WiMAX Forum® Network Architecture

Architecture, Detailed Protocols and Procedures

WiMAX® - 3GPP EPS Interworking

WMF-T37-009-R016v01

WiMAX Forum® Approved

(2010-11-30)

WiMAX Forum Proprietary

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability

Table of Contents

List of Figures

1. Introduction and Document Scope

3GPP Technical Specification 23.402 [4] specifies the stage 2 service description for providing IP connectivity using non-3GPP IP accesses (e.g. WLAN, WiMAX, HRPD etc.) to the 3GPP EPS. TS 23.402 [4] covers both roaming and non-roaming scenarios and covers all aspects related to the usage of non-3GPP IP accesses, including mobility between 3GPP and non-3GPP accesses, policy control and charging, and authentication.

This document specifies Stage 2 & 3 specifications for interworking between Mobile WiMAX® and Release-8 3GPP Evolved Packet System (EPS). The purpose of this document is to identify the requirements and impacts to the WiMAX network for interworking with 3GPP EPS and not to duplicate the content of TS 23.402 [4].

This specification assumes that the mobile terminal can operate in dual-radio mode i.e. both radios can transmit and receive simultaneously. Single-Radio operation will be covered in separate specification. This specification also assumes dual mode mobile terminal is connected to common 3GPP Core (EPC) via WiMAX ASN. Scenario where dual mode mobile terminal is connected to common WiMAX Core (CSN) via 3GPP access is not supported.

2. Abbreviations and Definitions

2.1 Abbreviations

For the purposes of the present document, following abbreviations apply

PMIP6	Proxy Mobile IP version 6
EPC	Evolved Packet Core
EPS	Evolved Packet System
S-GW	Serving Gateway
P-GW	PDN Gateway
ANID	Access Network Identity
MAG	Mobile Access Gateway

2.2 Terms & Definitions

Dual Radio Handover: In dual radio handovers *both* radios can be ON (can be simultaneously receiving and transmitting) at any given time during the handover process.

3. References

[1] WiMAX Forum® Mobile System Profile

[2] 3GPP TS 23.401, "GPRS Enhancements for E-UTRAN Access (Release 8)".

[3] 3GPP TS 23.402, "Architecture Enhancements for non-3GPP accesses (Release 8)".

[4] 3GPP TS 33.402, “3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses; (Release 8)”.

[5] IETF RFC 3344, “IP Mobility Support for IPv4”.

[6] IETF RFC 3775, “Mobility Support in IPv6”.

[7] 3GPP TS 23.203, “Policy and Charging Control Architecture (Release 8)”.

[8] 3GPP TS 24.302, “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (Release 8)”.

[9] 3GPP TS 23.003, “Numbering, Addressing and Identification”.

[10] IETF RFC 4187, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”.

[11] IETF RFC 3748, “Extensible Authentication Protocol (EAP)”.

[12] 3GPP TS 24.312, “Access Network Discovery and Selection Function (ANDSF) Management Object (MO); (Release 8)”.

[13] IETF Internet-Draft, draft-ietf-mext-binding-revocation, "Binding Revocation for IPv6 Mobility", work in progress.

[14] IETF RFC 5446, “Service Selection for Mobile IPv4”.

[15] 3GPP TS 29.273, “3GPP EPS AAA interfaces (Release 8)”.

[16] IETF RFC 2794, “Mobile IP network Access Identifier Extension for IPv4”.

[17] IETF RFC 5213, “Proxy Mobile IPv6”.

[18] IETF RFC 5448, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')”.

4. General Requirements and Principles

General concepts for interworking between 3GPP accesses and WiMAX® networks as specified in section 4.1.2 of TS 23.402 [4] shall apply.

General principle for handovers with optimizations between 3GPP Accesses and Mobile WiMAX as specified in section 10.1.1 (General Principles) of TS 23.402 [4] shall also apply.

5. Interworking Network Reference Model

This section defines the Network Reference Model for the interworking the 3GPP Evolved Packet System (EPS) with the Mobile WiMAX® system defined in the TS 23.402 [4] as Trusted Non-3GPP IP Access system.

The WiMAX ASN may be deployed directly by the 3GPP operator or by a WiMAX Operator which has a Contractual Agreement with the 3GPP operator to provide the ASN.

5.1 Non-Roaming Architecture

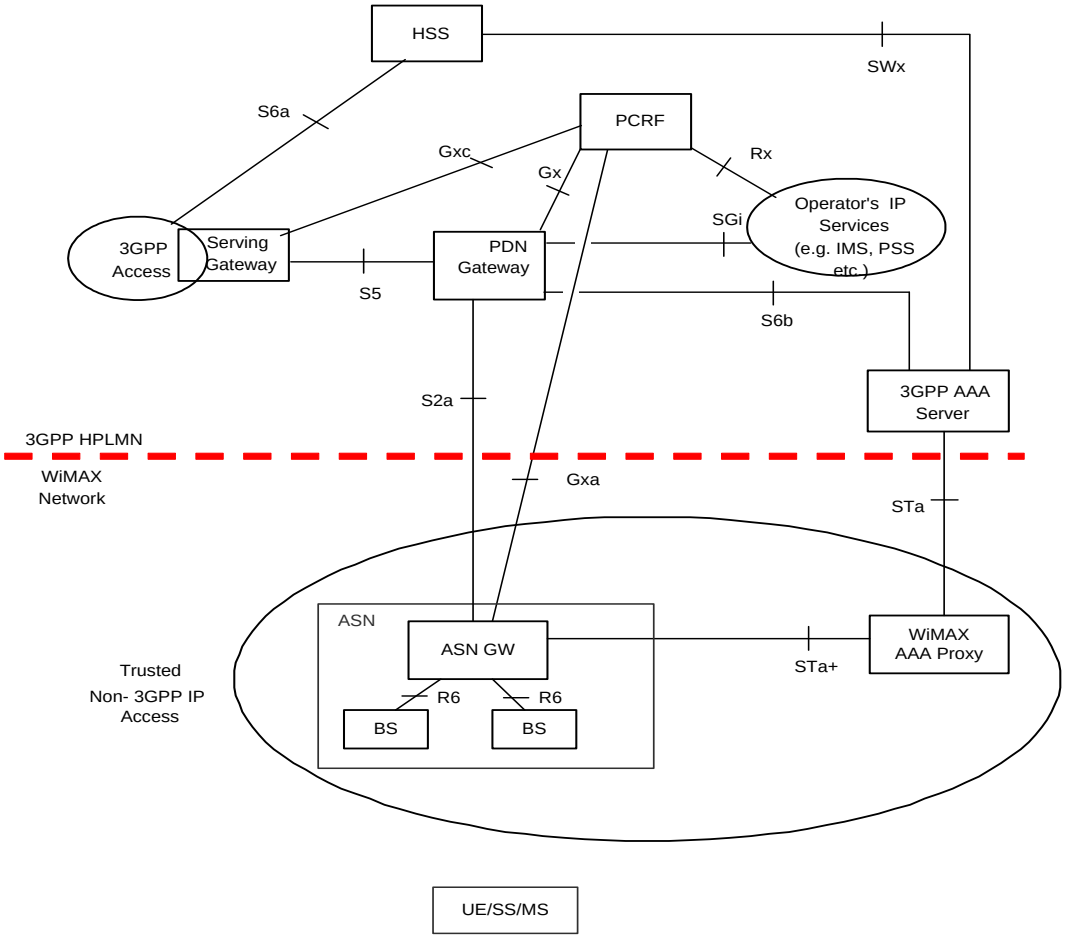

Figure 6-1 – 3GPP-WiMAX Non-Roaming Architecture

5.2 Roaming Architecture

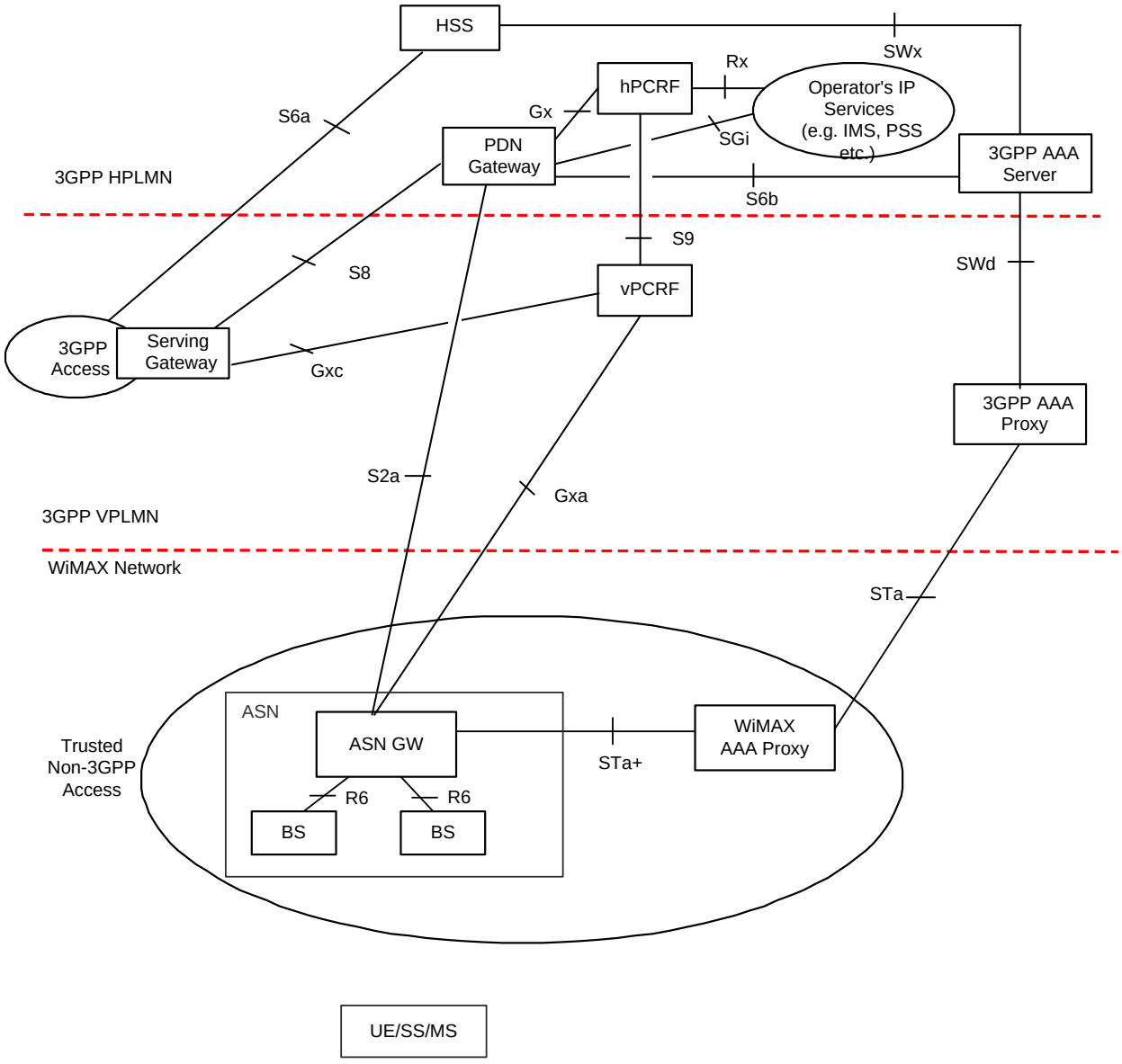

Figure 6-2 – 3GPP-WiMAX® Roaming Architecture - Home Routed

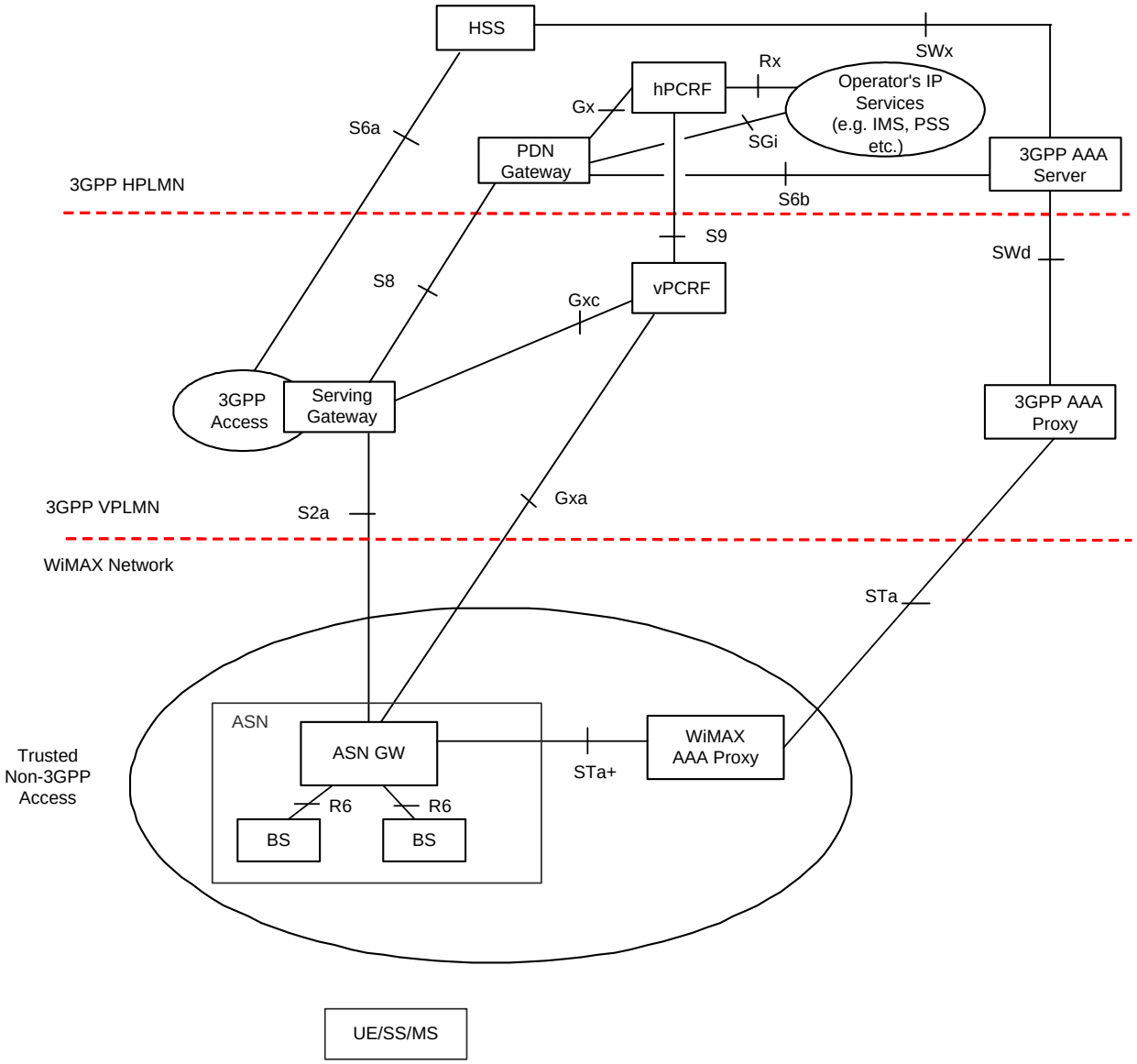

Figure 6-3 – 3GPP-WiMAX® Roaming Architecture (Chained PMIP-based S8 + S2a) - Home Routed

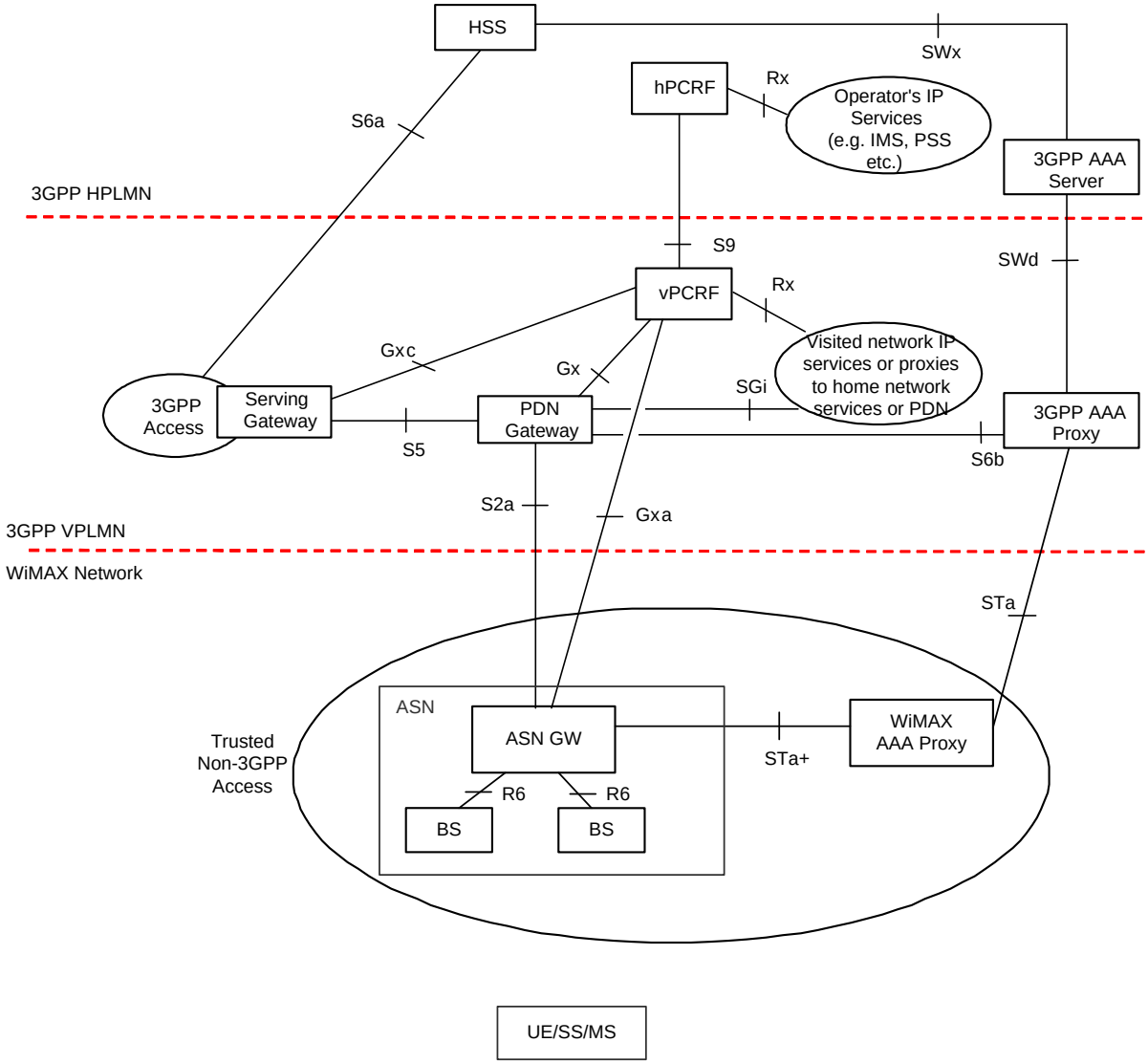

Figure 6-4 – 3GPP-WiMAX® Roaming Architecture– Local Breakout

5.3 Reference point mapping

The reference points relevant for interworking between the WiMAX® networks and 3GPP networks are described below:

S2a: This reference point provides the user plane and the related mobility management procedures between the WiMAX access network and 3GPP core network. It is defined between the Mobile Access Gateway (MAG) in WiMAX ASN-GW and 3GPP PDN Gateway. In case that the Mobile IPv4 is used as S2a protocol then the WiMAX side of this reference point SHALL be terminated by the MIP4 Foreign Agent function. This reference point is specified in 3GPP TS 23.402 [4].

The S2a corresponds to the PMIP6 part of R3 reference point of WiMAX NRM [1].

STa: This reference point is defined between the WiMAX AAA Proxy and the 3GPP AAA Server/Proxy function in the 3GPP Evolved Packet Core. It is used to carry the access authentication, authorization, QoS, accounting and mobility information related to a specific subscriber. Stage 2 for STa reference point is defined in the 3GPP TS 23.402 [4]. Stage 3 for STa reference point is defined in TS 29.273 [16].

STa+: This reference point is defined between the Authenticator function in the WiMAX ASN and the WiMAX AAA Proxy function. It is used to carry WiMAX specific attributes in addition to 3GPP AAA attributes define in STa [16].

6. PDN-GW Selection

Note: This release of the specification only supports a single PDN connection – the default PDN connection. The PDN Type could be IPv4, IPv6 or IPv4v6.

The WiMAX® ASN shall be responsible for PDN-GW selection for the default PDN connection. The PDN-GW selection mechanism is defined in TS 23.402 [4], section 4.5.1 with following modification. The PDN-GW selection is based on the following information received from the AAA/HSS:

- PDN-GW identifier information in the UE's subscription record for the default APN, which could be a logical name (FQDN) or IP address.
- APN information in the UE's subscription record if there is no PDN-GW identifier information present for the default APN.

If the PDN-GW identifier is available and the value is an IP address, the WiMAX ASN shall use this IP address received from AAA/HSS as part of access authentication as the PDN-GW's IP address for the default PDN connection.

If the PDN-GW identifier is available and it is a FQDN, the WiMAX ASN shall perform DNS resolution using that FQDN for PDN-GW address selection.

If the PDN-GW identifier is not available, the WiMAX ASN shall perform DNS based PDN-GW address resolution for the default APN.

If the UE's subscription allows it to have a PDN-GW assignment in VPLMN, the HSS record shall indicate that to the WiMAX ASN. The WiMAX ASN selects a PDN-GW in the VPLMN. This selection can be based on static configuration in the WiMAX ASN or using APN. If the WiMAX ASN cannot derive a PDN-GW address in the VPLMN, it shall use the APN information to resolve a PDN-GW address in the HPLMN.

7. Access Network Discovery and Selection

7.1 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 MS/UE, based on network triggers, and respond to requests from the MS/UE.

The detailed functionality for ANDSF is defined in section 4.8.2 of TS 23.402 [4]. ANDSF discovery shall be done as per section 4.8.4 of TS 23.402 [4].

7.1.1 Architecture for ANDSF

The following architecture shall be used for access network discovery and selection using ANDSF. Details of communication over S14 are specified in section 6.8 of TS 24.302 [9].

Note: ANDSF is a 3GPP Rel-8 specified network element that exists in the hPLMN of the 3GPP EPC.

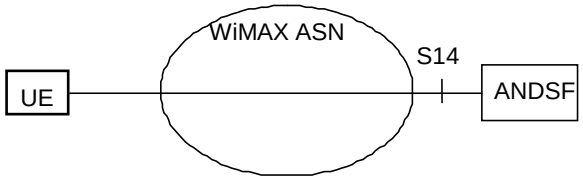

Figure 8-1 – Architecture for ANDSF

7.1.2 ANDSF Management Objects

General ANDSF Management Objects parameters and Management Objects for WiMAX networks are defined in 3GPP TS 24.312 [13].

8. Initial Attach to 3GPP EPC via WiMAX® ASN

8.1 Initial Attach Procedure with PMIP6 on S2a

Initial Attach Procedure with PMIP6 over S2a for home routed (anchoring at PDN-GW) and non-roaming, roaming, and local break-out are is defined in Section 6.2.1 of TS 23.402[4]. The initial attach procedure with PMIP6 on chained S2a and PMIP based S8 is defined in Section 6.2.4 of TS 23.402 [4]. WiMAX® specific triggers and procedures for home routed PMIP6 on S2a are highlighted below.

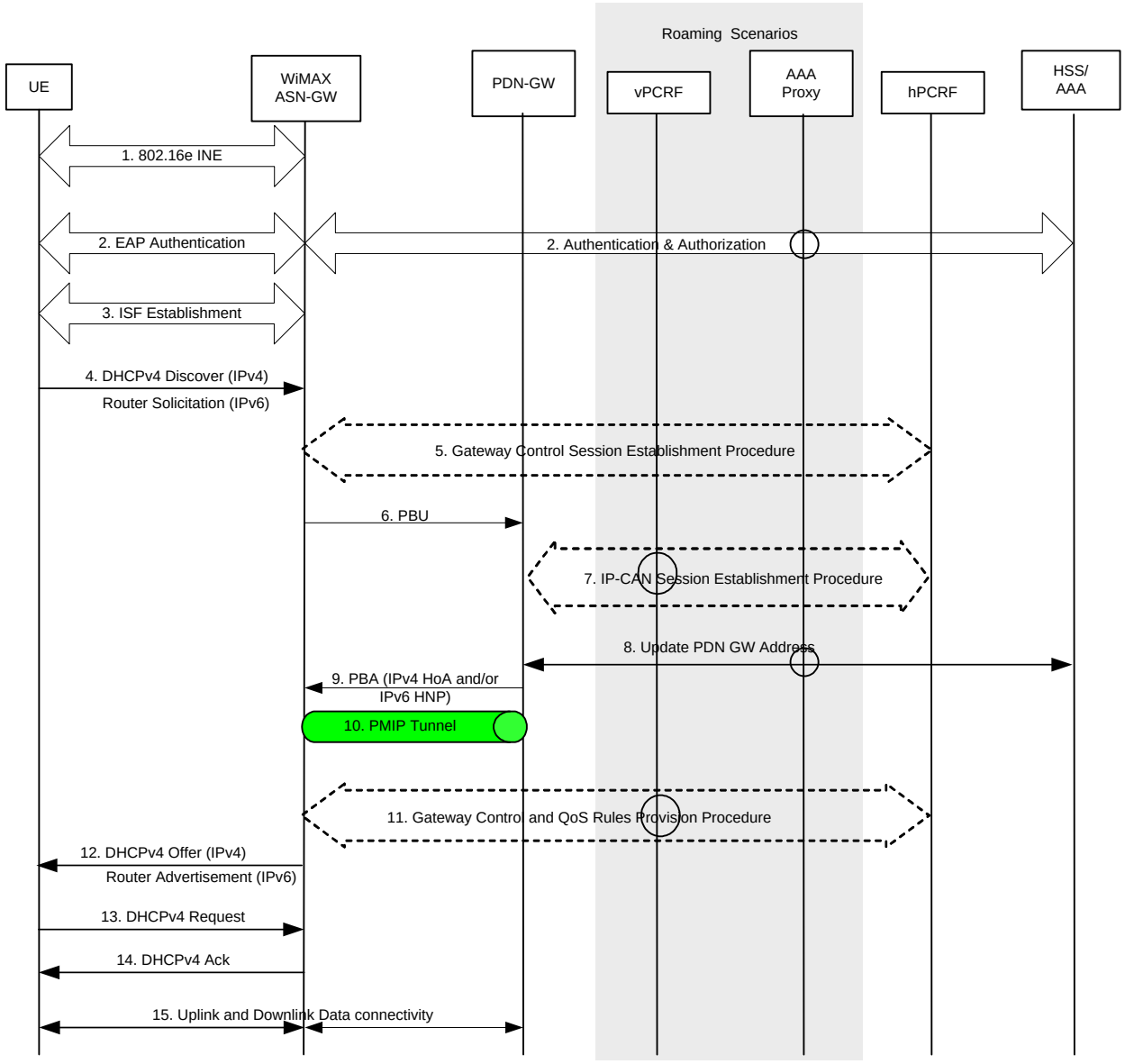

Figure 9-1 – Initial attachment with 3GPP EPC over S2a (PMIP6)

The optional interaction steps between the ASN and PDN gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in each gateway. The vPCRF and the AAA-Proxy are only involved in roaming and local break-out scenarios.

1) The initial WiMAX network entry procedures are performed up to the point where EAP authentication is triggered as defined in WiMAX NWG specification[1].

2) The EAP authentication procedure is initiated and performed involving the MS/UE. Details of EAP based access authentication procedure is specified in section 11.1. The PDN Gateway address is determined at this point as described in section 4.5.1 of TS 23.402.

   Note: ASN-GW knows that it is connecting to 3GPP EPC based on static pre-configuration

   Note: Device Authentication based on X.509 certificates is not applicable.

3) After successful authentication and authorization, the ASN will try to establish the Initial Service Flow(s) to the MS/UE according to the authorized PDN type downloaded during access authentication. If IPv4v6 is authorized, the ASN will try to establish one IPv4 ISF and one IPv6 ISF. The MS/UE may reduce the ISFs to only the PDN type it supports.

4) The MS/UE initiates either DHCPv4 for IPv4 or RS for IPv6 addressing or both for default PDN connection. The attach will always be treated as “Initial Attach”.

5 -11) Steps 5 to 11 are the same as defined under section 6.2.1 of TS 23.402[4] with following additional clarification. The PDN Type sent in PBU will be set to the type of ISFs established between the ASN and the MS/UE in step 4, i.e., IPv4, IPv6 or IPv4v6. The requested IP address type will be set corresponding to the PDN Type. If the PDN Type is IPv4, the requested IP address is IPv4 HoA. If PDN Type is IPv6, the requested IP address is IPv6 HNP. If the PDN Type is IPv4v6, both IPv4 HoA and IPv6 HNP are requested. The protocol configuration parameters in PCO are set and used according to the following clarification:

   If the ASN is configured to support DHCP proxy, the PCO in PBU will contain additional protocol configuration parameters necessary for MS/UE IP stack configuration. These parameters may include DNS server or P-CSCF server, depending on what MS/UE has asked for in DHCPDISCOVER message. The ASN is also responsible to translate the configuration parameters received from PCO in PBA sent by the PDN-GW, into the DHCPOFFER and DHCPACK messages sent to the MS/UE. For IPv6 MS/UE, these parameters need to be sent in PCO even if they are not received in RS. IPv6 MS/UE will use stateless DHCPv6 for parameter configuration after it has configured IPv6 address using SLAAC. In this case, the ASN is responsible to translate the configuration parameters received from PCO into the DHCPv6 Reply message.

   If the ASN is configured to support DHCP relay, configuration parameters need not be included in PCO. They are provided by the PDN-GW after PMIP tunnel establishment, when the ASN will relay the DHCP message to the PDN-GW. The PDN-GW acts as a DHCP server and provides all requested configuration parameters.

12) ASN-GW sends the DHCPv4 offer to MS/UE with assigned MN-HoA or RA with assigned IPv6 HNP.

13 - 14) MS/UE complete the DHCP procedure configuring the previously offered IP address. Steps 13 and 14 apply for IPv4 address allocation case only.

15) IP connectivity between the MS/UE and the PDN-GW for default PDN connection is set for uplink and downlink directions.

8.2 Initial Attach Procedure with CMIP4 on S2a

Initial Attach Procedure with CMIP4 over S2a is defined in Section 6.2.3 of TS 23.402[4] WiMAX specific triggers and procedures are highlighted below.

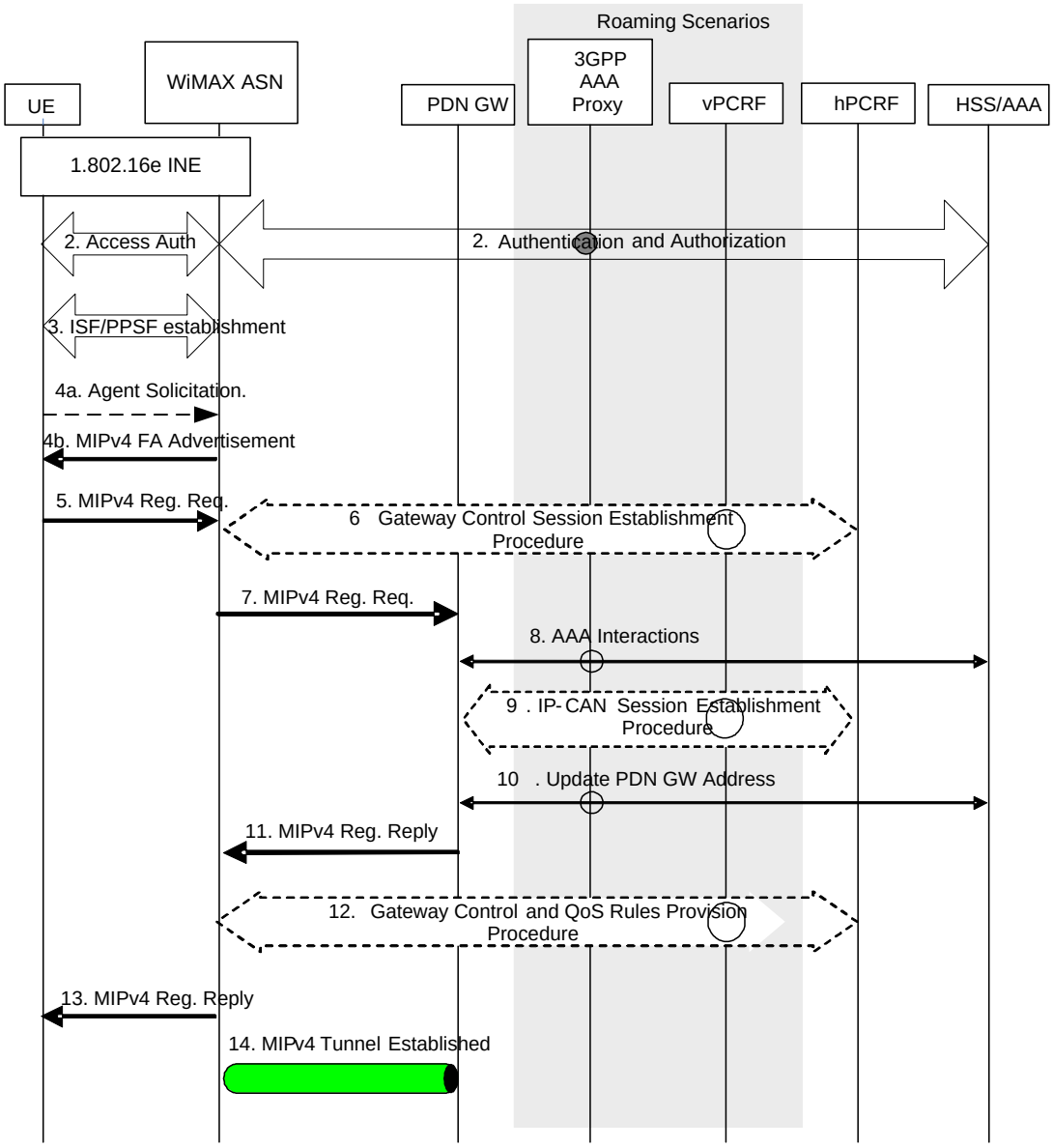

Figure 9-2 – Initial attachment with 3GPP EPC over S2a (CMIP4)

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

1) The initial WiMAX network entry procedures are performed up to the point where EAP authentication is triggered as defined in WiMAX NWG specification [1].

2) The EAP authentication procedure is performed as per section 11.1. The PDN-GW information is returned from the 3GPP AAA Server to the Authenticator at this point. The 3GPP AAA Server also returns to the Authenticator the MN NAI (permanent IMSI based MN NAI) to be used to identify the UE in Gateway Control Session Establishment messages (step 6).

After the successful authentication, both UE and AAA derive the MIP-RK, SPI, and other mobility keys such as FA-RK, MN-FA, MN-HA-CMIP4 that will be used for the security protection in CMIP4 registration messages.

3) After successful authentication and authorization, an Initial Service Flow (ISF) and/or the Pre-provisioned Service Flows (PPSF) are established for the MS within the ASN.

4) The FA in WiMAX ASN sends a Foreign Agent Advertisement (FAA) message to the MS/UE. The FAA message includes the Care-of Address (CoA). The MS/UE sends an Agent Solicitation to FA if the MS/UE doesn't receive FAA message after successful ISF establishment.

5) The MS/UE sends a Registration Request (RRQ) message to the FA as specified in RFC 3344 [6]. The NAI included in the RRQ shall be a permanent IMSI based MN NAI. The MS/UE sets the HA address field to ALL_ZERO_ONE address and it is updated when the Registration Reply is received from the FA.

The Authentication Extension in the RRQ should be calculated using keys derived in the step 2.

6 -12) Steps 6 to 12 are exactly same as defined under section 6.2.3 of TS 23.402[4].

Note: The selected PDN-GW obtains Authentication and Authorization information from the AAA/HSS at step 8.

13) The FA processes the RRP (MN-NAI, Home Address, Home Agent Address) according to RFC 3344[6] and sends a corresponding RRP message to the MS/UE.

14) IP connectivity from the MS/UE to the PDN-GW is now setup. A MIP tunnel is established between the FA in the ASN-GW and the PDN-GW.

9. Detach Procedure

9.1 MS/UE initiated detach procedure

9.1.1 MS/UE initiated detach procedure using PMIP6

Figure 10-1 presents MS/UE initiated detach procedure over S2a (PMIP6).

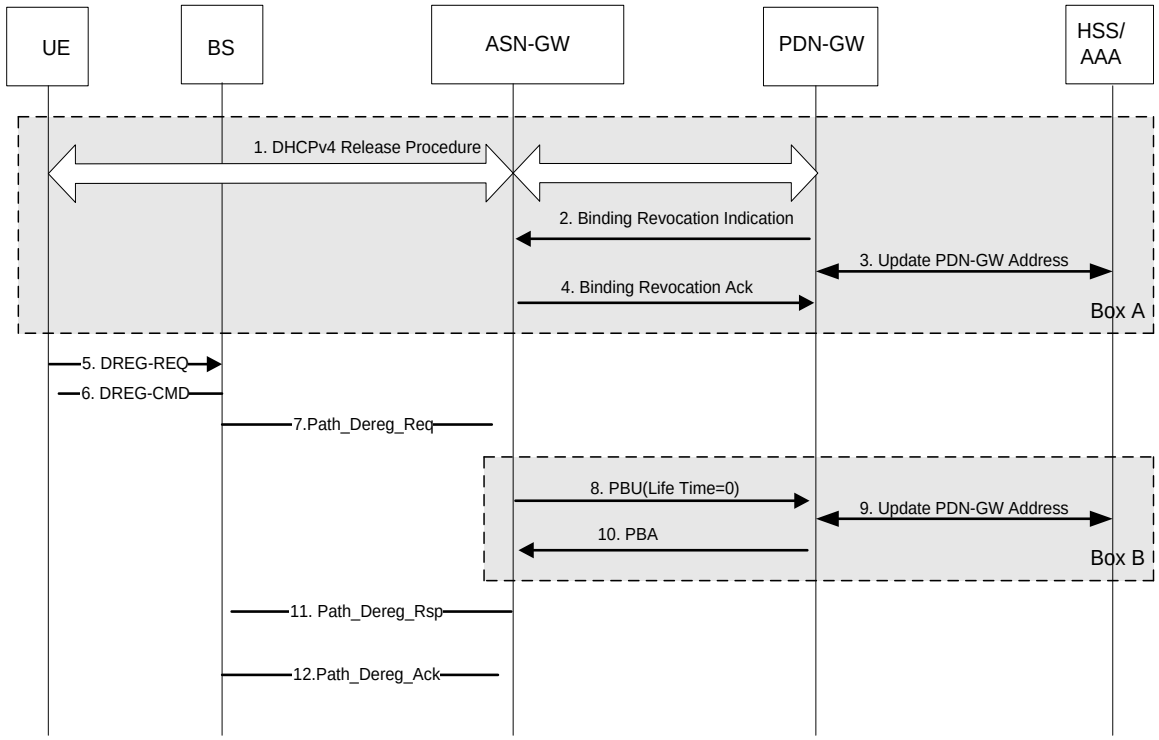

Figure 10-1 – MS/UE Initiated Detach Procedure over S2a (PMIP6)

1) MS/UE may initiate DHCPv4 Release Procedure in case of PMIP6 connection setup with DHCPv4. For IPv6 case, there is no DHCPv6 release procedure for the case of PMIP6 connection setup with stateless auto-configuration.

2) If the DHCPv4 Release is performed in step 1, the PDN-GW sends a Binding Revocation Indication message with Revocation Trigger field set to “8” i.e. User Initiated Session(s) Termination to Mobile Access Gateway (MAG) as defined in draft-ietf-mext-binding-revocation [14].

3) Then the PDN-GW updates the PDN GW identity information corresponding to the UE's PDN connection in the AAA Server/HSS. This identity information is de-registered from the HSS as described in clause 12 of TS 23.402 [4].

4) The MAG returns a Binding Revocation Acknowledgement message to the PDN GW.

Note：The steps 1 to 4 in the Box A occur in case ASN-GW acts as DHCP Relay.

5) MS/UE initiates detach procedure by sending a DREG_REQ message with De-Registration Request Code=0x00 to BS.

6) BS sends DREG_CMD message to the MS/UE with Action code=0x04.

7) BS sends *Path_Dereg_Req* message over R6 to the ASN-GW.

8）Upon receipt of a *Path_Dereg_Req* message over R6, if MS/UE did not perform DHCPv4 Release procedure in step 1, then the ASN-GW SHALL trigger MIP tunnel Release procedure with PDN-GW by sending PBU message with lifetime value set to "0".

9) The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information as described in step 3.

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

Note：The steps 8 to 10 in the Box B occur in case ASN-GW acts as DHCP Proxy.

11) ASN-GW sends a *Path_Dereg_Rsp* message over R6 to the BS.

12) BS sends *Path_Dereg_Ack* over R6 to the ASN-GW.

9.1.2 MS/UE initiated detach procedure using CMIP4

Figure 10-2 presents MS/UE initiated detach procedure over S2a (CMIP4).

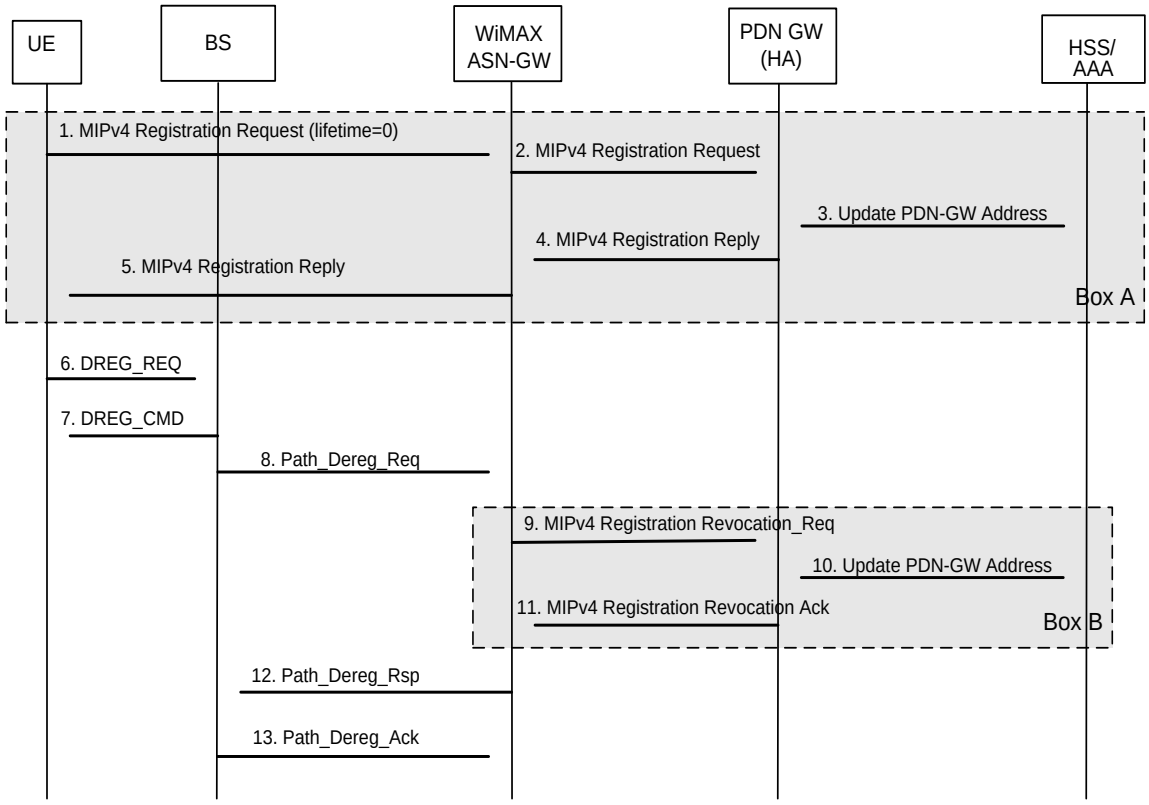

Figure 10-2 – MS/UE Initiated Detach Procedure over S2a (CMIP4)

1) MS/UE may perform MIP4 Registration Request (lifetime=0).

Note: Step 1 is expected to be performed by the MS/UE however in some cases the MS/UE may directly execute step 6 by sending *DREG-REQ*.

2) ASN-GW sends MIP4 Registration Request (lifetime=0) over S2a to PDN-GW.

3) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information corresponding to the UE's PDN connection. This information is de-registered from the HSS as described in clause 12 of TS23.402 [4].

4) The PDN-GW deletes all existing entries implied in the Registration Request message from its Binding Cache and sends a Registration Reply to the ASN-GW.

5) The ASN-GW sends a Registration Reply (lifetime=0) to the MS/UE.

6) MS/UE initiates a detach procedure by sending a DREG_REQ message with De-Registration Request Code=0x00 to BS.

7) BS sends DREG_CMD message to the MS/UE with Action code=0x04.

8) BS sends *Path_Dereg_Req* message over R6 to the ASN-GW.

9) Upon receipt of a *Path_Dereg_Req* message over R6, if the MS/UE did not perform MIP De-registration procedure in step 1, then the ASN-GW performs a MIP Revocation procedure (as shown under step 9 to 11 in Box B) by sending a Registration Revocation Req message to the PDN-GW.

10) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information as described in step 3.

11) The PDN-GW deletes all existing entries implied in the Registration Revocation Req message from its Binding Cache and sends a Registration Revocation Ack message to the ASN-GW.

12) ASN-GW sends a *Path_Dereg_Rsp* message over R6 to the BS.

13) BS sends *Path_Dereg_Ack* over R6 to the ASN-GW.

9.2 Network initiated detach procedure

9.2.1 ASN-GW/BS initiated detach procedure using PMIP6

Figure 10-3 presents ASN-GW or BS initiated detach procedure over S2a (PMIP6). The ASN/ASN-GW initiates the detach procedure during administration graceful shutdown. The BS initiate the detach procedure when it determines a loss of link with the MS/UE.

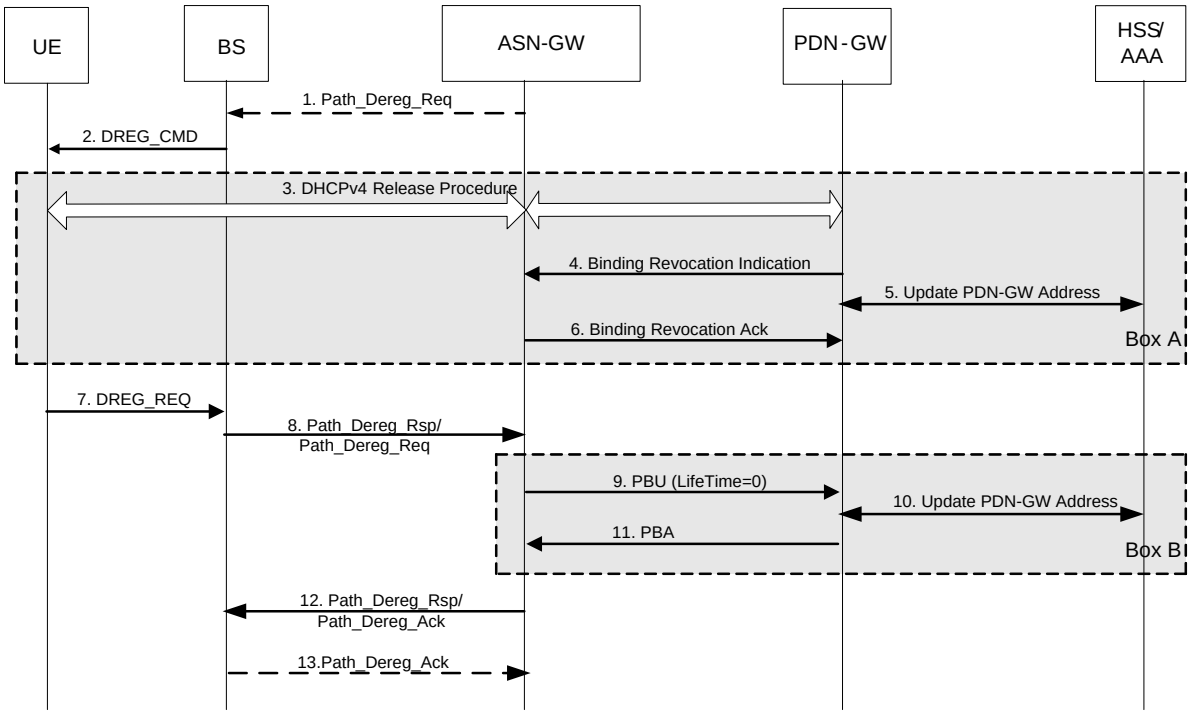

Figure 10-3 – ASN-GW/BS Initiated Detach Procedure over S2a (PMIP6)

1) ASN-GW determines that MS/UE detach is required (i.e. administration reasons) and then initiates data path deregistration procedure by sending Path_Dereg_Req message over R6 to BS with Action Code TLV set to indicate MS/UE detach from the network.

   Note: This step is only needed in case of ASN-GW initiated Detach.

   Note: Alternate network exit procedure is also allowed using *NetExit_MS_State_Change_Req/Rsp* message from ASN-GW as specified in section 4.5.2.1.2.4 of NWG Stage 3 specification [1].

2) BS sends DREG_CMD message to the MS/UE including Action Code=0x00.

   Note: This is the first step in case of BS initiated Detach.

3) The MS/UE may initiate DHCPv4 Release Procedure in case of PMIP6 connection setup with DHCPv4. For IPv6 case, there is no DHCPv6 release procedure for the case of PMIP6 connection setup with stateless auto-configuration.

4) If the DHCPv4 Release is performed in step 3, the PDN-GW sends a Binding Revocation Indication message with Revocation Trigger field set to “8” i.e. User Initiated Session(s) Termination to Mobile Access Gateway (MAG) as defined in draft-ietf-mext-binding-revocation [14].

5) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information corresponding to the UE's PDN connection. This information is de-registered from the HSS as described in clause 12 of TS 23.402 [4].

6) The MAG returns a Binding Revocation Acknowledgement message to the PDN-GW.

Note：Steps 3 to 6 in the Box A occur in case ASN-GW acts as DHCP Relay.

7) The MS/UE sends a DREG_REQ message with De-Registration Request Code=0x02 to BS.

8) For ASN-GW initiated Detach, BS sends *Path_Dereg_Rsp* message over R6 to the ASN-GW. Otherwise, for BS initiated Detach, BS will send *Path_Dereg_Req* message over R6 to the ASN-GW in order to start tearing down the R6 data path.

9) Upon receiving either a *Path_Dereg_Rsp* or *Path_Dereg_Req* message over R6, if MS/UE did not perform DHCPv4 Release procedure in step 3, the ASN-GW triggers MIP tunnel Release procedure with PDN-GW by sending PBU message with lifetime value set to “0”.

10) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information as described in step 5.

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

Note：The steps 9 to 11 in the Box B occur in case ASN-GW acts as DHCP Proxy.

12) For ASN-GW initiated Detach, the ASN-GW will send a *Path_Dereg_Ack* message over R6 to the BS. Otherwise, for BS initiated Detach, the ASN-GW will send a *Path_Dereg_Rsp* message over R6 to the BS.

13) For BS initiated Detach, the BS sends a *Path_Dereg_Ack* message over R6 to the ASN-GW.

Note: For Idle mode, since there is no data path, only steps 9-11 are needed.

9.2.2 HSS/AAA initiated detach procedure using PMIP6

Figure 10-4 presents HSS/AAA initiated detach procedure over S2a (PMIP6). 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.

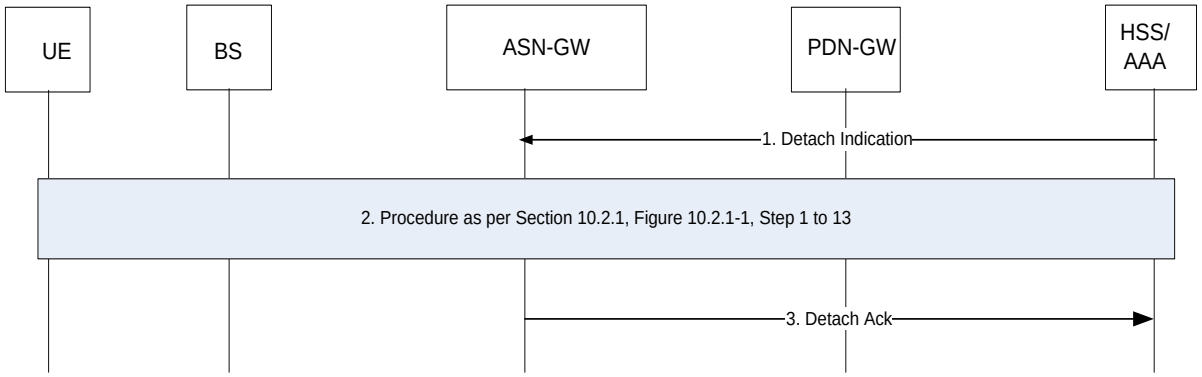

Figure 10-4 – HSS/AAA Initiated Detach Procedure over S2a (PMIP6)

1) The HSS/AAA sends a Detach Indication message to the Authenticator in the ASN-GW to detach a specific MS/UE.

   Authenticator sends a *NetExit_MS_State_Change_Req* message over R4 to MAG (Mobile Access Gateway)/Anchor DPF. MAG/Anchor DPF initiates the Data Path termination and MIP de-registration corresponding to the MS/UE's connections.

   If the Authenticator is located in the same ASN-GW with the MAG/Anchor DPF, the authenticator can send a *Path_Dereg_Req* message to the BS directly.

2) This includes step 1 to 13 as in Figure 10-3.

3) The MAG/Anchor DPF of the ASN-GW responds to the Authenticator by sending a *NetExit_MS_State_Change_Rsp* message to confirm the Data Path termination and MIP de-registration. The Authenticator sends a Detach Ack message to the HSS/AAA.

   If the Authenticator is located in the same ASN-GW with the MAG/Anchor DPF, the BS sends a *Path_Dereg_Rsp* message to the Authenticator directly.

9.2.3 ASN-GW/BS initiated detach procedure using CMIP4

Figure 10-5 presents an ASN-GW or BS initiated detach procedure over S2a (CMIP4). The ASN-GW initiates the detach procedure during administration graceful shut down. The BS initiates the detach procedure when it determines a loss of link with the MS/UE.

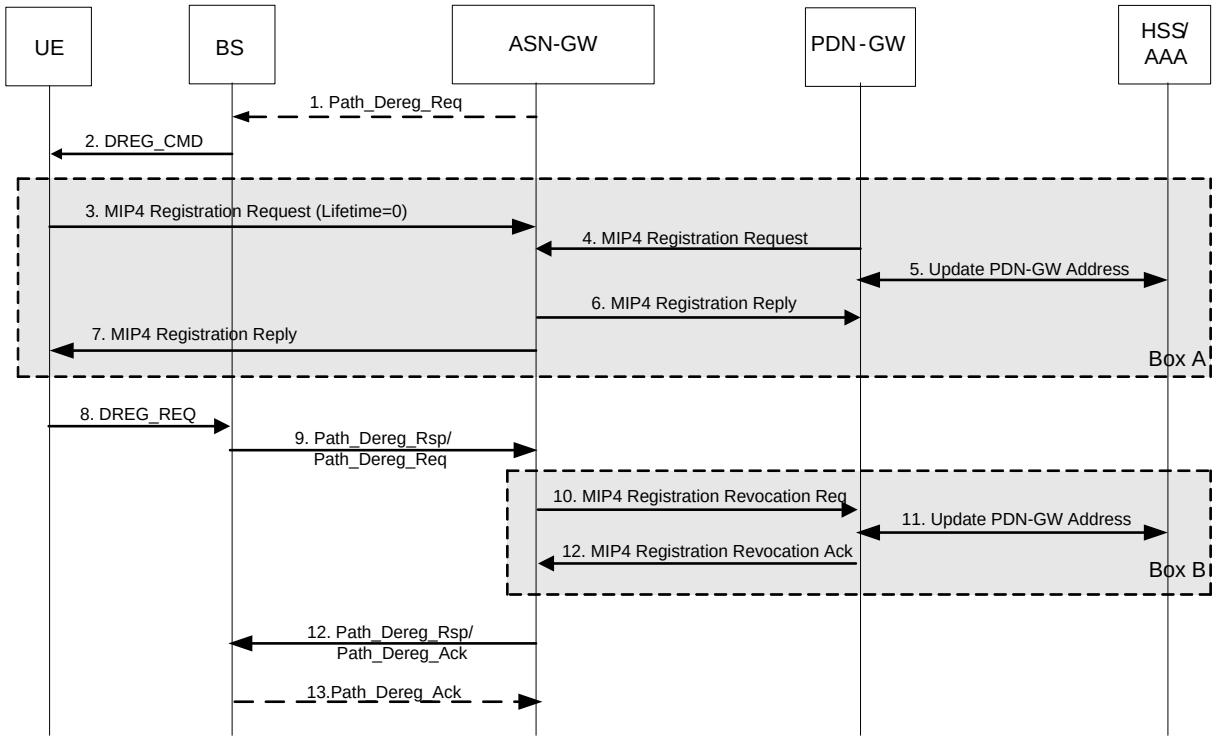

Figure 10-5 – ASN-GW/BS Initiated Detach Procedure over S2a (CMIP4)

1) ASN-GW determines that MS/UE detach is required (i.e. administration reasons) and initiates data path deregistration procedure by sending *Path_Dereg_Req* message over R6 to BS with Action Code TLV set to indicate MS/UE detach from the network.

   Note: This step is only needed in case of ASN-GW initiated Detach.

   Note: Alternate network exit procedure is also allowed using *NetExit_MS_State_Change_Req*/*Rsp* message from ASN-GW as specified in section 4.5.2.1.2.4 of NWG Stage 3 specification [1].

2) Either BS determined that MS/UE detach is required or triggered by ASN-GW *Path_Dereg_Req* message, the BS sends DREG_CMD message to the MS/UE including Action Code=0x00.

   Note: This is the first step in case of BS initiated Detach.

3) The MS/UE may perform MIP4 Release Procedure by sending Registration Request (lifetime=0) message.

4) The ASN-GW sends MIP4 Registration Request (lifetime=0) over S2a to PDN-GW.

5) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information corresponding to the UE's PDN connection. This information is de-registered from the HSS as described in clause 12 of TS 23.402[4].

6) The PDN-GW deletes all existing entries implied in the Registration Request message from its Binding Cache and sends a Registration Reply to the ASN-GW.

7) The ASN-GW sends a Registration Reply (lifetime=0) to the MS/UE.

Note: Step 3 is expected to be performed by the MS/UE however in some cases the MS/UE may directly send a *DREG-REG* message.

8) MS/UE sends a DREG_REQ message with De-Registration Request Code=0x02 to BS.

9) For ASN-GW initiated Detach, BS will send *Path_Dereg_Rsp* message over R6 to the ASN-GW. Otherwise, for BS initiated Detach, BS will send *Path_Dereg_Req* message over R6 to the ASN-GW in order to start tearing down the R6 data path.

10) Upon receipt of a *Path_Dereg_Req* or *Path_Dereg_Rsp* message over R6, if the MS/UE does not perform MIP De-registration procedure in step 3, then the ASN-GW shall perform a MIP Revocation procedure (steps 10 to 12 in Box B) by sending a Registration Revocation Req message to the PDN-GW.

11) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information as described in step 5.

12) The PDN-GW deletes all the existing entries implied in the Registration Revocation Req message from its Binding Cache and sends a Registration Revocation Ack message to the ASN-GW.

13) For ASN-GW initiated Detach, the ASN-GW will send a *Path_Dereg_Ack* message over R6 to the BS. Otherwise, for BS initiated Detach, the ASN-GW will send a *Path_Dereg_Rsp* message over R6 to the BS.

14) For BS initiated Detach, the BS sends a *Path_Dereg_Ack* message over R6 to the ASN-GW.

Note: For Idle mode, since there is no data path, only steps 10-12 are needed.

9.2.4 HSS/AAA initiated detach procedure using CMIP4

Figure 10-6 presents HSS/AAA initiated detach procedure over S2a (CMIP4). 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.

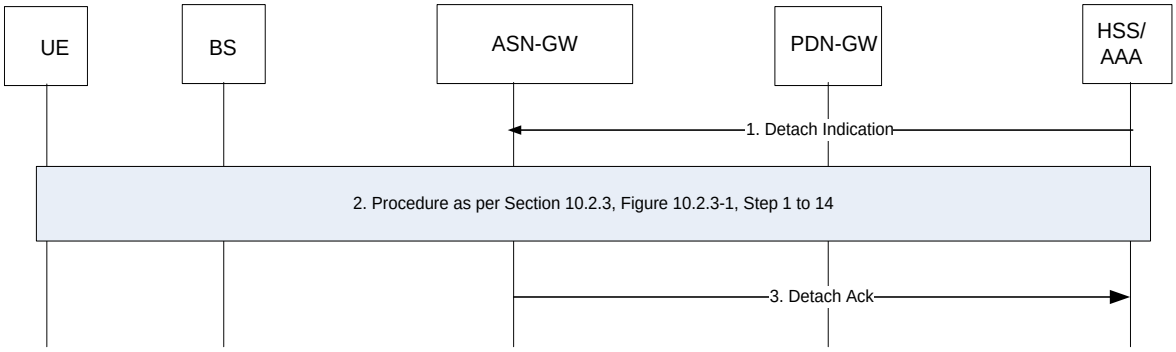

Figure 10-6 – HSS/AAA Initiated Detach Procedure over S2a (CMIP4)

1) The HSS/AAA sends a Detach Indication message to the Authenticator in ASN-GW to detach a specific MS/UE. The NAI and APN shall be included. The MN NAI identifies the MS/UE to detach. The APN is needed in order to determine which PDN-GW to deregister the MS/UE from, as some PDN-GWs may support multiple PDNs.

   Authenticator sends a *NetExit_MS_State_Change_Req* message over R4 to FA/Anchor DPF. FA/Anchor DPF initiates the Data Path termination and MIP de-registration corresponding to the MS/UE's PDN connections.

   If the authenticator is located in the same ASN with the FA/Anchor DPF, the authenticator can send a *Path_Dereg_Req* message to the BS directly.

2) This includes step 1 to 14 as in Figure 10-5.

3) The FA/Anchor DPF responds to the Authenticator by sending a *NetExit_MS_State_Change_Rsp* message to confirm the Data Path termination and MIP de-registration. The Authenticator sends a Detach Ack message to the HSS/AAA.

   If the authenticator is located in the same ASN with the FA/Anchor DPF, the BS sends a *Path_Dereg_Rsp* message to the Authenticator directly.

10. Authentication and Security

This section defines the authentication process for Access Control to the 3GPP core network, i.e. to permit or deny a subscriber to attach to and use the resources of a WiMAX® IP access which is interworked with the EPC network. WiMAX access authentication signalling is executed between the MS and the 3GPP AAA server/HSS.

3GPP based access authentication is executed across the STa reference point as per section 6. The MS/UE shall have a permanent ID that is an IMSI-based NAI as defined in TS 23.003 [10] for the initial authentication.

The WiMAX-3GPP dual mode device shall support EAP-AKA' [19] for the purpose of interworking with 3GPP.

10.1 Use of EAP-AKA' – Initial Authentication

For initial authentication, both MS/UE and 3GPP AAA/HSS SHALL execute the EAP-AKA' protocol [19] as specified in subclause 6.2 (Authentication and key agreement for trusted access) of TS 33.402 [5]. For execution of this protocol, both MS/UE and the 3GPP AAA/HSS SHALL set the ANID value to "WIMAX".

10.2 Use of EAP-AKA' – Fast Re-Authentication

EAP-AKA' Fast Re-Authentication shall be supported per IETF RFC 5448 [19]. Use of EAP-AKA' Fast Re-Authentication shall be as per 3GPP TS 33.402 [5].

10.3 Key derivation from EMSK

Key derivation from EMSK shall be as per 3GPP TS 33.402[5].

11. IP Address Allocation

11.1 IP Address Allocation in WiMAX® Networks using CMIP4 on S2a

IP Address allocation in WiMAX® networks using CMIP4 on S2a shall be as per RFC 3344[6].

11.2 IP Address Allocation in WiMAX using PMIP6 on S2a

IP address allocation in WiMAX using PMIP6 on S2a shall be as per section 4.7.2 of TS23.402[3].

Note: DHCP relay which is collocated in ASN-GW needs to be stateless, so ASN-GW will not send PBU with lifetime=0, as per section 4.7.2 of 3GPP TS 23.402 [3].

12. IP Mobility Mode Selection

IP Mobility Mechanism is statically configured in the MS/UE and network if operator plans to deploy a network with single mobility mechanism. For network supporting multiple mobility mechanism (PMIP6 & MIP4 FA-CoA), IP Mobility Mode is selected by HSS/AAA based on the information it has regarding the MS/UE, local/home network capabilities and local/home network policies. Support of CMIP4 and/or PMIP6 at WiMAX® ASN is known to HSS/AAA through static pre-configuration.

For WiMAX® ASN and EPC supports multiple protocols following principle applies:

- During initial attach over WiMAX, PMIP6 is used for providing connectivity. WiMAX ASN shall not send Agent Advertisement to MS/UE. If AAA/HSS indicates PMIP6 is not allowed, then the WiMAX ASN uses MIP4 and sends Agent Advertisements to MS/UE.

- During handover from 3GPP to WiMAX, PMIP6 is used for providing connectivity over WiMAX. WiMAX ASN shall not send Agent Advertisement to MS/UE. If AAA/HSS indicates PMIP6 is not allowed, then the WiMAX ASN uses MIP4 and sends Agent Advertisements to MS/UE.

13. Handover

13.1 WiMAX® to 3GPP access handover procedures

13.1.1 WiMAX® to E-UTRAN over GTP based S5/S8

General procedure for handover from WiMAX access to E-UTRAN access over GTP based S5/S8 interface is specified in section 8.2.1.1 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after handover to E-UTRAN is as defined in Section 15.

13.1.2 WiMAX® to E-UTRAN over PMIP6 based S5/S8

General procedure for handover from WiMAX access to E-UTRAN access over PMIP6 based S5/S8 interface is specified in section 8.2.1.2 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after handover to E-UTRAN is as defined in Section 15.

13.1.3 WiMAX® to UTRAN/GERAN over GTP based S5/S8

General procedure for handover from WiMAX access to UTRAN/GERAN access over GTP based S5/S8 interface is specified in section 8.2.1.3 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after handover to UTRAN/GERAN is as defined in Section 15.

13.1.4 WiMAX® to UTRAN/GERAN over PMIP6 based S5/S8

General procedure for handover from WiMAX access to UTRAN/GERAN access over PMIP6 based S5/S8 interface is specified in section 8.2.1.4 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after handover to UTRAN/GERAN is as defined in Section 15.

13.2 3GPP access to WiMAX®

13.2.1 Handover from 3GPP to WiMAX® with PMIP6

The steps involved in the handover from 3GPP Access connected to the EPC to WiMAX access connected to the EPC 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 MS/UE is served by the 3GPP Access, a PMIP6 or GTP tunnel is established between the S-GW and the PDN-GW in the evolved packet core.

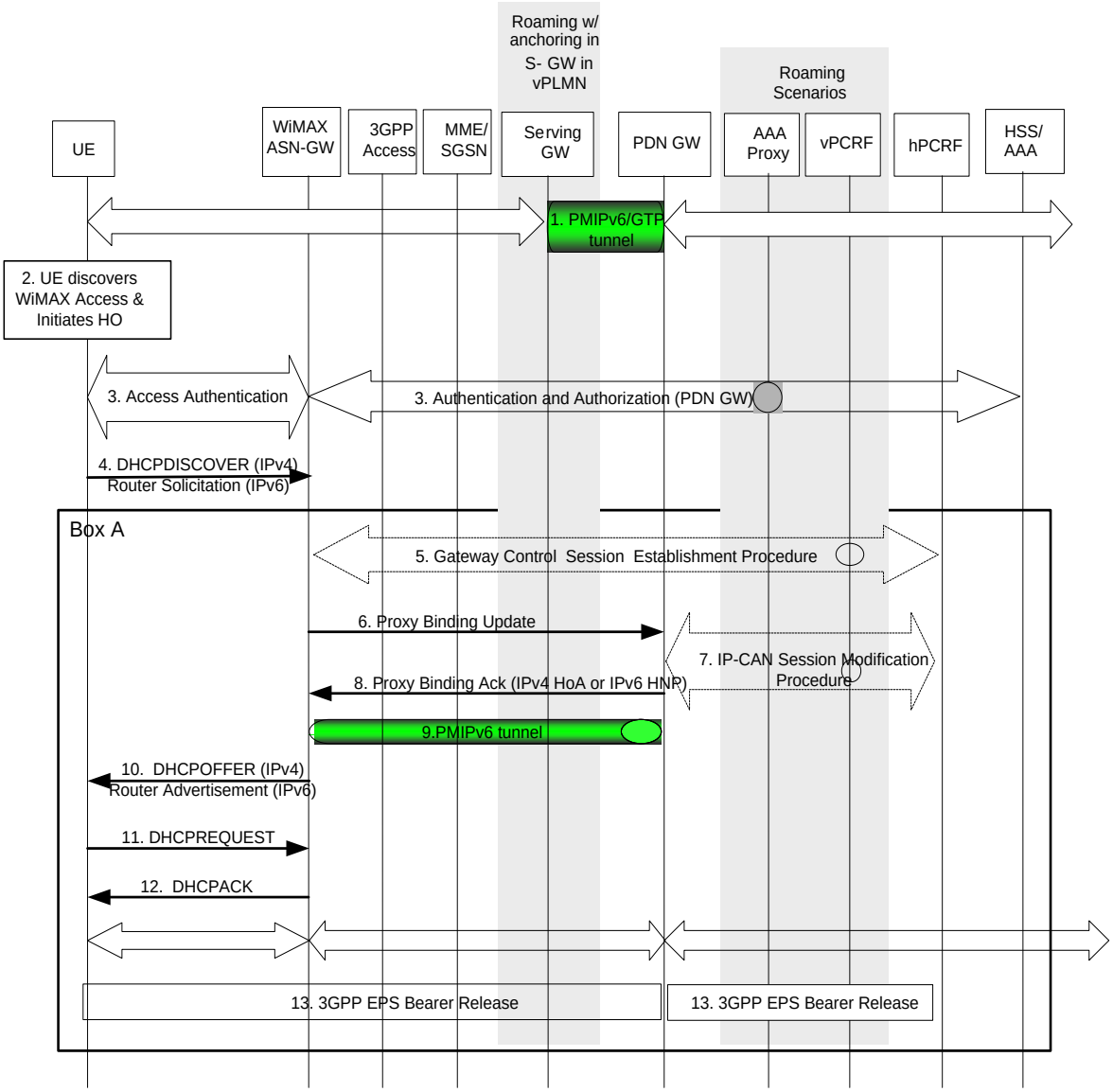

Figure 14-1 – Handover from 3GPP Access to WiMAX® with PMIP6 on S2a

The optional interaction steps between the gateways and the PCRF in Figure 14-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1) The MS/UE is connected in the 3GPP Access and has a PMIP6 or GTP tunnel on the S5 interface.

2) The MS/UE discovers the WiMAX access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered WiMAX access system. The mechanisms that aid the MS/UE to discover the WiMAX access system are specified in chapter 8 (Access Network Discovery and Selection).

3) The MS/UE performs access authentication and authorization in the WiMAX access system. The 3GPP AAA server authenticates and authorizes the MS/UE for access in the trusted non-3GPP system. The 3GPP AAA server queries the HSS and returns the PDN-GW address to the WiMAX access system at this step (upon successful authentication and authorization).

   Note: Device authentication based on X.509 certificates is not applicable.

   PDN-GW address selection is as described in the section 4.5.1 of 3GPP TS 23.402 [4].

4) After successful authentication and authorization, the DHCP DISCOVER (for IPv4) or Router Solicitation (for IPv6) procedure is triggered. The Router Solicitation message will be optional if the attach type was known at step 3.

5-8) Steps 5-8 under Box A are described as steps 5-8 in section 8.2.2 of 3GPP TS 23.402 [4].

Note: Steps 5-6 can happen anytime after step 3.

Note: In absence of “Attach Type” received over WiMAX access, if a PDN-GW for the default APN is returned to the WiMAX access during access authentication in step 3, the Handover Indicator in PBU (step 6) shall be set to ‘\”4” – Handover state unknown. Otherwise, Handover Indicator shall be set to “1” – attach over new interface.

9) The PMIP6 tunnel is set up between the WiMAX ASN-GW and the PDN-GW.

10) The ASN-GW sends the DHCP OFFER to the MS/UE with assigned MN-HoA or Router Advertisement with assigned IPv6 HNP.

11-12) For IPv4 case, the MS/UE configures the previously offered IPv4 address via DHCPv4 signalling.

13) Step 13 under box A is described as steps 12 in section 8.2.2 of 3GPP TS 23.402 [4].

13.2.2 Handover from 3GPP to WiMAX® with CMIP4

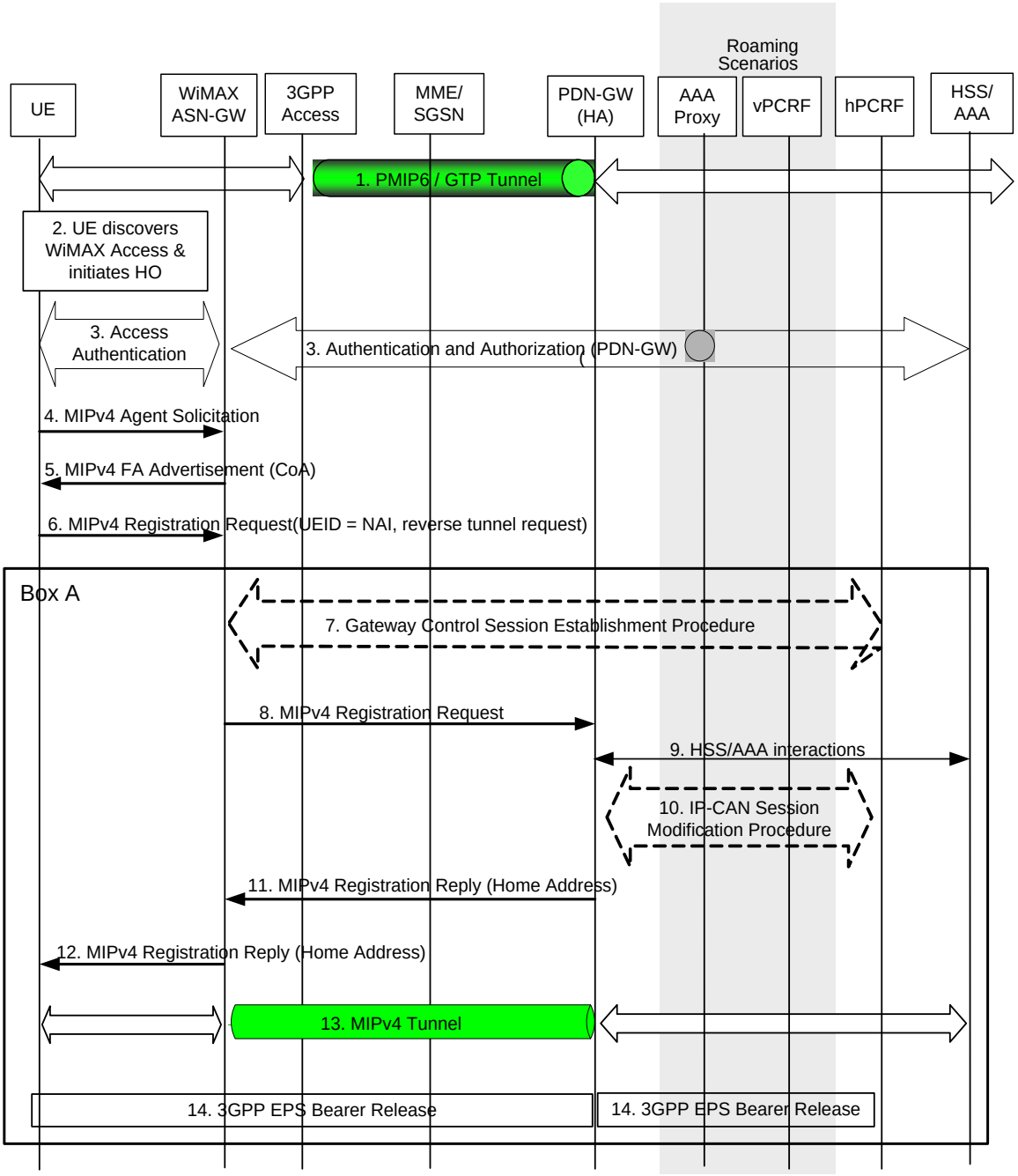

Figure 14-2 – 3GPP IP Access to WiMAX® Handover with CMIP4 on S2a

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 MS/UE is connected in the 3GPP Access and has a PMIP6 or GTP tunnel on the S5 interface.

2) The MS/UE discovers the WiMAX access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered WiMAX access system. The mechanisms that aid the MS/UE to discover the WiMAX access system are specified in chapter 8 (Access Network Discovery and Selection).

3) The MS/UE performs access authentication and authorization in the WiMAX access system. The 3GPP AAA server authenticates and authorizes the MS/UE for access in the WiMAX system. The 3GPP AAA server queries the HSS and returns the PDN-GW address to the ASN at this step (upon successful authentication and authorization).

   After the successful authentication, both MS/UE and AAA derive the MIP-RK, SPI, and other mobility keys such as FA-RK, MN-FA, MN-HA-CMIP4 that will be used for the security protection in CMIP4 registration messages.

4) The MS/UE may send an Agent Solicitation message (AS) RFC 3344 [6] to trigger the Handover procedure.

5) The FA sends a Foreign Agent Advertisement message (FAA) (RFC 3344 [6]) to the MS/UE. The FAA message includes the Care-of Address (CoA) of the Foreign Agent function in the FA. The number of times this message is sent can be configured.

6) The MS/UE sends a Registration Request (RRQ) (MN-NAI, lifetime) message as defined in RFC 3344 [6] to the FA as specified in RFC 3344 [6]. 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 [17]. The MS/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 MS/UE then receives the IP address of the PDN Gateway in step 12 as part of the Registration Reply (RRP) message. The MS/UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages.

   The Authentication Extension in the RRQ should be calculated using keys derived in the step 3.

7-14) Steps 7-14 under Box A are described in section 8.3 of 3GPP TS 23.402 [4].

14. Resource Deactivation Procedures

14.1 PDN GW initiated Resource Deactivation using PMIP6

The procedure described in this section is used for releasing of resources in WiMAX® system after handover to 3GPP access.

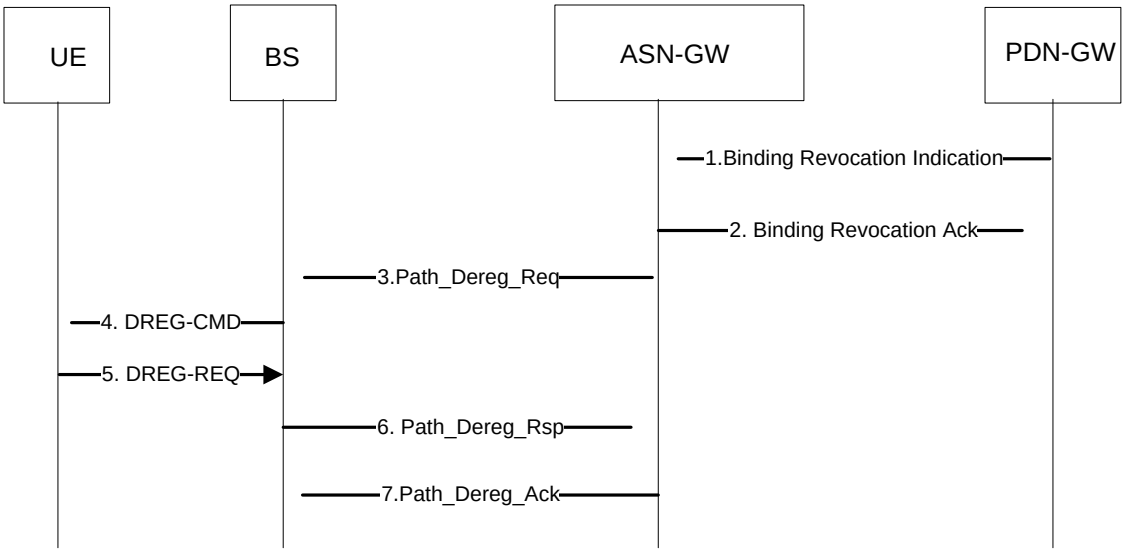

Figure 15-1 – PDN-GW Initiated resource deactivation (PMIP6)

1) PDN-GW initiates the Binding Revocation procedure by sending Binding Revocation Indication to the MAG as defined in draft-ietf-mext-binding-revocation [14]. For Handover, Revocation trigger indicates Inter-MAG Handover over different Access Types.
2) MAG in ASN-GW sends Binding Revocation Ack to acknowledge the successful resource release procedure.
3) ASN-GW determines that MS/UE detach is required and then initiates data path deregistration procedure by sending *Path_Dereg_Req* message over R6 to BS with Action Code TLV set to indicate MS/UE detach from the network to release the connection.
4) BS sends DREG_CMD message to the MS/UE including Action Code=0x00.
5) MS/UE sends a DREG_REQ message with De-Registration Request Code=0x02 to BS.
6) BS sends *Path_Dereg_Rsp* message over R6 to the ASN-GW.
7) ASN-GW sends a *Path_Dereg_Ack* message over R6 to the BS.

Note: For Idle mode, since there is no data path, only steps 1-2 are needed.

15. Policy and Charging Control

Note: PCC procedure assumes support of 3GPP Rel-8 PCC framework as defined in TS 23.402 [4] and TS 23.203 [8]. 3GPP PCC Rel-8 framework in context of WiMAX needs additional considerations and is outside the scope of this release of specification.

16. MS/UE implications

16.1 MS/UE Identities

MS/UE identities SHALL be as per section 4.6 of 3GPP TS 23.402 [3].

16.2 CMIP4 security key derivation

MS/UE SHALL derive CMIP4 security keys as per section 9.2.1.2.2 of TS 33.402 [5].

Note: This is not an implication on the MS/UE as CMIP4 security key derivation defined in TS 33.402 [5] and WiMAX specification [1] are same.

17. AAA implications

AAA Server SHALL derive CMIP4 security keys as per section 9.2.1.2.2 of TS 33.402[4].

Note: This is not an implication on the AAA as CMIP4 security key derivation defined in TS 33.402 [4] and WiMAX specification [1] are same.

18.1 WiMAX AAA Proxy Requirements

The WiMAX AAA Proxy may receive accounting records from the WiMAX ASN-GW. In response to “Accounting Request” the AAA Proxy SHOULD send the ASN-GW an “Accounting Response” using “Acct-Status-Type” with the value set to “8” (i.e. Accounting-off).

The WiMAX AAA proxy SHOULD discard the accounting information.

18. Accounting implications

In a WiMAX® 3GPP EPC interworking scenario, the subscriber is assumed to have a 3GPP network subscription only. In 3GPP, the PDN-GW generates the accounting records & User Data Records (UDR) for any access technology. Accounting records for a session using WiMAX access are generated by the 3GPP EPC & thus, no accounting records are needed from the WiMAX access.

Since ASN-GW generates the accounting records as a mandatory default behavior, the WiMAX accounting records are not needed for EPC IWK. For EPC IWK, ASN-GW sends “Accounting Request” to WiMAX AAA proxy and WiMAX AAA proxy upon receiving “Accounting Request” SHOULD send an “Accounting Response” using “Acct-Status-Type” with the value set to “8” (i.e. Accounting-off).

The WiMAX AAA proxy SHOULD discard the accounting information.