

Attachment 4-2-3

WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures

IP Multimedia Subsystem (IMS) Interworking

WMF-T33-101-R015v01

Note: This Document is reproduced without any modification with the consent of the WiMAX Forum®, which owns the copyright in them.



WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures

IP Multimedia Subsystem (IMS) Interworking

WMF-T33-101-R015v01

WiMAX Forum[®] Approved

(2009-11-21)

WiMAX Forum Proprietary

Copyright © 2007-2009 WiMAX Forum. All Rights Reserved.

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

Copyright 2007-2009 WiMAX Forum. All rights reserved.

The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for download from the WiMAX Forum and may be duplicated for internal use, provided that all copies contain all proprietary notices and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or distributed without the express written authorization of the WiMAX Forum.

Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance of the following terms and conditions:

THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY.

Any products or services provided using technology described in or implemented in connection with this document may be subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable jurisdiction.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.

The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, technologies, standards, and specifications, including through the payment of any required license fees.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT.

IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS MEMBERS RELATING TO THE USE OF THIS DOCUMENT.

The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is solely responsible for determining whether this document has been superseded by a later version or a different document.

“WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum. Third-party trademarks contained in this document are the property of their respective owners.

Table of Contents

1.	DOCUMENT SCOPE.....	7
2.	ABBREVIATIONS AND DEFINITIONS	8
2.1	Abbreviations	8
2.2	Terms & Definitions	9
3.	REFERENCES.....	10
4.	REQUIREMENTS AND PRINCIPLES	13
4.1	System Requirements	13
4.2	MS Requirements	14
4.2.1	IMS Client - Concepts and Principle.....	14
5.	NETWORK REFERENCE MODEL.....	15
5.1	Non-roaming Architectures	15
5.2	Roaming Architectures	16
5.3	Impacts to 3GPP and 3GPP2 IMS architecture	17
6.	IMS PRIVATE HEADERS.....	18
7.	PROCEDURES, MESSAGES, AND TLVS.....	19
7.1	IP Address Management and IP Version Interworking	19
7.1.1	IP Address Management	19
7.1.2	IP Version Interworking.....	19
7.2	P-CSCF Discovery	19
7.2.1	DHCP Proxy in ASN	20
7.2.2	DHCP Relay in ASN.....	21
7.2.3	P-CSCF Discovery for a Roaming User.....	22
7.3	Session Control.....	24
7.4	Emergency Services	24
7.4.1	IMS ES Network Reference Model (NRM) for a non-roaming user	25
7.4.2	IMS ES network reference model for a roaming user	25
7.4.3	ES call delivery for a non-roaming authenticated user and device.....	26
7.4.4	ES call delivery with a subscription less device or a user.....	28
7.4.5	ES call delivery during roaming.....	30
7.4.6	Initial network entry with an ES NAI	31
7.4.7	Prioritizing ES call.....	31
7.4.8	ES indicators	32
7.4.9	Interface between location server and ASN.....	32
7.5	QoS and PCC Procedures	32
7.5.1	IMS Session Establishment.....	32
7.5.2	IMS Session Establishment at Originating P-CSCF	34
7.5.3	IMS Session Modifications	35
7.5.4	IMS Session Termination.....	35
7.6	Charging Related Procedures and Correlation.....	36
7.7	Lawful Intercept	37
8.	STAGE 3 PROCEDURES.....	38
8.1	Detailed Procedures for IMS Private Headers	38
8.2	WiMAX specific values for Private Header	38

1	8.2.1	<i>P-Access-Network-Info</i>	38
2	8.2.2	<i>P-Charging-Vector</i>	39
3	8.3	DHCP Proxy in the ASN	39
4	8.3.1	<i>MS Requirements</i>	39
5	8.3.2	<i>DHCP Proxy requirements</i>	40
6	8.4	DHCP relay in the ASN.....	40
7	8.4.1	<i>MS Requirements</i>	40
8	8.4.2	<i>DHCP Relay requirements</i>	40
9	8.4.3	<i>DHCP Server requirements</i>	40
10	8.4.4	<i>P-CSCF Assignment requirements</i>	41
11	8.5	Hand Over Procedure during P-CSCF discovery	41
12	8.6	AAA Messages	43
13	8.6.1	<i>Radius Message between the AAA and the ASN</i>	43
14	8.6.2	<i>WiMAX Radius VSA Definition for P-CSCF Discovery</i>	44
15	8.7	Error Handling.....	45
16	8.7.1	<i>No P-CSCF IP address or FQDN in the Access Accept message</i>	46
17	8.7.2	<i>Inconsistent assignment of HA and P-CSCF</i>	46
18	8.7.3	<i>Timers consideration for DHCP Proxy in the ASN and DHCP Relay</i>	48
19	8.7.4	<i>Handling Error Condition</i>	48
20	9.	SECURITY ASPECTS	49
21	9.1	Inter-domain Security	50
22	9.2	Intra-domain Security	51
23	9.3	IMS access Authentication	51
24	10.	ANNEX A – INFORMATIVE NRM	52
25	11.	ANNEX B – CHARGING CORRELATION OF WIMAX ACCESS, PCC AND IM- CN	53
26			
27			

List of Figures

FIGURE 5-1: NON-ROAMING REFERENCE ARCHITECTURE OF THE IP MULTIMEDIA CORE NETWORK SUBSYSTEM INCLUDING THE WIMAX NETWORK ELEMENTS SUPPORTING MOBILITY. (MB STANDS FOR BEARER CONNECTION ONLY)	16
FIGURE 5-2: NON-ROAMING REFERENCE ARCHITECTURE OF THE IP MULTIMEDIA CORE NETWORK SUBSYSTEM INCLUDING THE WIMAX NETWORK ELEMENTS SUPPORTING SIMPLE IP. (MB STANDS FOR BEARER CONNECTION ONLY)	16
FIGURE 5-3: ROAMING REFERENCE ARCHITECTURE OF THE IP MULTIMEDIA CORE NETWORK SUBSYSTEM ANCHORED IN THE HOME NETWORK SUPPORTING MOBILE IP (MB STANDS FOR BEARER CONNECTION ONLY).....	17
FIGURE 5-4: ROAMING REFERENCE ARCHITECTURE OF THE IP MULTIMEDIA CORE NETWORK SUBSYSTEM ANCHORED IN THE VISITED NETWORK SUPPORTING MOBILE IP (MB STANDS FOR BEARER CONNECTION ONLY).....	17
FIGURE 7-1: P-CSCF DISCOVERY VIA DHCP PROXY PROCEDURE.....	20
FIGURE 7-2: P-CSCF DISCOVERY VIA DHCP RELAY PROCEDURE.....	21
FIGURE 7-3: P-CSCF DISCOVERY IN ROAMING	23
FIGURE 7-4: NETWORK REFERENCE MODEL TO DELIVER AN ES CALL THROUGH AN IMS NETWORK FOR A NON ROAMING USER.	25
FIGURE 7-5: NETWORK REFERENCE MODEL TO DELIVER AN ES CALL THROUGH AN IMS NETWORK FOR A ROAMING USER.	26
FIGURE 7-6: ES CALL DELIVERY FROM A NON-ROAMING DEVICE	27
FIGURE 7-7: ES CALL DELIVERY FROM A SUBSCRIPTION LESS DEVICE	29
FIGURE 7-8: ES CALL FROM A ROAMING DEVICE.....	30
FIGURE 7-9: CALL FLOW SHOWING PRIORITIZING ES CALL.....	31
FIGURE 7-10: IMS SESSION ESTABLISHMENT.....	33
FIGURE 7-11: IMS SESSION ESTABLISHMENT AT ORIGINATING P-CSCF	34
FIGURE 7-12: IMS SESSION MODIFICATION	35
FIGURE 7-13: IMS SESSION TERMINATION.....	36
FIGURE 7-14: CORRELATION OF IMS AND PCC CHARGING IDENTIFIERS (WIMAX DOMAIN NETWORK INCLUDES THE ACCESS NETWORK AND THE AAA)	37
FIGURE 8-1: – RESOLVING INCONSISTENT ASSIGNMENT OF HA AND P-CSCF	47
FIGURE 9-1: IMS SECURITY ARCHITECTURE.....	49
FIGURE 9-2: WIMAX AND IMS INTER DOMAIN SECURITY	50

1 **List of Tables**

2	TABLE 8-1 P-ACCESS_NETWORK_INFO	38
3	TABLE 8-2 ANCHOR DPF HO_REQ MESSAGE.....	41
4	TABLE 8-3 P-CSCF ATTRIBUTES IN FINAL RADIUS ACCESS-ACCEPT FROM AAA TO ASN	43
5	TABLE 8-4 ERROR PROCESSING DURING P-CSCF DISCOVERY	48

6

1 **Revision History**

November 6, 2009	Initial version of Release 1.5.
---------------------	---------------------------------

1. Document Scope

The scope of this document is to specify interwork of WiMAX Networks with the 3GPP Rel 7 and 3GPP2 IP Multimedia Subsystem (IMS). IMS is an open, standardized multi-media architecture for mobile and fixed IP services originally defined by the Third Generation Partnership Project (3GPP), and largely adopted by the Third Generation Partnership Project 2 (3GPP2). The IMS is based on standardized IETF protocols (e.g. SIP, DIAMETER, RTP). It is an access independent platform providing services in a standardized way. One of the main purposes of the IMS is to provide different kind of services from any location or access network where the IMS can be reached. In addition, the architecture is designed to allow dynamic QoS selection and flexible charging models (e.g., service-based and flow-based charging).

2. Abbreviations and Definitions

2.1 Abbreviations

ALG	Application Layer Gateway
AS	Application Server
ASN	Access Service Network
CMIP	Client Mobile IP
DNS	Domain Name server
E-CSCF	Emergency - Call Session Control Function
ES	Emergency Services
FQDN	Fully Qualified Domain Name
GPS	Global Positioning System
HA	Home Agent
h-HA	Home Agent located at the home network
hPCSCF	Proxy PCSF located at the home network
IBCF	Interconnection Border Control Function
IMS	IP Multimedia Subsystem
IM-CN	IP Multimedia – Core Network
LF	Location Function
LRF	Location Retrieval function
LS	Location Server
MIP	Mobile IP
NRM	Network Reference Model
NSP	Network Selection Provider
PCC	Policy and Charging Control
PCRF	Policy and Charging Rule Function
P-CSCF	Proxy –Call Session Control Function
PMIP	Proxy Mobile IP
PSAP	Public-safety Answering Point
PSTN	Public Switching Telecommunication Network
S-CSCF	Serving - Call Session Control Function
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
THIG	Topology Hiding Inter-network Gateway
UE	User Equipment
UICC	Universal Integrated Circuit Card

URI	Uniform Resource Identifier
URN	Uniform Resource Name
v-HA	Home Agent located at the visited network
vPCSCF	Proxy CSCF located at the visited network
HSS	- Home Subscriber Server
ISIM	- IM Services Identity Module
MS	- Mobile Station
LA	- Location Agent
LC	- Location Controller

1 **2.2 Terms & Definitions**

- 2 No new terms or definitions outside the references have been defined.

3. References

- [1]. IETF RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication"
- [2]. 3GPP TS 24.229, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", Release 7.
- [3]. 3GPP TS 33.203 "3G security; Access security for IP-based services", Release 7.
- [4]. 3GPP2 S.P0086-B "IMS Security Framework"
- [5]. 3GPP S3-070635. CR0105 rev5 against 33.203 Update to procedures to allow SIP Digest and TLS in IMS. Release 8 (Common IMS). July 2007
- [6]. IETF RFC 3455, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", January 2003.
- [7]. WiMAX Forum, T33-001-R015v01, "Detailed Protocols and Procedures, Base Specification", Release 1.5
- [8]. 3GPP TS 23.228, "IP Multimedia Subsystem (IMS)", Release 7
- [9]. 3GPP TS23.221, "Architectural requirements", Release 7
- [10]. TBD
- [11]. 3GPP TS 32.240, "Charging architecture and principles", Release 7
- [12]. 3GPPTS 32.260, "IP Multimedia Subsystem (IMS) charging", Release 7
- [13]. TBD
- [14]. 3GPP TS 23.002, "Network architecture", Release 7
- [15]. 3GPP TS 33.310 "3G security; Network Domain Security Authentication Framework (NDS/AF)", Release 7
- [16]. WiMAX Forum, T32-001-R015v01, T32-002-R015v01, T32-003-R015v01, T32-004-R015v01, T32-005-R015v01, "Architecture Tenets, Reference Model and Reference Points" Part0 to Part3 and Abbreviations, Release 1.5
- [17]. IETF RFC3261, "SIP: Session Initiation Protocol", June 2002.
- [18]. WiMAX Forum T33-102-R015v02, "Architecture, detailed Protocols and Procedures, Emergency Services Support", Release 1.5
- [19]. 3GPP TS 31.102, "Characteristics of the Universal Subscriber Identity Module (USIM) application", Release 7.
- [20]. 3GPP TS 31.103, "Characteristics of the IP Multimedia Services Identity Module (ISIM) application", Release 7.
- [21]. Recommendation and Requirements for Network based on WiMAX Forum Certificate Products, SPWG Release 1.5
- [22]. 3GPP TS 29.212, "Policy and Charging Control over Gx reference point", Release 7
- [23]. 3GPP TS 29.214, "Policy and Charging Control over Rx reference point", Release 7.
- [24]. WiMAX Forum T33-109-R015v01, "Architecture, detailed Protocols and Procedures, Policy and Charging Control", Release 1.5
- [25]. 3GPP TS 23.203, "Policy and Charging Control Architecture", Release 7.
- [26]. 3GPP TS 23.003, "Numbering, addressing and identification", Release 7.
- [27]. 3GPP TS 23.207, "End-to-end Quality of Service (QoS) concept and architecture.", Release 7.

- 1 [28]. TBD.
- 2 [29]. WiMAX Forum T33-102-R015v01, "Architecture, detailed Protocols and Procedures, Emergency Services
- 3 Support", Release 1.5
- 4 [30]. 3GPP2 X.S0013-012 "All-IP Core Network Multimedia Domain: IP Multimedia All-IP Core Network
- 5 Multimedia Domain: IP Multimedia "
- 6 [31]. 3GPP2 X.S0013-007-0, "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem – Charging
- 7 Architecture"
- 8 [32]. 3GPP TS 32.200, ""Charging management; Charging Principles"
- 9 [33]. TBD
- 10 [34]. 3GPP2 X.S0013-002-0, "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem Stage 2."
- 11 [35]. 3GPP TS 33.107, "3G security; Lawful interception architecture and functions"
- 12 [36]. IETF RFC 3024, "Reverse Tunneling for Mobile IP"
- 13 [37]. IETF draft-chakrabarti-mip4-mcbc-xx "IPv4 Mobility extension For Multicast and Broadcast Pockets"
- 14 [38]. IETF RFC 2131, "Dynamic Host Configuration Protocol"
- 15 [39]. IETF RFC 3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"
- 16 [40]. IETF RFC 3361, "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation
- 17 Protocol (SIP) Servers"
- 18 [41]. IETF RFC 3646, "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6
- 19 (DHCPv6)"
- 20 [42]. WiMAX Forum T33-110-R015v01, "Protocols and Procedures for Location Based Services", Release 1.5
- 21 [43]. 3GPP TS 22.101, "Service aspects; Service principles"
- 22 [44]. 3GPP2 X.S0013-004-B, "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol
- 23 Based on SIP and SDP Stage 3",
- 24 [45]. 3GPP TS 23.981, "Interworking aspects and migration scenarios for IPv4-based IP Multimedia Subsystem
- 25 (IMS) implementations", Release 7
- 26 [46]. 3GPP TS 29.162, "Interworking between the IM CN subsystem and IP networks", Release 7
- 27 [47]. 3GPP TS 23.167, "IP Multimedia Subsystem (IMS) emergency sessions ", Release 7
- 28 [48]. ATIS-0700005-2007 ""Alliance for Telecommunications Industry Solutions Technical Requirements for
- 29 Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia
- 30 Services.", 2007
- 31 [49]. 3GPP TS 33.108 "3G security; Handover interface for Lawful Interception (LI)" Rel 7
- 32 [50]. 3GPP2 X.S0013-014 "All-IP Core Network Multimedia Domain - Service Based Bearer Control - Ty
- 33 Interface Stage 3"
- 34 [51]. ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced
- 35 Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".
- 36 [52]. 3GPP TS 32.225 "Telecommunication management; Charging management; Charging data description for
- 37 the IP Multimedia Subsystem (IMS)", Release 7
- 38 [53]. 3GPP2 X.S0013-008-0, "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem –
- 39 Accounting Information."
- 40 [54]. ETSI TS 182 006 V1.1.1 (2006-03) "Telecommunications and Internet Converged Services and Protocols
- 41 for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description."

- 1 [55]. WiMAX Forum T33-104-R015v04, "Architecture, detailed Protocols and Procedures, WiMAX Over-The-
2 Air Provisioning & Activation Protocol based on OMA DM Specifications", Release 1.5
- 3 [56]. 3GPP TS 24.167 "3GPP IMS Management Object (MO); Stage 3"
- 4 [57]. 3GPP TS 29.213 "Policy and charging control signaling flows and Quality of Service (QoS) parameter
5 mapping" Release 7
- 6 [58]. LEAS for WiMAX Access, Part 1 North American region, August 2008
- 7 [59]. WiMAX Lawful Intercept, Part 0: Overview, August 2008
- 8 [60]. Uniform Resource Name (URN) for Emergency and other Well-Known Services (RFC 5031)
- 9 [61]. IETF RFC 5139 "Revised Civic Location Format for Presence Information Data Format Location Object
10 (PIDF-LO)"

11
12
13
14
15
16

4. Requirements and Principles

4.1 System Requirements

This section enumerates the applicable system requirements listed in [21], which this document complies with.

R-[280] The WiMAX network SHALL interwork with 3GPP/3GPP2/TISPAN IMS core network with full support for dynamic policy and charging control features including end-to-end QoS negotiation, authorizing QoS resources requested by the terminal and/or the IMS application, resource reservation and admission control, using:

- *3GPP Release 7 Policy and Charging Control (PCC) specified in [25] when interworking with a 3GPP-compliant IMS network*
- *3GPP2 Service Based Bearer Control (SBBC) specified in [30] and [50] when interworking with a 3GPP2-complaint IMS network*
- *ETSI TISPAN Resource Admission Control Subsystem (RACS) specified in [51] when interworking with an ETSI TISPAN-complaint IMS network.*

Based on this specification, the WiMAX network can interface with 3GPP and 3GPP2 core network services with full support for dynamic policy and charging features using 3GPP Release 7 PCC and 3GPP2 SBBC.

R-[283] The WiMAX network SHALL enable wireless users to access all IP Multimedia Subsystem (IMS) applications such as voice, video, messaging, data, and web-based applications.

The procedures defined in this specification enable wireless users to access all IMS applications via WiMAX network.

R-[284] The WiMAX network SHALL contain a policy charging and control enforcement function, similar to a PCEF as defined in [25] and [30], that can enforce policies and apply rules and restrictions on IMS bound bearer and control plane traffic over the WiMAX network.

Using WiMAX PCC specification [24] and the procedures defined in this specification, the WiMAX network can contain a policy enforcement function, that can enforce policies and apply rules and restrictions on IMS bound bearer and control plane traffic over the WiMAX network.

R-[287] The WiMAX network SHALL support offline and online IMS charging as defined in:

- *3GPP TS 32.200 [32] and 3GPP TS 32.225 [52] when it interworks with a 3GPP IMS network,*
- *3GPP2 X.S0013-007-0 [31]. when it interworks with a 3GPP2 IMS network.*

This SHOULD include charging correlation between IMS sessions and IP Connectivity Access Network bearer.

Using WiMAX PCC specification [24] and the procedures defined in this specification, the WiMAX network can support offline and online IMS charging as defined in 3GPP references [32] and [52] when interworking with 3GPP IMS network and as well as 3GPP2 references [31] and [53] when interworking with 3GPP2 IMS network. This includes charging correlation between IMS sessions and IP connectivity access network bearer.

R-[288] The WiMAX network SHALL support the use of private and public user identities as defined in

- *3GPP TS 23.228 [8] and 3GPP TS 23.003 [26] for registration with 3GPP IMS network.*
- *3GPP2 X.S0013-002-0 [34] for registration with 3GPP2 IMS network*
- *ETSI TS 182 006 [54] for registration with TISPAN IMS network.*

Based on this specification the WiMAX network supports the use of private and public user identities as defined in [8] and [26] for registration with 3GPP IMS networks and [34] for registration with 3GPP2 IMS network.

R-[289] WiMAX subscribers SHALL be able to establish a WiMAX bearer session to perform the P-CSCF discovery and IMS registration using procedures compatible with [2], [34], and [44].

This specification enables a WiMAX subscriber to establish a WiMAX bearer session to perform the P-CSCF discovery and IMS registration procedures compatible with the references [2] and [34] and [44].

4.2 MS Requirements

This section enumerates the applicable MS requirements listed in [21],

R-[282] WiMAX SS/MS SHALL run IMS client software to be compatible with an IMS network or networks.

R-[471] The IMS security methods and procedures SHALL include ISIM based authentication in addition to the WiMAX network authentication.

4.2.1 IMS Client - Concepts and Principle

Per requirement R- 282, this document assumes that the MS shall support an IMS client in order to access IMS applications. This document further assumes that the following principles shall apply to the IMS client residing in the MS.

1. It is expected that the IMS client will support the IMS access procedures including secure access to the IMS CN in compliance with [3] and section 9 of this documents
2. It is expected that the IMS client will conform to all the MS procedures, IMS call control and SIP extensions and applications specified in [8] and [2].
3. It is expected that the configuration of the IMS client may be done either manually, through ISIM, or through a device management system such as OMA DM or xDSL Forum TR-069. See references [55], 3GPP TS 24.167 [56] or xDSL Forum TR-069.

Support of UICC and its associates services and capabilities is optional. However if supported, this document assumes that the following requirements from SPWG document [21] SHALL define the expected behavior:

1. Per SPWG requirement R-497: The WiMAX MS/SS SHALL be able to support the WiMAX-SIM application on UICC. Exceptionally, where the WiMAX MS/SS does not support a UICC, the WiMAX-SIM equivalent functionality entity MAY reside on the MS/SS.
2. SPWG requirement R-503: The UICC hosting the WiMAX-SIM MAY support other UICC-based applications, e.g., Universal Subscriber Identity Module (USIM) [19], IMS Subscriber Identity Module (ISIM) [20].

5. Network Reference Model

The WiMAX IMS framework is built upon the overall WiMAX network architecture of Release 1.5 [7] including the IMS infrastructure for providing, among other things, commercial VoIP services. The interfaces to existing IMS infrastructure are identified, but the specification of these interfaces is beyond the scope of this document.

Figures 5-1, 5-2, 5-3 and 5-4 represent the WiMAX reference architecture for IMS interworking. The detail description of these nodes and the IMS interfaces are described in 3GPP TS 23.228

The following assumptions are made in the WiMAX IMS architecture:

1. The NRM model supports roaming and non roaming cases
2. The NRM model supports Mobile IP network (Figures 5-1, 5-3 and 5-4) and simple IP network (Figures 5-2)
3. Other than the ASN, which is part of the NAP, all the other network elements belong to the home or visited CSN. Note: the IMS provider could be different from the ASN and CSN provider(s).
4. The roaming case is extended to include the location of the P-CSCF (AF) in either the home or visited networks. The interaction of the AF with the PCRF is related to the QoS framework and described in the WiMAX PCC [24] document.
5. In the case of emergency call in a roaming environment, a P-CSCF in the visited network is required
6. The P-CSCF and the entity allocating addresses to the MS (i.e. DHCP server, HA)) are co-located in the same network (home or visited NSP). This is to avoid an undesirable trombone effect in routing the signaling traffic in a Mobile IP network first to the hCSN where the allocating entity is located, and then back to the vCSN where the P-CSCF is located.
7. The IMS Gm interface between MS and P-CSCF is not shown explicitly but is carried over R1, R3 and additional IMS Signaling interfaces in the figures within the following subclauses.
8. Non-emergency IMS services are always provided in the home NSP even in the case of local breakout for Emergency IMS services.

5.1 Non-roaming Architectures

Figures 5-1 and 5-2 represent the non-roaming reference architecture for WiMAX interworking with the IMS, for mobile and simple IP networks, respectively.

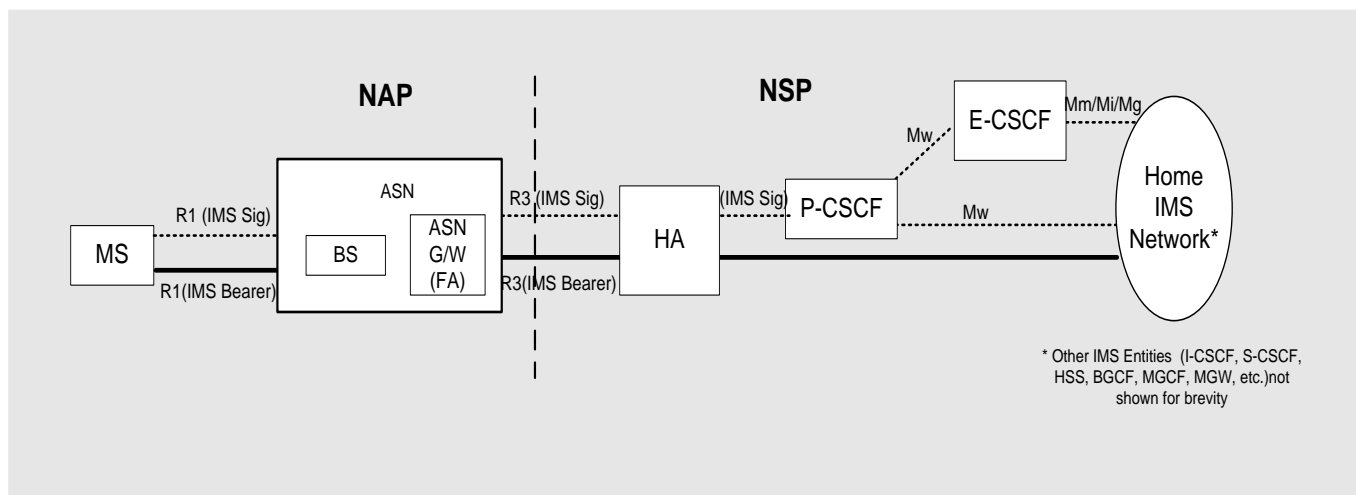


Figure 5-1: Non-roaming Reference Architecture of the IP Multimedia Core Network Subsystem including the WiMAX Network Elements supporting Mobility. (Mb stands for bearer connection only)

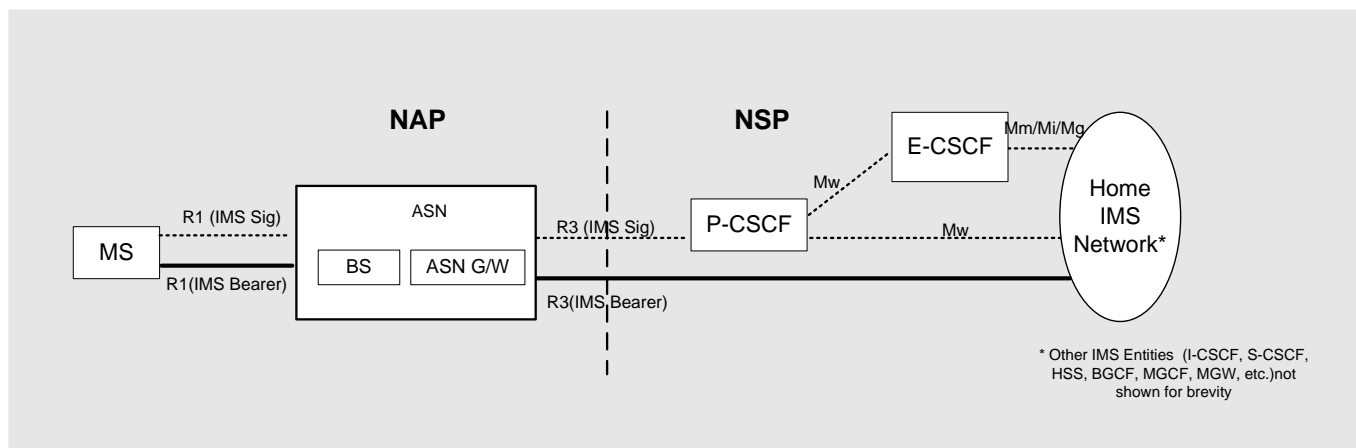


Figure 5-2: Non-roaming Reference Architecture of the IP Multimedia Core Network Subsystem including the WiMAX Network Elements supporting Simple IP. (Mb stands for bearer connection only)

5.2 Roaming Architectures

Figures 5-3 and 5-4 represent the roaming reference architecture for WiMAX interworking with the home based IMS, services, for mobility anchored in the home and visited networks, respectively.

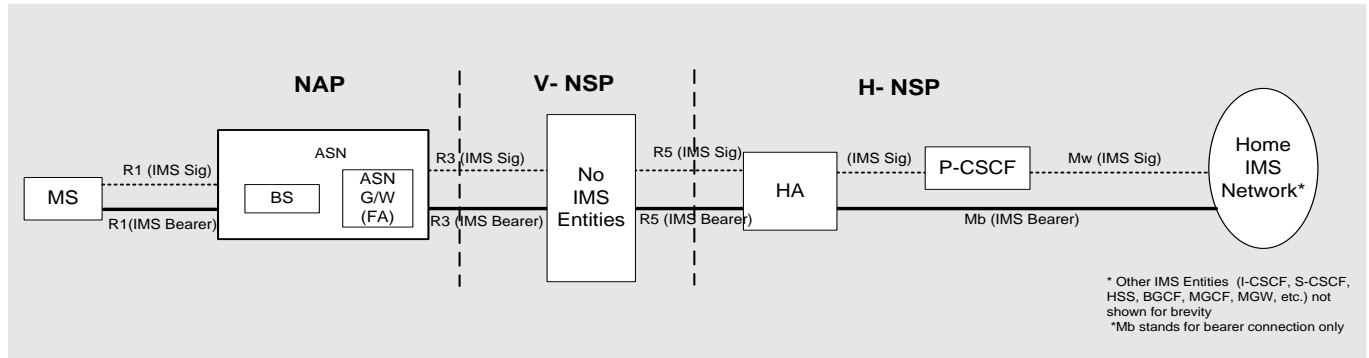


Figure 5-3: Roaming Reference Architecture of the IP Multimedia Core Network Subsystem anchored in the home network supporting Mobile IP (Mb stands for bearer connection only).

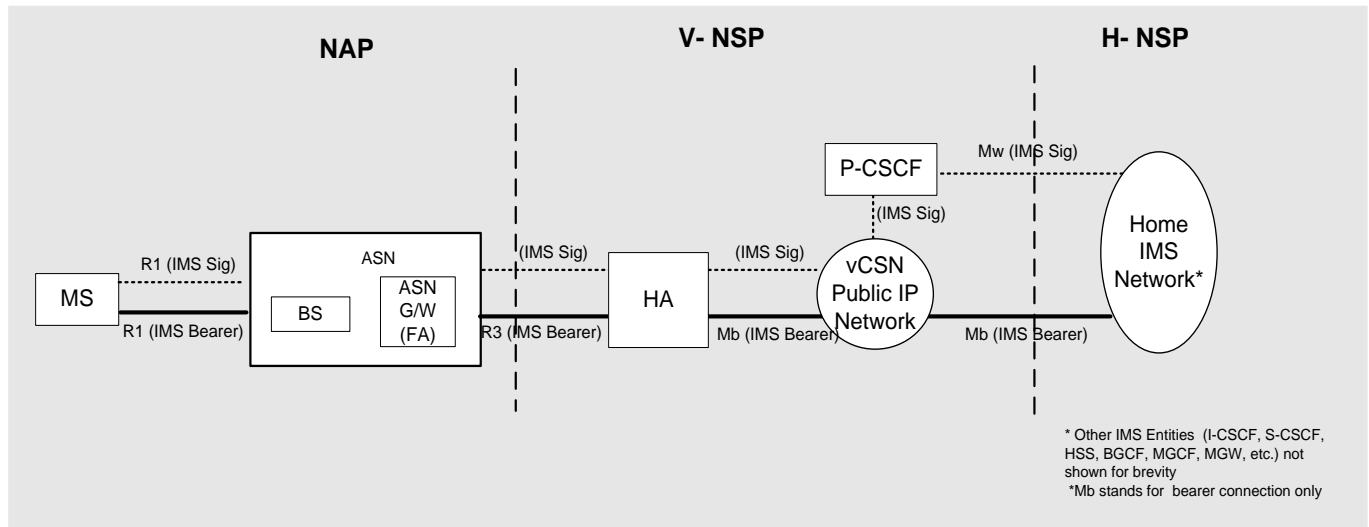


Figure 5-4: Roaming Reference Architecture of the IP Multimedia Core Network Subsystem anchored in the visited network supporting Mobile IP (Mb stands for bearer connection only).

5.3 Impacts to 3GPP and 3GPP2 IMS architecture

No changes to 3GPP and 3GPP2 IMS architecture are identified.

6. IMS Private Headers

IMS utilizes a set of private SIP headers [6] to extend the SIP protocol [17] for the IMS operations. Majority of these IMS specific headers are access network independent. This specification identifies WiMAX specific values for headers that are not access network independent.

- The WiMAX terminal providing IMS services SHALL set the values of the following headers based on [6]:P-Associated-URI
- P-Called-Party-ID
- P-Visited-Network-ID
- P-Charging-Function-Addresses
- P-Charging-Vector [Editor's Note: WiMAX specific values for this header are FFS].
- P-Preferred-ID

WiMAX access networks providing IMS services SHALL follow Section 8.2 for the values of the following headers:

- P-Access-Network-Info
- P-Charging-Vector

7. Procedures, Messages, and TLVs

7.1 IP Address Management and IP Version Interworking

This specification introduces no new requirements to the 3GPP and 3GPP2 IMS Release 7 specifications.

7.1.1 IP Address Management

IP address management, which refers to management of the Point of Attachment (PoA) address delivered to the MS, is described for IPv4 and IPv6 protocols in [16] and [7]. MS address management and interworking is also described in [44], [2], [8], and [9]. The IMS supports private addressing as discussed in [8].

7.1.2 IP Version Interworking

Since the MS can be assigned IP4 and/or IPv6 addresses and can access both IPv4 and IPv6 based services, situations may arise where interworking is needed to interoperate with IPv4 and IPv6 networks. The IP version interworking is defined in [2], [8], [9], [45], and [46].

It should be possible for users connected to an IMS network to communicate with users connected to SIP based networks that use a different IP version via interworking mechanism. It is described in [8] how such interworking is performed for IMS.

7.2 P-CSCF Discovery

The following describes the procedures on how the MS discovers the address(es) of P-CSCF in order to initiate the IMS session. P-CSCF discovery can be activated anytime after the MS has been successfully authenticated to access the ASN. In addition, in the case where CMIP or PMIP is enabled for the MS, the P-CSCF discovery can be initiated anytime after the successful MIP registration.

- For CMIP scenario, the MS and CMIP client SHALL send a DHCP Inform message with a SIP Server Option to retrieve P-CSCF address(es) or a list of fully qualified domain names (FQDN) of P-CSCF(s) after the CMIP registration. Such DHCP message may be broadcast. In order to ensure a proper network handling of the broadcast DHCP message, DHCP messages SHOULD not be encapsulated. DHCP messages SHOULD not be encapsulated even if the MS had negotiated with network, during the CMIP registration stage, to enable packet encapsulation of all the packets as described in RFC 3024 [36] or just the broadcast and multicast packets as described in draft-chakrabarti-mip4-mcbc-xx.txt [37]. If the broadcast DHCP message is nevertheless encapsulated by the MS, the ASN may handle the encapsulated DHCP packet either per the description in RFC 3024 or per the description in draft-chakrabarti-mip4-mcbc-xx.txt. When the HA receives such broadcast DHCP message from the FA, the handling of such message depends on the HA DHCP processing capability, which is outside the scope of this specification.
- For non-CMIP scenarios, client MAY add SIP Server option to DHCPREQUEST message sent during IP address configuration or it MAY send DHCP Inform with SIP Server Option in order to retrieve P-CSCF address(es) or a list of fully qualified domain names (FQDN) of P-CSCF(s).

[Editorial Note: This or parts of this section may be moved later on into NWG Rel 1.5 Stage 2 and Stage 3 amendments as part of the DHCP procedures]

7.2.1 DHCP Proxy in ASN

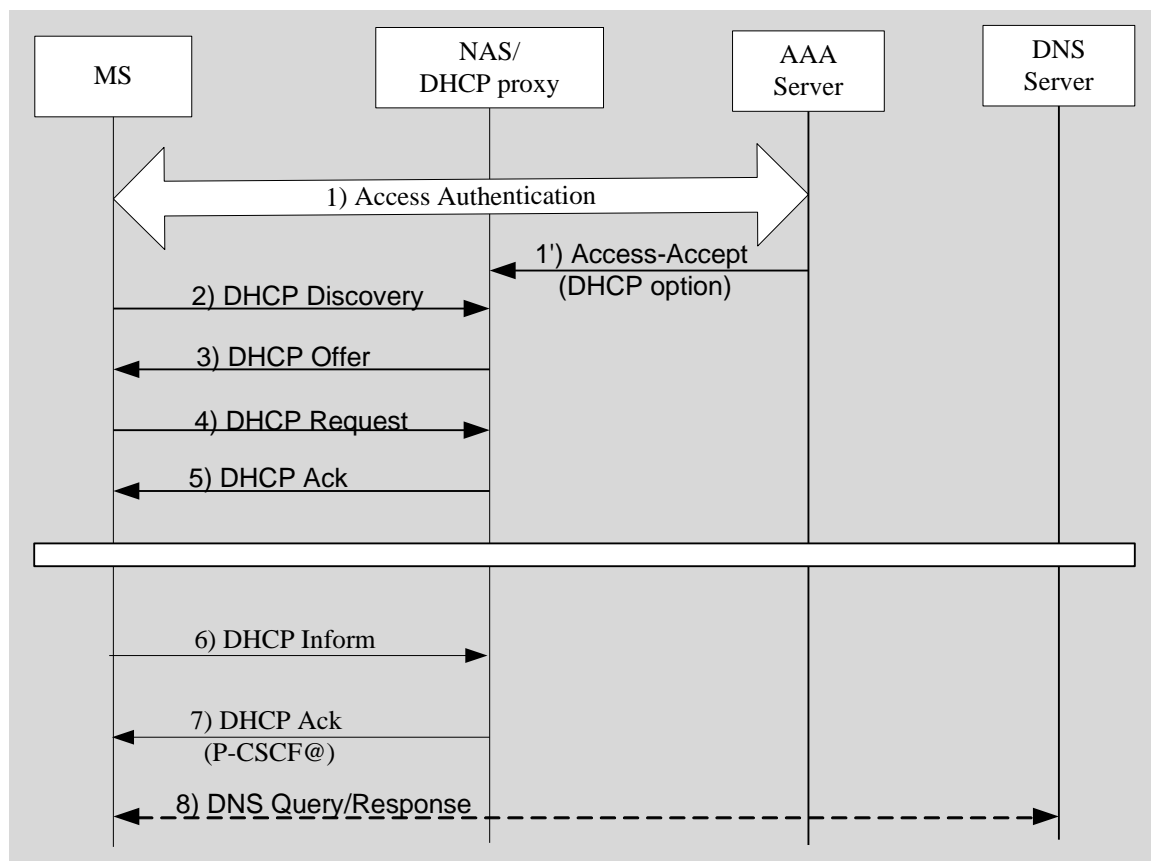


Figure 7-1: P-CSCF Discovery via DHCP Proxy Procedure

- 1) Step 1-1': Step 1' is part of the access authentication where the NAS may receive the P-CSCF address(es) or a list of fully qualified domain names (FQDN) of P-CSCF(s) from the AAA as shown in TABLE 8-3 at the time of successful Device/User Access Authentication.. Subsequently, the following steps happen.
- 2) Step 2-5: The MS retrieves IP address and optional P-CSCF address(es) or a list of fully qualified domain names of P-CSCF(s) in DHCP option via DHCP procedure as defined in RFC 2131 [38] for IPv4 or RFC 3315 [39] for IPv6., or based on DHCP options for SIP server (RFC3319) and Domain Name as defined in RFC 3361 [40] for IPv4 and in RFC 3646 [41] for IPv6. MS may optionally indicate ASN that it wants P-CSCF address or FQDNs of P-CSCF in the DHCP Discovery message. According to the indication, DHCP Proxy may optionally include the address(es) of the P-CSCF or a list of FQDNs of P-CSCF(s) in the DHCP ACK. If the address(es) of P-CSCF is included, the MS can refer to such address(es) to support for the future IMS session establishment.
- 3) Step 6: MS sends a DHCP Inform message to the NAS in order to acquire P-CSCF address(es) or a list of FQDN of P-CSCF, and all the other DHCP options.
- 4) Step 7: The DHCP Proxy acknowledges the P-CSCF address(es) or a list of FQDN of P-CSCF, and other configuration parameters by sending the DHCP Ack message as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6., or based on DHCP options for SIP server (RFC3319) and Domain Name as defined in RFC 3361 for IPv4 and in RFC 3646 for IPv6.
- 5) Step 8: If P-CSCF address(es) are not received but domain information in the DHCP Inform/Ack (for the FQDN domain returned in DHCP Ack) is received, the MS performs a DNS query to retrieve a list of P-CSCF(s) IP addresses.

NOTE: In CMIP scenario, DHCP message may be broadcast. However, such DHCP message SHOULD not be encapsulated even if the MS had negotiated with the network, during the CMIP registration stage, to enable packet

encapsulation of all the packets as described in RFC 3024 or just the broadcast and multicast packets as described in draft-chakrabarti-mip4-mcbc-xx.txt. Hence the network can process the DHCP messages via the support of the DHCP Proxy as described above.

7.2.2 DHCP Relay in ASN

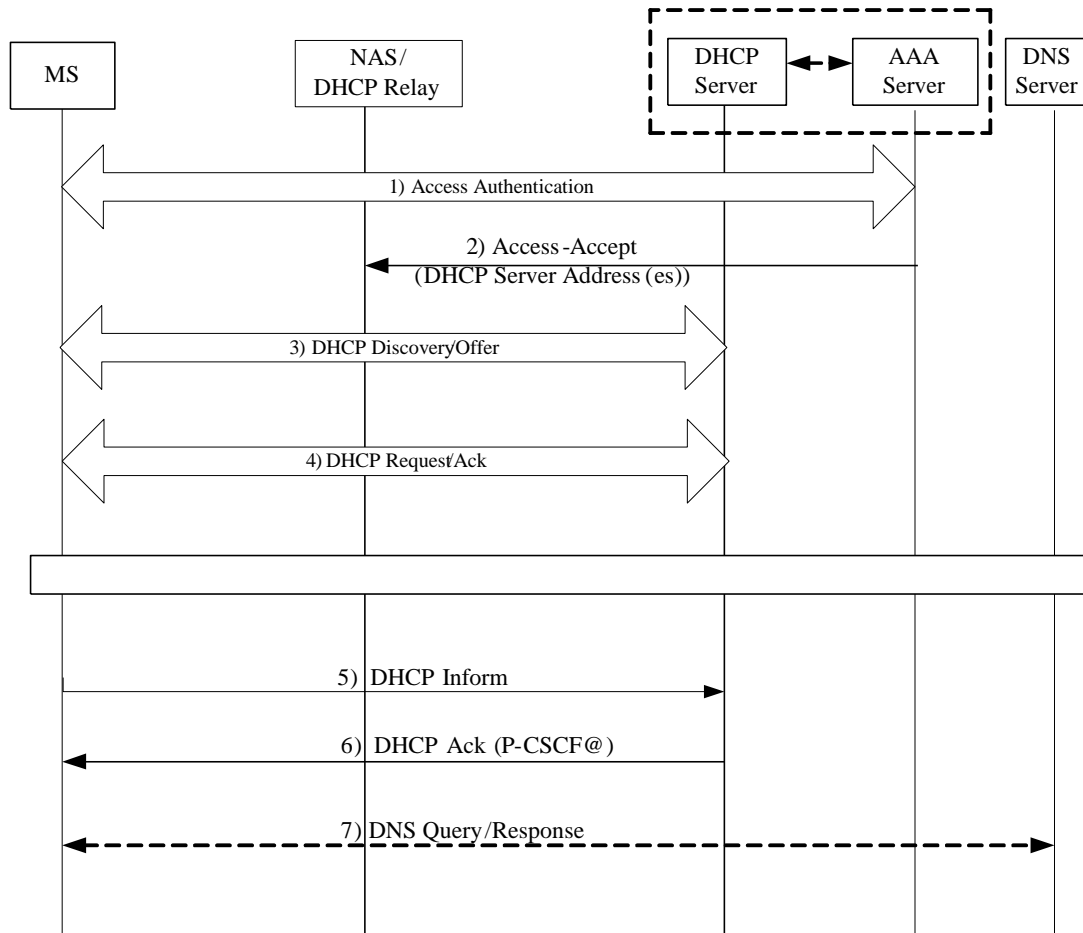


Figure 7-2: P-CSCF Discovery via DHCP Relay Procedure

- 1) The MS performs Device/User Access Authentication.
- 2) The AAA server MAY download the DHCP Server address(es) to the NAS in the Access-Accept. Subsequently, the following steps happen.
- 3) The MS sends a DHCP Discover to discover the IP address(es) of DHCP server. DHCP servers receiving the DHCP Discover request reply by sending a DHCP Offer message including an offered IP address.
- 4) The MS initiates DHCP procedure to DHCP server to retrieve IP address and optional P-CSCF address(es) or a list of FQDN of P-CSCF and other configuration information. MS may optionally indicate ASN that it wants P-CSCF address(es) or a list of FQDN of P-CSCF in the DHCP Discovery message. According to the indication, DHCP Server may optionally include the address(es) of the P-CSCF or a list of FQDN of P-CSCF in the DHCP Ack. If the address(es) of P-CSCF is included, the MS can refer to such address(es) to support for the future IMS session establishment and Step 5-6 will not then be performed. If FQDN of P-CSCF is included, the MS performs a DNS query to resolve a FQDN to an IP address and refers to such address for IMS session establishment.

1 5) MS sends a DHCP Inform message to DHCP server in order to acquire P-CSCF address(es) or a list of
2 FQDN of P-CSCF in the DHCP option.

3 6) The DHCP Server acknowledges the use of the P-CSCF address(es) or a list of FQDN of P-CSCF and other
4 configuration parameters as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6., or based on DHCP
5 options for SIP server (RFC3319) and Domain Name as defined in RFC 3361 for IPv4 and in RFC 3646 for
6 IPv6.

7 7) If P-CSCF address(es) are not received but domain information in the DHCP Inform/Ack, the MS performs
8 a DNS query (for the FQDN returned in DHCP Ack) to retrieve a list of P-CSCF(s) addresses .

9 NOTE: In CMIP scenario, DHCP message may be broadcast. However, such DHCP message SHOULD
10 not be encapsulated even if the MS had negotiated with network, during the CMIP registration stage, to
11 enable packet encapsulation of all the packets as described in RFC 3024 or just the broadcast and multicast
12 packets as described in draft-chakrabarti-mip4-mcbc-xx.txt. Hence, the network can process DHCP
13 messages via the support of the DHCP Relay as described above.

15 **7.2.3 P-CSCF Discovery for a Roaming User**

16 In roaming case, the P-CSCF can be assigned by either the home NSP or the visited NSP. For P-CSCFs in the
17 visited CSN the visited AAA MAY append the vP-CSCF address(es) or FQDNs in the AAA messages from the
18 ASN and the home AAA server. Based on the following criteria are used by H-AAA to assign the P-CSCF:

- 19 1. Roaming agreement with the visited operator.
- 20 2. Presence of vP-CSCFs' information,
- 21 3. End-user's subscription profile.

22 The H-AAA SHALL then assign the P-CSCF as well as the HA by appending the appropriate P-CSCF address or a
23 list of FQDN in the H-AAA reply to the ASN. The H-AAA SHOULD assign P-CSCF and other entities (i.e. DHCP
24 server, DNS server, HA) to be collocated within the same network (home NSP or visited NSP) to the MS.

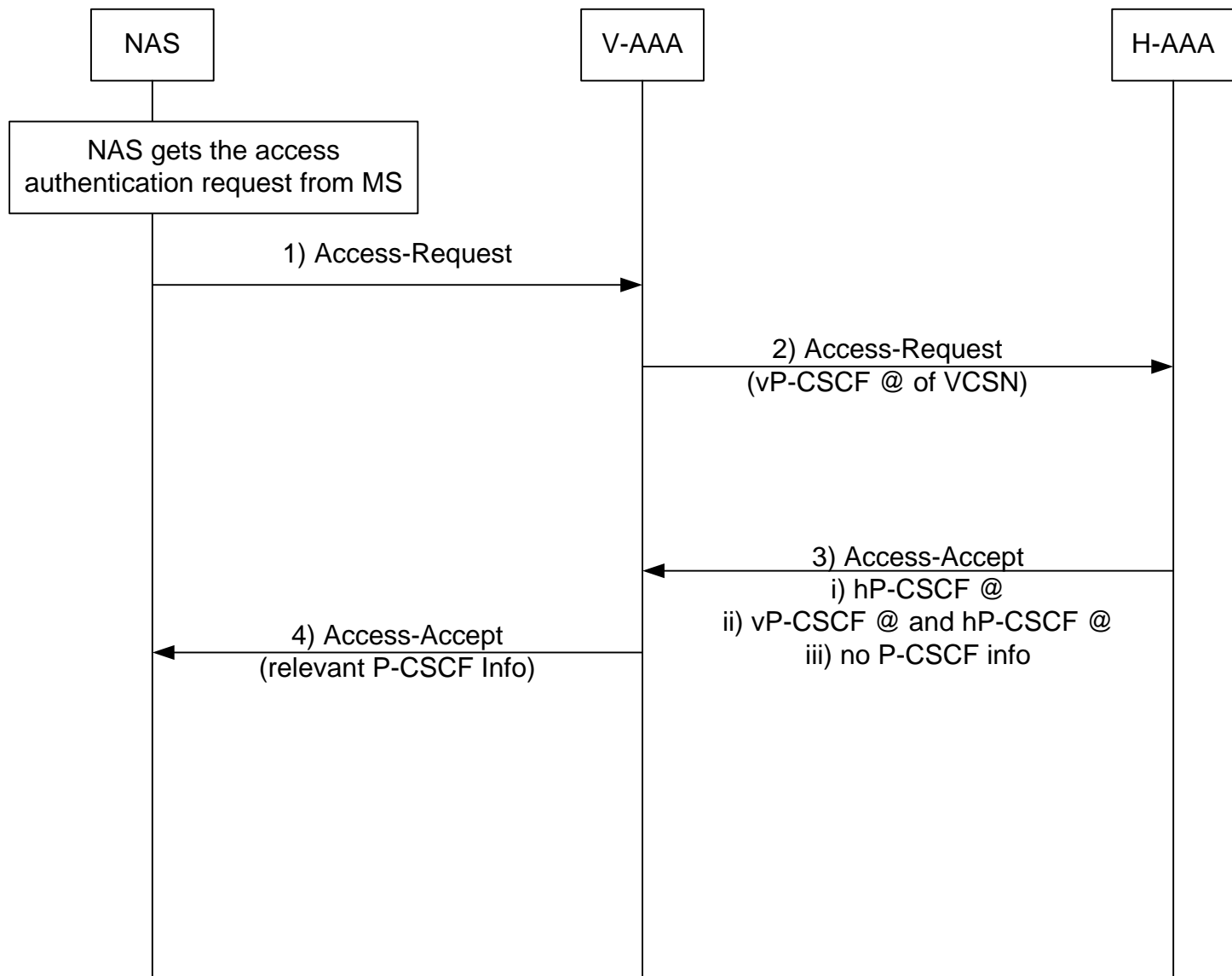


Figure 7-3: P-CSCF Discovery in Roaming

- 1) Step1: When the NAS in the visited ASN gets the access authentication request from the MS, the NAS sends the Access-Request message to V-AAA proxy in the Visited CSN.
- 2) Step 2: The V-AAA proxy forwards the Access-Request message to the H-AAA server. If P-CSCFs can be provided by the Visited CSN, the V-AAA proxy appends the visited P-CSCF address(es) or FQDNs belonging to the Visited CSN in this message to the H-AAA server.
- 3) Step 3: If P-CSCFs can be provided by the Home CSN, the H-AAA decides whether to assign the P-CSCF from the Home CSN or Visited CSN (if available) and appends either the visited and/or home P-CSCF addresses or FQDN in the Access-Accept message. If no P-CSCFs is available, no P-CSCF value is returned.
- 4) Step 4: The V-AAA proxy forwards the Access-Accept message including the P-CSCF information to the NAS in the visited ASN. If the returned TLV only includes the hP-CSCF address(es) or a list of home

1 FQDN, the NAS SHALL only assign home P-CSCF to the MS. If no P-CSCF TLV is returned in the
2 Access-Accept message, the V-AAA proxy may append the P-CSCF address(es) or FQDNs of the Visited
3 servers to the NAS. If on the other hand both vP-CSCF and hP-CSCF address(es) are included in the
4 Access-Accept message, the NAS can assign either one to the MS. The P-CSCF, HA and DHCP server
5 assigned by the NAS should be located in the same network. Only one set of either hP-CSCF and h-HA or
6 vP-CSCF and v-HA is provided to the mobile.

7 **7.3 Session Control**

8 The Serving-CSCF (S-CSCF) performs the IMS session control services. Section 4.6.3 of 3GPP TS 23.228 specifies
9 the functions of S-CSCF during an IMS session. An IMS session may involve one or two S-CSCFs. The session
10 flow is decomposed into three parts:

11 - Origination part that covers all network elements between the originating MS and the S-CSCF for that MS, as
12 described in TS 24.229,

13 - Inter S-CSCF part

14 - Termination part that covers all network elements between the S-CSCF for the terminating MS and that MS.

15 Sections 5.6 and 5.7 of 3GPP TS 23.228 define the origination and termination sequences, respectively; out of which
16 mobile origination and mobile termination sequences are applicable to WiMAX. The session control procedures are
17 defined using SIP signaling between MS and P-CSCF and between P-CSCF and S-CSCF.

18 **7.4 Emergency Services**

19 This section describes how an IMS based emergency services (ES) call is delivered to the nearest emergency
20 network. It provides three cases and shows the end to end (MS to the emergency network) call flows for each. The
21 first case is an ES call originating from a non-roaming IMS user using a valid device (one that can enter the network
22 after successfully completing all the normal network entry procedures). The second case is an ES call made by a
23 subscription less user using an invalid device, i.e., a device that is not allowed to enter the WiMAX network for non-
24 emergency purposes. The third case is ES call made by a user roaming in a visited network with mobile IP (MIP)
25 sessions authorized by the home network. How the user originates an ES call on an MS is implementation dependent
26 with some methods where the MS can detect the origination as emergency and others where the MS cannot. This
27 section also explains other features related to delivering an ES call – initial network entry with an ES NAI using a
28 subscription less device, prioritizing ES calls with QoS and service flow creation, ES indicators, interfaces between
29 a “location server” (that triggers the location estimation method of the MS) and different methods to estimate the
30 location of the MS.

7.4.1 IMS ES Network Reference Model (NRM) for a non-roaming user

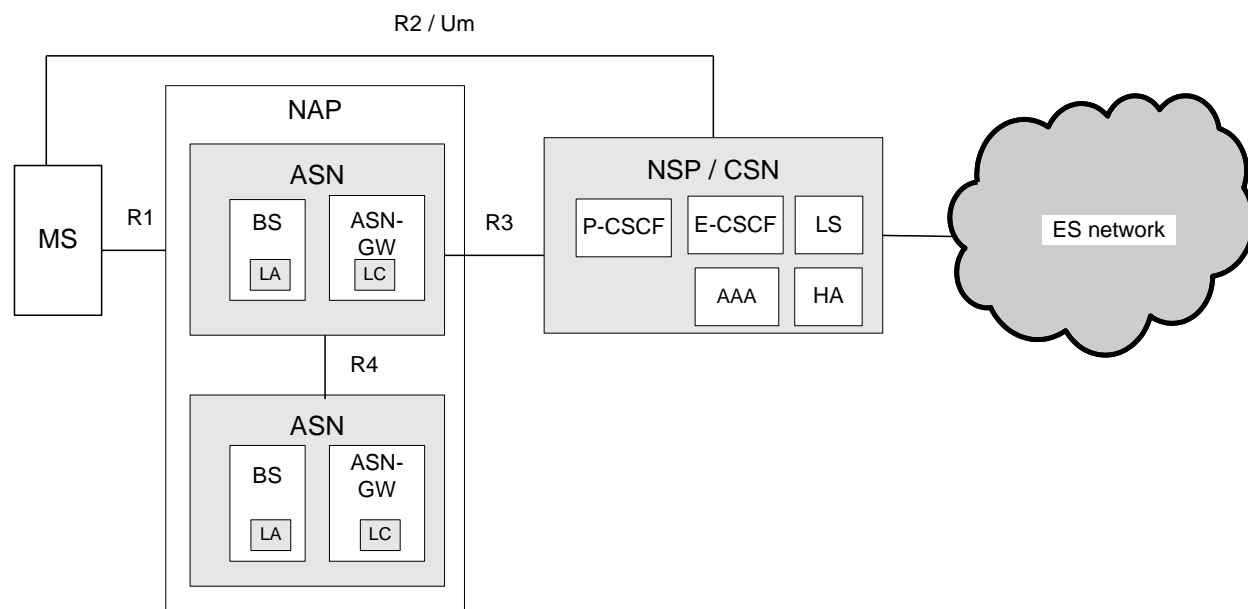


Figure 7-4: Network Reference Model to deliver an ES call through an IMS network for a non roaming user.

Figure 7-4 shows the IMS network reference model. It can deliver an ES call from a WiMAX terminal to an emergency network using the IMS core network. At a high level the figure shows the WiMAX access service network (ASN), home network and the emergency services network. The ASN network primarily consists of the base station and the ASN gateway. The NSP/CSN contains the P-CSCF, E-CSCF, AAA and Location Server (LS) - also called LRF (Location Retrieval Function) among several other network elements. The LRF and LS are described in [47] and [42] respectively.. Almost all the ES networks today are PSTN based networks.

ES call delivery involves two main steps – routing the ES call to an emergency network nearest to the MS based on the initial location estimate and finding the more accurate location of the MS. IMS core network finds the ES network nearest to the MS using a “location retrieval function” (the details are given in [47]). To find out the location of the MS, ES network queries LS, which in turn triggers a retrieval procedure as defined in LBS specification [42]. The measurement method depends on the MS and network capability. The BS and ASN GW have location functions (LC and LA) that work together with the Location Server (LS) to determine the geo-location coordinates or civic address of the distressed MS. Further details are described in Emergency Service specification [29] and LBS specification [42]. . The details of the location retrieval are given in the “WiMAX Networks Protocols and Architecture for Location Based Services” document.

7.4.2 IMS ES network reference model for a roaming user

The NRM for a roaming user is shown in Figure 7-5. Here, the P-CSCF, E-CSCF, LS, and v-AAA are assigned in the Visited-NSP for the ES call. Additionally, if Mobile IP is enabled, a home agent (HA) is also assigned in the V-NSP for emergency services. Figure 7-5 shows the NRM for a roaming user.

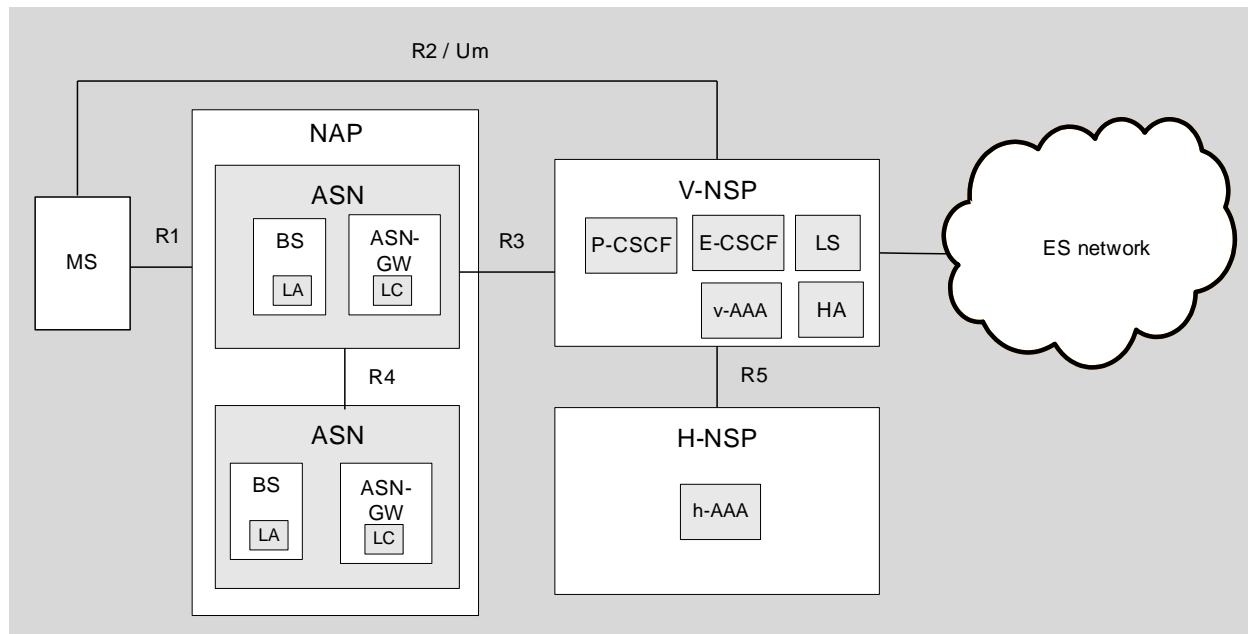


Figure 7-5: Network Reference Model to deliver an ES call through an IMS network for a roaming user.

7.4.3 ES call delivery for a non-roaming authenticated user and device

This section explains how an emergency services call originated from an MS that has successfully completed device and user authentication, is delivered to the nearest emergency network. Figure 7-6 shows the call flows and only highlight the WiMAX specific steps. For a full description of the non-WiMAX steps please refer to [47].

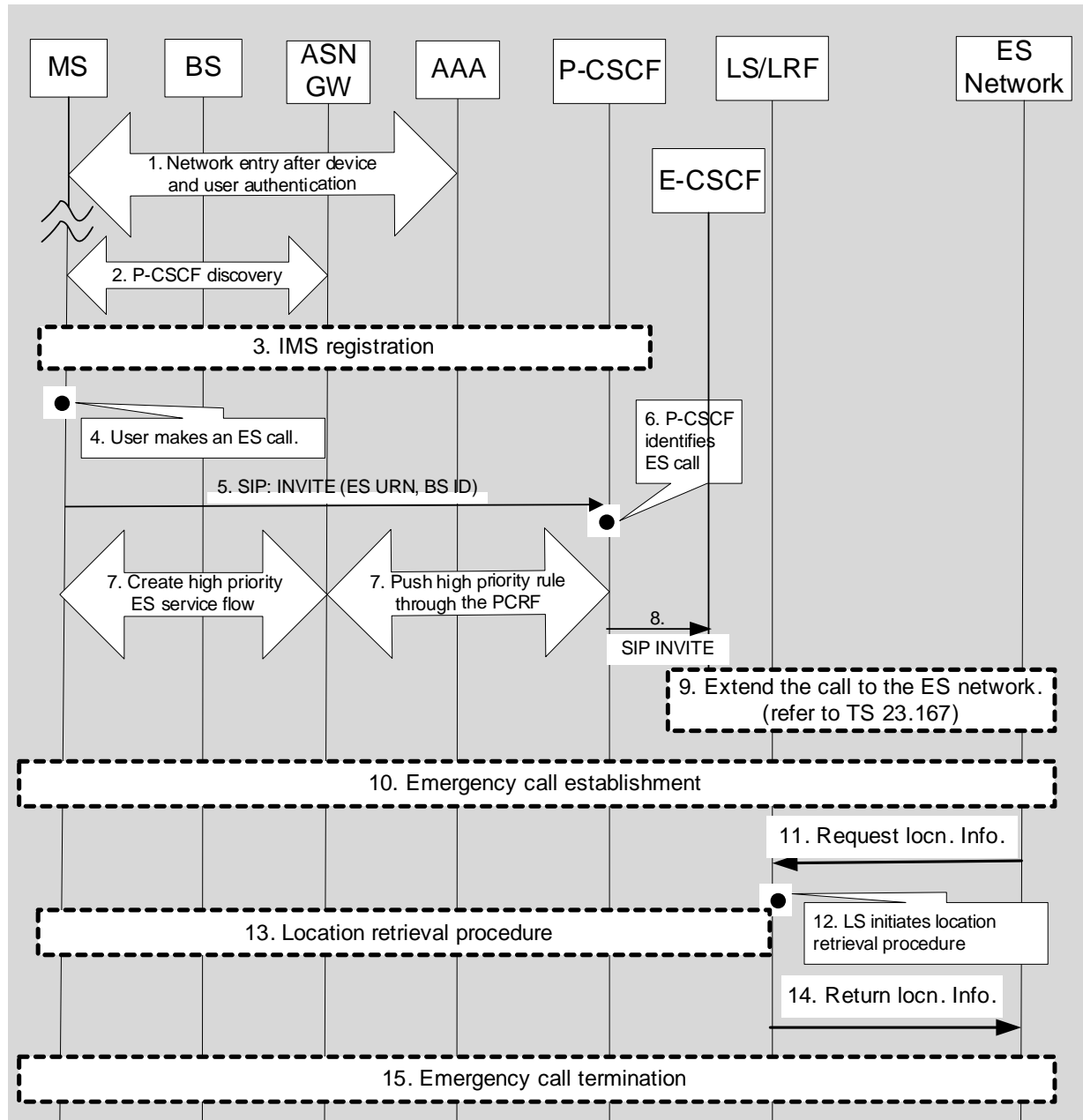


Figure 7-6: ES call delivery from a non-roaming device

1. Mobile device (MS) enters the network after device and user authentication,
2. MS obtains the P-CSCF address (see section 7.2 for details) The HA and P-CSCF are located in the same home network.
3. MS performs emergency registration if not already registered
4. User makes the ES VoIP call. As specified in 3GPP TS 24.229 [2], the MS shall translate any user indicated emergency number (per 3GPP TS 22.101[43]) to an emergency service URN (e.g., urn:services:sos) to indicate that the call is an ES call. MS shall be able to recognize Emergency Services dial strings from the home domain and include the Emergency Services URN in the SIP INVITE.

5. MS sends a SIP INVITE message to P-CSCF (through the WiMAX network). It uses an ES URN (e.g., urn:services:sos) to indicate that the call is an ES call. That is, the request URI field of the INVITE message has the ES URN to indicate that the call is an ES call. MS sets the P-Access-Network-Info field of the INVITE message to the WiMAX Base-Station ID (BSID = sector id). Optionally the MS may deliver geographic coordinates and/or civic address information in the SIP INVITE message. Location information may be obtained from a GPS or other methods specified in [42] and compatible to TS 24.229 [2]. The preferred civic address format is RFC-5139, as referenced in [42].
6. P-CSCF identifies the call as an ES call by looking at the request URI of the INVITE message.
7. P-CSCF can push for a high priority for the ES call through PCRF as described in Annex 5 of TS 29.214 [23]. ES call may be given a high priority on the WiMAX network (see Section 7.4.7 for details).
8. P-CSCF finds the routing number to complete the ES call to the appropriate ES network. P-CSCF directs the call to E-CSCF using a SIP INVITE message.
9. E-CSCF verifies the MS credentials. It may reject the call in some regions for lack of appropriate credentials or it may accept the emergency call without any verification. The E-CSCF in turn may enquire with the "Location Retrieval function" (LRF) to find a routing number to the appropriate ES network for the WiMAX device originating the ES call. If the LRF cannot determine the routing number to the appropriate PSAP within a pre-specified timeout period, a default routing number shall be generated. The LRF uses the location information (BS id, GPS coordinates coming from a GPS enabled terminal, civic address defined in [61] or information obtained from the LBS-ADV message) sent by the MS as part of the SIP INVITE message of the ES call. The call is directed to the appropriate ES network using the routing number. The details are given in [47].
10. An ES call is established between MS and the ES network nearest to the MS.
11. ES network may enquire with the location server (LS) to get the updated location of the MS once it had been authenticated. AAA authenticates LS as a valid entity that can trigger a location retrieval procedure.
12. LS triggers a location retrieval procedure to find out the geo-location coordinates of the MS, as described in [42].
13. LS works with BS and ASN GW of WiMAX network to find out the location of MS.
14. The updated location information of the MS is returned to the ES network. Steps 10 through 13 may be repeated as necessary when the ES network performs a location rebid.
15. The ES call is terminated and the allocated (over the air) resources are cleaned up.

7.4.4 ES call delivery with a subscription less device or a user

This section shows how an ES call originated from a subscription less device or subscription less user requesting unauthenticated emergency services. The ES call from the device or user, which may have had initial NSP subscription but can't presently access and authenticate to the WiMAX network, is delivered to the nearest emergency network. The unauthenticated subscription less device performs an unauthenticated emergency network entry using an ES NAI (see definition in section 7.4.8) and is allowed emergency network entry to complete the ES call. Figure 7-7 shows how an ES call initiated by a device, that does not have a valid WiMAX subscription, is delivered to the ES network. IMS subscription is not relevant since no IMS registration is expected in this scenario.

Support for this scenario depends on the WiMAX network supporting unauthenticated emergency service as described in ref [29]

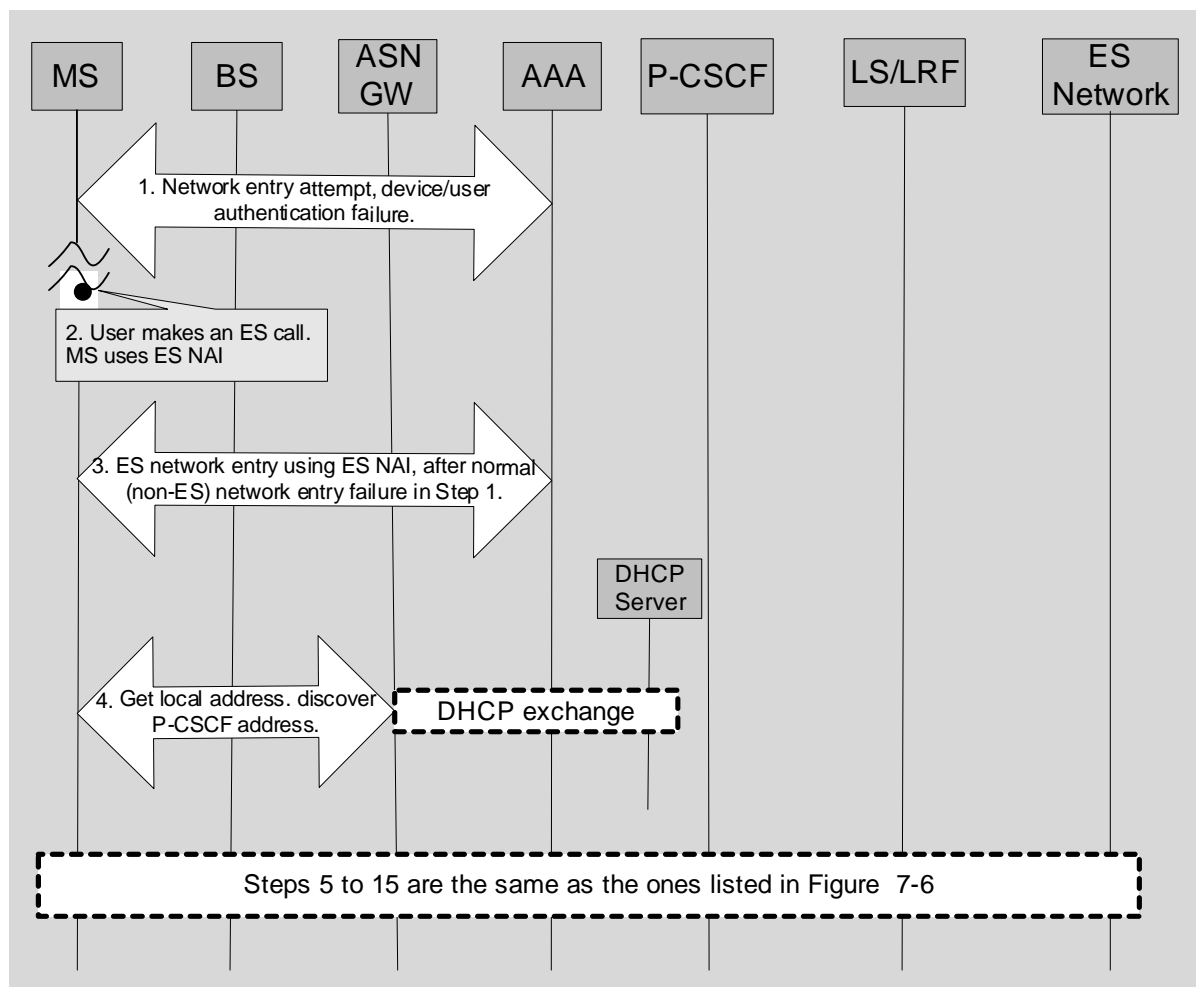


Figure 7-7: ES call delivery from a subscription less device

1. MS enters the WiMAX network. Device authentication (if mandated by the network provider) and user authentication fails. In some regions, step 1 cannot be optional and ES authentication is not allowed without a normal authentication attempt first, where the terminal uses its provisioned credentials.
2. User triggers the ES VoIP call establishment.
3. Since the normal (non-ES) network entry failed in Step 1, ES VoIP call triggers an emergency NAI using unauthenticated emergency service access as defined in [29]. The BS and ASN-GW permit access to the device for ES. ES user enters the network for the ES call, after proper key generation.
4. MS gets an IP address using DHCP and also discovers the P-CSCF address. P-CSCF discovery uses a DHCP exchange and is discussed in Section 7.2 of this document.
5. Steps 5 through 15 are the same as in the case where device and user authentication are successful. The call flow to deliver an ES call originated from a device that has a valid WiMAX subscription but an invalid IMS subscription is similar to the one shown in Figure 7-6. In this figure the initial network entry is not successful and the user needs to perform another full ES network entry (Step 3). The MS may try to perform an IMS registration but that will not succeed (since there is no valid IMS subscription). The user will next attempt to make an ES call with ES URN set in the SIP INVITE message. The device discovers the P-CSCF as shown in Step 4 of Figure 7-7. The P-CSCF identifies the ES call (as indicated in the ES

URN) and delivers the call to the ES network, as shown in Steps 5-15 of Figure 7-6 and explained in section 7.4.3.

7.4.5 ES call delivery during roaming

This section shows how an ES call originated from an MS roaming in a foreign network is delivered to the nearest emergency network. The local breakout details are FFS (see step 3 and NOTE 1).

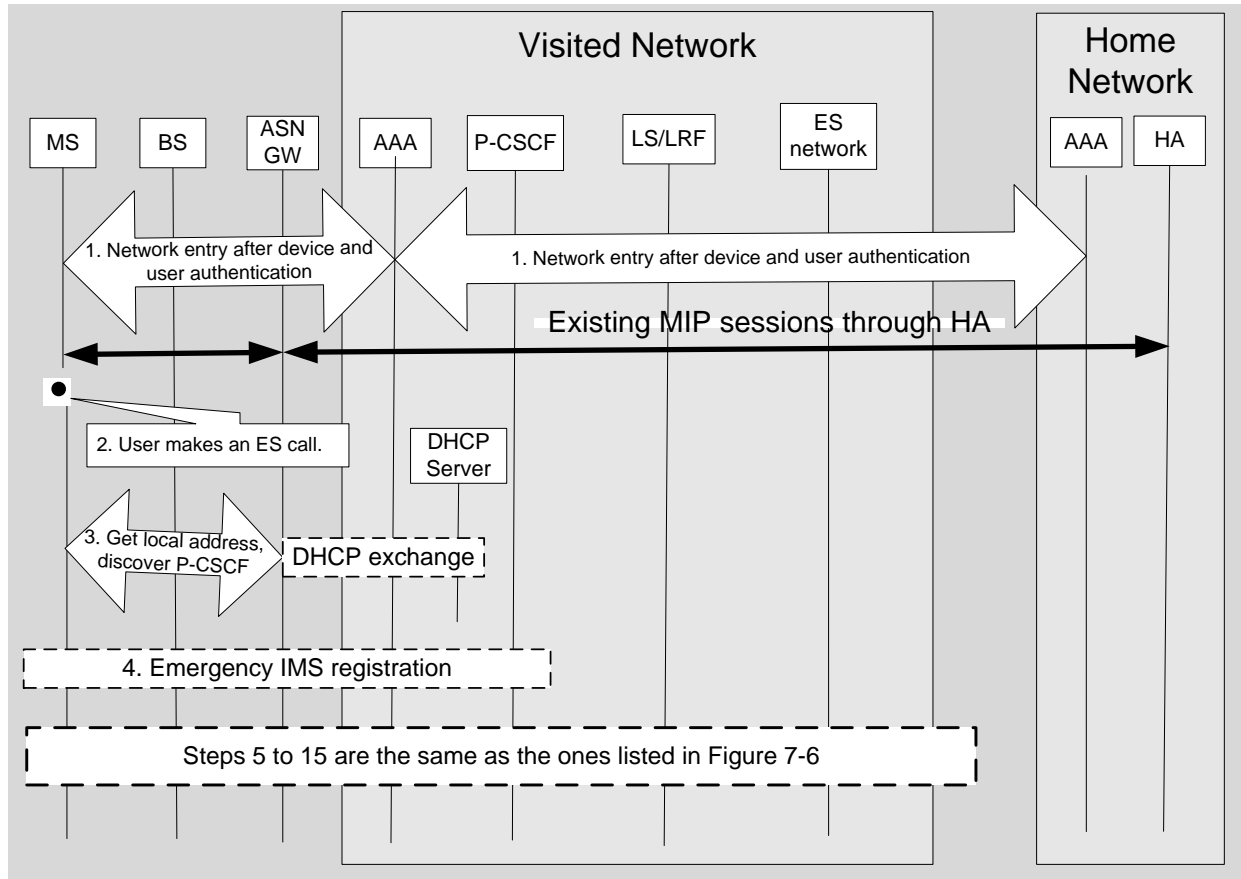


Figure 7-8: ES call from a roaming device

1. MS enters the WiMAX network. Device authentication (if mandated by the network provider) and user authentication are successful. V-AAA gets the user information from H-AAA. A MIP tunnel is established from HA to FA. User's non-emergency sessions go through HA.
2. User dials ES number. Assumptions: IMS client application running on MS can detect the ES call and the MS knows it is roaming through NSP-ID advertisement info.
3. The emergency session should be handled by the visited IMS, if available, because the visited IMS is better able to map the location of the MS to the correct PSAP, see NOTE 1. Therefore MS should obtain a local breakout and the visited network should provide a local service flow and a local IP address.
4. When roaming, MS shall always perform IMS emergency registration as specified in [47] and corresponding IMS specifications. The reason for IMS emergency registration is to overcome possible roaming restrictions for the MS and to provide a callback number of the user to the ES network. The MS, if capable, may be able to keep its existing normal IMS registration activated in parallel with the emergency registration.
5. Steps 5-15 are the same as in Figure 7-6.

NOTE 1: In case there is no IMS capability in the visited network the MS, if capable, could possibly initiate the emergency call with some other VSP, or alternatively the home IMS may be able to reroute the IMS emergency call to the visited country via PSTN. In such a solution it is technically challenging to handle the location information of the emergency call and the liability issues and technical solutions would need to be covered by roaming agreements between the operators involved, therefore the routing of Emergency Services from home to visited network is FFS.

7.4.6 Initial network entry with an ES NAI

Initial network entry is described in [7] section 4.5. The same procedure is also used by a subscription less device to enter a network to complete an ES call. The MS in [7] Figure 4-41 step 10 uses an ES NAI in the EAP Response/Identity used.

7.4.7 Prioritizing ES call

This section describes how an ES call is prioritized. The call flow in Figure 7-9 shows how an ES call originated is prioritized. However, the steps shown for prioritizing the call originated from a valid device are the same as the ones shown below. Note that the WiMAX standards do not mandate a service provider to prioritize an ES call, service providers may choose not to prioritize ES calls.

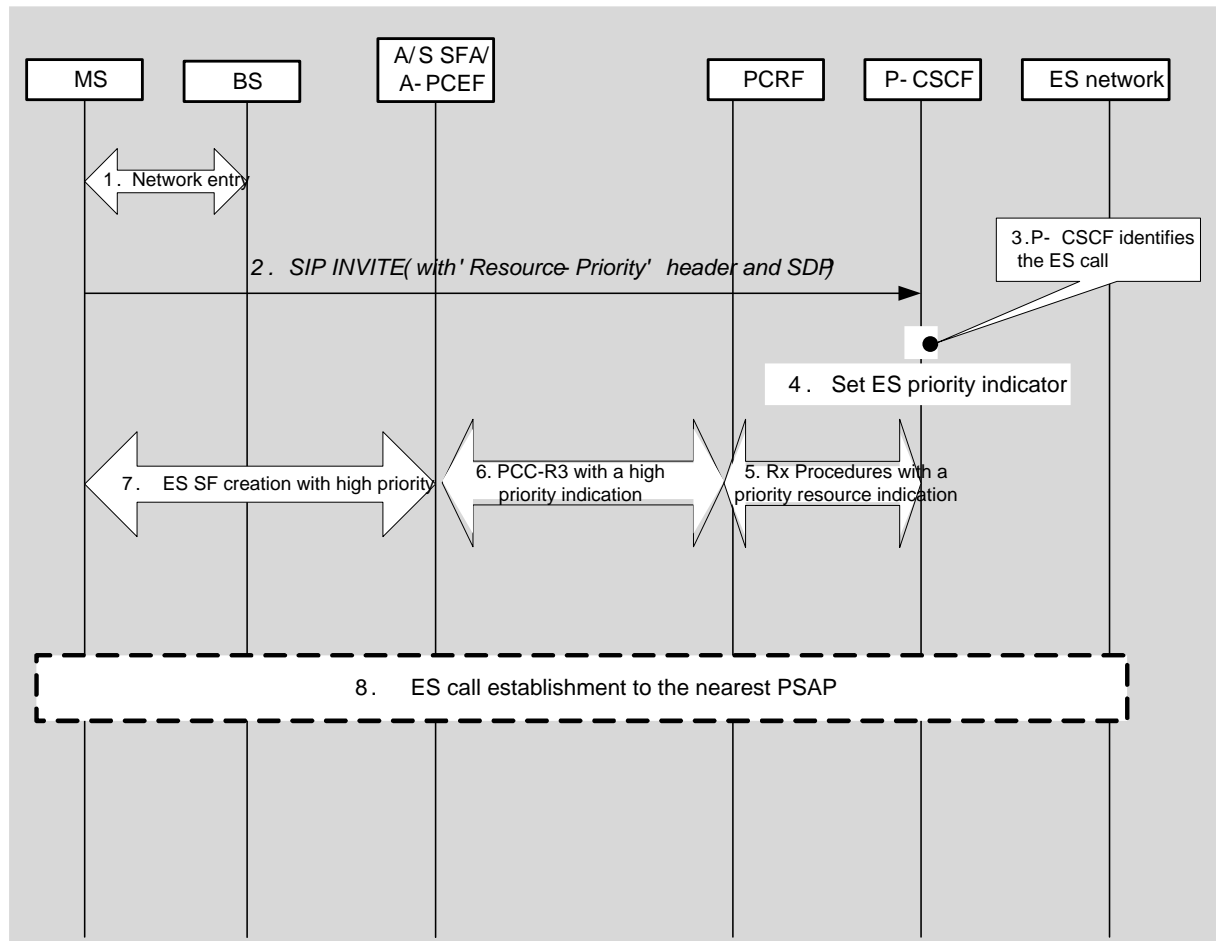


Figure 7-9: Call flow showing prioritizing ES call

1. The MS completes a network entry.
2. The MS initiates an ES call. A SIP INVITE message goes from the MS to the P-CSCF.

3. The P-CSCF identifies the ES call (requested URI has an ES URN).
4. The P-CSCF sets a high priority indicator by including a Resource-Priority header in the SIP message.
5. The P-CSCF indicates to the PCRF a high priority bearer by setting the reservation priority AVP.
6. The PCRF exchanges PCC-R3 messages, with a high priority indication, with the Anchor/Serving SFA/A-PCEF indicating high priority SF creation for ES call. The specific PCC-R3 mechanism for high priority SF is not in the scope of this document.
7. A high priority service flow is created by the S-SFA for an ES call.
8. An ES call is established.

7.4.8 ES indicators

Emergency situations are indicated in two contexts – network entry by a subscription less device using an “ES NAI” and emergency call indication in SIP INVITE (as part of request URI) using an “ES URN”. Some possible values of ES indicators are described in Section 4.5 of the Emergency Services Stage-3 specification [29].

The IMS client Shall decorate the NAI used for emergency services as follows:

{sm=2}username@NSPrealm (where 2 indicates ES call).

7.4.8.1 ES Uniform Resource Name (URN)

The special indications for emergency sessions within the SIP signaling as specified in TS 24.229 [2] SHALL be supported. (note: this covers emergency numbers and the emergency URNs specified in [60].

7.4.9 Interface between location server and ASN

The interface between the Location Server (LS) and the ASN, required for emergency services, is described in [42].

7.5 QoS and PCC Procedures

IMS Session establishment, Modification and Termination are managed by PCC framework as IP-CAN Session modification, i.e. as IP-CAN Bearer Establishment, Modification and Termination based on 3GPP TS 23.203 [25], 3GPP TS 29.213 [57] and WiMAX NWG Rel. 1.5 PCC specifications [24]. In the following, the same examples are reported. The detailed IMS signaling refers to 3GPP TS [57] specification and PCC procedures refer to WiMAX NWG Rel. 1.5 PCC specification.

7.5.1 IMS Session Establishment

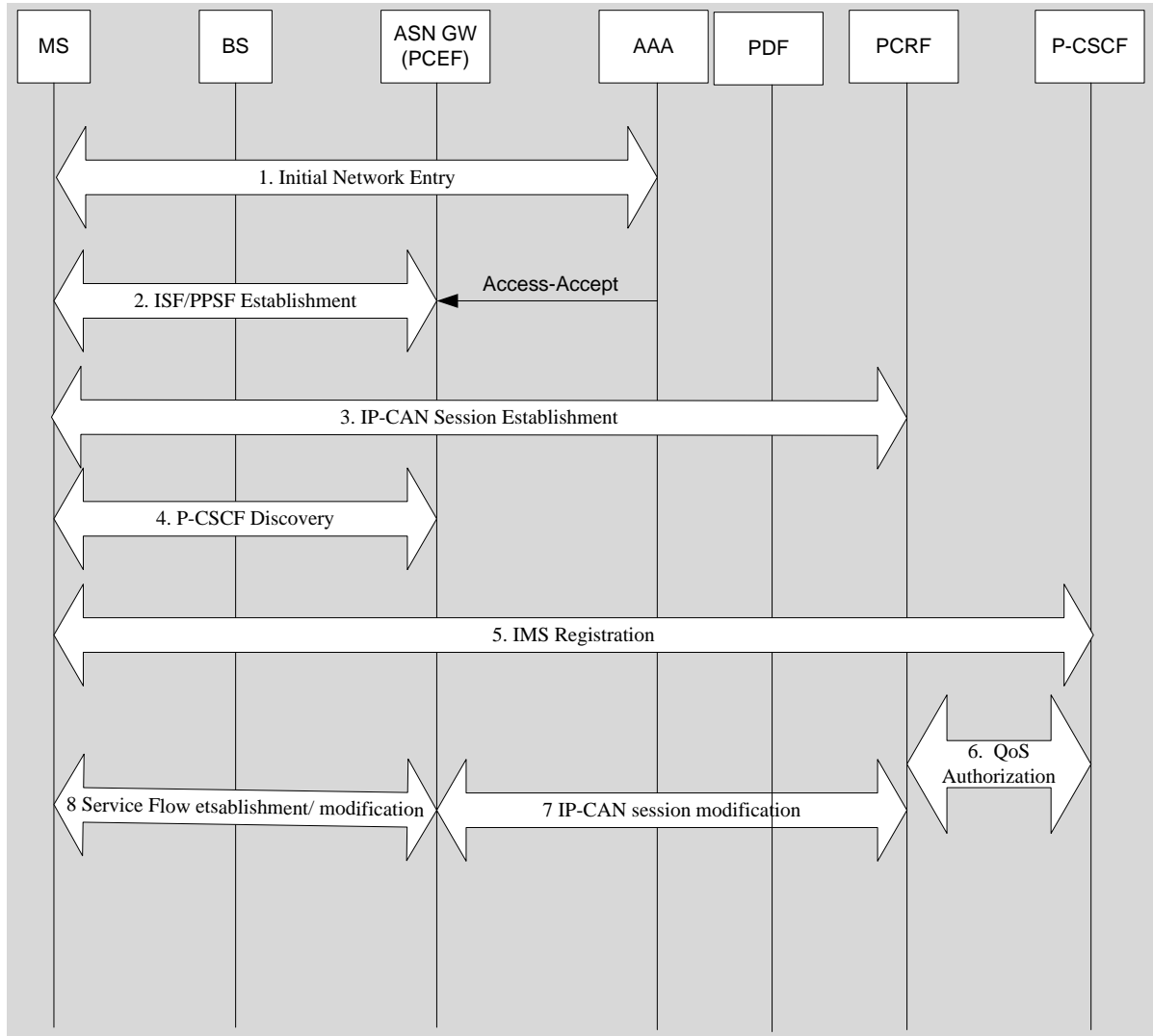


Figure 7-10: IMS Session Establishment

Note: Steps 1 through 3 may occur at network entry independent of the IMS Registration which may happen any time after the IP-CAN session establishment. P-CSCF discovery procedure may not immediately follow the IP-CAN Session Establishment procedure.

1. MS initiates network entry procedure as defined in NWG R1.3 specification.
2. After initial network entry, anchor SFA establishes ISF for the MS.
3. After the ISF/PPSF establishment and IP address assignment, A-PCEF initiates IP CAN Session Establishment with PCRF as defined in NWG R1.5 PCC Stage2 specification, A-PCEF may make ISF/PPSF modification as well.
4. MS performs P-CSCF Discovery procedure.
5. MS performs IMS registration with IMS network as defined in [8].
6. P-CSCF requests the establishment of a new Diameter Rx session to the PCRF. The PCRF performs a session binding and identifies the corresponding PCC rules related to IMS signaling.
7. PCRF initiates a IP-CAN Session Modification for the establishment/activation of the IP-CAN bearer for the IMS signaling.

8. A WiMAX Service Flow establishment/modification is performed by the A-PCEF as defined in [24].

7.5.2 IMS Session Establishment at Originating P-CSCF

The Figure 7-11 shows PCC and IMS procedures for a IMS Session establishment at the originating P-CSCF.

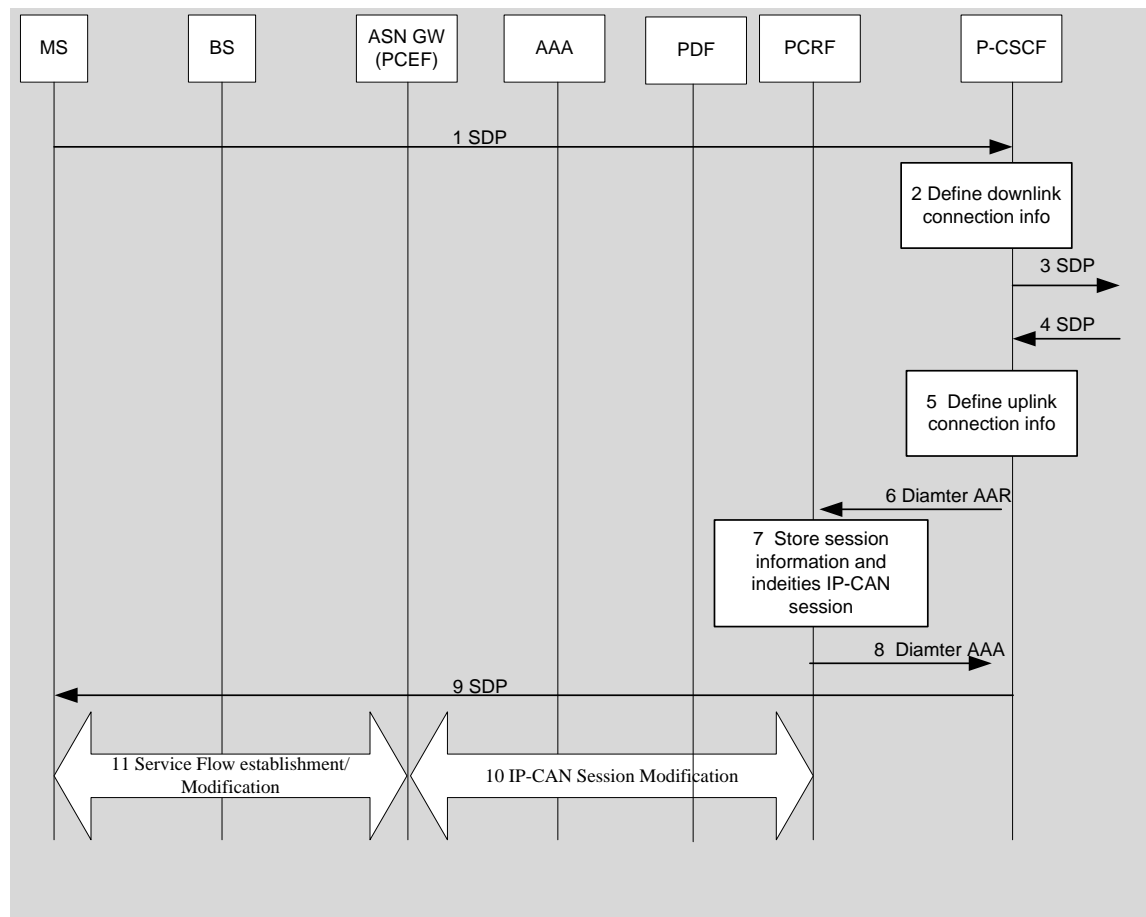


Figure 7-11: IMS Session Establishment at originating P-CSCF

Steps 1 through 9 are defined in 3GPP TS 23.203 and TS 29.213 [57] and are out of the scope of present WIMAX specification. They are shown here as example. For more details refer to the relevant 3GPP standards.

Step 1 through 9 – IMS session establishment at the originating P-CSCF. The P-CSCF derives the service information for the SDF offer/answer messages. The P-CSCF initiates a IP-CAN session modification with the PCRF to establish a new bearer carrying the IMS Session or modify an existing bearer.

Step 10: The IP-CAN session modification occurs between the PCRF and the A-PCEF as defined by WiMAX PCC specification [24]. Step 10 can occur in parallel with steps 8 and 9.

Step 11: A WiMAX Service Flow establishment/modification is performed by the A-PCEF as defined in [24].

7.5.3 IMS Session Modifications

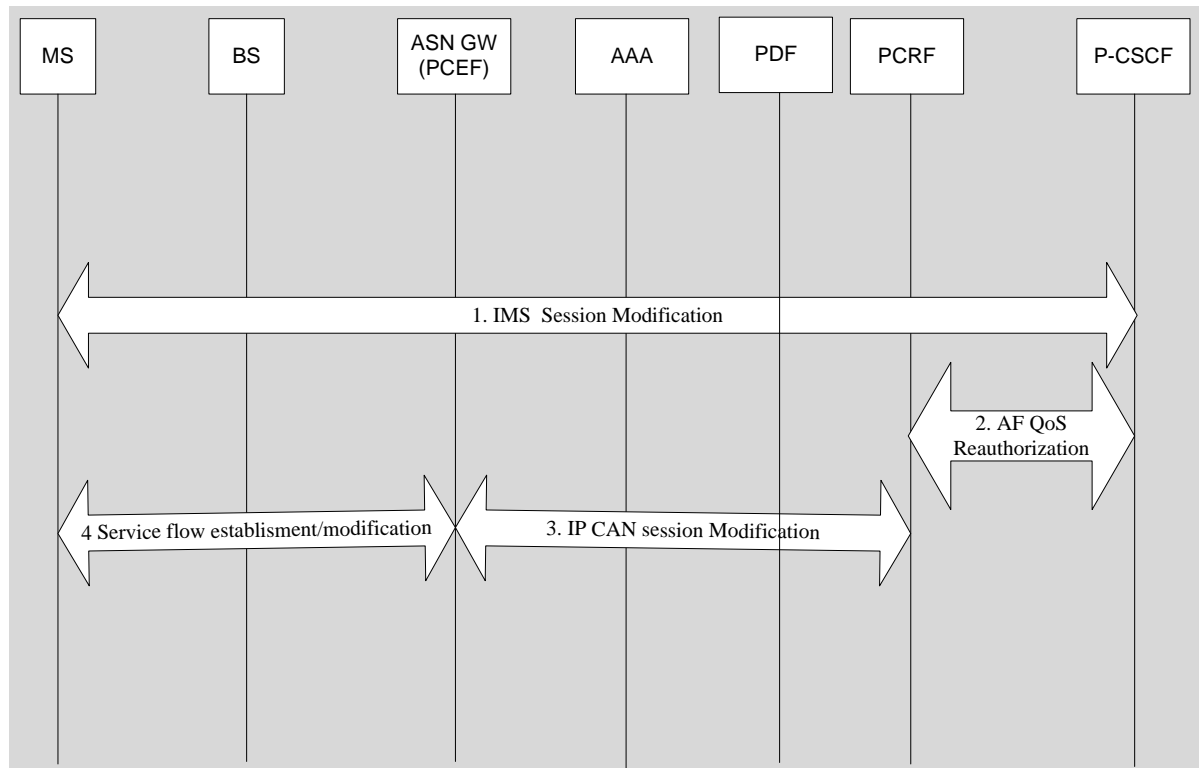


Figure 7-12: IMS Session Modification

1. The MS negotiates QoS with the P-CSCF by SIP signal exchange (Update or Re-invite) as defined in [8].
2. The P-CSCF performs QoS reauthorization with PCRF for the bearer modification via Rx interface. This step can be a part of step 1.
3. The PCRF initiates IP-CAN session modification as defined in [24].
4. A WiMAX Service Flow establishment/modification is performed by A-PCEF as defined in [24].

7.5.4 IMS Session Termination

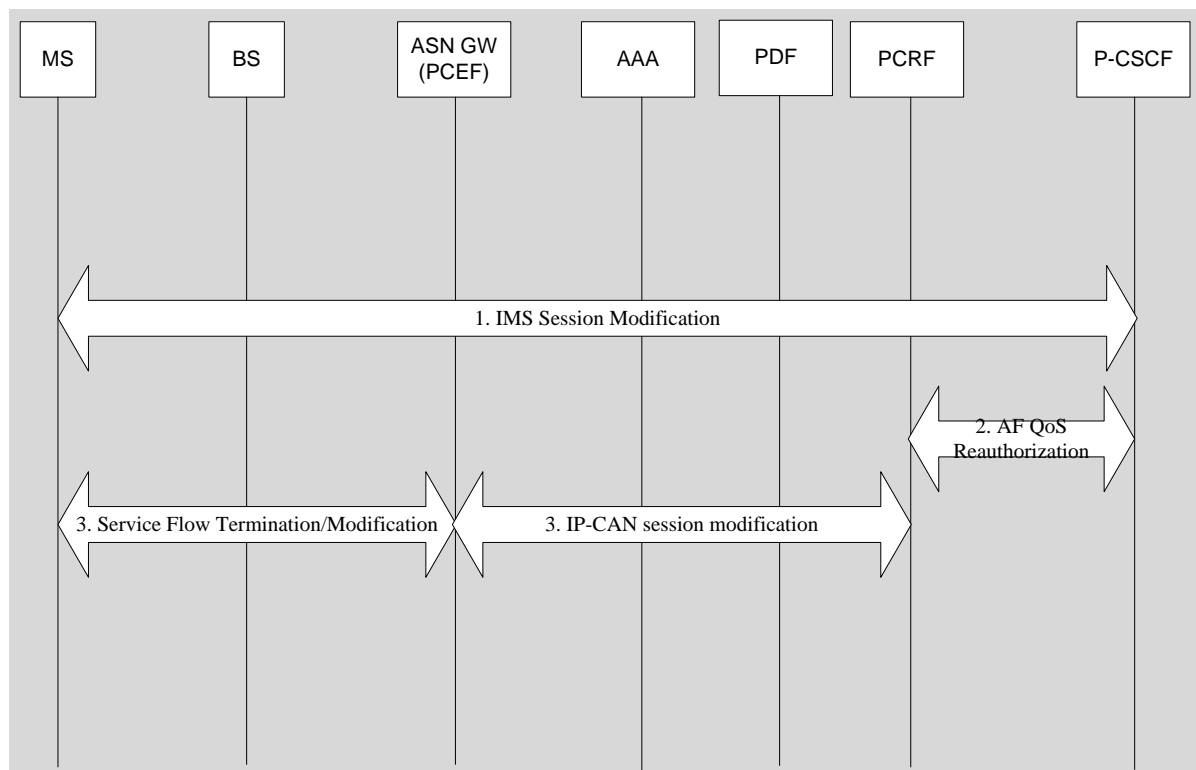


Figure 7-13: IMS Session Termination

1. The MS or P-CSCF initiates IMS Session Termination via P-CSCF by either SIP Bye message, a SIP CANCEL request, a SIP 3xx redirect response, or any 4xx, 5xx or 6xx SIP final error response..
2. The P-CSCF releases the IMS/AF session procedure as defined in 3GPP as defined in 3GPP 23.228.
3. The PCRF initiates IP-CAN session Modification or Termination Procedure for terminating the corresponding bearer as defined in [24].
4. A WiMAX Service Flow termination/modification is performed as defined in [24].

7.6 Charging Related Procedures and Correlation

The IM CN subsystem and the WiMAX network exchange charging information via the PCC framework [24] to correlate the WiMAX PCC related CDRs with the IM CN subsystem CDRs, i.e. to correlate the bearer level with the session level. The charging architecture, charging principles and charging data for IM CN subsystem are described in TS 32.240 [11] and TS 32.260 [12]. The informational elements that enable charging correlation between IM CN subsystem and WiMAX access domain with respect to OCS/OFCS are described in TS 24.229[2], TS 29.212 [22], and TS 29.214 [23]. The ICID (IMS Charging Identifier) is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems. The first IM CN subsystem entity involved in a SIP transaction will generate the ICID and include it in the ICID parameter of the P-Charging-Vector header in the SIP request. The ICID is used as the AF-Charging-Identifier in the PCC framework for correlation and is send by the AF (P-CSCF) to the WiMAX network over Rx/Gx interfaces. The WiMAX network in turn generates and sends the Access-Network-Charging-Identifier (ANCID) to the AF over the same GX/Rx interfaces.

The AF (P-CSCF) in the IMS-CN will populate the AF-Charging-Identifier (ICID) it generates and ANCID value it receives from the WiMAX domain in the P-Charging-Vector header which is passed to the S-CSCF. The S-CSCF may also pass the information to an AS, which may be needed for online pre-paid applications. The IM-CN elements will include these correlation identifiers in charging records send to the OFCS over the Rf interface. In the same way as shown in the Figure 7-14, the WiMAX domain also passes the charging identifiers to the OFCS over

the Gz interface. This enables the OFCS to correlate the charging information received from the WiMAX network with the charging information received from the IM- CN.

Note: The access network charging information for the originating network is used only within that network, and similarly the access network charging information for the terminating network is used only within that network. Thus the access network charging information is not shared between the calling and called networks. The access network charging information is not passed towards the external ASs from its own network.

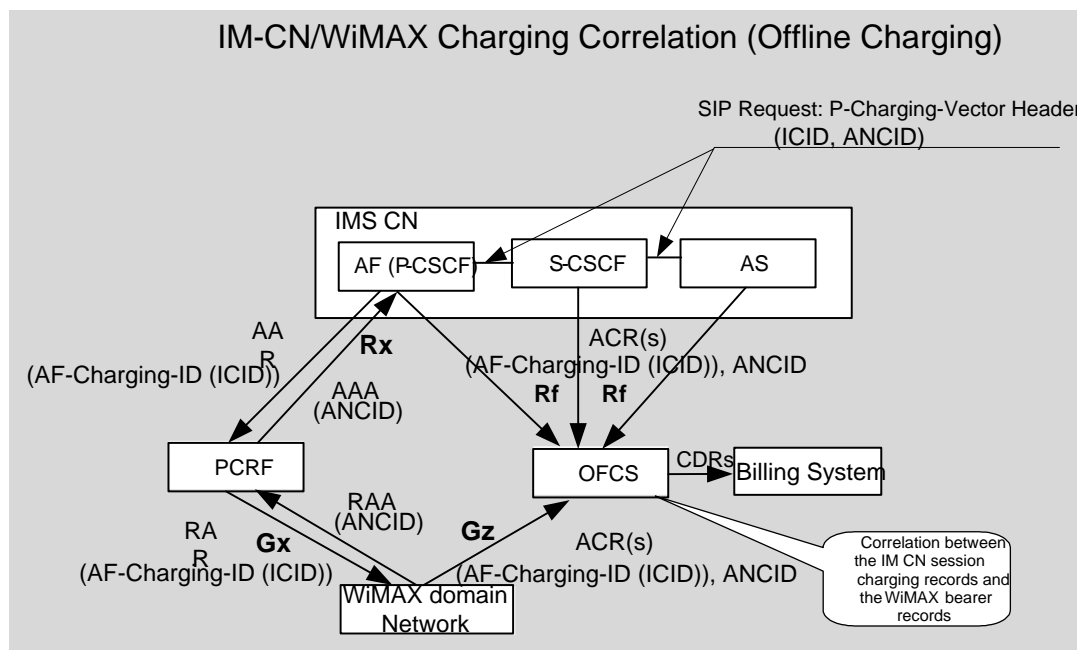


Figure 7-14: Correlation of IMS and PCC Charging Identifiers (WiMAX Domain Network includes the access network and the AAA)

7.7 Lawful Intercept

WiMAX IMS conforms to national/regional requirements for Lawful Intercept (LI). An overview for WiMAX aspects of LI is found in [59]. Specific requirements for packet data LI for North America is found in [58]. Location reporting requirements for Canada are described in Annex E of [58]. For IMS-based VoIP and other basic Multimedia Services (those relying on a basic session start and end) in the U.S. [48] should be used and for Canada TS 33.107 [35] and TS 33.108 [49] should be used. For more complex IMS multimedia services (e.g., push to talk), LI in NA will require additional study to determine LI requirements. Other regions will identify the specifications to be used for IMS LI in their region.

8. Stage 3 Procedures

The following provides Stage 3 description for the P-CSCF discovery procedure covered in section 7.2. The call flows described in section 7.2 are applicable for Stage 3 description and will not be repeated here.

8.1 Detailed Procedures for IMS Private Headers

The WiMAX MS SHALL follow the applicability, usage and procedures related to the UE in [6] and [2] with respect to all private SIP headers with the exception of the values of P-headers specified in clause 8.2.

All SIP IMS network elements associated with the WiMAX access network in both visited CSN and home CSN SHALL support all private SIP headers with the exception of the values of P-headers specified in clause 6.

8.2 WiMAX specific values for Private Header

8.2.1 P-Access-Network-Info

This specification extends the syntax of the P-Access-Network-Info defined in [6] to the following:

```
P-Access-Network-Info      = "P-Access-Network-Info" HCOLON access-net-spec
access-net-spec             = access-type *(SEMI access-info)
access-type                 = "WMF-Mobile WiMAX" / token
access-info                 = cgi-3gpp / utran-cell-id-3gpp / wimax-access-id /
extension-access-info      = gen-value
cgi-3gpp                    = "cgi-3gpp" EQUAL (token / quoted-string)
utran-cell-id-3gpp          = "utran-cell-id-3gpp" EQUAL (token / quoted-string)
wimax-access-id             = wimax-bs-id *(SEMI v-nsp-id)
wimax-bs-id                 = "wimax-bs-id" EQUAL gen-value
v-nsp-id                    = "v-nsp-id" EQUAL gen-value
nap-id                      = "nap-id" EQUAL gen-value
```

The WiMAX MS SHALL insert the P-Access-Network-Info header in any SIP request or response as required by [2]. The MS SHALL set the values in the P-Access-Network-Info header according to its current attachment to the ASN based on Table 8-1:

Table 8-1 P-Access_Network_Info

Parameter	Value
wimax-bs-id	BS-ID as defined in section 5.4.2.46 of [7]
v-nsp-id	If the MS is roaming then the visited NSP-ID as defined in section 5.4.2.56 of [7] If the MS is not roaming, this parameter is not included.
nap-id	NAP-ID as defined in section 5.4.2.45 of [7]

The following is an example of a P-Access-Network-Info header:

P-Access-Network-Info: WMF-Mobile WiMAX; wimax-bs-id=nnnnnnsssss;v-nsp-id=vvvvvv

Where nnnnnn is a 3 octet string for the NAP operator ID, ssssss is a 3 octet string for the base station ID and vvvvvv is a 3 octet string for the visited NSP ID.

8.2.2 P-Charging-Vector

This specification extends the syntax of the P-Charging-Vector defined in [6] to the following:

Access-network-charging-info	=	(gprs-charging-info / i-wlan-charging-info / xdsl-charging-info / packetcable-charging-info / wimax-charging-info / generic-param)
wimax-charging-info	=	ASN-GW *(SEMI ip-can-bearer) [SEMI extension-param]
ASN-GW	=	"ASN-GW" EQUAL gen-value
ip-can-bearer	=	ip-can-sig SEMI ip-can-cid SEMI * (flow-id)
ip-can-sig	=	"ip-can-sig" EQUAL ("yes" / "no")
ip-can-cid	=	"ip-can-cid" EQUAL gen-value
flow-id	=	"flow-id" EQUAL gen-value
extension-param	=	Token [EQUAL (token / quoted-string)]

The specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52] when the access network is WiMAX are: the wimax-charging-info parameter contains one ASN-GW child parameter and one or more child ip-can-bearer parameters. These parameters are conveyed to the P-CSCF by the WiMAX network over PCC interfaces. The ASN-GW parameter identifies the point of attachment of the UE to the WiMAX subsystem (ASN GW address). Each ip-can-bearer child parameter within wimax-charging-info corresponds to one WiMAX IP-CAN Bearer that was established by WiMAX for the UE. Each ip-can-bearer parameter contains an indicator if it is a WiMAX IP-CAN signaling bearer (ip-can-sig parameter), an associated IP-CAN Charging Identifier (ip-can-cid parameter), and one or more flow identifiers (flow-id parameter) that identify associated m-lines within the SDP from the SIP signaling [constructed by the P-CSCF as defined in Annex B of 3GPP 29.214].

For an IP-CAN Bearer that is only used for SIP signaling, i.e. no media stream requested for a session, then there is no authorization activity or information exchange over the respective WiMAX PCC interfaces. Since there is no ip-can-cid, or flow identifiers in this case, the ip-can-cid is set to zero and no flow identifier parameters are constructed by the P-CSCF.

8.3 DHCP Proxy in the ASN

The basic procedure of P-CSCF discovery when the DHCP Proxy functionality is provided in the ASN is shown in section 8.3.2. The requirements to support the connection setup are described next.

Note: this section may be moved into Stage 3 Rel 1.5

8.3.1 MS Requirements

The MS SHALL support the DHCP client function as defined in RFC 2131.

The MS SHALL send DHCP Inform with a SIP Server Option to acquire the P-CSCF address(es) or a list of FQDN of the P-CSCF(s). In the CMIP case, the DHCP messages may be broadcast. However, the MS SHOULD NOT encapsulate these messages even if the MS had negotiated with the network, during the CMIP registration stage, packet encapsulation of all the packets as described in RFC 3024 or just the broadcast and multicast packets as described in draft-chakrabarti-mip4-mcbc-xx.txt.

Upon receiving the DHCP ACK message as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6 from the DHCP Proxy, the P-CSCF address(es) or a list of FQDN of P-CSCF(s), and other configuration parameters SHALL be included as well as the DHCP options for SIP server (RFC 3319) and Domain Name as defined in RFC 3361 for IPv4 and in RFC 3646 for IPv6.

For the non CMIP scenario, the MS may optionally add SIP Server Option to the DHCP Discovery/Request or the DHCP Inform messages. Upon receiving DHCP ACK message from the network, the address(es) of the P-CSCF or a list of FQDNs of the P-CSCF(s) may optionally be included to support for the future IMS session establishment.

1 The MS SHALL perform a DNS query to retrieve a list of the P-CSCF(s) IP addresses, if the P-CSCF address(es)
2 are not received but the domain information in the DHCP Inform/Ack (for the FQDN domain returned in DHCP
3 Ack) is received from the DHCP Proxy.

4 **8.3.2 DHCP Proxy requirements**

5 The NAS may receive the P-CSCF address(es) or a list of fully qualified domain names (FQDN) of P-CSCF(s) from
6 the AAA server during the successful User Access Authentication, which SHALL be stored in the DHCP Proxy.

7 Upon receiving the DHCP Discovery/Request message, in which the P-CSCF address is requested, the DHCP Proxy
8 SHALL acknowledge the MS by sending the DHCP ACK message and may optionally include the P-CSCF
9 address(es) or FQDN list of the P-CSCF(s).

10 Upon receiving the DHCP Inform message from the MS, the DHCP Proxy SHOULD acknowledge the P-CSCF
11 address(es) or a FQDN list of the P-CSCF(s) by sending the DHCP Ack message to the MS as defined in RFC 2131
12 for IPv4 or RFC 3315 for IPv6. If the DHCP Proxy has stored P-CSCF information it SHALL include the P-CSCF
13 address(es) or FQDN list of the P-CSCF(s) in the DHCP Ack message. Other configuration parameters may be
14 included based on the DHCP options for SIP server (RFC3319) and Domain Name as defined in RFC 3361 for IPv4
15 and in RFC 3646 for IPv6 and made available to the DHCP proxy during the device/user authentication.

16 **8.4 DHCP relay in the ASN**

17 The basic procedure of P-CSCF discovery when a DHCP relay is located in the ASN is shown in section 7.2.2. The
18 requirements to support the connection setup are described next.

19 **8.4.1 MS Requirements**

20 The MS requirements are the same as described in section 8.3.1.

21 **8.4.2 DHCP Relay requirements**

22 The NAS may receive the DHCP server address(es) from the AAA server during the successful Device/User Access
23 Authentication, which SHALL be stored in the DHCP Relay.

24 Upon receiving the DHCP Discovery/Request message, in which the P-CSCF address is requested, the DHCP Relay
25 SHALL relay the message to the DHCP Server, and then acknowledges the MS by relaying the DHCP ACK message
26 which may optionally include the P-CSCF address(es) or a FQDN list of the P-CSCF(s).

27 Upon receiving the DHCP Inform message, The DHCP Relay SHOULD relay the message to the DHCP Server and
28 then acknowledge the P-CSCF address(es) or a FQDN list of the P-CSCF(s) by relaying the DHCP Ack message to
29 the MS from the DHCP Server as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6 which may optionally
30 include the P-CSCF address(es) or a FQDN list of the P-CSCF(s). Other configuration parameters may be included
31 based on the DHCP options for SIP server (RFC3319) and Domain Name as defined in RFC 3361 for IPv4 and in
32 RFC 3646 for IPv6 and made available to the DHCP server.

33 **8.4.3 DHCP Server requirements**

34 Upon receiving a DHCP Discovery/Request message where the P-CSCF address is requested, the DHCP Server
35 SHALL acknowledge the MS via the DHCP Relay by sending the DHCP ACK message that may include the P-
36 CSCF address(es) or a FQDN list of the P-CSCF.

37 Upon receiving a DHCP Inform message, The DHCP Server SHOULD acknowledge the P-CSCF address(es) or a
38 FQDN list of the P-CSCF by sending the DHCP Ack message as defined in RFC 2131 for IPv4 or RFC 3315 for
39 IPv6. If the DHCP Server has stored P-CSCF information, it SHALL include the P-CSCF address(es) or FQDN list
40 of the P-CSCF(s) in the DHCP Ack message. Other configuration parameters may be included based on the DHCP
41 options for SIP server (RFC3319) and Domain Name as defined in RFC 3361 for IPv4 and in RFC 3646 for IPv6,
42 which the DHCP server already has.

8.4.4 P-CSCF Assignment requirements

In a roaming case, the P-CSCF SHALL be assigned by either the Home NSP or the visited NSP. For Mobile IP networks, if the Visited AAA proxy assigns a vP-CSCF it SHALL also assign a vHA.

8.5 Hand Over Procedure during P-CSCF discovery

After a successful MS access authentication, the DHCP Proxy obtain the necessary information to enable the MS perform the P-CSCF Discovery procedure. How the DHCP Relay obtains the same information is not in scope of this specification. However, before or prior to the completion of the operation, a CSN anchored Mobility Handover might happen. After a successful MS access authentication, the MS obtains the necessary information to query the DHCP Proxy/Relay or the DNS server to perform the P-CSCF Discovery procedure.

According to [7] specification, the DHCP Proxy/Relay is collocated with the FA/Anchor DPF. During the FA relocation, the P-CSCF address related information is stored in the old serving DHCP Proxy/Relay and as part of the context transfer SHOULD be transferred to the new target DHCP Proxy/Relay. The Anchor ASN SHALL include the P-CSCF address related information in the Anchor DPF HO_Req message for that MS along with the other existing HO context information transferred to the Serving ASN.

Table 8-2 Anchor DPF HO_Req Message

IE	Reference	M/O	Notes
Anchor MM context	[7], subclause 5.3.2.11	M	DHCP Proxy Info, DHCP Server Info, P-CSCF address(es), a list of FQDN of P-CSCF(s), MIPv4 Info etc

Anchor MM Context

Type	11	
Length in octets	Variable	
Value	Compound	
Description	Information related with FA relocation, which means all context maintained by some entities binding with FA relocation	
Elements (Sub-TLVs)	TLV Name	M/O
	MS Mobility Mode	M
	MIPv4 Info	O
	DHCP Server List	O
	DHCP Proxy Info	O
	Idle Mode Info	O
	P-CSCF IP Address List	O
	P-CSCF FQDN List	O
	SF Info	O ¹
Parent TLV	MS Info	

¹ SF Info is Mandatory in Anchor MM Context when used in the Anchor DPF HO Request message.

Message Primitives That Use This TLV	Anchor DPF HO Request, Anchor DPF Relocate Request, R4 HO Request
---	---

1 **8.5.1.1 P-CSCF IPv4**

Type	400
Length in octets	4 bytes
Value	IPv4 address
Description	IPv4 address of the P-CSCF This TLV may be included multiple times as part of the P-CSCF IP Address List TLV.
Message Primitives That Use This TLV	P-CSCF IP Address List

2 **8.5.1.2 P-CSCF IPv6**

Type	401
Length in octets	16 bytes
Value	IPv6 address
Description	IPv6 address of the P-CSCF This TLV may be included multiple times as part of the P-CSCF IP Address List TLV.
Message Primitives That Use This TLV	P-CSCF IP Address List

3 **8.5.1.3 P-CSCF IP Address List**

Type	402	
Length in octets	Variable	
Value	Compound	
Description	List of P-CSCF IP Address(es).	
Elements (Sub-TLVs)	TLV Name	M/O
	P-CSCF IPv4, P-CSCF IPv6	O
Message Primitives That Use This TLV	Anchor MM Context	

4 **8.5.1.4 P-CSCF FQDN**

Type	403
Length in octets	variable
Value	ASCII string
Description	FQDN of the P-CSCF This TLV may be included multiple times as part of the P-CSCF FQDN List TLV.

Message Primitives That Use This TLV	P-CSCF FQDN List
---	------------------

8.5.1.5 P-CSCF FQDN List

Type	404	
Length in octets	Variable	
Value	Compound	
Description	List of P-CSCF FQDN.	
Elements (Sub-TLVs)	TLV Name	M/O
	P-CSCF FQDN	O
Message Primitives That Use This TLV	Anchor MM Context	

8.6 AAA Messages

The Radius attributes exchanged between the ASN and the HAAA are listed below:

8.6.1 Radius Message between the AAA and the ASN

The following table adds the P-CSCF (SIP) server attributes exchanged between the HAAA and the Authenticator located in the ASN as shown in Figure 7-2 step 1'. The attributes are conditional mandatory addition to Table 5-3 in [7] when IMS is supported.

Table 8-3 P-CSCF Attributes in Final RADIUS Access-Accept from AAA to ASN

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
hP-CSCF-IPv4	26/120	The IPv4 address of hP-CSCFs for IMS.	0	0	0-n[s][t]	0
hP-CSCF-FQDN	26/121	The FQDN of hP-CSCFs for IMS.	0	0	0-n[s][t]	0
vP-CSCF-IPv4	26/122	The IPv4 address of vP-CSCFs for IMS.	0-n[u]	0	0-n[s][t]	0
vP-CSCF-FQDN	26/123	The FQDN of vP-CSCFs for IMS.	0-n[u]	0	0-n[s][t]	0

FQDN		CSCFs for IMS.				
hP-CSCF-IPv6	26/124	The IPv6 address of hP-CSCFs for IMS.	0	0	0-n[s][t]	0
vP-CSCF-IPv6	26/125	The IPv6 address of vP-CSCFs for IMS.	0-n[u]	0	0-n[s][t]	0

1

2 Notes

[s] This attribute is only present when the MS has subscribed IMS.

[t] Attributes SHALL NOT appear in the Access Accept sent associated with the Device Authentication phase.

[u] Sent to HAAA by VAAA to let HAAA know that VAAA can assign the address. Should be sent with vHA-IP@, and also vDHCP Server Address if using DHCP Relay. If policies allow and HAAA authorizes the assignment by the vAAA attribute is returned in the Access Accept.

3 8.6.2 WiMAX Radius VSA Definition for P-CSCF Discovery

4 The following P-CSCF (SIP) server VSAs specify IP addresses or FQDNs of P-CSCF provided to the ASN for the
5 MS. The P-CSCF addresses SHALL be provided in order of preference.

6

```

7      0              1              2              3
8      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
9      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
10     |RADIUS TYPE 26 | Length          | Vendor-Id          |
11     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
12     | Vendor-Id (cont) | WiMAX TYPE    | Length          |
13     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
14     | Continuation | P-CSCF TLVs
15     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

16

WType-ID	120 for hP-CSCF-IPv4
Description	The IPv4 address of hP-CSCFs for IMS.
Length	6 + 3 + 4
Continuation	C-bit = 0

Value	Octet string containing one or a list of IPv4 addresses (most significant octet first)
--------------	--

WType-ID	121 for hP-CSCF-FQDN
Description	The hP-CSCF Domain Names for IMS.
Length	6 + 3 + (variable)
Continuation	C-bit = 0
Value	Octet string containing a Domain Name (most significant octet first)

WType-ID	122 for vP-CSCF-IPv4
Description	The IPv4 address of vP-CSCFs for IMS.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing a IPv4 addresses (most significant octet first)

WType-ID	123 for vP-CSCF-FQDN
Description	The vP-CSCF Domain Names for IMS.
Length	6 + 3 + (variable)
Continuation	C-bit = 0
Value	Octet string containing a Domain Names (most significant octet first)

WType-ID	124 for hP-CSCF-IPv6
Description	The IPv6 address of hP-CSCFs for IMS.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet string containing a IPv6 addresses (most significant octet first)

WType-ID	125 for vP-CSCF-IPv6
Description	The IPv6 address of vP-CSCFs for IMS.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet string containing a IPv6 addresses (most significant octet first)

8.7 Error Handling

This section describes error handling associated with P-CSCF discovery procedure.

8.7.1 No P-CSCF IP address or FQDN in the Access Accept message

If no P-CSCF IP address or FQDN is returned in the Access Accept message from the NAS after the MS has been successfully authenticated, the MS SHALL either rely on a pre-configured information, if available, or otherwise assume that IMS services are not available.

8.7.2 Inconsistent assignment of HA and P-CSCF

The P-CSCF and HA SHALL be hosted by the same network, home or visited CSN. If the visited network supports an HA and/or a P-CSCF, it SHALL include a v-HA TLV and/or a vP-CSCF TLV in the Access Request to the home network, respectively. If the home network authorizes the use of a visited HA, it SHALL return a v-HA TLV in the Access Accept to the visited network. If the home network authorizes the use of a P-CSCF in the visited network it SHALL either include a vP-CSCF TLV in the Access Accept to the visited network or it SHALL include a vP-CSCF TLV in the DHCP response to the visited network.

If the home network authorizes the assignment of a visited HA but the visiting network does not either support IMS or doesn't receive a vP-CSCF TLV from the home network, the visited network SHALL NOT make use an HA in the visited network. In this case, the visited network FA (IPv4) or AR (IPv6) in the NAS SHALL forward MIP RRQs to the home HA address downloaded during the access authentication and not to the visited HA. This will force the HA and P-CSCF to be both hosted in the home network.

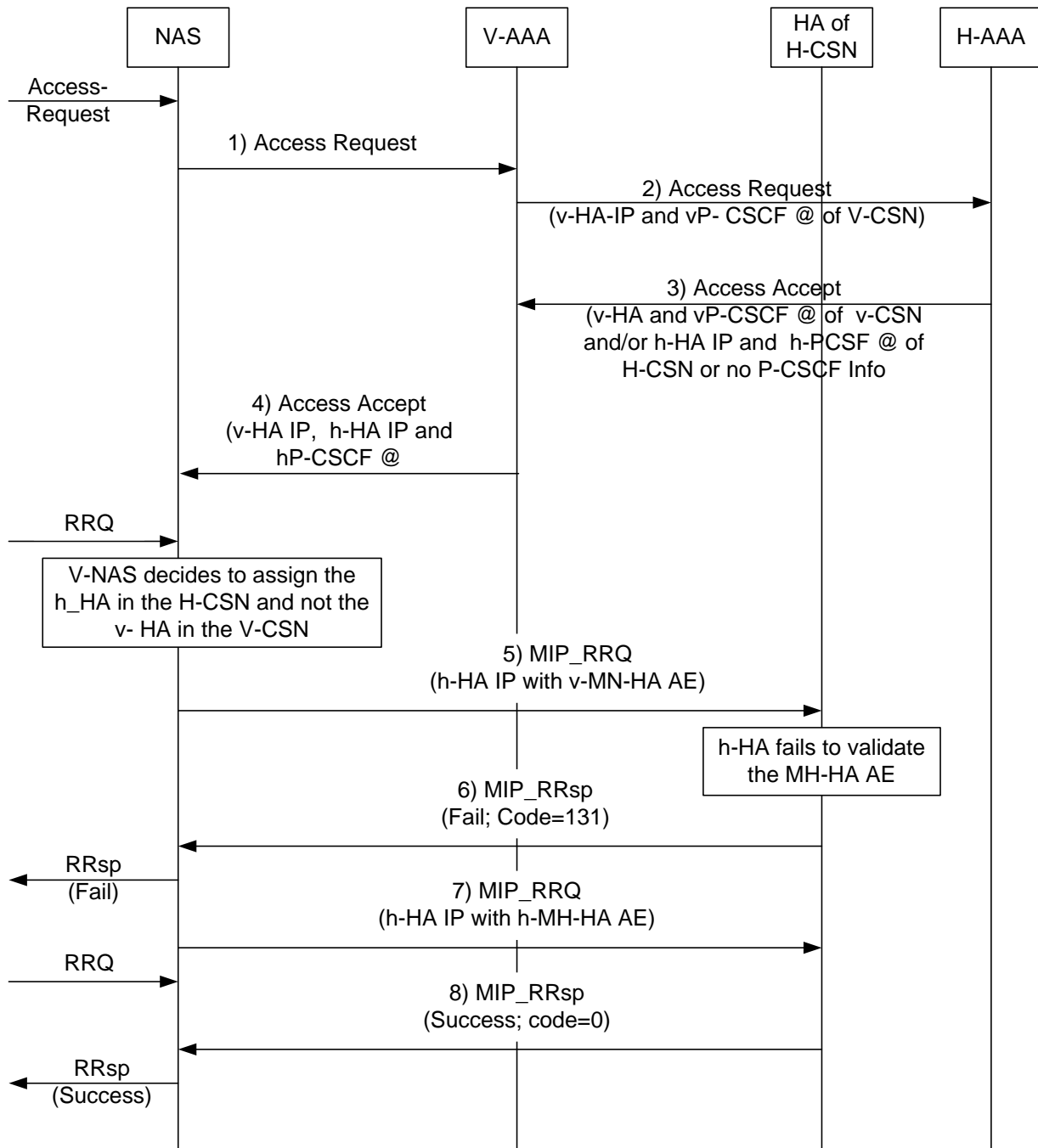


Figure 8-1: – Resolving inconsistent assignment of HA and P-CSCF

- Step 1: When Access Requests arrives at the visited ASN, per roaming agreement the NAS may append the v-HA IP attribute and send it to V-AAA. The NAS may also provide the visited P-CSCF address to the V-AAA.
- Step 2: The V-AAA forwards the Access Request to the H-AAA and appends the v-HA and the visited P-CSCF address.
- Step 3: The H-AAA may authorize the assignment of the v-HA and vP-CSCF by including the same information in the Access Accept. Alternately, the H-AAA may append the address of the h-HA and home P-CSCF in the Access Accept.

Step 4: If the Access Accept to the NAS doesn't include the vP-CSCF address, this implies the vP-CSCF is not authorized by the h-AAA or the v-AAA. Another possible scenario for this to happen is due to the omission of the vP-CSCF info in step 2. Otherwise, the Access Accept SHALL include either the v-HA and/or vP-CSCF, or h-HA and/or hP-CSCF.

Step 5: Recognizing lack of vP-CSCF information, the visited NAS forwards the MIP RRQ to the h-HA if hP-CSCF information was provided, and not to the v-HA as originally intended.

Step 6: Upon receiving MIP_RReq the HA in the home CSN determines that the v-MN-HA Authentication Extension (AE) in the MIP RRQ can't be validated, it SHALL reject the request and return to the NAS the MIP RRsp message with a failing error code 131.. The same MIP_Rsp message is returned to the Mobile IP client.

Step 7: After the error code is received by the MIP Client, it shall then start the MIP Registration process again and send another MIP RRQ protected by the proper h-MN-HA AE to the HA in the H-CSN.

Step 8: When the MIP_RReq is received and the h-MN-HA AE is verified and authorized successfully by the h-HA, it SHALL respond with MIP_Rsp to the NAS and the MIP Client by appending success code = 0 in MIP RRsp message.

Note: The amount of MIP_Req retransmission attempts by the MIP client is outside the scope of this document.

8.7.3 Timers consideration for DHCP Proxy in the ASN and DHCP Relay

All the timers shall be set and cleared according to RFC 2131 (DHCP), RFC 3315 (DHCPv6), RFC 3344 (MIP) and RFC 3775 (MIPv6) specifications.

8.7.4 Handling Error Condition

Table 8-4 lists the behavior for various error conditions during P-CSCF Discovery procedure:

Table 8-4 Error processing during P-CSCF Discovery

	Failure Case	Action
1	DHCP Offer is not received by the MS when timeout	Retransmit the DHCP Discovery message as described in RFC 2131 for IPv4 or RFC 3315 for IPv6
2	DHCP Ack is not received by the MS when timeout	Retransmit the DHCP Request/Inform message as described in RFC 2131 for IPv4 or RFC 3315 for IPv6
3	DNS Response is not received by the MS when timeout	Retransmit the DNS Query message as described in RFC 2131 for IPv4 or RFC 3315 for IPv6
5	hP-CSCF is assigned by H-AAA or DHCP server and visited HA is assigned by H-AAA or V-AAA	Forward all MIP RRQ to the home HA per procedure described in section 8.7.2

9. Security Aspects

Security Architecture overview

An MS is not provided services until a security association is established between the MS and the WiMAX network. IMS is essentially an overlay to the WiMAX network and has a low dependency on WiMAX security mechanism. Consequently a separate security association is required between the multimedia client and the IMS network before access is granted to multimedia services. The IMS security architecture is shown in the following figure.

IMS authentication keys and functions at the user side may be stored on a secure location on the MS. It shall be possible for the IMS authentication keys and functions to be logically independent to the keys and functions used for the access network authentication. However, this does not preclude common authentication keys and functions from being used for IMS and the access network authentication according to the guidelines given in subclause 8 of TS.33.203[3]

For the purposes of this section the ISIM or the secure memory in the MS is a term that indicates the collection of IMS security data and functions on the MS. Further information on the ISIM is given in TS 33.203[3].

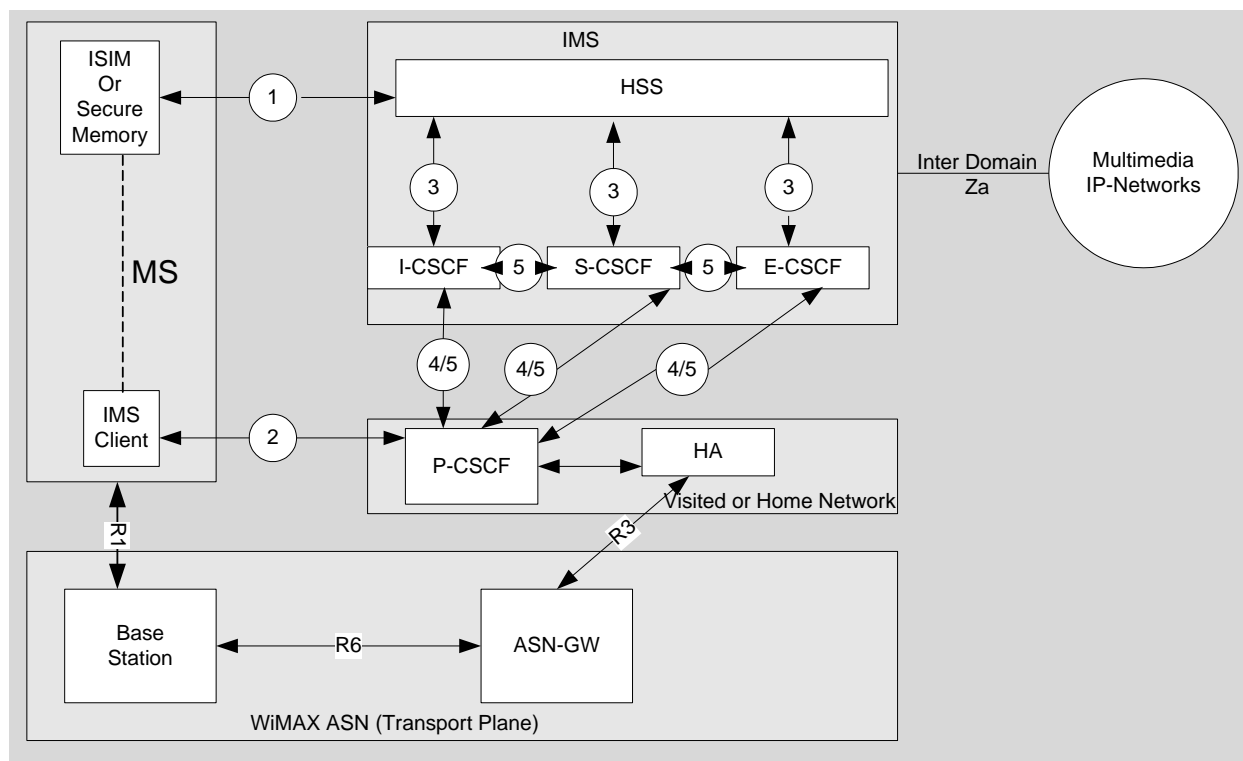


Figure 9-1: IMS security architecture

There are five different security associations and different needs for security protection for IMS and they are numbered 1, 2, 3, 4 and 5 in figure 9-1 where:

1. Provides mutual authentication. The HSS delegates the performance of subscriber authentication to the S-CSCF. The long-term key in the ISIM or in the secure memory of the MS and the HSS is associated with the user private identity. The subscriber will have one (network internal) user private identity and at least one external user public identity. The relation between the user private identity and user public identity is described in [8].
2. Provides a secure link and a security association between the IMS client residing in the MS and a P-CSCF for protection of the Gm reference point. Data origin authentication is provided i.e. the corroboration that

the source of data received is as claimed. For the definition of the Gm reference point see 3GPP TS 23.002 [14].

3. Provides security within the network domain internally for the Cx-interface. This security association is outside the scope of this document. It may be provided as specified by 3GPP TS 33.310 [15]. For the definition of the Cx-interface cf. 3GPP TS 23.002 [14]
4. Provides security between different networks for SIP capable nodes. This security association is outside the scope of this document. It may be provided as specified by 3GPP TS 33.310 [15]. This security association is only applicable when the P-CSCF resides in the visited network as described in TS 33.203 [3]. If the P-CSCF resides in the home network, bullet point number five below applies.
5. Provides security within the network internally between SIP capable nodes. This security association is outside the scope of this document. It may be provided as specified by 3GPP TS 33.310 [15]. Note that this security association also applies when the P-CSCF resides in the home network.

9.1 Inter-domain Security

There may be other interfaces to nodes outside the Home Network, which are also intended to be covered by this section. The involved nodes shall be capable of IPsec. Privacy protection shall be applied with cryptographic strength greater than DES. Integrity protection shall be applied. IPsec may be used in either transport mode or tunnel mode. When used in tunnel mode, one or both of the network security domains may use Security Gateways as shown in Figure 9-2. Security associations between nodes in different networks shall be negotiated using IPsec/IKE.

An inter-domain data path between the SEGs is established when a message is delivered across the domains. In WiMAX networks, in addition to the mechanism described in TS 33.310 [15], the security association for the Za data paths can be established through Pre Shared Keys (PSK) or through a dynamic negotiation using Public Key Infrastructure.

It is necessary that nodes outside the home network should be secure and trustworthy, perhaps using mechanisms such as firewalls, packet filters, and so on. However such details are outside the scope of this document.

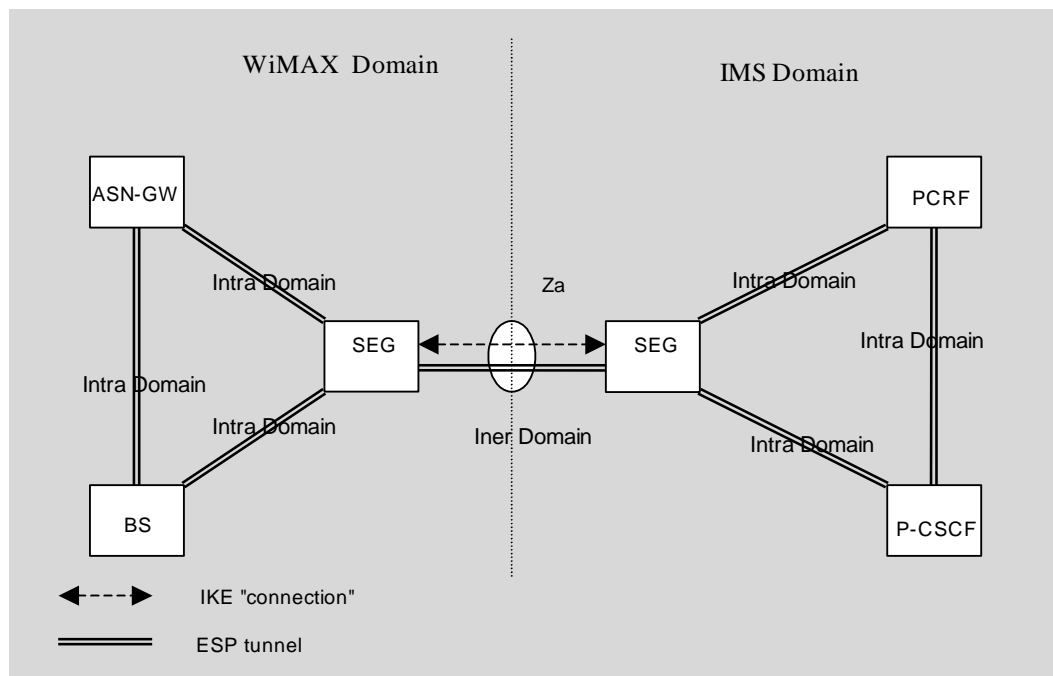


Figure 9-2: WiMAX and IMS inter domain security

9.2 Intra-domain Security

The interface labeled 5 in Figure 9-1 is between SIP-capable nodes in the same network security domain. The interface labeled 3 in Figure 9-1 is between the I-CSCF/S-CSCF and the HSS. There may be other interfaces to nodes inside the Home Network, which are also intended to be covered by this section. As these interfaces exist entirely within one network security domain, the administrative authority may choose any mechanism to secure this interface including, in addition to the cryptographic methods, physical security where appropriate.

9.3 IMS access Authentication

To ensure interoperation with all IMS systems, the IMS Client SHALL support the mandatory IMS AKA based authentication and key generation as well as IPsec protection of IMS signaling as described in the IMS specifications [2] and [3].

In addition, the IMS Client in WiMAX terminal SHOULD support SIP Digest Authentication and TLS as specified in [5].

10. Annex A – Informative NRM

Figure 10-1 provides an IMS reference architecture including interfaces towards non WiMAX legacy networks and other IP based multimedia systems. The detail description of these nodes and the IMS interfaces are described in 3GPP TS 23.228 [8]. For an illustrative purpose, the figure provides a consolidated view of the IMS functions, non-roaming PCC NEs and a Mobile IP WiMAX access network.

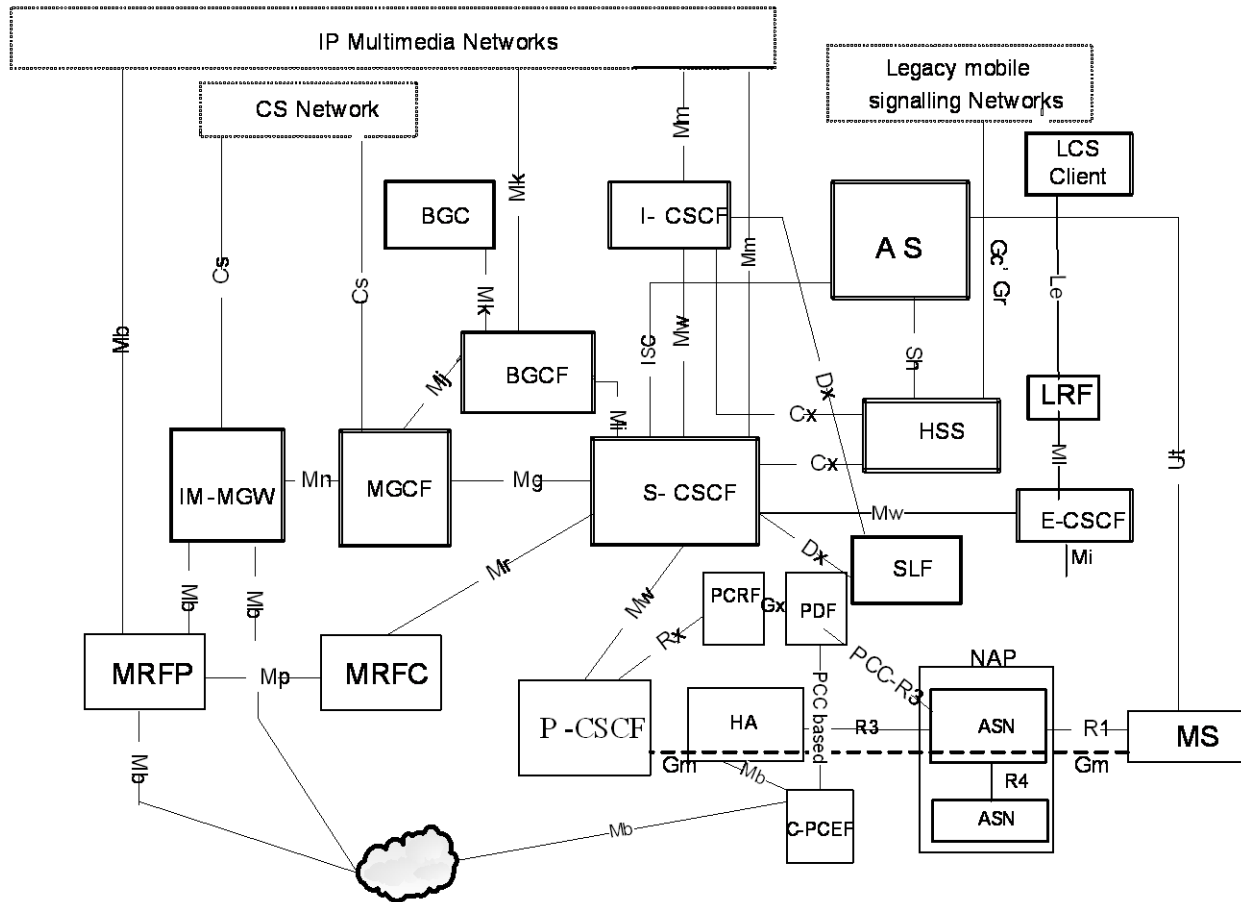


Figure 10-1: Reference Architecture of the IP Multimedia Core Network Subsystem including the WiMAX Network Elements supporting mobility. (Mb stands for bearer connection only)

11. Annex B – Charging Correlation of WiMAX Access, PCC and IM- CN

Informative

Figure 11-1 below shows the end to end offline charging scenario. The goal is to have one accounting stream for both AAA and OFCS/PCC charging in the WiMAX domain. The A-PCEF/Accounting Client in the WiMAX network performs an attribute translation of the AF-Charging-Identifier received from the AF and maps it to the WiMAX SDFID (service data flow identifier) attribute. It also maps the generated Access-Network-Charging-Identifier Values to the WiMAX PDFIDs (Packet Data Flow Identifiers). It includes both the translated attributes, i.e. SDFID and PDFIDs plus the Access-Network-Charging-Address (IP address of the CDR generator) in the accounting records send to the OFCS via AAA. The AAA server will provide an attribute translation of the SDFID and PDFID attributes to AF-Charging-Identifier and ANCID attributes before sending the accounting records to the OFCS.

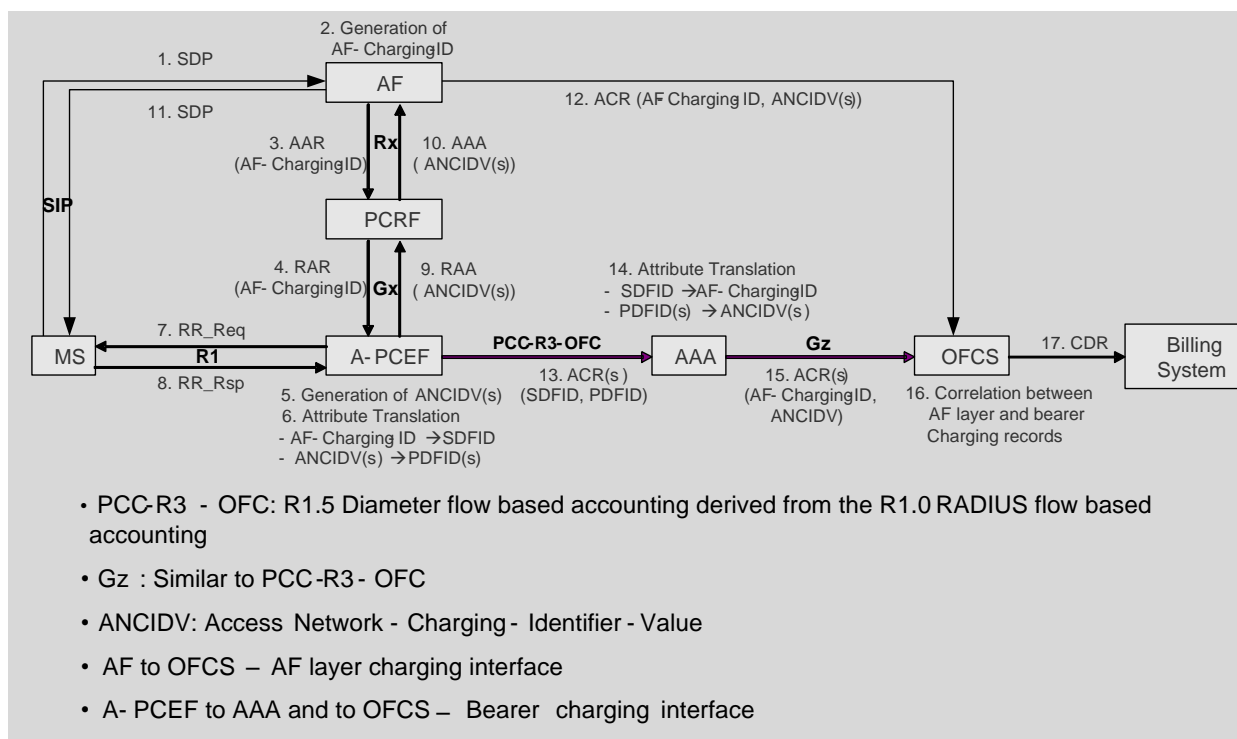


Figure 11-1: Offline Charging Scenario Using Charging Identifiers Mapping

