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

Copyright 2011 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 by the WiMAX Forum members, 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 or registered trademarks of the WiMAX Forum. All other trademarks are the property of their respective owners.
TABLE OF CONTENTS

1. INTRODUCTION AND SCOPE .......................................................................................................................1
  1.1 BACKGROUND .........................................................................................................................................1
  1.2 TERMINOLOGY .......................................................................................................................................1
  1.3 INTERWORKING SOLUTION MODEL AND ASSUMPTIONS ......................................................................2
  1.4 SCENARIOS ...........................................................................................................................................3
  1.5 CONTROL PLANE PROTOCOLS AND PROCEDURES ................................................................................5
  1.6 CLIENT MIP REQUIREMENTS ..................................................................................................................12
  1.7 HA AND H-AAA REQUIREMENTS .........................................................................................................13
  1.8 QoS FOR IPv4 .......................................................................................................................................13

2. WiMAX® PMIP – CDMA2000® CMIP INTERWORKING SOLUTION MODEL AND
   ASSUMPTIONS ...............................................................................................................................................13
  2.1 ASSUMPTIONS: .......................................................................................................................................13
  2.2 HANDOFF CALL FLOWS AND DESCRIPTION ......................................................................................14
  2.3 CONTROL PLANE PROTOCOLS AND PROCEDURES ............................................................................19
  2.4 CMIP4 SPECIFIC REQUIREMENTS .........................................................................................................19
  2.5 PMIP4 SPECIFIC REQUIREMENTS .........................................................................................................19
  2.6 DEVICE REQUIREMENTS .........................................................................................................................20
  2.7 HA REQUIREMENTS ...............................................................................................................................20
  2.8 H-AAA REQUIREMENTS .........................................................................................................................21

TABLE OF FIGURES

23 Figure 1 - Loosely-Coupled Interworking of WiMAX® with 3GPP2 .....................................................................3
24 Figure 2 - MIP4 Registration by a Hybrid WiMAX® – 3GPP2 MIP Client ............................................................7
25 Figure 3 - Key Computation and RRQ generation by Hybrid 3GPP2 – WiMAX® MIP Client ...............................8
26 Figure 4 - MIP4 Associated Transactions, Network Perspective ........................................................................9
27 Figure 5 - WiMAX® CMIP Call Flow .........................................................................................................10
28 Figure 6 - CDMA CMIP Call Flow .............................................................................................................11
1 References


1. Introduction and Scope

In the spirit of Stage 2 [3], this section specifies the loosely coupled method of interworking between WiMAX® systems and cdma2000® systems. This architecture is applicable to an operator that owns both access technologies and provisions its users with a dual mode device (dual radios) that can connect to the core network through any one of the two technologies.

1.1 Background

The 3GPP2 provides in document 3GPP2 S.R0087-A cdma2000®-Wlan Interworking the requirements for interworking between cdma2000® systems and Wireless Local Area Networks (WLANs). The intent of that document is to extend cdma2000® packet data and multimedia services and/or capabilities to the WLAN environment, and to support inter technology handoff of data sessions or voice calls between WLAN and cdma2000® 1X circuit-switched (CS) environments.

According to the document, potential areas of interworking between a WLAN systems and cdma2000® systems may include the following:

- Common authentication, authorization, and accounting functions to allow for a single bill for access of both systems.
- Access to common services from both the WLAN and cdma2000® systems.
- Creation of mechanisms for selecting and switching between the WLAN and cdma2000® systems.
- Support for mechanisms to allow session continuity as the mobile switches access between the WLAN and cdma2000® systems.
- Support for mechanisms to allow service continuity as the mobiles switches access between the WLAN and cdma2000® systems (including support for multimedia services).
- Support for handoff of voice calls between the WLAN and cdma2000® 1X CS-based systems.

Based on these classifications, the S.R0087-A cdma2000®-Wlan Interworking requirement document further specifies five interworking scenarios:

- Scenario 1: Common Billing and Customer Care.
- Scenario 2: cdma2000® System based Access Control and Charging and Access to the Internet via the WLAN system.
- Scenario 3: Access to the cdma2000® Packet Data Services via the WLAN system.
- Scenario 4: Session Continuity.
- Scenario 5: Access to cdma2000® circuit switched services and support of handoff between WLAN and cdma2000® 1X CS systems.

1.2 Terminology

1. **Dual Mode Device:** A multi radio device with cdma2000® and WiMAX® chipsets that leverages both cdma2000® EVDO/Rev A and WiMAX networks. This device could be a data card/USB/Handset. The dual mode device is also interchangeably referred as dual mode Mobile Node (MN), Mobile Station (MS), Mobile Device in the document.

---

1 cdma2000 is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000 is a registered trademark of the Telecommunications Industry Association (TIA USA) in the United States.
2. **Session Continuity (SC):** Capability that enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network from cdma2000® technology to WiMAX and vice versa.

### 1.3 Interworking Solution Model and Assumptions

WiMAX®-3GPP2 interworking refers to the integration of a WiMAX access network to an existing 3GPP2 core network infrastructure. Loosely coupled interworking, as specified in Stage 2 [3], is described in this section. The loosely coupled architecture enables a 3GPP2 operator to use common core elements such as AAA, HA, DHCP servers, provisioning and charging elements for both access technologies.

The loosely coupled architecture assumes a dual mode device (dual radios) and a connection manager that includes an EAP supplicant and most importantly, a client MIP that can set up same bindings (HoA and NAI) with the common HA through any of the available radio links and its associated CoA. The case of Proxy MIP to Proxy MIP inter technology handover is out of scope. To enable interworking between WiMAX and cdma2000®, an assumption about trust existing between the two networks is made. The cdma2000® and WiMAX networks may be within the scope of a single administrative domain or a trust relationship exist between the two networks when they are part of different administrative domains. WiMAX Forum® Network Architecture Stage 2 and 3 [2] does not address roaming and interworking among untrusted domains where devices such as PDIF may be required.

The following scenarios can be supported with the loosely coupled approach:

- **Scenario 1:** Common Billing and Customer Care.
- **Scenario 2:** cdma2000® System based Access Control and Charging and Access to the Internet via the WiMAX system
- **Scenario 3:** Access to the cdma2000® Packet Data Services via the WiMAX system
- **Scenario 4:** Session Continuity
- **Scenario 5:** Access to cdma2000 Circuit Switched Services and Support of Handoff between WiMAX and cdma2000® 1X CS Systems.

---

2 Connection Manager is a software client that runs in the MS to manage radio connection(s) that the MS is capable of.
1.4 Scenarios

The five network access and session mobility scenarios are described in this section. It is described how each of the scenarios can be implemented with the loosely coupled 3GPP2 – WiMAX® interworking architecture. In these scenarios, it is assumed that the 3GPP2 system is the home system of the dual mode devices and the WiMAX system is the visited system for these devices.

Scenario 1: Common Billing and Customer Care

By definition, when both access technologies are owned by the same operator, this scenario has no impact on the 3GPP2 or WiMAX specifications and will not be discussed further.

Scenario 2: Access to the Internet
To provide simple Internet access, the device/user would authenticate itself to the visited WiMAX system using its credentials. It would identify itself by NAI during the authentication exchange, and the realm portion of the NAI would indicate the 3GPP2 home system. This would enable authentication, authorization, and accounting messages to be routed to and from the 3GPP2 home system. Access to the Internet would be via the common 3GPP2 Core Network.

**Scenario 3: Access to the Home 3GPP2 Services via WiMAX®**

In loosely-coupled approach, Scenario 3 shall be implemented through the common access to the Home Agent of the 3GPP2 home system. As all the 3GPP2 services can be accessed through the HA, the MS can access any of these services offered by the 3GPP2 home network.

**Scenario 4.a: Session Continuity – Make Before Break using MS with Dual Radios**

Session continuity means the ability to continue a packet data session when handing off from a cdma2000® interface to a WiMAX interface (or vice-versa). Essentially, this means keeping the IP address (Home Address in Mobile IP) assigned to a MS at one point of attachment so that it can continue to send and receive packets for an ongoing IP session.

This scenario can be implemented as client software on the MS together with the deployment of suitable mobility agents in the network such as the 3GPP2 Mobile IP Home Agent. In this case, the client could re-register its current point of attachment (Care-of Address) whenever it changes WiMAX AR/FA or when it switches between WiMAX and cdma2000® interfaces.

Seamless session continuity means minimization of packet loss during a change in point of attachment. When handing off between heterogeneous interface technologies, such as between cdma2000® and WiMAX, a seamless handoff can be obtained simply by keeping both interfaces active for a period of time when adequate and overlapping coverage is available. Thus, Mobile IP4 or other registration procedures can take place on the new radio interface while packets are still being sent and received on the old radio interface. With proper management of the two radio interfaces in the MS, no packets should be lost over and above the native error rate of each technology type. In order to minimize packet loss during inter-technology handoff, the HA can accept packets from the previous Care-of Address for a limited period of time.

Use of simultaneous binding is for further study. Please note that a dual mode radio device operating in a dual coverage area is assumed in this specification. When dual coverage is not available, break before make algorithms are used and a lengthy data session interruption should be expected. When the handover between WiMAX and cdma2000® technology or vice-versa uses break-before-make type of algorithms, duration of interruption to ongoing sessions is likely higher as compared to the scenario where make-before-break algorithms can be applied.

**Scenario 4.b: Session Continuity Break Before Make**

In the case of break before make and PMIP to CMIP scenarios, issues such as dealing with IP address retention need to be addressed and will be studied in the future. In the CMIP to CMIP scenario the client will retain the IP address.

**Scenario 5: Access to cdma2000® Circuit Switched Services and Support of Handoff between WiMAX® and cdma2000® 1X CS Systems.**

The device may be able to listen for cdma2000® circuit switched services even when it is in WiMAX network coverage so as to support circuit switched voice and other cdma2000® 1X based services (SMS, location requests, etc.). Voice services are assumed to be supported through cdma2000® 1X circuit switched technology. If VoIP based voice services are available on WiMAX, then the device can utilize that service for voice services. This scenario is for future study Impetus for Loosely-Coupled Scheme.

### 1.4.1 Impetus for Loosely-Coupled Scheme

The loosely-coupled solution complies with the 3GPP2 S.R0087-A cdma2000®-Wlan Interworking requirements. The motivation is to make available an interworking solution for an operator that owns and operates both networks.

In order to enable interworking between WiMAX and cdma2000® networks, this architecture leverages the capabilities of cdma2000® network entities. It is a very convenient user interface and easy user management for the service provider that controls and operates both access technologies.
1) The WiMAX and cdma2000® networks can evolve independently. The cdma2000® network only needs to add the function to allow WiMAX users’ access to its AAA infrastructure, in addition to its original functions.

2) The users’ MS for this interworking can be WiMAX MS, 1X or 1x EV-DO MS, or dual mode MS for WiMAX and cdma2000® technology. This interworking scheme can also provide access for the WiMAX only users.

3) This interworking achieves unified authentication, authorization and accounting for WiMAX and cdma2000® users, which is well-suited to accounting of one-user-one-account or one-user-many-accounts.

4) Because of unified authentication, authorization and accounting and the unified access model, it will be convenient to realize the unified management for WiMAX and cdma2000® users, which will be a great advantage to the service providers.

5) Because of the unified access server point, data service continuity can be carried through WiMAX and cdma2000® networks for Simple IP’s access mode, and data service can be kept continuous in the process of handoff between and across WiMAX and cdma2000® networks.

6) Handoff between WiMAX and cdma2000® networks is processed by Mobile IP’s access mode. This method requires a common HA (Home Agent) network element and needs support for Mobile IP in the MS.

7) In the process of data services, the users can be provided the best services and need not concern if the access network is WiMAX or cdma2000®. That is, when the user is in WiMAX service area, the access network will be WiMAX, and when there is no sufficient WiMAX signal, the access network will be cdma2000® network. If so provisioned, the user MAY control the type of access network and decide if hand over should be executed when the user enters a WiMAX area.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Interworking Scenario</th>
<th>Impact to WiMAX®–cdam2000® Interworking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Common Billing and Customer Care</td>
<td>Loosely-Coupled: No impact on WiMAX and cdma2000® standards; possible to support</td>
</tr>
<tr>
<td>2</td>
<td>cdma2000® System based Access Control and Charging and Access to the Internet via the WiMAX system</td>
<td>Loosely-Coupled: No impact on WiMAX standard if independent access to both networks are supported by MS. Possible to support</td>
</tr>
<tr>
<td>3</td>
<td>Access to the cdma2000® Packet Data Services via the WiMAX system</td>
<td>Loosely-Coupled: No impact on WiMAX standard if independent access to both networks are supported by MS. Possible to support</td>
</tr>
<tr>
<td>4</td>
<td>Session Continuity</td>
<td>Loosely-Coupled: The continuity of a packet data session while switching of network connection takes places between the available access systems. Possible to support no impact.</td>
</tr>
<tr>
<td>5</td>
<td>Access to cdma2000® circuit switched services &amp; support of handoff between WLAN and cdma2000® 1X CS systems</td>
<td>Impacts WiMAX standard, cdma2000® circuit switched services cannot be accessed from WiMAX network. <strong>Not Supported.</strong></td>
</tr>
</tbody>
</table>

1.5 Control Plane Protocols and Procedures

This section provides the detailed description of WiMAX®-cdma2000® interworking.

1.5.1 Network Access Differentiation

The mobile uses an implementation-specific indication to identify the type of network it is accessing; e.g., whether it is the cdma2000® network, WiMAX network, etc.

In the absence of, or in addition to any other assured implementation-specific indications that the mobile is accessing either the WiMAX or cdma2000® network, the CMIPv4 capable MS MAY use other methods (e.g. unique 3GPP2 mobility extensions or features).

If mobile determines that it accessed the 3GPP2 network, the mobile shall behave according to the IETF RFC 3012. That is, the MS may possibly use either opaque or pre-configured value of SPI associated with authentication
extensions. Value of SPI SHALL indicate specific security association between MS and HA (MN-HA key) and algorithm used in computation of the MN-HA Authentication Extension.

If the mobile determines that it accessed the WiMAX network, the mobile SHALL comply with IETF RFC 3344. Specifically, among other required processes, MS will generate and include the MN-HA Authentication Extension in the MIP4 RReq or MIP6 BU. For this the MS will use the MN-HA key bootstrapped from the MIP-RK, which is in turn computed from the EMSK, upon successful completion of EAP Access Authentication Procedures.

MS shall use the value of the SPI associated with current MIP4 or MIP6 security association. This value will be set to SPI-CMIP4 or SPI-CMIP6 accordingly, computed from the EMSK upon successful completion of EAP-based Device/User Network Access Authentication and Authorization Access Procedures. Therefore, a tight deterministic association will be created between the SPI and all Mobile IP keys.
1.5.1.1 MIP Registration by the MS

Figure 2 shows the registration process and the SPI selection, as described in WiMAX Forum® Network Architecture Stage 3 Section 4.3.5.1, for use in the MIP registration by the hybrid 3GPP2-WiMAX® MIP Client. The modem cards/radio in the MS indicates the specific access technology to the connectivity client.

Figure 2 - MIP4 Registration by a Hybrid WiMAX® – 3GPP2 MIP Client
Figure 3 shows a simplified process of computation of Mobile IP keys and Registration Requests by a MIP4 Hybrid WiMAX®-3GPP2 Client.

1.5.1.2 MIP Registration Process in the WiMAX® Network

The following is the summary of logical steps in the process.

1) 3GPP2 PDSN/FA will receive the MIP_RReq that contains FA CHALLENGE extension and MN-AAA-AE. As specified in X.S0011 [1], the PDSN/FA will issue the RADIUS Access Request to the H-AAA to validate the MN-AAA-AE, even if the routable HA-ID is included in the MIP_RReq. Once the Access Accept is received, the PDSN/FA will copy/forward the MIP_RReq to the HA.

2) The WiMAX FA/A_DPF in the ASN will receive the MIP_RReq that does not contain MN-AAA-AE and MN-FACE. The WiMAX FA/A_DPF will already have the routable HA-ID from the RADIUS Access Accept received at the successful completion of the EAP Access Authentication process. If for some reason MN-AAA AE is delivered to the WiMAX FA/A_DPF, the MIP_RReq will be rejected with an error code 65 (administratively prohibited). If for some reason MN-FACE is delivered to the WiMAX FA/A_DPF, the extension will be dropped and will not be forwarded. If not rejected, the FA/A_DPF forwards the MIP_RReq to the HA.

3) The HA examines the SPI associated with the MN-HA-AE against a local database of active MN-HA keys. If the MN-HA key associated with SPI is present, HA validates MN-HA-AE. Otherwise, HA requests the MN-HA key from the H-AAA to validate the MN-HA-AE included in the MIP_RReq.

4) The H-AAA has to distinguish between X.S0011 [1] and WiMAX access in order to apply correct rule for deriving the MN-HA key. This is accomplished by examining the SPI associated with MN-HA-AE.
   - If SPI reported by HA is equal to SPI-CMIP4, H-AAA returns the WiMAX MN-HA key associated with MIP4 to the HA.
   - If SPI reported by HA is equal to SPI-PMIP4, H-AAA returns the WiMAX MN-HA key to the HA.
   - If SPI reported by HA is equal to SPI-CMIP6, H-AAA returns the WiMAX MN-HA key associated with MIP6 to the HA.
1. If SPI reported by HA is not equal to either SPI-CMIP4, SPI-CMIP6, or SPI-PMIP4, H-AAA returns the current pre-provisioned 3GPP2 MN-HA key to the HA, if allowed by local policy.

2. HA validates the MN-HA-AE and issues the MIP_RRep, which is then forwarded by the FA to the MN.

3. Note: Although the HA-ID should be obtained during the initial WiMAX access process, the MIP client can also obtain it dynamically by setting the HA field in the MIP_RReq to either 255.255.255.255 or 0.0.0.0 (ALL-ZERO-ONE-ADDR).

4. Simplified flowchart in Figure 4 exemplifies processing of the MIP4 RRQ by network elements.

![Flowchart](image-url)

**Figure 4 - MIP4 Associated Transactions, Network Perspective**
1.5.1.3 MIP Call Flows - WiMAX® Network Access

Figure 5 - WiMAX® CMIP Call Flow

1) ASN/FA sends a Foreign Agent Advertisement to the Mobile.
2) Mobile sends a Registration Request (MIP_RReq) containing the Mobile NAI Extension (MN-NAI), and the Mobile –Home Authentication Extension (MN-HA) to the ASN/FA.
3) ASN/FA sends MIP_RReq on to Home Agent (HA) with MN-NAI and MN-HA.
4) If the HA has the MN-HA shared key it validates the MN-HA-AE. Otherwise the HA sends RADIUS Access Request to the AAA Server to request the MN-HA key.
5) The AAA returns a RADIUS Access Accept with the MN-HA key to the HA.
6) The HA issues a Registration Reply (MIP_RRep) with a Reply code of 0 – “registration accepted” - which is sent to the ASN/FA. Also included are the MN-NAI and the MN-HA.
7) The ASN/FA forwards the MIP_RRep “registration accepted” with the MN-NAI and MN HA to the Mobile.
1.5.1.4 MIP Call Flows – 3GPP2 Network Access

Figure 6 - CDMA CMIP Call Flow

1) PDSN/FA sends a Foreign Agent Advertisement with Agent Advertisement Challenge Extension (AACE) to the Mobile.

2) Mobile sends a Mobile IP Agent Solicitation to the PDSN/FA.

3) PDSN/FA sends a Foreign Agent Advertisement with Agent Advertisement Challenge Extension (AACE) to the Mobile.

4) Mobile sends a Registration Request (MIP_RReq) containing the Mobile NAI Extension (MN-NAI), the Mobile Home Authentication Extension (MN-HA AE), Mobile-AAA Authentication Extension (MN-AAA AE), and the MN-FA Challenge Extension (MN-FA CE) to the PDSN/FA.

5) PDSN/FA sends RADIUS Access Request to the AAA Server including the MN-NAI, MN-HA AE, MN-AAA AE and MN-FA CE to validate the MN-AAA AE.

6) The AAA returns a RADIUS Access Accept with Attributes to the PDSN/FA.

7) PDSN/FA sends MIP_RReq on to Home Agent (HA) with MN-NAI and MN-HA AE (optionally the MN-AAA AE, and the MN-FA CE).

8) If the HA has the MN-HA key associated with the SPI, it validates the MN-HA AE. Otherwise the HA sends RADIUS Access Request to the AAA Server to request the MN-HA key for validating the MN-HA AE.

9) The AAA returns a RADIUS Access Accept with the MN-HA key to the HA.
10) The HA issues a Registration Reply (MIP_RRep) with a Reply code of 0 – “registration accepted” which is sent to the PDSN/FA. Also included are the MN-NAI and the MN-HA AE.

11) The PDSN/FA forwards the MIP_RRep “registration accepted” with the MN-NAI, MN-HA AE and the MN-FA CE to the Mobile.

### 1.6 Client MIP Requirements

As depicted in Figure 7-66 Stage 2 Section 7.8.1.9 [2], the MIP client resides above the Network Interface Card and is part or integrated into the operating system stack. The basic connection setup procedure using CMIP4 is shown in Stage 2 [2], Section 7.8.1.9.1.

The MIP4 client is common to both technologies and used by the dual-mode hybrid MS to connect to the 3GPP2 and WiMAX networks. Manual and automatic network selection mechanism SHALL be supported. If so enabled by the provisioning operator, in manual mode the user SHALL be able to override any selection criteria. In automatic mode, the MS will select one of the available networks. The automatic network selection procedure and criteria are out of scope for this document.

The Mobile IPv4 Client behavior assumes that the Mobility stack in the MS conform to IETF standards such as RFC 3344 and SHALL support procedures defined in RFC 3012 for the 3GPP2 access. The remainder of this section describes the detailed Stage 3 node requirements for each phase of the user’s session via CMIP4.

If the CMIP4 capable MS receives an Agent Advertisement from the FA that contains CHALLENGE extension, or CHALLENGE extension was delivered to the Mobile IPv4 Client in the previous MIP_RRep during the existing mobility session, the MS SHALL assume behavior according to IETF RFC 3012.

Accordingly, the MS SHALL include the CHALLENGE extension in the MIP_RReq. The MS SHALL generate the MN-AAA Authentication Extension according to IETF RFC 3012 and include it in the MIP_RReq. If MS also requests dynamic home agent assignment, it SHALL set the HA field to either 255.255.255.255 or 0.0.0.0.0 (termed as ALL-ZERO-ONE-ADDR). The MS SHALL compute the MN-HA Authentication Extension according to IETF RFC 3012 and include it in the MIP_RReq. Value of SPI SHALL indicate specific security association between the MS and HA (MN-HA key) and algorithm used in computation of the MN-HA Authentication Extension.

If the CMIP4 capable MS receives an Agent Advertisement from the FA that does not contain CHALLENGE extension, or CHALLENGE extension was not delivered to the Mobile IPv4 Client in the previous MIP_RReply during the same mobility session, the MS SHALL assume behavior according to the remainder of this section.

Due to the EAP based method of bootstrapping Mobility Keys, after successful Device/User Network Access Authentication and Authorization, the Mobile IP Client SHALL have access to all the mobility keys that it requires, such as MN-HA-CMIP4, and the outer NAI used during authentication. From the same EAP based bootstrapping, the Mobile IP Client SHALL also have access to the value of the SPI associated with the MN-HA-CMIP4, namely SPI-CMIP4.

A CMIP4 capable MS SHALL send a Mobile IPv4 RReq to the FA after it receives an Agent Advertisement (that is received solicited or unsolicited) from the FA containing a new FA-CoA. In the MIP_RReq from the WiMAX network, the MS SHALL include an NAI extension that is consists of the pseudoidentity@realm that was used as the outer NAI during EAP based Device/User Network Access Authentication and Authorization.

As mention before, when the MIP Client starts its access and MIP registration from the WiMAX network, it uses pseudoidentity@realm. The client will have to apply the same NAI and HoA values during the 3GPP2 MIP re-registration process in order to maintain its original mobility binding with the HA and the session. Similarly if initial access is through the 3GPP2 network using a fully qualified user NAI, the same NAI and HoA values will be used for re-registration (re-binding) through the WiMAX systems in order to maintain same HA mobility binding and the session.

The MIP_RReq SHALL also contain MN-HA AE, the revocation support extension and may also contain MN-FA AE and FA-HA AE.

---

3 For pre-provisioned value of MN-HA key the value of SPI will most likely also be pre-provisioned, or be opaque.
In the HoA field in the MIP_RReq, if the MS desires a fresh dynamic address allocation by the home agent, it SHALL include 0.0.0.0.

If the Mobile IP Client has access to the address of the Home Agent from the EAP based bootstrapping, the Mobile IPv4 Client SHALL set the HA field in the MIP_RReq to this address. Although the address of the HA should be obtained during the initial bootstrapping, the MIP client can also obtain it dynamically by setting the HA field in the MIP_RReq to either 255.255.255.255 or 0.0.0.0 (ALL-ZERO-ONE-ADDR).

Upon receiving a MIP_RRep in response to the MIP_RReq with reply code = 0 (success), the MS SHALL use the HoA contained in the MIP_RRep as the HoA for the mobility session. In this case, the HA address contained in the MIP_RRep SHALL be treated as the assigned home agent for the session (if dynamic home agent assignment was requested).


The error handling and retransmission behavior of the MS SHALL be governed by the Mobile IPv4 standard RFC 3344.

When connected to a WiMAX network, if the MS uses MIP4, it SHALL NOT invoke DHCP for IPv4 address acquisition before starting the Mobile IP procedures. The scenario when the MS performs CMIP4 registration after the network performs PMIP4 procedures is out of scope.

### 1.7 HA and H-AAA Requirements

The common HA and AAA elements SHALL comply with both 3GPP2 and WiMAX® requirements. The AAA needs to support RFC-2865 and RFC-4372 and the HA needs to support NAS-Port-Type (Type 5) and the WiMAX capability (Type 26) attributes. The WiMAX requirements for the HA and H-AAA are listed in Sections 2.7 and 2.8 and the ones for 3GPP2 are listed in X.S0011-D [1].

### 1.8 QoS for IPv4

Mapping of service flows with different QoS attributes between 3GPP2 and WiMAX® access technologies during handover is out of scope for this release. It is assumed that for service continuation, the service flow admission at the target technology is done at a lower level and when a session is handed over to the target technology while anchored at the HA, all the flows are handed over and contained within the respected FA to HA tunnels.

### 2. WiMAX® PMIP – cdma2000® CMIP Interworking Solution

#### 2.1 Assumptions:

1. The dual mode device with Session Continuity is able to connect to WiMAX® networks using DHCP exchange so that Proxy-Mobile IP (PMIP) can be used. Also, the dual mode device is able to connect to cdma2000® networks so that Client Mobile IP can be used.
2. The dual mode device camps on one network while trying to acquire a target network without losing IP connectivity or active data session.
3. It is assumed that the AAA servers used for cdma2000® access and WiMAX access are either the same or they have access to the same session state and subscriber database.

The mechanism for maintaining the AAA session continuity after intertechnology handover where the AAA-Session-ID is removed due to the accounting stop message is FFS.
2.2 Handoff Call Flows and description

This section describes the handoff call flows for mobility between cdma2000® and WiMAX® access systems. It is assumed that the cdma2000® systems uses CMIP4 for network layer connectivity and mobility management and the WiMAX system uses PMIP4 for network layer connectivity and mobility management.

2.2.1 3GPP2 CMIP4 to WiMAX® PMIP4 Handoff
Figure 8 – 3GPP2 – WiMAX® (CMIP4 – PMIP4) Handoff Call Flow

X.S0011-D Procedures* - The transactions shown in this box are for illustrative purposes only. The X.S0011 procedures [1] take precedence over any potential inconsistencies appearing in this box.

Description of the Steps:

a. It is assumed that the HRPD session is already established. The MS builds CMIP RRQ using ALL-ZERO-ONES value for HoA and HA fields (dynamic HA and HoA assignment).

b. The FA generates a RADIUS Access-Request message including the initial NAI (initial NAI = cdma2000 NAI) and MN-AAA Authentication Extension to authenticate MS (as per RFC 3012) and sends the message to the HAAA.
c. The H-AAA attempts to determine whether the MS has an ongoing mobility session or not. If not found, it creates a new mobility session and stores the assigned HA.

d. The H-AAA returns the assigned HA value in a RADIUS Access-Accept message.

e. The PDSN/FA relays the RRQ to the assigned HA, FA includes the Revocation Support Extension. The HA value in the MIP RRQ is not changed. The PDSN/FA may remove the MN-AAA AE in the RRQ. Absence of the WiMAX PMIP Access Technology Type extension in the RRQ allows the HA to determine that the RRQ is associated with MS’s cdma2000® access.

f. The HA detects that there is no existing mobility binding for the MS, and communicates with AAA to obtain MN-HA key, using NAI as identifier.

g. HA validates the RRQ using the Client MN-HA AE (as per X.S0011-D specification [1]). Upon successfully validating the RRQ, the HA assigns HoA for the MS and sends MIP RRP to PDSN/FA.

h. The PDSN/FA forward RRP to the MS.

i. The MS detects WiMAX coverage and decides to initiate WiMAX network entry procedures as per (WiMAX Forum® Network ArchitectureR1.5 specification). Note that a new WiMAX session is established at the time the MS decides to handover from the 3GPP2 network to the WiMAX network.

j. The MS uses the same NAI value (initial NAI = cdma2000 NAI) that it used to connect to the cdma2000® network (ref step b) as the NAI for the outer value to perform access authentication (EAP) in the WiMAX network.

k. Upon successful access authentication, the H-AAA retrieves the stored HA value from step c and generates the mobility keys.

l. The H-AAA sends the previously assigned HA and mobility keys to the Authenticator ASN at the completion of access authentication for the MS.

m. Upon completion of WiMAX network entry, the MS broadcasts a DHCPDISCOVER message. In addition, DHCPDISCOVER may carry previously assigned HoA in yiaddr.

n. The DHCP proxy receives the DHCPDISCOVER and determines the MS associated with the data path over which the DHCP message was received. The PMIP client, on behalf of the MS, generates a MIP RRQ using the NAI returned by the HAAA used for initial binding, the HA, and the mobility keys received in step l. RRQ SHALL contains PMIP Access Technology Type Extension (draft-leung-mip4-proxy-mode-06.txt) indicating WiMAX access type and SHALL also includes the Revocation support Extension. RRQ may contain previously assigned HoA received from H-AAA or in DHCPDISCOVER.

o. The HA receives MIP RRQ and detects the presence of PMIP Access Technology Type extension. This determines that the RRQ is associated with MS’s session over a WiMAX ASN. The HA locates the existing mobility binding by using the NAI value in the RRQ as the index.

p. In order to validate the RRQ, the HA (after detecting that SPI had changed) generates a RADIUS Access-Request message including the MN-NAI and MN-HA authenticator extensions and sends the message to the H-AAA. The AAA server authenticates the user and sends an Access-Accept message back to the HA.

q. Upon successfully validating the RRQ, the HA updates the binding with the CoA of the WiMAX ASN-GW (CoA-1) for the MS’s WiMAX access. The HA also in step p replies to the PMIP client with MIP RRP.

r. After removing old binding HA sends a Registration Revocation message to remove the CDMA session.

s. Upon receiving the RRP from the HA with successful registration indication, the PMIP client prompts the DHCP proxy to generate a DHCPOFFER and send it to the MS.

t. MS completes DHCP procedures (Request and Ack) as per WiMAX Forum® Network Architecture R1.5 [2] and continues with the data session over the WiMAX access.

Note: The session removal in the cdma2000® network is FFS.
2.2.2 WiMAX® PMIP4 to 3GPP2 CMIP4 Handoff

Figure 9 – WiMAX® – 3GPP2 (PMIP4 – CMIP4) Handoff Call Flow

X.S0011-D Procedures* - The transactions shown in this box are for illustrative purposes only. The X.S0011 procedures [1] take precedence over any potential inconsistencies appearing in this box.
Description of the Steps:

a. The MS connects to WiMAX network and initiates access authentication (EAP) using an initial NAI (initial NAI = cdma2000 NAI).

b. Upon successful access authentication (i.e. EAP success), H-AAA assigns an HA for the MS’s session and stores that HA value.

c. The H-AAA completes access authentication by sending an Access-Accept to the Authenticator ASN. In this message it includes the assigned HA value and the necessary mobility keys.

d. Because there is no data session active, the MS broadcasts a DHCPDISCOVER message.

e. The DHCP proxy receives the DHCPDISCOVER and determines the MS associated with the data path over which the DHCP message was received. The PMIP client, on behalf of the MS, generates a MIP RRQ using the initial NAI, the HA, and the mobility keys, received in step c. The RRQ SHALL contain PMIP Access Technology Type Extension (draft-leung-mip4-proxy-mode-06.txt) indicating WiMAX access type and also SHALL include the Revocation support Extension. The PMIP Client then sends the MIP RRQ to the HA.

f. Upon receiving the RRQ, the HA detects the presence of PMIP Access Technology Type Extension. This determines that the RRQ is associated with the MS’s access over a WiMAX network. The HA detects that there is no existing mobility binding for the MS (identified by the NAI). The HA initiates AAA interaction as per WiMAX Forum® Network Architecture R1.5 spec to fetch the mobility keys necessary to validate the authentication extensions in the RRQ.

g. After successfully validating the RRQ, the HA assigns HoA for the MS and responds to the PMIP client with a MIP RRP.

h. The PMIP client validates the RRP and prompts the DHCP proxy to generate a DHCPOFFER with the assigned HoA to the MS.

i. The MS responds to the DHCPOFFER with a DHCPREQUEST

j. The DHCPProxy replies to the DHCPREQUEST with a DHCPACK and the WiMAX data session setup is complete

k. The MS detects cdma2000® network coverage and decides to initiate network entry into the cdma2000 network. If the MS already has a dormant session in the cdma2000 Network, the session is re-activated.

l. Upon receiving Agent Advertisement from the PDSN/FA in the cdma2000® network, the MS constructs CMIP4 RRQ using zero values in the HoA and HA fields. The MS also includes MN-FA CE, MN-AAA AE and NAI extension as per X.S0011-D specification [1]. The value in the NAI extension contains the same NAI (initial NAI = cdma2000 NAI) that the MS used to access the WiMAX network in step a.

m. The PDSN/FA receives the RRQ and generates a RADIUS Access-Request message in order to validate the MN-AAA AE for the MS (identified by the NAI in the NAI extension) with the H-AAA server. This step is performed as per X.S0011-D specification [1].

n. The H-AAA searches for an HA IP value associated with the NAI. It assigns the same HA from the MS’s session state database. This is the HA that the MS was assigned in the WiMAX system.

o. The AAA returns this HA IP value to the PDSN/FA along with the Access-Accept message. The AAA server does not instruct the PDSN/FA to remove the MN-AAA AE from the RRQ while forwarding it to the HA.

p. The PDSN/FA forwards the RRQ to the assigned HA from step o. The PDSN/FA may remove the MN-AAA AE from the RRQ. The PDSN includes the Revocation Support Extension.

q. The HA receives MIP RRQ and detects the absence of PMIP Access Technology Type extension. This determines that the RRQ is associated with MS’s session over a cdma2000® network. The HA locates the
existing mobility binding by using the NAI value in the RRQ as the index. In order to validate the RRQ, the
HA processes the included authentication extensions (MN-AAA AE, MN-HA and if present FA-HA AE).
The included SPI values in these extensions indicate to the HA that the security associations are different
than the one it currently has (i.e. security associations associated with the WiMAX access for the MS). If
the HA does not have the necessary security associations (mobility keys) corresponding to the SPI values in
these extensions, the HA initiates interaction with the AAA server (as per X.S0011-D specification [1])
10 obtain MN-HA key, using NAI as identifier.
11
r. Upon successfully validating the RRQ, the HA updates the binding with the CoA of the cdma2000
12 PDSN/FA (CoA-2) for the MS’s cdma2000 access.
13
s. The HA generates a MIP RRP and sends it to the PDSN/FA including the HoA value associated with the
14 existing MIP session.
15
t. Upon receiving the RRP from the HA with successful registration indication, the FA/PDSN validates the
16 necessary authentication extensions (FA-HA if present) and then sends it to the MS. The MS in turn
17 validates the RRP and if successful moves ahead with the packet data session over the cdma2000® access.
18
u. The HA sends Registration Revocation to the FA in the ASN-GW, removing the WiMAX session.
19
Note: It should also be noted that assignment of the same address to another interface when the MN moves from one access type
20 to another does not guarantee session continuity. As an example, additional software such as a shim to hide the physical interface
21 may be required to enable session continuity.
22
2.3 Control Plane protocols and Procedures
23
2.3.1 Network Access Differentiation
24
The HA identifies that the RRQ came from WiMAX® by the presence of the PMIP Access Technology Type
25 Extension (draft-leung-mip4-proxy-mode-06.txt) indicating WiMAX access type.
26
2.4 CMIP4 Specific Requirements
27
The dual mode device SHALL use the same NAI that it used in the WiMAX® system as an outer NAI while
28 constructing the RRQ in the cdma2000® system.
29
2.5 PMIP4 Specific Requirements
30
1. The dual mode device SHALL use the NAI that is pre-provisioned for access in cdma2000® system while
31 performing access authentication in the WiMAX® system. The pre-provisioned cdma2000® system NAI
32 SHALL be used both as inner and as outer NAI in the WiMAX access.
33
2. The device and the network SHALL support all PMIP4 requirements documented in the WiMAX Forum®
34 Network Architecture [2].
35
3. When the MS moves from cdma2000® to WiMAX, the HAAA SHALL assign the same HA that was
36 assigned when the MN was in the cdma2000® network. The Access Accept message includes the assigned
37 HA value as part of the access authentication procedure.
38
4. The PMIP4 RRQ message SHALL contain only the following extensions:
39       a. MN_NAI
40       b. MN_HA
41       c. PMIP Access technology type extension indicating the WiMAX access type.
5. The PMIP4 RRQ message SHALL NOT contain the MN-AAA AE.

2.6 Device Requirements

In this solution, the dual mode device camps on one network while trying to acquire a target network without losing IP connectivity or active data session.

1. The dual mode MS SHALL use the static NAI (the NAI that is pre-provisioned for access to the cdma2000 system) on both cdma2000® and WiMAX network authentication.

2. The dual mode MS SHALL support simultaneous radio connections on each access network while changing between cdma2000 EVDO and WiMAX networks, if coverage is available on both networks.

3. The dual mode MS SHALL use DHCP in WiMAX so that all PMIP4 specific requirements as documented in WiMAX Forum® Network Architecture [2] apply.

4. The CMIP4 RRQ message SHALL contain the following extensions in the following order:
   a. MN_NAI
   b. MN_HA
   c. MN_FA (Optional)
   d. MN_AAA
   e. Foreign Agent Challenge Extension (FACE)

2.7 HA Requirements

The Home Agent SHALL support the following requirements for dual mode device session continuity:

1. The HA SHALL recognize the identity of the radio access technology by examining the CVS Extension appended by the ASN-GW. If in the future the PDSN also appends a CVSE, the value carried will provide the access type.

2. The HA MAY update mobility bindings for different access technology types while temporarily maintaining the prior binding.

3. The same HA SHALL be able to handle in-transit packets from the MS with the previous Care-of Address when the mobility binding is already switched and pointing to a new Care-of Address. This is to mitigate packet loss in the uplink during seamless mobility across access technologies.

4. The HA SHALL enforce the use of same NAI on both access networks. If the NAI in a RRQ message does not match the same in existing mobility bindings, the HA SHALL treat the RRQ as a new MIP registration.

5. For PMIP4 based RRQ processing, the HA SHALL follow the procedures defined in [2] to interact with the AAA server. For CMIP4 based RRQ processing, if the HA determines that the RRQ is associated with a cdma2000® access, the HA SHALL use X.S0001-D specific procedures [1] to interact with the AAA server.

6. The HA SHALL support session revocation.
The HA MAY support simultaneous binding, in particular for the support of HO between PMIP and CMIP.

### 2.8 H-AAA Requirements

1. For WiMAX®, the AAA SHALL perform access authentication when the MS uses static NAI. The AAA server shall perform the access authentication procedures as per WiMAX Forum® Network Architecture R1.0 Rev 1.3 specification.

2. For WiMAX, the AAA SHALL assign an HA upon successful access authentication (EAP completion) and reply to the Authenticator ASN with the assigned HA (in Access-Accept).

3. For cdma2000® technology, the AAA SHALL perform MN-AAA AE authentication as per X.S0011-D specification [1]. In cdma2000® systems, the MS uses static NAI by default.

4. For cdma2000® technology, the AAA SHALL assign an HA during MN-AAA authentication and reply with an Access Accept including the assigned HA address.

5. The AAA SHALL store the assigned HA to support session continuity.

6. The AAA SHALL assign the same HA for both WiMAX and cdma2000® session set-ups. Re-registrations and mobility management.

7. The AAA SHALL maintain the NAI to HA-IP@ association for a configurable duration after receiving an indication of session termination from the source network.