2 of the procedure in clause 5.4.1 correspond to the box (B1).

- **9.2.3.2A: PDN GW-Initiated EPS Bearer Modification Procedure**

Step A.1 of the procedure in clause 5.4.1 occurs instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.3.2A, Figure 71c. Steps B.1 and B.2 of the procedure in clause 5.4.1 correspond to the box (A2).

5.10.5 UE released resources

The UE may release dedicated resources by means of off-path signalling to support PMIP-based S5/S8 deployments, as shown in clause 5.5.

- **9.2.4.1A: MS- and SGSN Initiated Bearer Deactivation using S4**

  Steps A.1, B.1 and B.2 of the procedure in clause 5.5 occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.4.1A, figure 74a.

5.10.6 PDN GW released resources

The PDN GW may release resources by means of off-path signalling to support PMIP-based S5/S8 deployments as shown in clause 5.4.1. The following procedures in TS 23.060 [21] employ this procedure:

- **9.2.4.3A: PDN GW-Initiated PDP Context Deactivation Procedure using S4**

  Step A.1 in clause 5.4.1 corresponds to the steps shown in box (A1) of TS 23.060 [21], clause 9.2.4.3A, figure 77a.

- **9.2.4.3B: PDN GW-Initiated PDP Context Deactivation Procedure using S4**

  Steps B.1 and B.2 in clause 5.4.1 correspond to the steps in the box (B1) in TS 23.060 [21], clause 9.2.4.3B, figure 77b.

5.10.7 Attach

The GPRS Attach Procedure is supported by the following PMIP-based S5/S8 procedures:

Clause 5.3 is employed instead of box (A) in TS 23.060 [21], clause 6.5.3A, figure 22A. clause 5.3 is also used instead of box (B) in TS 23.060 [21], clause 6.5.3B, figure 22Bs.

5.10.8 Detach interaction using S4

The MS-, SGSN- and HLR-initiated GPRS detach procedures are supported by the following equivalent PMIP-based S5/S8 procedure:

Clause 5.3 is employed instead of the gray box (A1) in TS 23.060 [21], clause 6.6.3, Figure 25A.

6 Functional Description and Procedures for Trusted Non-3GPP IP Accesses

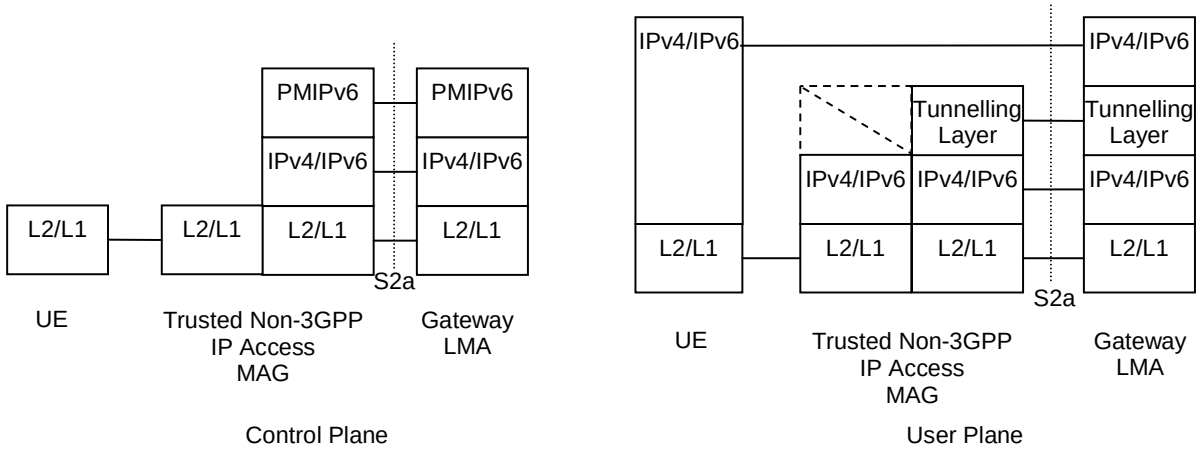
6.1 Control and User Plane Protocol Stacks

6.1.1 Protocol Stacks for S2a

The following protocols shall be supported on S2a:

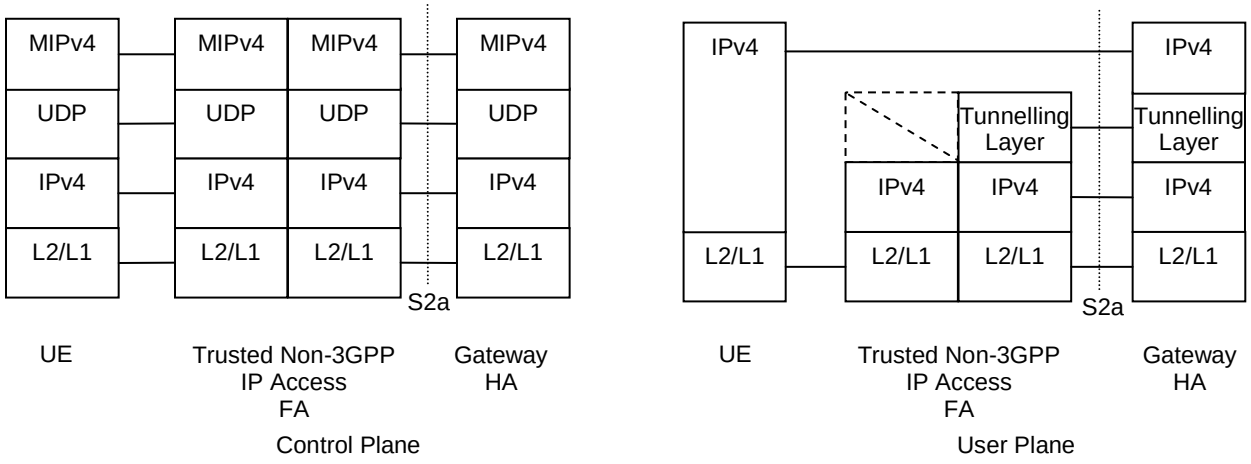
- PMIPv6
- MIPv4 FA mode

The figures below illustrate the control planes for Mobility Management (MM) and the user planes for each protocol option.



Legend:
- According to terms defined in PMIPv6 (draft-ietf-netlmm-proxymip6 [8]), the functional entities terminating both the control and user planes are denoted MAG in the non-3GPP IP access and LMA in the Gateway. LMA includes also the function of a Home Agent.
- The MM control plane stack is PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network.
- The tunnelling layer implements GRE encapsulation applicable for PMIPv6 [36].

Figure 6.1.1-1: Protocols for MM control and user planes of S2a for the PMIPv6 option



Legend:
- According to terms defined in MIPv4 RFC 3344 [12], the functional entities terminating both the control and user planes are denoted MN (Mobile Node) in the UE, FA (Foreign Agent) in the non-3GPP IP access, and HA (Home Agent) in the Gateway.
- The MM control plane stack is MIPv4 RFC 3344 [12] over UDP over IPv4.
- The user plane carries remote IPv4 packets over an IPv4 transport network.
- The tunnelling layer implements IP encapsulation applicable for MIPv4 as defined in RFC 3344 [12]. In some cases the tunnelling layer may be transparent.

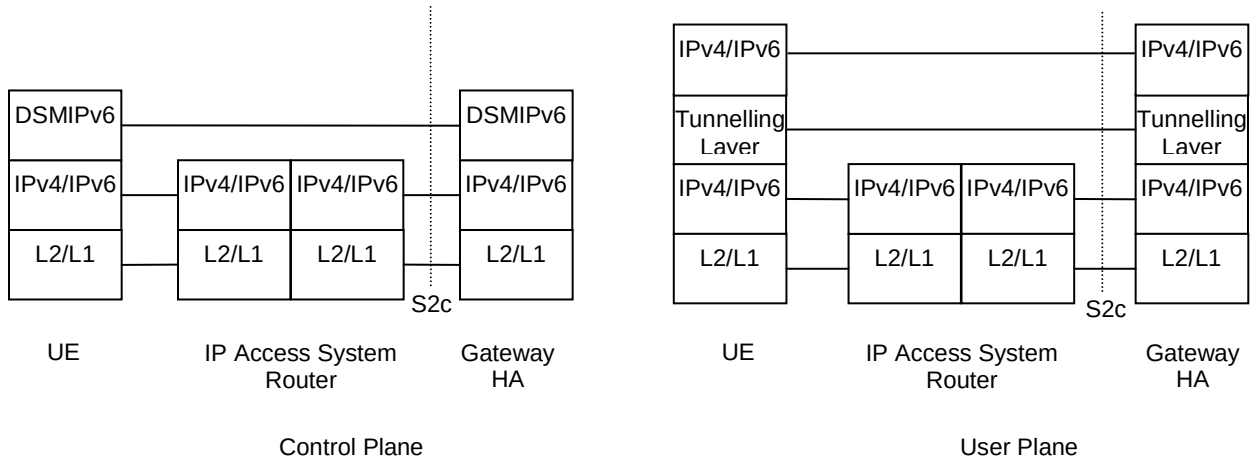
Figure 6.1.1-2: Protocols for MM control and user planes of S2a for the MIPv4 FA mode option

6.1.2 Protocol Stacks for S2c over Trusted Non-3GPP IP Accesses

The following protocol shall be supported on S2c over Trusted Non-3GPP IP Accesses:

- DSMIPv6, with IPsec and IKEv2 used to secure mobility signaling, as specified in RFC 4877 [22]

The figure below illustrates the control plane for Mobility Management (MM) and the user plane.



Legend:

- According to terms defined in DSMIPv6 [10], the functional entities terminating both the control and user planes are denoted MN (Mobile Node) in the UE, and HA (Home Agent) in the Gateway.
- The MM control plane stack is DSMIPv6 [10] over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network.
- The tunnelling layer implements IP encapsulation applicable for MIPv6 as defined in DSMIPv6 [10]. In some cases the tunnelling layer may be transparent.

Figure 6.1.2-1: Protocols for MM control and user planes of S2c for the DSMIPv6 option

6.2 Initial Attach on S2a

6.2.1 Initial Attach Procedure with PMIPv6 on S2a and Anchoring in PDN GW

PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) is used to setup a PMIPv6 tunnel between the trusted non-3GPP IP access and the PDN GW. In both roaming and non-roaming cases, S2a is present. It is assumed that MAG exists in the trusted non-3GPP IP access.

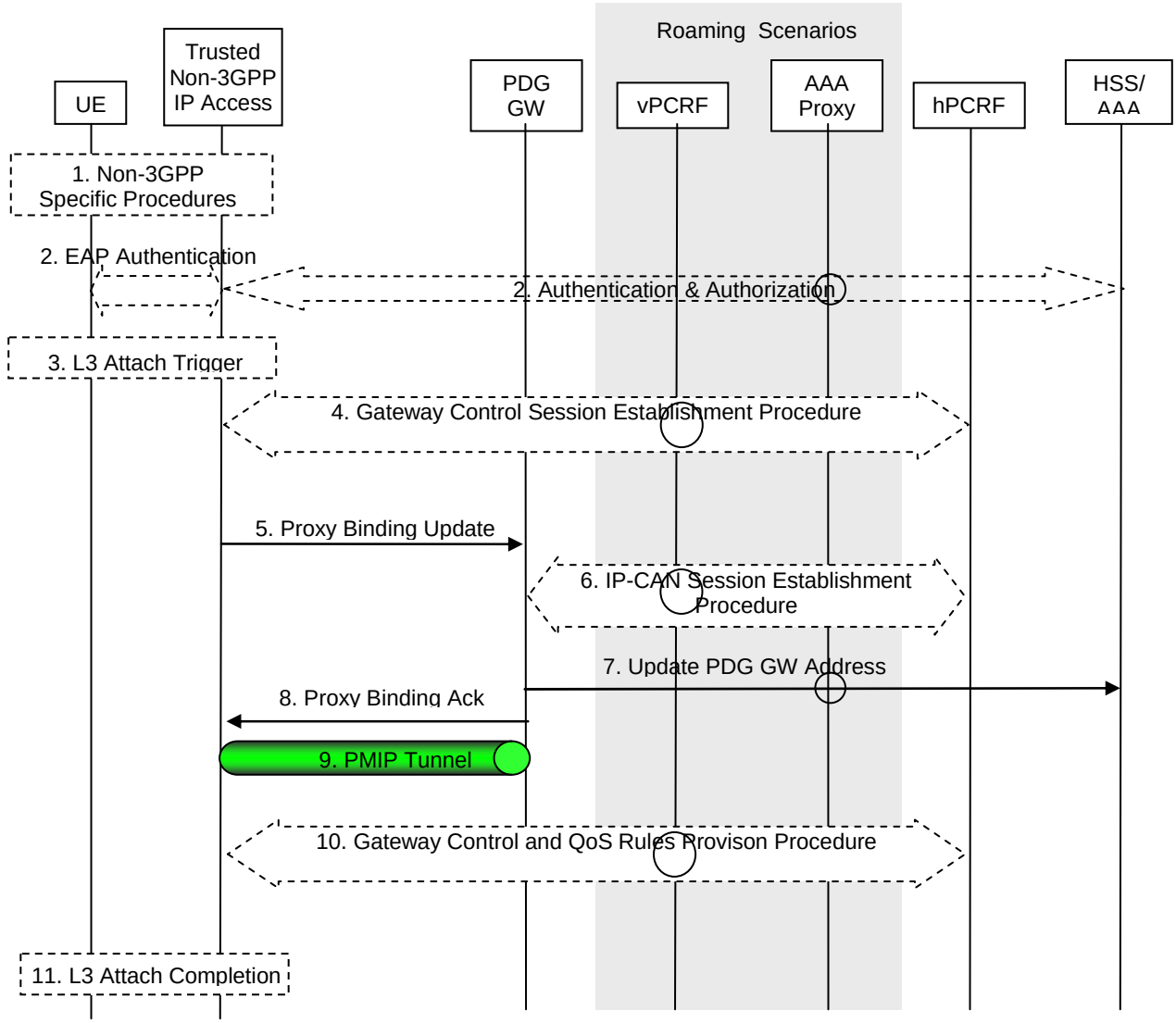


Figure 6.2.1-1: Initial attachment with Network-based MM mechanism over S2a for roaming, LBO and non-roaming scenarios.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved.

1) The initial Non-3GPP access specific L2 procedures are performed. These procedures are Non-3GPP access specific and are outside the scope of 3GPP;

2) The EAP authentication procedure is initiated and performed involving the UE, Trusted Non-3GPP IP Access and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. The PDN Gateway address is determined at this point as described in section 4.5.1. The PDN GW information is returned as part of the reply from the 3GPP AAA Server to the MAG in the trusted non-3GPP access. This may entail an additional interaction with the Domain Name Server function in order to obtain the PDN GW address. The list of all the APNs along with additional PDN GW selection information and part of the subscriber profile needed for authorization for each of the authorized PDNs is returned to the access gateway in order to provide authorization information for UE-initiated connectivity to additional PDNs as defined in clause 6.8.1. The 3GPP AAA Server also returns to the MAG the MN NAI to be used to identify the UE in Proxy Binding Update and Gateway Control Session Establishment messages (steps 5 and 10). If supported by Non-3GPP access network, the Attach Type is indicated to the Non-3GPP access network by the UE. The mechanism for supporting attach type is access technology specific and out of scope for 3GPP standardization. Attach Type indicates "Handover" when

the UE has already an activated PDN GW/HA due to mobility from 3GPP access to non-3GPP accesses. If the PDN subscription profile contains a PDN GW identity and the Attach Type does not indicate "Handover", the Non-3GPP access GW may request a new PDN GW as described in clause 4.5.1, e.g. to allocate a PDN GW that allows for more efficient routing. If the PDN subscription profile contains no PDN GW address for the default PDN and the Attach Type indicates "Handover" the non-3GPP access GW or ePDG selects a new PDN GW as described in clause PDN GW selection function;

NOTE 1: The MN NAI returned from the 3GPP AAA Server to the MAG is a permanent IMSI based MN NAI.

3) After successful authentication and authorization, the non-3GPP access specific L3 attach procedure is triggered;

4) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in step 6 and also to convey subscription related parameters to the PCRF.

5) The MAG function of Trusted Non-3GPP IP Access sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, *Additional Parameters*) message to PDN GW. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value in the case of a registration and a zero value in the case of a de-registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. Handover Indicator is set to "initial" attach if the UE has provided Attach Type indicating "Initial" attach or if the the Attach Type indicates "Handover" and the PDN subscription profile contains no PDN GW. Otherwise, Handover Indicator is set to "handover". The Additional Parameters may include Protocol Configuration Options and other information.

6) The PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session and associate Gateway Control Sessions established in step 4 correctly. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers.

7) The selected PDN GW informs the 3GPP AAA Server of its identity and the APN corresponding to the UE's PDN Connection. This information is registered in the HSS as described in clause 12.

8) The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates IP address for the UE. The PDN GW then sends a Proxy Binding Acknowledgement (MN NAI, Lifetime, *UE Address Info*, *GRE key for uplink traffic*, *Additional Parameters*) message to the MAG function in Trusted Non-3GPP IP Access, including the IP address(s) allocated for the UE. The UE Address Info includes one or more IP addresses. The Lifetime indicates the duration of the binding. The Additional Parameters may include Protocol Configuration Options and other information.

NOTE 2: If UE requests for both IPv4 and IPv6 addresses, both are allocated. If the UE requests for only IPv4 or IPv6 address only one address is allocated accordingly.

9) The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW.

10) In case the QoS rules have changed, the PCRF updates the QoS rules at the S-GW by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

11) L3 attach procedure is completed via non-3GPP access specific trigger. IP connectivity between the UE and the PDN GW is set for uplink and downlink directions.

6.2.2 Initial Attach Procedure with PMIPv6 on S2a and Chained S2a and GTP-based S8

This procedure applies to both PMIPv6 on S2a and to PMIPv6 on S2b.

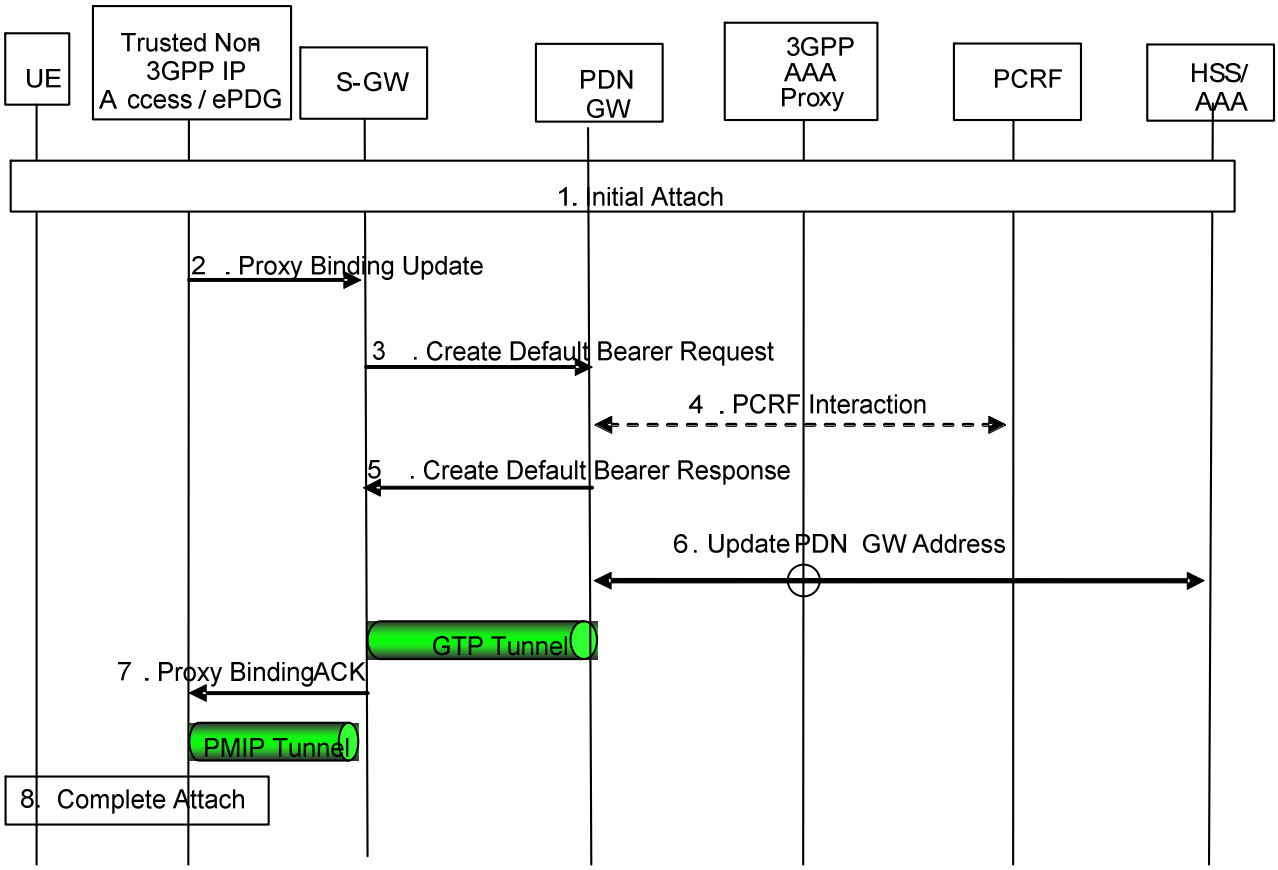


Figure 6.2.2-1: Default Bearer establishment for GTP-based S8 – S2a/b chained scenario

1. The initial access authentication and authorization is performed as described in steps 1-3 in clause 6.2.1 (for trusted non-3GPP access) and step 1 in clause 7.2.1 for untrusted non-3GPP access. As part of this procedure the 3GPP AAA proxy obtains the PDN GW information from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. Both PDN GW and Serving GW information is provided to the MAG function of the trusted non-3GPP access or ePDG.

2. The Trusted Non-3GPP IP Access / ePDG sends a Proxy Binding Update (MN_NAI, APN, PDN GW address) message to the Serving GW in the VPLMN.

3. The Serving GW sends a Create Default Bearer Request (Serving GW address for the user plane, Serving GW TEID for the user plane, Serving GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR) to the PDN GW.

NOTE: In this Release of the specification, the Serving GW uses a pre-configured QoS profile to establish the GTP-based S8 bearer to the PDN GW.

4. PDN-GW may interact with the PCRF for provisioning of PCC rules.

5. The PDN GW Sends a Create Default Bearer Response (PDN GW address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Address Information; Default Bearer QoS) to the Serving GW. This results in the establishment of a GTP-C and GTP-U tunnel between the two gateways.

Editor's Note: Details on alternatives for IP address allocation in the chained S2a/b – GTP-based S8 case is FFS.

6. The selected PDN GW informs the 3GPP AAA Server of the PDN GW's address. The 3GPP AAA Server then informs the HSS of the PDN GW address for the UE.

7. The Serving GW sends a Proxy Binding Ack message (MN_NAI, PDN Address Information) to the Trusted Non-3GPP IP Access / ePDG. A PMIPv6 tunnel is established between the Trusted Non-3GPP IP Access /ePDG and the Serving GW. To this is concatenated a GTP tunnel between the Serving GW and the PDN GW.

6.2.3 Initial Attach procedure with MIPv4 FACoA on S2a and Anchoring in PDN-GW

MIPv4 [12] is used to setup a MIP tunnel between the Trusted non-3GPP IP Access and the PDN GW. It is assumed that a Foreign Agent (FA) is located in the Trusted non-3GPP IP Access.

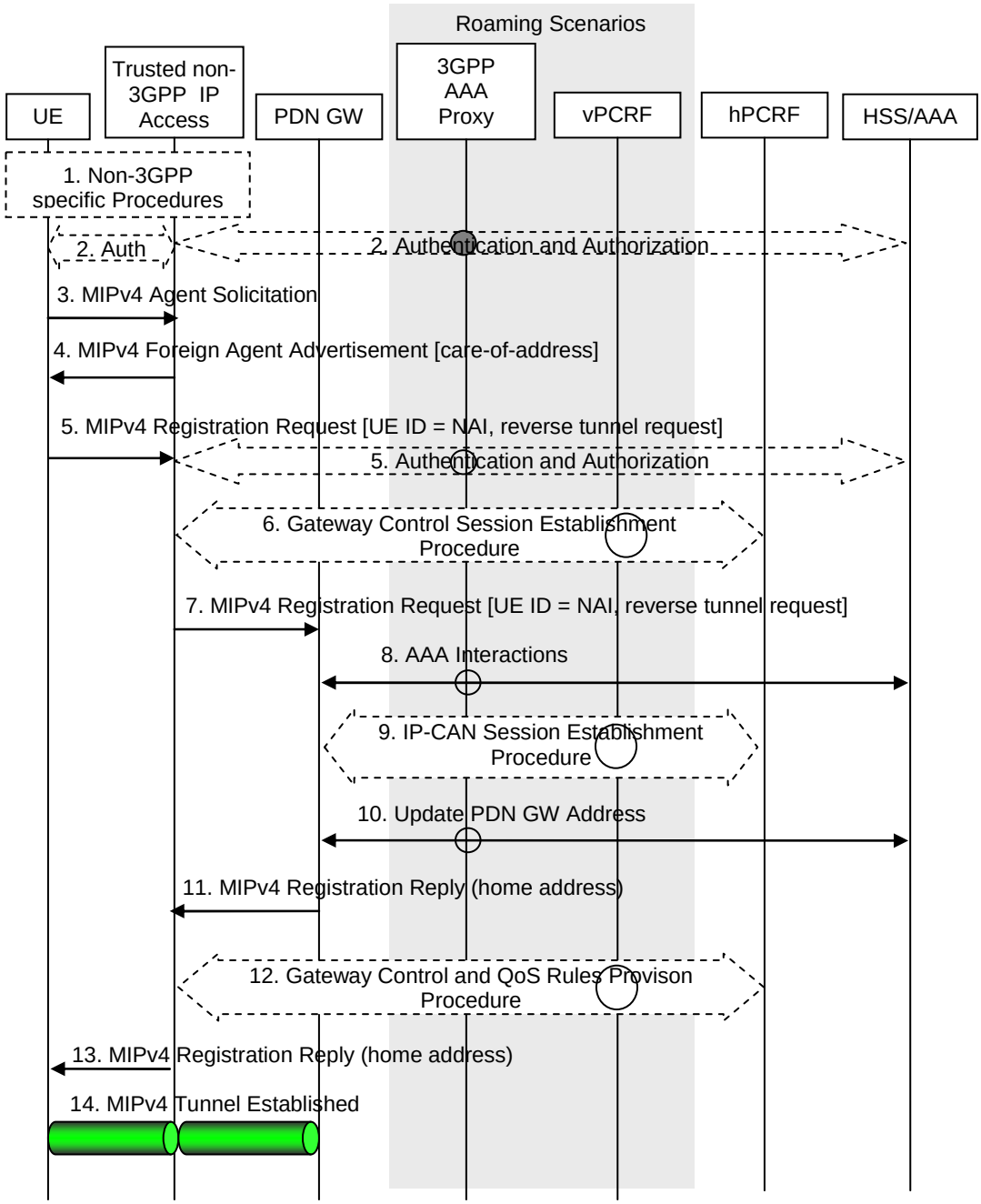


Figure 6.2.3-1: Initial attachment when MIPv4 FACoA mode MM mechanism is used over S2a

When the Attach procedure occurs in the Non-Roaming case (Figure 4.2.2-1), the vPCRF is not involved. The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

In the case of Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-5), the vPCRF is employed to forward messages from the hPCRF in the HPLMN, by way of the vPCRF in the VPLMN to the non-3GPP access. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN.

The event that triggers Authentication and Authorization in step 2 or step 5 between the Trusted Non-3GPP IP Access and the 3GPP AAA Server, or whether this step occurs at all, depends on the specific access technology.

1) The initial Non-3GPP access specific L2 procedures are performed. These procedures are outside the scope of 3GPP.

2) The Non-3GPP access specific authentication procedure is performed. The authentication procedure between UE and Trusted non-3GPP IP Access is outside the scope of 3GPP. Depending on the type of non-3GPP access system, the PDN Gateway address may be determined at this point as described in clause 4.5.1, otherwise it is determined in step 5 below. The PDN Gateway information is returned as part of the reply from the 3GPP AAA Server to the FA in the trusted non-3GPP access. This may entail an additional name resolution step. The Attach Type is indicated to the Non-3GPP access network by the UE as described in the step 2 of clause 6.2.1.

3) The UE may send an Agent Solicitation (AS) RFC 3344 [12] message. Specification of this message is out of the scope of 3GPP.

4) The FA in the Trusted Non-3GPP IP Access sends a Foreign Agent Advertisement (FAA) [12] message to the UE. The FAA message includes the Care-of Address (CoA) of the Foreign Agent function in the FA. Specification of this message is out of the scope of 3GPP.

5) The UE sends a Registration Request (RRQ) (MN-NAI) message to the FA as specified in RFC 3344 [12]. The MN NAI identifies the UE. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34]. The UE may not indicate a specific Home Agent address in the RRQ message, in which case the PDN Gateway/Home Agent is selected by the FA. The UE then receives the IP address of the PDN Gateway in step 13 as part of the Registration Reply (RRP) message. The UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages.

6) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in Step 10 and also to convey subscription related parameters to the PCRF.

7) The FA processes the message according to RFC 3344 [12] and forwards a corresponding RRQ (MN-NAI) message to the PDN GW.

8) The selected PDN GW obtains Authentication and Authorization information from the AAA/HSS.

9) The PDN GW allocates an IP address for the UE. The PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session and associate Gateway Control Sessions established in step 4 correctly. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers.

10) The selected PDN GW informs the 3GPP AAA Server of the PDN GW's address and the APN corresponding to the UE's PDN Connection. This information is registered in the HSS as described in clause 12.

11) The PDN GW sends a RRP (MN-NAI, Home Address, Home Agent Address, Lifetime) as defined in RFC 3344 [12] to the FA. The Home Address includes UE Home IP address, the Home Agent Address contains the IP address of Home Agent. The Lifetime indicates the duration of the binding.

Editor's note: Whether the PDN GW should authenticate the Registration Request message is FFS.

12) In case the QoS rules have changed, the PCRF updates the QoS rules at the S-GW by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

13) The FA processes the RRP (MN-NAI, Home Address, Home Agent Address) according to RFC 3344 [12] and sends a corresponding RRP message to the UE.

14) IP connectivity from the UE to the PDN GW is now setup. A MIP tunnel is established between the FA in the Trusted Non-3GPP IP Access and the PDN GW.

6.2.4 Initial Attach Procedure with PMIPv6 on S2a and Chained S2a and PMIP-based S8

This clause defines the initial attach procedure for the PMIP-based S8/S2a chaining. This procedure also applies to the initial attach for PMIP-based S8/S2b chaining.

Editor's note: Any solutions or extensions defined for the GTP-based and PMIP-based S8-S2a/b chaining shall not adversely impact procedures defined for non-chaining cases.

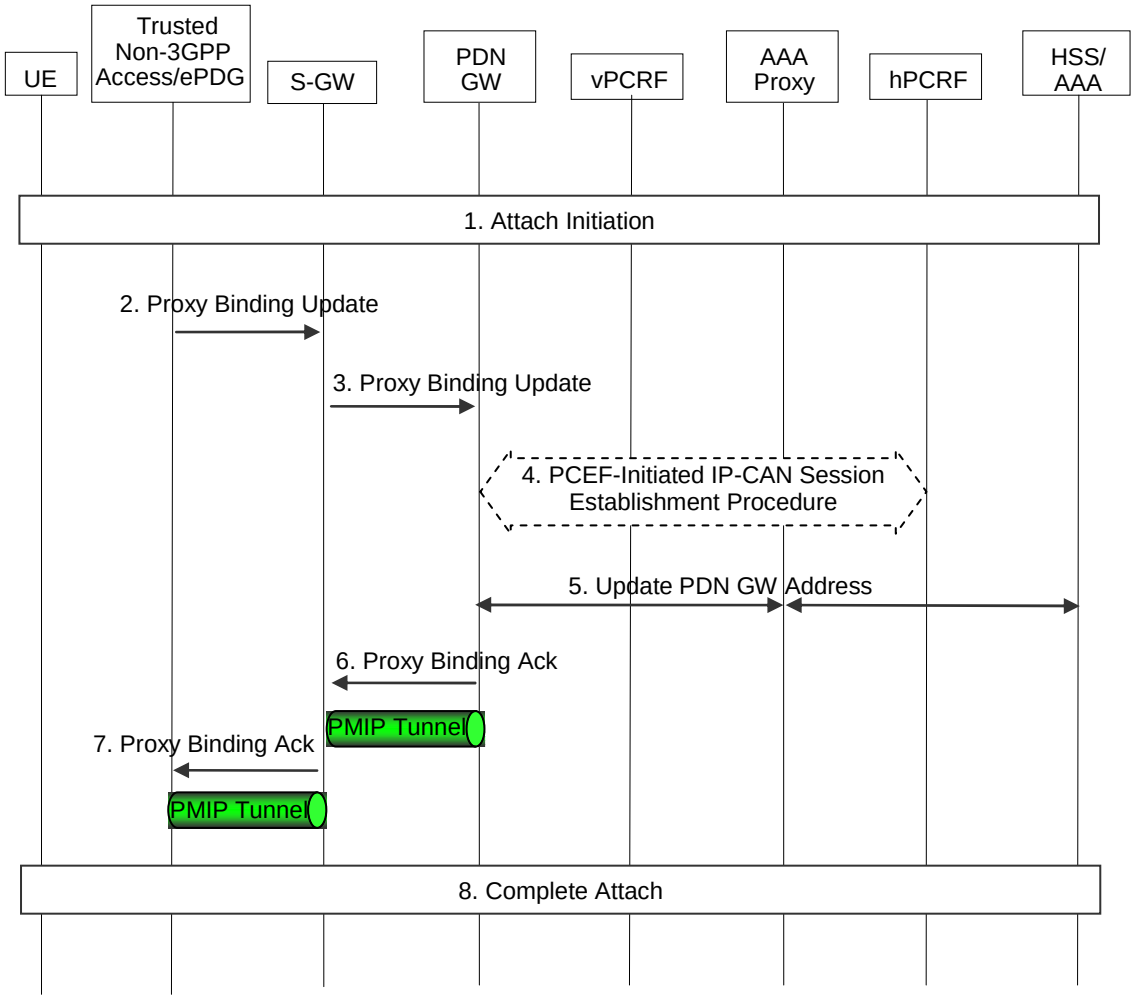


Figure 6.2.4-1: Initial attachment for chained PMIP-based S8-S2a/b roaming scenarios

1) The attach initiation on the trusted or untrusted non-3GPP access is performed as described in steps 1-3 of clause 6.2.1 (for trusted non-3GPP access) and step 1 of clause 7.2.1 (for untrusted non-3GPP access). As part of the authentication procedure, the 3GPP AAA proxy obtains the PDN GW information from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. Both, PDN GW and Serving GW information is provided to the MAG function of the trusted non-3GPP access or ePDG.

2) The MAG function of Trusted Non-3GPP IP Access or ePDG sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, PDN GW address, Additional Parameters) message to the Serving GW in the VPLMN. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value, indicating registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. Handover Indicator is set to indicate attachment over a new interface. The Additional Parameters may include Protocol Configuration Options and other information.

3) The Serving GW sends a corresponding Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, Additional Parameters) message (as in step 2) to the PDN GW.

4) The PDN GW initiates the PCEF-initiated IP CAN Session Establishment Procedure with the hPCRF, as specified in TS 23.203 [19].

5) The selected PDN GW informs the 3GPP AAA Server of its address. The 3GPP AAA Server then informs the HSS of the PDN GW address for the UE.

6) The PDN GW processes the proxy binding update and allocates IP address(es) for the UE. The PDN GW creates a binding cache entry for the PMIPv6 tunnel towards the Serving GW and sends a Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE Address Info includes one or more IP addresses. The Additional Parameters may include Protocol Configuration Options and other information.

NOTE: If UE requests for both IPv4 and IPv6 addresses, both are allocated. If the UE requests for only IPv4 or IPv6 address only one address is allocated accordingly.

7) The Serving GW processes the proxy binding acknowlegdement and creates a binding cache entry for the PMIPv6 tunnel towards the MAG function in the trusted non-3GPP access or ePDG. At this point, the Serving GW also establishes the internal forwarding state for the concatenation of the PMIPv6 tunnels. The Serving GW then sends a corresponding Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message (as in step 7) to the MAG function of Trusted Non-3GPP IP Access or ePDG.

8) The attach procedure is completed as described in steps 10-14 of clause 6.2.1 (for trusted non-3GPP access) and steps 7-8 of clause 7.2.1 (for untrusted non-3GPP access).

6.3 Initial Attach Procedure with DSMIPv6 on S2c in Trusted Non-3GPP IP Access

This section is related to the case when the UE attaches to a Trusted Non-3GPP Access network and host based mobility management mechanisms are used. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface.

The S2c attach can be seen to consist of several modules:

A. The UE sets up local IP connectivity in a Trusted Non-3GPP Access

B. The UE discovers the HA, and establishes a security association.

C. The UE performs a Binding Update with the PDN GW

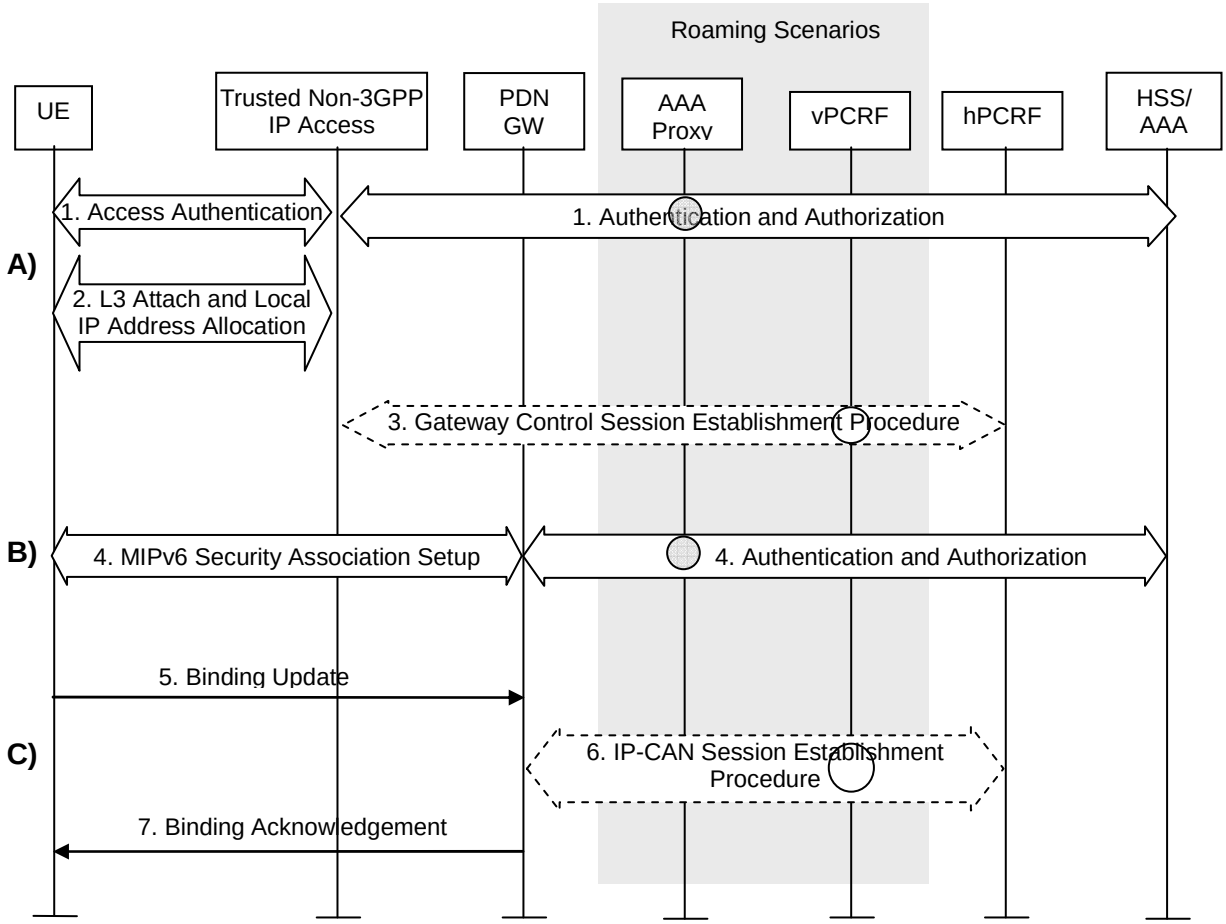


Figure 6.3-1: Initial attachment from Trusted Non-3GPP IP Access with DSMIPv6

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-5) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

A) Setup of Local IP connectivity

1) The initial access specific L2 and authentication procedures are performed. As indicated above, in the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN, as specified in TS 23.234 [5]. As part of the AAA exchange for network access authentication, the AAA/HSS and/or the 3GPP AAA Proxy may return to the Trusted non-3GPP IP Access a set of home/visited operator's policies to be enforced on the usage of local IP address, or IPv6 prefix, allocated by the access system upon successful authentication.

2) After successful authentication the L3 connection is established between the UE and the Trusted Non-3GPP Access system. As a result of this procedure, an IP address or an IPv6 prefix is also assigned to the UE by the access system (i.e. a Local IP address that will be used as a Care-of Address for DSMIPv6 over the S2c reference point).

NOTE 1: It is assumed that the access system is aware that network-based mobility procedures do not need to be initiated.

NOTE 2: The access system may complete the step 2 after step 3.

3) If the access system supports PCC-based policy control, the access gateway initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. The message includes at least the UE IP address or IPv6 prefix allocated by the access system. The message includes also the IP-CAN type.

Based e.g. on the UE identity and user profile, operator's policies and the IP-CAN type, the PCRF decides on the QoS policy rules and completes the session establishment towards the access gateway. The rules provided in this step are referred to the address assigned by the trusted non-3GPP access.

In the roaming case, PCC signalling is sent via a vPCRF in the VPLMN.

NOTE 3: The UE identity information to be used by the access system to establish the session with the PCRF may be piggybacked by the AAA/HSS in step 1.

B) PDN GW/HA Discovery and HoA Configuration.

4) The UE discovers the PDN GW (Home Agent) as specified in clause 4.5.2 of TS 23.402. A security association is established between UE and PDN GW to secure the DSMIPv6 messages between UE and PDN GW. The UE initiates the establishment of the security association using IKEv2 [9]; EAP [11] is used over IKEv2 for authentication purposes. The PDN GW communicates with the AAA infrastructure in order to complete the EAP authentication.

   If the PDN requires an additional authentication and authorization with an external AAA Server, an additional authentication is executed in this step. Details on these multiple authentications are specified in RFC 4739 [50] and in TS 23.234 [5] for I-WLAN (Private Network Access (PNA)).

   During this step an IPv6 home address/prefix is assigned by the PDN GW to the UE as defined in RFC 4877 [22]. During this step the UE may include the APN of the PDN it wants to access and it can also request the IPv6 home address as defined in RFC 4877 [22] in order to influence the IP address/prefix assignment procedure.

   During this step, the PDN GW also informs the 3GPP AAA Server of the identity of the selected PDN GW and the APN corresponding to the UE's PDN Connection. This information is registered in the HSS as described in clause 12.

NOTE 4: The MN NAI and APN string are delivered from the UE to the PDN GW in step 4 in order to support PCC interactions in step 6.

C) Binding Update

5) The UE sends the DSMIPv6 Binding Update (IP Addresses (HoA, CoA)) message to the PDN GW as specified in draft-ietf-mip6-nemo-v4traversal [10].

   The PDN GW processes the binding update. During the processing the PDN GW performs authentication and authorization of the message using the IPsec security association established in Step 4. During this step the UE can request an IPv4 home address to the PDN GW as defined in draft-ietf-mip6-nemo-v4traversal [10].

6) If PCC is supported, in 6a, the PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. The message includes at least the HoA and the CoA. The message may also include a permanent UE identity and an APN string. The PDN GW shall provide information about the mobility protocol tunneling header to the PCRF.

   The PCRF decides on the PCC rules and Event Triggers and provisions them to the PDN GW. The PDN GW installs the received PCC rules.

NOTE 5: The permanent UE identity to be used by the PDN GW to establish the session with the PCRF may be piggybacked by the AAA/HSS in step 4.

7) The PDN GW sends the DSMIPv6 Binding Ack (Lifetime, IP Addresses (HoA, CoA)) message to the UE. In this step the PDN GW may include the duration of the binding and the IP address allocated for the UE as specified in draft-ietf-mip6-nemo-v4traversal [10], if previously requested by the UE.

NOTE 6: Rules related to the HoA can be sent to the Trusted Non-3GPP Access based on the procedure in clause 6.6.2.

6.4 Detach for S2a

6.4.1 UE/Trusted Non-3GPP IP Access Network Initiated Detach Procedure with PMIPv6

6.4.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

UE/Trusted Non-3GPP Access Network-initiated detach procedure with PMIPv6 is illustrated in figure 6.4.1.1-1. The UE can initiate this procedure, e.g. when the UE is power off. The Trusted Non-3GPP Access Network can initiate this procedure due to administration reason or detecting the UE's leaving by, e.g. Link-layer event specific to the access technology (refer to PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) for more information).

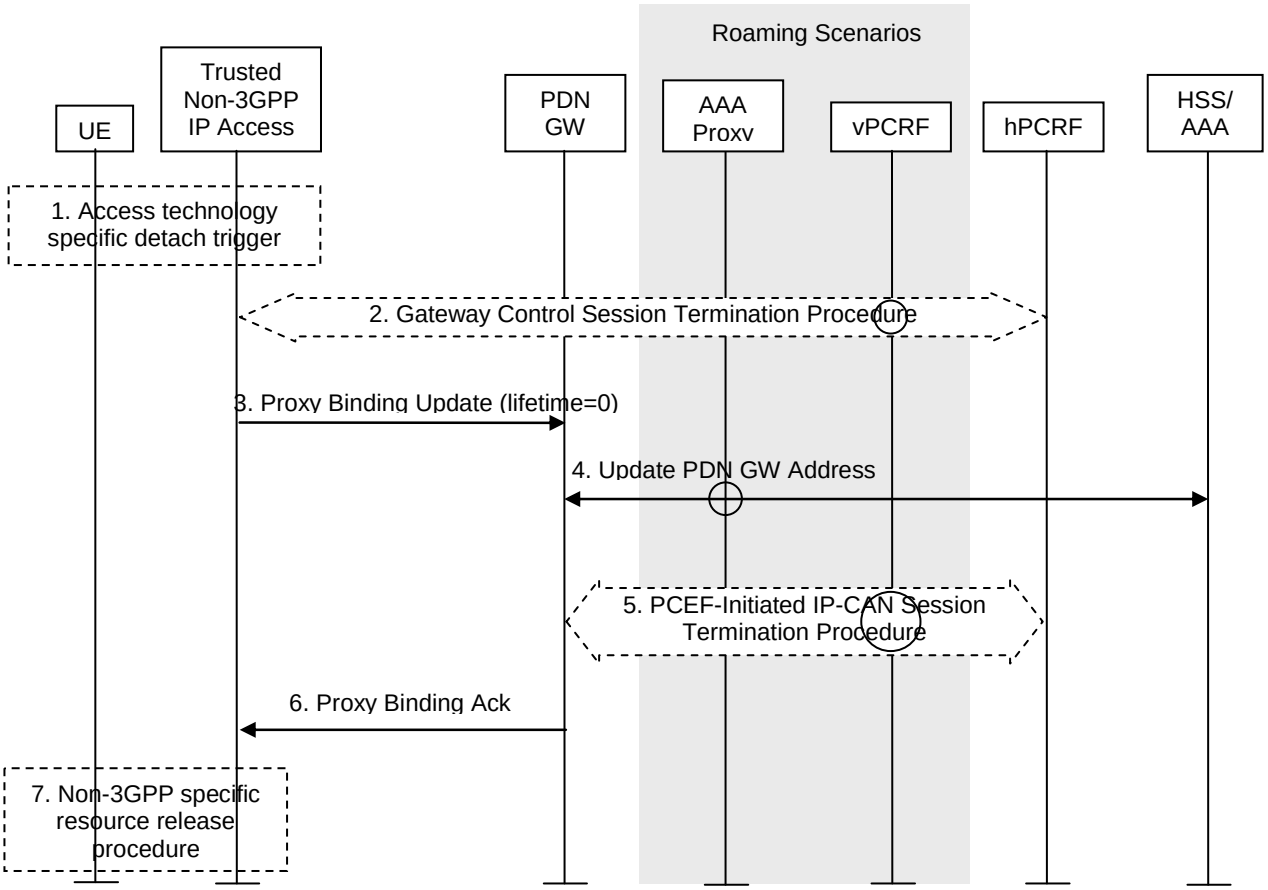


Figure 6.4.1.1-1: UE/Trusted Non-3GPP Access Network initiated detach procedure with PMIPv6

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-5) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 3 and 4 do not occur. Instead, the PDN GW may employ static configured policies.

1) The UE or the Trusted Non-3GPP Access Network triggers PMIPv6 de-registration by an access technology specific detach procedure.

2) The Trusted Non-3GPP Access Network initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to service data flows for this UE..

3) The Mobile Access Gateway (MAG) in the Trusted Non-3GPP IP Access sends a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the PDN GW with lifetime value set to zero, indicating de-registration. The

MN NAI identifies the UE to deregister from the PDN GW. The APN is needed in order to determine which PDN GW to deregister the UE from, as some PDNs may support multiple PDNs.

4) The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information and APN corresponding to the UE's PDN connection. This information is de-registered from the HSS as described in clause 12.

5) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

6) The PDN GW deletes all existing entries implied in the Proxy Binding Update message from its Binding Cache and sends a Proxy Binding Ack (MN NAI, lifetime=0) message to the MAG.

7) Non-3GPP specific resource release procedure is executed. The resources of Trusted Non-3GPP Access Network are released.

6.4.1.2 Chained PMIP-based S8-S2a Roaming Case

This clause defines the UE/Trusted Non-3GPP IP Access Network-initiated detach procedure for PMIP-based S8-S2a chaining. This procedure also applies to UE/ePDG-initiated detach procedure for PMIP-based S8-S2b chaining.

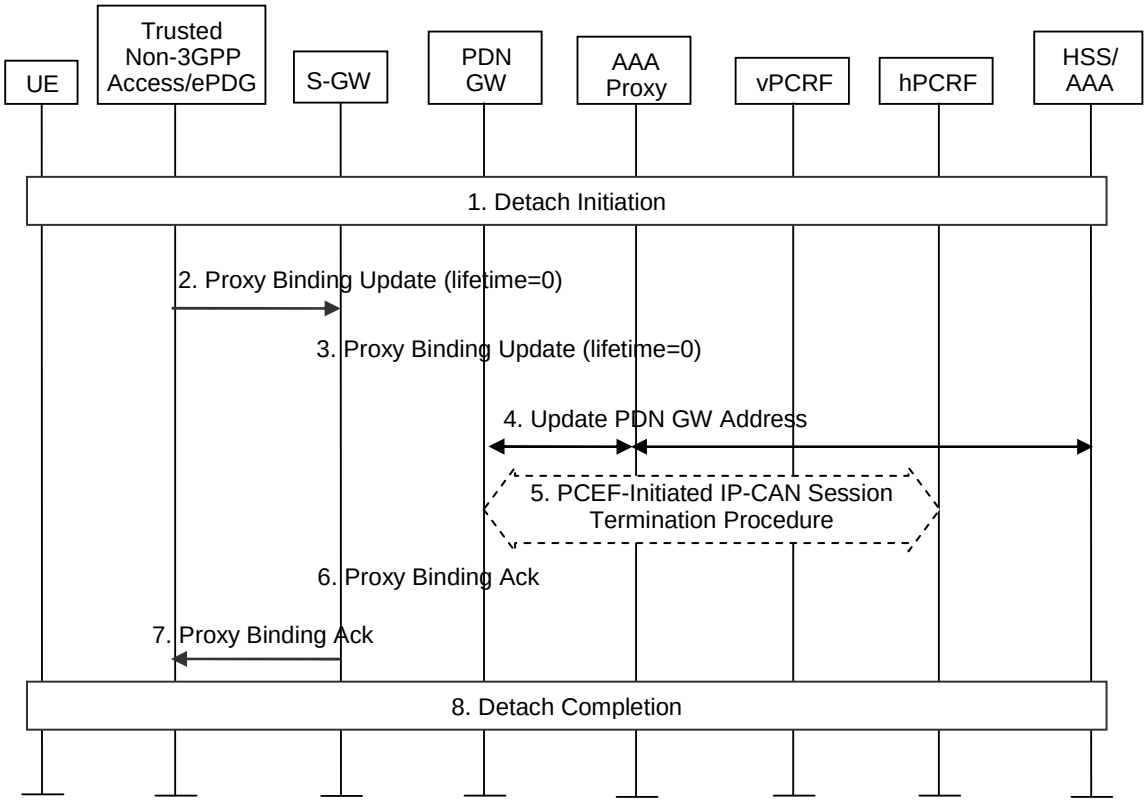


Figure 6.4.1.2-1: UE/ePDG/Trusted Non-3GPP Access Network initiated detach procedure for chained PMIP-based S8-S2a/b roaming scenarios

1) Initial steps of the detach is performed as described in steps 1-3 of clause 6.4.1.1 (for trusted non-3GPP access) and step 1 of clause 7.4.1.1 (for untrusted non-3GPP access).

2) The MAG in the Trusted Non-3GPP IP Access or ePDG sends a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the Serving GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the PDN GW. The APN is needed in order to determine which PDN GW to deregister the UE from, as some PDNs may support multiple PDNs.

3) The Serving GW deletes all existing entries implied in the Proxy Binding Update message from its Binding Cache and releases all associated resources (e.g. GRE tunnel), and then sends a corresponding Proxy Binding Update Update message (as in step 2) to the PDN GW in the HPLMN.

4) The PDN GW informs the AAA Server/HSS to remove the PDN GW address information for the UE.

5) The PDN GW initiates the PCEF-initiated IP CAN Session Termination Procedure, as specified in TS 23.203 [19].

6) The PDN GW deletes all existing entries implied in the Proxy Binding Update message from its Binding Cache and releases all associated resources, and then sends a Proxy Binding Ack (MN NAI, lifetime=0) message to the Serving GW in the VPLMN.

7) The Serving GW sends a corresponding Proxy Binding Ack message (as in step 6) to the MAG function in Trusted Non-3GPP IP Access.

8) The detach procedure is completed as described in step 9 of clause 6.4.1.1 (for trusted non-3GPP access) and step 7 of clause 7.4.1.1 (for untrusted non-3GPP access).

6.4.2 HSS/AAA Initiated Detach Procedure with PMIPv6

6.4.2.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

HSS/AAA-initiated detach procedure with PMIPv6 is illustrated in figure 6.4.2.1-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

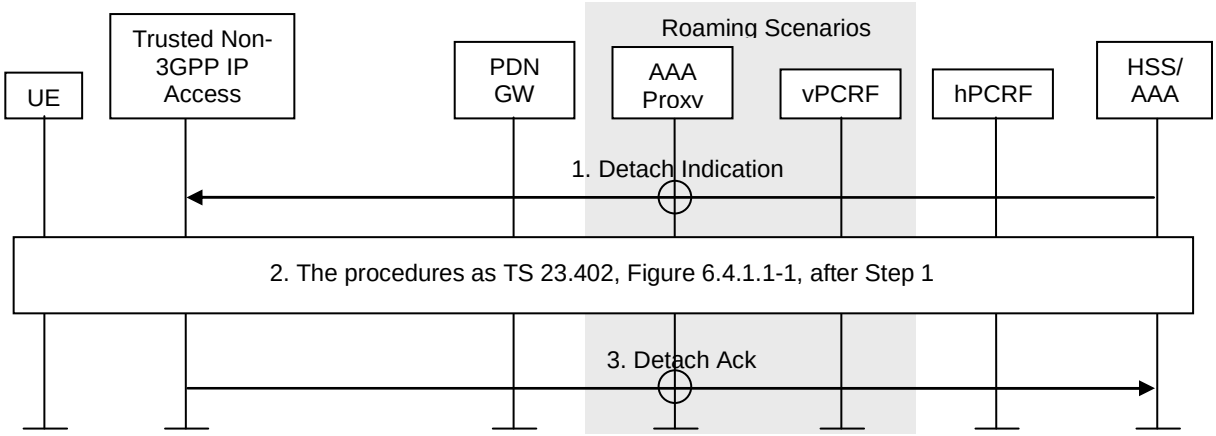


Figure 6.4.2.1-1: HSS/AAA-initiated detach procedure with PMIPv6

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-5) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 3 and 4 do not occur. Instead, the PDN GW may employ static configured policies.

1) The HSS/AAA sends a Detach Indication message to the MAG in the Trusted Non-3GPP Access Network to detach a specific UE.

2) This includes the procedure after step 1 as in figure 6.4.1.1-1.

3) The MAG of the Trusted Non-3GPP Access Network sends a Detach Ack message to the HSS/AAA.

6.4.2.2 Chained PMIP-based S8-S2a Roaming Case

This clause defines the HSS/AAA-initiated detach procedure for PMIP-based S8-S2a chaining. This procedure also applies for PMIP-based S8-S2b chaining.

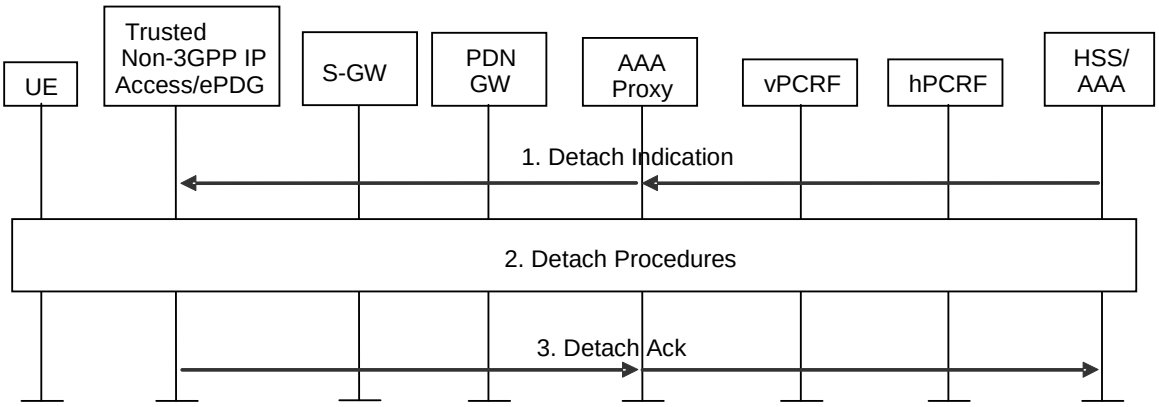


Figure 6.4.2.2-1: HSS/AAA-initiated detach procedure for chained PMIP-based S8-S2a/b roaming scenarios

1) The HSS/AAA sends a Detach Indication message to the MAG in the Trusted Non-3GPP Access Network or ePDG to detach a specific UE.

2) The detach procedure as described in steps 2-9 of clause 6.4.1.1 is performed for trusted non-3GPP accesses and according to steps 2-7 of clause 7.4.1.1 for untrusted non-3GPP accesses.

3) The MAG of the Trusted Non-3GPP Access Network or ePDG sends a Detach Ack message to the HSS/AAA.

6.4.3 UE-initiated Detach Procedure with MIPv4 FACoA

UE-initiated detach procedure with MIPv4 FACoA Mode is illustrated in Figure 6.4.3-1. The UE can initiate this procedure, e.g. when the UE is power off.

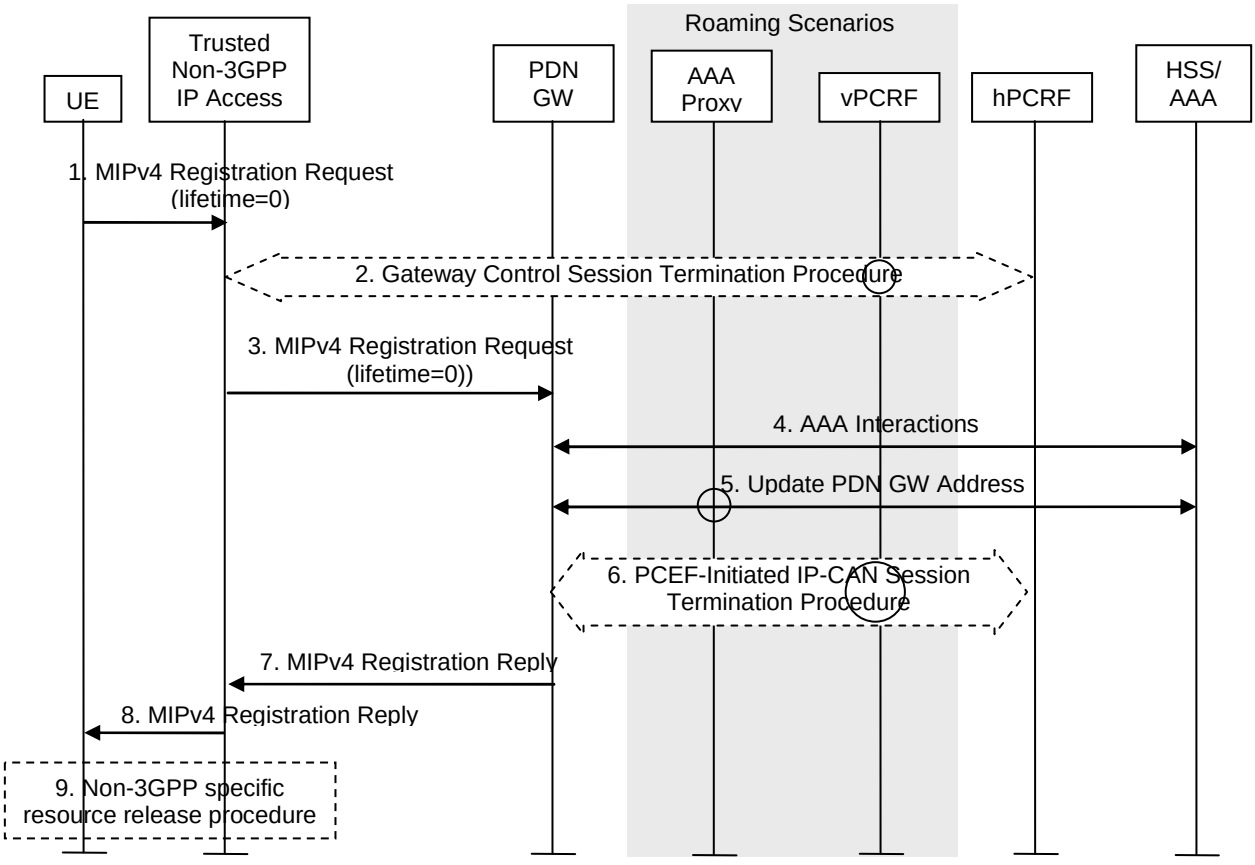


Figure 6.4.3-1: UE-initiated detach procedure with MIPv4 FACoA

NOTE: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-5).

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

1) The UE sends a MIPv4 Registration Request (RRQ) (MN-NAI, Home Address, Home Agent Address, Care-of Address, lifetime = 0) message to the Foreign Agent (FA) in the Trusted Non-3GPP Access Network with lifetime value set to zero, indicating de-registration. The MN-NAI identifies the UE. The Home Address includes UE Home IP addresses, the Home Agent Address contains the IP address of Home Agent. Care-of Address indicates the CoA used by the UE for the binding.

2) The Trusted Non-3GPP Access Network initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to service data flows for this UE.

3) The FA relays this MIPv4 RRQ (MN-NAI, lifetime = 0) message to the PDN GW.

4) The selected PDN GW obtains Authentication and Authorization information from the AAA/HSS.

5) The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information and APN corresponding to the UE's PDN Connection. This information is de-registered from the HSS as described in clause 12.

6) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

7) The PDN GW sends a MIPv4 Registration Reply (RRP) (MN-NAI, Home Address, Home Agent Address, Lifetime=0) message to the FA.

8) Anytime after step 4, the FA relays this MIPv4 RP (MN-NAI, Home Address, Home Agent Address, Lifetime=0) message to the UE.

9) After step 7, Non-3GPP specific resource release procedure is executed.

6.4.4 Network Initiated Detach Procedure with MIPv4 FACoA

Trusted Non-3GPP Access Network initiated detach procedure with MIPv4 FACoA Mode is illustrated in Figure 6.4.4-1. The Trusted Non-3GPP Access Network can initiate this procedure due to administration reason or detecting the UE's leaving by, e.g. Link-layer event specific to the access technology (see RFC 3543 [25] for more information).

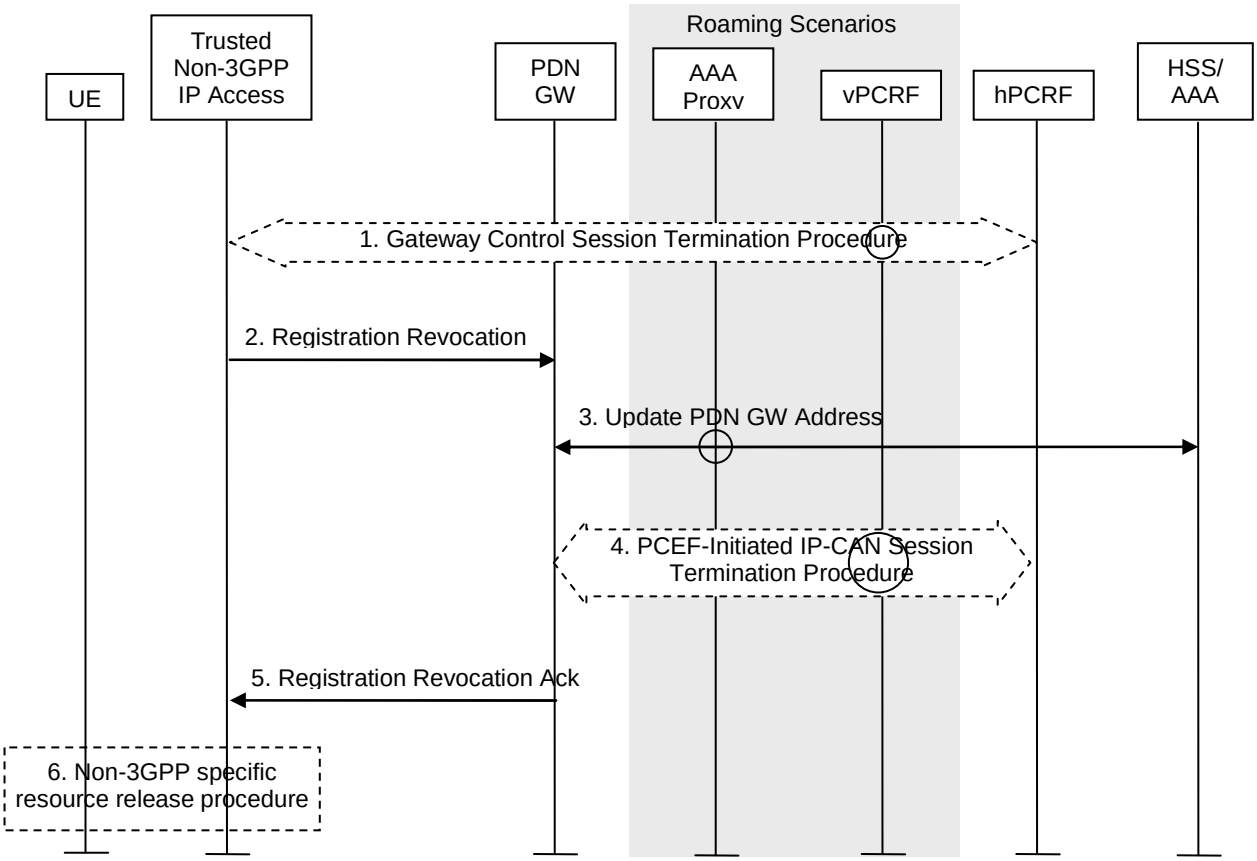


Figure 6.4.4-1: Trusted Non-3GPP Access Network initiated detach procedure with MIPv4 FACoA

NOTE: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-5).

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

1) The Trusted Non-3GPP Access Network detects the UE's leaving and initiates a Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to service data flows for this UE.

2) The FA sends a Registration Revocation (Home Address, Home Agent Address, Care-of Address) message (see RFC 3543 [25]) to the PDN GW.

3) The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information and APN corresponding to the UE's PDN Connection. This information is de-registered from the HSS as described in clause 12.

4) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5) The PDN GW sends a Registration Revocation Ack (Home Address) message (see RFC 3543 [25]) to the FA.

6) The Trusted Non-3GPP Access Network executes a specific resource release procedure.

6.4.5 HSS/AAA-initiated detach procedure with MIPv4 FACoA

HSS/AAA-initiated detach procedure with MIPv4 FACoA Mode is illustrated in Figure 6.4.5-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

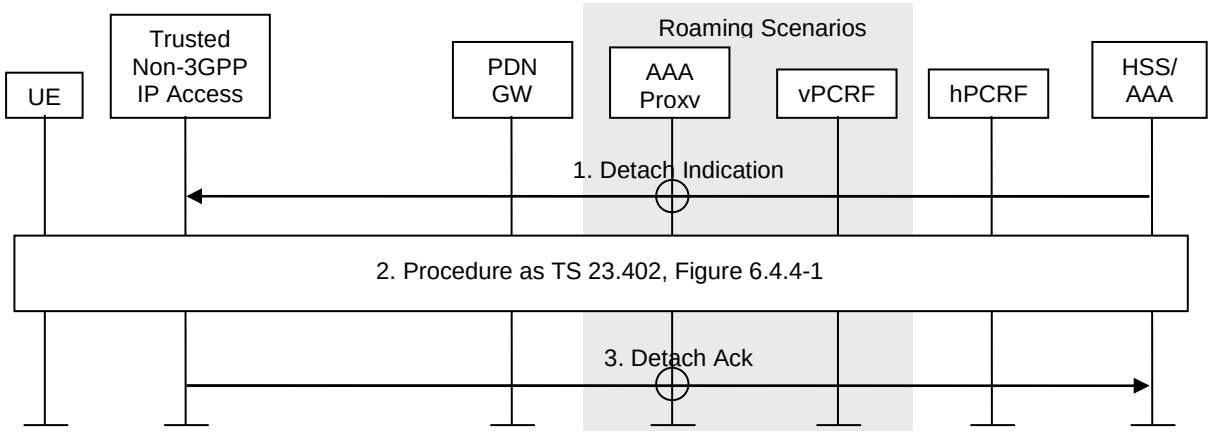


Figure 6.4.5-1: HSS/AAA-initiated detach procedure with MIPv4 FACoA

NOTE: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-5).

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

1) The HSS/AAA sends a detach indication message to the FA in the Trusted Non-3GPP Access Network to detach a specific UE.

2) This includes the procedure in figure 6.4.4-1.

3) The FA sends a Detach Ack message to the HSS/AAA.

6.5 Detach for S2c in Trusted Non-3GPP IP Access

6.5.1 General

This section is related to the case when a DSMIPv6 detach procedure is performed. The Detach procedure is on a per PDN basis and allows:

- the UE to inform the network that it does not want to use S2c any longer, and
- the network to inform the UE that it does not have access to the EPS through S2c any longer.

The UE is detached either explicitly or implicitly:

- Explicit detach: The network or the UE explicitly requests detach and signal with each other.
- Implicit detach: The network detaches the UE, without notifying the UE. This is typically the case when the network presumes that it is not able to communicate with the UE, e.g. due to radio conditions.

Two detach procedures are provided when the UE accesses the EPS through S2c:

- UE-Initiated Detach Procedure;
- AAA/HSS-Initiated Detach Procedure.

6.5.2 UE-initiated Detach Procedure

The Detach procedure when initiated by the UE is illustrated in Figure 6.5.2-1. The Detach procedure defined in this section must be repeated for each PDN.

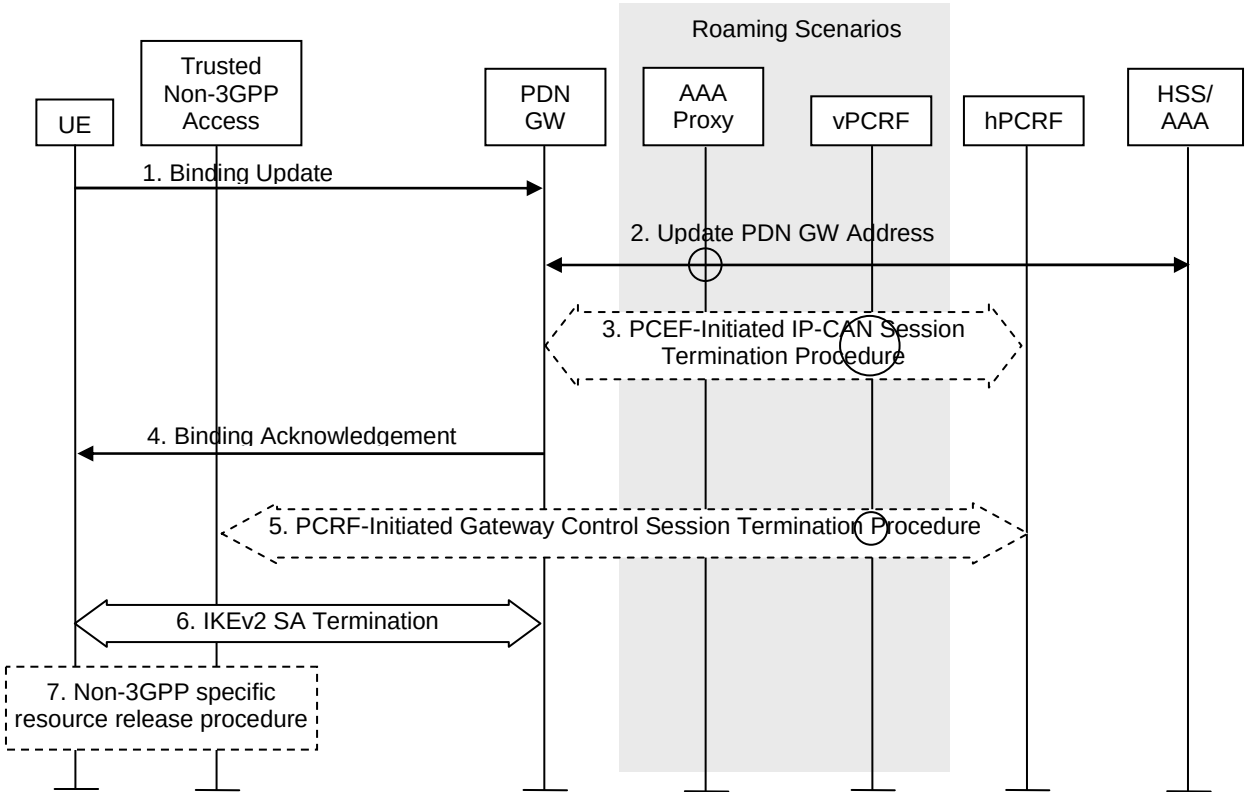


Figure 6.5.2-1: UE-initiated S2c detach procedure in Trusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-2), home routed roaming (Figure 4.2.3-4) and Local Breakout (Figure 4.2.3-5) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. If the UE wants to terminate a S2c session for a given PDN, it shall send a de-registration Binding Update (HoA, Lifetime=0) as specified in draft-ietf-mip6-nemo-v4traversal [10].
2. The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information for the UE. If the PDN GW is in the VPLMN, signalling may be routed via a 3GPP AAA Proxy in the VPLMN.
3. If there is an active PCC session for the UE, the PDN GW shall execute a PCEF-Initiated IP-CAN session Termination Procedure with the PCRF as specified in TS 23.203 [19].
4. The PDN GW shall send a Binding Acknowledgement as specified in draft-ietf-mip6-nemo-v4traversal [10]
5. The PCRF shall remove all active QoS rules which refer to the Home Address. The PCRF executes a PCRF-Initiated Gateway Control Session Termination Procedure with the Trusted Non-3GPP IP Access as specified in TS 23.203 [19]. The Trusted Non-3GPP IP Access will no longer perform any QoS policy or gateway control function associated with the terminated session.
6. The UE terminates the IKEv2 security association for the given PDN as defined in RFC 4306 [9]
7. After IKEv2 SA termination, non-3GPP specific resource release procedure may be executed.

6.5.3 HSS-initiated Detach Procedure

The Detach procedure when initiated by the HSS/AAA is illustrated in Figure 6.5.3-1. The Detach procedure defined in this section must be repeated for each PDN.

In the explicit detach procedure steps 2, 3 and 7 of Figure-6.5.3-1, are performed as illustrated. In the implicit detach, steps 2, 3 and 7 of Figure 6.5.3-1, are omitted.

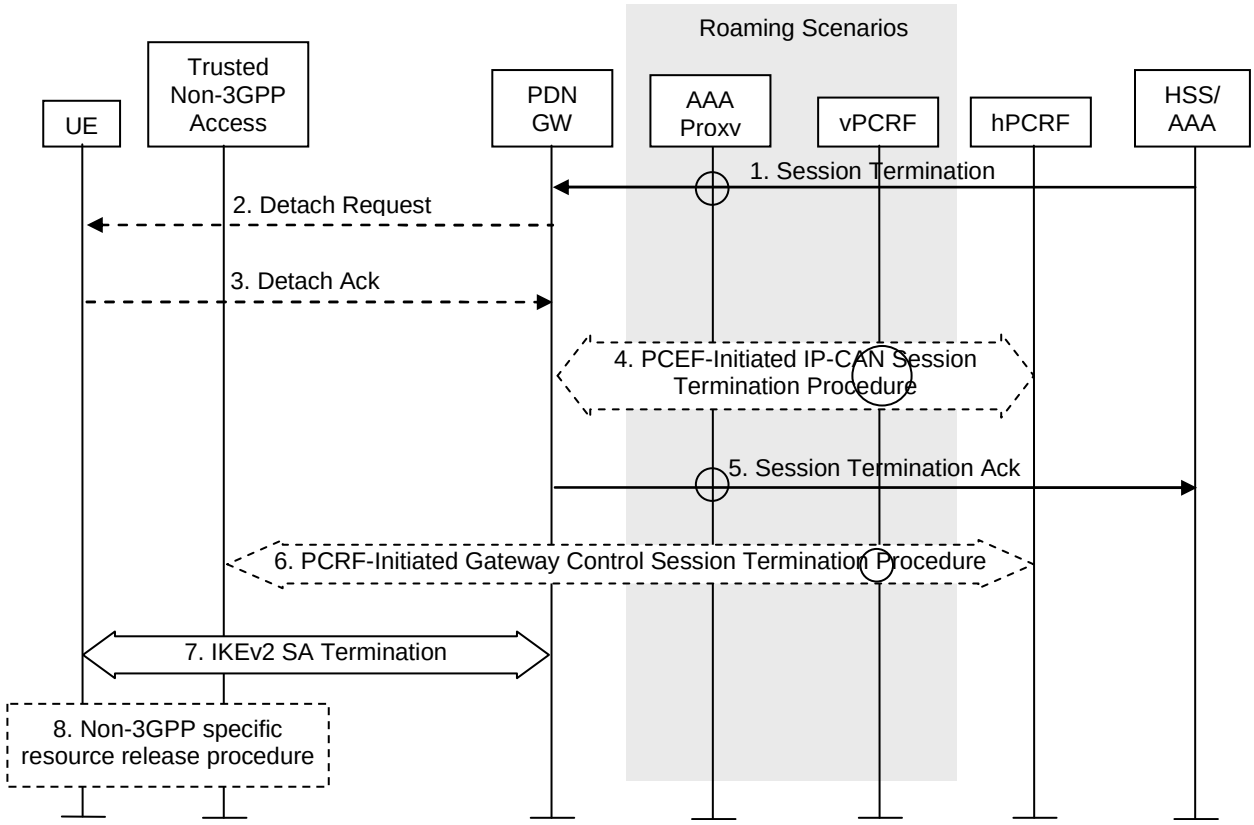


Figure 6.5.3-1: AAA/HSS-initiated S2c detach procedure in Trusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-2) and Local Breakout (Figure 4.2.3-5) cases are supported by this procedure. The 3GPP AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the 3GPP AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 4 and 6 do not occur. Instead, the PDN GW may employ static configured policies.

1. If the HSS/AAA wants to request the immediate termination of a S2c session for a given UE and a given PDN, it shall send a Session Termination message to the PDN GW. In the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN.

2. In the explicit detach procedure the PDN GW shall send a detach request message as specified. In the implicit detach procedure this step is omitted.

3. In the explicit detach procedure, the UE shall acknowledge the detach request. In the implicit detach procedure this step is omitted.

NOTE: How the detach request and acknowledge messages are implemented is a stage 3 detail.

4. If there is an active PCC session for the UE, the PDN GW shall execute a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5. The PDN GW shall acknowledge the termination of the S2c session to the AAA. The PDN GW information and APN associated with the UE's PDN Connection are de-registered from the HSS. As this is an HSS-initiated procedure, the mechanism described in clause 12 is not necessary.

6. The PCRF shall remove any active QoS Policy rule which is referred to the Home Address. The PCRF executes a PCRF-Initiated Gateway Control Session Termination Procedure with the Trusted Non-3GPP IP Access as specified in TS 23.203 [19]. The Trusted Non-3GPP IP Access will no longer perform any QoS policy or gateway control function associated with the terminated session.

NOTE: If no QoS Policy rules remain in the Trusted Non-3GPP Access, the Trusted Non-3GPP Access terminates the gateway control session towards the hPCRF.

7. In the explicit detach the PDN GW or the UE terminates the IKEv2 security association for the given PDN as defined in RFC 4306 [9]. In the implicit detach procedure this step is omitted.

8. After IKEv2 SA termination, non-3GPP specific resource release procedure may be executed.

6.6 Network-initiated Dynamic PCC

6.6.1 Network-initiated Dynamic PCC on S2a

If dynamic PCC is deployed, the procedure given in Figure 6.6.1-1 is used by the PCRF to provision rules to the Trusted non-3GPP IP access and for the Trusted non-3GPP IP access to enforce the policy by controlling the resources and configuration in the trusted non-3GPP access. The access specific procedure executed in the trusted non-3GPP access is not within the scope of this specification.

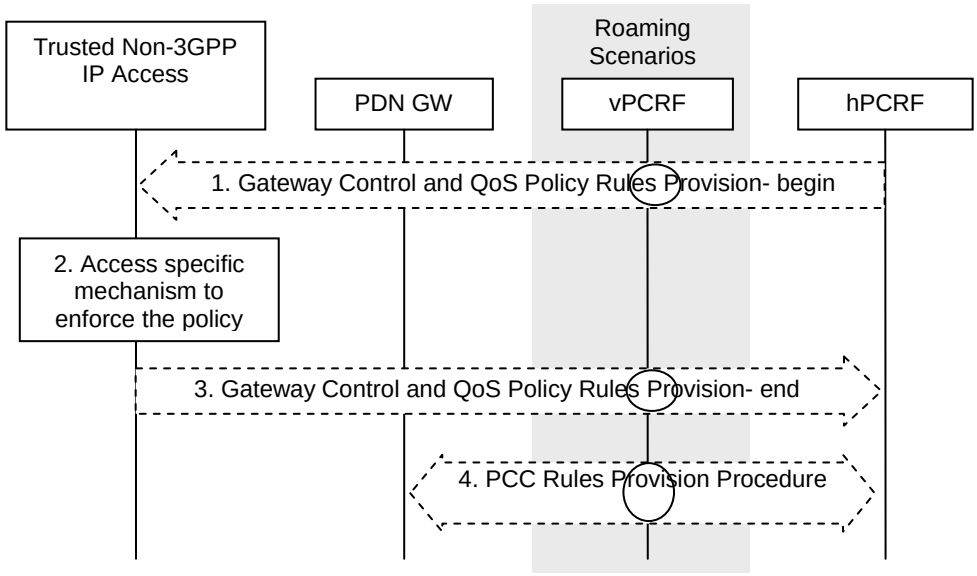


Figure 6.6.1-1: Network-initiated dynamic policy control procedure in Trusted Non-3GPP IP Access for S2a

This procedure concerns both the non-roaming (as Figure 4.2.2-1) and roaming case (as Figure 4.2.3-1). In the roaming case, the vPCRF in the VPLMN forwards messages between the Trusted Non-3GPP IP Access and the hPCRF in the HPLMN. In the case of Local Breakout (as Figure 4.2.3-5), the vPCRF forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. The PCRF initiates the Gateway Control and QoS Policy Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the QoS rules and Event Trigger information to the Trusted non-3GPP access network..

2. The Trusted Non-3GPP IP Access enforces the rules provisioned to it, and establish all necessary resources and configuration in the non-3GPP access system, ,for eg. initiate a dedicated bearer activation, modification or deactivation, if supported. The details of this step are out of the scope of this specification.

3. The Trusted Non-3GPP IP Access responds to the PCRF indicating its ability to enforce the rules provisioned to it in Step 1 and thus completing the GW Control and QoS Rules Provision procedure started in step A.1.

4. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [19]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of an PCC Rules Provision procedure specified in TS 23.203 [19].

NOTE: Step 4 may occur before step 1 or performed in parallel with steps 1-3 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

6.6.2 Network-initiated Dynamic PCC for S2c over Trusted Non-3GPP IP Access

This section is related to the case when network-initiated dynamic resource allocation is supported, and it is utilized for the S2c SDFs.

The procedure described in this section may also be used subsequent to the S2c Attach procedure described in Section 6.3

In this case, the PCRF may push specific PCC rules to the PDN GW and QoS Policy rules to the Trusted Non-3GPP Access system, in case the Access System supports PCC.

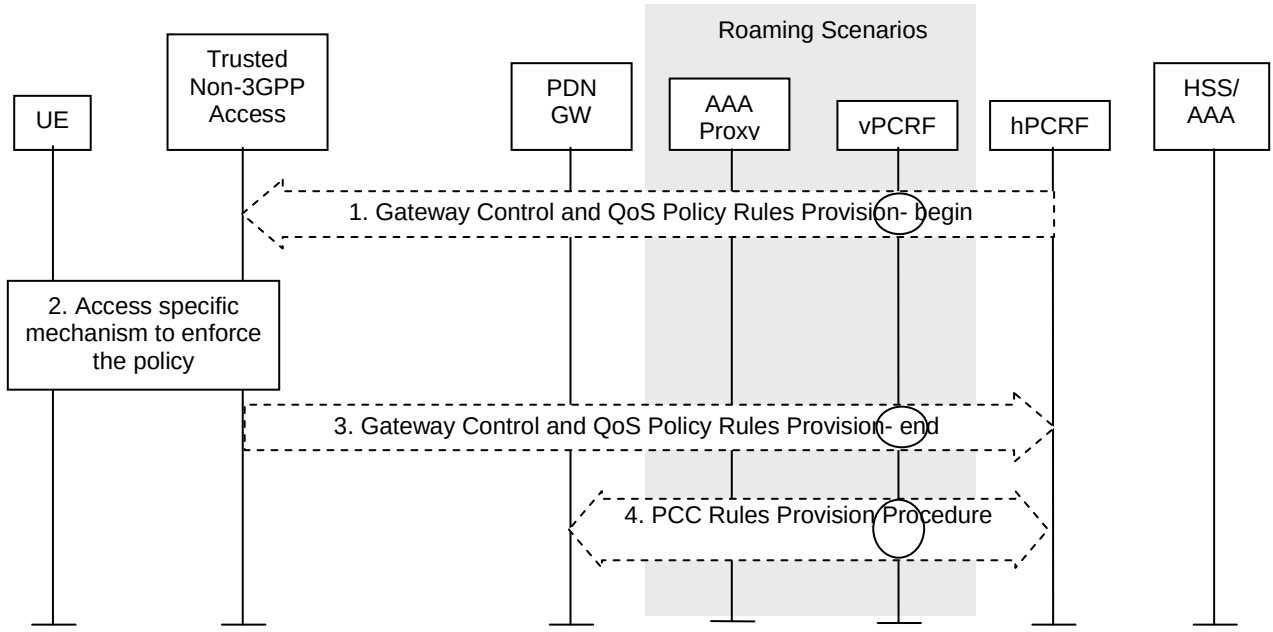


Figure 6.6. 2-1: Network-initiated dynamic policy control for S2c over Trusted Non-3GPP IP Access

This procedure concerns both the non-roaming (as Figure 4.2.2-2) and roaming case (as Figure 4.2.3-4). In the roaming case, the vPCRF in the VPLMN forwards messages between the Trusted Non-3GPP IP Access and the hPCRF in the HPLMN. In the case of Local Breakout (as Figure 4.2.3-5), the vPCRF forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

Steps 1-4 are the same as in steps 1-4 in clause 6.6.1.

6.7 UE-initiated Resource Request and Release

6.7.1 UE-initiated Resource Request and Release on S2a

This procedure is applicable to both PMIPv6 on S2a and DSMIPv6 on S2c.

This section is related to the case when UE-initiated resource request and release is supported in the Trusted Non-3GPP IP Access, and it is utilized for the S2a/S2c SDFs.

Figure 6.7.1-1 depicts the procedure for the roaming and non-roaming cases.

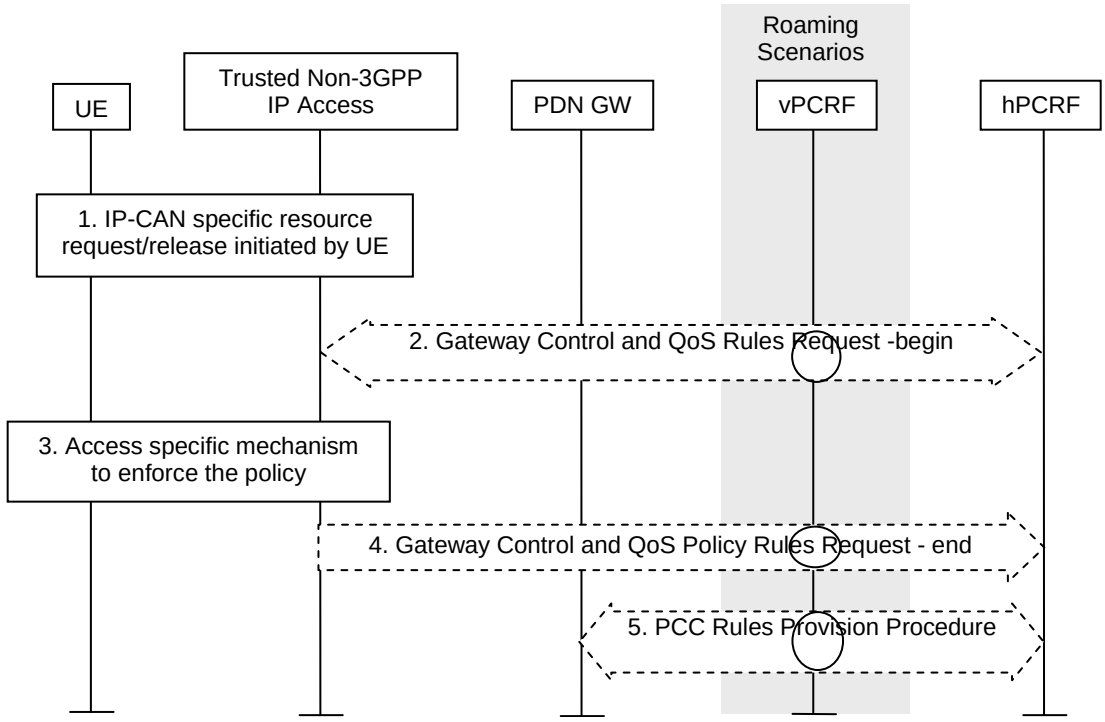


Figure 6.7.1-1: UE-initiated resource request/release with S2a or S2c

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

1. The trusted non-3GPP access receives an IP-CAN specific resource allocation or resource release request initiated by the UE.

2. The trusted non-3GPP access initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19]. The Serving GW provides the UE request or release of resources as an Event Report. The PCRF makes a PCC decision as a result of the Gateway Control and QoS policy request and provides the updated QoS Rules to trusted non-3GPP access.

3. An IP-CAN specific resource allocation or resource release procedure may be triggered by the enforcement of the received policy rules. In this step, a response for the resource request/release is sent to the UE.

4) The trusted non-3GPP access indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not and thus completing the GW Control and QoS Rules Provision procedure.

5) The PCRF initiates the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19] to update the PCC rules in the PDN GW. The updated PCC Rules and Event Triggers include any adjustments to resources due to the decision taken in step 2.

NOTE: Step 5 may be performed in parallel with Steps 2-4 if acknowledgement of resource allocation is not required at the PCRF to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

Step 2 may be omitted if the Trusted non-3GPP access has already received authorisation for the UE's request from the PCRF, eg. QoS rules downloaded at handover.

6.7.2 UE-initiated Resource Request for S2c over Trusted Non-3GPP IP Access

The procedure is specified in Section 6.7.1.

6.8 UE-initiated Connectivity to Additional PDN

6.8.1 UE-initiated Connectivity to Additional PDN with PMIPv6 on S2a

6.8.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

Establishment of connectivity to an additional PDN over trusted access with S2a is supported only for the accesses that support such feature and the UEs that have such capability.

PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) is used to setup a IP connectivity between the trusted non-3GPP IP access and the EPC during initial attach. In both roaming and non-roaming cases, S2a is present. It is assumed that MAG exists in the trusted non-3GPP IP access.

NOTE: The PDN GW treats each MN-ID+APN as a separate binding and may allocate a new IP address/prefix for each binding.

Editor's Note: It is FFS if and how multiple PDN connections to one APN from a single UE is supported, i.e. whether the MN-ID + APN is sufficient to uniquely identify a PDN connection instance, or whether additional parameter(s) are needed.

The procedure is also used for the re-establishment of existing PDN connectivity after the UE performed the handover from 3GPP accesses for the first PDN connection by the Attach procedure.

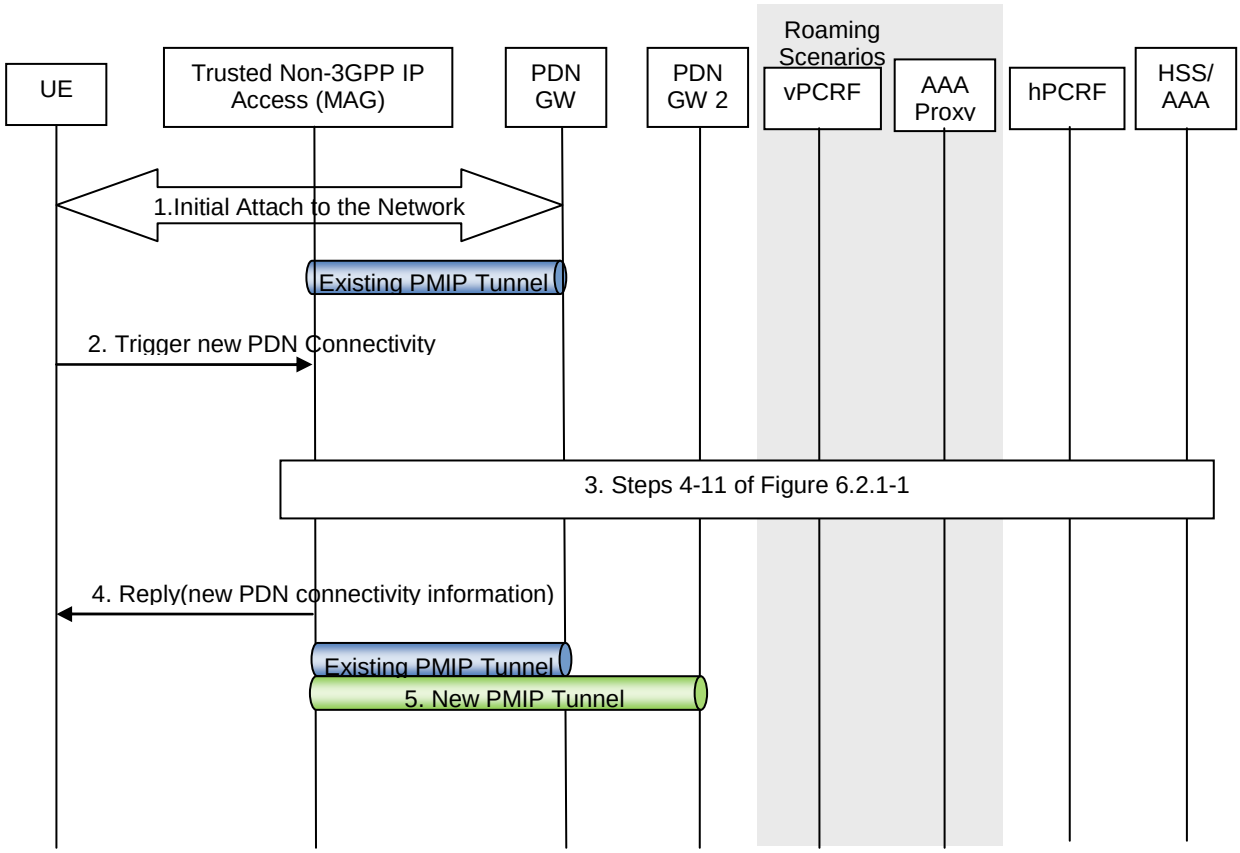


Figure 6.8.1.1-1: Additional PDN connectivity with Network-based MM mechanism over S2a for non-roaming and roaming

The steps in the procedure which are marked as optional occur only if dynamic policy provisioning has been deployed.

In the roaming case, messages are forwarded between the Trusted Non-3GPP IP Access and the hPCRF via the vPCRF. In the case of LBO, messages are forwarded between the PDN GW and the hPCRF via the vPCRF also. Further, in the case of LBO, messages between the PDN GW and the 3GPP AAA Server are sent via the 3GPP AAA Proxy.

If dynamic policy provisioning is not deployed, the optional steps 3 and 4 do not occur. Instead, the PDN GW may employ static configured policies.

1) The UE performs initial attach to the trusted non-3GPP access and gets IP connectivity to a default PDN served by a certain PDN GW, as indicated by the user profile.

2) When the UE wishes to connect to an additional PDN, it sends a trigger indicating that connectivity with that specific PDN is desired. The UE provides information about the new PDN by using an APN. The UE triggers the re-establishment of existing PDN connectivity after the handover by providing a Request Type indicating "Handover" on accesses that support the indication.

Editors Note: The definition of the trigger that the UE provides to the access network (MAG) is out of scope for 3GPP

3) Steps 4 to 11 according to clause 6.2.1 are executed with PDN GW2 instead of PDN GW1.

   If the UE provides the Request Type indicating "Handover" in step 2, or the MAG determines based on the Subscriber Data obtained during authentication that the UE is already connected to this PDN before the handover, the following applies:

   - In step 4 of clause 6.2.1 the MAG provides the Handover Indicator to indicate this is a handover;
   - Steps 5 and 6 of clause 6.2.1 correspond to the PCEF-Initiated IP-CAN Session Modification procedure specified in TS 23.203 [19];
   - Step 7 of clause 6.2.1 is not performed;
   - In step 8 of the clause 6.2.1, the UE Address Info shall contain the same IP address the UE obtained during PDN connectivity establishment over the 3GPP access.

4) The trusted non-3GPP access system sends the reply message to the UE with the allocated IP address from the PDN that the UE indicated at 2. Since UE requested for additional PDN connectivity, the UE configures the IP address received from the MAG without deleting its configuration for connectivity with any other previously established PDN. For handover, the UE is returned the IP address the UE obtained during PDN connectivity establishment over the 3GPP access.

Editors Note: It is FFS that which message will be used to carry the new connectivity information to the UE and it may be out of scope of 3GPP.

5) The PMIPv6 tunnel is thus set up between the Trusted Non-3GPP IP Access and the PDN GW corresponding to the requested additional PDN while maintaining tunnels previously established for other PDNs.

6.8.1.2 Chained PMIP-based S8-S2a Roaming Case

This clause defines the UE-initiated Connectivity to Additional PDN for PMIP-based S8-S2a chaining. This procedure also applies for PMIP-based S8-S2b chaining.

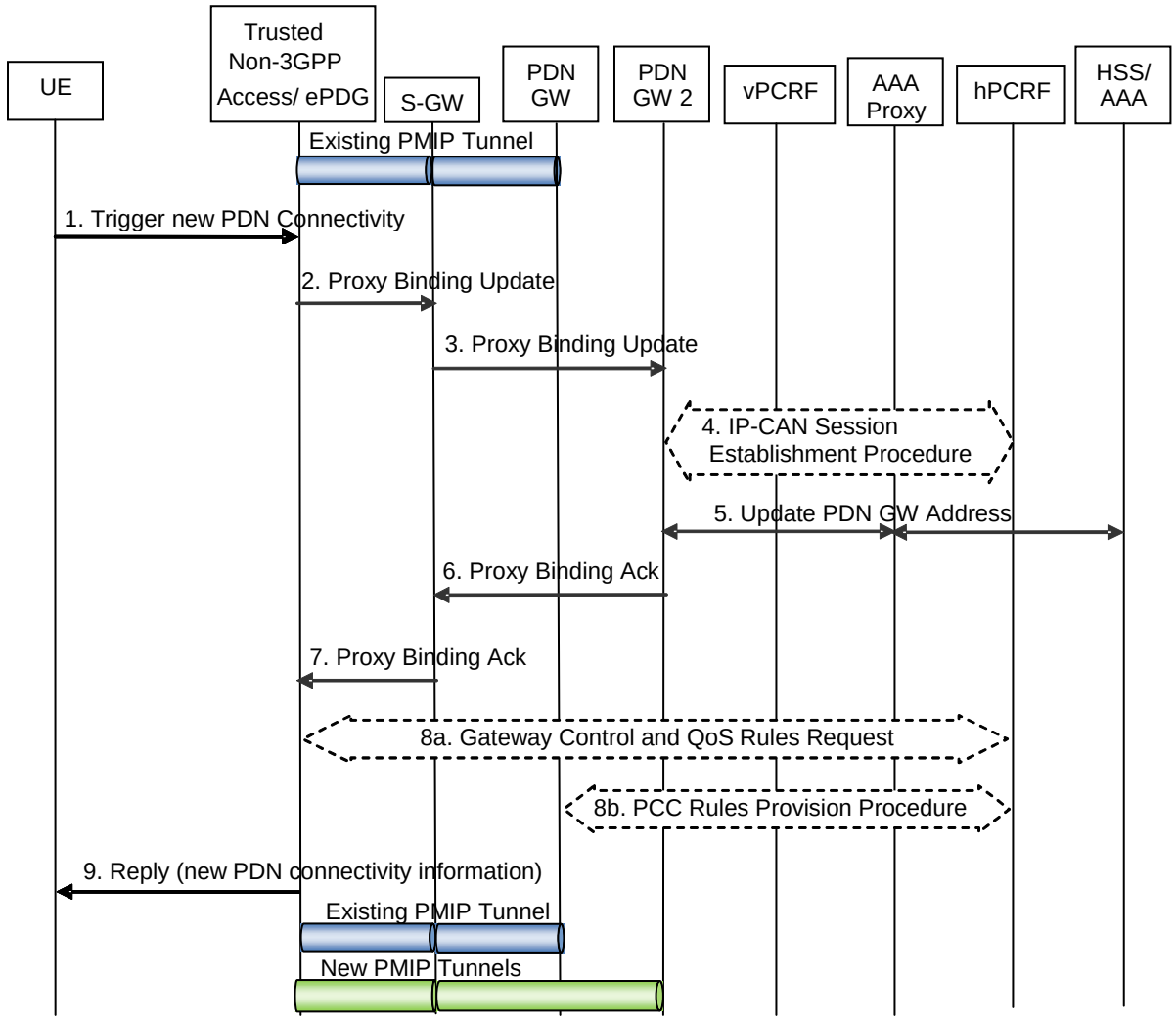


Figure 6.8.1.2-1: Additional PDN connectivity for chained PMIP-based S8-S2a/b roaming scenarios

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The gateway control signalling in steps 8a-8b between the gateway and PCRF occur only for Trusted Non-3GPP IP Accesses.

1) When the UE wishes to connect to an additional PDN, it sends a trigger indicating that connectivity with that specific PDN is desired. The UE provides information about the new PDN by using an APN.

Editors Note: The definition of the trigger that the UE provides to the access network (MAG) is out of scope for 3GPP.

2) When the MAG function of the trusted non-3GPP access or the ePDG receives this trigger for additional PDN connectivity, it selects a suitable PDN GW based on the APN information in the indication from the UE and sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, PDN GW address, Additional Parameters) message to the Serving GW in the VPLMN. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value, indicating registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. Handover Indicator is set to indicate attachment over a new interface. The Additional Parameters may include Protocol Configuration Options and other information.

3) The Serving GW sends a corresponding Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, Additional Parameters) message (as in step 2) to the PDN GW.

4) The PDN GW initiates the IP CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19].

5) The selected PDN GW informs the 3GPP AAA Server of its address. The 3GPP AAA Server then informs the HSS of the PDN GW address for the UE.

6) The PDN GW processes the proxy binding update and allocates IP address(es) for the UE. The PDN GW creates a binding cache entry for the PMIPv6 tunnel towards the Serving GW and sends a Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The UE Address Info includes one or more IP addresses. The Lifetime indicates the duration of the binding. The Additional Parameters may include Protocol Configuration Options and other information.

7) The Serving GW processes the proxy binding acknowlegdement and creates a binding cache entry for the PMIPv6 tunnel towards the MAG function in the trusted non-3GPP access or ePDG. At this point, the Serving GW also establishes the internal forwarding state for the concatenation of the PMIPv6 tunnels. The Serving GW then sends a corresponding Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message (as in step 7) to the MAG function of the Trusted Non-3GPP IP Access or ePDG.

8) In case of PMIP-based S8/S2a chaining, the trusted non-3GPP access initiates the Gateway Control and QoS Rules Request Procedure with the hPCRF (step 8a), as specified in TS 23.203 [19]. In turn, the hPCRF initiates the PCC Rules Provision Procedure with the PDN GW to updates the rules in the PDN GW, using the information provided by the Serving GW (step 8b), as specified in TS 23.203 [19].

NOTE: This step does not apply in case of PMIP-based S8/S2b chaining.

9) The trusted non-3GPP access system or ePDG sends the reply message to the UE with the allocated IP address from the PDN that the UE indicated at step 2. Since UE requested for additional PDN connectivity, the UE configures the IP address received from the MAG or ePDG without deleting its configuration for connectivity with any other previously established PDN.

Editors Note: It is FFS that which message will be used to carry the new connectivity information to the UE and it may be out of scope of 3GPP.

6.8.2 UE-initiated Connectivity to Additional PDN with MIPv4 FACoA on S2a

NOTE: The PDN GW treats each MN-ID+APN as a separate binding and may allocate a new IP address/prefix for each binding.

Editor's Note: It is FFS if and how multiple PDN connections to one APN from a single UE is supported, i.e. whether the MN-ID + APN is sufficient to uniquely identify a PDN connection instance, or whether additional parameter(s) are needed.

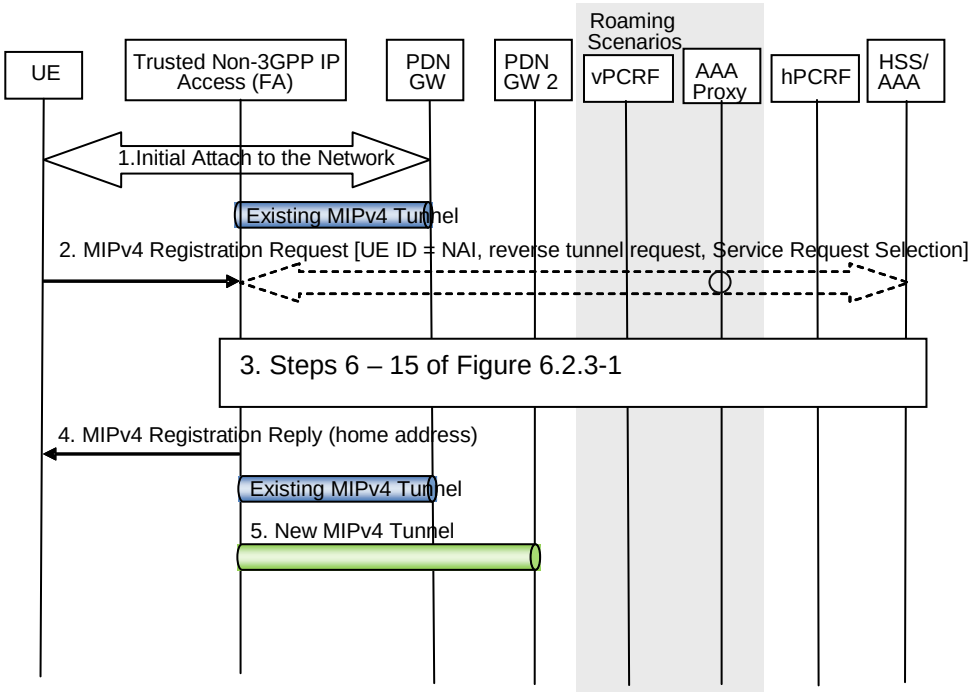


Figure 6.8.2-1: UE-initiated Connectivity to Additional PDN with MIPv4 FACoA on S2a

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

1) The UE performs initial attach to the trusted non-3GPP access and gets IP connectivity to a default PDN served by a certain PDN GW, as indicated by the user profile.

2) When the UE wishes to connect to an additional PDN, UE sends a Registration Request (RRQ) (MN-NAI, lifetime, APN) RFC 3344 [12] message to the FA as specified in RFC 3344 [12]. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34]. The UE may not indicate a specific Home Agent address in the RRQ message, in which case the PDN Gateway/Home Agent is selected by the FA. The UE then receives the IP address of the PDN Gateway in step 13 as part of the Registration Reply (RRP) message. The UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages. The UE provides information about the new PDN by using an APN as specified in draft-korhonen-mip4-service [39].

3) Steps 6-15 of clause 6.3.2 are excecuted with PDN GW2 instead of PDN GW1.

4) The FA processes the RRP (MN-NAI, Home Address, Home Agent Address) message according to RFC 3344 [12] and sends a corresponding RRP message to the UE.

5) The MIPv4 tunnel is thus set up between the Trusted Non-3GPP IP Access and the PDN GW corresponding to the requested additional PDN while maintaining tunnels previously established for other PDNs.

6.8.3 UE-initiated Connectivity to Additional PDN from Trusted Non-3GPP IP Access with DSMIPv6 on S2c

This section is related to the case when the UE attaches to a Trusted Non-3GPP Access network and host-based mobility management mechanisms are used. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface. This case describes the scenario when UE adds connectivity to one or more additional PDN at any time after initial attach. Since host-based mobility mechanisms are used, the procedure is similar to the initial attach procedure.

NOTE: Based on the MN-ID and APN, the PDN GW may allocate a new IP address/prefix for a new binding.

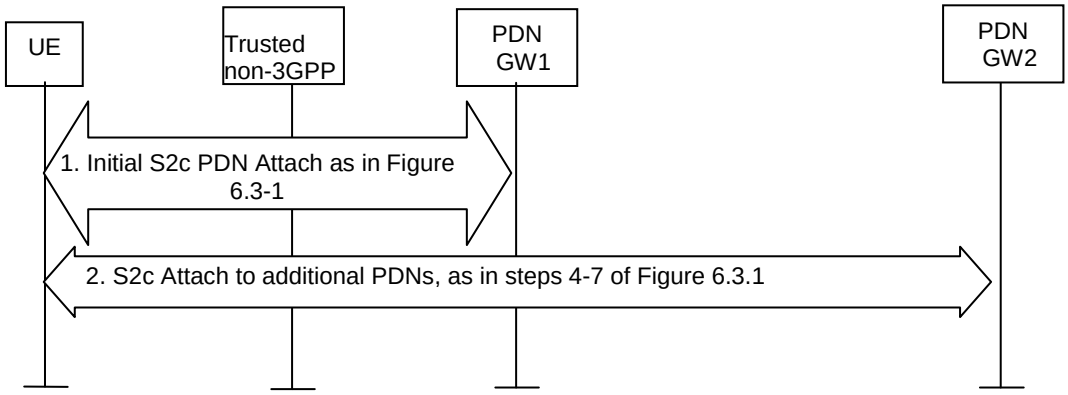


Figure 6.8.3-1: UE-initiated connectivity to multiple PDNs from Trusted Non-3GPP IP Access with DSMIPv6

When the initial attachment is performed, the UE performs procedures described in clause 6.3, Figure 6.3-1, to obtain connectivity with a PDN GW and a specific PDN. If at any time, the UE wants to obtain connectivity with additional PDNs, it repeats steps 4-7 of Figure 6.3-1.

1) The UE performs S2c PDN Attach procedure as defined in clause 6.3, Figure 6.3-1.

2). The UE repeats steps 4-7 of clause 6.3, Figure 6.3-1 for each additional PDN the UE wants to connect to. This step can be performed and be repeated at any time after step 1 for one or multiple PDNs.

If the UE discovers a different PDN GW for the additional PDN connectivity, when the current PDN GW could provide access to the additional PDN, the PDN GW reallocation procedure may be used, as defined in clause 6.10.

6.9 ME Identity Check Procedures for Trusted Non-3GPP IP Accesses

< This subclause will contain details on ME identity checking (e.g. IMEI checking)>

6.10 PDN GW reallocation upon initial attach on S2c

The PDN GW reallocation procedure depicted in figure 6.10-1 can be used by the HSS/AAA to force the assignment of a new PDN GW to the UE upon initial attach with DSMIPv6 in a trusted or untrusted non-3GPP IP access. The decision on whether to trigger PDN GW reallocation is taken by the HSS/AAA according to the principles described in clause 4.5.1.

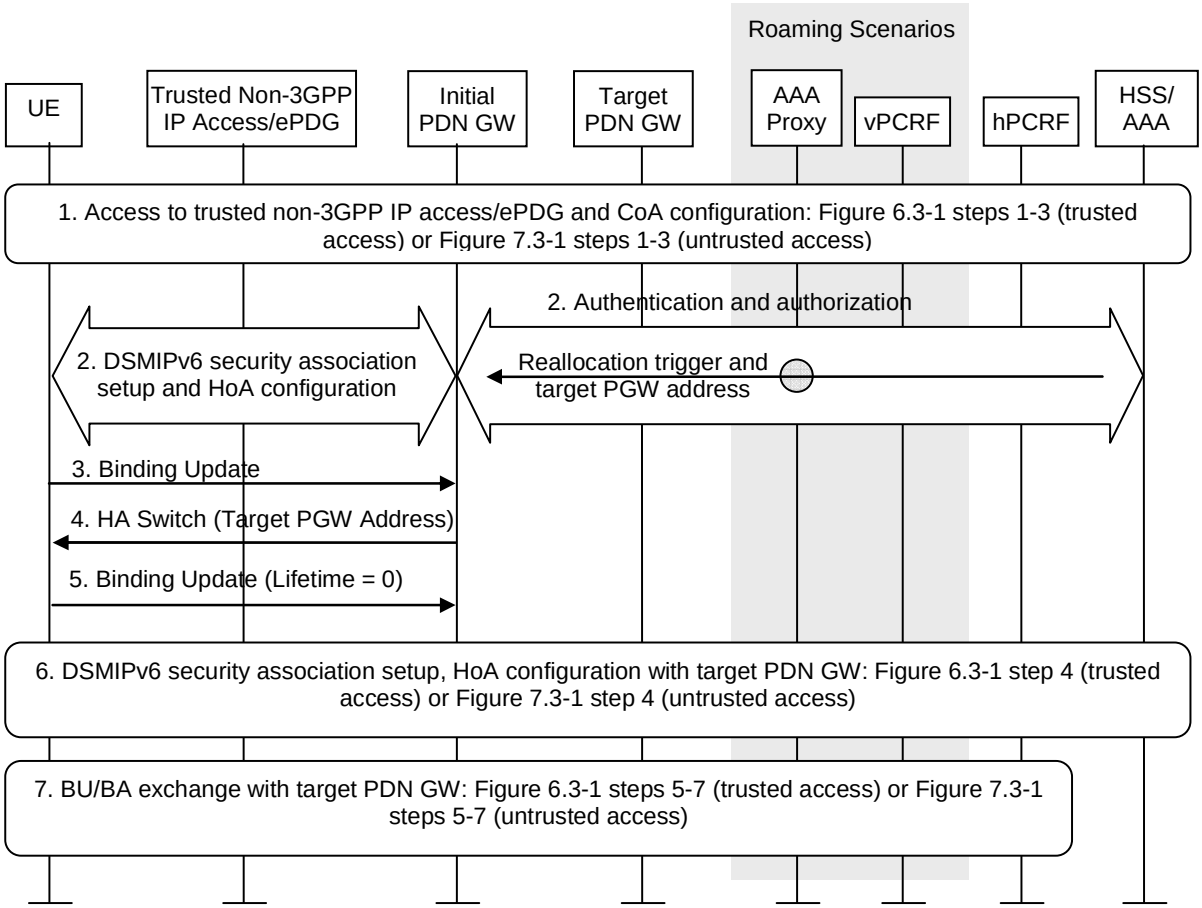


Figure 6.10-1: PDN GW reallocation upon initial attach on S2c

The following is a detailed description of the involved steps:

1) The UE authenticates in the trusted non-3GPP access, or establishes the IPsec tunnel with the ePDG, and obtains a local IP address to be used as care-of address for DSMIPv6.

2) The UE establishes the DSMIPv6 SA with the initially discovered PDN GW. This implies a AAA exchange with the HSS/AAA. The HSS/AAA triggers the PDN GW and the APN associated with the UE's PDN Connection reallocation piggybacking a reallocation indication and the address of the target PDN GW in the AAA exchange. This information is registered in the HSS as described in clause 12.

3) The UE delivers the BU to the initially discovered PDN GW.

4) The PDN GW replies to the BU with a HA Switch message (draft-ietf-mip6-ha-switch [42]), including the address of the target PDN GW received from the HSS/AAA in step 2.

5) The UE acknowledges the HA Switch message with the deregistration BU, that is a Binding Update with lifetime set to zero.

6) After having deregistered from the initially discovered PDN GW, the UE establishes the DSMIPv6 SA with the target PDN GW provided by the network in the HA Switch message.

7) The UE performs the DSMIPv6 registration with the target PDN GW.

6.11 S2c Bootstrapping via DSMIPv6 Home Link over a Trusted Access

When the UE is connected on a trusted non-3GPP access considered to be DSMIPv6 home link for the UE, the UE may trigger the establishment of S2c IKEv2 SA, e.g. to optimize future handovers to other accesses using S2c. For each PDN connection, the S2c IKEv2 SA establishment has to be performed separately.

NOTE: A trusted non-3GPP access can be defined as DSMIPv6 Home Link in addition to the 3GPP access.

Once the UE is attached to the PDN over the trusted non-3GPP access, the procedure describing the bootstrapping is in clause 15.1.

6.12 PDN GW initiated Resource Allocation Deactivation

6.12.1 PDN GW initiated Resource Allocation Deactivation with S2a PMIP

All the resource allocations associated with the PDN address are released in this procedure.

Both the roaming and non-roaming scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the Gateway Control Session Termination message from the Serving GW in the VPLMN to the hPCRF in the VPLMN. The vPCRF receives the Acknowledgment from the hPCRF and forwards it to the trusted non-3GPP IP access. In the non-roaming case, the vPCRF is not involved at all.

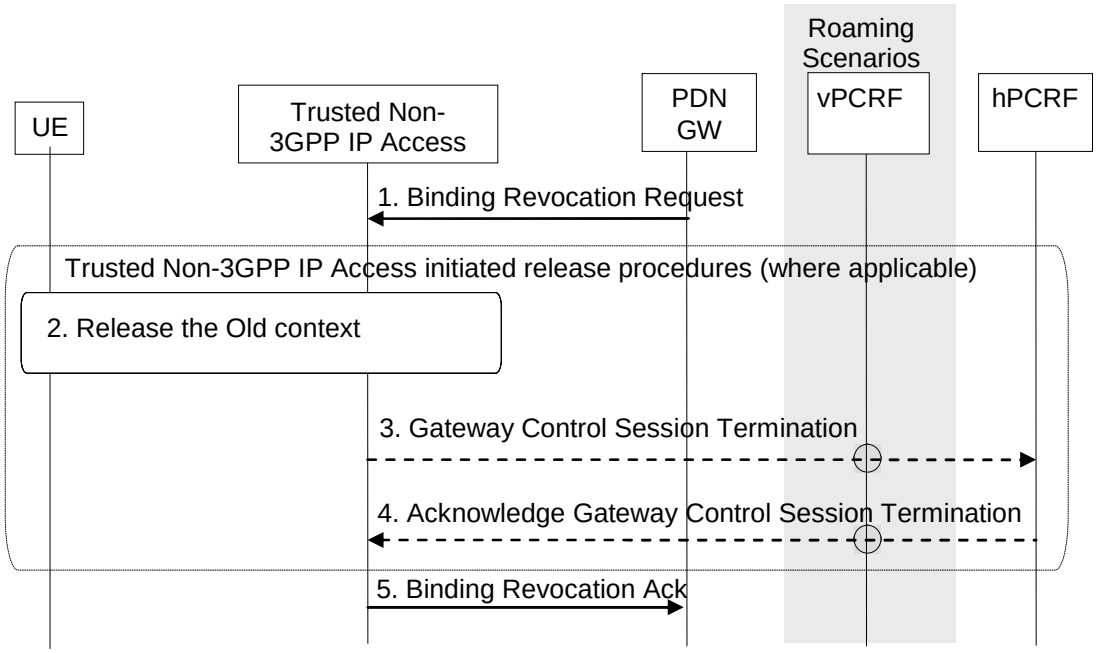


Figure 6.12.1-1 PDN GW Initiated Binding Revocation with S2a PMIP

Both the roaming (figure 4.2.1-2) and non-roaming (figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the Gateway Control Session Termination message from the Serving GW in the VPLMN to the hPCRF in the HPLMN. The vPCRF receives the Acknowledgment from the hPCRF and forwards it to the Serving GW. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 6.12.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. The PDN GW sends a Binding Revocation Indication message to the trusted non-3GPP IP access as defined in draft-muhanna-mip6-binding-revocation [35].

2. The resources may be released in trusted non-3GPP IP access, according to an access specific, trusted non-3GPP IP access initiated, release mechanism.

3. If resources are released in trusted non-3GPP IP access, the non-3GPP access sends a Gateway Control Session Termination message to the PCRF.

4. The PCRF responds the trusted non-3GPP IP access with Acknowledge Gateway Control Session Termination message.

5. The trusted non-3GPP IP access returns a Binding Revocation Acknowledgement message to the PDN GW.

NOTE: For some accesses, the resources may be released independently of deactivation from the PDN GW.

6.12.2 PDN GW initiated Resource Allocation Deactivation with S2a MIPv4

All resource allocations associated with the PDN address are released in this procedure.

Both the roaming and non-roaming scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the Gateway Control Session Termination message from the Serving GW in the VPLMN to the hPCRF in the HPLMN. The vPCRF receives the Acknowledgment from the hPCRF and forwards it to the trusted non-3GPP IP access. In the non-roaming case, the vPCRF is not involved at all.

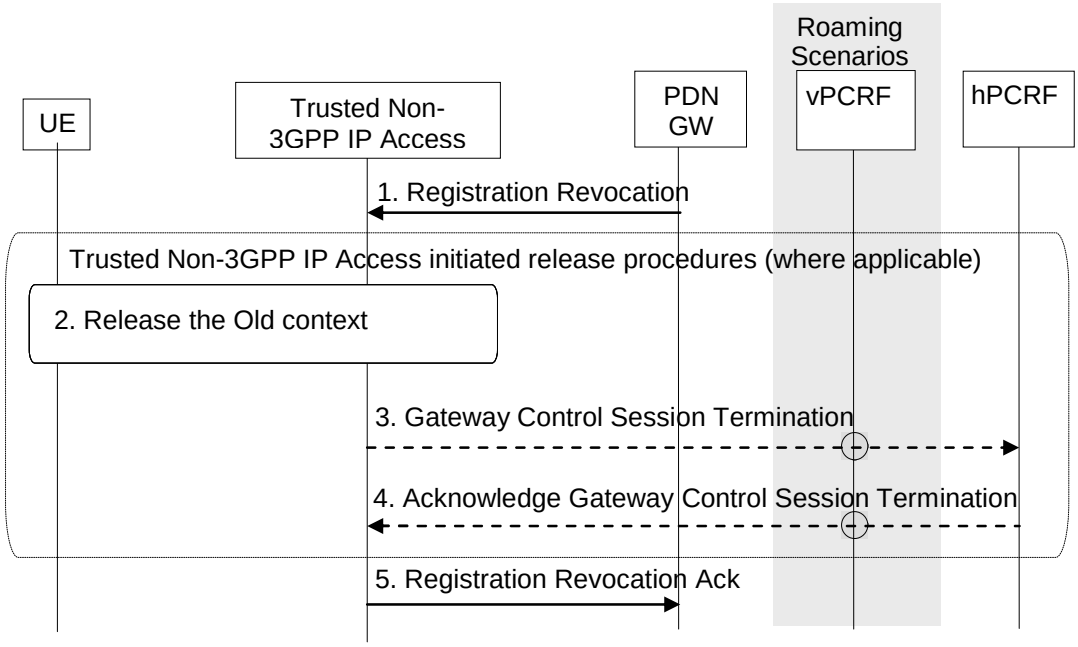


Figure 6.12.2-1 PDN GW Initiated Registration Revocation over S2a MIPv4 interface

Both the roaming (figure 4.2.1-2) and non-roaming (figure 4.2.1-1) scenarios are depicted in figure 6.12.2-1. In the roaming case, the vPCRF acts as an intermediary, sending the Gateway Control Session Termination message from the Serving GW in the VPLMN to the hPCRF in the HPLMN. The vPCRF receives the Acknowledgment from the hPCRF and forwards it to the Serving GW. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 6.12.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. If the revocation support has been negotiated, the PDN GW sends a Registration Revocation message to the trusted non-3GPP IP access as defined in RFC 3543 [25].

2. The resources may be released in the trusted non-3GPP IP access, according to an access specific, trusted non-3GPP IP access initiated, release mechanism.

3. If resources are released in trusted non-3GPP IP access, the trusted non-3GPP IP access sends Gateway Control Session Termination message to the PCRF.

4. The PCRF responds the trusted non-3GPP IP access with Acknowledge Gateway Control Session Termination message.

5. The trusted non-3GPP IP access returns a Registration Revocation Acknowledgement message to the PDN GW.

NOTE: For some accesses, the resources may be released independently of deactivation from the PDN GW.

6.12.3 PDN GW initiated Resource Allocation Deactivation for Chained PMIP-based S8-S2a Roaming

This clause defines the PDN GW initiated resource allocation deactivation for chained PMIP-based S8-S2a roaming. This procedure also applies for PMIP-based S8-S2b chaining.

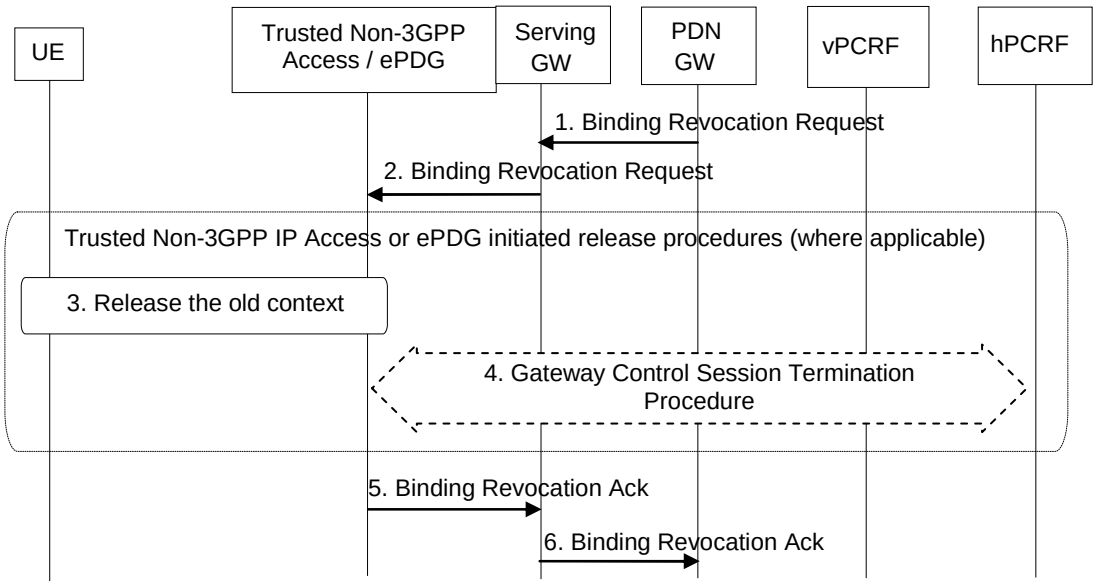


Figure 6.12.3-1: PDN GW Initiated Binding Revocation for Chained PMIP-based S8-S2a Roaming Case

The optional interaction step between the gateways and the PCRF in the procedures in figure 6.12.3-1 occur only if dynamic policy provisioning is deployed. Otherwise policies may be statically configured in the gateway.

1. The PDN GW sends a Binding Revocation Indication message to the MAG function in the Serving GW as defined in draft-muhanna-mip6-binding-revocation [35].

2. The Serving GW sends a corresponding Binding Revocation Indication message to the MAG function of the trusted non-3GPP IP access or ePDG.

3. The trusted non-3GPP IP access or ePDG may release allocated resources in the non-3GPP IP access according to access specific release mechanisms.

4. In case a Gateway Control Session between the trusted non-3GPP access or ePDG and hPCRF exists, the Gateway Control Session Termination procedure, as specified in TS 23.203 [19], is performed.

5. The MAG function of the trusted non-3GPP IP access or ePDG returns a Binding Revocation Acknowledgement message to the Serving GW.

6. The MAG function of the Serving GW or ePDG sends a corresponding Binding Revocation Acknowledgement message to the PDN GW.

NOTE: For some accesses, the resources may be released independently of deactivation from the PDN GW.

7 Functional Description and Procedures for Un-trusted Non-3GPP IP Accesses

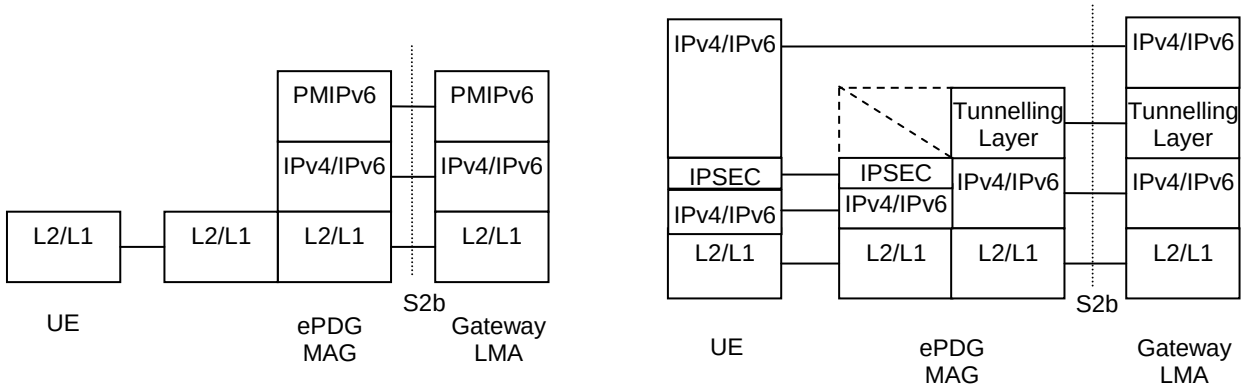
7.1 Control and User Plane Protocol Stacks

7.1.1 Protocol Options for S2b

The following protocol shall be supported on S2b:

- PMIPv6

The figure below illustrates the control plane for Mobility Management (MM) and the user plane.



Legend:

- According to terms defined in PMIPv6 (draft-ietf-netlmm-proxymip6 [8]), the functional entities terminating both the control and user planes are denoted MAG in the non-3GPP IP access and LMA in the Gateway. LMA includes also the function of a Home Agent.
- The MM control plane stack is PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network. Between the UE and the ePDG, packets are encapsulated using IPSEC RFC 3948 [48].
- The tunnelling layer implements GRE encapsulation applicable for PMIPv6 [36].

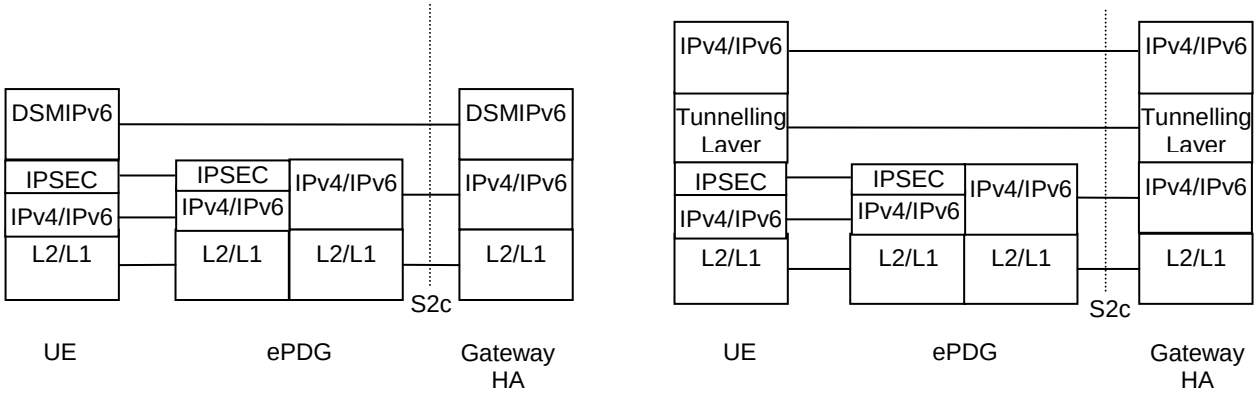
Figure 7.1.1-1: Protocols for MM control and user planes of S2b for the PMIPv6 option

7.1.2 Protocol Options for S2c over Un-trusted Non-3GPP IP Accesses

The following protocols shall be supported for S2c over un-trusted non-3GPP IP accesses:

- DSMIPv6, with IPsec and IKEv2 used to secure mobility signalling, as specified in RFC 4877 [22].

The figure below illustrates the control plane for Mobility Management (MM) and the user plane.



Legend:

- According to terms defined in DSMIPv6 [10], the functional entities terminating both the control and user planes are denoted MN (Mobile Node) in the UE, and HA (Home Agent) in the Gateway.
- The MM control plane stack is DSMIPv6 [10] over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network. Between the UE and the ePDG, packets are encapsulated using IPSEC RFC 3948 [48].
- The tunnelling layer implements IP encapsulation applicable for MIPv6 as defined in DSMIPv6 [10]. In some cases the tunnelling layer may be transparent.

Figure 6.1.2-1: Protocols for MM control and user planes of S2c for the DSMIPv6 option

7.2 Initial Attach on S2b with PMIPv6

7.2.1 Initial Attach with PMIPv6 on S2b

This section is related to the case when the UE powers-on in an untrusted network via S2b interface.

In the non-roaming case, PMIPv6 (draft-ietf-netlmm-proxymip6 [8]) is used to setup a PMIPv6 tunnel between the ePDG and the PDN GW. It is assumed that MAG is collocated with ePDG. The IPsec tunnel between the UE and the ePDG provides a virtual point-to-point link between the UE and the MAG functionality on the ePDG.

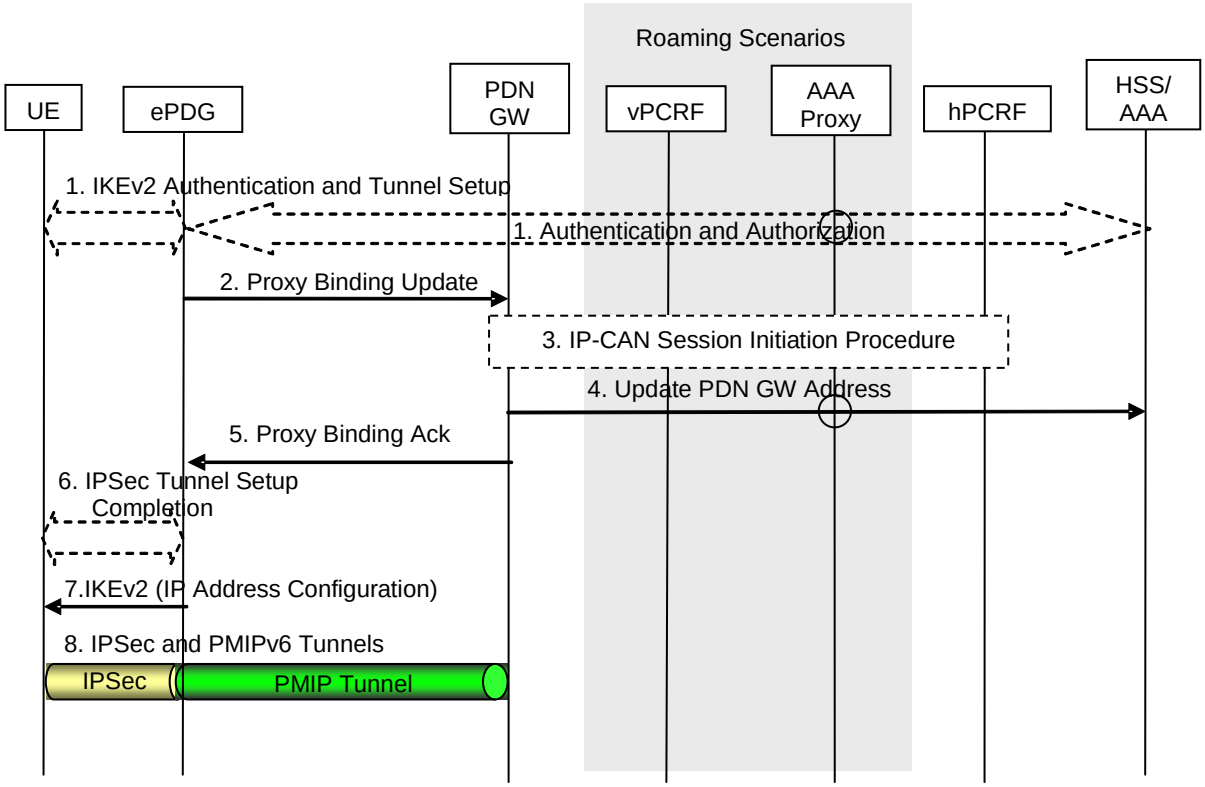


Figure 7.2.1-1: Initial attachment when Network-based MM mechanism are used over S2b for roaming, non-roaming and LBO

NOTE: Before the UE initiates the setup of an IPsec tunnel with the ePDG it configures an IP address from an untrusted non-3GPP access network. This address is used for sending all IKEv2 [9] messages and as the source address on the outer header of the IPsec tunnel.

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-5) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure.

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and visa versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.

- In the home routed roaming and non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

If dynamic policy provisioning is not deployed, the optional steps 3 and 4 do not occur. Instead, the PDN GW may employ static configured policies.

1) The IKEv2 tunnel establishment procedure is started by the UE. The UE may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The ePDG IP address to which the UE needs to form IPsec tunnel is discovered via DNS query as specified in clause 4.5.4. After the UE is authenticated, UE is also authorized for access to the APN. The procedure is as described in TS 33.234 [7]. The PDN GW address is determined at this point as described in section 4.5.1. The PDN GW information is returned as part of the reply from the 3GPP AAA Server to the ePDG. This may entail an additional name resolution step, issuing a request to a DNS Server. If supported by Non-3GPP access network, the Attach Type is indicated to the Non-3GPP access network by the UE. Attach Type indicates "Handover" when the UE has already an activated PDN GW/HA due to mobility from 3GPP access to non-3GPP accesses. If the PDN subscription profile contains a PDN GW address and the Attach Type does not indicate "Handover", the Non-3GPP ePDG may request a new PDN GW as described in clause 4.5.1, e.g. to allocate a PDN GW that allows for more efficient routeing.

2) The ePDG sends the Proxy Binding Update (MN-NAI, Lifetime, APN, Access Technology Type, Handover Indicator, GRE key for downlink traffic) message to the PDN GW. Access Technology Type option is set to a value matching the characteristics of the non-3GPP access. Handover Indicator is set to indicate attachment over a new interface. The proxy binding update message shall be secured. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value in the case of a registration and a zero value in the case of a de-

registration. The APN is used by the PDN GW to determine which PDN to establish connectivity for, in the case that the PDN GW supports multiple PDN connectivity.

3) The PDN GW initiates the IP CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19].

4) The selected PDN GW informs the 3GPP AAA Server of the PDN GW identity. The 3GPP AAA Server then informs the HSS of the PDN GW identity and APN associated with the UE's PDN Connection. This information is registered in the HSS as described in clause 12.

5) The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates an IP address for the UE. The PDN GW then sends a Proxy Binding Ack (MN NAI, UE Address Info, GRE Key for uplink traffic) message to the ePDG, including the IP address(es) allocated for the UE (identified by the MN NAI).

NOTE: If UE requests for both IPv4 and IPv6 addresses, both are allocated. If the UE requests for only IPv4 or IPv6 address only one address is allocated accordingly.

6) After the Proxy Binding Update is successful, the ePDG is authenticated by the UE.

7) The ePDG sends the final IKEv2 message with the IP address in IKEv2 Configuration payloads.

8) IP connectivity from the UE to the PDN GW is now setup. Any packet in the uplink direction is tunnelled to the ePDG by the UE using the IPSec tunnel. The ePDG then tunnels the packet to the PDN GW. From the PDN GW normal IP-based routing takes place. In the downlink direction, the packet for UE (HoA) arrives at the PDN GW. The PDN GW tunnels the packet based on the binding cache entry to the ePDG. The ePDG then tunnels the packet to the UE via proper IPsec tunnel.

7.2.2 Initial Attach Procedure with PMIPv6 on S2b and Chained S2b and GTP-based S8

This procedure is described in clause 6.2.2.

7.2.3 Initial Attach Procedure with PMIPv6 on S2b and Chained S2b and PMIP-based S8

This procedure is described in clause 6.2.4.

7.3 Initial Attach Procedure for S2c in Untrusted Non-3GPP IP Access

This section is related to the case when the UE powers-on in an untrusted network and host-based mobility management mechanism is used to establish IP connectivity and to perform inter-access Handover. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface.

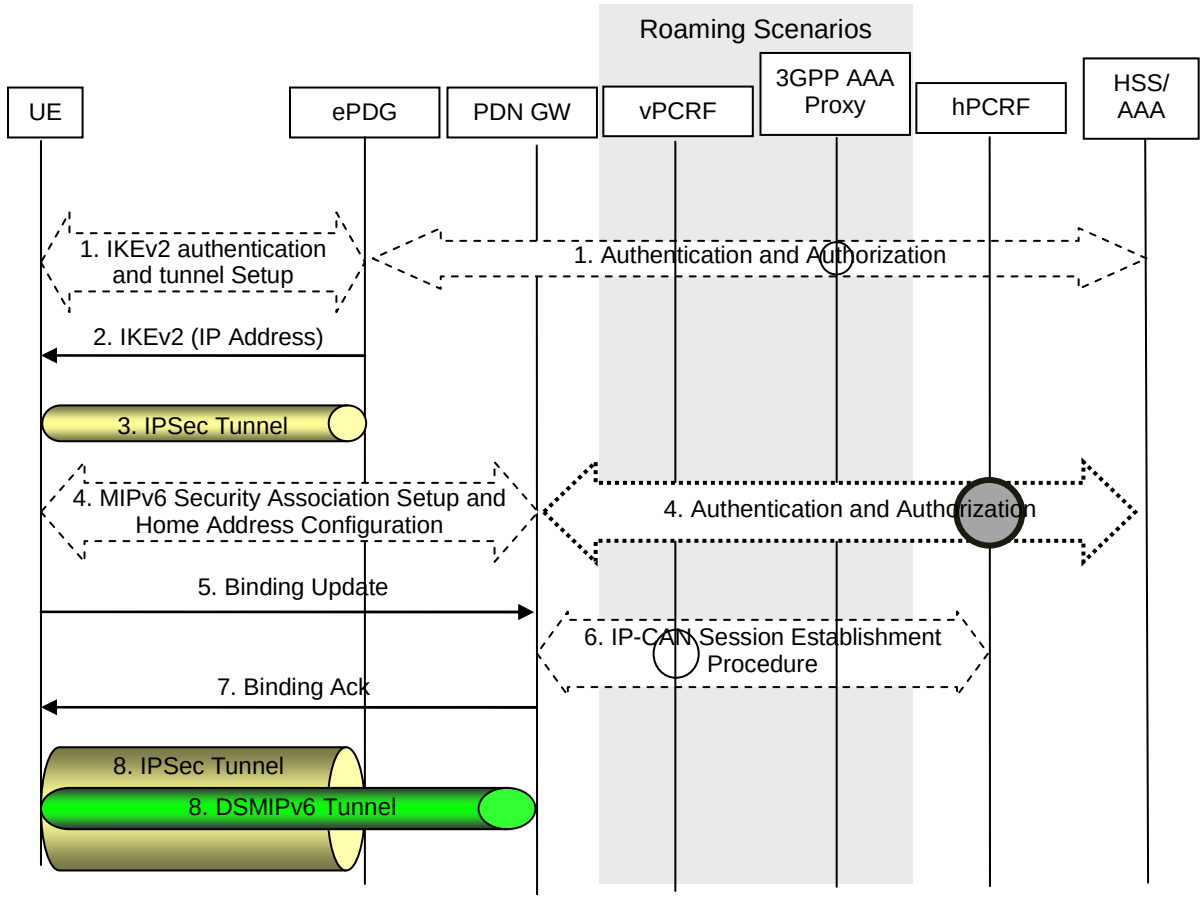


Figure 7.3-1: Initial attachment when Host-based MM mechanism are used over S2b

The non-roaming (Figure 4.2.2-2), Roaming (Figure 4.2.3-4) and LBO (Figure 4.2.3-6) are all covered in this procedure. In the Roaming and LBO case, the ePDG communicates with the 3GPP AAA Server by way of the 3GPP AAA Proxy, functioning as a relay for AAA messages. In the LBO case, the PDN GW in the VPLMN interacts with the PCRF by means of the vPCRF. In the non-roaming case, the 3GPP AAA Proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 3 and 4 do not occur. Instead, the PDN GW may employ static configured policies.

The UE is authenticated and authorised to access the Untrusted Non-3GPP Access network, After the authentication, UE is configured with Local IP Address from the access network domain. This address is used for sending all IKEv2 [9] messages and as the source address on the outer header of the IPsec tunnel.

1) The IKEv2 tunnel establishment procedure is started by the UE. The UE may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The ePDG IP address to which the UE needs to form IPsec tunnel is discovered via DNS query as specified in clause 4.5.4. After the UE is authenticated, UE is also authorized for access to the APN. The procedure is as described in TS 33.234 [7].

2) The ePDG sends the final IKEv2 message with the assigned IP address in IKEv2 Configuration payloads.

3) IPsec Tunnel between the UE and ePDG is now setup.

4) A security association is established between UE and PDN GW to secure the DS-MIPv6 messages between UE and PDN GW. This step is performed as specified in step 4 of clause 6.3

5) The UE sends the Binding Update (IP Addresses (HoA, CoA)) message to the PDN GW. The Binding Update is as specified in draft-ietf-mip6-nemo-v4traversal [10].

6) The PDN GW executes a IP-CAN Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. The message from the PDG GW includes at least the HoA and the CoA. The message may also include a permanent UE identity and an APN string.

The PCRF decides on the PCC rules and Event Triggers and provisions them to the PDN GW. The PDN GW installs the received PCC rules.

7) The PDN GW processes the binding update and creates a binding cache entry for the UE. The PDN GW allocates an IP address for the UE. The PDN GW then sends a Binding Ack to the UE, including the IP address allocated for the UE.

NOTE: If UE requested for both IPv4 and IPv6 addresses, both IPv4 and IPv6 addresses are allocated. In the case only IP address of either IPv4 or IPv6 is requested, then IP address of only the requested IP version is allocated.

8) The IP Connectivity is now setup.

7.4 Detach for S2b

7.4.1 UE/ePDG-initiated Detach Procedure with PMIP

7.4.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

UE/ePDG-initiated detach procedure with PMIPv6 is illustrated in Figure 7.4.1-1. The UE can initiate this procedure, e.g. when the UE is power off. The ePDG can initiate this procedure due to administration reason or the IKEv2 tunnel releasing.

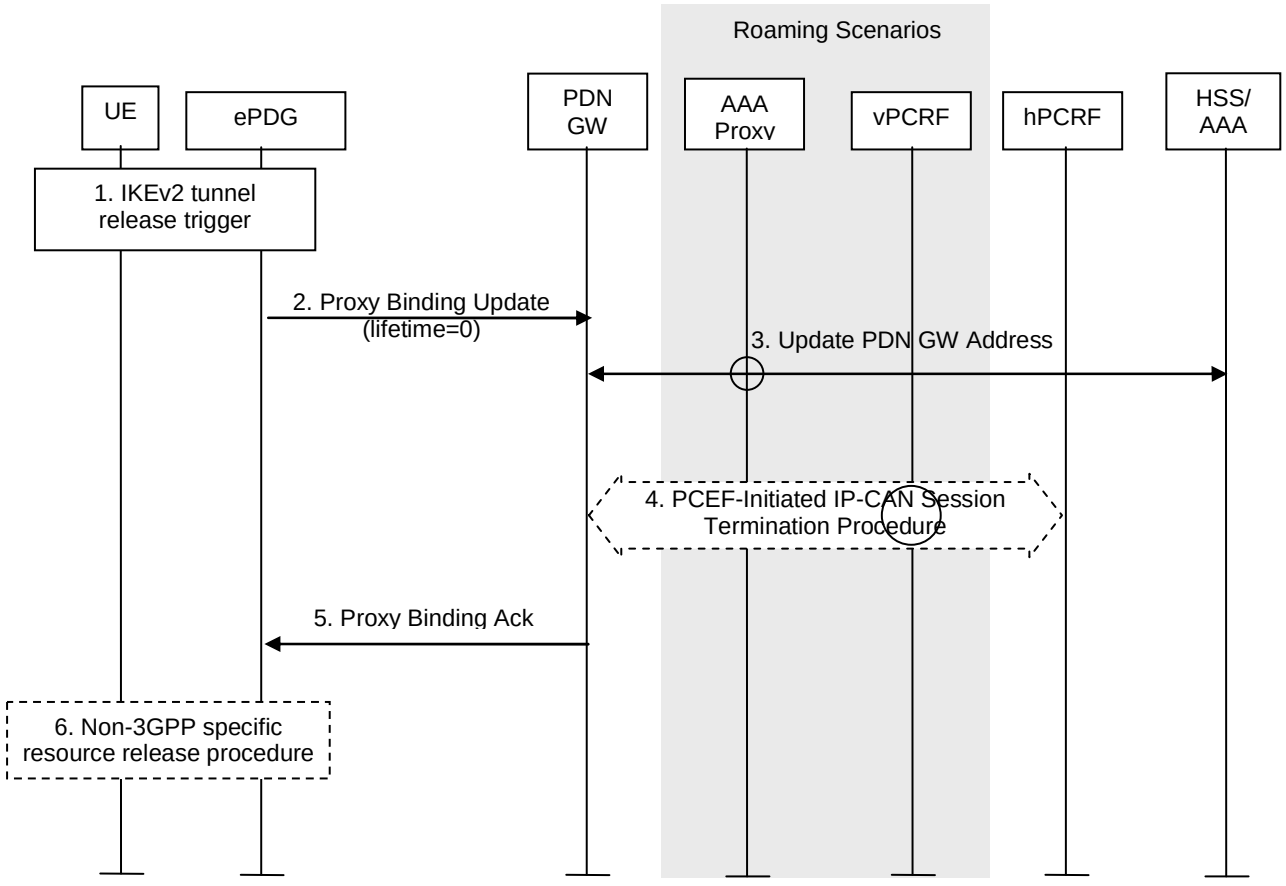


Figure 7.4.1-1: UE/ePDG-initiated detach procedure with PMIPv6

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-5) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure. In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and visa versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN. In the non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

If dynamic policy provisioning is not deployed, the optional steps 4 and 5 do not occur. Instead, the PDN GW may employ static configured policies.

1) IKEv2 tunnel release triggers PMIP tunnel release.

2) The MAG in the ePDG sends a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the PDN GW. The MN NAI identifies the UE. The APN disambiguates the IP CAN session in the case where the same PDN GW is used for multiple PDN access. The lifetime value set to zero, indicates this is a PMIP de-registration.

3) The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information and APN associated with the UE's PDN Connection. This information is registered in the HSS as described in clause 12.

4) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5) The PDN GW deletes all existing entries for the indicated HoA from its Binding Cache and sends a Proxy Binding Ack (MN NAI, lifetime=0) message to the MAG in the ePDG. The PDN GW sends a Proxy Binding Ack message to the ePDG. The MN NAI value and the lifetime=0 values indicate that the UE has been successfully deregistered.

6) Non-3GPP specific resource release procedure is executed.

7.4.1.2 Chained PMIP-based S8-S2b Roaming Case

This procedure is described in clause 6.4.1.2.

7.4.2 HSS/AAA-initiated Detach Procedure with PMIP

7.4.2.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

HSS/AAA-initiated detach procedure with PMIPv6 for non-roaming case is illustrated in Figure 7.4.2-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

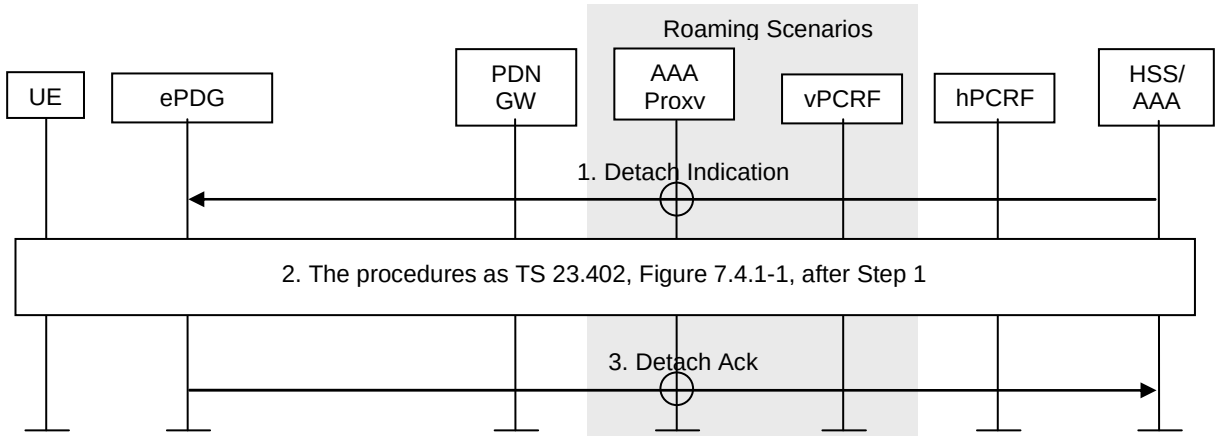


Figure 7.4.2-1: HSS/AAA-initiated detach procedure with PMIPv6

NOTE: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-5).

1) The HSS/AAA sends a detach indication message to the ePDG to detach a specific UE.

2) This include the procedure after step1 as Figure 7.4.1-1.

3) The ePDG sends a Detach Ack message to the HSS.

7.4.2.2 Chained PMIP-based S8-S2b Roaming Case

This procedure is described in clause 6.4.2.2.

7.5 Detach for S2c in Un-trusted Non-3GPP IP Access

7.5.1 General

This section is related to the case when a DSMIPv6 detach procedure is performed. The Detach procedure is on a per PDN basis and allows:

- the UE to inform the network that it does not want to use S2c any longer; and
- the network to inform the UE that it does not have access to the EPS through S2c any longer.

The UE is detached either explicitly or implicitly:

- **Explicit detach:** The network or the UE explicitly requests detach and signal with each other;
- **Implicit detach:** The network detaches the UE, without notifying the UE. This is typically the case when the network presumes that it is not able to communicate with the UE, e.g. due to radio conditions.

7.5.2 UE-Initiated Detach Procedure

The Detach procedure when initiated by the UE is illustrated in Figure 7.5.2-1. The Detach procedure defined in this section must be repeated for each PDN.

In the non-roaming case, none of the optional entities in Figure 7.5.2-1 are involved. The optional entities are involved in other cases. In the roaming cases, however, the 3GPP AAA Proxy relays all interaction between the 3GPP AAA Server in the HPLMN and the PDN GW in the VPLMN.

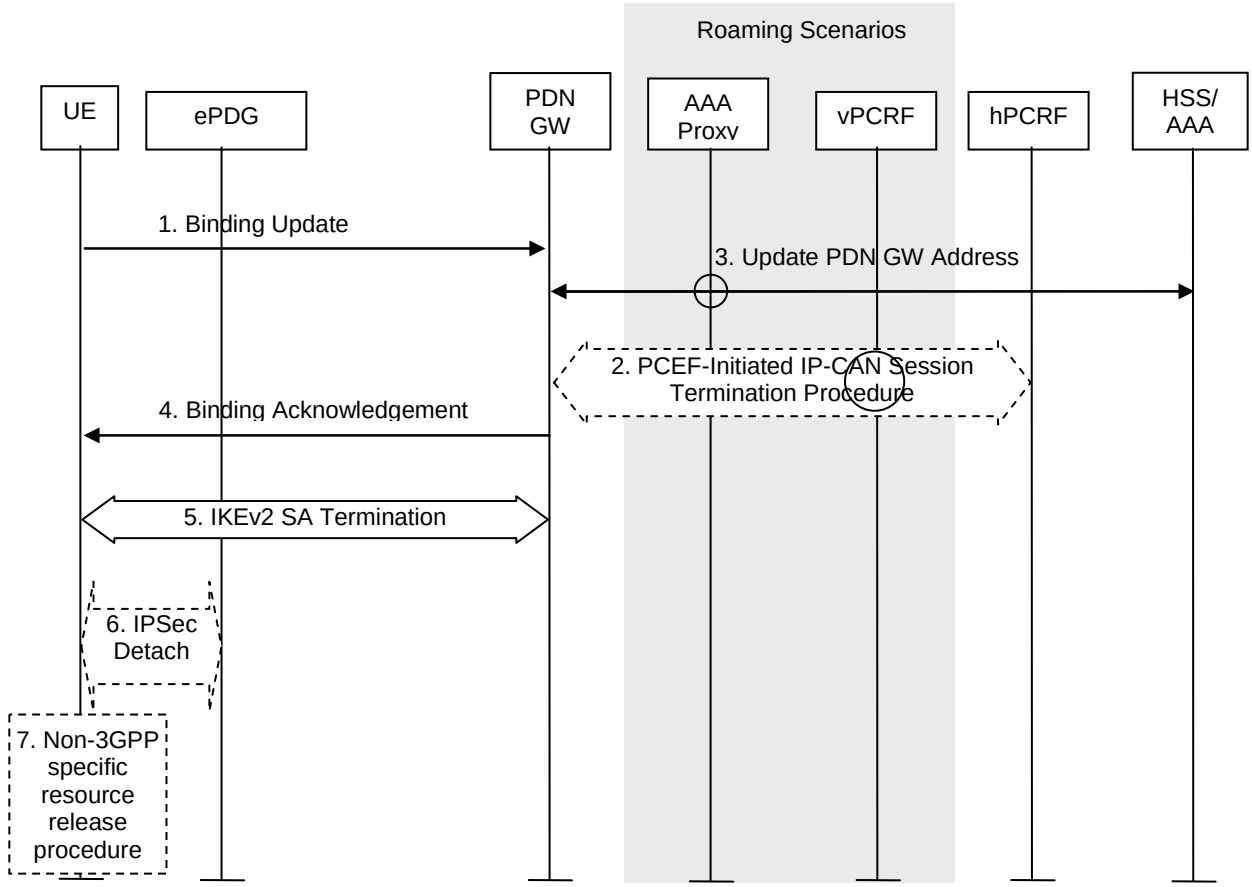


Figure 7.5.2-1: UE-initiated S2c detach procedure in Untrusted Non-3GPP Access Network

Non-roaming (figure 4.2.2-2), home routed roaming (figure 4.2.3-4) and Local Breakout (figure 4.2.3-5) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 2 and 5 do not occur. Instead, the PDN GW may employ static configured policies.

1. If the UE wants to terminate a S2c session, it shall send a de-registration Binding Update (Lifetime=0, IP Addresses (HoA, Lifetime=0) message to the PDN GW as specified in draft-ietf-mip6-nemo-v4traversal [10].

2. The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information and the APN associated with the UE's PDN Connection. This information is registered in the HSS as described in clause 12. This information is de-registered from the HSS as described in clause 12.

3. If there is an active PCC session for the UE, the PDN GW xecutes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

4. The PDN GW shall send a Binding Acknowledgement to the UE as specified in draft-ietf-mip6-nemo-v4traversal [10].

5. The UE terminates the IKEv2 security association for the given PDN as defined in RFC 4306 [9].

6. If after step 5 the UE has no other PDN sessions, the UE should terminate the IPSEC tunnel to the ePDG according to RFC 4306 [9].

7. After IPsec tunnel termination, non-3GPP specific resource release procedure may be executed.

7.5.3 HSS-initiated Detach Procedure

The Detach procedure when initiated by the HSS/AAA is illustrated in Figure 7.5.3-1. The Detach procedure defined in this section must be repeated for each PDN.

In the implicit detach, steps 2, 3 and 6 of Figure 7.5.3-1, are omitted.

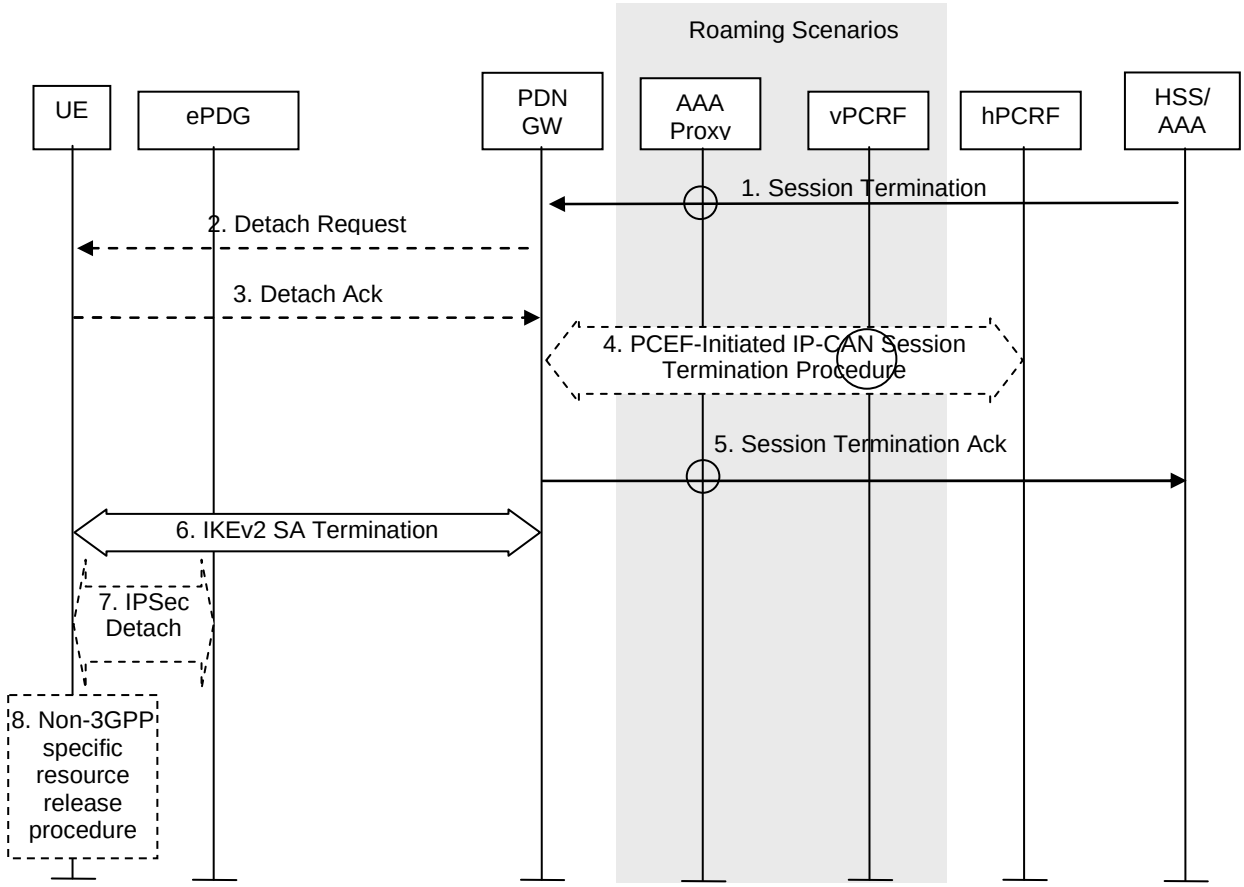


Figure 7.5.3-1: AAA/HSS-initiated S2c detach procedure in Untrusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-2), home routed roaming (figure 4.2.3-4) and Local Breakout (figure 4.2.3-5) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 4a and 4b do not occur. Instead, the PDN GW may employ static configured policies.

1. If the HSS/AAA wants to request the immediate termination of a S2c session for a given UE and a given PDN, it shall send a Session Termination message to the PDN GW.

2. In the explicit detach procedure the PDN GW sends a detach request message as specified. In the implicit detach procedure this step is omitted.

3. In the explicit detach procedure, the UE shall acknowledge the detach request. In the implicit detach procedure this step is omitted.

NOTE: Whether messages 2 and 3 are needed and if they are needed how the detach request and acknowledge messages are implemented is a stage 3 issue.

4. If there is an active PCC session for the UE, the PDN GW executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5. The PDN GW shall acknowledge the termination of the S2c session to the 3GPP AAA Server/HSS. As part of this interaction with the 3GPP AAA Server/HSS, the PDN GW indicates that the AAA Server should remove the PDN GW address and APN associated with the the UE's PDN Connection. As this is an HSS-initiated procedure, the mechanism described in clause 12.1.2 is not necessary.

6. In the explicit detach the PDN GW or the UE terminates the IKEv2 security association for the given PDN as defined in RFC 4306 [9]. In the implicit detach procedure this step is omitted.

7. If after step 6 the UE has no other PDN sessions, the UE should terminate the IPSEC tunnel to the ePDG according to RFC 4306 [9].

8. After IPsec tunnel termination, non-3GPP specific resource release procedure may be executed.

7.6 UE-initiated Connectivity to Additional PDN

7.6.1 UE-initiated Connectivity to Additional PDN with PMIPv6 on S2b

NOTE: The PDN GW treats each MN-ID+APN as a separate binding and may allocate a new IP address/prefix for each binding.

Editor's Note: It is FFS if and how multiple PDN connections to one APN from a single UE is supported, i.e. whether the MN-ID + APN is sufficient to uniquely identify a PDN connection instance, or whether additional parameter(s) are needed.

7.6.2 UE-initiated Connectivity to Additional PDN from Un-trusted Non-3GPP IP Access with DSMIPv6 on S2c

This section is related to the case when the UE powers-on in an untrusted network and host-based mobility management mechanism is used for obtaining connectivity. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface. This case covers the scenario when UE obtains connectivity with one or more additional PDNs at any time after initial attach Since host-based mobility mechanisms are used, the procedure is similar to the initial attach procedure.

NOTE: Based on the MN-ID and APN, the PDN GW may allocate a new IP address/prefix for a new binding.

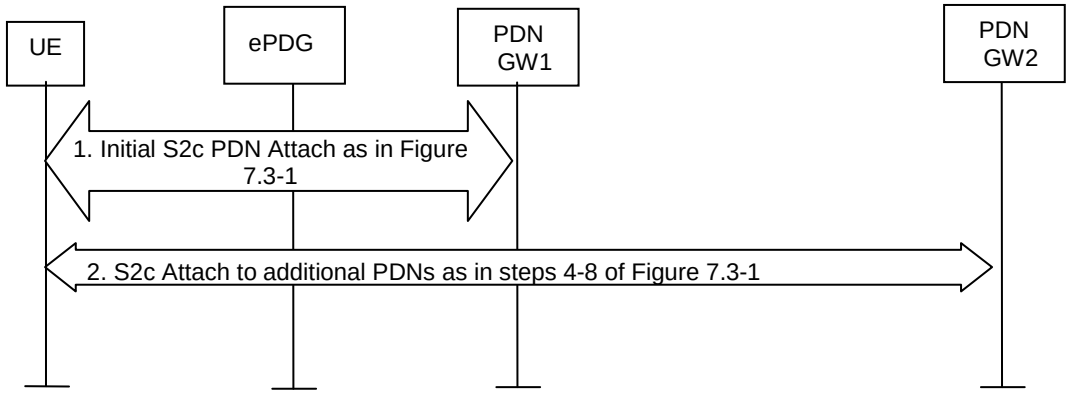


Figure 7.6.2-1: UE-initiated connectivity to additional PDN from Un-trusted Non-3GPP IP Access with DSMIPv6

When the initial attachment is performed, the UE performs procedures described in clause 7.3, Figure 7.3-1, to obtain connectivity with a PDN GW and a specific PDN. If at any time the UE wants to obtain connectivity with additional PDNs, it repeats steps 4-8 of Figure 7.3-1.

1) The UE performs initial S2c PDN Attach procedure as defined in clause 7.3, Figure 7.3-1.

2) The UE repeats steps 4-8 of clause 7.3, Figure 7.3-1 for each additional PDN the UE wants to connect to. This step can be performed and repeated at any time after step 1 for one or multiple PDNs.

7.7 ME Identity Check Procedures for Un-trusted Non-3GPP IP Accesses

< This subclause will contain details on ME identity checking (e.g. IMEI checking)>

7.8 S2c Bootstrapping via DSMIPv6 Home Link over an Un-Trusted Access

When the UE is connected on an un-trusted non-3GPP access considered to be DSMIPv6 home link for the UE, the UE may trigger the establishment of S2c IKEv2 SA, e.g. to optimize future handovers to other accesses using S2c. For each PDN connection, the S2c IKEv2 SA establishment has to be performed separately.

NOTE: An un-trusted non-3GPP access can be defined as DSMIPv6 Home Link in addition to the 3GPP access.

Once the UE is attached to the PDN over the un-trusted non-3GPP access, the procedure describing the bootstrapping is in clause 15.1.

7.9 PDN GW initiated Resource Allocation Deactivation

The PDN GW initiated resource allocation deactivation procedure as defined in clause 6.12.1 should also apply to S2b PMIP reference point.

8 Handovers without Optimizations Between 3GPP Accesses and Non-3GPP IP Accesses

8.1 Common Aspects for Handover without Optimizations for Multiple PDNs

This section describes the common aspects of handover for connectivity with multiple PDNs.

The support of multiple PDNs has the following impacts on the handover procedures for single PDN connectivity:

- Upon handover from 3GPP access to non-3GPP access, and from non-3GPP access to another non-3GPP access, using S2a or S2b, during the access authentication the HSS/AAA returns to the Trusted Non-3GPP Access or the ePDG the IP address of the PDN GW and associated APN for each PDN the UE is connected to. For non-3GPP accesses that support UE to establish connectivity to PDNs after attach, the UE performs an attach to the target non-3GPP access indicating that it is a handover, resulting in the UE being connected to one PDN and the UE establishes connectivity with the remainder PDNs it was connected to in the 3GPP system before the handover, using UE-initiated Connectivity to Additional PDN.

  For non-3GPP accesses that support re-connecting the UE to multiple PDNsit, when the UE connects to the non-3GPP access, the non-3GPP access may reconnect the UE to all the PDNs indicated by the PDN GW information provided by the HSS/AAA during authentication.

NOTE: The PDN GW information in the HSS/AAA may not correspond to the PDNs that the UE is connected to before the handover.

- Upon handover from non-3GPP access to 3GPP access, if the MME has changed since the last detach or if there is no valid Subscriber context for the UE in the MME, or if the ME identity has changed, during the access authentication the HSS returns the Subscriber Data to the MME, including the IP address of the PDN GW and associated APN for each PDN the UE is connected to before the handover. The UE performs an attach to the 3GPP access with and indication for "handover" and then establishes connectivity with the remainder of PDNs that it was connected with over the non-3GPP system before the handover, using UE requested PDN connectivity specified in TS 23.401 [4]. The UE provides an indication of "handover" by providing Attach Type indicating "handover" in the PDN connectivity request message as specified in TS 23.401 [4].

- For connectivity based on S2c:

  - Upon handover from 3GPP access to non-3GPP access, and from non-3GPP access to another non-3GPP access, the UE will perform DSMIPv6 bootstrapping (if needed) and binding procedures with each PDN GW.

  - Upon handover from non-3GPP access, the UE will de-register DSMIPv6 from each PDN GW.

Editor's Note: It is FFS whether a single hPCRF for all PDNs or a hPCRF for each PDN should be considered. Similarly, it is FFS whether a single vPCRF or multiple vPCRFs should be considered.

8.2 Handovers between non-3GPP IP access and 3GPP Access on S2a or S2b

8.2.1 Handover from Trusted or Untrusted Non-3GPP IP Access to 3GPP Access on S2a/S2b

8.2.1.1 General Procedure for GTP based S5/S8 for E-UTRAN Access

The steps involved in the handover from a trusted or untrusted non-3GPP IP access to E-UTRAN connected to EPC are depicted below for both the non-roaming and roaming cases and when PMIPv6 is used on S2a or S2b or MIPv4 FACoA is used on S2a. It is assumed that while the UE is served by the trusted or untrusted non-3GPP IP access, a PMIPv6 tunnel or MIPv4 tunnel is established between the non-3GPP access network and the PDN GW in the EPC.

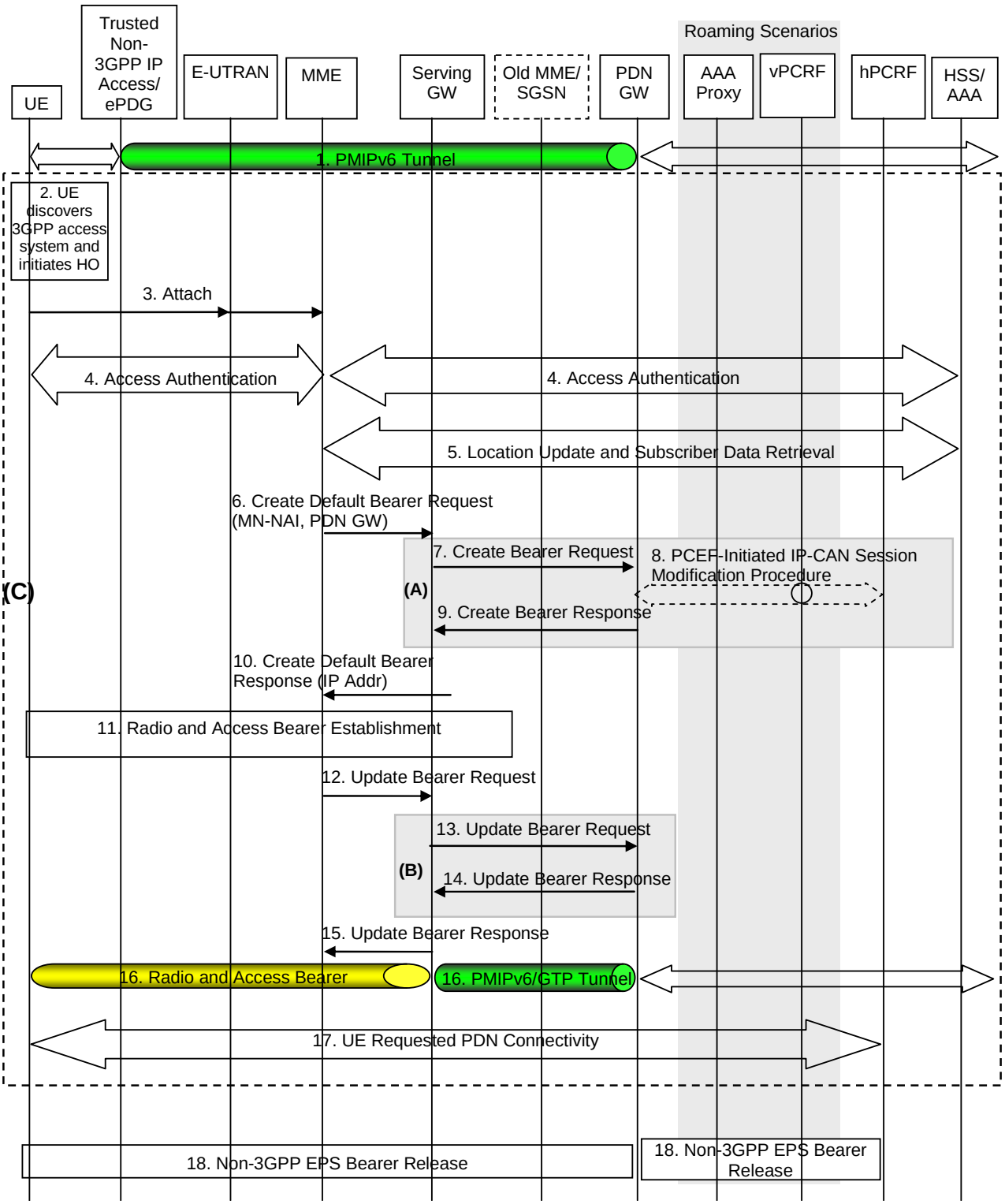


Figure 8.2.1.1-1: Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN with PMIP on S2a or S2b or MIPv4 on S2a and GTP on S5/S8 interfaces

NOTE 1: All steps outside of (A) and (B) are common for architecture variants with GTP-based S5/S8 and PMIP-based S5/S8. Procedure steps (A) and (B) for PMIP-based S5/S8 are described in Section 8.2.1.2.

NOTE 2: The flow here assumes that this is an initial attach of the UE and no bearers for the UE exists in E-UTRAN.

NOTE 3: In case of connectivity to multiple PDNs, the steps in 17 are repeated for each PDN the UE is connected to. The steps in 17 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The steps involved in the handover are discussed below.

1) The UE uses a trusted or untrusted non-3GPP access system and is being served by PDN GW (as PMIPv6 LMA or MIPv4 HA).

2) The UE discovers the E-UTRAN access and determines to transfer its current sessions (i.e. handover) from the currently used non-3GPP access system to E-UTRAN. The mechanisms that aid the UE to discover the 3GPP Access system, are specified in Section 4.8 (Network Discovery and Selection).

3) The UE sends an Attach Request to the MME with Attach Type indicating "Handover" Attach. The message from the UE is routed by E-UTRAN to the MME as specified in TS 23.401 (E-UTRAN).

4) The MME contacts the HSS and authenticates the UE. The MME receives information on the PDNs the UE is connected to over the non-3GPP access in the Subscriber Data obtained from the HSS.

5) After successful authentication, the MME performs location update procedure and subscriber data retrieval from the HSS as specified in TS 23.401. Since the Attach Type is "Handover" Attach, the PDN GW address conveyed to the MME will be stored in PDN subscription context.

6) For connectivity to multiple PDNs, even if the UE had disconnected from the Default PDN before the handover, the MME selects a serving GW as described in TS 23.401 and sends a Create Default Bearer Request (including IMSI, MME Context ID (SGSN equivalent is TBD), PDN-GW address, Handover Indication) message to the selected Serving GW. Since the Attach Type is "Handover" Attach, a Handover Indication information is included.

7) The Serving GW sends a Create Default Bearer Request (Handover Indication) message to the PDN-GW in the VPLMN or HPLMN as described in TS 23.401. Since the MME includes Handover Indication information in Create Default Bearer Request message, the Serving GW includes this information in Create Default Bearer Request message.

   Since Handover Indication is included, the PDN GW should not switch the tunnel from non-3GPP IP access to 3GPP access system at this point.

8) Since Handover Indication is included, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW in the VPLMN or HPLMN to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

   If the updated PCC rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step 12. The establishment of dedicated bearers in combination with the default takes place as described in Annex F of TS 23.401 [4].

NOTE: PDN GW address and Serving GW address selection is as described in the clause "GW selection" in TS 23.401 [4].

9) The PDN GW responds with a Create Default Bearer Response message to the Serving GW as described in TS 23.401.The Create Default Bearer Response contains the IP address or the prefix that was assigned to the UE while it was connected to the non-3GPP IP access.

10) The Serving GW returns a Create Default Bearer Response message to the MME as specified in TS 23.401 [4]. This message also includes the IP address of the UE. This message also serves as an indication to the MME that the S5 bearer setup and update has been successful. At this step the PMIPv6 or GTP tunnel(s) over S5 are established.

11) Radio and Access bearers are established at this step in the 3GPP access as specified in TS 23.401 [4].

12) The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID, Handover Indication) message to the Serving GW.

13) Since the Handover Indication is included in step 12), the Serving GW sends an Update Bearer Request message to the PDN GW to prompt the PDN GW to tunnel packets from non 3GPP IP access to 3GPP access system and immediately start routing packets to the Serving GW for the default and any dedicated EPS bearers established.

14) The PDN GW acknowledges by sending Update Bearer Response to the Serving GW.

15) The Serving GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.

16) The UE sends and receives data at this point via the E-UTRAN system.

17) For connectivity to multiple PDNs, the UE establishes connectivity to each PDN, the UE was connected to before the handover, besides the Default PDN, by executing the UE requested PDN connectivity procedure specified in TS 23.401 [4].

18) The PDN GW shall initiate resource allocation deactivation procedure in the trusted/untrusted non-3GPP IP access as defined in clause 6.12 or clause 7.9.

8.2.1.2 Using PMIP-based S5/S8

When a Trusted or Untrusted Non-3GPP IP Access to 3GPP Access handover occurs, the following steps are performed instead of and in addition to the steps performed in the GTP-based S5/S8 case (see previous section). In the case of PMIP-based S5/S8, a Create Bearer Request and Update Bearer Request is not sent from the Serving GW to the PDN GW. Rather, the serving GW interacts with the hPCRF and PMIP messages are exchanged between the Serving GW and the PDN GW.

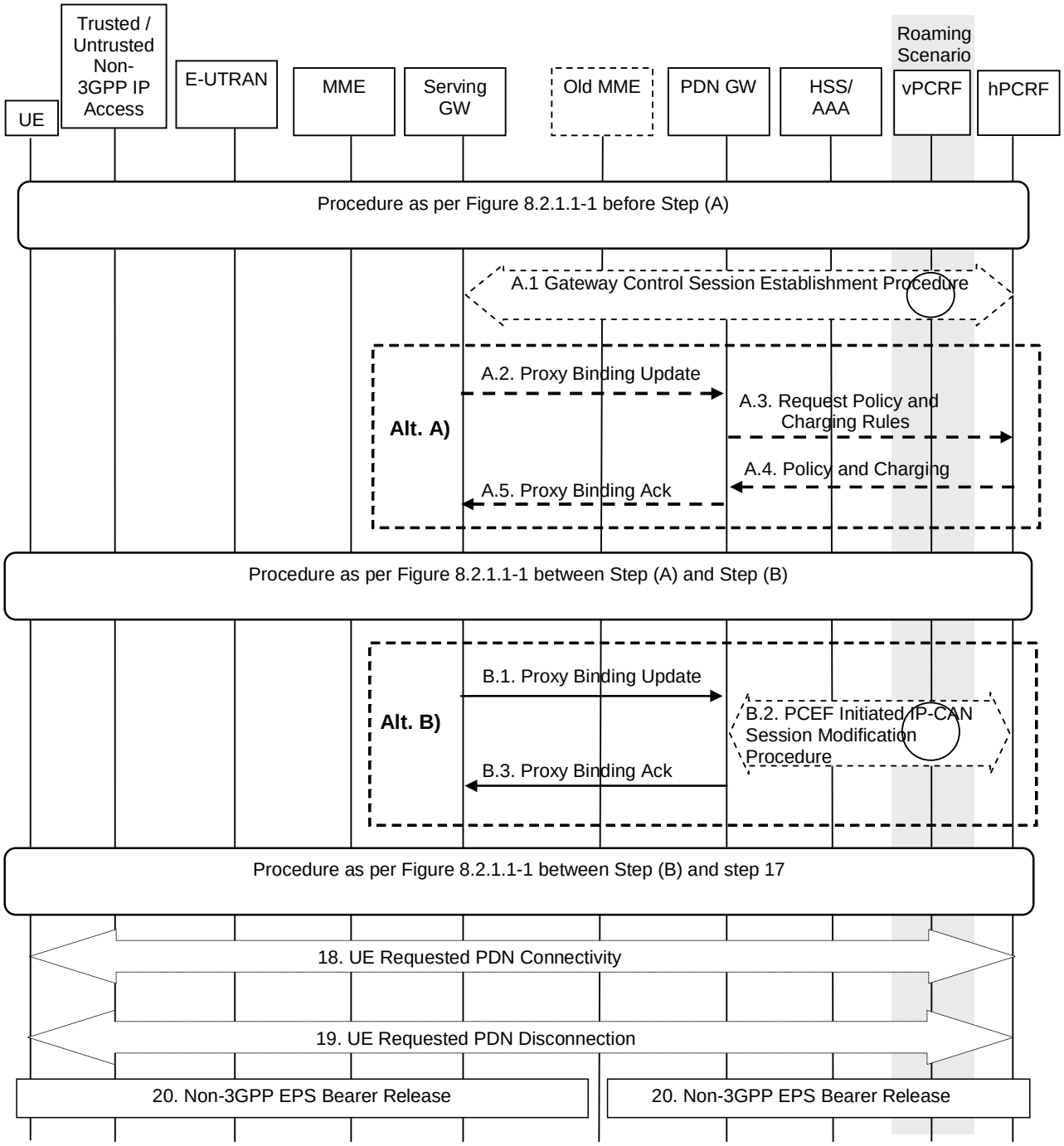


Figure 8.2.1.2-1: Trusted/Untrusted Non-3GPP IP Access to E-UTRAN Handover over PMIP-based S2a and using PMIP-based S5/S8

This procedure supports the home routed (Figure 4.2.2.1), roaming (Figure 4.2.3-1) and Local breakout (Figure 4.2.3-5) case. The Serving GW establishes a Gateway Control Session with the PCRF in the HPLMN. In the case of the roaming or local breakout scenario, the Serving GW interacts with the hPCRF by way of the vPCRF. The signalling takes place through the vPCRF in the VPLMN. In the case of Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF. The vPCRF then exchanges messages with the hPCRF in the HPLMN.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.1.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The steps shown in (Alt A) and (Alt B) are mutually exclusive in this procedure, i.e. either steps A.2-A.5 are executed or steps B.1-B.3. In order to execute the alternative (Alt B), the IP Address(es) of the UE needs to be available after step A.1. The IP Address(es) of the UE is received in step A.1, if dynamic policy provisioning is deployed.

In case the IP address(es) of the UE is available after step A1, (Alt B) provides lower jitter for dual radio handovers. In case the IP address(es) of the UE is not available after step A1, (Alt A) shall be used.

NOTE 1: In case of connectivity to multiple PDNs, steps A and B are repeated for each PDN the UE is connected to. Other impacts related to the handover for multiple PDNs are described in Section 8.1.

A.1) The Serving GW initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the Serving GW to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure.

If the updated QoS rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step B1. The establishment of dedicated bearers in combination with the default takes place as described in Annex F of TS 23.401 [4].

A.2) The same description as in B.1 applies

A.3-A.4) The same description as in B.2 applies

A.5) The same description as in B.3 applies. Since this step is triggered by the Proxy Binding Update message from the Serving GW in step A.2, it can occur after step A.2 and does not need to wait for steps A.3 and A.4.

NOTE 2: PDN GW address selection is as described in TS 23.401 [4].

Steps between A and B.1 are described in Section 8.2.1.1.

B.1) The Serving GW sends a PMIPv6 Proxy Binding Update (MN NAI, Lifetime, Access Technology Type, Handover Indicator, IP Address Requested, APN, GRE Key for downlink traffic, *Additional Parameters*) message to the PDN GW. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value in the case of a registration. Access Technology Type is set to indicate RAT type (E-UTRAN). The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The optional Additional Parameters may contain information, for example, protocol configuration options.

B.2) The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW to function as the PCEF for all the active IP sessions the UE has established with new IP-CAN type.

B.3) The PDN GW responds with a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE address info returns the IP Address assigned to the UE. The optional Additional Parameter information element may contain other information, including for example Protocol Configuration Options. The Serving GW acts as the MAG (in terms of PMIPv6). Since this step is triggered by the Proxy Binding Update message from the Serving GW in step B.1, it can occur after step B.1 and does not need to wait for step B.2.

8.2.1.3 General Procedure for GTP-based S5/S8 for UTRAN/GERAN

The steps involved in the handover from a trusted non-3GPP IP access to UTRAN/GERAN connected to EPC are depicted below for both the non-roaming and roaming cases and when PMIPv6 is used on S2a. It is assumed that while the UE is served by the trusted non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the PDN GW in the EPC.

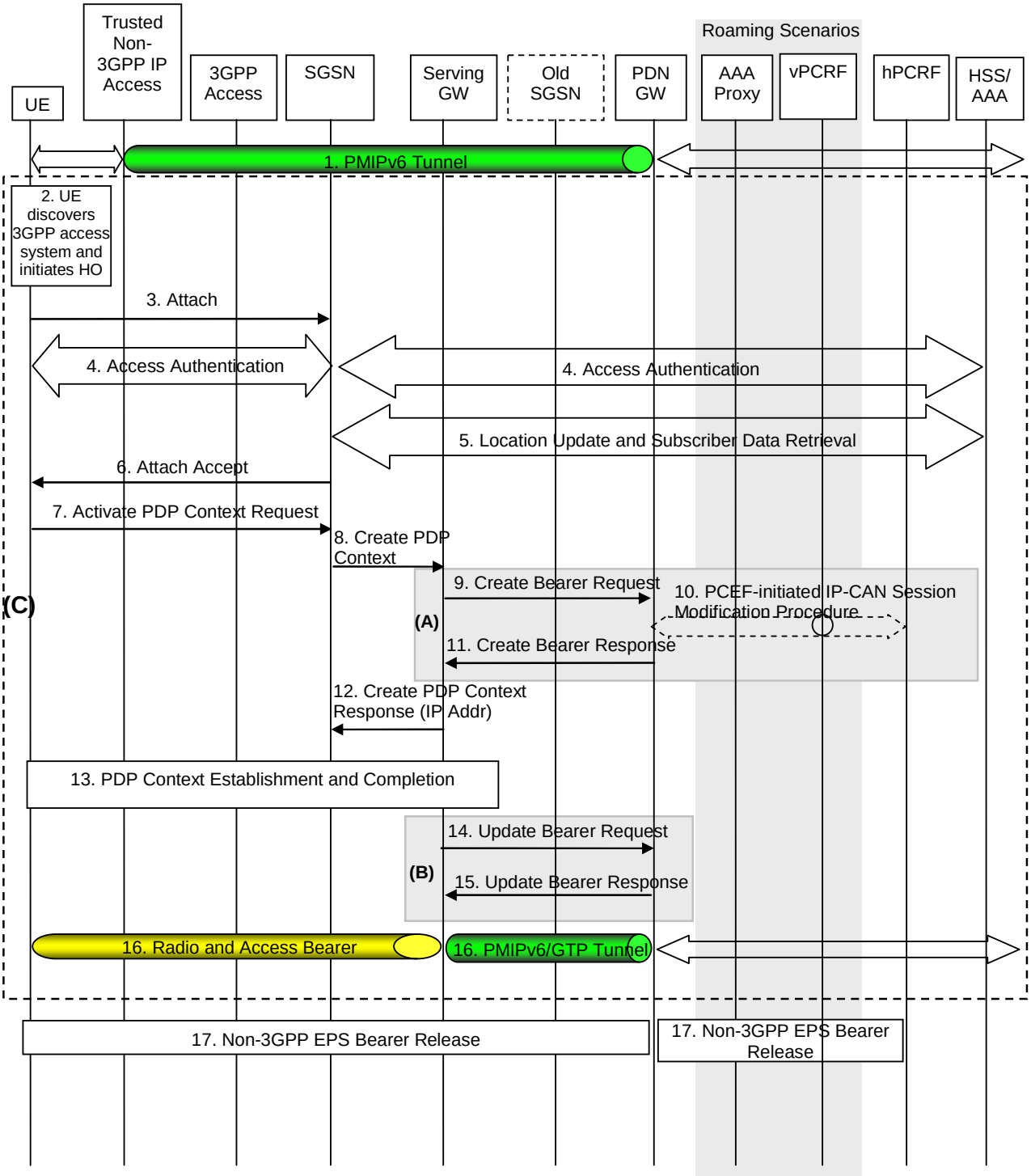


Figure 8.2.1.3-1: Handover from Trusted Non-3GPP IP Access to UTRAN/GERAN with PMIP on S2a and GTP or PMIP-based S5/S8

NOTE 1: All steps outside of (A) and (B) are common for architecture variants with GTP based S5/S8 and PMIP based S5/S8. Procedure steps (A) and (B) for PMIP based S5/S8 are described in clause 8.2.1.2.

NOTE 2: The flow here assumes that this is an initial attach of the UE and no bearers for the UE exists in UTRAN/GERAN.

NOTE 3: Steps in (C) are repeated for each PDN the UE is connected to before handover in case of connectivity to multiple PDNs. The steps in (C) can occur in parallel for each PDN.

The steps involved in the handover are described below.

1. The UE uses a trusted non-3GPP access system and is being served by PDN GW (as PMIPv6 LMA).

2. The UE discovers the 3GPP Access system (UTRAN or GERAN) and determines to transfer its current sessions (i.e. handover) from the currently used non-3GPP access system to the discovered 3GPP Access system. The mechanisms that aid the UE to discover the 3GPP Access system, are specified in Section 4.8 (Network Discovery and Selection).

3. The UE sends an Attach Request to the SGSN. The message from the UE is routed by 3GPP Access to the SGSN as specified in TS 23.060 [21].

4. The SGSN contacts the HSS and authenticates the UE. As part of the authentication procedure, the IP address of the PDN GW that needs to be used is conveyed to the SGSN. It is FFS whether this is going to be described in TS 23.401 [4] or TS 23.060 [21].

5. After successful authentication, the SGSN performs location update procedure and subscriber data retrieval from the HSS as specified in TS 23.060 [21].

6. The SGSN sends the Attach Accept request to the UE to indicate the completion of the attach procedure as defined in TS 23.060 [21].

7. The UE initiate at this stage this establishment of the primary PDP context as defined in TS 23.060 [21].

Editor's Note: Steps 3-7 need to be updated with references to specific sections of TS 23.060 [21] when the structure of TS 23.060 [21] Rel.8 is defined.

8. The SGSN selects a Serving GW as described in TS 23.401 [4] and sends Create PDP Context Request (Information Contained FFS) message to the selected Serving GW.

9. The Serving GW sends a Create Bearer Request message to the PDN-GW as described in TS 23.401 [4]. The PDN GW should not switch the tunnel from non-3GPP IP access to 3GPP access system at this point.

10. The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

    If the updated PCC rules require establishment of dedicated EPS bearers for the UE, the establishment of those bearers take place before step 12. The Dedicated bearer shall be mapped to Secondary PDP contexts by the Serving Gateway. The default and dedicated bearers are synchronised as described in Annex F of TS 23.401 [4].

Editor's Note: It is FFS how the establishment of the default and dedicated bearers is synchronized.

NOTE: PDN GW address and Serving GW address selection is as described in the clause "GW selection" in TS 23.401 [4].

11. The PDN GW responds with a Create Bearer Response message to the Serving GW as described in TS 23.401 [4].The Create Bearer Response contains the IP address or the prefix that was assigned to the UE while it was connected to the non-3GPP IP access.

12. The Serving GW returns a Create PDP Context Response message to the SGSN as specified in TS 23.060 [21]. This message also includes the IP address of the UE. This message also serves as an indication to the SGSN that the S5 bearer setup and update has been successful. At this point the Serving Gateway will also initiate the establishment of network-initiated secondary PDP contexts as defined in TS 23.060 [21].

13. The rest of the PDP context establishment as specified in TS 23.060 [21] is completed here.

14. The Serving GW sends an Update Bearer Request message to the PDN GW in the VPLMN or the HPLMN including the RAN procedures ready flag that prompts the PDN GW to tunnel packets from non 3GPP IP access to 3GPP access system and immediately start routing packets to the Serving GW for the default and any dedicated EPS bearers established. In case of non-roaming or roaming with home routed traffic this message is sent to the PDN GW in the HPLMN. In case of local breakout traffic the message is sent to the PDN GW in the VPLMN.

15. The PDN GW acknowledges by sending Update Bearer Response to the Serving GW.

16. The UE sends and receives data at this point via the 3GPP access system. The PDN-GW performs address allocation based on the procedure described in clause 4.7.

17. The PDN GW shall initiate resource allocation deactivation procedure in the trusted/untrusted non-3GPP IP access as defined in clause 6.12 or clause 7.9.

8.2.1.4 Using PMIP-based S5/S8

When a Trusted Non-3GPP IP Access to UTRAN/GERAN handover occurs, the following steps are performed instead of and in addition to the steps performed in the GTP based S5/S8 case (see previous section). In the case of PMIP based S5/S8, a Create Bearer Request and Update Bearer Request is not sent from the Serving GW to the PDN GW. Rather, the serving GW interacts with the hPCRF and PMIP messages are exchanged between the Serving GW and the PDN GW.

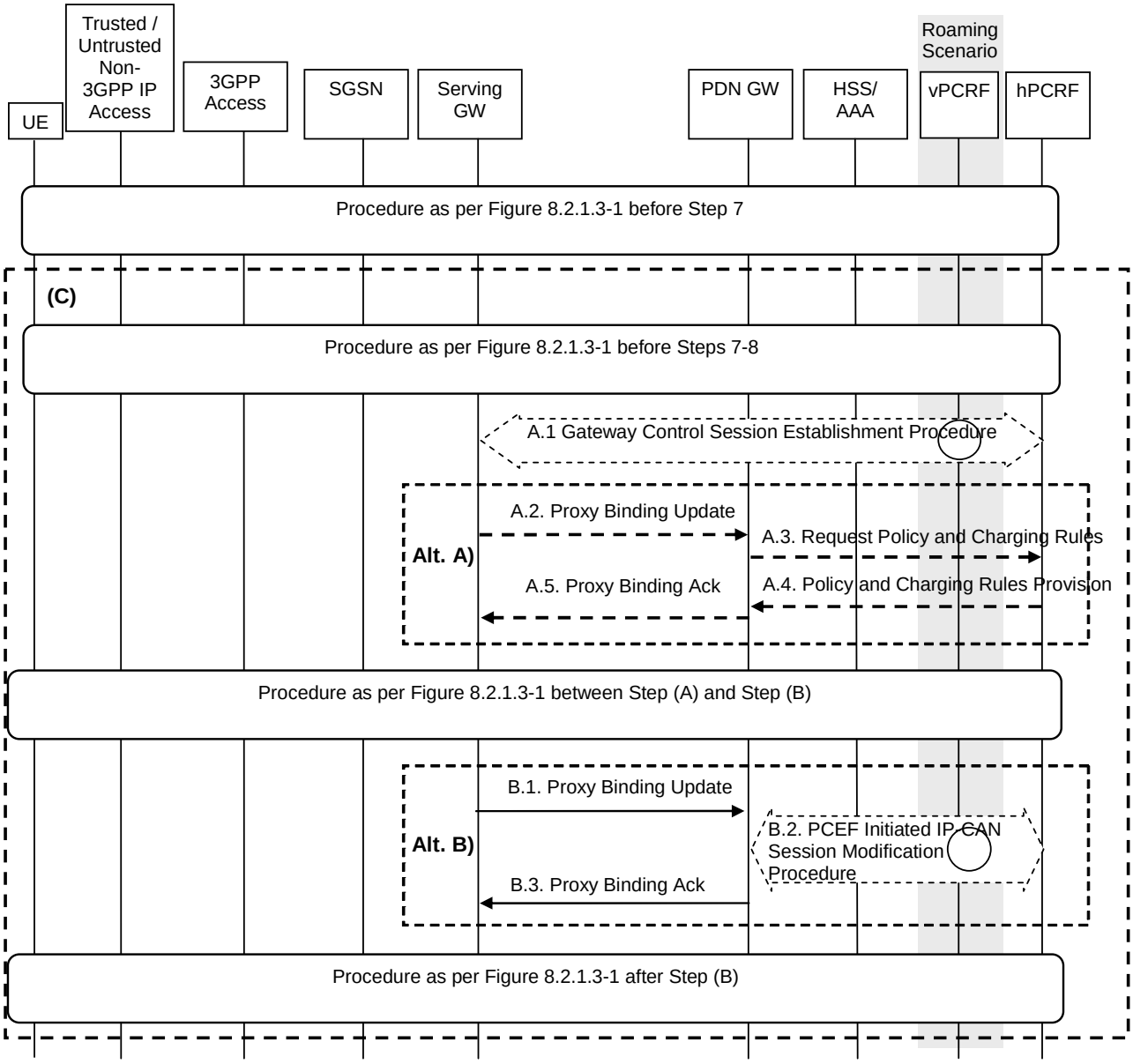


Figure 8.2.1.4-1: Trusted Non-3GPP IP Access to GERAN/UTRAN over PMIP-based S2a and using PMIP-based S5/S8

NOTE 1: Steps in (C) are repeated for each PDN the UE is connected to before handover in case of connectivity to multiple PDNs. The steps in (C) can occur in parallel for each PDN.

This procedure supports the home routed (Figure 4.2.2-1), roaming (Figure 4.2.3-1) and Local breakout (Figure 4.2.3-5) case. The Serving GW establishes a Gateway Control Session with the PCRF in the HPLMN. In the case of the roaming or local breakout scenario, the Serving GW interacts with the hPCRF by way of the vPCRF. The signalling takes place through the vPCRF in the VPLMN. In the case of Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF. The vPCRF then exchanges messages with the hPCRF in the HPLMN.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.1.4-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The steps shown in (Alt A) and (Alt B) are mutually exclusive in this procedure, i.e. either steps A.2-A.5 are executed or steps B.1-B.3. In order to execute the alternative (Alt B), the IP Address(es) of the UE needs to be available after step A.1. The IP Address(es) of the UE is received in step A.1, if dynamic policy provisioning is deployed.

In case the IP address(es) of the UE is available after step A1, (Alt B) provides lower jitter for dual radio handovers. In case the IP address(es) of the UE is not available after step A1, (Alt A) shall be used.

A.1) The Serving GW initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the Serving GW to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure.

If the updated PCC rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step B.1. It is FFS how the establishment of the default and dedicated bearers is synchronized.

A.2) The same description as in B.1 applies

A.3-A4) The same description as in B.2 applies

A.5) The same description as in B.3 applies. Since this step is triggered by the Proxy Binding Update message from the Serving GW in step A.2, it can occur after step A.2 and does not need to wait for steps A.3 and A.4.

NOTE 2: PDN GW address a selection is as described in TS 23.401 [4].

Steps between A.1 and B.1 are described in clause 8.2.1.3.

B.1) The Serving GW sends a Proxy Binding Update (MN NAI, Lifetime, APN, Additional Parameters) to the PDN GW in order to establish the new registration. The MN NAI identifies the UE for whom the message is being sent. The Lifetime field must be set to a nonzero value in the case of a registration. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The optional Additional Parameters may contain information, for example, protocol configuration options.

B.2) The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW to function as the PCEF for all the active IP sessions the UE has established with new IP-CAN type.

B.3) The PDN GW responds with a PMIP Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE address info returns the IP Address assigned to the UE. The optional Additional Parameter information element may contain other information, including for example Protocol Configuration Options. Since this step is triggered by the Proxy Binding Update message from the Serving GW in step B.1, it can occur after step B.1 and does not need to wait for step B.2.

8.2.2 3GPP Access to Trusted Non-3GPP IP Access Handover with PMIPv6 on S2a

The steps involved in the handover from 3GPP Access connected to the EPC to trusted non-3GPP IP access are depicted below for the case of non-roaming, roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving Gateway in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 or GTP tunnel is established between the S-GW and the PDN GW in the evolved packet core.

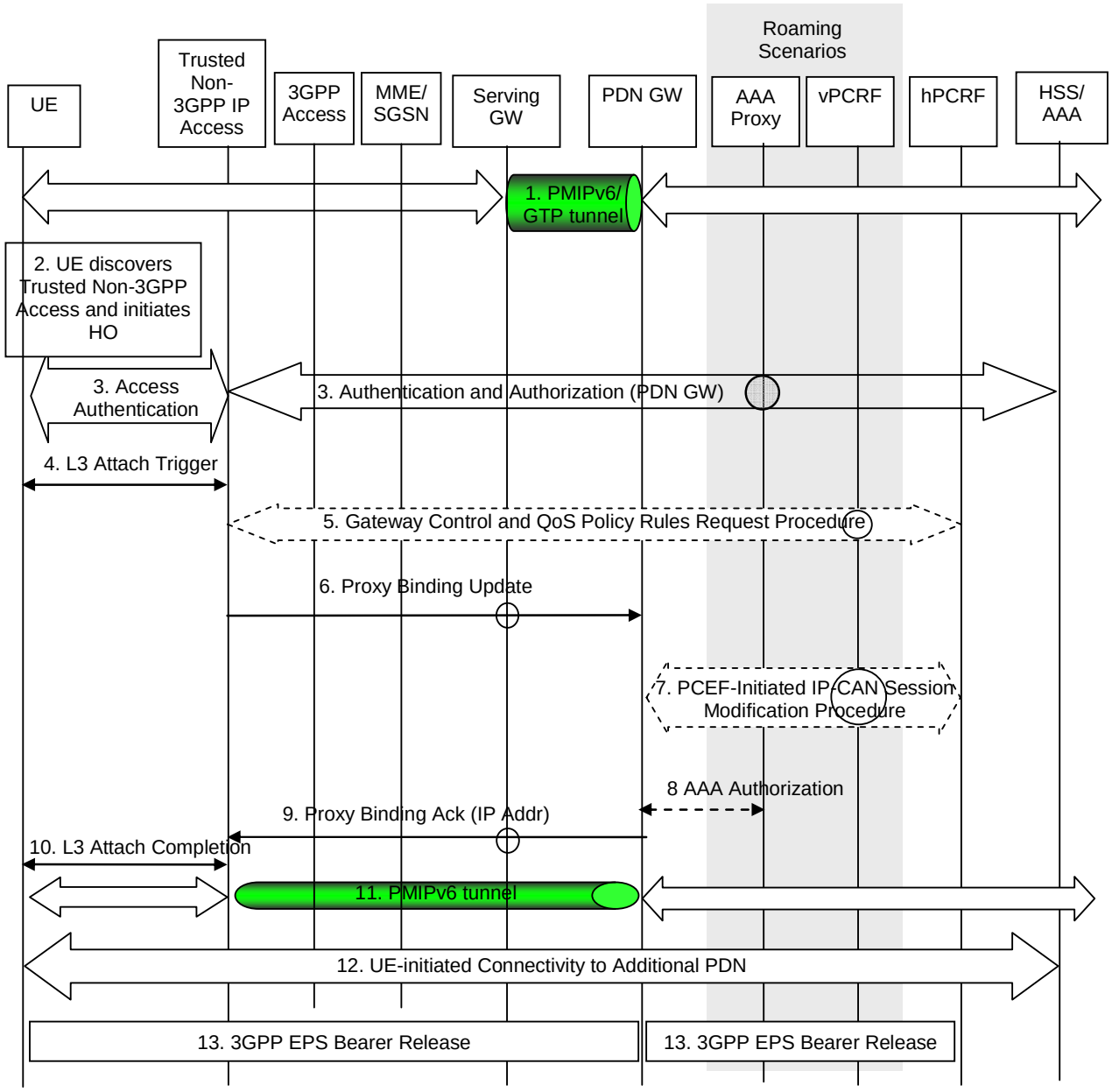


Figure 8.2.2-1: Handover from 3GPP Access to Trusted Non-3GPP IP Access with PMIPv6 on S2a and PMIPv6 or GTP on S5 interface

This procedure supports the home routed (Figure 4.2.2.1), roaming (Figure 4.2.3-1) and Local breakout (Figure 4.2.3-5) case. The PCRF in the HPLMN is informed of the change and any change in the policy that results is signalled to the Serving GW. The signalling takes place through the vPCRF in the VPLMN. In the case of Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

NOTE: For connectivity to multiple PDNs, step 12 is repeated for each PDN the UE is connected to. Step 12 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in Section 8.1.

Editor's Note: Text regarding roaming considerations to be provided here.

1) The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5 interface.

2) The UE discovers the trusted non-3GPP IP access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered trusted non-3GPP IP access system. The

mechanisms that aid the UE to discover the trusted non-3GPP IP access system, are specified in Section 4.8 (Network Discovery and Selection).

3) The UE performs access authentication and authorization in the non-3GPP access system. The 3GPP AAA server authenticates and authorizes the UE for access in the trusted non-3GPP system. The 3GPP AAA server queries the HSS and returns the PDN-GW address to the trusted non-3GPP access system at this step (upon successful authentication and authorization). The 3GPP AAA Server also returns to the trusted non-3GPP access system the MN NAI to be used to identify the UE in Proxy Binding Update and Gateway Control Session Establishment messages (steps 5 and 6).

   PDN GW address selection is as described in clause 4.5.1 of this specification. The PDNs the UE is connected to before handover are obtained from the HSS with the UE subscriber data.

NOTE: The MN NAI returned from the 3GPP AAA Server to the trusted non-3GPP access system is a permanent IMSI based MN NAI.

4) After successful authentication and authorization, the L3 attach procedure is triggered.

5) The Trusted Non-3GPP IP Access initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the Trusted Non-3GPP IP Access to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure.

   If the updated PCC rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step 6. The establishment of dedicated bearers in combination with the default takes place as described in Annex F of TS 23.401 [4].

6) The entity in the Trusted non-3GPP IP Access acting as a MAG sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic) message to the PDN GW in order to establish the new registration. The MN NAI identifies the UE for whom the message is being sent. The Lifetime field must be set to a nonzero value in the case of a registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW.

7) The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19]. The Event Report indicates the change in Access Type.

8) The PDN-GW may interact with the 3GPP AAA server to perform authorization function, e.g. authorization of the new MAG. Since this step is triggered by the Proxy Binding Update message from the Trusted non-3GPP IP Access in step 6, it can occur after step 6 and does not need to wait for step 7.

9) The PDN GW responds with a PMIP Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, Additional Parameters, GRE key for uplink traffic) message to the Trusted Non-3GPP IP Access. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE address info returns the IP Address assigned to the UE. The optional Additional Parameter information element may contain other information. Since this step is triggered by the Proxy Binding Update message from the Trusted non-3GPP IP Access in step 6 and the result of the optional step 8, it can occur after step 8. If step 8 is not taken, this step can occur after step 6.

10) L3 attach procedure is completed at this point. The IP address(es) assigned to the UE by the PDN-GW is conveyed to the UE.

11) The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW. The UE can send/receive IP packets at this point.

12) For connectivity to multiple PDNs, the UE establishes connectivity to all the PDNs that the UE was connected to before the handover besides the Default PDN, as described in clause 6.8.1.

13) The PDN GW shall initiate resource allocation deactivation procedure in 3GPP access as defined in clause 5.4.5.2.

8.2.3 E-UTRAN to Untrusted Non-3GPP IP Access Handover with PMIPv6 on S2b

This section shows a call flow for a handover when a UE moves from a E-UTRAN to an untrusted non-3GPP access network. PMIPv6 is assumed to be used on the S5/S8 and S2b interfaces.

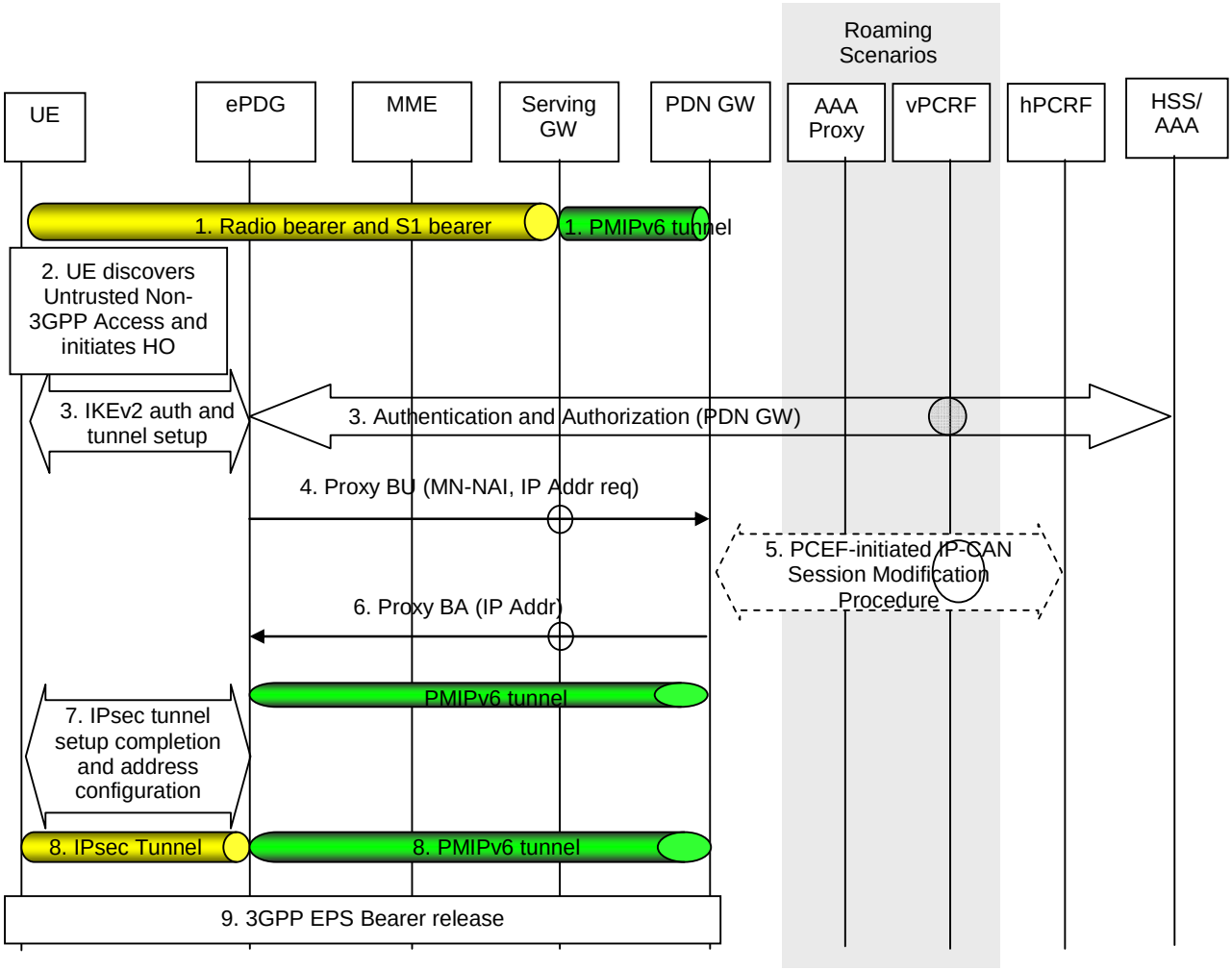


Figure 8.2.3-1: E-UTRAN to Untrusted Non-3GPP IP Access Handover

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

1) The UE is initially attached to the E-UTRAN network.

2) The UE moves and attaches to an untrusted non-3GPP IP access network.

3) The IKEv2 tunnel establishment procedure is started by the UE. The ePDG IP address to which the UE needs to form IPsec tunnel with is discovered as specified in clause 4.5.3. After the UE is authenticated, UE is also authorized for access to the APN. The procedure is as described in TS 33.234 [5]. As part of access authentication the PDN GW information is sent to the ePDG by the 3GPP AAA server.

4) The ePDG sends the Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, IP Address Requested, GRE key for downlink traffic) message to the PDN GW. Access Technology Type is set to a value matching the characteristics of the non-3GPP access.

5) If PCC is supported, the PDN GW requires configuration for enforcing policy, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19].

6) The PDN GW processes the Proxy Binding Update message from the ePDG, updates the binding cache entry for the UE and responds with a Proxy Binding Acknowledgement (GRE key for uplink traffic) message. In the proxy Binding Ack, the PDN GW replies with the same IP address or prefix that was assigned to the UE earlier. At this point a PMIPv6 tunnel exists between PDN GW and ePDG. The PDN GW triggers the bearer release in the 3GPP Access using the PDN GW initiated Bearer Deactivation procedure. Radio Bearers associated with the PDN address are released if existing. Since this step is triggered by the Proxy Binding Update message from the ePDG in step 4, it can occur after step 4 and does not need to wait for step 5.

7) The ePDG and the UE continue the IKEv2 exchange and IP address configuration.

8) At the end of the handover procedure there is a default bearer for the UE that consists of an IPsec tunnel between the UE and the ePDG and a PMIPv6 tunnel between the ePDG and the PDN GW.

9) The PDN GW shall initiate resource allocation deactivation procedure in 3GPP access as defined in clause 5.4.5.2.

8.2.4 Trusted Non-3GPP IP Access to 3GPP Access Handover with PMIPv6 on S2a and Chained S2a and GTP-based S8

8.2.4.1 General Handover Procedure with Serving GW relocation

The steps involved in the handover from a trusted non-3GPP IP access to 3GPP Access connected to EPC are depicted below for roaming cases with chained S2a and GTP-based S8. It is assumed that while the UE is served by the trusted non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the Serving GW in the EPC and a GTP tunnel between the Serving GW and the PDN GW.

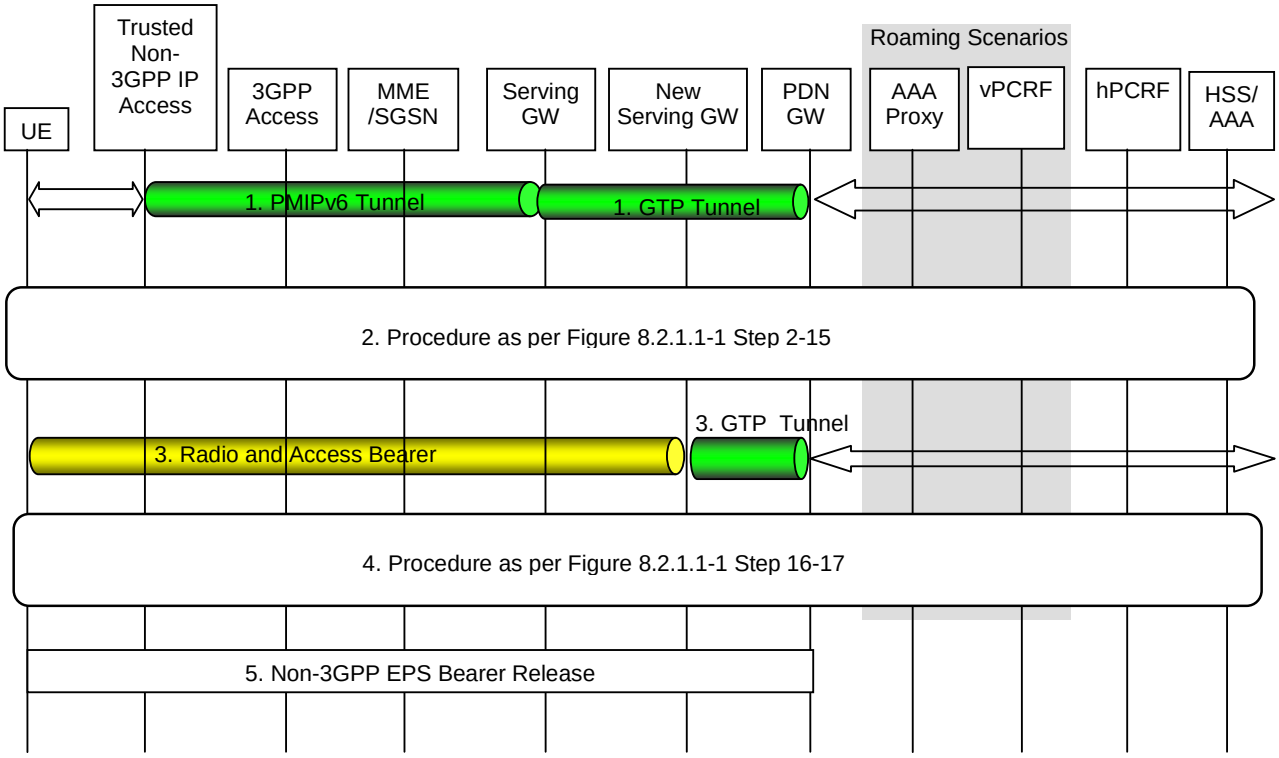


Figure 8.2.4-1: Handover from Trusted Non-3GPP IP Access to 3GPP Access with chained S2a and GTP-based S8 anchored in the visited network and Serving GW relocation

NOTE: The flow here assumes that this is an initial attach of the UE and no bearers for the UE exists in E-UTRAN.

Editor's Note: The alignment of the handover procedure with the attach procedure over PMIP based S5/S8 is FFS.

Editor's Note: The documentation of handover from trusted non-3GPP IP Access to legacy 2G/3G is FFS.

NOTE: The following procedure assumes that the Serving GW that was anchoring the non-3GPP IP Access is not necessarily anchoring the target 3GPP Access after the handover completes.

Editor's Note: The case of using the same Serving GW is FFS.

1. The UE uses a trusted non-3GPP access system. A PMIPv6 tunnel is established between the trusted non-3GPP access and the Serving GW. Then a GTP tunnel is concatenated between the Serving GW and the PDN GW.
2. The UE discovers and attaches to the 3GPP access as defined in step 2 of clause 8.2.1.1.
3. The UE sends and receives data via the 3GPP access.
4. Steps 16 and 17 of clause 8.2.1.1
5. The PDN GW triggers resource release in the non-3GPP access. The exact signalling messages used in order to release the EPS bearers in the non-3GPP Access are FFS.

8.2.4.2 Handover Procedure without Serving GW relocation

The steps involved in the handover from a trusted non-3GPP IP access to 3GPP Access connected to EPC are depicted below for roaming cases with chained S8a/S2a. It is assumed that while the UE is served by the trusted non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the Serving GW in the EPC and a GTP tunnel between the Serving GW and the PDN GW. And it is assumed that the Serving GW is not changed during the HO procedure.

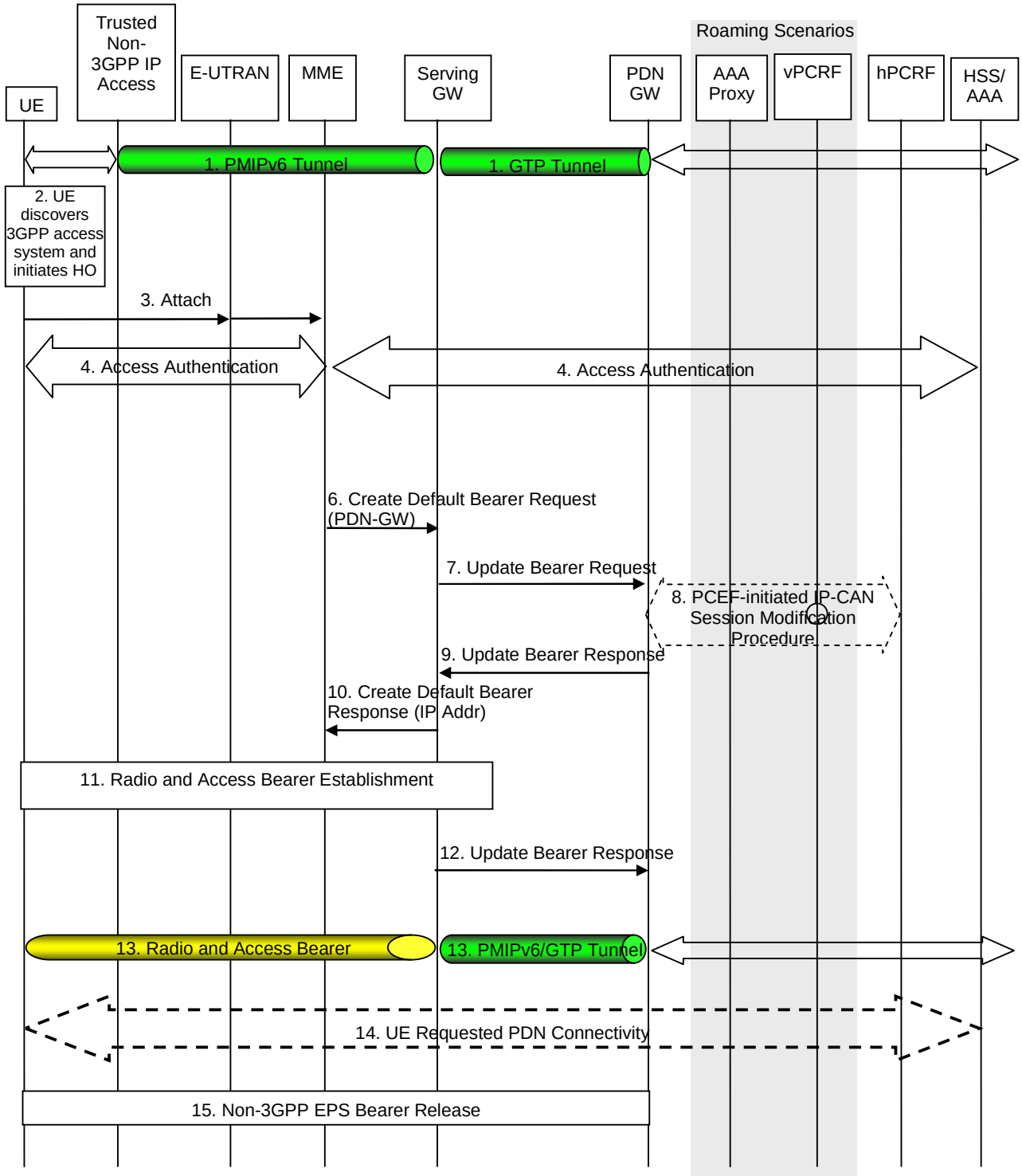


Figure 8.2.4-2: Handover from Trusted Non-3GPP IP Access to 3GPP Access with chained S8a/S2a anchored in the visited network and without Serving GW relocation

1. The UE uses a trusted non-3GPP access system. A PMIPv6 tunnel is established between the trusted non-3GPP access and the Serving GW. Then a GTP tunnel is concatenated between the Serving GW and the PDN GW.

2) The UE discovers the E-UTRAN access and determines to transfer its current sessions (i.e. handover) from the currently used non-3GPP access system to E-UTRAN. The mechanisms that aid the UE to discover the 3GPP Access system, are specified in Section 4.8 (Network Discovery and Selection).

3) The UE sends an Attach Request to the MME. The message from the UE is routed by E-UTRAN to the MME as specified in TS 23.401 [4] (E-UTRAN).

4) The MME contacts the HSS and authenticates the UE.

5) After successful authentication, the MME performs location update procedure and subscriber data retrieval from the HSS as specified in TS 23.401 [4]. The PDN GW address is conveyed to the MME with the subscriber data as described in TS 23.401 [4].

6) The MME selects a serving GW as described in TS 23.401 [4] and sends a Create Default Bearer Request (including IMSI, MME Context ID (SGSN equivalent is TBD), and PDN-GW address) message to the selected Serving GW.

7) The Serving GW detects that it already has the default bearer context and sends an Update Bearer Request (RAT Type, QoS Profile) message to the PDN-GW in the HPLMN.

8) The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW in the VPLMN or HPLMN to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

   If the updated PCC rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step 12. It is FFS how the establishment of the default and dedicated bearers is synchronized.

NOTE: PDN GW address and Serving GW address selection is as described in the clause "GW selection" in TS 23.401 [4].

9) The PDN GW responds with an Update Bearer Response message to the Serving GW. The dedicated bearer request may be sent together with the Update Bearer Response to the Serving GW from the PDN GW after step 9.

10) The Serving GW returns a Create Default Bearer Response message and dedicated bearer request to the MME as specified in TS 23.401 [4]. This message includes the IP address of the UE.

11) Radio and Access bearers are established at this step in the 3GPP access as specified in TS 23.401 [4]. A RAN procedure Ready flag is sent to the Serving GW after all the Radio and Access bearers are established.

12) The Serving GW send update bearer response to the PDN GW if the dedicated bearer request is sent in step 9.

13) The UE sends and receives data at this point via the E-UTRAN system.

14) For connectivity to multiple PDNs, the UE establishes connectivity to each PDN, the UE was connected to before the handover, besides the Default PDN, by executing the UE requested PDN specified in TS 23.401 [4].

15) The Serving GW triggers resource release in the non-3GPP access. The exact signalling messages used in order to release the EPS bearers in the non-3GPP Access are FFS.

8.2.5 3GPP Access to Trusted Non-3GPP IP Access Handover with PMIPv6 on S2a and Chained S2a and GTP-based S8

8.2.5.1 General Handover Procedure with Serving GW relocation

The steps involved in the handover for chained S2a and GTP-based S8 from 3GPP Access connected to the EPC to trusted non-3GPP IP access are depicted below for the case of roaming with home routed traffic with anchoring in the Serving GW in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 or GTP tunnel is established between the Serving GW and the PDN GW in the evolved packet core.

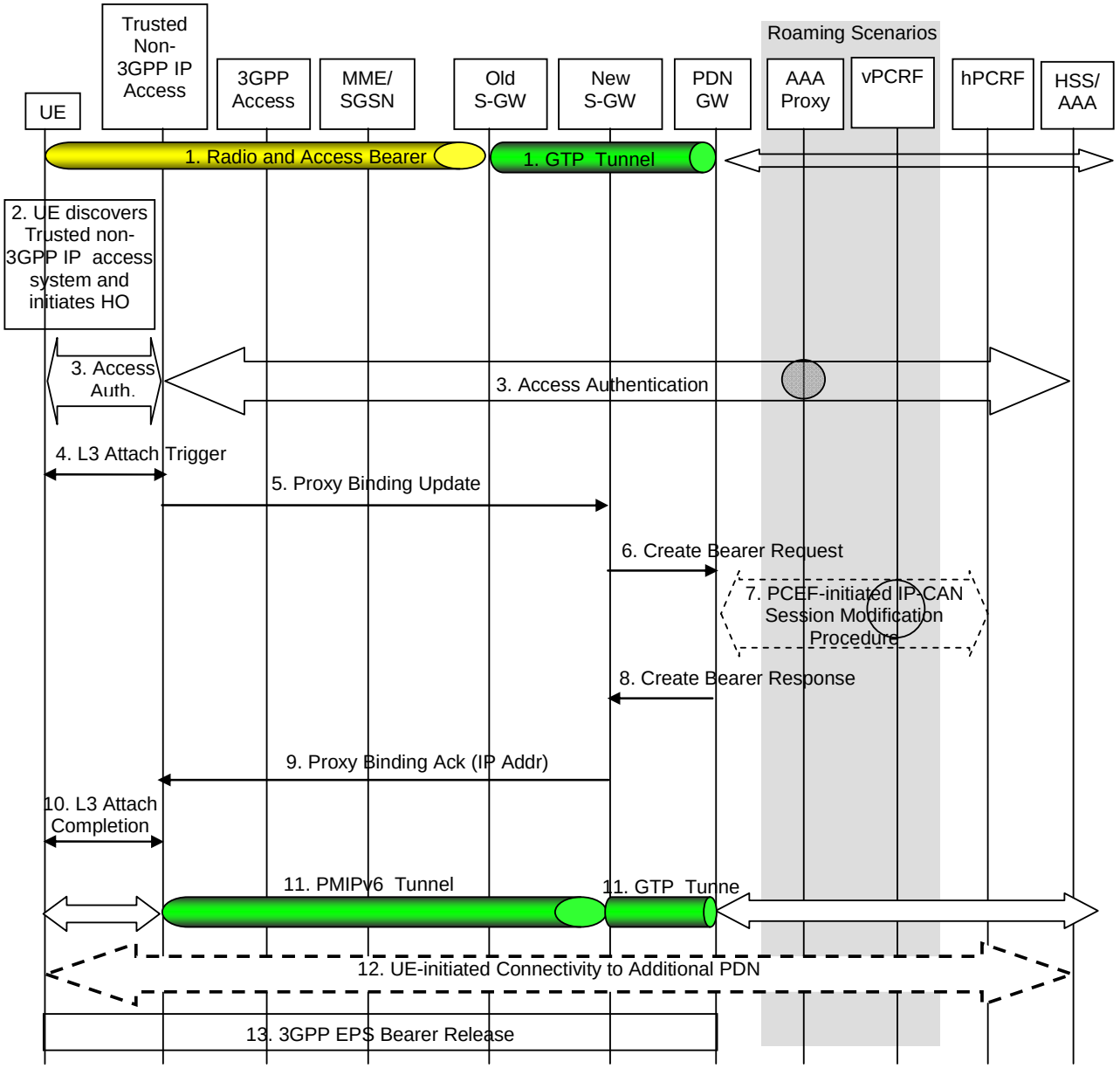


Figure 8.2.5-1: Handover from 3GPP Access to Trusted Non-3GPP IP Access with chained S2a and GTP-based S8 anchored in the visited network with Serving GW relocation

NOTE 1: The following procedure assumes that the Serving GW that was anchoring the 3GPP Access is not necessarily anchoring the target non-3GPP IP Access after the handover completes.

NOTE 2: In case of connectivity to multiple PDNs, step 13 is repeated for each PDN the UE is connected to. Step 13 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

1. The UE is connected in the 3GPP Access and has a GTP tunnel on the S8 interface.

2. The UE discovers the trusted non-3GPP IP access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered trusted non-3GPP IP access system.

   The mechanisms that aid the UE to discover the trusted non-3GPP IP access system are specified in Section 4.8 (Network Discovery and Selection).

3. The UE performs access authentication and authorization in the non-3GPP access system. The 3GPP AAA server authenticates and authorizes the UE for access in the trusted non-3GPP system. As part of this procedure, the 3GPP AAA proxy obtains the PDN GW information from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. Both, PDN GW and Serving GW information is

provided to the MAG function of the trusted non-3GPP access. The authentication credentials are relayed from the AAA proxy in the visited PLMN to the HSS/AAA in the HPLMN. The PDNs the UE is connected to before handover are obtained from the HSS with the UE subscriber data.

4. After successful authentication and authorization, the L3 attach procedure is triggered.

5. The entity in the Trusted non-3GPP IP Access acting as a MAG sends a PMIPv6 Proxy Binding Update message (MN_NAI, GRE key for downlink traffic, PDN GW address). As the traffic is anchored in the Serving GW, the entity in the Trusted non-3GPP IP access acting as a MAG sends the "Proxy Binding Update" to the Serving GW in the VPLMN.

6. The Serving GW sends a Create Bearer Request message to the PDN GW in the HPLMN as described in TS 23.401. The PDN GW should switch the tunnel from 3GPP IP access to non-3GPP access system at this point.

NOTE 3: In this Release of the specification, the Serving GW uses a pre-configured QoS profile to establish the GTP-based S8 bearer to the PDN GW.

7. The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW in the VPLMN or HPLMN to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

8. The PDN GW responds with a Create Bearer Response message to the Serving GW as described in TS 23.401.The Create Bearer Response contains the IP address or the prefix that was assigned to the UE while it was connected to the non-3GPP IP access. Since this step is triggered by the Create Bearer Request message from the Serving GW in step 9, it can occur after step 9 and does not need to wait for the PCC interaction in step 10.

9. The Serving GW processes the proxy binding update and updates the binding cache entry for the UE. It confirms the IP address (es) for the UE sending a Proxy Binding Acknowledgement (GRE key for uplink traffic) to the MAG function in Trusted non-3GPP IP Access, including the IP address (es) allocated for the UE.

10. L3 attach procedure is completed at this point. The IP address (es) assigned to the UE by the PDN GW is conveyed to the UE.

11. The PMIPv6 tunnel is set up between the Trusted non-3GPP IP Access and the Serving GW and a GTP tunnel is established between the Serving GW and the PDN GW. The UE can send/receive IP packets at this point.

12. For connectivity to multiple PDNs, the UE establishes connectivity to each PDN, the UE was connected to before the handover, besides the Default PDN, by executing the UE requested PDN specified in TS 23.401 [4].

13. The PDN GW triggers the bearer release in the 3GPP Access using the PDN GW initiated Bearer Deactivation procedure. The 3GPP access resources associated with the PDN address are released if existing

8.2.5.2 Handover Procedure without Serving GW relocation

The steps involved in the handover for chained S8a/S2a from 3GPP Access connected to the EPC to trusted non-3GPP IP access are depicted below for the case of roaming with home routed traffic with anchoring in the Serving GW in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a GTP tunnel is established between the Serving GW and the PDN GW in the evolved packet core. And it is assumed that the Serving GW is not changed during the HO procedure for this clause.

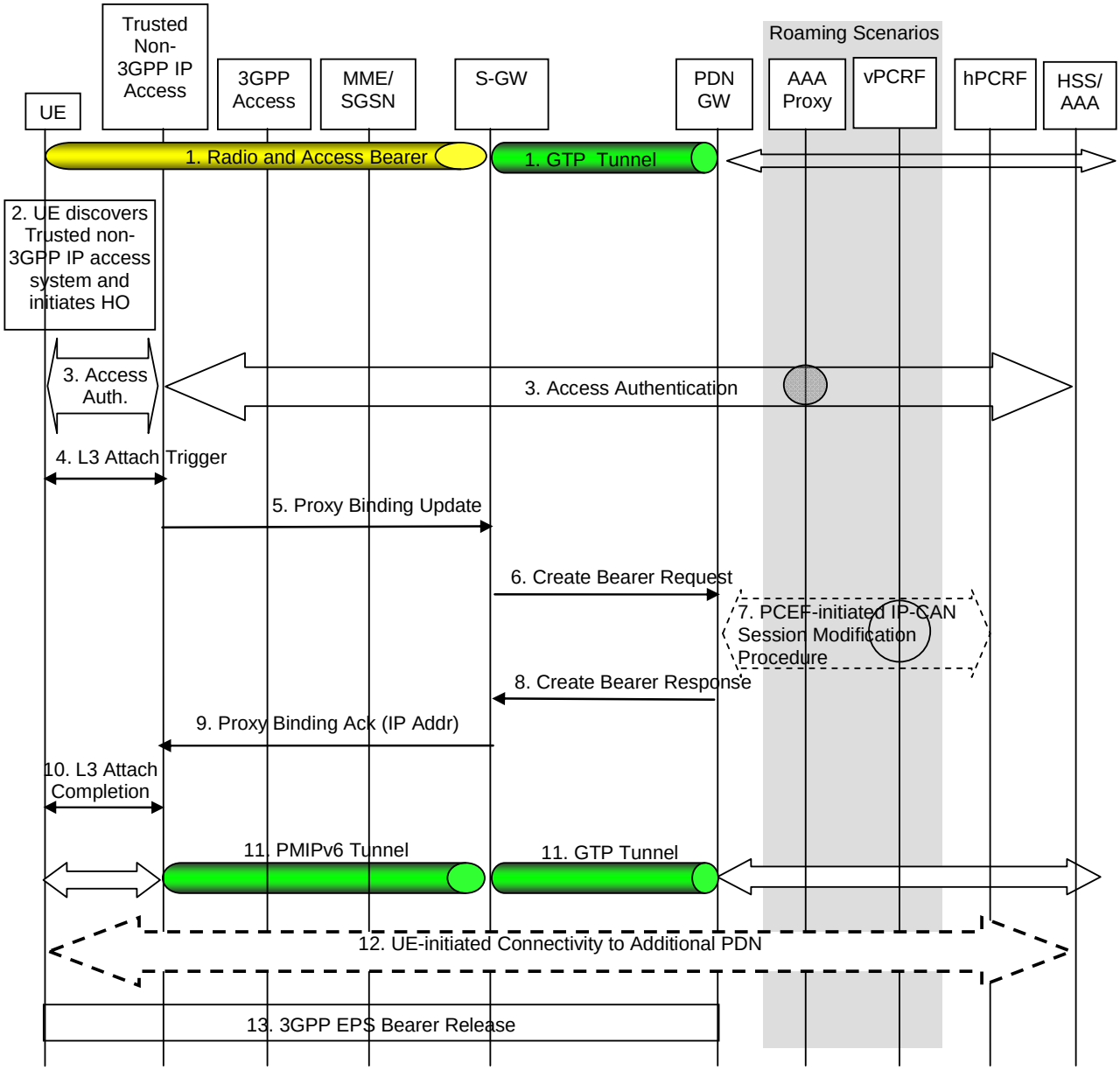


Figure 8.2.5-2: Handover from 3GPP Access to Trusted Non-3GPP IP Access with chained S8a/S2a anchored in the visited network and without Serving GW relocation

NOTE 1: The following procedure assumes that the Serving GW that was anchoring the 3GPP Access is the same as anchoring the target non-3GPP IP Access after the handover completes.

NOTE 2: In case of connectivity to multiple PDNs, step 13 is repeated for each PDN the UE is connected to. Step 13 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

1. The UE is connected in the 3GPP Access and has a GTP tunnel on the S8 interface.

2. The UE discovers the trusted non-3GPP IP access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered trusted non-3GPP IP access system.

   The mechanisms that aid the UE to discover the trusted non-3GPP IP access system are specified in clause 4.8 (Network Discovery and Selection).

3. The UE performs access authentication and authorization in the non-3GPP access system. The 3GPP AAA server authenticates and authorizes the UE for access in the trusted non-3GPP system. As part of this procedure, the 3GPP AAA proxy obtains the PDN GW information from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. Both, PDN GW and Serving GW information is

provided to the MAG function of the trusted non-3GPP access. The authentication credentials are relayed from the AAA proxy in the visited PLMN to the HSS/AAA in the HPLMN. The PDNs the UE is connected to before handover are obtained from the HSS with the UE subscriber data.

4. After successful authentication and authorization, the L3 attach procedure is triggered.

5. The entity in the Trusted non-3GPP IP Access acting as a MAG sends a PMIPv6 Proxy Binding Update message (MN_NAI, PDN GW address). As the traffic is anchored in the Serving GW, the entity in the Trusted non-3GPP IP access acting as a MAG sends the "Proxy Binding Update" to the Serving GW in the VPLMN.

6. The Serving GW sends an Update Bearer Request message (RAT Type, QoS Profile) to the PDN GW in the HPLMN as described in TS 23.401.. The PDN GW judge the UE access via an non-3GPP access according the new RAT Type, then the PDN GW removed all the dedicater bearer associated the PDN address.

7. The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW in the VPLMN or HPLMN to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

8. The PDN GW responds with an Update Bearer Response message to the Serving GW as described in TS 23.401 [4]. Since this step is triggered by the Update Bearer Request message from the Serving GW in step 9, it can occur after step 9 and does not need to wait for the PCC interaction in step 10.

9. The Serving GW processes the Proxy Binding Update and updates the binding cache entry for the UE. It confirms the IP address (es) for the UE sending a "Proxy Binding Acknowledgement (PBA)" to the MAG function in Trusted non-3GPP IP Access, including the IP address (es) allocated for the UE.

10. L3 attach procedure is completed at this point. The IP address (es) assigned to the UE by the PDN GW is conveyed to the UE.

11. The PMIPv6 tunnel is set up between the Trusted non-3GPP IP Access and the Serving GW and a GTP tunnel is established between the Serving GW and the PDN GW.

12. For connectivity to multiple PDNs, the UE establishes connectivity to each PDN, the UE was connected to before the handover, besides the Default PDN, by executing the UE requested PDN specified in TS 23.401 [4].

13. The Serving GW triggers the bearer release in the 3GPP Access using the Serving GW initiated Bearer Deactivation procedure. The 3GPP access resources associated with the PDN address are released if existing.

8.2.6 Non-3GPP IP Access to 3GPP Access Handover with PMIPv6 on S2a/b for Chained PMIP-based S8

The steps involved in the handover from a trusted or non-trusted non-3GPP IP access to a 3GPP access connected to EPC are depicted below for roaming cases with chained S2a/b and PMIP-based S8. It is assumed that while the UE is served by the non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the Serving GW and another one between the Serving GW and the PDN GW.

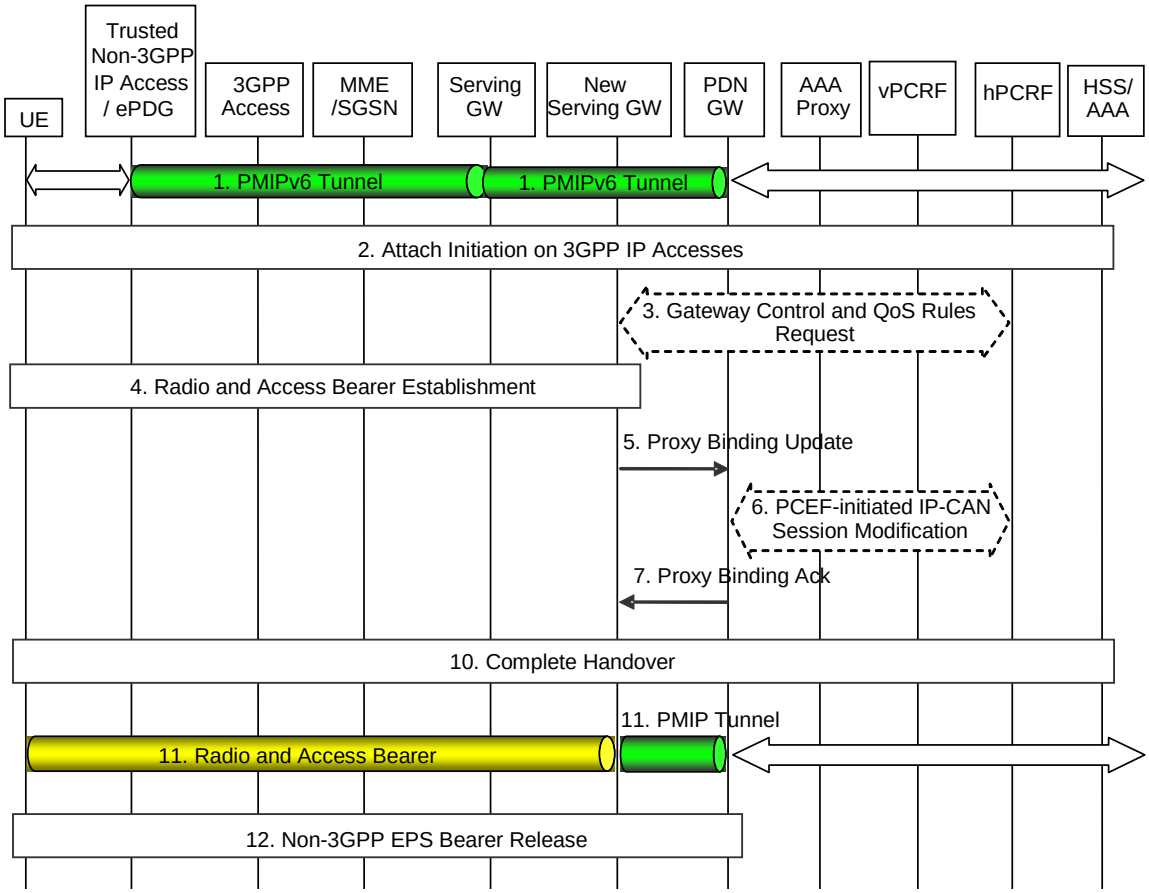


Figure 8.2.6-1: Handover from Trusted or Untrusted Non-3GPP IP Access to 3GPP Access with chained S2a/b and PMIP-based S8

NOTE: The flow here assumes that the UE is not yet attached in E-UTRAN in step 1.

NOTE: The procedure applies both for the case where a new Serving GW is selected during attach on 3GPP access or for the case where the Serving GW is not changed.

1) The UE uses a trusted or untrusted non-3GPP access system. PDN connectivity is achieved through concatenated PMIPv6 tunnels between the trusted non-3GPP access or ePDG and the Serving GW, and between the Serving GW and the PDN GW.

2) The attach initiation on the 3GPP IP access is performed as described in steps 2-6 of clause 8.2.1.1 (for E-UTRAN) and step 2-8 of clause 8.2.1.2 (for UTRAN/GERAN).

3) In case of PMIP-based S8/S2a chaining, the Serving GW initiates the Gateway Control Session Establishment Procedure with the hPCRF, as specified in TS 23.203 [19].

4) The 3GPP radio and access bearers are setup as described in steps 11-12a of clause 8.2.1.1 (for E-UTRAN) and step 13-14 of clause 8.2.1.3 (for UTRAN/GERAN).

5) The Serving GW sends a PMIPv6 Proxy Binding Update (MN NAI, Lifetime, Access Technology Type, Handover Indicator, IP Address Requested, APN, GRE Key for downlink traffic, Additional Parameters) message to the PDN GW. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value in the case of a registration. Access Technology Type is set to indicate RAT type (E-UTRAN). The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The optional Additional Parameters may contain information, for example, protocol configuration options.

6) The PDN GW initiates the PCEF-Initiated IP-CAN Session Modification Procedure to update the rules in the PDN GW, as specified in TS 23.203 [19].

7) The PDN GW responds with a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE address info

returns the IP Address assigned to the UE. The optional Additional Parameter information element may contain other information, including for example Protocol Configuration Options. The Serving GW acts as the MAG (in terms of PMIPv6). Since this step is triggered by the Proxy Binding Update message from the Serving GW in step 5, it does not need to wait for steps 6.

10) For trusted non-3GPP accesses, the handover attach procedure is completed as described in steps 12a of clause 8.2.1.1.

11) PDN connectivity is now achieved through concatenated GTP tunnels between the 3GPP access to the Serving GW and a PMIPv6 tunnel between the Serving GW and the PDN GW.

12) In case a new Serving GW has been selected during the attach on 3GPP access, the PDN GW triggers the bearer release in the non-3GPP access. Otherwise, the Serving GW triggers resource release in the non-3GPP access. The exact signalling messages used in order to release the EPS bearers in the non-3GPP Access are FFS.

8.2.7 3GPP Access to Non-3GPP IP Access Handover with PMIPv6 on S2a/b for Chained PMIP-based S8

The steps involved in the handover from a 3GPP access to a trusted or non-trusted non-3GPP IP access connected to EPC are depicted below for roaming cases with chained S2a/b and PMIP-based S8.

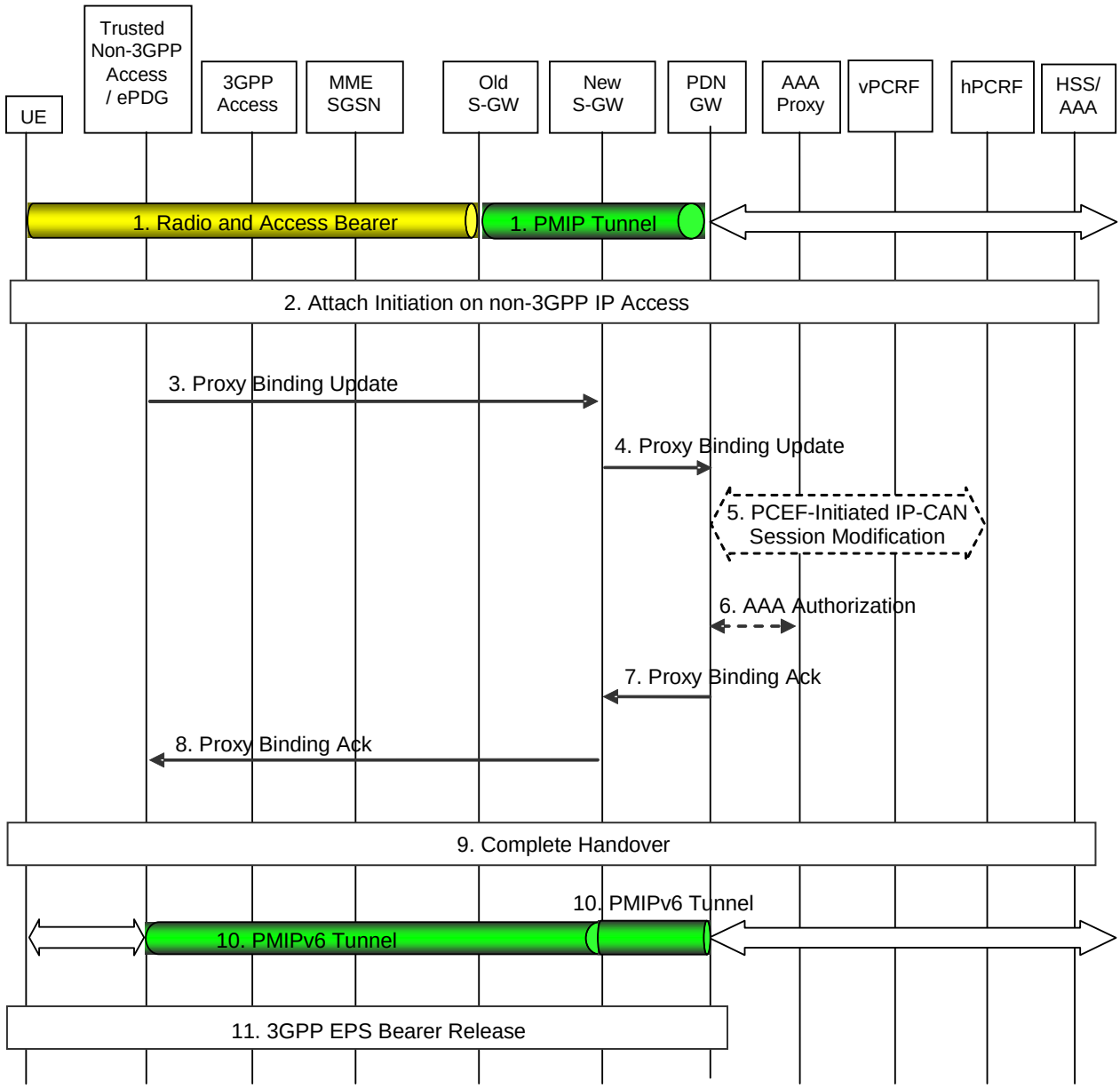


Figure 8.2.7-1: Handover from 3GPP IP Access to Trusted or Untrusted Non-3GPP Access with chained S2a/b and PMIP-based S8

NOTE: The procedure applies both for the case where a new Serving GW is selected during attach on 3GPP access, or for the case where the Serving GW is not changed.

1) The UE is connected to the PDN via a 3GPP Access and has a PMIPv6 tunnel on the S8 interface.

2) The attach initiation on the trusted or untrusted non-3GPP access is performed as described in steps 2-6 of clause 8.2.2 (for trusted non-3GPP access) and steps 2-3 of clause 8.2.3 (for untrusted non-3GPP access). As part of the authentication procedure, the 3GPP AAA proxy obtains the PDN-GW address from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. Both, PDN GW and Serving GW information is provided to the MAG function of the trusted non-3GPP access or ePDG.

3) The MAG function of Trusted Non-3GPP IP Access or ePDG sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, PDN GW address, Additional Parameters) message to the Serving GW in the VPLMN. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value, indicating registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. Handover Indicator is set to indicate attachment over a new interface. The Additional Parameters may include Protocol Configuration Options and other information.

4) The Serving GW sends a corresponding Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, Additional Parameters) message (as in step 3) to the PDN GW.

5) The PDN GW initiates the PCEF-Initiated IP-CAN Session Modification Procedure with the hPCRF to update the rules in the PDN GW, as specified in TS 23.203 [19].

6) The PDN-GW may interact with the 3GPP AAA server to perform authorization, e.g. authorization of the new MAG. Since this step is triggered by the Proxy Binding Update message in step, it can occur after step 5 and does not need to wait for step 6.

7) The PDN GW processes the proxy binding update and creates a binding cache entry for the PMIPv6 tunnel towards the Serving GW. The PDN GW responds with a Proxy Binding Acknowledgement (MN-NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The MN-NAI is identical to the MN-NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE Address Info includes one or more IP addresses. The Additional Parameters may include Protocol Configuration Options and other information.

8) The Serving GW processes the proxy binding acknowlegdement and creates a binding cache entry for the PMIPv6 tunnel towards the MAG function in the trusted non-3GPP access or ePDG. At this point, the Serving GW also establishes the internal forwarding state for the concatenation of the PMIPv6 tunnels. The Serving GW then sends a corresponding Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message (as in step 8) to the MAG function of Trusted Non-3GPP IP Access or ePDG.

9) The handover attach procedure is completed as described in step 12 of clause 8.2.2 (for trusted non-3GPP access) and steps 8-9 of clause 8.2.3 (for untrusted non-3GPP access).

10) The UE is connected to the PDN via the non-3GPP access system. PDN connectivity is achieved through concatenated PMIPv6 tunnels between the trusted non-3GPP access or ePDG and the Serving GW, and between the Serving GW and the PDN GW.

11) In case a new Serving GW has been selected during the attach on the non-3GPP access, the PDN GW triggers the bearer release in the 3GPP access using the PDN GW initiated Bearer Deactivation procedure. Otherwise, the Serving GW triggers the bearer release in the 3GPP Access using the Serving GW initiated Bearer Deactivation procedure. The 3GPP access resources associated with the PDN address are released if existing.

8.3 Handover from 3GPP access to Trusted Non-3GPP IP Access with MIPv4 FACoA on S2a

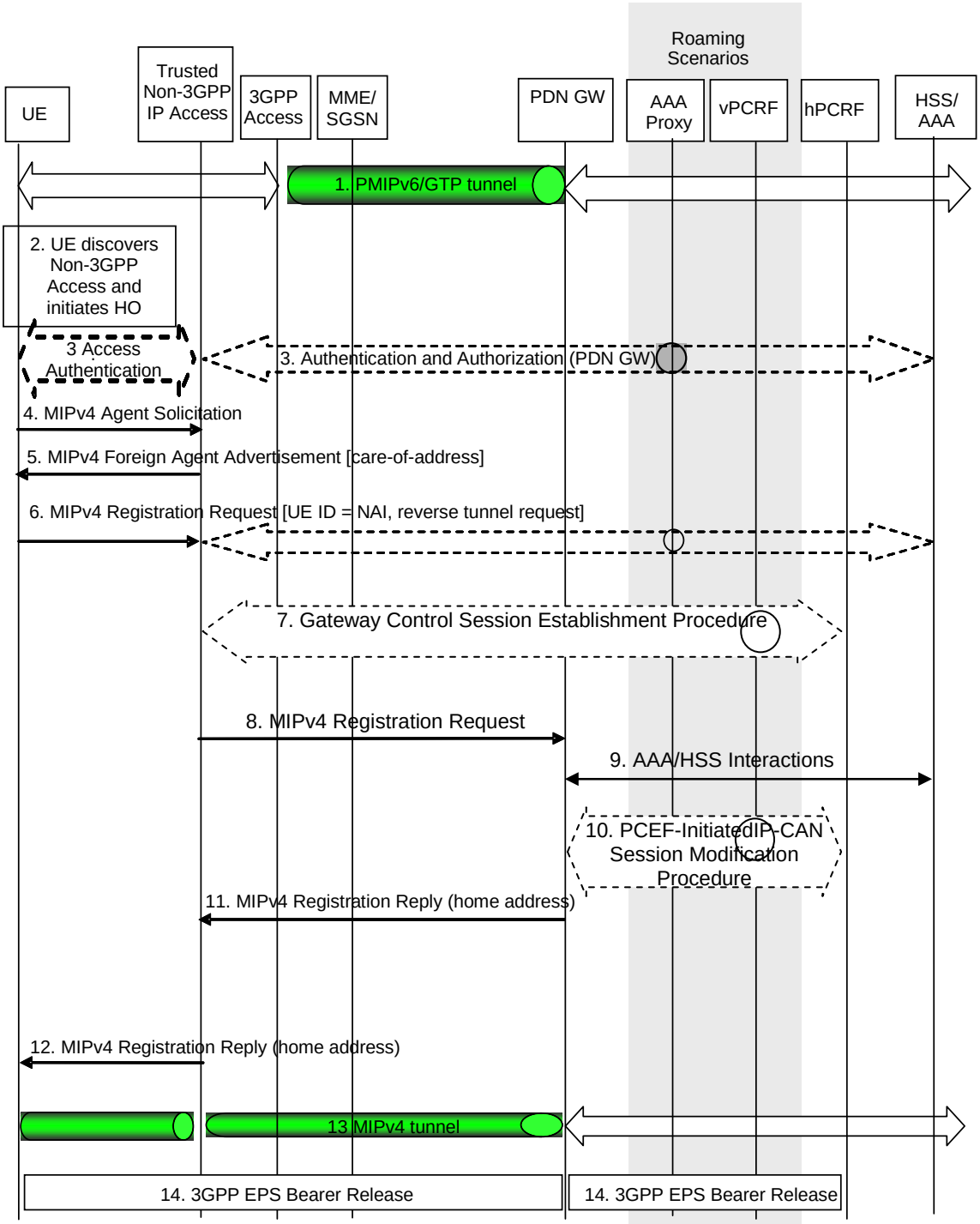


Figure 8.3-1: 3GPP IP Access to Non-3GPP IP access Handover over MIPv4-based S2a

NOTE: In case of connectivity to multiple PDNs, steps in (C) are repeated for each PDN the UE is connected to. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The steps involved in the handover from 3GPP Access connected to the EPC to trusted non-3GPP IP access are depicted below for the case of non-roaming, roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving Gateway in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 or GTP tunnel is established between the S-GW and the PDN GW in the evolved packet core.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The event that triggers Authentication and Authorization in step 3 or step 6 between the Trusted Non-3GPP IP Access and the 3GPP AAA Server, or whether this step occurs at all, depends on the specific access technology.

1) The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5 interface.

2) The UE discovers the trusted non-3GPP IP access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered trusted non-3GPP IP access system. The mechanisms that aid the UE to discover the trusted non-3GPP IP access system, are specified in clause 4.8 (Network Discovery and Selection).

3) The UE may performs access authentication and authorization in the non-3GPP access system. The 3GPP AAA server authenticates and authorizes the UE for access in the trusted non-3GPP system. The 3GPP AAA server queries the HSS, a DNS query is performed for resolving the identity of the PDN GW, and returns the PDN-GW address to the trusted non-3GPP access system at this step (upon successful authentication and authorization).

4) The UE may send an Agent Solicitation (AS) RFC 3344 [12] message. Specification of this message is out of the scope of 3GPP.

5) The FA in the Trusted Non-3GPP IP Access sends a Foreign Agent Advertisement (FAA) (RFC 3344 [12]) message to the UE. The FAA message includes the Care-of Address (CoA) of the Foreign Agent function in the FA. Specification of this message is out of the scope of 3GPP.

6) The UE sends a Registration Request (RRQ) (MN-NAI, lifetime) message as defined in RFC 3344 [12] to the FA as specified in RFC 3344 [12]. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34]. The UE may not indicate a specific Home Agent address in the RRQ message, in which case the FA uses the PDN GW address as received in step 3. The UE then receives the IP address of the PDN Gateway in step 11 as part of the RRP message. The UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages.

7) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in step 10 and also to convey subscription related parameters to the PCRF.

8) The FA processes the message according to RFC 3344 [12] and forwards a corresponding RRQ (MN-NAI, lifetime) message to the PDN GW.

9) The selected PDN GW obtains Authentication and Authorization information from the AAA/HSS.

10) The PDN GW allocates an IP address for the UE. The PDN GW initiates the IP CAN Session Modification Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF that the IP-CAN type has changed and the PCRF responds to the PDN GW with PCC rules and event triggers.

11) The PDN GW sends a Registration Reply (RRP) (MN-NAI, Home Address, Home Agent Address) message as defined in RFC 3344 [12] to the FA.

12) The FA processes the RRP (MN-NAI, Home Address) according to RFC 3344 [12] and sends a corresponding RRP message to the UE.

13) IP connectivity from the UE to the PDN GW is now setup. A MIP tunnel is established between the FA in the Trusted Non-3GPP IP Access and the PDN GW.

14) The PDN GW shall initiate resource allocation deactivation procedure in 3GPP access as defined in clause 5.4.5.2.

8.4 Handovers with DSMIPv6 on S2c

8.4.1 Trusted or Untrusted Non-3GPP IP Access to 3GPP Access Handover with DSMIPv6 over S2c

In this scenario, the session starts in a trusted or untrusted non-3GPP access system using DSMIPv6 and subsequently, the session hands over to a 3GPP access system.

The steps involved in the handover from a trusted/untrusted non-3GPP IP access to 3GPP Access connected to EPC are depicted below when DSMIPv6 is used on S2c over non-3GPP system.

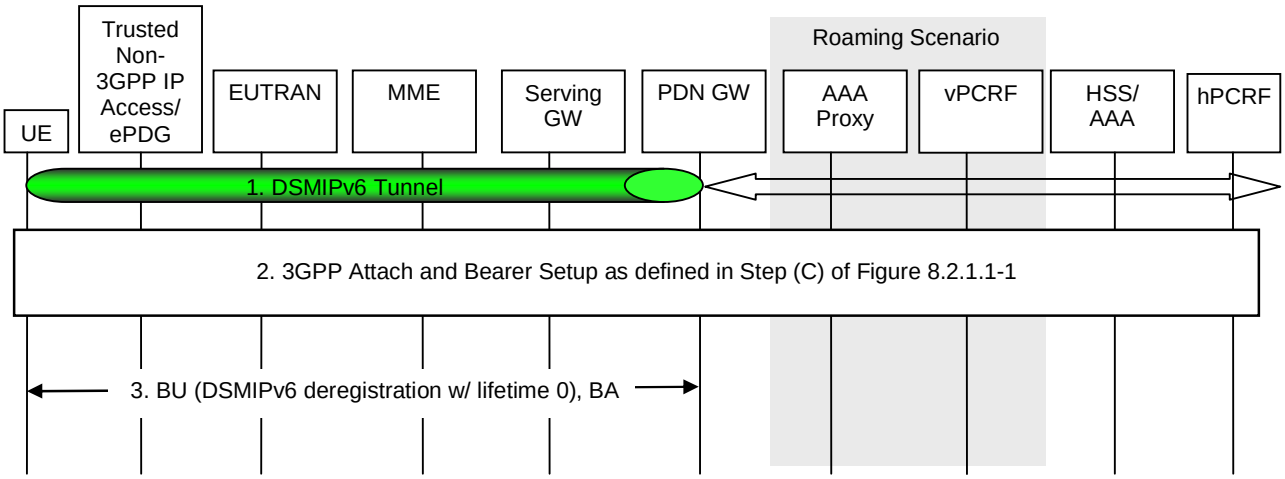


Figure 8.4.1-1: Trusted Non-3GPP S2c (DSMIPv6) to 3GPP with S5 handover

NOTE: In case of connectivity to multiple PDNs, step 18 of Figure 8.2.1.1-1 and steps 3 of Figure 8.4.1-1 are repeated for each PDN the UE is connected to. Other impacts related to the handover for multiple PDNs are described in Section 8.1.

1) The UE uses a trusted or untrusted non-3GPP access system. It has a DSMIPv6 session with the PDN GW.

2) The UE discovers and attaches to the 3GPP access as defined in Step (C) of Figure 8.2.1.1-1.

3) The UE sends a BU (lifetime) to the PDN GW to de-register its DSMIPv6 binding, as defined in draft-ietf-mip6-nemo-v4traversal [10] that was created while the UE was in non-3GPP access system. The PDN GW responds with a BA message as defined in draft-ietf-mip6-nemo-v4traversal [10].

According to RFC 4877 [22] the security associations should not be immediately deleted. As the security associations were created dynamically using IKEv2 they will be automatically deleted when they expire. The IP address used by the UE as home address is not released by the UE and the PDN GW as a result of the deletion of such security associations if the UE remains connected to the PDN GW. This applies also to the scenario where the UE performed the initial attach over a 3GPP access and was given a IP address, bootstrapped the DSMIPv6 over the 3GPP access, performed an handover to the non-3GPP access using S2c, and is now performing an handover towards 3GPP access and therefore returning to the Home Link.

8.4.2 3GPP Access to Trusted Non-3GPP IP Access Handover with DSMIPv6 over S2c

In this scenario, the session starts in 3GPP access (e.g. E-UTRAN) using PMIPv6 or GTP over S5 or no S5 is used (co-located Serving GW and PDN GW). The session hands over to the trusted non-3GPP access system that does not use PMIPv6 where the UE will receive a different prefix than the one it was using in 3GPP access system. The UE subsequently initiates DSMIPv6 with the same PDN GW to maintain the IP session.

Support of PCC for Trusted non-3GPP accesses is optional. The PCC interactions shown in Figure 8.4.2-1 are omitted if the Trusted non-3GPP access does not support PCC. If PCC is not supported, policy rules may be configured by other means.

In the non-roaming case, none of the optional entities in Figure 8.4.2-1 are involved.

The optional entities are involved in other cases.

- In the roaming cases, however, the 3GPP AAA Proxy mediates all interaction between the 3GPP AAA Server in the PLMN and entities in the VPLMN and non-3GPP access.
- Similarly, interaction between hPCRF in the HPLMN and entities in the VPLMN and non-3GPP access occurs by way of the vPCRF in the VPLMN. In both these cases, messages are relayed by the optional entities towards and from the HPLMN.

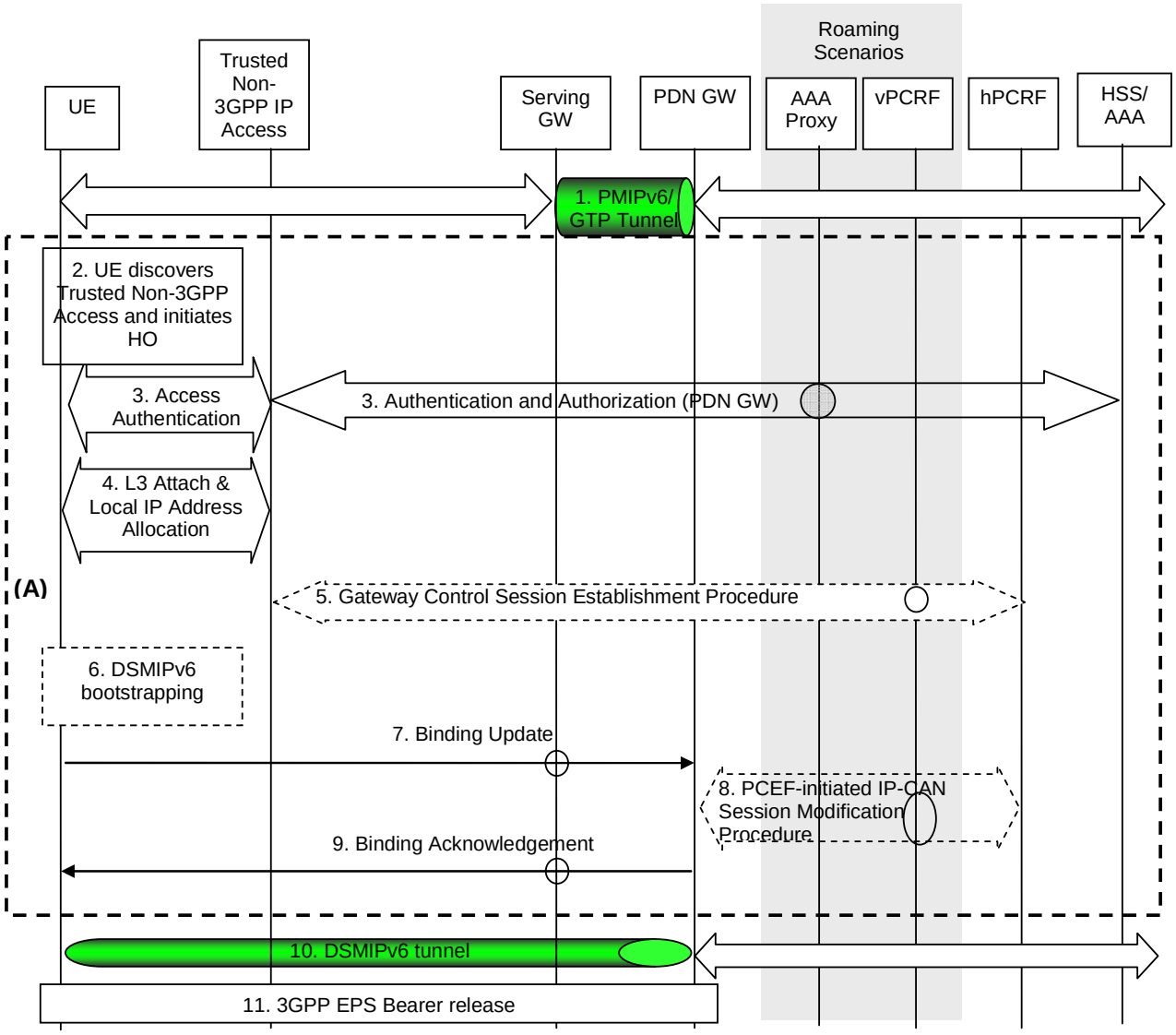


Figure 8.4.2-1: 3GPP S5 to Trusted Non-3GPP S2c (DSMIPv6) Handover

NOTE: In case of connectivity to multiple PDNs, Steps 6 to 9 are repeated for each PDN the UE is connected to. Other impacts related to the handover for multiple PDNs are described in Section 8.1

1) The UE uses a 3GPP access system. It has an IP address that is supported over S5 interface.

2) At this point the UE decides to initiate non-3GPP access procedure. The decision is based on any number of reasons e.g. local policies of the UE.

3) The UE performs access authentication and authorization in the non-3GPP access system. The 3GPP AAA server authenticates and authorizes the UE for access in the non-3GPP system. In the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN, as specified in TS 23.234 [5]. As part of the AAA exchange for network access authentication, the 3GPP AAA Server and/or the 3GPP AAA Proxy may return to the non-3GPP access system a set of home/visited operator's policies to be enforced on the usage of local IP address, or IPv6 prefix, allocated by the access system upon successful authentication.

4) The UE performs L3 attach and gets an IP address that is different from the IP address it was using in 3GPP access system.

5) The access gateway requests a new PCC session towards the PCRF (5a) by sending an Indication of IP-CAN session establishment (local IP address/prefix, IP-CAN type), where local IP address/prefix is the IPv4 address or IPv6 prefix allocated to the UE by the Trusted non-3GPP access.

   Based e.g. on the UE identity and user profile, operator's policies and the IP-CAN type, the PCRF decides on the QoS policy rules and completes the PCC session establishment towards the access gateway (5b)

   In the roaming case, PCC signalling is sent via a vPCRF server in the VPLMN

6)If bootstrapping was not performed prior to the handover defined here, the UE may discover PDN GW address using MIPv6 bootstrapping procedures defined in clause 4.5.2. If the PDN GW discovered by the UE upon MIPv6 bootstrapping is different from the PDN GW that was in use on the 3GPP access, a PDN GW reallocation as per steps 2-6 in clause 6.10 is performed. The target PDN GW that is communicated to the UE as part of the reallocation procedure must be exactly the PDN GW that was serving the UE while on the 3GPP access.

7) The UE sends a DSMIPv6 BU message to the PDN GW to register its CoA.

8) If PCC is supported, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19].

   In the roaming case, PCC signalling is sent via a vPCRF server in the VPLMN.

9) The PDN GW sends the MIP Binding Ack to the UE. The PDN GW triggers the bearer release in the 3GPP Access using the PDN GW initiated Bearer Deactivation procedure. Radio Bearers associated with the PDN address are released if existing. Since this step is triggered by the Binding Update message from the UE in step 7, it can occur after step 7 and does not need to wait for step 8.

   The PDN GW may send message 9 before the procedure in step message 8 is complete.

10) The UE continues with IP service using the same IP address.

11) The PDN GW shall initiate resource allocation deactivation procedure in 3GPP access as defined in clause 5.4.5.2.

8.4.3 3GPP Access to Untrusted Non-3GPP IP Access Handover with DSMIPv6 over S2c

In this scenario, the session starts in 3GPP access (e.g. E-UTRAN) using either GTP or PMIPv6 is used over S5, or no S5 is used (co-located Serving GW and PDN GW).). In the roaming case instead of S5, S8 is used. The session hands over to an untrusted non-3GPP access system that does not use PMIPv6 where the UE will receive a different prefix from the ePDG than the one it was using in 3GPP access system The UE subsequently initiates DSMIPv6 with the its PDN GW to maintain the IP session.

Support of PCC for Untrusted non-3GPP accesses is optional. The PCC interactions shown in Figure 8.4.3-1 are omitted if the Untrusted non-3GPP access does not support PCC. If PCC is not supported, policy rules may be configured by other means.

In the non-roaming case, none of the optional entities in Figure 8.4.3-1 are involved.

The optional entities are involved in other cases.

- In the roaming cases, however, the 3GPP AAA Proxy mediates all interaction between the 3GPP AAA Server in the PLMN and entities in the VPLMN and non-3GPP access.

- Similarly, interaction between hPCRF in the HPLMN and entities in the VPLMN and non-3GPP access occurs by way of the vPCRF in the VPLMN. In both these cases, messages are relayed by the optional entities towards and from the HPLMN.

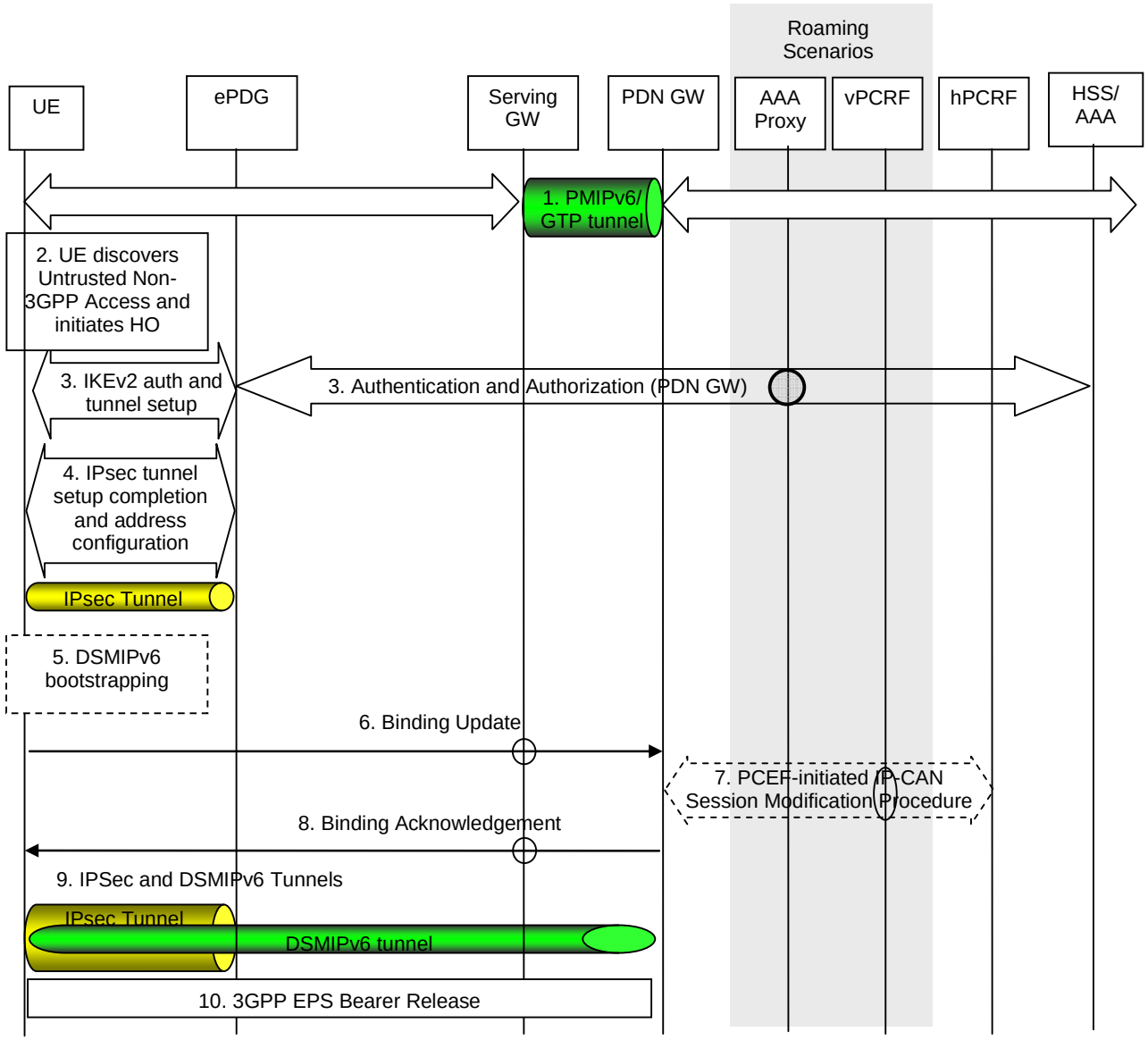


Figure 8.4.3-1: 3GPP Access to Untrusted Non-3GPP IP Access with S2c (DSMIPv6) Handover

NOTE: In case of connectivity to multiple PDNs, Steps 6 to 8 are repeated for each PDN the UE is connected to. Other impacts related to the handover for multiple PDN GWs are described in Section 8.1

1. The UE uses a 3GPP access system. It has an IP address that is supported over S5 interface.

2. At this point the UE decides to initiate non-3GPP access procedure. The decision is based on any number of reasons e.g. local policies of the UE.

Editor's note: The criteria / policy used in determining when handover to 3GPP access should be invoked are FFS.

3. The IKEv2 tunnel establishment procedure is started by the UE. The UE may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The ePDG IP address to which the UE needs to form IPsec tunnel is discovered via DNS query as specified in clause 4.5.4. After the UE is authenticated, UE is also authorized for access to the APN. The procedure is as described in TS 33.234 [7].

NOTE: It is assumed that the access system is aware that network-based mobility procedures do not need to be initiated.

The ePDG sends the final IKEv2 message with the assigned IP address in IKEv2 Configuration payloads. IPsec Tunnel between the UE and ePDG is now setup.

4. The IKEv2 procedure is completed and the IPSEC tunnel is set-up. As a result of this procedure, an IP address or an IPv6 prefix is also assigned to the UE by the access system (i.e. a Local IP address that will be used as a Care-of Address for DSMIPv6 over the S2c reference point).

5. If bootstrapping was not performed prior to the handover defined here, the UE may discover PDN GW address using DSMIPv6 bootstrapping procedures defined in clause 4.5.2. If the PDN GW discovered by the UE upon MIPv6 bootstrapping is different from the PDN GW that was in use on the 3GPP access, a PDN GW reallocation as per steps 2-6 in clause 6.10 is performed. The target PDN GW that is communicated to the UE as part of the reallocation procedure must be exactly the PDN GW that was serving the UE while on the 3GPP access.

6. The UE sends a DSMIPv6 BU message to the PDN GW to register its CoA.

7. If PCC is supported, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW in the VPLMN or HPLMN to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

8. The PDN GW sends the DSMIPv6 Binding Ack to the UE. The PDN GW triggers the bearer release in the 3GPP Access using the PDN GW initiated Bearer Deactivation procedure. Radio Bearers associated with the PDN address are released if existing. Since this step is triggered by the Binding Update message from the UE in step 6, it can occur after step 6 and does not need to wait for step 7.

   The PDN GW may send message 8 before the procedure in step 8 is complete.

9. The UE continues with IP service using the same IP address.

10. The PDN GW shall initiate resource allocation deactivation procedure in 3GPP access as defined in clause 5.4.5.2.

8.5 Handover with Access Network Discovery and Selection

8.5.1 Handover between 3GPP Access and Trusted / Untrusted Non-3GPP IP Access with access network discovery and selection

The figure below shows the main steps involved in a handover between a 3GPP access and a non-3GPP IP access (also called and inter-system handover) when network discovery and selection information is provided by the network (see clause 4.8). This information is provided in order to control the UE's inter-system handover decisions and in order to reduce the battery consumption for inter-system mobility.

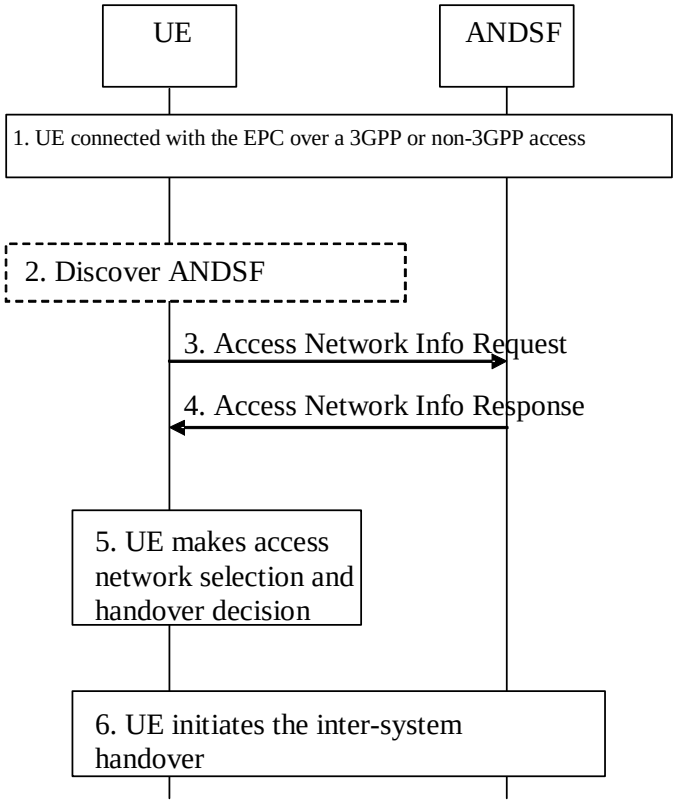


Figure 8.5.1-1: Handover between 3GPP Access and trusted / untrusted non-3GPP IP Access with Access Network Discovery and Selection

1. The UE is connected with a source access network (either a 3GPP access or a trusted / untrusted non-3GPP IP access). Its radio interfaces not connected to any access network may be in power saving or powered down mode.

2. If the inter-system mobility policies (see clause 4.8) in the UE indicate that inter-system mobility is allowed with at least one access technology type, then the UE may decide to discover neighbour access networks with assistance by the network. In this case, the UE discovers the address of ANDSF (if needed) as specified in clause 4.8 and requests access network info from the ANDSF as specified in the steps below.

3. The UE sends an Access Network Info Request (UE Capabilities, UE Location) message to the ANDSF to retrieve network discovery and selection information. The UE Capabilities indicate the capabilities of the UE pertaining to access network discovery, such as the access technology types that can be supported by the UE. The UE Location may be included in the message to indicate the UE's current location (e.g. cell identity or other location data). If the UE Location is not included then other mechanisms may be used by ANDSF to identify the UE's current location.

Editor's note: It is FFS if the ANDSF can request and retrieve the current UE's location.

4. The ANDSF responds with an Access Network Info Response (Available Access Network Info, Updated Inter-system Mobility Policies) message to the UE. The Available Access Networks Info contains a list of access networks that are available in the vicinity of UE. If the UE included one or more access technology types in the Access Network Info Request, then information about neighbour access network with the requested access technology types is included. The Updated Inter-system Mobility Policies may be included in order to update / install operator defined rules / preferences in the UE. These rules / preferences may indicate a preference value for an available access network and help the UE select an available access network that is more preferable to the current access network.

5. The UE powers up its appropriate radio interface(s) and measures the available access networks for which inter-system mobility is allowed, as indicated by the updated / current inter-system mobility policies. The UE selects the most preferable available access network for inter-system mobility.

6. If the UE selects a preferable access network for handover, then the UE initiates handover to the selected access network according to the S2a/S2b/S2c procedures described in clause 8.

NOTE: Steps 2, 3 and 4 in the above procedure may not immediately result in an inter-system handover.

9 Handovers with Optimizations Between E-UTRAN Access and CDMA2000 Accesses

9.1 Architecture and Reference Points

9.1.1 Architecture for Optimized Handovers between E-UTRAN Access and cdma2000 HRPD Access

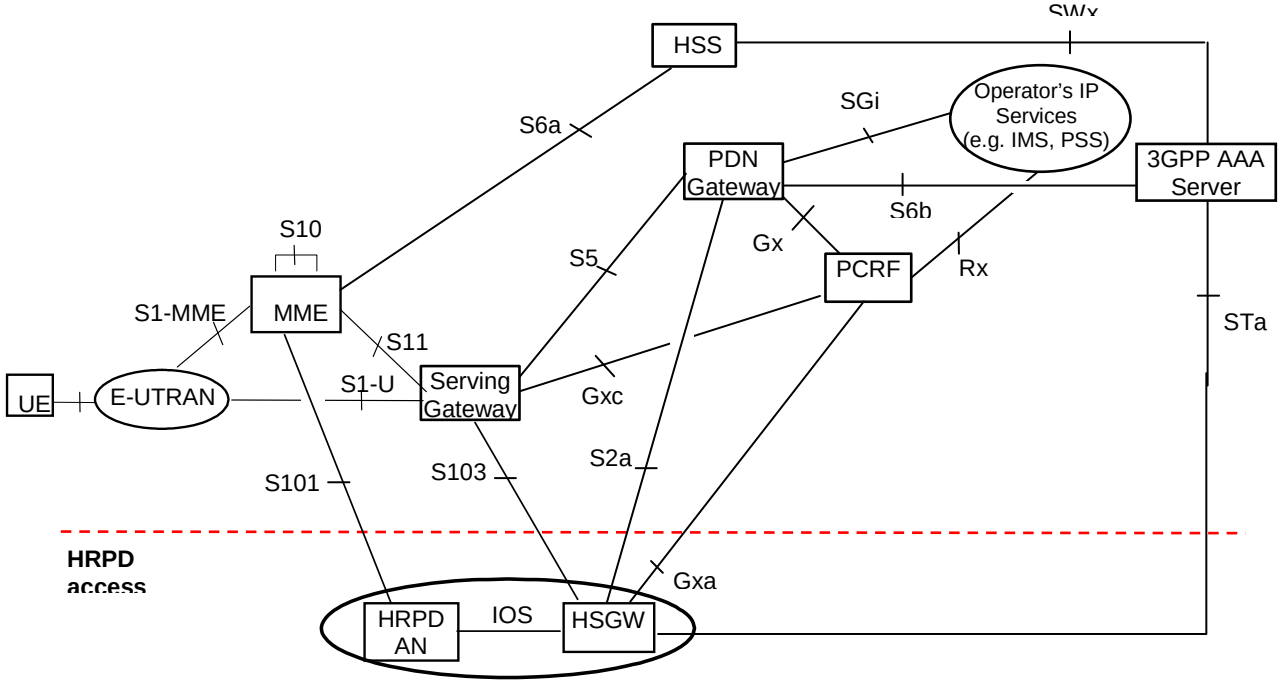


Figure 9.1.1-1: Architecture for optimised handovers between E-UTRAN access and cdma2000 HRPD access (non-roaming case)

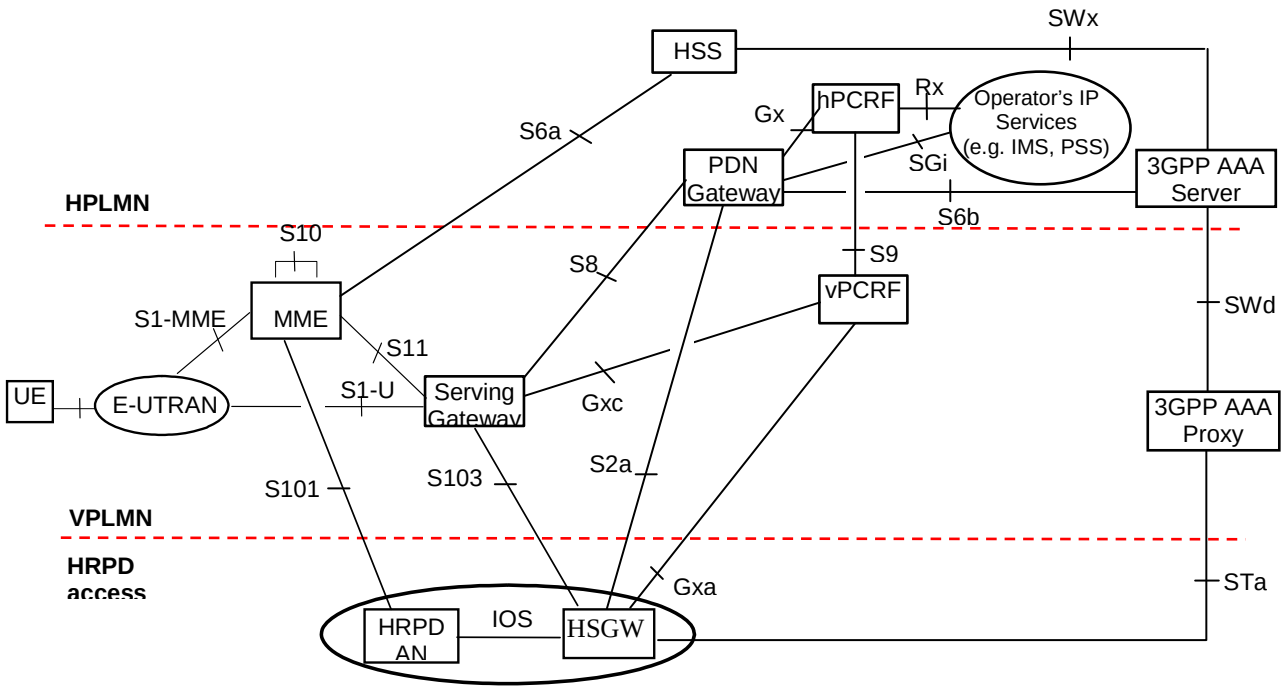


Figure 9.1.1-2: Architecture for optimised handovers between E-UTRAN access and cdma2000 HRPD access (roaming case; Home routed)

NOTE 1: Optimized handover supported by this architecture is intended for the scenario where the operator owns both the E-UTRAN access and the HRPD access, or where there is a suitable inter-operator agreement in place.

NOTE 2: Gxc is used only in the case of PMIP variant of S5 or S8.

NOTE 3: For further specification of the functions and interfaces of the HRPD Serving GW (HSGW) refer to 3GPP2 X.P0057 [51].

Depicted in Figure 9.1-1 is an access specific architecture providing support for optimised 3GPP-HRPD handovers. in the non-roaming case. Depicted in figure 9.1.1-2 is an access specific architecture providing support for optimised 3GPP-HRPD handovers in the roaming case with Home routed traffic.

9.1.2 Reference Points

9.1.2.1 Reference Point List

S101: It enables interactions between EPS and HRPD access to allow for pre-registration and handover signalling with the target system.

S103: This User Plane interface is used to forward DL data to minimize packet losses in mobility from E-UTRAN to HRPD.

9.1.2.2 Requirements for the S101 Reference Point

The S101 interface supports procedures for Pre-Registration, Session Maintenance and Active handovers between E-UTRAN and HRPD networks. This is based on tunnelling over S101 signalling of one technology while the UE is in the other technology. The HRPD air interface messages tunnelled over S101 in E-UTRAN to HRPD mobility are defined in 3GPP2 C.S0087-0 [49].

The S101 reference point shall support the following requirements:

- HPRD and E-UTRAN/EPS messages shall be transported as opaque containers without modifications by the MME or HRPD AN.

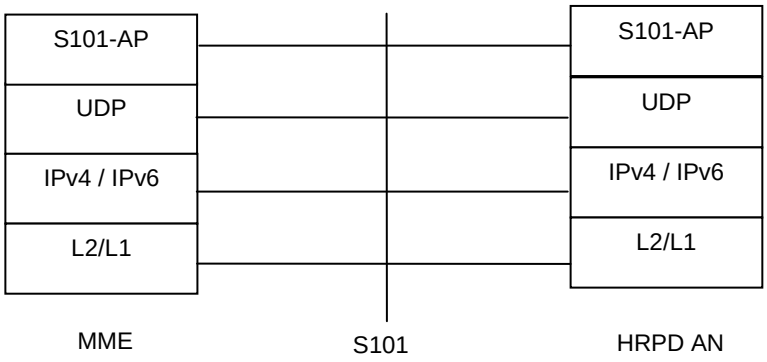
- Messages may carry separate information IEs to indicate status, message types (e.g. handover command) forwarding addresses etc. as required by signaling procedures.

- Provide identifiers (i.e. S101 Session ID) to distinguish messages belonging to different UEs in order to allow responses originating from the target system to an UE to be appropriately forwarded to the UE by the source system.

- Reliable transport for S101 messages should be provided at the application layer and will not require transport layer reliability mechanism.

9.1.2.3 S101 Protocol Stack

The figure below shows the protocol stack for the S101 interface.



Legend:
- S101 Application Protocol (S101-AP): It is the Application Layer Protocol between the MME and HRPD AN
- User Datagram Protocol (UDP): This protocol transfers messages. UDP is defined in RFC 768 [xx].
- S101 Application Protocol (S101-AP) provides application layer reliability for its messages, if required.

Figure 9.1.2.3-1: Protocol Stack for the S101 Reference Point

9.1.2.4 S101 Session Identifier

All S101 messages contain a S101 Session ID which serves to identify the UE context at the MME and the HRPD AN. The S101 Session ID is a scalar value and is unique on the instance of the S101 interface between a HRPD AN and an MME. The S101 Session ID is created by the node (i.e. either the MME or the HRPD AN) which sends the first S101 message on the interface for the UE. The S101 Session Identifier is valid on the interface between a HRPD AN and an MME as along as both ends possess the UE context / session. When either end changes due to procedures such as MME relocation or HRPD dormant session handover, a S101 Session ID unique to the interface is selected for the UE between the two new pair of nodes. The S101 Session ID is structured to partition the identifier space to allow end points to create session identifiers which are unique on this interface. Once a S101 Session ID is established for the UE on an interface instance by an end point (either the MME or the HRPD AN), both nodes will include the S101 Session ID in all S101 signalling messages without modification as long as both end points possess the UE context.

9.1.2.5 Requirements for the S103 Reference Point

The S103 interface between the Serving GW and HRPD PDSN supports the forwarding of DL data during mobility from E-UTRAN to HRPD. Signalling procedures on the S101 interface are used to set up tunnels on the S103 interface.

The S103 reference point shall support the following requirements:

- The S103 interface shall support the ability to tunnel traffic on a per-UE, per-PDN basis

- The S103 interface shall support Generic Routing Encapsulation (GRE) RFC 2784 [23] including the Key Field extension RFC 2890 [24]. The Key field value of each GRE packet header uniquely identifies the PDN connectivity that the GRE packet payload is associated with.

9.1.2.6 S103 Protocol Stack

The figure below shows the protocol stack for the S103 interface.

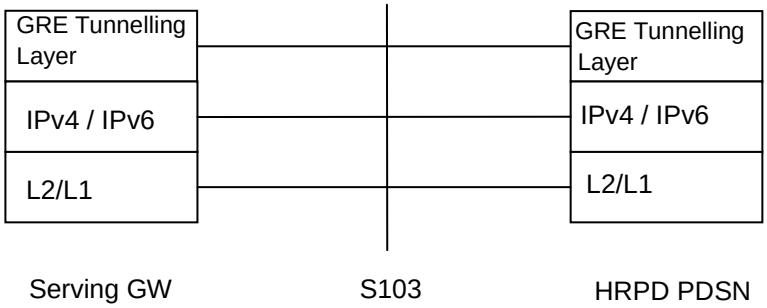


Figure 9.1.2.6-1: Protocol Stack for the S103 Reference Point

Legend:

- On the S103 interface, the tunnelling layer implements GRE encapsulation with the Key Field extension RFC 2784 [23], RFC 2890 [24].

9.2 Overview of Handover Procedures

The S101 reference point, and E-UTRAN and HRPD access is used for transparent transfer of pre-registration and handover signalling between the UE and the target access system

The purpose of the procedures is to minimise the total service interruption time experienced at the UE, by allowing the UE to attach and perform service activation (in the case of E-UTRAN) or to perform a session configuration or traffic allocation request (in the case of HRPD) in the target access system before leaving the source access system.

In case where the UE is connected to the E-UTRAN 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.

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.

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

This section describes the Optimised Handover from E-UTRAN Access to cdma2000 HRPD Access in two phases, pre-registration and the actual handover. In pre-registration phase the UE registers to the cdma2000 HRPD Access, while the UE remains to be connected to the E-UTRAN. The pre-registration may take place well in advance of the need to make the actual handover. In the handover phase, the connection is handed over to cdma2000 HRPD Access, and the UE leaves E-UTRAN.

9.3.1 Pre-registration Phase

Figure 9.3.1-1 illustrates a high-level call flow for the optimised E-UTRAN to HRPD handover procedure, Pre-registration phase.

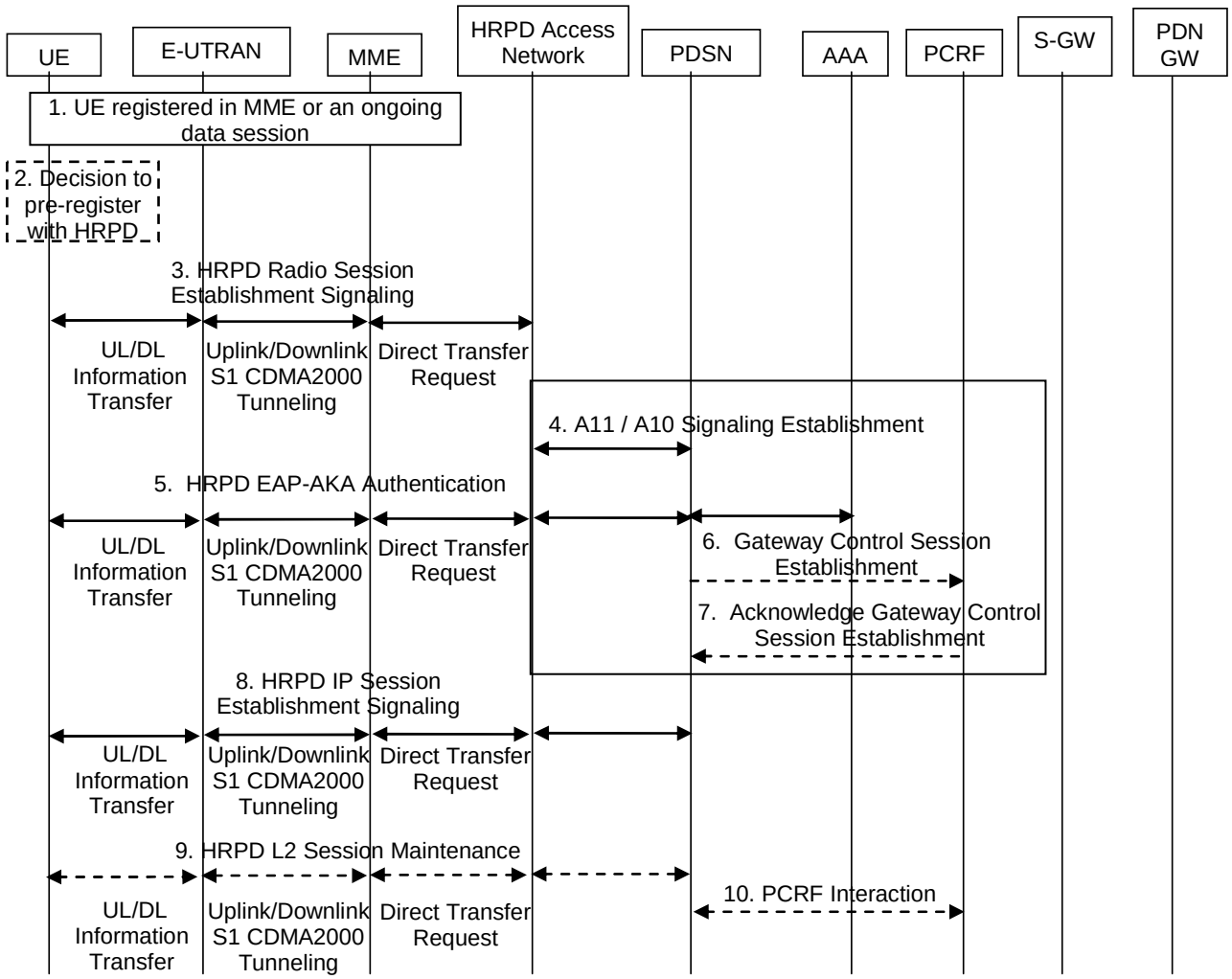


Figure 9.3.1-1: HRPD registration via LTE/SAE tunnel

1. The UE is registered with E-UTRAN/MME. It may have an ongoing data session established over EPS/E-UTRAN access.

2. Based on a Radio Layer trigger (e.g., an indication from the E-UTRAN when the UE is in connected state or an indication over the broadcast channel), the UE decides to initiate a pre-registration procedure with potential target HRPD access. The pre-registration procedure allows the UE to establish and maintain a dormant session in the target HRPD access, while attached to the E-UTRAN/MME.

3. Registration to the HRPD is achieved by exchanging a series of HRPD messages between the UE and the HRPD Access Network. The HRPD signalling that is tunneled transparently over the E-UTRAN and EPC creates an HRPD session context between the UE and the HRPD Access Network. The procedures described below are used in steps 3, 5, 8 and 9.

   The UE generates an UL Information Transfer message (UL HRPD message, CDMA2000 message type). The UL HRPD message is transferred from the UE to the eNB as a parameter in the UL Information Transfer.

   The eNB sends Uplink S1 CDMA2000 Tunneling message (UL HRPD message, Sector ID) to the MME. The SectorID is statically configured in the eNB.

   The MME selects an HRPD access node address. In order to be able to distinguish S101 signalling transactions belonging to different UEs, the MME allocates an S101 Session ID to identify signalling related to that UE on S101. The MME sends a Direct Transfer Request message (S101 Session ID, SectorID, UL HRPD message) to the HRPD access node. The MME determines the correct HRPD access node entity from the SectorID.

   The HRPD Access Network sends signalling in the DL direction to the MME using Direct Transfer Request message (S101 Session ID, DL HRPD message). The S101 Session ID is used to associate the signalling to a particular UE.

The MME sends the information on to the eNB using the Downlink S1 CDMA2000 Tunneling message (DL HRPD message).

The eNB uses the DL information transfer message (DL HRPD message) to transport the signalling the UE.

4. The HRPD Access Network creates a signalling relationship with the PDSN for the UE with interactions in HRPD network A10 / A11 interfaces.

5. The UE, PDSN, and 3GPP AAA exchange EAP-AKA signalling to authenticate the UE on the HRPD system. The PDSN receives the selected P-GW address from AAA during authentication.

6. The PDSN sends a Gateway Control Session Establishment message to the PCRF.

7. The PCRF responds to the message, sending an Acknowledge Gateway Control Session Establishment message to the PDSN. This response includes the QoS Policy rules.

8. The UE and PDSN exchange signalling to establish context to support the bearer traffic environment in use over the E-UTRAN.

9. At any time prior to the Handover Phase, if session maintenance activity is required, the UE or HRPD access network shall perform session maintenance signalling by tunnelling the HRPD session maintenance messages over the S101. If QoS parameters require updating, then this step includes the PCRF interaction. The MME uses the S101 Session ID to identify the UE context over the S101 interface.

NOTE: Between Step 8 and Step 9 the UE may enter ECM-IDLE state. To execute the session maintenance procedures at Step 9 it is necessary for the UE to enter ECM-CONNECTED state.

9.3.2 Handover Phase

Figure 9.3.2-1 illustrates a high-level call flow for the optimised E-UTRAN to HRPD handover procedure, Handover phase.

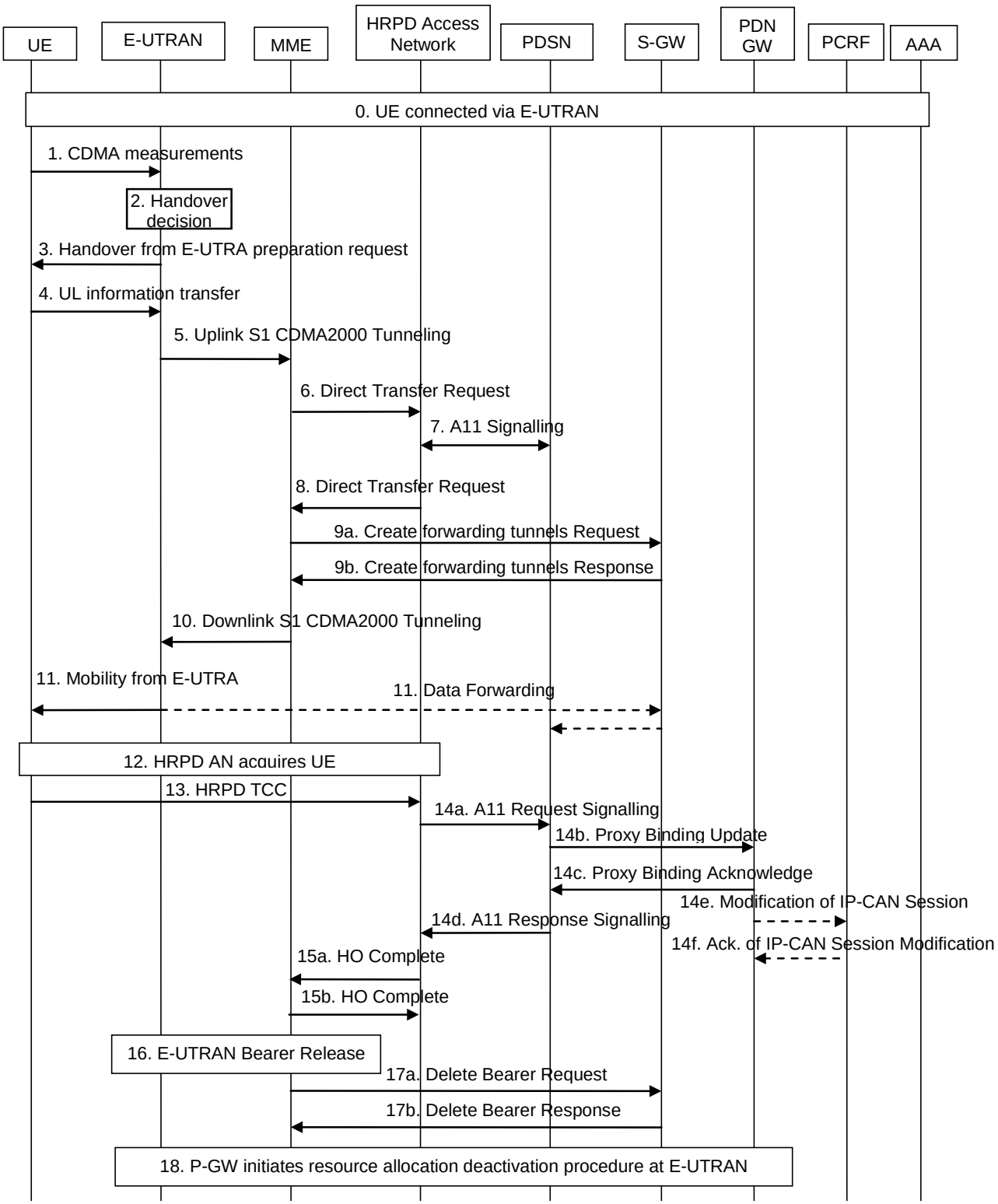


Figure 9.3.2-1: E-UTRAN to HRPD handover

0. Ongoing session established over EPS/E-UTRAN access.

1. The eNB receives measurement reports from the UE.

2. The eNB makes the handover decision.

3. The handover decision is signalled to the UE with Handover from E-UTRA preparation request message.

4. UE sends an UL handover preparation transfer message (HRPD message starting HO access, CDMA2000 message type) to the eNB. The HRPD message starting HO access will be carried transparently to the HRPD access node, and its purpose is to request information for accessing an HRPD traffic channel. The CDMA2000 message type parameter indicates to the eNB that the UE is responding to the Handover from E-UTRA preparation request message, and is requesting information for accessing an HRPD traffic channel.

5. The eNB sends the Uplink S1 CDMA2000 Tunneling message (HRPD message starting HO access, and SectorID, CDMA2000 HO Required Indication) to the MME. The SectorID is statically configured in the eNB. The eNB will also include CDMA2000 HO Required Indication IE to Uplink S1 CDMA2000 Tunneling message, which indicates to the MME that the handover preparation has started.

6. When receiving Uplink S1 CDMA2000 Tunneling message with CDMA2000 HO Required Indication the MME selects an HRPD access node. This selection bases on the SectorID. The MME allocates an S101 Session ID to identify signalling related to that UE on S101. The MME sends aDirect Transfer Request message (S101 Session ID, SectorID, PDN GW Address(es), GRE key(s) for uplink traffic, APN(s), HRPD message starting HO access) to the HRPD access node.

7. The HRPD access allocates the requested radio access resources, and requests a forwarding address from PDSN. The information sent in the request from the HRPD access to PDSN includes PDN GW Address(es) and GRE key(s) for uplink traffic. The response includes the PDSN Address and GRE key(s) for forwarded traffic on S103. There is one GRE key for each PDN connection for which traffic is to be forwarded.

8. The HRPD access sends the Direct Transfer Request message (S101 Session ID, HRPD message with HO access information, PDSN Address and GRE key(s) for forwarded traffic, CDMA2000 HO Status) to the MME. The PDSN Address and GRE key(s) for forwarded traffic are sent if data forwarding applies. If the HRPD access did not allocate the resources as requested, this will be indicated to the MME and eNB with the CDMA2000 HO Status IE, and the embedded HRPD message indicates the failure to the UE.

9a. If Direct Transfer Request message included PDSN Address and GRE key(s) for forwarded traffic, the MME determines which of the S1-U bearers should be forwarded to the HRPD and configures resources for indirect data forwarding by sending Create forwarding tunnels Request (PDSN address, GRE key(s) for forwarded traffic, EPS bearer ID(s) subject to forwarding) to the Serving GW.

9b. The Serving GW confirms data forwarding resources for S103 and allocates forwarding address for S1 in Create forwarding tunnels Response (cause, S-GW address, S1-U uplink TEID(s)). The S1-U uplink TEIDs are provided one per S1-U bearers subject to forwarding.

10. The MME sends the Downlink S1 CDMA2000 Tunneling message (HRPD message with HO access information, S-GW address, S1-U uplink TEID(s), CDMA2000 HO Status) to the E-UTRAN. If the CDMA2000 HO Status indicates that handover preparation failed, the Downlink S1 CDMA2000 Tunneling message will be sent with appropriate cause, and the embedded HRPD message that indicates the failure to the UE. The message from the MME provides the eNB also with the data forwarding S1-U uplink TEIDs allocated at the Serving GW.

11. The E-UTRAN forwards the HRPD message with HO access information to the UE in Mobility from E-UTRA message. This is perceived by the UE as a Handover Command message. If handover preparation failed, DL Information transfer message will be sent nstead, with the embedded HRPD message that indicates the failure to the UE.

    The E-UTRAN starts forwarding received downlink data to the S-GW on a per-S1-U bearer forwarding tunnel, which then forwards these packets on a per-PDN per-UE S103 tunnel to the PDSN. The forwarding starts at the same moment as the Mobility from E-UTRA message is sent to the UE.

12. The UE retunes to the HRPD radio access network and performs traffic channel acquisition.

13. The UE sends an HRPD Traffic Channel Complete (TCC) message to the HRPD access.

14a-e The E-UTRAN triggers switching the flow in the EPC with the following sequence:

    14a. The HRPD access sends A11 request signalling to PDSN to start setting up the U-Plane connection between the HRPD access and PDSN.

14b. The PDSN sends Proxy Binding Update to PDN GW. The PDSN sends the all zero IPv4 Home Address (0.0.0.0) or all zero IPv6 Home Prefix (0::/0) in the PBU message. In order to support session continuity, the P-GW performs the Binding Cache entry existence test based on the NAI and assigns the same IPv4 Home Address and/or IPv6 Home Prefix to the UE and acknowledge in the PBA message.

14c. The PDN GW switches the flow from Serving GW to PDSN, and sends Proxy Binding Acknowledge to PDSN.

14d. The PDSN responses with A11 response signaling to the HRPD access.

14e. The PDN GW sends a Modification of IP-CAN Session message to the PCRF. Otherwise, information configured with the PGW may be used to determine policy. Since Steps 14c and 14d are both triggered by the Proxy Binding Update in Step 14b, Steps 14c and 14d may occur in parallel.

14f. If the PDN GW sent a message in step 14d, the PCRF responds with an Ack. of IP-CAN Session Modification message, including the policy the PDN GW will enforce.

If multiple PDN connection information is provided in step 6, steps 14b-14e are performed for each PDN connection.

15a. The HRPD radio access network sends a HO Complete (S101 session ID) message to the MME (including the S101 session ID to identify the UE context).

15b. The MME responds by sending a HO Complete ACK (S101 session ID) to the HRPD radio access network.

16. The MME releases the E-UTRAN bearers based on the normal E-UTRAN procedure.

17a. This step is only performed in case of Serving GW resource is not released yet. The MME releases S-GW resources by sending a Delete Bearer Request (Cause, TEID) message to the Serving GW. The MME shall indicate to the Serving GW that the Serving GW shall not initiate a delete procedure towards the PDN GW.

17b. The Serving GW acknowledges resource removal with Delete Bearer Response (TEID) message.

18. At any time after step 14c, the PDN GW shall initiate resource allocation deactivation procedure at E-UTRAN as defined in clause 5.4.5.2.

9.4 Optimized Idle-mode Mobility: E-UTRAN Access to cdma2000 HRPD Access

This procedure is used in the case the UE has a dormant HRPD session in the target HRPD network, either through the pre-registration procedure or previous HRPD attachment.

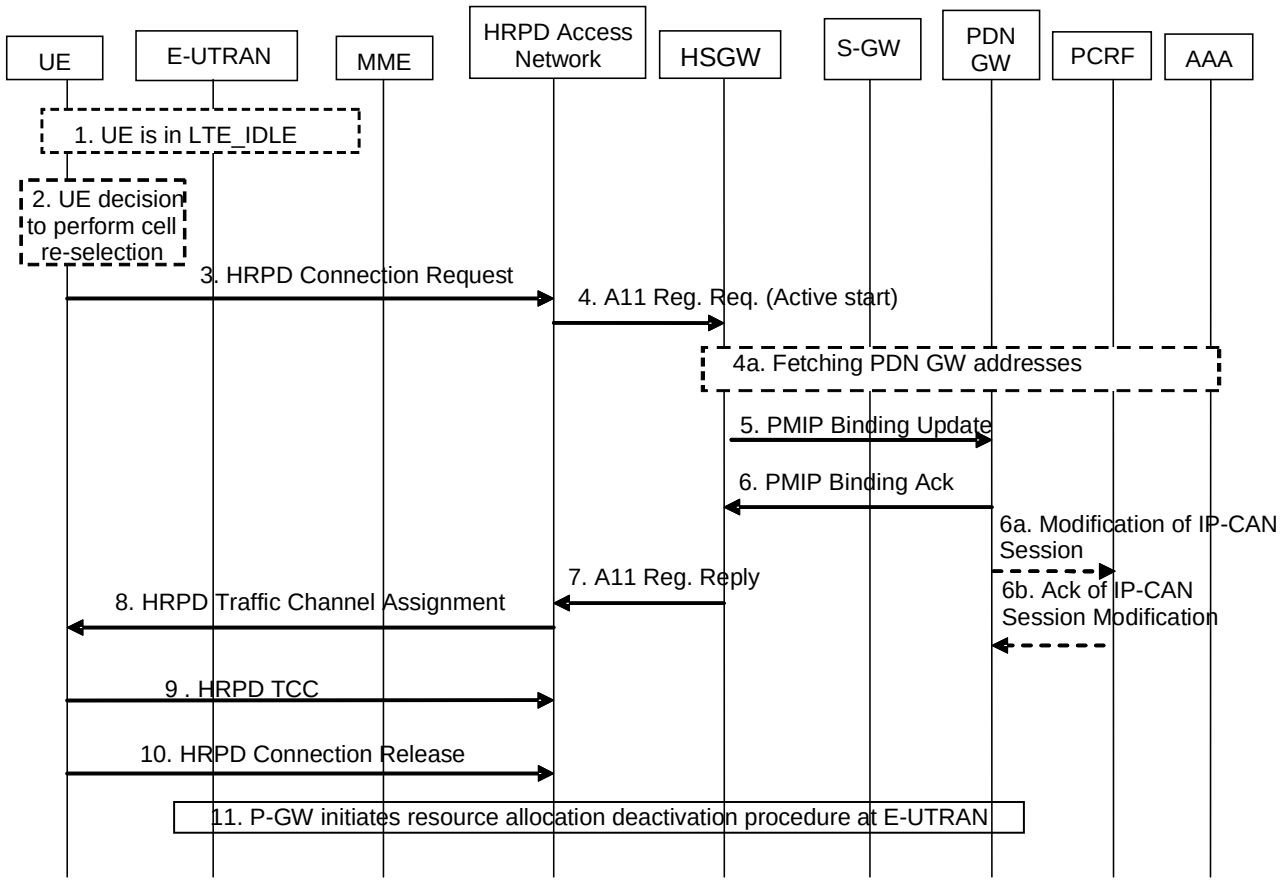


Figure 9.4-1: E-UTRAN to HRPD mobility in idle-mode

1. The UE is attached to E-UTRANLTE network and stay in ECM_IDLE state. The UE has a dormant HRPD session in the target HRPD network, either through the pre-registration procedure or previous HRPD attachment

2. The UE is in idle mode. Based on some trigger, the idle UE decides to perform cell re-selection to the HRPD system. Note, the cell re-selection decision can be made at any time when the UE is attached in the E-UTRAN network (including as soon as the UE has completed pre-registration).

3. The UE moves to HRPD radio and starts the idle mode mobility procedure. The UE sends an HRPD Connection Request message to request an HRPD traffic channel.

4. The HRPD access allocates the requested radio access resources and triggers the HSGW to switch from idle to active mode.

4a. The HSGW may fetch the PDN GW addresses of all active PDN connections from the AAA.

5~6. The HSGW exchanges a PMIP BU/BA with the PDN GW. The UE address information in PMIP BA returns the IP Address assigned to the UE. At this point the user plane is switched in the PDN GW towards the HRPD access network via the HSGW.

6a-6b. The PDN GW sends an Indication of IP-CAN Session Modification message to the PCRF and PCRF acknowledges. Since steps 6 and 6a are both triggered by the Proxy Binding Update in step 5, steps 6 and 6a may occur in parallel.

NOTE: For multiple PDN connections, steps 5-6 and 6a-6b are performed for each PDN connection.

7. The HSGW acknowledges the HRPD access.

8. The HRPD access replies to the UE with the HRPD Traffic Channel Assignment (TCA) message.

9. The UE sends an HRPD Traffic Channel Complete (TCC) message to the HRPD access.

10. Then the UE can go back to dormant mode by initiating the HRPD connection release procedure. Otherwise, at this step the UE traffic may flow in both uplink and downlink directions via the HRPD access.

11. At any time after step 6, the P-GW shall initiate resource allocation deactivation procedure in E-UTRAN as defined in clause 5.4.5.2.

9.5 Optimised Active Handover: cdma2000 HRPD Access to EUTRAN

9.5.1 General Procedure for GTP-based S5/S8

Figure 9.5.1-1 illustrates a high-level call flow for an optimised HRPD to EUTRAN handover procedure.

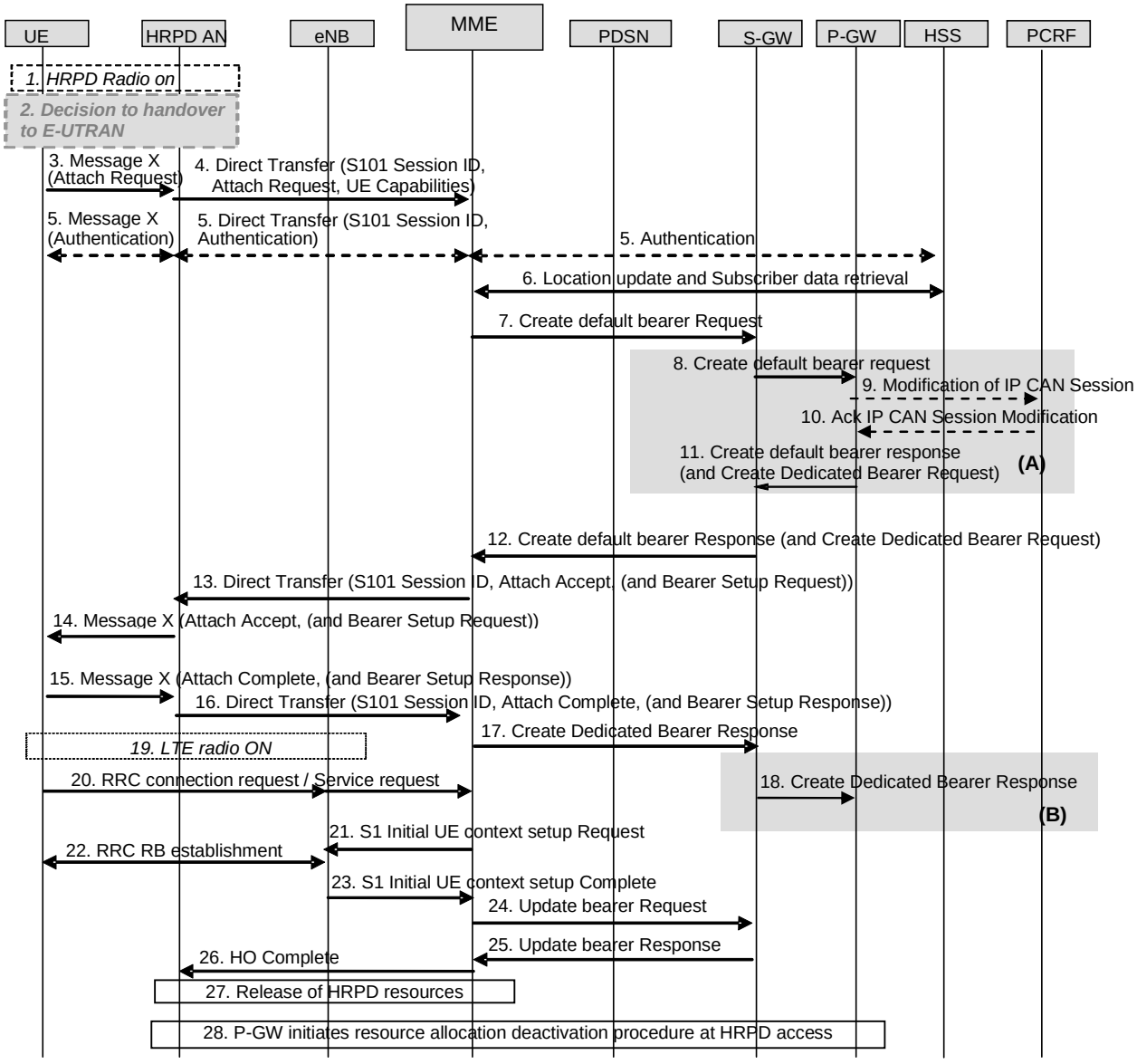


Figure 9.5.1-1: HRPD to EUTRAN handover with GTP-based S5/S8

Editors Note: Message name Message X need to be changed when 3GPP2 have decided their actual names.

NOTE 1: UE may need to perform a Tracking Area Update procedure in step 20.

NOTE 2: UE may perform E-UTRAN attach directly over the E-UTRAN radio.

1. The UE is registered with HRPD. If may have an ongoing data session established over HRPD access.

2. Handover decision occurs.

NOTE 4: The means by which a handover decision is made shall be specified in 3GPP2.

3. Upon handover decision, the UE initiates the Attach procedure by transmission of a NAS Attach Request message over tunneling mechanism to the HRPD AN.

4. When receiving Message X the HRPD AN selects an MME. This selection is based on a mapping from the current HRPD reference sector to corresponding MMEs. The HRPD AN allocates an S101 Session ID to identify signalling related to that UE on S101. The HRPD AN sends an S101 DT to the MME.

NOTE 5: It is assumed that the NAS UE capabilities shall be transferred as part of the Attach Request. AS UE capabilities shall be obtained by the eNB using existing RRC procedures.

5. If no UE context for the UE exists anywhere in the network, authentication must be performed. If UE was unknown to the target MME and the old MME, target MME will send an Identity Request to request the UE's IMSI prior to step 5. PDN GW identity is sent from HSS to MME in this step. These messages are tunnelled to/from the UE via the HRPD tunnelling mechanism and the S101 Direct Transfer capability.

6. If the MME has changed since the last detach, or if it is the very first attach, the MME sends an Update Location) to the HSS. Also, The HSS sends Insert Subscriber Data message to the new MME. MME performs checks on the UE, if all checks are successful then the MME constructs a context for the UE and returns an Insert Subscriber Data Ack message to the HSS. The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. HSS also sends the subscriber data to the MME in this step.

7. The MME selects a Serving GW as described in TS23.401 and sends a Create Bearer Requestmessage to the selected Serving GW.

8. The Serving GW creates a new entry in its EPS Bearer table and sends a Create Bearer Request message to the PDN GW.

9. The PDN GW sends an IP-CAN Session Modification message (IP-CAN Type) to the PCRF to obtain any new QoS policy and charging rules for all the active sessions as a result of the handover procedure.

10. The PCRF sends to the PDN GW an Acknowledge IP-CAN Session Modification message (PCC Rules) including QoS policy and charging rules for the new IP-CAN type.

11. The PDN GW returns a Create Bearer Response message to the Serving GW, with the proper TEIDs and bearer-related information. After this step, the path switch has occurred. The PDN GW may send a Create Dedicated Bearer Request message combined with the Create Default Bearer Response message, which starts the Dedicated Bearer Activation Procedure.

12. The Serving GW returns a Create Default Bearer Response message to the new MME. The Create Dedicated Bearer Request message may be sent together with the Create Default Bearer Response message.

13. Upon receiving the Create Default Bearer Response message, the MME sends an Attach Accept message (and the Bearer Setup Request message if Create Dedicated Bearer Request message was received) to the UE over the S101 interface. S-TMSI is included if the MME allocates a new S-TMSI.

14. The HRPD AN forwards the Attach Accept (and the Bearer Setup Request message) to the UE.

15. The UE sends the Attach Complete message (and the Bearer Setup Response message) over the HRPD AN tunnelling mechanism.

16. The HRPD AN forwards the Attach Complete message (and the Bearer Setup Response message) to the MME.

17. The MME sends a Create Dedicated Bearer Response message to Serving GW.

18. The Serving GW sends a Create Dedicated Bearer Response message to PDN GW.

19. Upon completion of the E-UTRAN Attach procedure, UE switches over to EUTRAN.

NOTE 6: Messages 20-25 are intended to be identical to the corresponding messages for UE Initiated Service Request Procedures as described in TS 23.401 [4].

20. UE performs the NAS service request procedure. The UE sends NAS message Service Request towards the MME encapsulated in an RRC message to the eNodeB. The RRC message(s) that can be used to carry this NAS

message are described in TS 36.300 [6]. The eNodeB forwards the NAS Service request message to MME. NAS message is encapsulated in an S1-AP: Initial UE Message. Details of this step are described in TS 36.300 [6].

21. The MME sends S1-AP Initial Context Setup Request message to the eNodeB.

22. The eNodeB performs the RRC radio bearer establishment procedure. The user plane security is established at this step. This step implicitly confirms the Service Request. This step is described in detail in TS 36.300 [6]. When user plane security has been established the EPS bearer state is synchronized between the UE and the network, i.e. the UE should remove any internal resources for bearers that are not set up.

    The uplink data from the UE can now be forwarded by eNodeB to the Serving GW. The eNodeB sends the uplink data to the Serving GW address and TEID provided in the step 14.

    For connectivity to multiple PDNs the UE initiates re-establishment of the additional PDN connections using the UE requested PDN connectivity procedure described in clause 5.6.1.

23. The eNodeB sends an S1-AP message Initial Context Setup Complete to the MME. This step is described in detail in TS 36.300 [6].

24. The MME sends an Update Bearer Request message to the Serving GW. The Serving GW is now able to transmit downlink data towards the UE.

25. The Serving GW sends an Update Bearer Response to the MME.

26. MME sends HO complete to the HRPD AN, so that it can release resources.

27. The HRPD resources may be released according to the 3GPP2 specific release mechanism.

28. At any time after step 9, the P-GW shall initiate the Resource Allocation Deactivation Procedure in HRPD network.

9.5.2 Using PMIP-based S5/S8

Figure 9.5.2-1 shows the steps that are different from the procedure for GTP based S5/S8 (see clause 9.5.1).

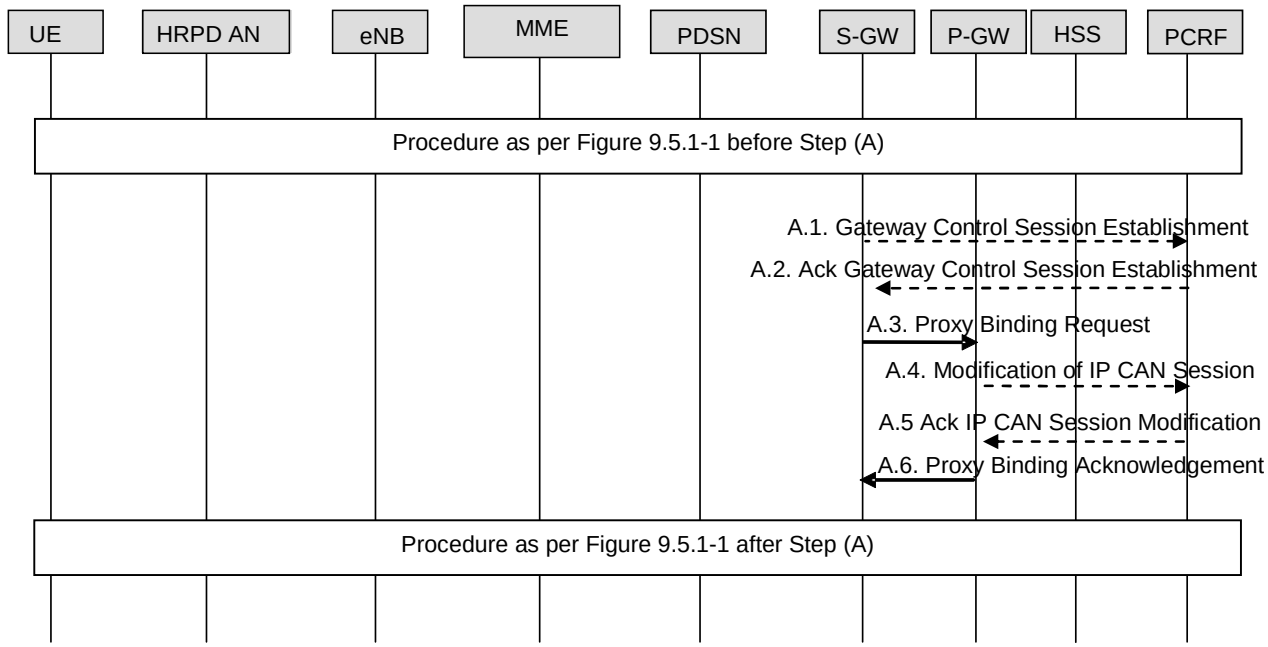


Figure 9.5.2-1: HRPD to EUTRAN handover with PMIP-based S5/S8

Steps before A.1 are described in clause 9.5.1.

A.1. The Serving GW sends a Gateway Control Session Establishment (IP-CAN Type, MN-NAI, APN, RAT Type) message to the PCRF to obtain the rules required for the Serving GW to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure. The Serving GW sends

information, including the IP-CAN Type supported by the Serving GW; the UE's MN-NAI to identify the subscriber; the APN requested, to be used in hPCRF selection to locate the PCRF function with the corresponding IP-CAN session established by the PDN GW; the RAT-type.

A.2. The PCRF sends to the Serving GW an Acknowledge GW Control Session Establishment (QoS Rules, Event Trigger) message including QoS policy rules enabling the Serving GW to perform the bearer binding. The Event Trigger specifies which events will result in the Serving GW sending event reports to the PCRF.

If the updated QoS rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place at step 12.

A.3. At same time of performing step 8, the Serving GW creates a new entry in its EPS Bearer table and sends a Proxy Binding Request message to the PDN GW.

A.4. The PDN GW sends an IP-CAN Session Modification (IP-CAN Type) message to the PCRF to obtain any new QoS policy and charging rules for all the active sessions as a result of the handover procedure.

A.5. The PCRF sends to the PDN GW an Acknowledge IP-CAN Session Modification (PCC Rules) message including QoS policy and charging rules for the new IP-CAN type.

A.6. The PDN Gateway returns a Proxy Binding Acknowledgement. After this step, the path switch has occurred.

Steps after A.6 are described in clause 9.5.1, except that step 18 is not performed.

9.6 Optimized Idle Mode Mobility: cdma2000 HRPD Access to E-UTRAN Access

This clause describes the optimized Idle Mode Handover from cdma2000 HRPD Access to E-UTRAN Access. The UE pre-registers to the E-UTRAN network while in HRPD-dormant mode in the cdma2000 HRPD Access.

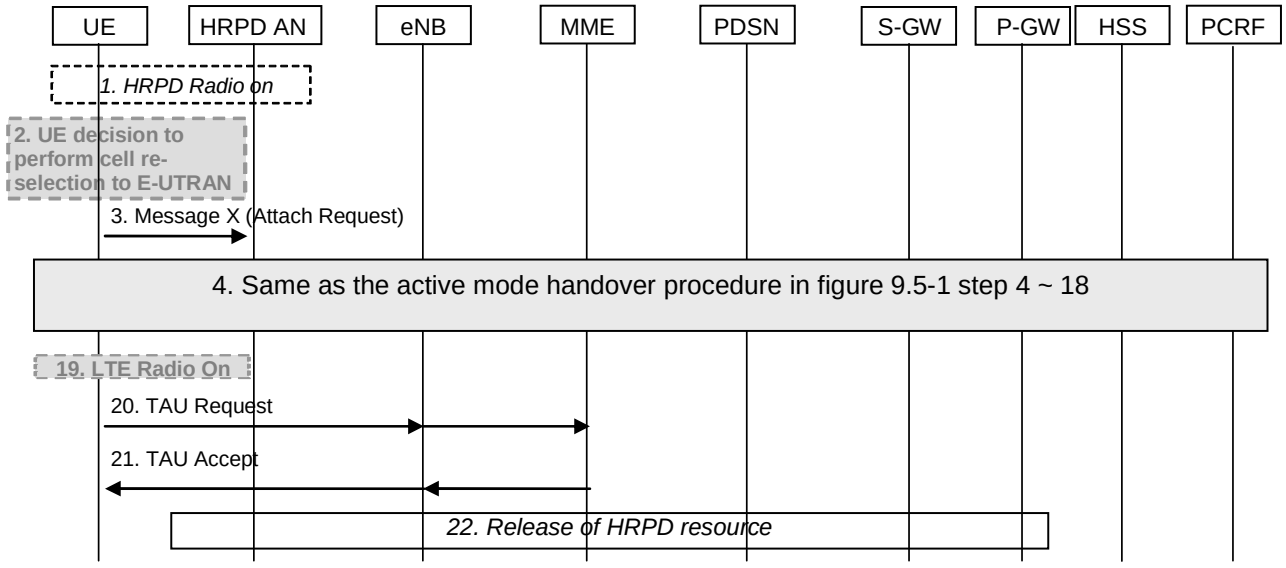


Figure 9.6.2-1: Optimized idle mode mobility from HRPD to E-UTRAN using GTP or PMIP based S5/S8

1. The UE is registered with HRPD and stays in HRPD-dormant mode.
2. The UE decides to handover to E-UTRAN network.
3. UE sends Attach Request message to HRPD access node to trigger the attach procedure to E-UTRAN.
4. This attach procedure is same as the active mode handover procedure in figure 9.5-1 steps 4-18.

19. The UE switches to E-UTRAN radio.

20. The UE synchronises with the target cell and sends a TAU message to the MME.

21. The MME returns a TAU Accept message to the UE.

22. HRPD resources are released.

9.7 S101 Tunnel Redirection Procedure

S101 Tunnel Redirection Procedure is used when the UE perform TAU with MME change while the UE has already triggered a pre-registration procedure from LTE to the HRPD as described in clause 9.3.1 and the S101 session exists from the MME and the HPRD Access Network.

The detail procedure for the idle case is depicted as figure 9.7-1.

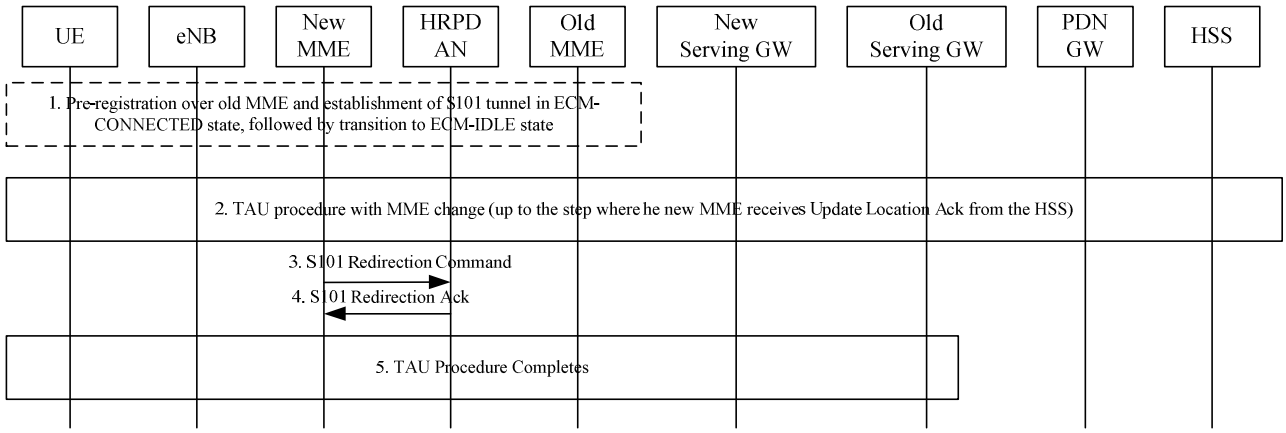


Figure 9.7-1: S101 tunnel redirection during TAU with MME change

1. UE performs pre-registration over the old MME while in ECM-CONNECTED state, followed by transition to ECM-IDLE state. The S101 tunnel exists between the old MME and the HRPD Access Network.

2. TAU procedure with MME change as described in TS 23.401 [4], figure 5.3.3.1-1, prior to the step where the new MME receives Update Location Ack from the HSS. The HRPD Access Network ID is transferred to the new MME via the Context Response message.

3. The new MME sends S101 Redirection Command message to the HRPD Access Network. After receiving this message, the HRPD Access Network associates the S101 tunnel for this specific UE with the new MME. Then the HRPD Access Network releases any context associated with the old MME.

4. In response to the S101 Redirection Command message, the HRPD Access Network sends a S101 Redirection Ack message to the target MME.

5. The TAU procedure is completed.

The detailed procedure for the active case is depicted as figure 9.7-2.

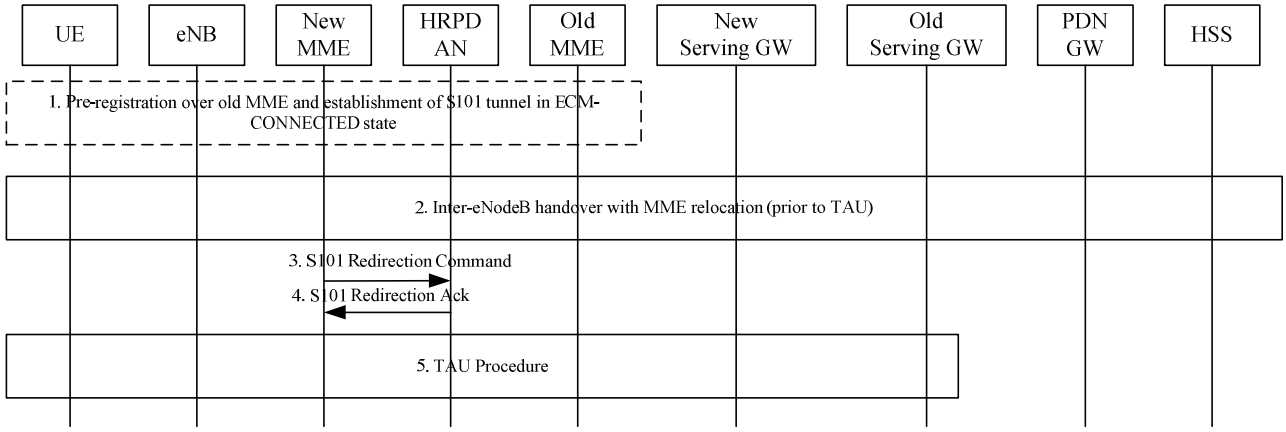


Figure 9.7-2: S101 tunnel redirection during inter-eNodeB handover with MME relocation

1. UE performs pre-registration over the old MME while in ECM-CONNECTED state. The S101 tunnel exists between the old MME and the HRPD Access Network.
2. Inter-eNodeB handover with MME relocation procedure as described in TS 23.401 [4], figure 5.5.1.2-1, steps prior to TAU. The HRPD Access Network ID is transferred to the new MME via the Forward Relocation Request message.
3. The new MME sends S101 Redirection Command message to the HRPD Access Network. After receiving this message, the HRPD Access Network associates the S101 tunnel with the new MME. Then the HRPD Access Network releases any context associated with the old MME.
4. In response to the S101 Redirection Command message, the HRPD Access Network sends a S101 Redirection Ack message to the target MME.
5. The TAU procedure occurs.

10 Handovers with Optimizations Between 3GPP Accesses and Mobile WiMAX

10.1 General Principles

The solution for network-controlled dual radio handover between 3GPP accesses (GERAN, UTRAN, E-UTRAN) and Mobile WiMAX is based on the concepts of clause 4.1.2, and in addition on the following principles.

1) The EPS shall support mechanisms for delivery of inter-system mobility, network discovery and selection policies over the Sx interface described in clause 4.8.

2) The policies shall contain information e.g. on availability of WiMax access networks that control the UE selection of available WiMax access network and the UE decision and triggering of 3GPP - WiMax handovers

Editor's Note: The definition of the exact semantic of the policies is work in progress.

3) The handover procedure will be executed according to the S2a/S2c procedures described in clause 8.

11 Handover Optimizations Applicable to All Non-3GPP Accesses

<This sub-section describes handover optimization procedures that are generic and applicable to all non-3GPP accesses. >

12 Interactions Between HSS and AAA Server

12.0 General

The interaction between the 3GPP AAA Server and the HSS is not explicitly presented in several figures of this specification. Though these entities are depicted as "AAA/HSS" in these figures, these functions are distinct and interact over the SWx reference point.

12.1 Location Management Procedures

The location management procedures between HSS and 3GPP AAA Server is described in this clause.

Non-3GPP access location management procedures define the process in which the 3GPP AAA Server interacts with the HSS for the following purposes:

- To register the current 3GPP AAA Server address in the HSS for a given 3GPP user. This procedure is invoked by the 3GPP AAA Server after a new subscriber has been authenticated by the 3GPP AAA Server (either at attach and handover). As part of the response, the HSS returns the subscriber's user profile data (QoS profile, user capabilities, etc.) to the 3GPP AAA Server.

- To register the current PDN GW identity and its association with the UE and APN in the HSS for a given user. The allocated PDN GW identity and APN associated with the UE's PDN Connection are provided by the AAA Server to the HSS at attachment to that particular PDN.

- To acquire the IP address(es) of the already allocated PDN Gateway(s) with the corresponding PDN information from the HSS over the SWx reference point. This is for the case when the UE has already been assigned PDN Gateway(s) due to a previous attach in a 3GPP access (when the UE is handed over from a 3GPP access to a non-3GPP access).

- To de-register the currently registered 3GPP AAA Server-address in the HSS for a given user and purge any related non-3GPP user status data in the HSS. The 3GPP AAA Server de-registers its address and purges user status data when e.g. the UE has disappeared from non-3GPP access coverage, when another EPC core network entity (e.g. charging system) has initiated a disconnection, when a re-authentication failure in the 3GPP AAA Server occurs, etc. If a UE has changed to a 3GPP access RAT, the 3GPP AAA Server initiated De-Registration procedure should not affect any currently selected PDN GW identity and APN associated with the UE's PDN Connection stored in the HSS and in use in the 3GPP access.

- HSS-initiated de-registration procedure to purge the UE from the 3GPP AAA server. This happens when the user's subscription has been cancelled or other operator-determined reasons. As a result, the 3GPP AAA server should deactivate any UE tunnel in the PDN GW and/or detach the UE from the access network.

The previous procedures are described in more detail in the following sub-sections. These procedures between the 3GPP AAA Server and the HSS are common to all non-3GPP accesses, whether trusted or non-trusted, and are independent of the mobility protocol used.

12.1.1 UE Registration Notification

After a UE has successfully been authenticated and authorised by the 3GPP AAA Server to make use of a given non-3GPP access (over SWa/STa), ePDG (over SWm) or PDN GW (over S6b for S2c), the 3GPP AAA Server registers its address to the HSS, unless already done. In turn, the HSS should store the address of the registered 3GPP AAA server for the given user and mark the user as registered in the 3GPP AAA Server. In the response, the HSS returns user profile data.

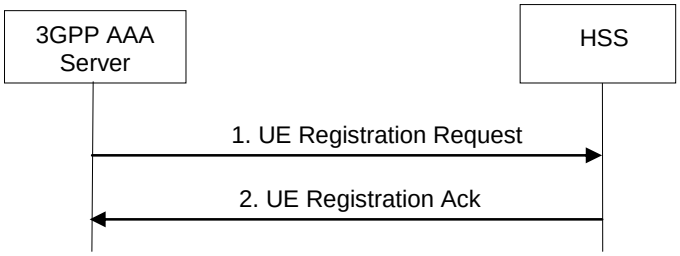


Figure 12.1.1-1: UE Registration Notification

1. Once the UE has been successfully authenticated by the 3GPP AAA server, the 3GPP AAA Server sends a UE Registration Request (User Identity, 3GPP AAA Server address) to the HSS.

2. The HSS checks that the user is known and that the stored 3GPP AAA Server address is the same one stored for the user and that it is the same 3GPP AAA Server that previously requested authentication vectors for this same user. If this is successful, the HSS marks the 3GPP AAA Server as the registered 3GPP AAA Server for user. The HSS responds with a UE Registration Ack (User Identity, Subscription Data). The subscription data includes information to be used by the PDN GW selection function or an already selected PDN GW identity and APN if present.

12.1.2 AAA-initiated UE De-registration Notification

The 3GPP AAA Server requests the HSS to De-Register the currently registered UE. In doing so, the 3GPP AAA Server is notifying the HSS that the UE no longer has any context in the 3GPP AAA Server. The HSS should in turn delete the registered 3GPP AAA Server address.

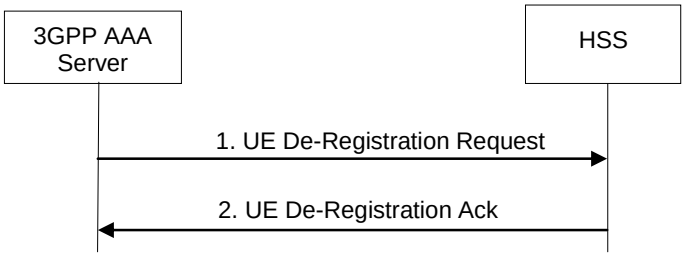


Figure 12.1.2-1: AAA-initiated UE De-registration Notification

1. The 3GPP AAA Server sends a UE De-Registration Request (User Identity, Cause) to the HSS. The "Cause" field may take values such as Authentication-Failure, UE-Detached, Charging-System-Request, etc.

2. The HSS marks the UE as not-registered, removes the 3GPP AAA Server address previously stored for the UE and responds with a UE De-Registration Ack.

12.1.3 HSS-initiated UE De-registration Notification

The HSS requests the 3GPP AAA Server to de-register a UE, for instance, when a subscription is withdrawn or other operator determined reasons. The 3GPP AAA Server should purge user data, set the user to not-registered and detach the UE and/or deactivate any network resources allocated to the user.

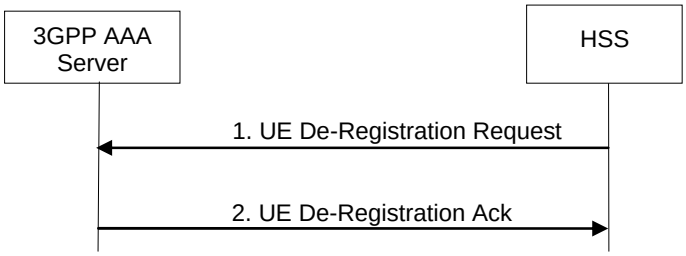


Figure 12.1.3-1: HSS-initiated UE De-registration Notification

1. The HSS server sends a UE De-Registration Request (User Identity, Cause) to the 3GPP AAA Server. The "Cause" field may take values such as Subscription Withdrawn, Administrative-Reason, etc.

2. The 3GPP AAA Server marks the user as not-registered and purges any user data. It responds with a UE De-Registration Ack. In addition, the 3GPP AAA Server should initiate detach of the UE or de-activation of any network resources.

12.1.4 PDN GW Address Notification

The 3GPP AAA Server updates the HSS with the PDN GW identity and APN associated with the UE's PDN Connection. This procedure only occurs when the 3GPP AAA Server has in turn successfully received the PDN GW identity and APN from the PDN GW the UE is attached to. The 3GPP AAA server should subsequently always update the HSS with the PDN GW identity. This procedure can be used for both PDN GW registration and de-registration.

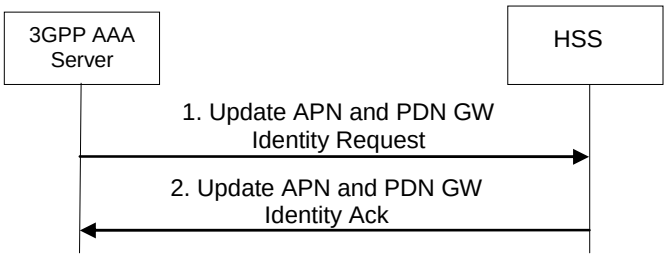


Figure 12.1.4-1: PDN GW Address Notification

1. The 3GPP AAA Server sends a Update PDN GW Identity Request (PDN GW Identity, APN, User Identity) to the HSS.

2. The HSS checks that the user is known and that the stored 3GPP AAA Server name is the currently registered 3GPP AAA server for this same user. If this is successful, the HSS returns a Update PDN GW Identity Acknowledgement.

12.2 Subscriber Profile Management Procedures

The subscriber profile management procedures between HSS and 3GPP AAA Server is described in this clause.

The procedure is invoked by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification of user profile data in the HSS.

The 3GPP AAA Server may also request the user profile data from the HSS. This procedure is invoked when for some reason the subscription profile of a subscriber is lost or needs to be updated.

12.2.1 HSS-initiated User Profile Update Procedure

The HSS may send a User Profile Update request to the 3GPP AAA Server whenever the subscriber profile in the HSS is modified since it was previously sent to the 3GPP AAA Server. The User Profile Update procedure is depicted in the following figure.

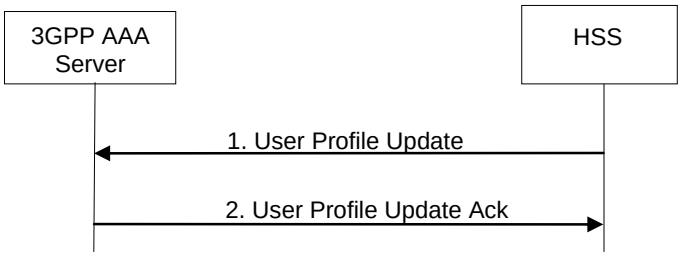


Figure 12.2.1-1: HSS-initiated User Profile Update Procedure

1. The HSS sends a User Profile Update (User Identity, Subscription Data) message to the 3GPP AAA Server. If the HSS is aware of the non-3GPP access type it may return only the subscription data that affects the non-3GPP access.

2. The 3GPP AAA Server updates its subscription data and acknowledges the User Profile Update message by returning a User Profile Update Ack (User Identity) message. As a result, the 3GPP AAA Server may need to update the non-3GPP access network and the PDN GW with new authorisation data, the PDN GW with new service authorisation data and new subscribed QoS data.

12.2.2 AAA-initiated Provide User Profile Procedure

The 3GPP AAA Server may send a Provide User Profile request to the HSS when the user subscription profile of a subscriber is lost or is corrupt or for any other reason.

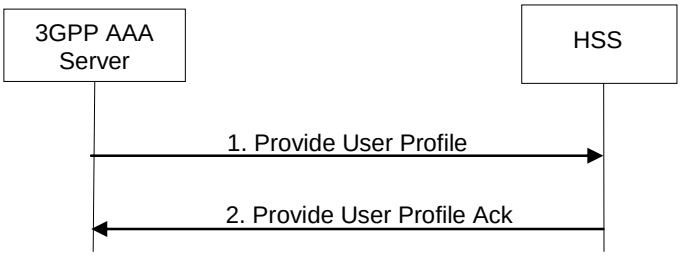


Figure 12.2.2-1: AAA-initiated Provide User Profile Procedure

1. The 3GPP AAA Server sends a Provide User Profile (User Identity) to the HSS.

2. The HSS checks that the user is known and that the stored 3GPP AAA Server address is the same one stored for the user and that it is the same server that previously requested authentication of the same user. If this is successful, the HSS returns a Provide User Profile Ack (user identity, subscription data). If the HSS is aware of the non-3GPP access type it may return only the subscription data that affects the non-3GPP access.

12.3 Authentication Procedures

The authentication procedures between HSS and 3GPP AAA Server are described in TS 33.402 [45].

The authentication procedures define the process in which the 3GPP AAA Server interacts with the HSS to acquire necessary data (i.e. Authentication Vectors for EAP-AKA) from the HSS to successfully authenticate the user for accessing the non-3GPP system.

13 Information Storage

<This section describes the context information that is stored in the different nodes for non-3GPP accesses support>

13.1 HSS

The data held in the HSS when non 3GPP accesses are not used is defined in TS 23.401 [4].

The additional data held in the HSS when non 3GPP accesses are used is defined in table 13.1-1 below.

Table 13.1-1: HSS EPS Data (additional aspects for non 3GPP accesses)

Field	Description
Serving node IP address	The IP address of the node serving the UE in the current Non 3GPP system.
Current access system RAT Type	RAT type of the Last known access system
QoS profile per access	The quality of service profile subscribed for a particular access for a specific APN
ODB	Indicates that the status of the operator determined barring for a specific access.
Access Restriction	Indicates the access restriction subscription information.

13.2 MME

Information storage for the MME is described in TS 23.401 [4]. The additional data held in the MME when optimized interworking with CDMA2000 HRPD is used is defined in table 13.2-1 below.

Table 13.2-1: MME storage requirements to support optimized interworking with CDMA2000 HRPD

Field	Description
S101 HRPD access node IP address	The IP address of the HRPD AN used for the S101 tunnel for a UE. This is stored on a per UE basis.
S103 Forwarding Address	HSGW IP address used for data forwarding to the HRPD access over S103 interface. This is stored on a per UE basis.
S103 GRE key(s)	GRE Key(s) used for the data forwarding tunnel to the HSGW - one per UE-PDN connection. This is stored on a per UE basis.

13.3 S-GW

Information storage for the S-GW is described in TS 23.401 [4]. The additional data held in the S-GW when optimized interworking with CDMA2000 HRPD is used used is defined in table 13.3-1 below.

Table 13.3-1: S-GW storage requirements to support optimized interworking with CDMA2000 HRPD

Field	Description
S103 Forwarding Address	HSGW IP address used for data forwarding to the HRPD access over S103 interface. This is stored on a per UE basis.
S103 GRE key(s)	GRE Key(s) used for the data forwarding tunnel to the HSGW - one per UE-PDN connection. This is stored on a per UE basis.

14 Interactions with Other Services

< This section describes the interactions with other services/features, e.g. location services, emergency/priority access, possibly terminal configuration, etc. when connecting non-3GPP accesses to the EPC>

15 Functional Description and Procedures for 3GPP Accesses with S2c

15.1 S2c Bootstrapping via DSMIPv6 Home Link

When connected over the UE home link (i.e. 3GPP access as defined in section 4.1), the UE may trigger the establishment of S2c IKEv2 SA, e.g. to optimize future handovers to non-3GPP accesses using S2c. For each PDN connection, the S2c IKEv2 SA establishment has to be performed separately.

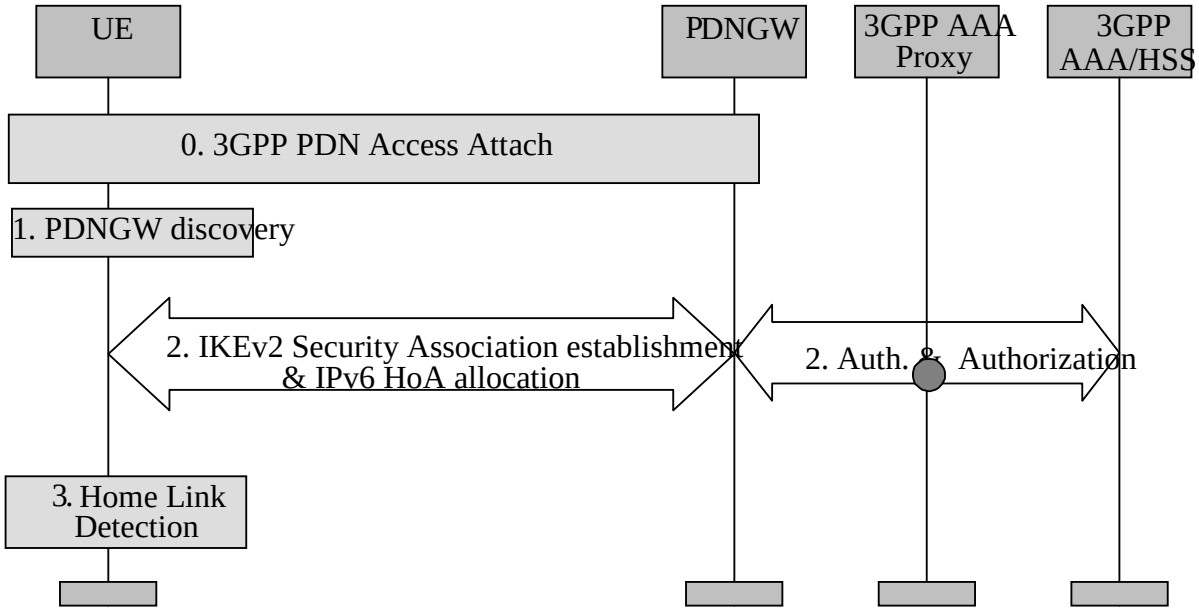


Figure 15.1-1: S2c PDN Attach via DSMIPv6 home link

0. In this procedure it is assumed that UE is already attached to the PDN over the 3GPP access system as defined in TS 23.401 [4]. This step, according to TS 23.401 [4] could be an initial attach to a default PDN or a UE initiated subsequent attach to another PDN.

1. The UE discovers the PDN GW providing access to the PDN it connected to in Step 0, as defined in the clause 4.5.2. To ensure rechability of the PDN GW, signalling associated with this step as well as step 2 below, should be performed over the connection established by step 0 above.

2. A security association is established between the UE and PDN GW to secure the DSMIPv6 messages related to this PDN connection between the UE and the PDN GW.

   The UE initiates the establishment of the security association using IKEv2 [9]; EAP [11] is used over IKEv2 for authentication purposes. The PDN GW communicates with the AAA infrastructure in order to complete the authentication.

   During this step an IPv6 home address/prefix is assigned by the PDN GW to the UE as defined in RFC 4877 [22]. During this step the UE may include the APN of the PDN it wants to access. The PDN GW address and APN associated with the UE's PDN Connectivity are registered by the AAA server with the HSS as described in clause 12.

In this step, the PDN GW may be either in the HPLMN or in the VPLMN. When the PDN GW is in the VPLMN, the interaction between the PDN GW in the VPLMN with the AAA/HSS in the HPLMN may involve a 3GPP AAA Proxy in the VPLMN as specified in TS 23.234 [5].

3. UE confirms that it is located in its DSMIPv6 home link for the given PDN, as described for DSMIPv6 Home Link Detection Function in clause 4.5.6.

   In some cases this procedure may result in a PDN GW that is different than the one the UE is connected to in step 0. In this case the PDN GW reallocation procedure defined in clause 6.10 is applied.

Annex A (informative): GTP - PMIP Roaming

The scenarios below identify and describe various deployment scenarios for interworking between EPC networks based on GTP and EPC network based on PMIP. The scenario described here is the direct peering scenario.

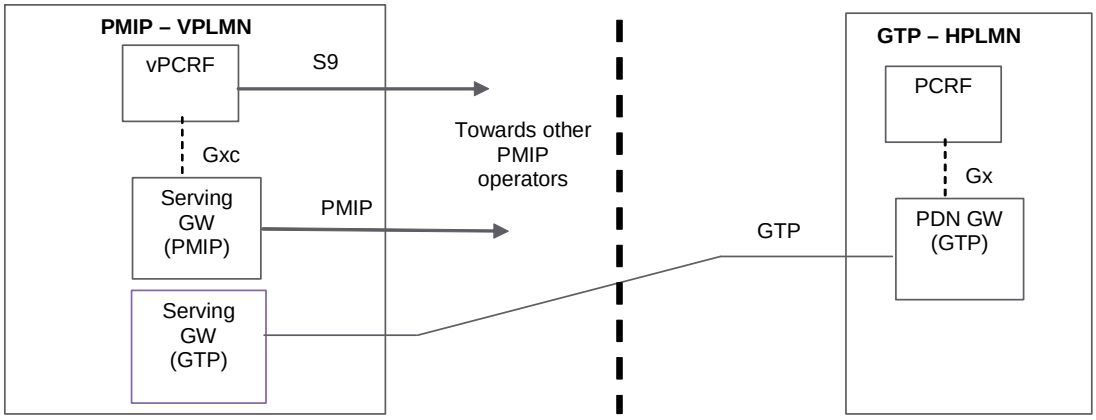
NOTE: Identification of additional scenarios is FFS.

Editor's note: Multiple PDN Connection needs to be supported, detailed solution is FFS.

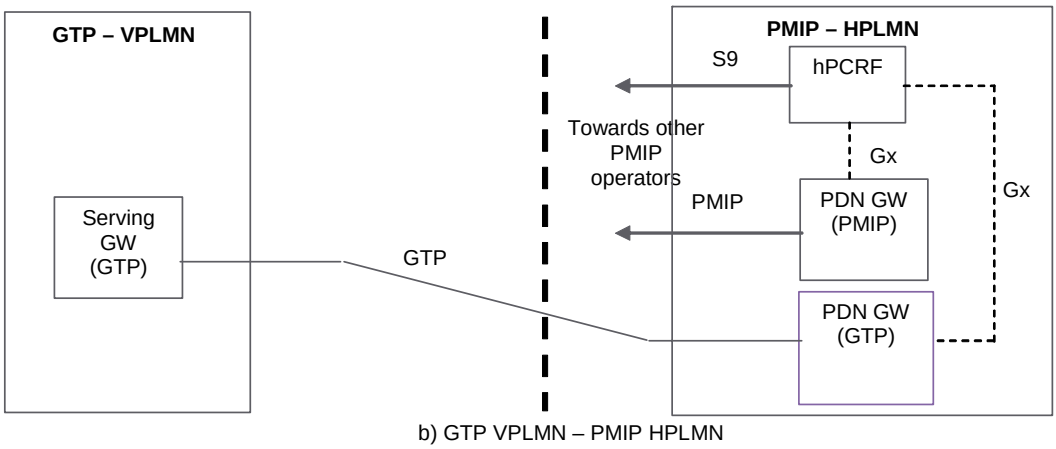
A.1 Direct Peering Scenario

The "direct peering" scenario consists in having one of the two roaming partners provide support for both variants of roaming flavour (e.g. a PMIP operator would support GTP-based roaming interface towards a GTP-only roaming partner, or vice versa) in order to make roaming possible.

The support for such roaming flavour can be provided either on the same GW node or on different GW nodes. Upon establishment of connectivity for a specific roaming UE, the Visited network chooses a GTP-based or a PMIP-based S8 interface (on the same GW node or on different GW nodes, note that for a single user only a single Serving GW is allocated when connecting to EPC), depending on the preferences of the roaming partner that owns the subscriber.



a) PMIP VPLMN – GTP HPLMN



b) GTP VPLMN – PMIP HPLMN

Figure A.1-1: Direct peering examples: a) PMIP-based VPLMN to GTP-based HPLMN; b) GTP-based VPLMN to PMIP-based HPLMN

Depicted in Figure A.1-1 (a) is an example of "direct peering" interworking between a GTP-based HPLMN and a PMIP-based VPLMN. When roamers whose subscription is owned by the GTP-based operator attach to the EPS network of the PMIP-based operator, they are assigned a GTP-capable GW acting in the role of SGW. The SGW selection is carried out by MME or SGSN based on the subscriber's HPLMN. In case of the Serving GW supporting both GTP and PMIP, the MME/SGSN should indicate the Serving GW which protocol should be used over S5/S8 interface.

Depicted in Figure A.1-1 (b) is an example of "direct peering" interworking between a PMIP-based HPLMN and a GTP-based VPLMN. When roamers whose subscription is owned by the PMIP-based operator attach to the EPS network of the GTP-based operator, they are assigned a GTP-capable SGW. The information provided by the PMIP-based HPLMN for the PGW selection function must take into account that the Visited network is GTP-only, in order to return either the IP address (or an APN that can be resolved to an IP address according to the PDN GW resolution mechanism) that points to a GTP-capable PDN GW.

Figure A.1-2 depicts the scenario in which a UE from a GTP-based network roams in a PMIP-based network, local breakout is used, and home-routed bearers are also possible. As with the home-routed case, the MME or SGSN in the PMIP-based VPLMN selects a GTP-capable Serving GW, but it selects a PMIP capable PDN GW. As a result, the SGW in this example supports both GTP and PMIP based S5/S8. This allows the local breakout bearer and any associated home-routed bearer for the user (e.g. the default bearer) to be served by the same Serving GW. Support of S9 may not be required in all local breakout scenarios.

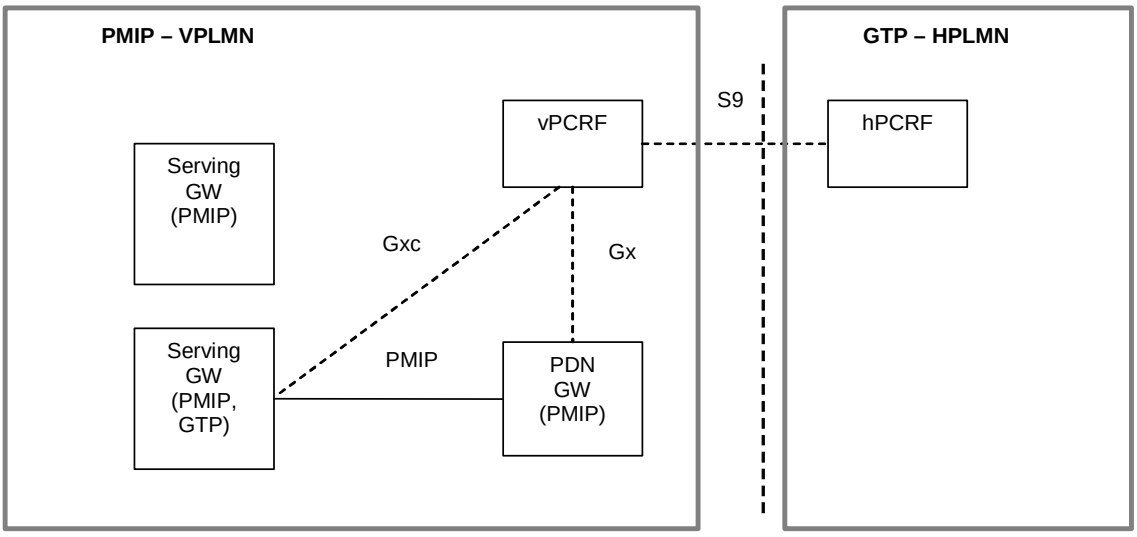


Figure A.1-2: Direct peering example: Local Breakout, UE from GTP HPLMN Roaming in PMIP VPLMN

Figure A.1-3 depicts the scenario in which a UE from a PMIP-based network roams into a GTP-based network and local breakout is used. As with the home-routed case, the MME/SGSN in the GTP-based VPLMN selects a GTP-capable Serving GW and the PDN GW selection function selects a GTP-capable PDN GW. This allows the local breakout bearer and any associated home-routed bearer for the user (e.g., the default bearer) to be served by the same Serving GW. Support of S9 may not be required in all local breakout scenarios.

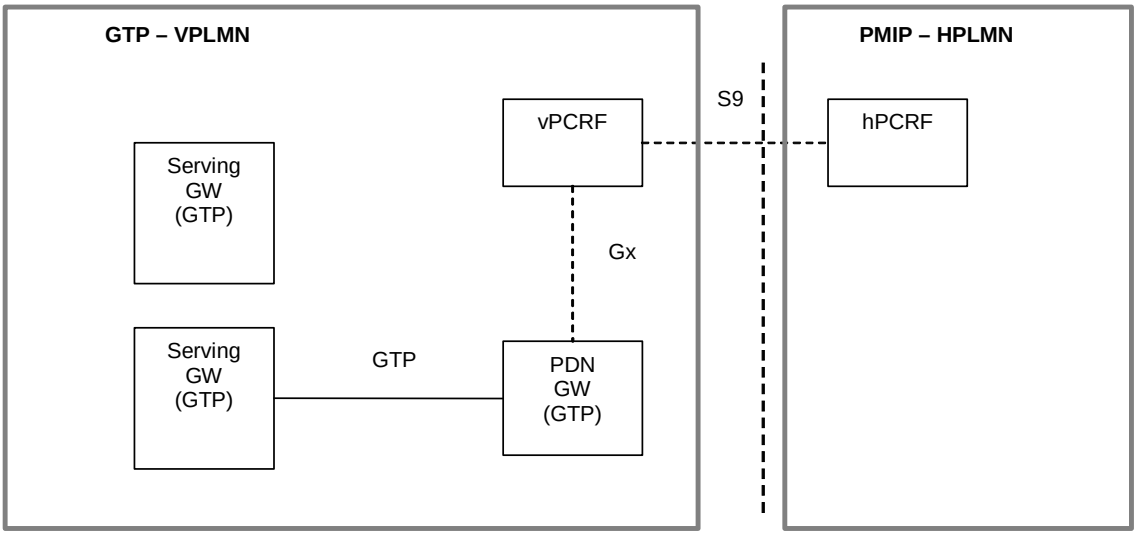
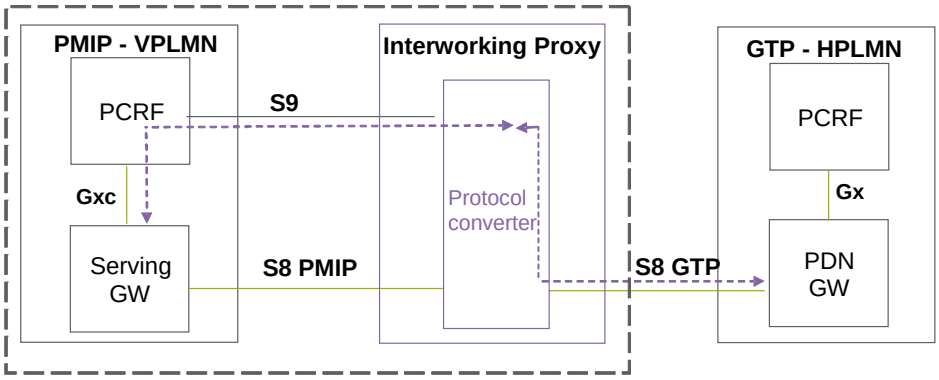


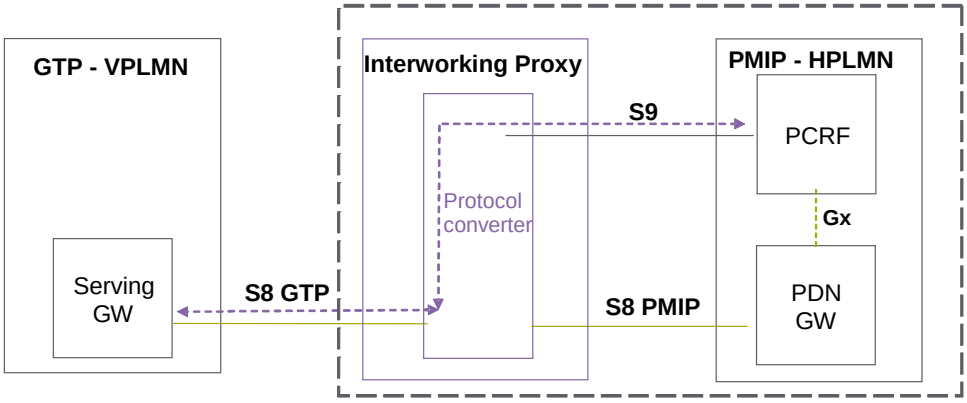
Figure A.1-3: Direct peering example: Local Breakout, UE from PMIP HPLMN Roaming in GTP VPLMN

A.2 Proxy-based interworking

In this scenario an Interworking Proxy (IWP) sits between the GTP-based PLMN and the PMIP-based PLMN to perform protocol conversion between the GTP protocol on one side and the PMIP and Diamater protocols on the other side.



a) GTP HPLMN - PMIP VPLMN



b) PMIP HPLMN - GTP VPLMN

Figure X1: Roaming Via Interworking Proxy: a) GTP-based HPLMN to PMIP-based VPLMN; b) PMIP-based HPLMN to GTP-based VPLMN

The IWP is inserted transparently in the signalling and bearer path i.e. no changes to the GTP, PMIP and Diameter protocols are required.

Annex B (informative): Guidance for Contributors to this Specification

The following guidance is provided for drafting figures for TS 23.402 that share some common procedures with TS 23.401 [4].

Representation of PMIP or GTP variants of S5/S8:

- Flows to TS 23.401 will contain the complete procedures for GTP-based S5/S8.
- In TS 23.401 [4], section(s) of a flow that is different for PMIP version of S5/S8 interface are shown surrounded by shaded box indexed by capital letter in ascending order, e.g. "A", "B", "C", etc.

  At the bottom of the flow, the following text should be included, e.g.

  NOTE: Procedure steps (A) and (B) for an PMIP-based S5/S8 are defined in TS 23.402.
- In TS 23.402, each step for the relevant section, belonging to say section A, of the flow should be indicated by "A.1, A.2, …" . In TS 23.402 common sections of the flow captured in TS 23.401, should be indicated by shaded boxes with text, e.g. "Procedures in TS 23.401, Figure x.y.z-k, before A", "Procedures in TS 23.401 [4], Figure x.y.z-k, between A and B", etc.

For an illustrative example of the drafting guidelines rule, please refer to Figure 5.4.1-1 in TS 23.401 [4] and corresponding Figure 5.4.1-1-1 in this specification.

Representation of different architectural cases:

- For each case supported, indicate the presence of the optional network entities that may be included in the procedure step. These optional entities appear between the source and destination of the procedure interaction arc as a gray circle. For example, a vPCRF may stand between the Serving GW and the hPCRF.
- In text following a procedure diagram, list the different cases supported by the figure.
- For each case that is supported, indicated what the role of the optional network entity is, when it occurs in the interaction. For example, "In the roaming case, the vPCRF forwards messages between the Serving GW and the PDN GW".

While it is possible to describe these interactions in each step in which they might occur, this will tend to clutter and complicate the procedure diagrams and should be avoided. A single paragraph found beneath each procedure including optional network elements should suffice to clarify that procedure.

Representation of the impact of multiple PDN connectivity:

- In text following a procedure diagram, list the specific impacts arising from multiple PDN connectivity. This will chiefly include a description of which interactions in the figure may be repeated N times for each PDN connected to.

Annex C (informative): Handover Flows Between Non-3GPP Accesses

C.1 General

This section describes non-exhaustive examples of flows for handover between non-3GPP accesses connected to the EPC. The handover scenarios are based on the mechanisms defined in Section 8 of this document.

C.2 Trusted Non-3GPP IP Access to Trusted Non-3GPP IP Access with DSMIPv6 over S2c Handover

In this scenario, the session starts in trusted non3GPP access using DSMIPv6 over S2c. The session hands over to another trusted non-3GPP access system. The UE subsequently initiates DSMIPv6 with the same PDN GW to maintain the IP session.

In the non-roaming case, none of the optional entities in Figure C.2-1 are involved.

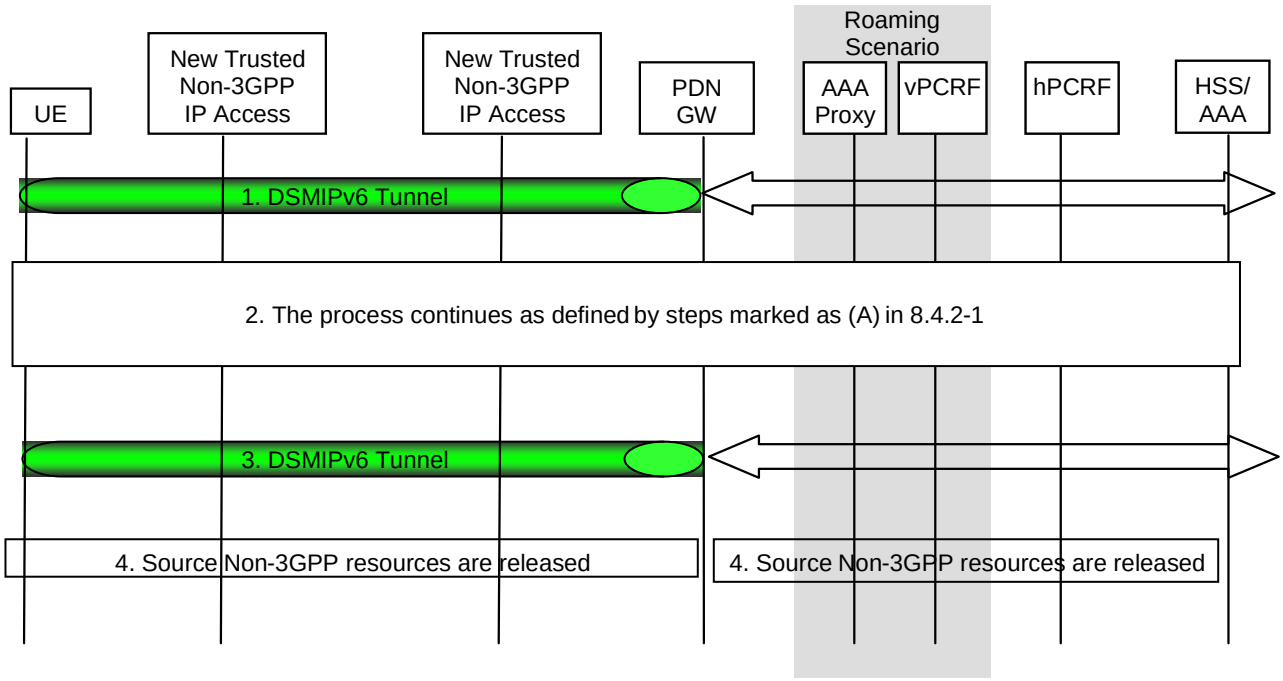


Figure C.2-1: Trusted non-3GPP to Trusted non-3GPP handover based on S2c

1. The UE uses a Trusted non3GPP access system. It has a local IP address from the non3GPP system which is used as a care-of address in the DSMIPv6 registration to the PDN GW. The UE maintains a security association with the PDN GW.
2. The UE decides to initiate an access procedure with a new Trusted non-3GPP access. The procedure continues with the steps defined in Figure 8.6-1 (A)
3. The UE continues the ongoing session(s) via the same PDN GW maintaining the same IP address.
4. Resources in the old Trusted Non-3GPP access may be released

C.3 Untrusted Non-3GPP IP Access with PMIPv6 to Trusted Non-3GPP IP Access with PMIPv6 Handover in the Non-Roaming Scenario

This clause shows a call flow for a handover when UE moves from an untrusted non-3GPP IP access network to the trusted non-3GPP access network. PMIPv6 is assumed to be used on S2a and S2b interfaces.

NOTE: The procedure is also applicable to the handover within PMIP-based S2a interfaces or PMIP-based S2b interfaces.

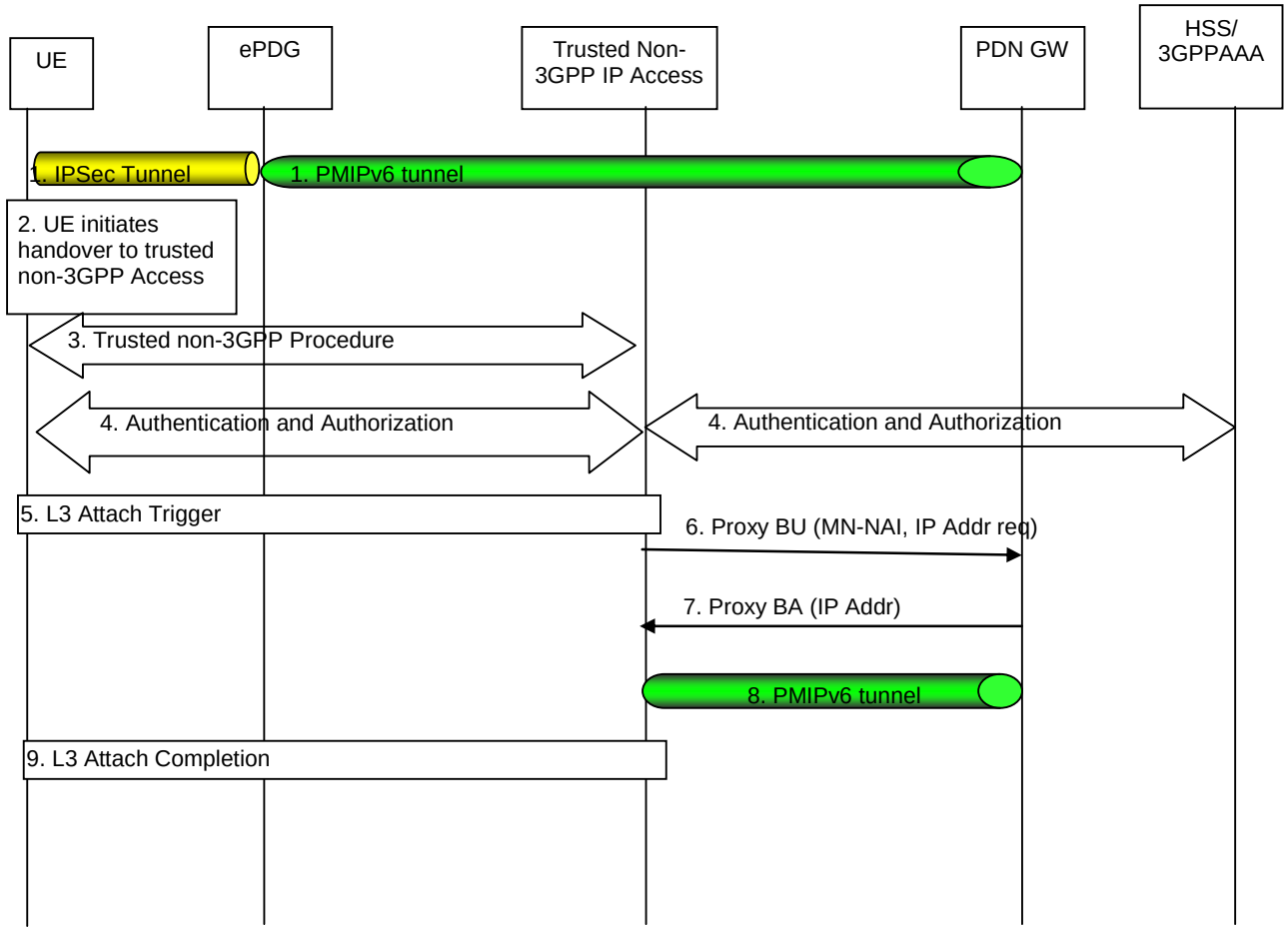


Figure C.3-1: S2b to S2a (PMIPv6) Handover

1) The UE is connected to the untrusted Non-3GPP Access. There is an IPsec tunnel between the UE and the ePDG and a PMIPv6 tunnel between the ePDG and the PDN GW.

2) The UE moves to a Trusted Non-3GPP Access network.

3) The access specific procedures of the Trusted Non-3GPP Access are performed. These procedures are outside of the scope of 3GPP.

4) The EAP authentication procedure is initiated and performed involving the UE, Trusted Non-3GPP IP Access and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. As part of the authentication procedure, the information of the selected PDN GW, e.g. PDN GW's address, is conveyed to the MAG in the Trusted Non-3GPP IP Accesses.

5) After successful authentication and authorization, the L3 attach procedure is triggered.

6) The MAG function in the Trusted Non-3GPP IP Access sends Proxy Binding Update message to the PDN GW.

Editor's Note: If the PCC is applied how to interact with PCRF is FFS.

7) The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates IP address for the UE. The PDN GW then sends a Proxy Binding Acknowledgement to the MAG function in the Trusted Non-3GPP IP Access, including the IP address(s) allocated for the UE. The IP address allocated is same as that was assigned to UE before over the Untrusted Non-3GPP Accesses.

8) The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW.

9) L3 attach procedure is completed. IP connectivity between the UE and the PDN GW is set for uplink and downlink direction over the trusted non-3GPP IP access.

Editor's Note: How to tear down the resource in the old access network is FFS.

C.4 Trusted/Untrusted Non-3GPP IP Access with DSMIPv6 to Trusted Non-3GPP IP Access with PMIPv6 Handover in the Non-Roaming Scenario

This clause shows a call flow for a handover when UE moves from a source trusted/untrusted non-3GPP IP access network to a target trusted non-3GPP access network. PMIPv6 is assumed to be used on S2a and DSMIPv6 is assumed to be used on source trusted/untrusted access network.

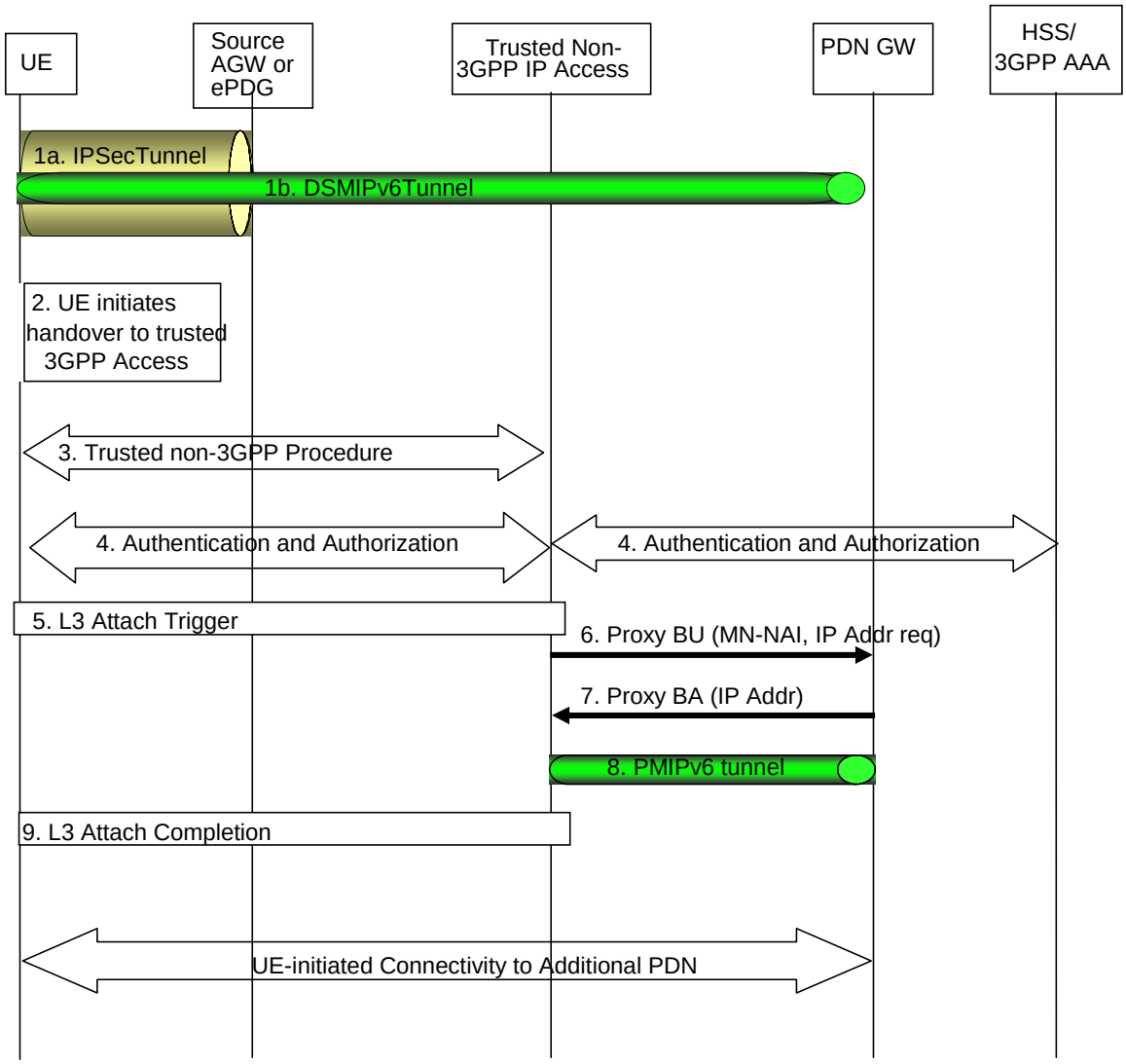


Figure C.4-1: S2b to S2a (PMIPv6) Handover

NOTE: In case of connectivity to multiple PDNs, the steps in (A) are repeated for each PDN the UE is connected to. The steps in (A) can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

1. The UE is connected to the trusted/untrusted Non-3GPP Access using S2c.

1a. There is an IPsec tunnel between the UE and the ePDG if UE is connected over untrusted access network.

2. The UE moves to a Trusted Non-3GPP Access network.

3. The access specific procedures of the Trusted Non-3GPP Access are performed. These procedures are outside of the scope of 3GPP.

4. The EAP authentication procedure is initiated and performed involving the UE, Trusted Non-3GPP IP Access and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. As part of the authentication procedure, the information of the selected PDN GW, e.g. PDN GW's address, is conveyed to the MAG in the Trusted Non-3GPP IP Accesses. The PDNs the UE is connected to are obtained from the HSS with the UE subscriber profile.

5. After successful authentication and authorization, the L3 attach procedure is triggered.

6. The MAG function in the Trusted Non-3GPP IP Access sends Proxy Binding Update message to the PDN GW.

Editor's Note: If the PCC is applied how to interact with PCRF is FFS.

7. The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates IP address for the UE. The PDN GW then sends a Proxy Binding Acknowledgement to the MAG function in the Trusted Non-3GPP IP Access, including the IP address(s) allocated for the UE. The IP address allocated is same as that was assigned to UE before over the Untrusted Non-3GPP Accesses.

8. The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW.

9. L3 attach procedure is completed. IP connectivity between the UE and the PDN GW is set for uplink and downlink direction over the trusted non-3GPP IP access.

10. In case of connectivity to multiple PDNs, the UE establishes connectivity to all the PDNs besides the Default PDN that the UE was connected to before the handover as described in clause 6.8.1.

Editor's Note: How to tear down the resource in the old access network is FFS.

C.5 Handover Between Two Untrusted Non-3GPP IP Accesses Connected to the Same ePDG

This handover case is handled by MOBIKE [18], i.e. the existing IPSec tunnel, via the first untrusted non-3GPP IP access, is only modified for the use with the second untrusted non-3GPP access (and not torn down and re-created from scratch). It is assumed that the MOBIKE support indication has been sent by UE to ePDG in the initial attach.

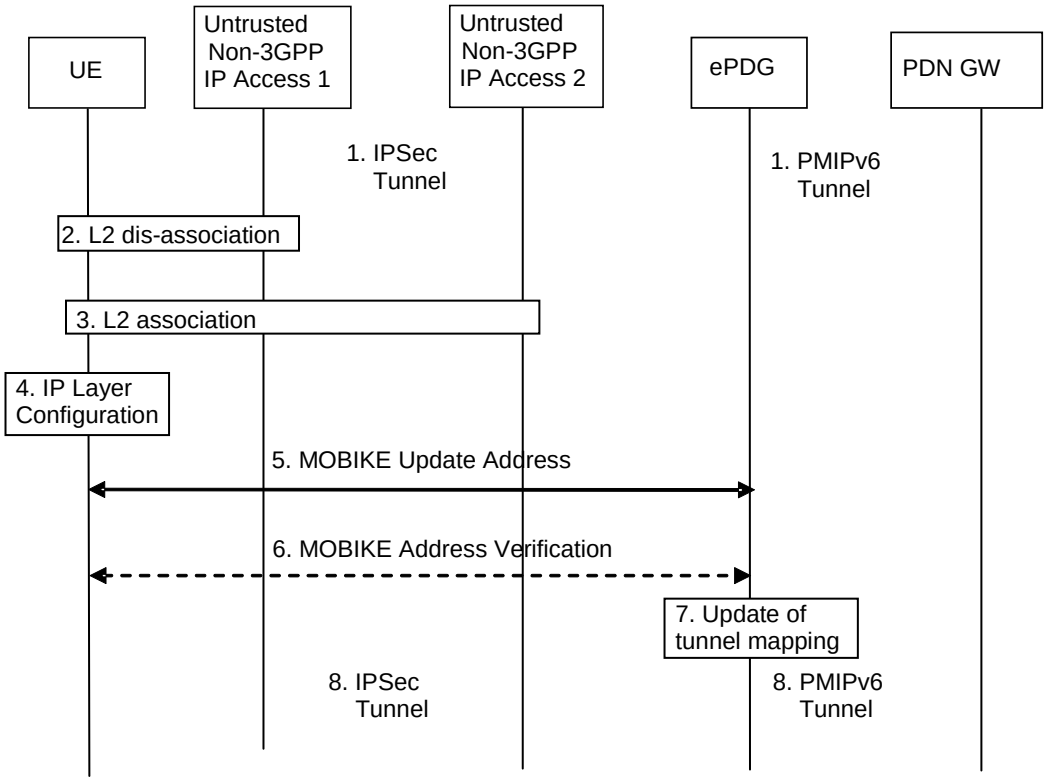


Figure C.5-1: Message flow for handover between two untrusted non-3GPP IP accesses based on MOBIKE

The following steps are performed:

1. The UE is connected via the IPSec tunnel to ePDG, from where a PMIPv6 tunnel is established to the PDN GW. The UE is utilizing a local IP address (for previous IKEv2 signaling and outer IP header address).
2. The UE disconnects on L2 from untrusted non-3GPP IP access 1.
3. UE establishes L2 connectivity to untrusted non-3GPP IP access 2.
4. Configuration of a local IP address. (In case of dual radio multihoming capability with respect to the local IP address is required).
5. MOBIKE update address message exchange (in both directions, initiated by UE).
6. MOBIKE address verification, initiated by ePDG; this step is optional as per MOBIKE [18].
7. The tunnel mapping (between PMIPv6 tunnel and IPSec tunnel) is updated.
8. The modified IPSec tunnel is now in operation.

For dual radio, step 2 is done after step 8.

Annex D (informative): Network Discovery and Selection

This section collects the results of discussions related to network discovery and selection in order to support the progress of discussion on the topic.

D.1 Examples of Operational Scenarios

Some exemplary operational scenarios have been identified:

- The assistance data/policies provided by the network to the UE is associated with a time validity set by the network, with the assumption that when the validity expires new assistance data/policies is provided
- The UE and the network may interact according to a series of models, including:
- Triggering takes place in the terminal based on a specific event; the terminal sends a request/indication to home network based on the event; the home network returns additional/new assistance data/policies; the terminal acts upon the received assistance data/policies (e.g. scan for a certain access, switch connectivity between access technologies, etc.)
- Triggering takes place in the home network based on an event; the home network provides new or additional assistance data/policies to UE; the terminal acts upon the received assistance data/policies (e.g. scan for a certain access, switch connectivity between access technologies, etc.)

Additional scenarios are FFS.

D.2 Architectural Options

The following architectural options have been identified:

- Provision of assistance data/policies for network discovery and selection through access-specific mechanisms in the visited network, with potential input provided from home network in the roaming case
- Transport level solutions between the UE and the home network

Others are FFS.

Annex E (Informative): Gateway Relocation in the Trusted Non-3GPP IP Access

Gateway relocation within the Trusted Non-3GPP IP Access is possible using the procedures defined in this clause. The trigger for gateway relocation and any mechanisms for preserving or transferring context between gateways within the Trusted Non-3GPP IP Access is considered out of scope of this specification and should be handled within standards external to 3GPP.

In both the case of PMIPv6 and MIP v4 FACoA on S2a, the Gateway Control Session for the target gateway of the relocation is established before the intra-non-3GPP handover occurs. After the handover, the Gateway Control Session in the source gateway of the handover is terminated.

The mobility management and policy control signalling are both shown as optional messages. This is to allow flexibility depending on the requirements of the trusted non-3GPP IP access system. This allows a policy control signalling relocation (on S7a) or a relocation of the local mobility anchor (S2a) or both (S7a and S2a).

E.1 Gateway Relocation with PMIPv6 on S2a

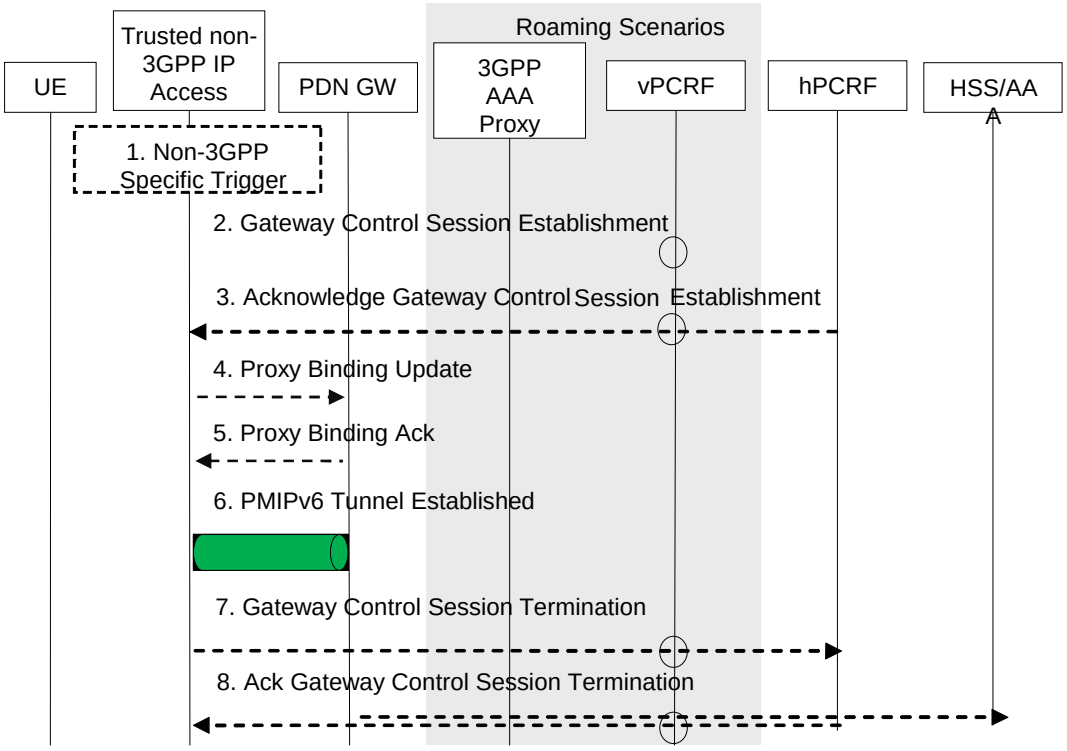


Figure E.1-1: Gateway Relocation when PMIPv6 MM mechanism is used over S2a

When the Gateway Relocation procedure occurs in the Non-Roaming case (Figure 4.2.2-1), the vPCRF is not involved.

In the case of Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-5), the vPCRF is employed to forward messages from the hPCRF in the home PLMN, by way of the vPCRF in the VPLMN to the non-3GPP access.

1) A gateway relocation is triggered, to be initiated by the Trusted Non-3GPP IP Access. These trigger is outside the scope of 3GPP standardization.

2) The target Gateway in the Trusted Non-3GPP IP Access sends a Gateway Control Session Establishment message to the hPCRF.

3) The PCRF responds to the target Gateway an Ack Gateway Control Session Establishment (QoS Rules, Event Triggers) message. The PCC rules provide the PDN GW with information required to enforce the dedicated bearer policy. The event triggers indicate to the PDN GW when to report an event back to the PCRF related to the dedicated bearer.

4) The target Gateway sends a Proxy Binding Update (MN NAI) message to the PDN GW to register the UE at the PDN-GW. The MN NAI identifies the UE.

5) After creating the binding cache entry for the UE, the PDN GW responds with a Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info) message to the MAG. The MN NAI repeats the UE identity sent previously. The Lifetime expresses the duration of validity of the binding. The UE Address info includes the allocated IP Address(es) corresponding to the IP CAN session.

6) The PMIP tunnel from the target gateway to the PDN GW is established.

7) The source Gateway in the Trusted Non-3GPP IP Access system sends a Gateway Control Session Termination to the PCRF. This gateway ceases to perform Bearer Binding and associated policy controlled functions.

8) The PCRF sends an Acknowledge Gateway Control Session Termination message to the Trusted Non-3GPP IP Access acknowledging the termination of the control session.

E.2 Gateway Relocation with MIPv4 FACoA on S2a

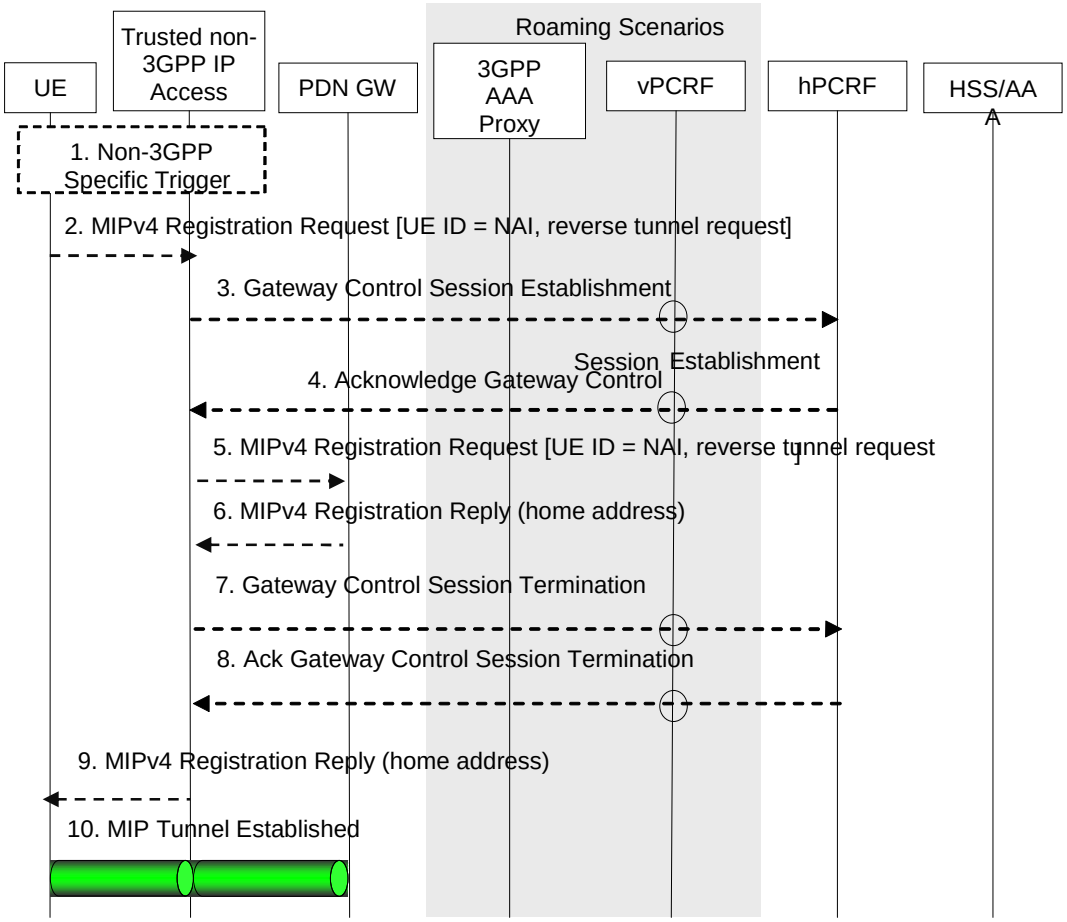


Figure E.2-1: Gateway Relocation when MIPv4 FACoA mode MM mechanism is used over S2a

When the Gateway Relocation procedure occurs in the Non-Roaming case (Figure 4.2.2-1), the vPCRF is not involved.

In the case of Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-5), the vPCRF is employed to forward messages from the hPCRF in the home PLMN, by way of the vPCRF in the VPLMN to the non-3GPP access.

1) A gateway relocation is triggered, to be initiated by the UE. This trigger is outside the scope of 3GPP standardization.

2) The UE sends a Registration Request (RRQ) RFC 3344 [12] message to the FA. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 3775 [14] and the Home Agent Address.

3) The Trusted non-3GPP access sends a Gateway Control Session Establishment message to the hPCRF from the target gateway system within the Trusted Non-3GPP IP Access.

4) The hPCRF responds to the message sent by the non-3GPP access in step 3. The hPCRF, sends an Acknowledge Gateway Control Session Establishment (QoS Rules, Event Triggers) message to the Trusted Non-3GPP IP Access. This response includes QoS Policy rules and triggers for subsequent reports to the hPCRF by the Trusted Non-3GPP IP Access.

5) The FA processes the message according to RFC 3344 [12] and forwards a corresponding RRQ message to the PDN GW.

6) The PDN GW allocates an IP address for the UE and sends a Registration Reply (RRP) RFC 3344 [12] to the FA, including the IP address allocated for the UE.

Editor's Note: Whether the PDN GW should authenticate the Registration Request message is FFS.

7) The Trusted non-3GPP access sends a Gateway Control Session Termination message to the hPCRF from the source gateway system within the Trusted Non-3GPP IP Access.

8) The hPCRF responds to the message sent by the non-3GPP access in step 8. The hPCRF, sends an Acknowledge Gateway Control Session Termination message to the non-3GPP IP Access.

9) The FA processes the RRP according to RFC 3344 [12] and sends a corresponding RRP message to the UE.

10) IP connectivity from the UE to the PDN GW is now setup. A MIP tunnel is established between the FA in the Trusted Non-3GPP IP Access and the PDN GW.

Annex F (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2007-12	SP-38	SP-070829	-	-	-	MCC editorial update for presentation to TSG SA for approval	1.5.1	2.0.0
2007-12	SP-38	-	-	-	-	Release 8 Version created after approval at TSG SA #38	2.0.0	8.0.0
2008-03	SP-39	SP-080123	0158	-	C	Attach Type for 3GPP accesses and Incorporation of MIPv4 into Non-3GPP-to-EUTRAN Handover	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0157	1	F	Reference points renaming	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0156	1	C	Informing the PCRF about existence of tunneled traffic	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0154	-	C	IEs for Non-3GPP Detach & Additional PDN Procedures and Updates for currently valid version of PMIPv6 draft	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0153	-	C	Cleanup/Merge of CR0063R1: Clean-up and addition of IEs for consistency	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0151	-	F	Merger of 23.402 CR0066R3 (MIPv4 FA CoA procedures for non-3GPP access to SAE) and 23.402 CR0074R2 (Editorial corrections for TS 23.402)	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0150	1	C	Clarifications related to IKE at handover from host-based mobility to network-based mobility	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0147	-	C	Removal of the FFS concerning the uplink signalling of RAT when we don't have SGW relocation	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0139	3	F	Removal of editor's notes for IP Mobility Management Selection	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0138	2	C	On description and clarification for IPMS	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0136	1	F	IPMS corrections	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0135	3	C	Handover with Network Discovery and Selection	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0134	3	F	Information provided by the ANDSF	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0133	3	B	ANDSF Discovery	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0121	2	B	Addition of PMIP-based S5/S8 UE-triggered Service Request Procedure to 23.402	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0117	1	F	IP Address Allocation and parameter configuration in case of S2c	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0116	1	C	Refinements to GW selection	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0115	1	C	Dual stack support (IPv4/IPv6) in PMIP for E-UTRAN	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0114	-	F	Adding procedure for HSS Initiated QoS Subscribed Modification to TS 23.402	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0111	2	C	Merge of CR0072 (Modification to handover procedure from non 3GPP to EUTRAN when S5/S8 is PMIP based) and CR0069Rev2 (Clean up of S2 Handover procedures) and CR0025 (Clean up of S2 Handover procedures)	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0109	1	F	PCC related corrections to various flows	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0107	2	C	Handover Indication as UE capability for Network address preservation in 3GPP access	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0106	1	B	Handover flows between non-3GPP and 3GPP with chained S2/S8a	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0105	2	F	S2c and Multiple PDNs cleanup	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0104	2	C	S2c Detach for Untrusted non-3GPP Accesses	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0102	-	F	S2c Detach over Trusted Non-3GPP Access Cleanup	8.0.0	8.1.0
2008-03	SP-39	SP-080125	0101	3	F	Functional Description and Procedures for 3GPP Accesses with S2c	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0100	-	C	GRE Key Exchange Using PMIP	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0099	2	B	Principles for 3GPP-Mobile Wimax interworking	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0098	-	C	Serving GW Relocation and Modification of Handover and Tracking Area Update Procedures when PMIP is used at S5/S8	8.0.0	8.1.0
2008-03	SP-39	SP-080123	0096	3	C	Context transfer information for PMIP-based CN node Relocation	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0095	2	C	HRPD to EUTRAN handover call flows for default bearer case	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0092	7	C	Updates in TS 23.402 for currently valid version of PMIPv6 draft	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0090	4	C	Update on IP Mobility Mode Selection	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0085	3	C	On IPMS solutions	8.0.0	8.1.0
2008-03	SP-39	SP-080128	0082	5	C	On IPMS on handover between accesses	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0081	1	F	Special situations in EUTRAN - HRPD HO	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0080	1	F	Alignment of EUTRAN-HRPD HO with RAN2 and SA2 decisions	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0079	4	C	Alignment of EUTRAN - > HRPD HO with updated inter S-GW HO	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0074	3	F	Editorial corrections for TS 23.402	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0073	2	B	PDN GW reallocation procedure for the S2c reference point	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0065	-	C	Addition of IEs to Non-3GPP Untrusted Procedures	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0064	1	C	Addition of IEs to Non-3GPP Resource Control Procedures	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0062	2	C	Addition of IEs to PMIP-based S5/S8 Procedures	8.0.0	8.1.0

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2008-03	SP-39	SP-080124	0061	1	F	Cleanup PDN Selection Procedure	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0060	1	B	Non-3GPP Gateway Control Session Relocation	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0056	2	F	Removal of FFS Statements on Proxy Binding Update Security	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0055	2	F	Cleanup of Wa*, Wd*, Wx*, Wm* references points	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0054	2	F	ePDG discovery during a handover from EUTRAN to untrusted non-3GPP access networks	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0050	1	C	Establishment of dedicated bearers during handover	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0049	3	C	Cleanup of the handover from trusted non-3GPP to GERAN/UTRAN	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0045	1	F	Dedicated Bearer Activation at Attach for PMIP-S5/S8	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0044	2	C	Principles and Protocol Stack for S103 Interface	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0043	2	C	Timing of PCC and PMIP Signalling at Handover	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0039	4	F	ePDG selection	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0031	3	F	Relation of DSMIPv6 and 3GPP access	8.0.0	8.1.0
2008-03	SP-39	SP-080167	0030	1	F	Clarification on Access Authentication	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0028	1	F	ePDG Function Clarification	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0027	3	B	Principles of multiple PDN support in 23.402	8.0.0	8.1.0
2008-03	SP-39	SP-080124	0018	1	F	Clarification on S-GW selection when Handover	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0016	3	B	Modification on S8/S2 Chained Attach Procedure	8.0.0	8.1.0
2008-03	SP-39	SP-080121	0015	1	B	Optimized Idle Mode Handover from HRPD to E-UTRAN	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0012	3	C	Attach Type for Non-3GPP accesses	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0007	3	C	Activation of additional PDN connection for PMIP-based S5/S8	8.0.0	8.1.0
2008-03	SP-39	SP-080122	0006	1	C	PDN GW selection for multiple PDN connections with S2a	8.0.0	8.1.0
2008-03	SP-39	SP-080167	0002	1	C	IP address allocation and protocol configuration using DHCP	8.0.0	8.1.0
2008-03	-	-	-	-	-	Update by MCC to correct Figure 8.2.1.4-1 due to error in implementing CR0049R3	8.1.0	8.1.1
2008-06	SP-40	SP-080387	0038	5	F	PDN GW function	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0140	1	C	On providing indication to UE about the mobility mode protocol selected	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0152	6	B	Trusted/untrusted non-3GPP access network detection	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0159	2	F	Harmonization of Access Authentication in non-3GPP networks with SA3 specification	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0163	1	C	Handling of UE initiated resource request at HO to non-3GPP accesses for pre-existing flows	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0165	5	B	Addition of description of inter-system mobility policies	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0166	5	C	Addition of description of the DSMIPv6 home link detection function	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0170	4	F	Clarification on terms of Trusted and Untrusted non-3GPP networks	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0171	4	F	Clarification on simultaneous access to EPS	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0173	3	F	ANDSF-initiated transactions	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0174	3	F	Clarifications on the information provided by ANDSF	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0175	2	F	ANDSF - Removal of editor's note about privacy	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0176	3	C	ANDSF	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0177	2	F	Clarification of forwarding behaviour of S-GW on the S103 reference point	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0181	4	C	Update to 23.402 for dedicated resource-allocation	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0182	1	F	Updating HSS Initiated Subscribed QoS Modification Procedure for PMIP-based S5/S8	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0183	2	F	Updating Protocol Stack for Trusted and Untrusted 3GPP Accesses	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0185	2	C	Revised DNS Function for Service Selection	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0186	2	C	PDN GW-AAA Server-HSS Interaction clean up	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0189	2	C	FFS Removal	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0199	2	C	Clarification to the S2c Bootstrapping via DSMIPv6 Home Link	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0200	2	C	Clarification for connectivity with multiple PDNs with PMIP.	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0201	3	C	Clarification for multiple PDNs and the mobility protocols used.	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0211	5	C	IP address(es) allocation in PMIP based S5/S8	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0213	2	F	GTP-PMIP Roaming via an Interworking Proxy	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0220	5	F	Clarification on ePDG selection	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0222	1	F	Clarification on IP address allocation for non-3GPP IP access networks	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0223	4	F	Removing PCC flow details from TS 23.402	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0224	1	D	Removing note about HRPD credentials in E-UTRAN -> HRPD Handover	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0225	1	F	Clarification on MN NAI in trusted non-3GPP accesses	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0227	1	F	Adding reference to PP2 spec on CDMA interworking to TS 23.402	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0228	3	B	Additional CDMA interworking related storage parameters	8.1.1	8.2.0
2008-06	SP-40	SP-080388	0229	6	C	Completion of missing functionality for PMIP-based S8-S2 chaining (Section 4)	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0230	7	C	Completion of missing functionality for PMIP-based S8-S2	8.1.1	8.2.0

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
						chaining (Section 6)		
2008-06	SP-40	SP-080384	0231	2	C	Completion of missing functionality for PMIP-based S8-S2 chaining (Section 7)	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0232	6	C	Completion of missing functionality for PMIP-based S8-S2 chaining (Section 8)	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0244	3	F	Refining of Optimized handover from HRPD to E-UTRAN	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0245	2	F	Alignment of Release Old context at optimized inter-access handover between E-UTRAN and HRPD	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0246	1	F	Alignment of Release Old context at optimized inter-access handover between E-UTRAN and HRPD	8.1.1	8.2.0
2008-06	SP-40	SP-080434	0261	4	C	Alignment of non-3GPP to 3GPP Handover and Attach procedures	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0262	-	F	23.402 Clean-up	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0263	-	C	PDN GW identification	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0266	1	C	Preventing misuse of DSMIPv6 CoA	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0268	2	F	Alignment of Section 12 with other relevant AAA functions and features	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0278	1	F	Limitation of the frequency of UE requested ANDSF interactions	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0279	1	F	Clarification on the IPv6 prefix delegation and IPv4 Home address allocation for S2c	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0280	1	F	IP Mobility Mode Selection FFS cleanup	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0281	1	F	ANDSF FFS cleanup	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0282	-	F	S2c Handover FFS cleanup	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0283	-	F	S2c Multiple PDN FFS cleanup	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0284	2	F	S2c Untrusted Attach FFS cleanup	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0287	1	F	Corrections on IPv4 home address assignment for S2c initial attachment procedure	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0288	-	F	Corrections of references	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0290	2	C	Support for handover with multiple PDNs in TS 23.402	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0291	2	C	Handling Multiple PDN during handover attach procedure	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0293	1	F	Clarification to the use of IPSec assosciation for S2c Handover.	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0296	-	F	External authentication when S2c is used	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0297	2	B	PMIP-based S5/S8 support for GPRS procedures	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0298	1	C	Partial support of PCC - FFS Removal	8.1.1	8.2.0
2008-06	SP-40	SP-080383	0302	2	F	Clarification on PDN GW selection for S2c	8.1.1	8.2.0
2008-06	SP-40	SP-080384	0305	-	F	Cleaning up Annex C	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0317	-	F	Removal of editor notes from Initial attach procedure over S2a	8.1.1	8.2.0
2008-06	SP-40	SP-080382	0320	1	F	Access network discovery information	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0321	1	C	PDN GW information provisioning for GTP- based S8-S2 chaining	8.1.1	8.2.0
2008-06	SP-40	SP-080385	0324	1	F	Handling of multiple PDNs during Idle mode mobility from E-UTRAN to HRPD	8.1.1	8.2.0
2008-06	SP-40	SP-080386	0327	2	B	S101 tunnel redirection	8.1.1	8.2.0
2008-06	SP-40	SP-080387	0328	1	F	Updated architecture figure for optimised handover between HRPD and E-UTRAN	8.1.1	8.2.0

History

Document history		
V8.2.0	November 2008	Publication