WiMAX Forum™ Network Architecture

WiMAX - 3GPP2 Interworking

WMF-T37-004-R010v3

WiMAX Forum Approved

(2008-01-11)

WiMAX Forum Proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

Revision History

March 2007	Initial draft, from contribution “061026_NWG _WiMAX-3GPP2 IWK_Annex V7 V8 clean.doc”.
November 06, 2007	Implemented all Stage 3 accepted contributions from 00000_r055_NWG-Rel-1.0.0-CR-Tracking-Spreadsheet.xls
January 11, 2008	Implemented all Stage 3 accepted contributions from 00000_r069_NWG-Rel-1[1].0.0-CR-Tracking-Spreadsheet.xls

References

[1] IS-835, which can be found at http://www.3gpp2.org/Public_html/specs/X.S0011-001-D_v1.0_060301.pdf

1. Introduction and Scope

In the spirit of Stage 2, 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.

http://www.3gpp2.org/Public_html/specs/X.S0011-001-D_v1.0_060301.pdf

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 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, 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[1] that includes an EAP supplicant and most importantly, a client MIP that can set up same bindings (HoA and NAI) with the

[1] Connection Manager is a software client that runs in the MS to manage radio connection(s) that the MS is capable of.

common HA through any of the available radio links and its associated CoA. The case of Proxy MIP for inter-technology handover is out of scope for this release.

For this interworking solution, we are also assuming dual network ownership and trusted domains of both technologies. For cases where the same operator doesn't own both technologies, loosely coupled architecture can still be deployed by two separate operators if they trust each other's secured air link protection and mandate a secure link between the respected FAs and the designated common HA. Release 1.0.0 is not addressing roaming scenario and interworking among untrusted domains where devices such as PDIF may be required.

We introduce here the notion of WiMAX access network by analogy to the WLAN access network discussed in *3GPP2 S.R0087-A CDMA2000-Wlan Interworking* and further claim that the following four scenarios can be easily addressed 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.

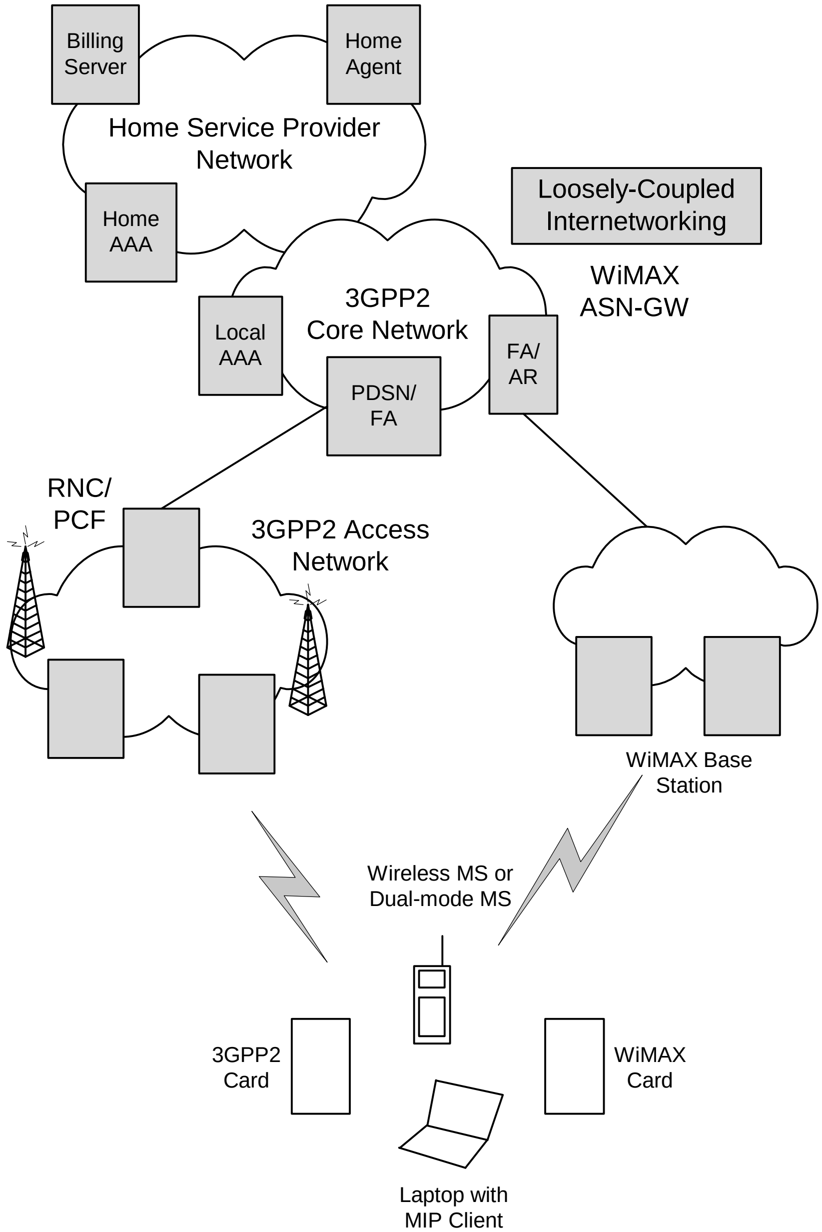

Figure 1 - Loosely-Coupled Interworking of WiMAX with 3GPP2

1.3 Scenarios

Below we discuss the four scenarios and briefly describe how each scenario can be implemented with the loosely coupled architecture.

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 Core Serving Network (CSN) with no additional tunneling necessary.

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 therefore access any of these services on the home network.

Scenario 4: Session Continuity

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 assigned to a MS at one point of attachment so that it can continue to send and receive packets from an ongoing session.

Scenario 4 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 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 types, 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. If simultaneous binding is supported by the HA, Mobile IP or other registration can take place on the new interface while packets are still being sent and received on the old interface. With proper MS management of the two interfaces, no packets should be lost over and above the native error rate of each technology type.

Please note that for the purpose of this specifications a dual mode device (dual radios) operating in a dual coverage area is assumed. When dual coverage is not available, break before make algorithms is used and a lengthy data session interruption is expected. The interruption period is related to the required setup time of the alternate link including authentication and authorization by remote AAAs and HA infrastructure, which may exceed one second.

Scenario 5: Access to cdma2000™ Circuit Switched Services and Support of Handoff between WiMAX and CDMA2000 1X CS Systems.

Access to circuit switched services and voice services is not supported in this WiMAX release. This scenario is not supported in this release (Release 1.0.0).

1.3.1 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 the time frame of NWG Release 1.0.0.

In order to enable interworking between WiMAX and cdma2000™ networks, this architecture leverages the capabilities of CDMA 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 CDMA networks can evolve independently. The CDMA 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 CDMA. This interworking scheme can also provide access for the WiMAX only users.

3) This interworking achieves unified authentication, authorization and accounting for WiMAX and CDMA 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 CDMA 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 CDMA 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 CDMA 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 CDMA. 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 CDMA. 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.

Scenario	Interworking Scenario	Impact to WiMax –CDMA2000 Interworking
1	Common Billing and Customer Care	Loosely-Coupled: No impact on WiMAX and cdma standards; possible to support
2	CDMA2000 System based Access Control and Charging and Access to the Internet via the WiMAX system	Loosely-Coupled: No impact on WiMAX standard if independent access to both networks are supported by MS. Possible to support
3	Access to the CDMA2000 Packet Data Services via the WiMAX system	Loosely-Coupled: No impact on WiMAX standard if independent access to both networks are supported by MS. Possible to support
4	Session Continuity	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.
5	Access to CDMA2000 circuit switched services & support of handoff between WLAN and CDMA2000 1X CS systems	Impacts WiMAX standard, CDMA2000 circuit switched services cannot be accessed from WiMAX network. **Not Supported.**

1.4 Control Plane Protocols and Procedures

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

1.4.1 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 CMIP4 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.

1.4.1.1 MIP Registration by the MS

Figure 2 shows the registration process and the SPI selection, as described in NWG 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.

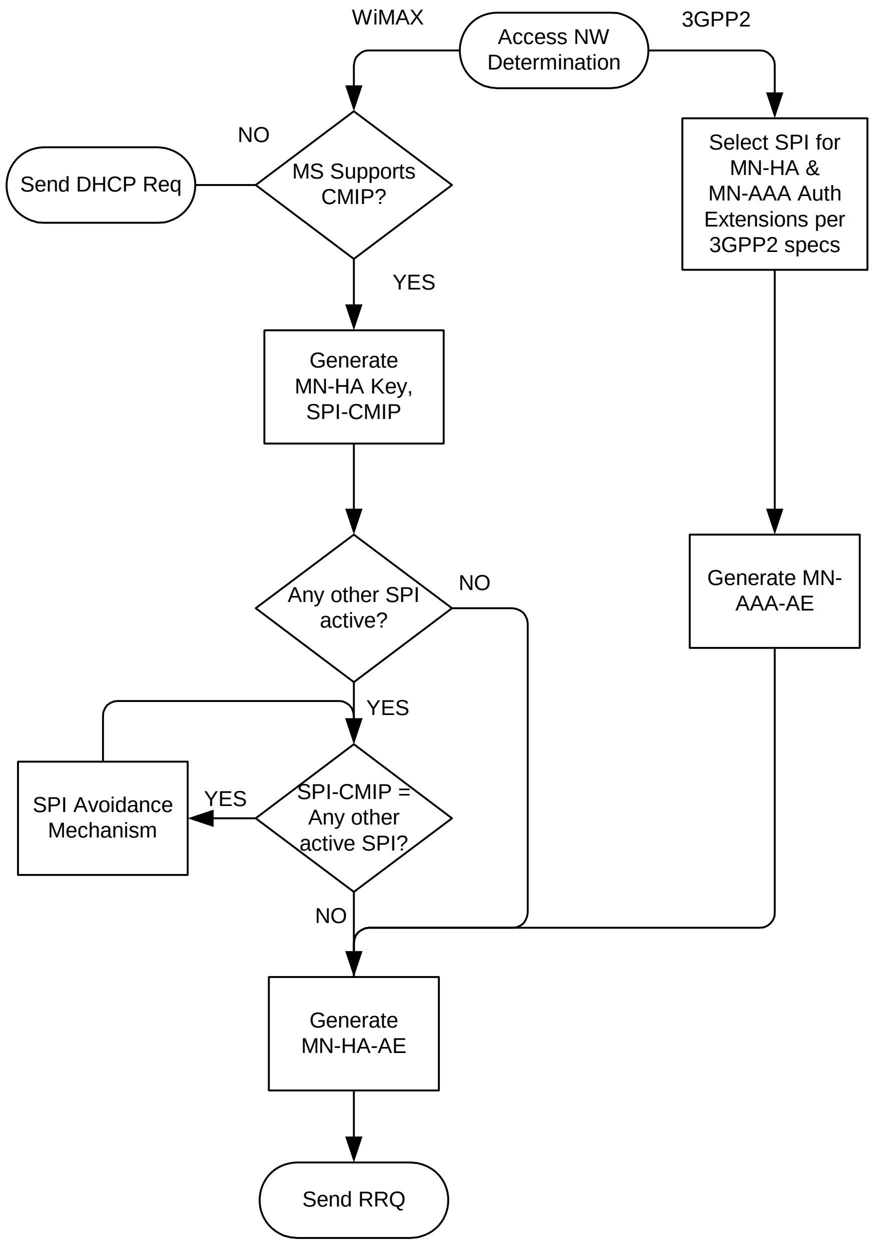

Figure 2 - MIP4 Registration by a Hybrid WiMAX – 3GPP2 MIP Client

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

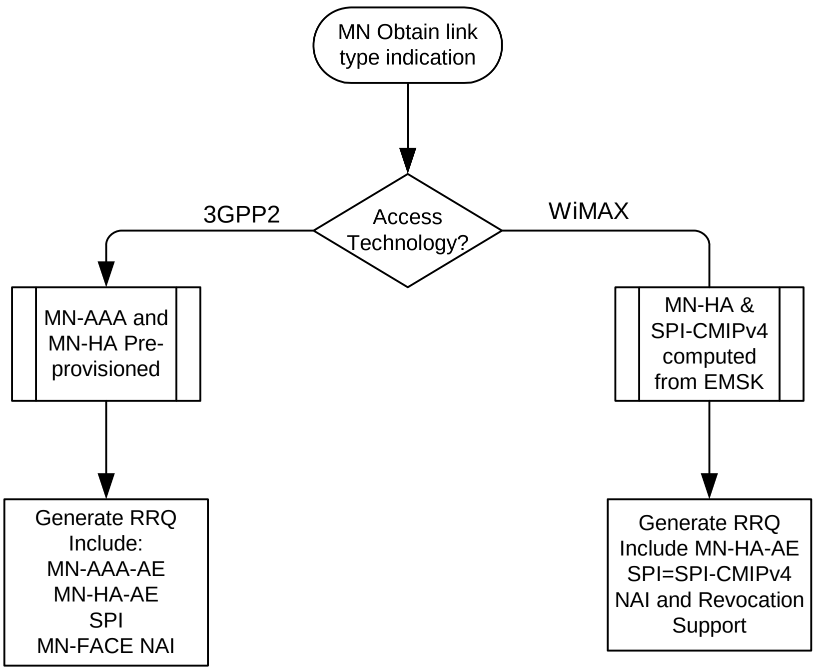

Figure 3 - Key Computation and RRQ generation by Hybrid 3GPP2 – WiMAX MIP Client

1.4.1.2 MIP Registration Process in the WiMAX Network

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

1) 3GPP2 PDSF/FA will receive the MIP_RReq that contains FA CHALLENGE extension and MN-AAA-AE. As specified in IS-835 [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-FACEThe 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. The HA requests the MN-HA key from the H-AAA to validate the included MN-HA-AE.

4) The H-AAA has to distinguish between IS-835 [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 PMN-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.

- 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.

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

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).

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

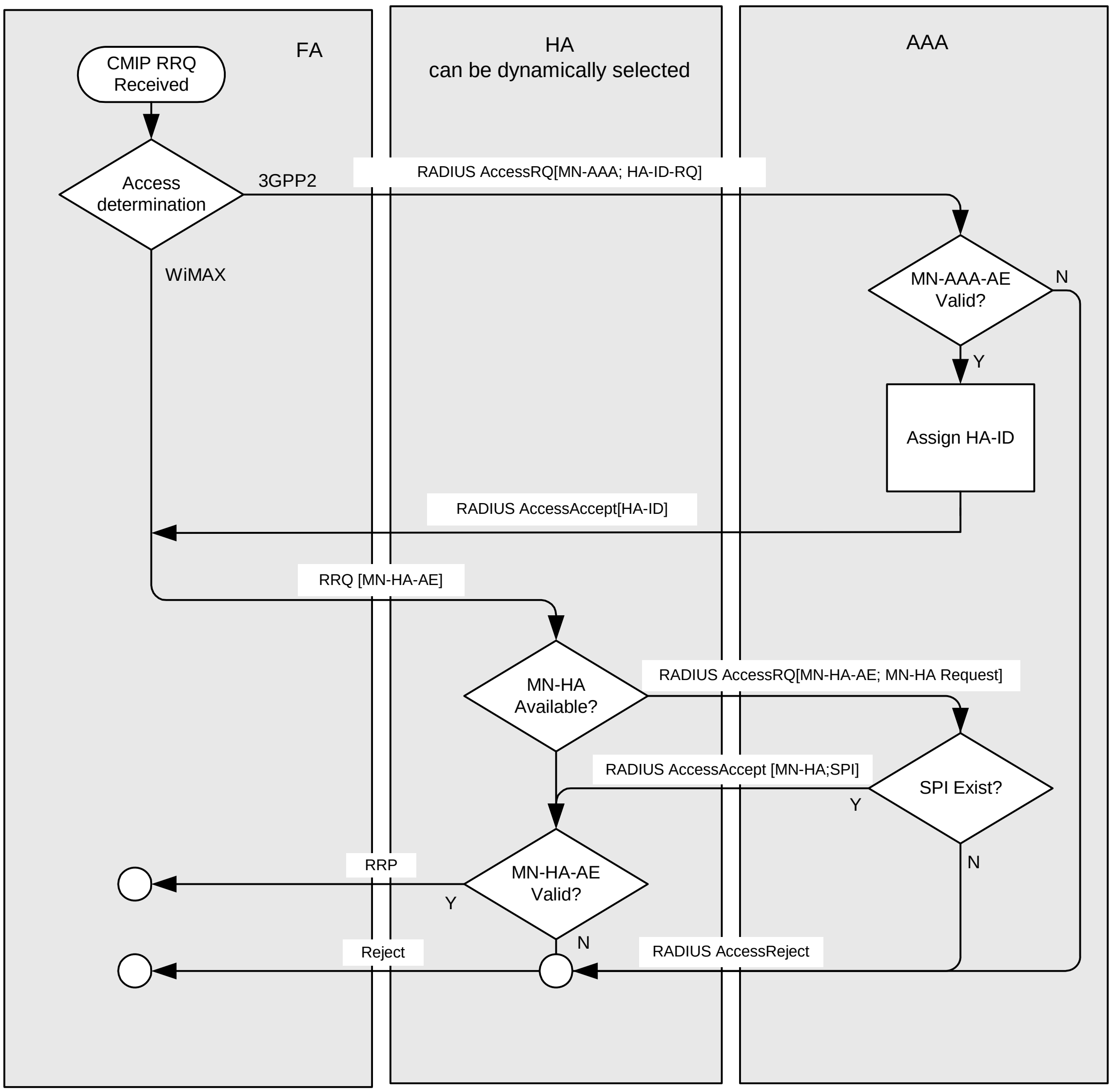

Figure 4 - MIP4 Associated Transactions, Network Perspective

1.4.1.3 MIP Call Flows - WiMAX Network Access

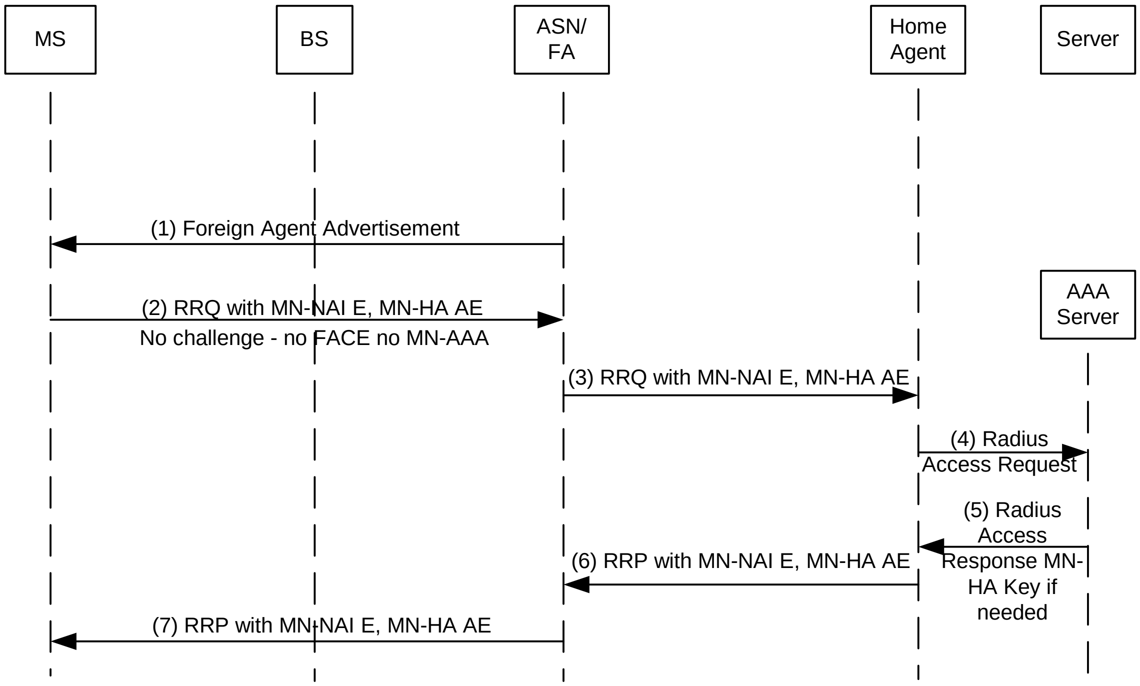

Figure 5 - WiMAX CMIP Call Flow

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) HA sends RADIUS Access Request to the AAA Server to validate the MN-HA.

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.

1.4.1.4 MIP Call Flows – 3GPP2 Network Access

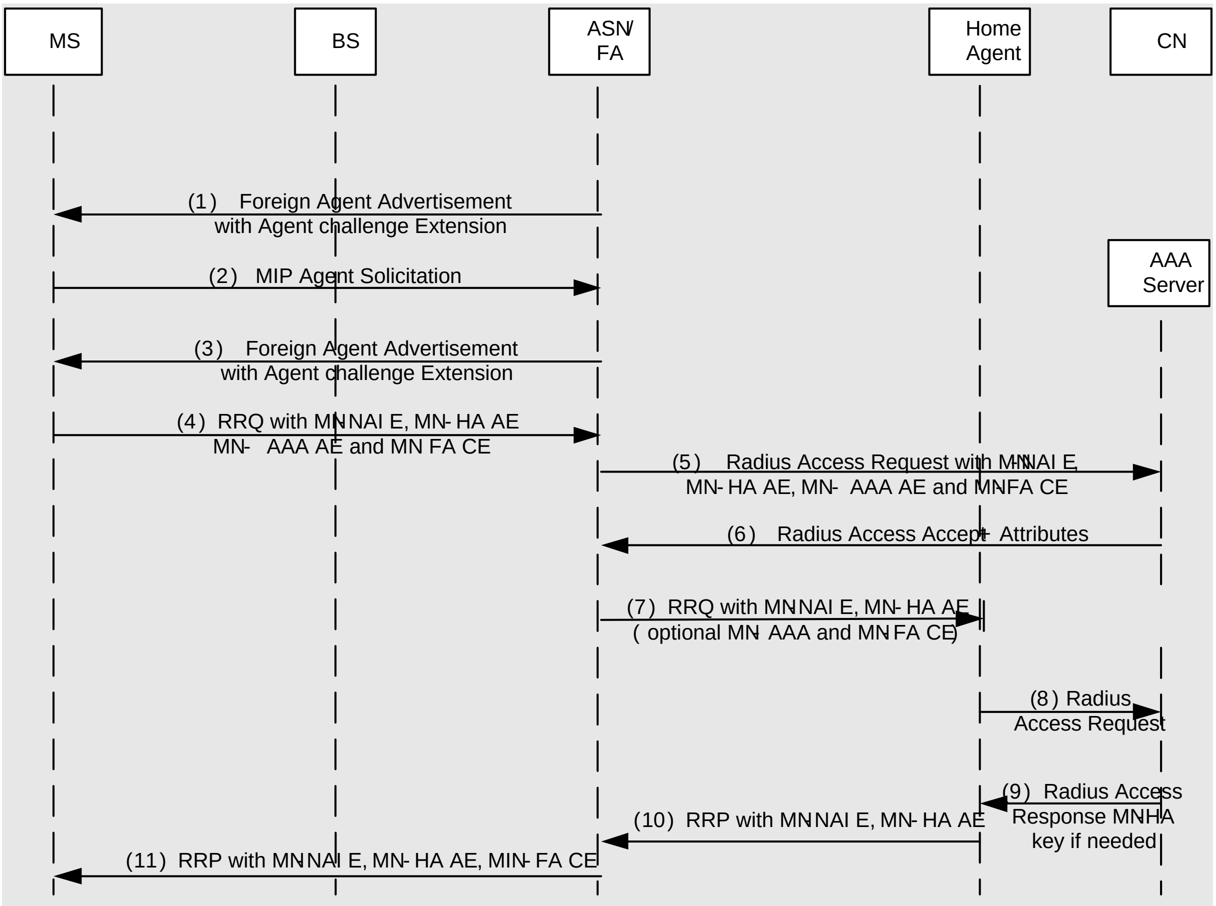

Figure 6 - CDMA CMIP Call Flow

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 the 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) 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.

1.5 Client MIP Requirements

As depicted in Figure 7-66 Stage 2 Section 7.8.1.9, 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, 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 MS MAY use RFC 3012 procedures for WiMAX access as well. 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 (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[2].

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.

---

[2] 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).

Support for the MN-FA Challenge Extension as specified in [28] is optional for WiMAX but mandated for cdma2000™.

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 not in the scope of Release 1.0.0.

1.6 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 5.8.2.1.1 and 5.8.2.2.3 and the ones for 3GPP2 are listed in IS-835D [1].

1.7 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