WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[3GPP – WiMAX Interworking]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

Copyright © 2005-2007 WiMAX Forum.   All Rights Reserved.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLES

1. Internetworking with 3GPP

1.1 Introduction and Scope

3GPP specifies how interworking with non-3GPP IP access networks (such as WiMAX ASNs) shall take place. Within the 3GPP Release 7 set of specifications, interworking with WLAN networks is specified in [TS23.234] and [T33.234] for security, where the following interworking scenarios are distinguished:

- Scenario 1 is the simplest case which impacts neither 3GPP nor the interworking network architecture. This just means a transparency for the subscriber in its relationship with his/her operator: the subscriber will be charged on the same bill for usage of both 3GPP and non-3GPP services, and custom care will be ensured without dependency on the connecting platform.

- In Scenario 2 (or Direct IP access), a subscriber MAY use the non-3GPP access network to access e.g. the Internet, but AAA operations are handled by the 3GPP platform.

- Scenario 3 (or 3GPP IP access) allows the operator to extend 3GPP system Packet Switched (PS) based services to the non-3GPP network. In this scenario, an authenticated 3GPP subscriber can access to 3GPP PS services through a non-3GPP access network interworking with its 3GPP PLMN (non roaming case) or with a visited 3GPP PLMN (roaming case).

Table 1 - WiMAX-3GPP Interworking Scenarios (Based on Table 3 of 3GPP TR 22.934)

	Scenarios		
Service and operational Capabilities:	**Scenario 1: Common Billing and Customer Care**	**Scenario 2: 3GPP system based Access Control and Charging**	**Scenario 3: Access to 3GPP system PS based services**
Common Billing	X	X	X
Common Customer Care	X	X	X
3GPP System Based Access Control		X	X
3GPP System Based Access Charging		X	X
Access to 3GPP System PS Based Services from WiMAX			X

In this document *WiMAX-3GPP interworking* is specified based on the I-WLAN architecture described in [TS23.234] and [T33.234] by 3GPP. The solution covers both Direct IP access ("scenario 2") and 3GPP IP access ("scenario 3"), denoted *WiMAX Direct IP access* and *WiMAX 3GPP IP access* in the context of this specification.

This solution does not modify [TS23.234] and [TS33.234] in any way, but builds on top of it by providing missing interworking functionality from the WiMAX perspective, within the WiMAX CSN. The motivation for this is to make available an interworking solution in the time frame of the WiMAX NWG Release 1 architecture as well as the 3GPP Release 7 timeframe that is focused on scenarios 2 and 3.

1 It is, however, understood that for future releases, a more advanced and integrated interworking solution between
2 WiMAX networks and 3GPP networks is under development as part of the 3GPP SAE (system architecture
3 evolution) effort. The interworking solution specified in this document does not limit such future architectures.

4 Additional considerations for IPv6 related to scenario-3 interworking are out-of-scope for this release of the
5 document.

6 ## 1.2 Control Plane Protocols and Procedures

7 This section provides the detailed description of WiMAX-3GPP interworking

8 ### 1.2.1 WiMAX specifics in direct and 3GPP IP access

9   Due to a number of features that are specific to the WiMAX NWG architecture but are not available for WLAN
10 networks covered by the 3GPP I-WLAN specification, WiMAX-3GPP interworking requires a set of additional
11 functions to support these features, for enabling standard operation within the WiMAX part of the interworking
12 architecture.

13 WiMAX networks as specified by [NWG Stage-3] allow access to IP services for users subscribed to a WiMAX
14 CSN operator. For gaining access to WiMAX network resources, the user's MS has to perform an initial network
15 entry procedure as specified in [NWG Stage-3, section 5.5]. During initial network entry, the following major steps
16 need to be performed:

17 • Network discovery and selection

18 • User/Device Authentication

19 • QoS and Service Flow establishment

20 • Mobile IP registration and tunnel establishment

21 This document details how these steps shall be performed for the WiMAX-3GPP interworking case.

22 For access to WiMAX networks, security for the 802.16-2005 wireless link needs to be established. Hence, for
23 WiMAX 3GPP IP access, WiMAX Direct IP access shall be performed first to establish appropriate key material in
24 the ASN Authenticator for initiating protection of the R1 wireless link (PKMv2). This is required to allow access to
25 the WiMAX ASN/CSN resources and initiate the final establishment of the secure Wu tunnel for WiMAX-3GPP IP
26 access (according to [TS23.234] I-WLAN 3GPP IP access).

1   ## 1.2.2   Detailed Solution
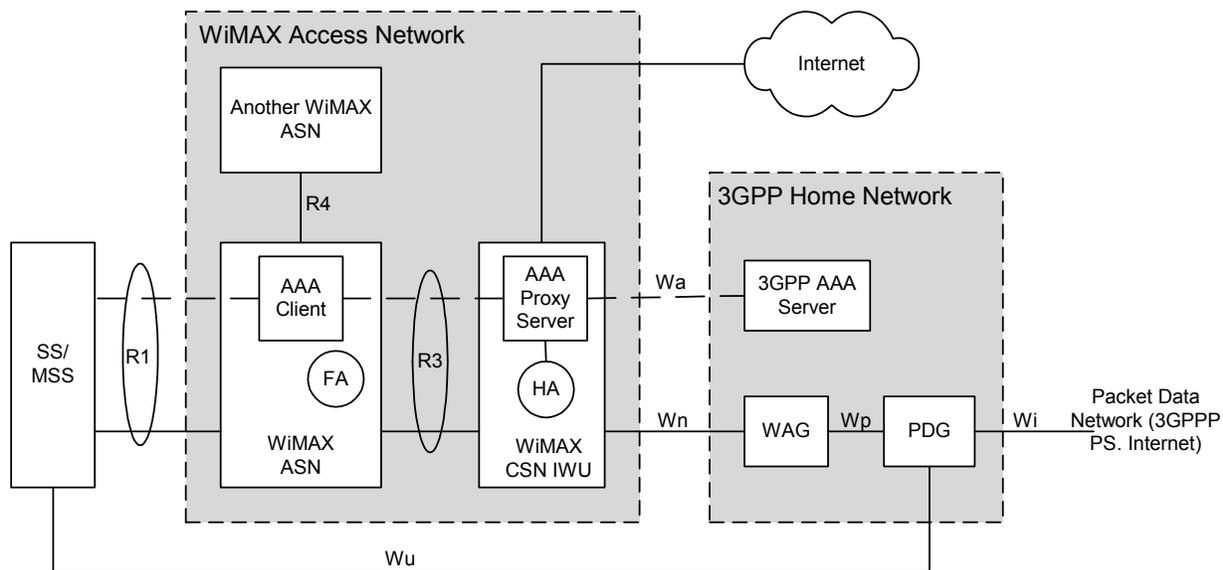
2

3   **Figure 1- WiMAX-3GPP Interworking (Non-Roaming Case)**

4   Figure 1 represents the WiMAX-3GPP Interworking architecture and the appropriate Reference Points.

5   Unless otherwise mentioned, all the content of [TS23.234] and [T33.234] shall be applied to the WiMAX
6   Interworking case. This includes the specification of the Wa, Wn and Wu inter-technology interfaces.

7   The WiMAX ASN and CSN networks provide standard WiMAX functionality as specified in [NWG stage-3].
8   Accordingly, Internet connectivity, Mobile IP and IP address management are provided by the WiMAX CSN
9   (except those aspects covered by the Wu tunnel for WiMAX-3GPP IP access).

10   Based on this, the following sections specify functionality required in the WiMAX ASN and CSN to support
11   interworking with 3GPP networks for roaming 3GPP subscribers using a WiMAX MS or WiMAX-enabled 3GPP
12   UE (which is for brevity also denoted a MS in this specification).

13   ### 1.2.2.1   General Requirements to the WiMAX Network

14   The WiMAX ASN supporting WiMAX-3GPP interworking shall support PMIP operation for any WiMAX-3GPP
15   interworking MS in compliance with [NWG stage-3], section 5.8.

16   The WiMAX CSN shall provide an interworking AAA proxy/server that is in the path of the AAA signaling
17   between the Authenticator of the ASN and the 3GPP AAA server responsible for user authentication in the 3GPP
18   home network (Wa interface to the 3GPP core network). It is responsible for:

19   •   Generating PMIP keys

20   •   Distributing these keys to the involved entities of the WiMAX network (HA and PMIP client).

21   •   Handling the RADIUS attributes that are WiMAX-specific or needed for Mobile IP

22   ### 1.2.2.2   Network Discovery and Selection

23   Once the MS has detected the available ASNs and corresponding CSN that provides WiMAX-3GPP interworking
24   support in a given area by the means of methods described in [NWG stage-3], the selection of the 3GPP PLMN shall
25   be done accordingly to TS 23.234.

26   ### 1.2.2.3   User/Device Authentication

27   For WiMAX-3GPP interworking, the WiMAX user authentication shall be based on EAP-SIM or EAP-AKA.
28   Device authentication is not supported by 3GPP AAA servers. If device and user authentication (double EAP) is
29   performed, the device authentication is performed within the WiMAX network. A 3GPP AAA server does not

1 support the WiMAX-specific authentication mode of combined device/user authentication (using single-EAP) or
2 device-only authentication, so these authentication modes are not supported with 3GPP interworking.

3 Hence, the MS shall not run a combined device/user authentication using single-EAP (AuthMode {4}). The AAA
4 proxy may reject an unsupported authentication mode by checking the provided NAI that encodes the authentication
5 mode as decoration .

6 **User-only Authentication:**

7 A single EAP authentication run takes place between MS and the 3GPP AAA server, with the CSN interworking
8 AAA proxy/server in the path. If the authentication is successful (EAP-Success), the interworking AAA
9 proxy/server forwards the resulting MSK key to the AAA client in compliance with the common WiMAX and 3GPP
10 procedures.

11 A number of AAA attributes used within the WiMAX AAA architecture are WiMAX defined VSAs not known to,
12 or provided by, the 3GPP AAA server.

13 For this, the following RADIUS WiMAX VSAs are added by the interworking AAA proxy/server to support
14 standard WiMAX operation in the path of user authentication, to the RADIUS Access-Accept message that is sent
15 by the 3GPP AAA server to the Authenticator after successful user authentication:

16 • WiMAX-Capability (type 26/1)

17 • Framed-IP Adress (HoA)

18 • AAA-Session ID (type 26/4)

19 • MSK (type 26/5), carries the MSK received from the 3GPP AAA server

20 • RADIUS VSAs between ASN and HAAA for bootstrapping mobility service as specified in [NWG-stage-3]
21   table [tbd].

22 • RADIUS attributes between ASN and HAAA for DHCP relay as specified in [NWG-stage-3] table [tbd] in case
23   DHCP relay is supported.

24 • For Mobile IP, the interworking AAA proxy/server adds the RADIUS attributes and values that are required for
25   WiMAX operation of Mobile IP but that are not supported by the 3GPP AAA server. It shall add this HA
26   address in the same way as a WiMAX AAA server would do.

27 The keys for MIP are added. They are derived from MIP-RK' using the derivation defined in section 5.3.5. MIP-
28 RK' is created by the interworking AAA proxy/server. It is internal to the interworking AAA proxy/server how to
29 create MIP-RK'. This can be a random number (MIP-RK' = RAND). RAND shall be a random number created for
30 each user authentication by a cryptographically strong random number generator. The interworking AAA
31 proxy/server also generates HA-RK according to the rules given in section 5.3.5 of [NWG-stage-3].

32 The interworking AAA proxy/server acts as AAA proxy during the network access authentication. Once receiving
33 the EAP-Success message from the 3GPP AAA server, it stores the NAI of the authenticating user (marked as
34 authenticated) and creates and stores the associated MIP-RK' and HA-RK keys for this session (used later for
35 bootstrapping the Mobile IP HA).

36 **Device and User Authentication (Double EAP):**

37 Device authentication may be performed in advance to user authentication, if user authentication terminates in the
38 3GPP AAA server. If device authentication is performed during WiMAX-3GPP interworking, it must terminate in
39 the WiMAX network (ASN or CSN). Subsequent user authentication is performed as described above.

40 **NAI Considerations:**

41 3GPP 33.234 requires that the (outer) NAI used for EAP-SIM/AKA contains either a pseudonym allocated to the
42 WLAN-UE in previous authentication or, in the case of first authentication, the IMSI, if user identity privacy is
43 used. The NAI construction as specified for [RFC4186] and [RFC4187] with the additional considerations given in
44 [TS33.234] shall be used, with the following exception:

- The Authentication Mode preceding the user part of the WiMAX NAI shall be added by the MS for WiMAX-3GPP interworking.

The WiMAX-3GPP interworking AAA proxy shall remove the WiMAX authentication mode from the NAI when forwarding AAA messages to the 3GPP AAA server, and shall add the same value for AAA messages sent back to the AAA client.

1.2.2.4   Mobile IP registration support

The Mobile IP keys are created by the interworking AAA proxy/server in the CSN. These keys are distributed to the involved entities of the WiMAX network (i.e., HA and Authenticator). Distribution of these key happens in compliance with the mechanisms specified in section 5.3.5 of [NWG-stage-3], where the interworking AAA proxy/server (instead of the 3GPP AAA server that is not assumed to be WiMAX MIP-aware) interfaces with the HA in the CSN, and adds the PMIP keys to the RADIUS Access-Accept message of the 3GPP AAA server during user authentication, such that the Authenticator in the ASN receives the keys required for PMIP operation for this specific MS.

The interworking AAA proxy/server acts as AAA proxy during the network access authentication. When it receives the EAP-Success message from the 3GPP AAA server, it shall store the NAI of the authenticating user (marked as authenticated) and create and store the MIP-RK' and HA-RK keys for this session. MIP-RK' is generated as described in section 1.2.2.3 above. This generation of MIP-RK' is specific to WiMAX-3GPP interworking: The 3GPP AAA server does not provide MIP keys, and it does not export the EMSK key that would be needed for regular MIP-RK derivation as described in section 5.3.1 of [NWG Stage-3]. As the MIP_RK' generation is internal to the WiMAX network it can only be used for PMIP. A 3GPP interworking MS shall not use CMIP.

When the Interworking PMIP client sends the MIP-RRQ message to the assigned HA, the HA requests the MIP keys from the interworking AAA proxy/server as described in [NWG-stage-3]. The interworking AAA proxy/server checks stored NAIs and returns the associated MIP keys when a matching entry for the NAI is available. These keys are derived from MIP-RK' that was generated and stored during the preceded network access authentication for the same NAI.

The key derivation of MIP keys from MIP-RK' is done as defined in section 5.3.5 of [NWG Stage-3]. The AAA proxy shall return an Access-Reject if no corresponding user session state (containing NAI and corresponding MIP-RK') can be found.

1.2.2.5   Detailed Requirements to the MS

The MS shall not register with CMIP when using a subscription with a 3GPP operator for network access. If the WiMAX CSN receives a CMIP registration attempt by a 3GPP subscriber using WiMAX direct IP access, this registration attempt will fail due to wrong CMIP keys.

When using a 3GPP subscription for user authentication, the MS shall use EAP-SIM or EAP-AKA as EAP method.

For the outer NAI that is used in the EAP identity exchange, the NAI shall be constructed as specified in [TS23.234] for 3GPP-WLAN interworking, with the following exception: The authentication mode indication preceding the user part of the WiMAX authentication method "{n}" should be added by the MS for WiMAX-3GPP interworking.

The MS shall not run a combined device/user authentication using single-EAP (AuthMode {4}). This is due to the fact that a 3GPP AAA server cannot be assumed to support this WiMAX-specific Authentication Mode. If a terminal attempts to authenticate using this specific authentication mode, the interworking AAA proxy/server will respond with an error message, and the MS will not be able to gain access to the WiMAX network.

It is, however, possible to perform device authentication in addition to user authentication for a roaming 3GPP user, if device authentication terminates in the WiMAX network (ASN or CSN).

1.2.3   Limitations of this specification

- WiMAX-3GPP IP access based on the Wu Reference point IPsec tunnel might not allow the WiMAX terminal to enter the idle mode for power consumption saving due to the maintenance of the IPsec connection in an active state. Further development with 3GPP SA2 is required to enable idle terminals.

- WiMAX provides powerful and flexible QoS handling which is transparent to Direct IP access but can't be fully utilized within WiMAX-3GPP IP access. 3GPP SA2 is currently extending the specification for utilizing QoS-enabled IP-based access networks.

- Handoff capability from 3GPP network to WiMAX network is usually referred as scenario 4 (intersystem mobility) and 5 (seamless intersystem mobility). These scenarios are out of scope of release 1, but they will be addressed in future releases.

- CMIP operation, due to the fact that:

  - a 3GPP AAA server cannot be assumed to derive WiMAX-specific mobility keys from the EMSK, and

  - the (visited) WiMAX network and roaming 3GPP subscribers cannot be assumed to have pre-shared mobility keys,

  is not supported by this WiMAX release.

1.3   Reference Point Mapping and Security

1.3.1   Reference Points Linking the WiMAX Access Network to the 3GPP System

This section lists the relevant 3GPP reference points as specified by [TS23.234], and provides their mapping to WiMAX-3GPP interworking.

- Wa is the reference point transporting all AAA messages between the interconnected WiMAX and 3GPP networks. At the WiMAX side, it is terminated by a AAA proxy/server. At the 3GPP side, it is terminated by either the 3GPP AAA server, or an optional AAA proxy/server in the 3GPP network that is interconnected with the 3GPP AAA server. In cases where the WiMAX and 3GPP AAA infrastructure speak different AAA protocols, RADIUS/Diameter translation needs to be done at one side of the Wa interface. For co-existence of RADIUS and Diameter, the considerations given in [TS33.234], annex A.3.2 apply.

- Wn links the WiMAX Access network and the WAG (WLAN Access Gateway). The WAG is a gateway toward which the data coming from the WiMAX Access Network SHALL be routed. It is used to enforce the routing of packets through the appropriate PDG. WAG functionalities are described in details in [TS23.234].

- Wu refers to tunnel establishment and tear down between MS and the appropriate PDG (Packet Data Gateway), as well as user data packet transmission through this tunnel. PDG functionalities are described in details in [23.234]. The 3GPP technical solution for 3GPP IP access in [TS23.234] shall apply.

- Ww: connects the MS to the WiMAX Access Network; this reference point maps to the WiMAX NWG R1 reference point.

1.3.2   Reference Point Security

For reference point security of affected WiMAX network reference points, the recommendations and profiles given in [NWG stage-2], section [tbd] and [NWG stage-3], section [tbd] apply as specified. For securing reference points between the WiMAX network and the 3GPP networks, the following considerations shall apply:

- Wa: Interface between AAA proxy/server in the WiMAX CSN and 3GPP AAA server responsible for interworking.
  If the interface is based on RADIUS, protection is achieved by means of RADIUS standard procedures. In particular, the attribute MS-MPPE-Recv-Key [RFC 2548] provides protection of the MSK key derived in the 3GPP AAA server. If the interface is based on Diameter (i.e., a RADIUS/Diameter translation gateway is at the WiMAX side of the reference point), IPsec shall be used if there is no physical protection for this reference point (the support of IPsec for Diameter is mandatory as stated in [RFC3588]).

- Wn: It shall be possible to protect the integrity and confidentiality of IP packets sent through a tunnel between the WiMAX side and the 3GPP side of this reference point.

- Wu: The technical solution chosen by 3GPP for WLAN 3GPP IP access security [TS33.234] shall apply. With this, all data transferred through this tunnel is secured by IPsec.

1   •   Ww: wireless MAC layer security is provided in compliance with [NWG-stage3] and [802.16-2005] through
2   PKMv2. Device and user authentication are based on EAP methods. For WiMAX-3GPP interworking, EAP-
3   SIM or EAP-AKA shall be used as EAP methods.

4

5