WiMAX FORUM® ROAMING GUIDELINES

based on WiMAX Forum Certified™ Products

Release 1.0 Version 2

DRAFT-T40-001-R010v02-A
WiMAX Forum Approved
(2009-06-24)

WiMAX Forum Proprietary

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

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

The purpose of this document is to provide guidelines, technical information, and recommendations on deployment of WiMAX™ networks to enable WiMAX™ roaming. These roaming guidelines provide an overview of WiMAX roaming for the benefit of potential and existing WiMAX™ operators, infrastructure and equipment developers and WiMAX™ Roaming eXchange Providers (WRX).

This document provides a description of the roaming architecture, process and functions, and an overview of a technical solution for roaming service between WiMAX™ Network Service Providers (NSP).

The scope of this document is limited to roaming services based on best effort Internet Protocol (IP) connectivity. It assumes network functionality per WiMAX Forum® Network Working Group (NWG) Network Architecture [2] and [3].

1.1 Roaming

Roaming involves the use of wireless services in a different location to that of the Network Service Provider's (NSP) home network. Roaming occurs between two network service providers which operate networks located either in the same country or in different countries. Roaming enables service providers to extend services available to their subscribers beyond their home networks.

Roaming services refer, in the context of the present document, to the provision of best effort IP connectivity, in support of applications, such as, File Transfer Protocol (FTP), e-mail, instant messaging, web browsing, Virtual Private Networks (VPNs), Voice over IP (VoIP), streaming audio/video, gaming and other applications and services available through IP connectivity, all on a best effort basis. Roaming Guidelines Release 1.0 provides no deterministic Quality of Service (QoS) guarantees associated with roaming services, since the scope of QoS in the current release of WiMAX™ systems is limited to the radio access network only.

The WiMAX Forum Service Provider Working Group (SPWG) provides a general definition of roaming as follows: "A technical and business relationship between two different WiMAX™ operators (these are typically different Network Service Providers, but could involve different Network Access Providers (NAPs)) that enables the WiMAX™ subscribers of the first network (home network) to connect and receive services in the second (visited or serving network) network." See "Recommendations and Requirements for Networks based on WiMAX Forum Certified™ Products, Release 1.0" [1] for additional information.

1.2 The Roaming Process

There are two distinct phases to the roaming process: pre-commercial and commercial.

1.2.1 Pre-Commercial

The pre-commercial phase begins with two or more parties considering and then agreeing to roam with each other.

This phase includes the documentation and signing of a roaming agreement and the configuration of systems to enable roaming. The pre-commercial phase concludes with system testing amongst all parties involved in the Roaming Agreement [8]. System testing includes testing of network discovery and selection, control messaging, e.g. Authentication Authorization and Accounting (AAA), Mobile IP (MIP), bearer plane traffic for data, clearing and billing, and can include testing of devices and specific applications.

Roaming Guidelines can be used in the Pre-Commercial phase to verify if the networks and systems of the roaming partners are configured properly.

1.2.2 Commercial Phase

With all the pre-commercial phase activities completed, end users can roam on different networks to initiate data sessions knowing that their network usage will be identified and billed by their home NSP, irrespective of pre-paid or post-paid arrangements.

1.3 Unilateral, Bi-lateral and Multi-lateral Roaming

Roaming agreements can take one of three discrete forms: unilateral, bi-lateral or multi-lateral. Unilateral roaming occurs when subscribers of one NSP roam onto the network of a second NSP, without reciprocity. Bi-lateral roaming occurs when subscribers of two NSPs roam onto each other's networks. Multi-lateral roaming occurs when subscribers of more than two NSPs roam onto each other's networks and are typically linked by a hub operated by a third party or by one of the NSPs. Multi-lateral agreements can be used to provide the legal framework for services between more than two operators. This enables a NSP to link with a group of NSPs for roaming services through a single agreement.

1.4 The Roaming Functions

Once the network is enabled and tested for roaming, various functions within an NSP support the ongoing operations of roaming.

The roaming exchange function ensures the exchange of information between two NSPs and includes the extraction and validation of data on a daily basis to enable the processing and rating of roaming usage records and support fraud detection. The billing and financial settlement function includes preparing wholesale invoices and completing financial settlement between NSPs. Information generated by this function is also used by NSPs in the production of retail billing invoices for their subscribers who use roaming services.

The fraud prevention function includes using information extracted in the roaming exchange process to monitor potential fraud. Information is used to create high usage reports and as input for other tools to detect fraud.

2 Abbreviation/Acronyms, definition and conventions

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication Authorization and Accounting
AES	Advanced Encryption Standard See http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
AH	Authentication Header
ASN	Access Service Network
ASN-GW	Access Service Network – Gateway
ASP	Access Service Provider
BE	Best Effort
BS	Base Station
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining – Message Authentication Code
CMIP	Client Mobile IP
CoA	Care of Address
CSN	Connectivity Service Network
CUI	Chargeable Unit Identity
DES	Data Encryption Standard. See http://www.itl.nist.gov/fipspubs/fip46-2.htm.
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
GRE	Generic Routing Encapsulation
EAP	Extensible Authentication Protocol
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled Transport Layer Security
EAP-AKA	EAP - Authentication and Key Agreement
ERT-VR	Extended Real Time - Variable Rate
ESP	Encapsulating Security Payload
ETWG	Evolutionary Technology Working Group
FA	Foreign Agent
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GHz	Giga Hertz
GMT	Greenwich Mean Time
GRWG	Global Roaming Working Group
GSM	Global System for Mobile communications
HA	Home Agent
H-AAA	Home – Authentication Authorization and Accounting
H-ASN	Home - Access Service Network
H-CSN	Home - Connectivity Service Node

HMAC	(keyed) Hash Message Authentication Code See http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
H-NSP	Home Network Service Provider
IEEE 802.16	Institute of Electrical and Electronics Engineers Working Group on Broadband Wireless Access Standards
IKE	Internet Key Exchange
IKEv1	Internet Key Exchange version 1
IKEv2	Internet Key Exchange version 2
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CS	IP - Convergence Sublayer
IPoETH-CS	IP over Ethernet - Convergence Sublayer
ISF	Initial Service flow
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MAC	Medium Access Control
MCC	Mobile Country Code
MHz	Mega Hertz
MIP	Mobile IP
MNC	Mobile Network Code
MS	Mobile Station
MS-Cert	Mobile Station Certificate
MTU	Maximum Transmission Unit
ND&S	Network Discovery & Selection
NAI	Network Access Identifier
NAP	Network Access Provider
NRT-VR	Near Real-Time – Variable Rate
NAS	Network Access Server
NSP	Network Service Provider
NWG	Network Working Group
NWIOT	Network Interoperability Task Group
OID	Operator ID
OFDMA	Orthogonal Frequency Division Multiplexing Access
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PMIP	Proxy Mobile IP
PoA	Point of Attachment
PF	Policy Function
PHY	Physical
PKMv2	Privacy Key Management protocol Version 2
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RFC	Request For Comments

RRQ	Registration Request message
RT-VR	Real-Time – Variable Rate
SA	Security Association
SA-TEK	Security Association – Traffic Encryption Key
SBC-REQ	SS Basic Capability Request
SBC-RSP	SS Basic Capability Response
SFA	Service Flow Authorization
SFM	Service Flow Management
SHA	Secure Hash Algorithm
SII-ADV	Service Identity Information Advertisement
SIM	Subscriber Identity Module
SPWG	Service Provider Working Group
SS	Subscriber Station
SSL	Secure Socket Layer
SUBC	Subsciber Root Key
TDD	Time Division Duplex
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
TWG	Technical Working Group
UDR	User Data Record
UGS	Unsolicited Grant Service
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UTC	Universal Coordinated Time
V-AAA	Visited - Authentication Authorization and Accounting
V-ASN	Visited - Access Service Node
V-CSN	Visited – Connectivity Service Node
V-NSP	Visited - Network Service Provider
VoIP	Voice over IP
VPN	Virtual Private Network
VSA	Vendor Specific Atrributes
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WRA	WiMAX Roaming Agremeent
WRI	WiMAX Roaming Interface
WRX	WiMAX Roaming eXchange Provider
X.509	ITU-T standard for public key infrastructure
XCBC	Version of Cipher Block Chaining to handle variable length messages See http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/xcbc-mac/xcbc-mac-spec.pdf
XML	Extensible Markup Language

3 References

3.1 WiMAX Forum® References

[1] WMF-T31-001-R010 WiMAX Forum® "Recommendations and Requirements for Networks based on WiMAX Forum Certified™ Products Release 1.0".

[2] WMF-T32-001-R010v04 WiMAX Forum® "WiMAX Forum® Network Architecture Stage 2 Release 1.0 Version 4".

[3] WMF-T33-001-R010v04 WiMAX Forum® "WiMAX Forum® Network Architecture Stage 3 Release 1.0 Version 4".

[4] WMF-T42-001-R010 WiMAX Forum® WiMAX™ Roaming Interface Code Release 1.0.

[5] WMF-T42-001-R010 WiMAX Forum® WiMAX™ Roaming Interface Stage 2 Release 1.0.

[6] WMF-T43-001-R010 WiMAX Forum® WiMAX™ Roaming Interface Stage 3 Release 1.0.

[7] WMF-T45-001-R010 WiMAX Forum® Pre-Commercial Roaming Testing Release 1.0.

[8] WMF-T48-001-R010 WiMAX Forum® "WiMAX™ Roaming Agreement 1 (WRA1)" and WMF-T48-002-R010 "WiMAX™ Roaming Agreement 2 (WRA2)".

3.2 IETF References

3.2.1 RFCs

[9] IETF RFC 2865 "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson, June 2000.

[10] IETF RFC 2869 "RADIUS Extensions", C.Rigney, W. Willats, P. Calhoun, June 2000.

[11] IETF RFC 4109 "Algorithms for Internet Key Exchange version 1 (IKEv1)", P. Hoffman, May 2005.

[12] IETF RFC 4282 "Network Access Identifier", B. Aboba, M. Beadles, J. Arkko, P. Eronen, December 2005.

[13] IETF RFC 4372 "Chargeable User Identifier", F. Adrangi, A. Lior, J. Korhonen, J. Loughney, January 2006.

[14] IETF RFC 4835 "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", V. Manral, April 2007.

3.3 3GPP References

[15] 3GPP TS 33.210 v8.0.0 (2008-03) "IP Network Layer Security (Release 8)"

4 Inter WiMAX™ Roaming – Reference Architecture

4.1 Network Reference Model

The WiMAX Forum Network Reference Model for roaming is shown below in Figure 1. Inter WiMAX roaming is achieved by using the reference points defined in [2] and particularly reference points R5 and R3, which consist of a set of protocols for interworking between the home NSP and the visited NSP. In particular:

- R3 is terminated between the visited Access Service Provider (ASP) (operated by the Network Access Provider, which can be the visited NSP itself or a different provider) and the home or the visited Connectivity Service Network (CSN); It consists of both control protocols to support Mobile Station (MS) mobility and bearer protocols to transfer user data between Visited ASN (V-ASN) and home or Visited CSN (V-CSN).
- R5 consists of only control protocols; R5 handles the Authentication, Authorization and Accounting procedures for roaming users and is terminated between the visited CSN and the Home CSN (H-CSN).

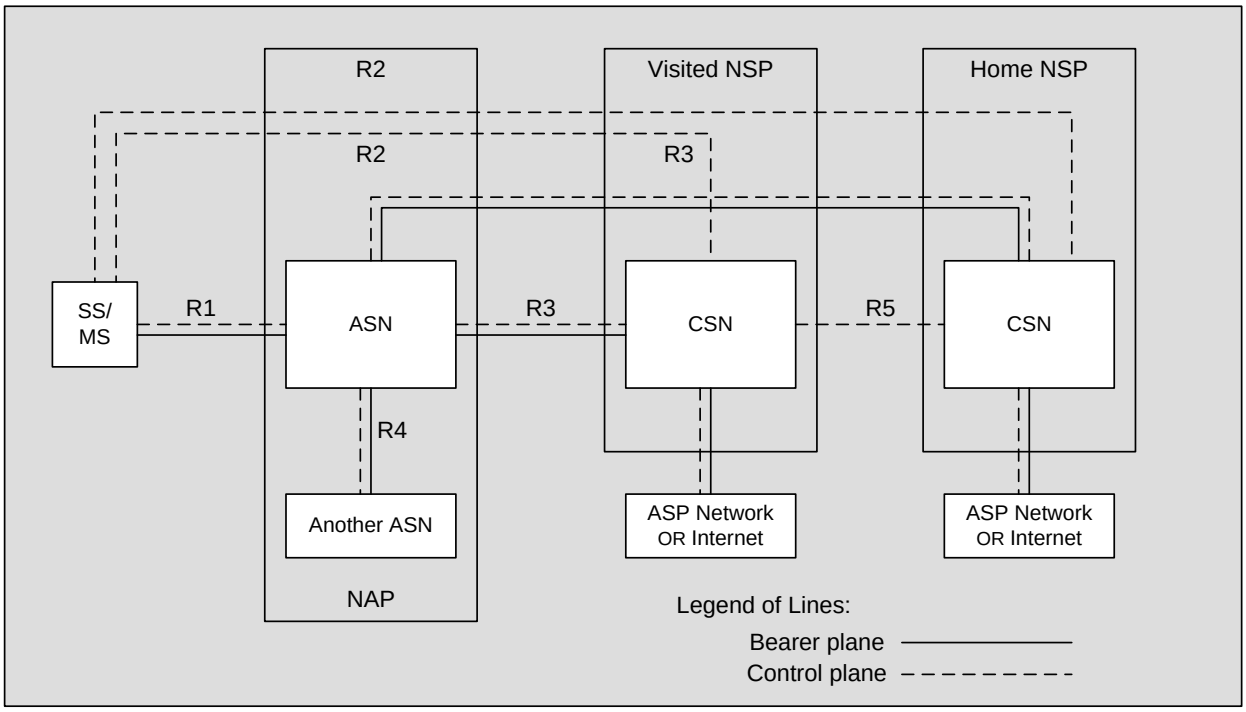

Figure 1 Network Reference Model

In the roaming case, the AAA traffic is transported only via R5.

4.2 Roaming Scenarios

In mobile WiMAX networks, the Home Agent (HA) is the anchor point for traffic of the MS, during its movement across different Base Stations (BSs) and different ASNs. From a roaming perspective, depending on where the Home Agent is allocated, WiMAX networks can support two roaming scenarios:

- MS connect via HA located in the visited network (V-CSN)
- MS connect via HA located in the home network (H-CSN)

If an HA is present in both V-CSN and H-CSN, the HA selection procedure as per [3] allows the selection of either the Home HA or the Visited HA.

4.2.1 Roaming with HA Located in the Visited NSP

Figure 2 shows the reference architecture for providing service to a roaming MS when the HA is located in the visited CSN. Authentication, authorization and policy information are provided from the home CSN to the visited CSN over the reference point R5. Accounting information is forwarded from the visited CSN to the home CSN over R5. Internet access is established through the visited CSN.

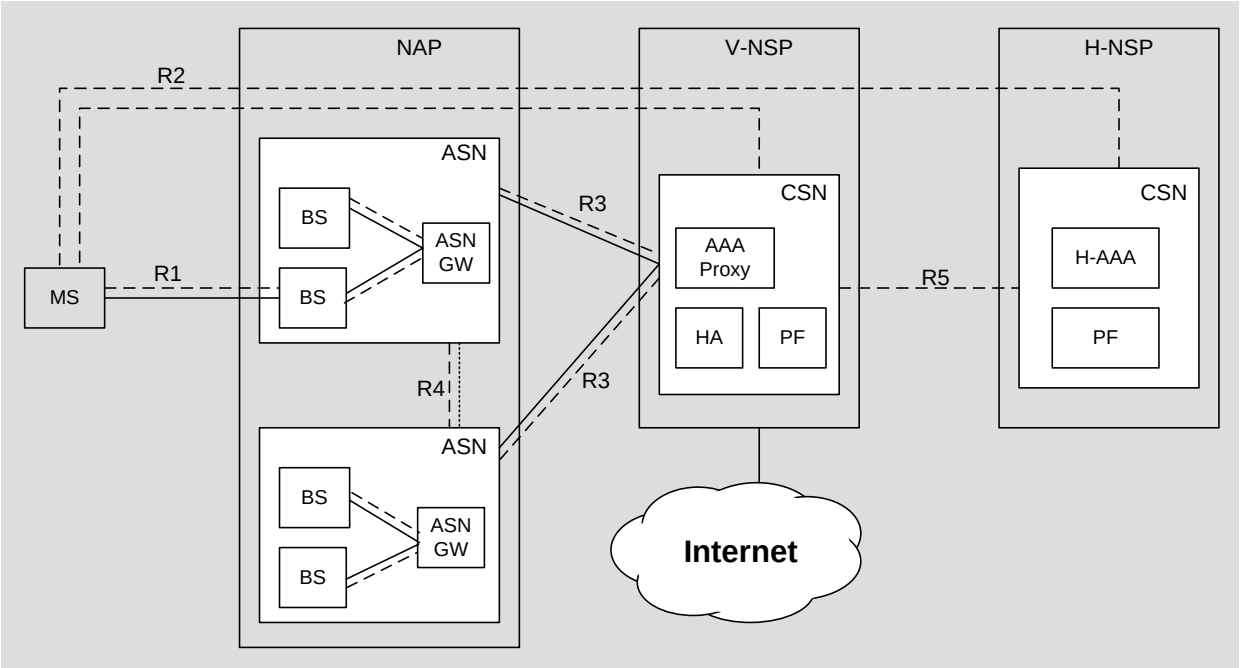

Figure 2 Network Reference Model with HA Located in the Visited NSP

Note: Solid lines represent the bearer plane and dashed lines represent the control plane. For a complete list of relevant acronyms used in Figure 2, see Section 2.

4.2.2 Roaming with HA Located in the Home NSP

Figure 3 shows the reference architecture for providing service to a roaming MS using the HA in the home CSN. In this case, the visited CSN becomes a proxy for R3. The home CSN is connected to the visited CSN over R5 reference point with Mobile IP passing through the visited CSN and terminating in the HA in the home CSN.

In this scenario, the traffic from MS is anchored at the HA in the home CSN and all services are accessed through the home CSN; Hence, Internet is accessed from the home NSP only.

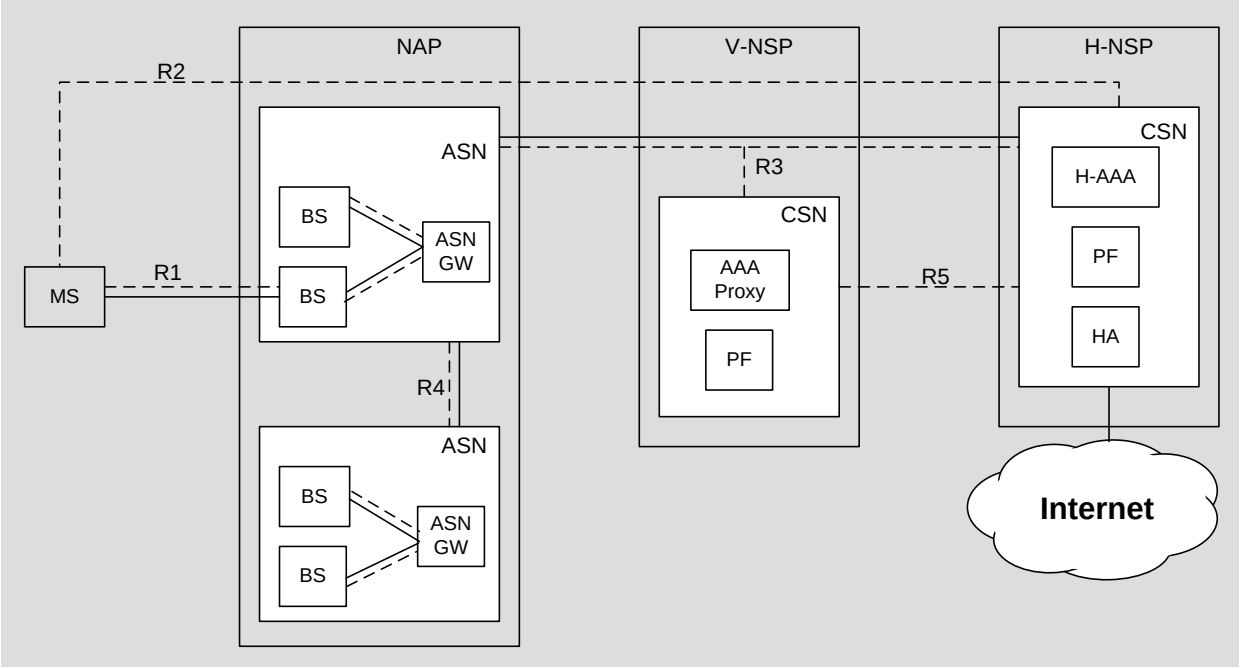

Figure 3 Network Reference Model with HA Located in the Home NSP

Note: Solid lines represent the bearer plane and dashed lines represent the control plane. Also, bearer traffic does not have to flow back through the Visited Network Service Provider (V-NSP) as shown in the diagram. As an alternative example, bearer traffic could be routed via the internet back to the Home Network Service Provider (H-NSP). For a complete list of relevant acronyms used in Figure 3, see Section 2.

4.3 Roaming Via 3rd Party Roaming Exchange

A third roaming model is one in which the V-NSP and H-NSP connect with each other via a 3rd party WiMAX Roaming eXchange Provider. Although this model is not explicitly described in [2] and [3], currently defined frameworks for AAA and mobility management are believed to accommodate it with no additional changes. In fact, the 3rd party WRX must only act as a proxy for control plane messaging or bearer traffic.

The connection via a 3rd party WRX can be used to support both bearer traffic and AAA traffic, only AAA traffic, or only bearer traffic. When a NSP is connected to a WRX, it can roam with multiple NSPs connected to the same WRX. It is also possible for a WRX to peer with other WRXs to increase the possibility of roaming with multiple NSPs via a single interface.

As shown in the following Figure 4, AAA traffic is transported over R5 and bearer traffic is transported over R3. R3 transports data traffic between the vASN which acts as a Foreign Agent (FA) and the Home Agent in H-NSP. If the HA is in V-NSP, R3 reference point is not required.

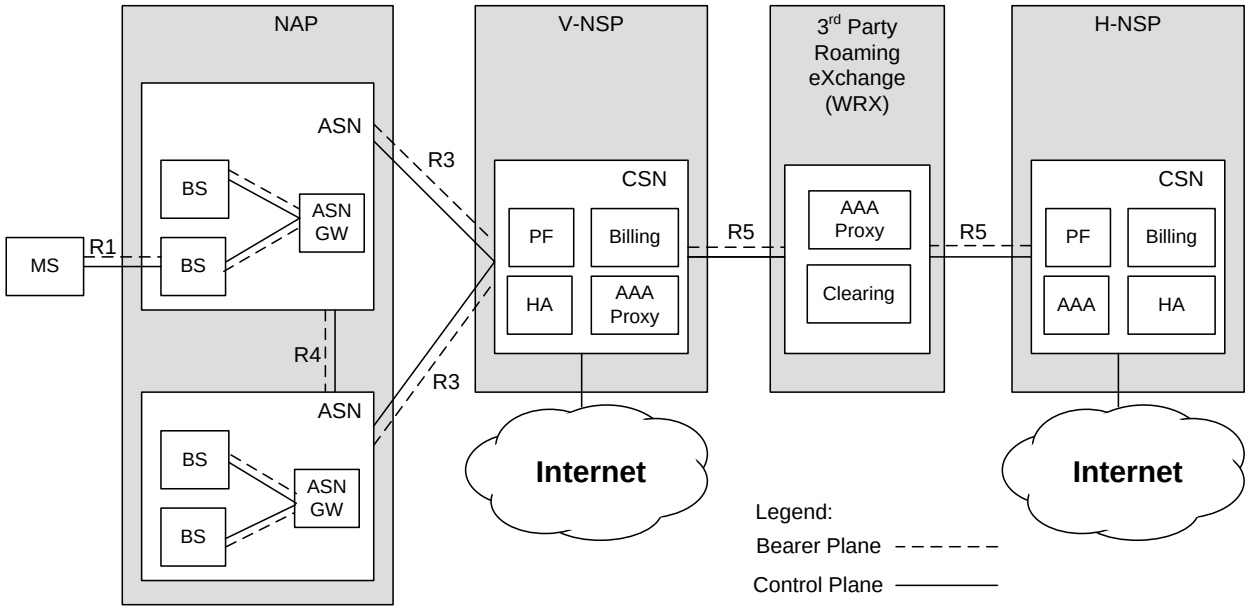

Figure 4 Network Reference Model with WRX

Access to Internet and Data Services is provided by V-NSP or H-NSP based on where the serving HA is located. If the serving HA is located in the V-NSP, the V-NSP will provide the access to Internet and Data Services. If the serving HA is located in the H-NSP, the H-NSP will provide the access to Internet and Data Services. For a complete list of relevant acronyms used in Figure 4, see Section 2.

4.4 Protocols

Figure 5 shows the generic protocol layering for the control and the bearer planes on R1, R3, R4 and R6 reference points, when the IP Convergence Sublayer (IP-CS) is used. As stated above, the HA can be located in home CSN or in the visited CSN. For a complete list of relevant acronyms, see Section 2.

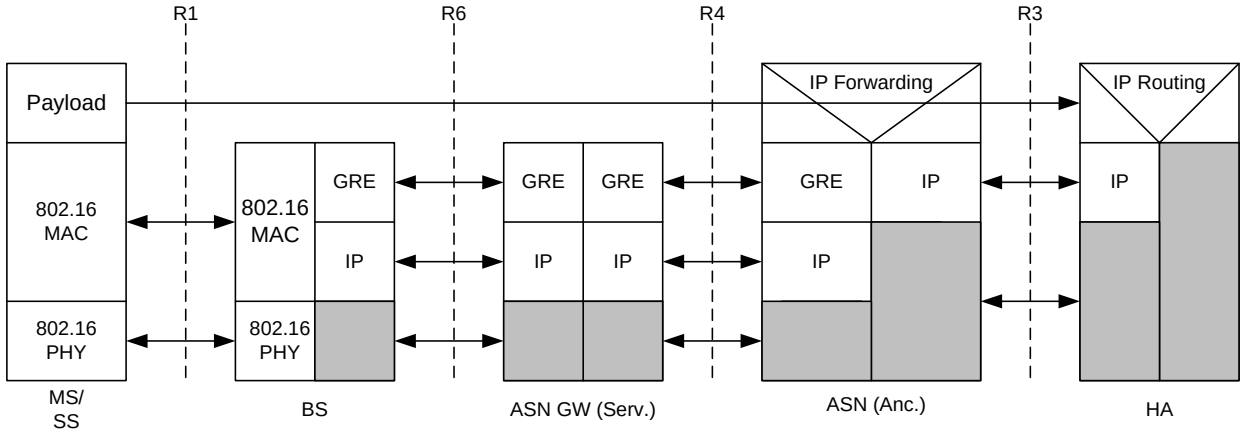

Figure 5 Protocol Layer Architecture (for IP-CS sub layer)

For other types of service e.g., for fixed/nomadic access scenarios, such as, access to Digital Subscriber Loop (DSL) infrastructure, IP over Ethernet Convergence Sublayer (IPoETH-CS) is used. Refer to [2] and [3] for the relevant protocol architecture.

4.5 WiMAX™ Roaming Connection – General Description

This section provides a brief overview of the WiMAX network procedures which will be detailed in subsequent sections of this document.

4.5.1 Network Discovery & Selection (ND&S) / Reselection

WiMAX NAP/NSP discovery refers to a process whereby an Mobile Station/Subscriber Station (MS/SS) discovers available NAP(s) and NSP(s) in its Radio Frequency (RF) range, using NAP and NSP identifiers, broadcasted by the visited network. In a roaming case, the MS/SS is allowed to select a network that can provide access to its home network services.

An MS/SS executes the network discovery procedures based on a stored NSP/NAP list, various preference criteria, or MS/SS configuration information. Moreover, a roaming user can perform the selection manually, taking into account other criteria, like preferred roaming agreements and tariff preferences.

4.5.2 Authentication

Subscription Authentication refers to a procedure used to verify the subscription right to access the WiMAX network. The authentication procedure can be user authentication only, or both device and user authentication at the same authentication domain, which, for [2], [3] is always the Home Network.

To conduct device/user authentication while roaming, an MS/SS is required to store security credentials which may include Subscriber Root Key (SUBC) and Private/Public Certificate Based keys (MS-Cert).

To enable roaming by customers with different terminals and credentials, WiMAX networks support authentication mechanisms which provide various types of credentials with WiMAX specific attributes for subscribers and SS/MSs. Currently, WiMAX networks support: username and passwords, Universal Subscriber Identity Module (USIM) and digital certificates. Device Authentication is achieved by using X.509 device certificates.

WiMAX networks support roaming using a RADIUS AAA framework.

4.5.3 IP Address Assignment

A MS/SS may obtain IP addresses belonging to the IP address space in the home CSN or in the visited CSN, depending on the roaming agreement between H-NSP and V-NSP, user subscription profile and policy of the H-NSP. MS mobility is handled with IP-based mobility management protocols.

4.5.4 Security

During roaming, user data security is provided by means of control-path/data-path encryption: the necessary cryptographic material is created after the authentication and authorization phase and automatically delivered to involved network elements, such as, the Access Service Network – Gateway (ASN-GW).

A WiMAX subscriber is able to obtain secure access from the visited network even when the visited network provides different security mechanisms, services, or tariff structures than the WiMAX subscriber‘s home network.

For reference point specific security mechanisms between the WiMAX™ access networks and any other access networks and/or core networks, please refer to [2] Section 7.3.2, and [3].

4.5.5 QoS

The scope of QoS in the current release of the WiMAX Forum NWG Network Architecture [2] [3] is limited to the radio access network. Currently, QoS is provided via pre-provisioned service flows, i.e., service flows that are activated at the network entry after successful MS/SS access authentication. The subscriber QoS profile, which includes the permissible number and schedule type of WiMAX service flows and permissible range of values for associated QoS parameters, is downloaded from the Home AAA (H-AAA) to the V-ASN during network access.

4.5.6 Accounting and Billing

After network entry, the different network elements, such as, ASN-GW and HA, start collecting accounting information for the users they are managing. This information is then collected by an accounting server, usually co-located with the authentication and authorization server, to be used for billing purposes.

Roaming users are charged for roaming services directly from their home NSP. It is recommended that a process of wholesale rating, clearing and settlement be in place, by which a V-NSP invoices the H-NSP for the usage of its network by the H-NSP's roaming users.

5 Inter WiMAX™ Roaming – Services

5.1 Roaming Guidelines Release 1.0 Services

The scope of the Roaming Guidelines Release 1.0 document is limited to WiMAX Forum NWG Network Architecture [2] and [3]. The present document covers WiMAX to WiMAX roaming for Best Effort IP connectivity services in support of applications, such as, File Transfer Protocol (FTP), e-mail, instant messaging, web browsing, Virtual Private Networks (VPNs), VoIP, streaming audio/video, gaming and other applications and services available through IP connectivity, all on a best effort basis.

This document provides no recommendations regarding deterministic QoS guarantees associated with roaming services.

5.2 Services to be Covered by Future Roaming Guidelines

Future Roaming Guideline documents will address new WiMAX roaming recommendations arising from the evolution of the WiMAX network architecture and new features enabled by future network releases. In particular, dynamic QoS support will enable additional services and can enhance services covered by this Roaming Guidelines document. Dynamic QoS enables managed IP services in support of applications, such, as audio/video streaming, VoIP, IP Multimedia Subsystem (IMS) services, multimedia IP conferencing, location and presence triggered IP applications, managed VPNs (client-based, network operator provisioned & enterprise), and interactive gaming.

Future guidelines will also address mandated regulatory services, such as, emergency services and lawful interception, and roaming aspects associated with Multimedia Session Continuity, WiMAX-WLAN handover and WiMAX – 3GPP/3GPP2 interworking.

6 Entry Procedures for WiMAX™ Roaming

6.1 Network Discovery & Selection

Network Discovery & Selection procedures (ND&S) are described in Section 7.1.4 of [2] and Section 4.1 of [3].

During roaming, the Home ASN (H-ASN) is not available and the H-CSN is only reachable through the CSN of a single Visited-NSP. In this situation, the goal of ND&S procedure is to enable the MS to discover all accessible NSPs in its radio coverage area and to select one NSP through which all subsequent AAA packets can be correctly routed to the subscriber's H-NSP. As explained below in this section and later in Section 6.2, AAA packets are routed towards the H-NSP using the realm part of the Network Access Identifier (NAI) used during Authentication.

6.1.1 V-NSP Deployment: NAP+NSP and NAP Sharing Cases

As described in [2] and [3], a WiMAX network can be deployed using two different architectures as follows:

- 'NAP+NSP' in which a NAP is associated with only one NSP. In this case, the V-NSP directly operates its own ASN, as illustrated in Figure 6.

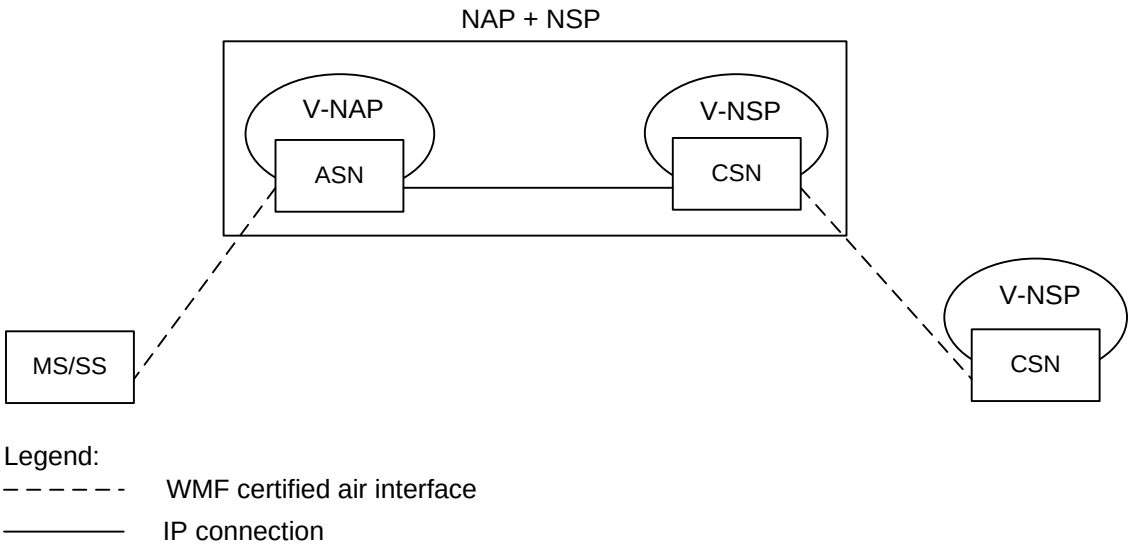

Figure 6 ND&S Paths for a NAP+NSP Deployment - Roaming Scenario

Figure 7 depicts a more complex roaming scenario for performing ND&S. In this scenario, the H-NSP is reachable indirectly through more than one V-NSP, V-NSP-1 and V-NSP-2, which, in turn, are each connected to a single Visited-NAP, respectively, V-NAP-1 and V-NAP-2, which deploy their own ASN. Path selection is dictated by the ND&S process and parameters.

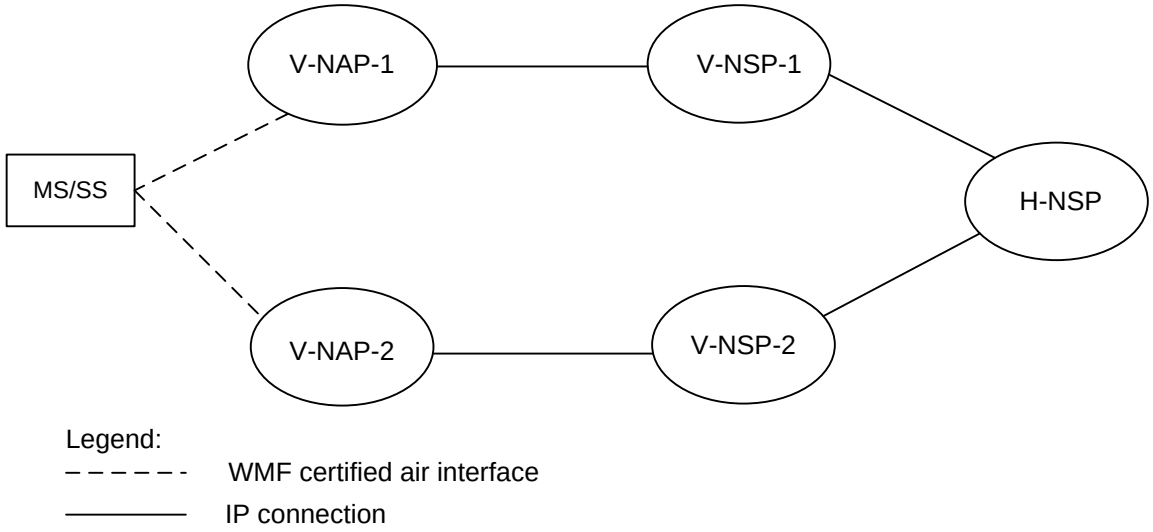

Figure 7 Depicts ND&S Paths through Multiple NAPs and NSPs

- 'NAP Sharing' in which a NAP provides ASN connectivity to more than one NSP as illustrated in Figure 8.

Figure 8 depicts a roaming scenario where an H-NSP has roaming available with more than one V-NSP. Additionally, in this scenario, each V-NSP is connected via more than one NAP. The H-CSN can be reached through multiple paths. The potential paths are through NSP-2, connected via NAP-1 or NAP-2 or through NSP-3 connected via NAP-1 or NAP-2. Path selection is dictated by the ND&S process and parameters.

Please note that this document covers only the relationship between the H-CSN and the V-CSN (highlighted in Figure 8). NAP Sharing relationships between NSPs and NAPs are beyond the scope of this document as NAP Sharing does not constitute roaming per se. Refer to Appendix D of this document and [2] and [3] for additional information about NAP Sharing.

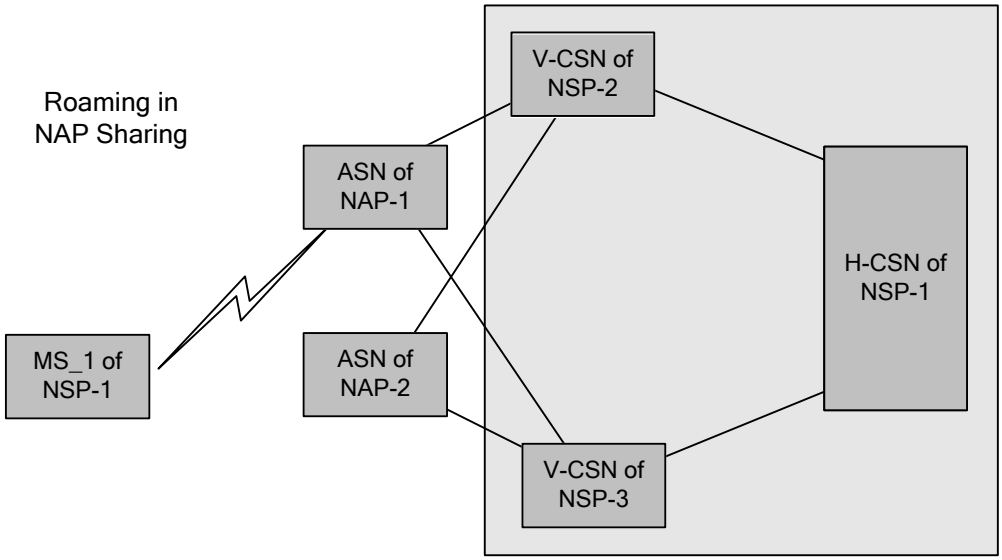

Figure 8 ND&S Paths in a NAP Sharing Deployment – Roaming Scenario

6.1.1.1 ND&S Steps

Figure 9 contains a high-level representation of ND&S steps.

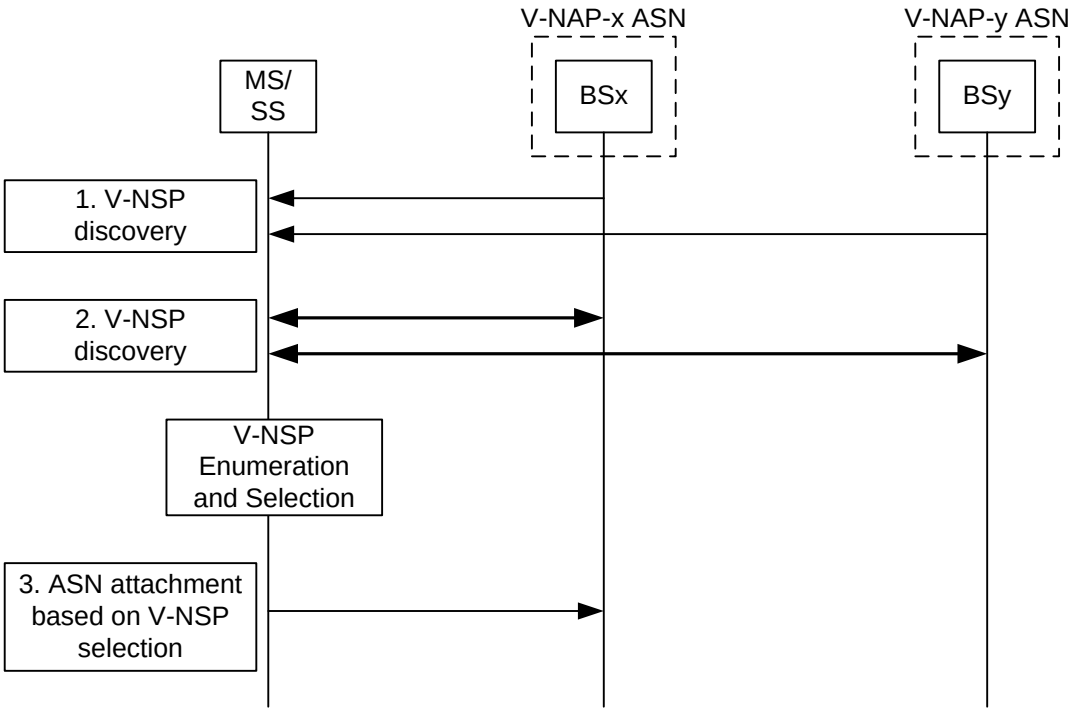

Figure 9 ND&S Steps (note: only MS and BSs are involved)

1. V-NAP and V-NSP Discovery: This procedure is described in Sections 4.1.2.1 and 4.1.2.2 of [3]. During this step, the MS/SS first discovers the available V-NAPs in its coverage area. Next, a list of the V-NSPs identifiers reachable through each V-NAP is transmitted to the MS/SS, periodically or on-demand. This list is required to accurately identify the network and provide adequate information to the MS/SS to make a network selection decision as described in the next step. In the NAP+NSP case, only one identifier (per visited network) will be advertised.

   The V-NSP identifiers are 24-bit strings: The format of this ID can vary. This identifier can be assigned by the IEEE or is derived from International Telecommunication Union ITU-T E.212 Mobile Network Code/Mobile Country Code (MNC/MCC) codes. The V-NSPs list can also contain verbose names to facilitate subscribers in selection procedures using 'Manual Mode'. It is not mandatory for the MS/SS to "blindly" perform NAP/NSP discovery if it has sufficient configuration information, such as, when information was already stored during a previous WiMAX Network Entry.

2. V-NSP enumeration and selection: The MS/SS produces a list of available V-NSPs obtained through V-NSP Discovery in the available V-NAPs, using its available internal configuration information. The NSP enumeration list is used for both manual and automatic selection. Manual and automatic selection modes are described in details in Section 4.1.2 of [3]. For manual selection, the user manually selects the most preferred NSP based on the dynamic information obtained within the coverage area. Manual selection can also enable user scenarios where a non-subscribed user wants to connect to a detected network. For example, the user wants to exercise an initial provisioning procedure with a specific NSP, or wishes to use the network on "pay for use" basis.

3. ASN attachment based on V-NSP selection:

After a V-NSP is selected, the MS/SS attaches to the ASN associated with the selected V-NSP. The MS/SS maps the 24-bit NSP identifiers received in the previous steps into realms of corresponding NSPs and provides its identity and Home NSP identity in the form of an NAI, constructed as described in Sections 7.1.4.4 of [2] and 4.1.2.4 of [3]. The ASN uses the realm portion of the NAI to route AAA transactions for the MS/SS. An example of valid decorated NAI is:

home.com!user@visited.com

Note that only for NSP+NAP case, where there is no need to indicate the V-NSP chosen by the MS/SS to the V-NAP, the MS/SS could optionally use the following NAI form:

user@home.com

Note also that the default behavior of the MS/SS is to provide a decorated NAI, unless the MS/SS is sure it may provide a non-decorated NAI. See Appendix D for details on NAI decoration used in a NAP sharing environment.

The NAI uniquely identifies the user and will subsequently be used during AAA procedures. Additional considerations and recommendations on the choice and formats of the user identity are provided in Section 6.2.

Note: CSNs of V-NSPs are not involved in the ND&S process.

6.1.2 Recommendations

Operator ID:

The roaming partners must use a public Operator ID (OID) for NAP-ID and NSP-ID as per Section 4.1.2.2 of [3]. Use of a public OID ensures its uniqueness and is used for both network entry and identification of the home and the visited NSP to which the AAA accounting messages exchanged via the R5 reference relate to. In the WiMAX™ Roaming Interface Architecture [5] [6], the WiMAX™ Roaming Interface (WRI) Code is included in information exchanged between WRI logical entities to uniquely identify the home NSPs, visited NSPs, and the sending and the receiving WRXs. The first three characters of the WRI Code represent the country the operator or the WRX is operating in or are assigned by WiMAX Forum while the remaining three characters identify the operator or the WRX. The WiMAX Forum administers and issues the WRI Code. Additional information on the detailed use of WRI code and application procedures are detailed in [2],[3] and [4] respectively.

The visited network must support processing of decorated and non-decorated NAIs

NSP-ID list:

- The advertised NSP-ID list must contain only the NSP that is directly connected to the NAP's network.
- The valid formats for NAP-ID and NSP-ID are defined in Section 4.1.2.2 of [3]. For example, an operator, which already operates a cellular network (e.g. GSM), is likely to have a NSP-ID that contains MNC and MCC code. If a terminal is allowed to roam from the home operator's network to another operator's network, the home operator must configure the terminal with the other operator's NSP-ID. The format of the NSP-ID in the terminal's roaming list is dictated by the other operator.
- The list of NSP-IDs and verbose NSP names presented over the air interface as part of Service Identity Information Advertisement (SII-ADV) and/or SS Basic Capability Response (SBC-RSP) and all NSP realms that can be obtained using SS Basic Capability Request/Response (SBC-REQ/RSP) message must be uniform across all Base Stations of the same NAP-ID. See Section 4.1.2.2 of [3].

A "Verbose NSP Names" list is needed if the network transmits a list of Verbose NSP Names over the air interface (as part of SII-ADV and/or SBC-RSP), along with the list of NSP-IDs.

Recommend MS/SS Configuration:

1. NAP-ID of roaming partners in the 'Operator Preferred NAP' list. This list is controlled by the H-CSN.
2. User Controlled NAP list. This list is controlled by the user and is not under the control of any network operator.
3. NSP-IDs of roaming partners in the 'Operator Preferred NSP' list. This list is controlled by the H-CSN.
4. User Controlled NSP list. This list is controlled by the user and is not under the control of any operator.
5. It is recommended that verbose names of roaming partners be available in a pre-configured list (NAP/NSP mapping list).
6. If information useful in the MS discovery of a NAP, including previously detected and retained values, stored information, such as, channel, center frequency, and Physical (PHY) profile is available in configuration information, it is recommended that it be used to improve the efficiency of NAP discovery.
7. Mapping Table to map the V-NSP-ID to a realm if needed.

6.2 Authentication

6.2.1 Authentication and AAA Proxy

Network access authentication is a part of the process that authorizes a MS/SS to obtain WiMAX access service. WiMAX Forum NWG Network Architecture specifications, [2] and [3], use the Extensible Authentication Protocol (EAP) framework for authentication. EAP supports multiple authentication methods. Messages belonging to the specific methods are encapsulated in EAP packets and transported via the radio interface, using Privacy Key Management protocol version 2 (PKMv2) messages and then towards the H-NSP AAA server, passing through an AAA Proxy in the V-NSP network, encapsulated in RADIUS messages. This process is illustrated in Figure 10. For a complete list of relevant acronyms used in Figure 10, see Section 2.

WiMAX Forum NWG Network Architecture specifications, [2] and [3], support three EAP methods, namely EAP - Transport Layer Security (EAP-TLS), EAP - Tunneled Transport Layer Security (EAP-TTLS), both certificate-based, and EAP - Authentication and Key Agreement (EAP-AKA). The latter is Subscriber Identity Module (SIM)-card-based for authenticating the subscribers against a 3GPP AAA server.

In networks deployed in accordance with WiMAX Forum network specifications [2] and [3], the H-NSP always performs authentication to verify the subscriber credentials only or the device credentials only or the subscriber and the device credentials jointly. V-NSP will not perform authentication.

The functional blocks of the authentication procedure are presented below.

Table 1 Functional Blocks of the authentication procedure

Entity	Function
MS/SS	MS/SS acts as the EAP peer.
NAS	Network Acess Server (NAS) consists of the EAP authenticator and is the receiver of service authorization attributes. It resides in the ASN. The NAS is usually co-located with the ASN Gateway.
V-AAA	The AAA Proxy that resides in the V-CSN.
H-AAA	The H-AAA server resides in the H-CSN. The EAP authentication server typically resides within this H-AAA server. The H-AAA server has access to the user profiles and is also involved in the authentication of the mobility operations.

It is assumed that WRX/AAA Proxies are trusted, act in a pass-through fashion and do not modify the RADIUS packets unless agreed between the parties involved.

After successful network access authentication, the H-AAA delivers agreed authorization attributes to the NAS. The H-AAA will return agreed data to the Visited AAA (V-AAA) which may then be modified to provide appropriate parameters for control of the visited network.

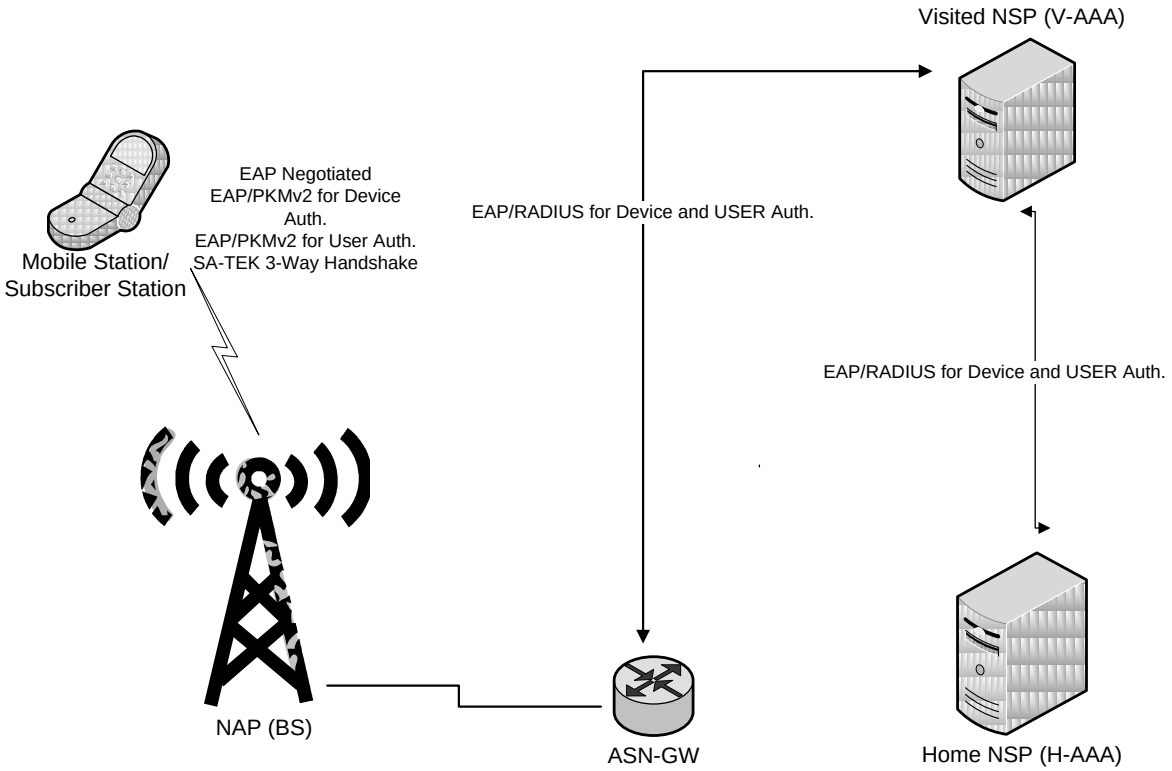

Figure 10 Flow of Protocols for Device and/or User Authentication

All details about user/device authentication are provided in [2] and [3] Section 4.4.1.

6.2.2 NAI

An NAI is assigned to a WiMAX subscriber by its home operator and serves as the primary identification for AAA purposes. It is used as an identifier within EAP-based user and MS/SS network access authentication. WiMAX networks [2] and [3] use NAIs as defined in IETF RFC 4282 [12] allowing for decorated NAIs.

6.2.3 Roaming Identity Selection

A user may have multiple subscriptions. Prior to establishment of communication with the visited network, the MS/SS needs to use the applicable configuration parameters associated with the selected visited NSP so that the RADIUS and accounting messages can be routed to the appropriate home AAA or WiMAX Roaming eXchange. The configuration parameters which need to be determined include:

1. The subscription to be used:

   User-Name & Password (if required) and/or

   Appropriate credentials (if required). This may involve the use of the appropriate security certificates.

2. The authentication method(s) to be used for the connection.

3. The Access-Request Identity to be used for the request (NAI).

After having detected each available ASN and each NSP-ID during ND&S process, a decision must be made with regard to the Roaming Identity to be used for the connection based upon the NSP Identifier Flag.

The Standard Identity, user@home.com, is the default identity used in an AAA Access Request as specified by the WiMAX Forum. The decorated NAI, instead of the Standard NAI, is used when the routing information is available.

Where NAP Sharing is used for a "Roaming" connection over a partner network, in response to the Visited Network's Identity Request, the MS/SS must transmit a decorated NAI in the Identity Response to indicate which V-NSP is to route the AAA requests to the Home Network responsible for authenticating the user and authorizing service to the user's MS/SS account. As such, the user's Decorated Identity describes the Home Realm's billable AAA relationship to the V-NSP at the time of connection.

6.2.3.1 Network Access Identifier (NAI)

The Standard Identity, user@home.com, is the default identity to be used in an AAA Access Request as specified by the WiMAX Forum. This NAI applies in both the roaming and non-roaming cases.

Use of the Standard Identity assumes that the Home Realm is a Fully Qualified Domain Name (FQDN) and is recognized by all V-NSP AAA Proxies via direct business relationships and network peering. This Standard Identity is typically the user and domain that the NSP or end-user provides to the MS/SS. The Standard Identity represents the Principal Name or Pseudo-Name of the user's subscription defined in the home domain. It is assumed that in this case if the user has multiple subscriptions with the home operator, the subscription selected by the roaming user is to be used.

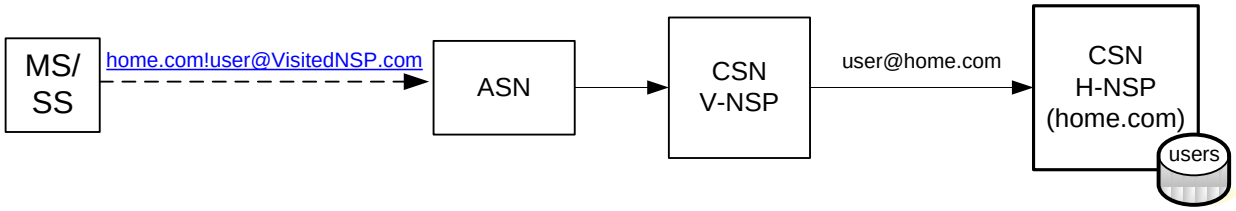

Figure 11 Standard Identity NAI Construction

6.2.3.2 Decorated Identity

The Decorated Identity is used in NAP Sharing but may also be used in non-NAP sharing cases when a known or preferred route to the home realm is only available to the MS via a 3rd party AAA or WiMAX Roaming eXchange for a particular NSP-ID. In general, the NSP identifier flag is set to 1 in NAP sharing scenarios.

It is recommended that the MS/SS uses the following approaches:

1. When the NSP Identifier Flag is set to "1", the terminal decorates the NAI with:
    i. V-NSP. In this case, the V-NSP and intermediate AAA Proxies/WRXs may need to decorate the NAI when insufficient routing information is available to route the messages to the home domain.
    ii. End-to-end route if all the necessary routing information is available.
2. When the NSP Identifier Flag is set to "0", the terminal uses:
    i. Standard NAI.
    ii. Decorated NAI including the visited NSP without having full knowledge of the end-to-end route.
    iii. Decorated NAI with end-to-end route if all the necessary routing information is available.

In order to maintain simple suffix-based AAA RADIUS User-Name proxy rules for a FQDN, the decorated Identity "transforms" the Standard Identity into an alternate NAI construction form using the Realm Construction rules in IETF RFC 4282 Section 2.7 [12]. The MS/SS uses the network selection procedure to select the Visited NSP which is responsible for routing the AAA request to the Home NSP. The FQDN of the visited NSP may be added to the NAI decoration. The MS/SS may have to add additional data (i.e. decorates) to the NAI so that AAA traffic such as the authentication requests can be routed to the home domain

The terminal can decorate the NAI with the information if available else it will use the Standard NAI format. In any roaming case, where multiple logical AAA paths exist for any identified ASN peer, source-routed AAA routes are described in multiple "chained" NAI prefixes delimited with an Exclamation Mark (!). The assumption has been made that all AAA peers in the path of the chain and terminal must support this feature.

Each mediating AAA, WRX, must be added to a Decorated NAI in the order required for routing.

Listed below are some examples of possible decorated NAIs.

1. Message is to be routed from the NAS to the Visited NSP to the Home NSP.

home.com!user@VisitedNSP.com.

2. Messages are to be routed from the NAS to the Visited NSP to the Home NSP via an intermediary:

   intermediary.com!home.com!user@VisitedNSP.com.

Note:

- It is possible that the messages are traversing one or more intermediaries but the MS/SS may not have the knowledge to decorate the NAI with all the intermediate entities.

- Additional functionality in the MS/SS may be needed to add the intermediate routes to the NAI.

6.2.3.3 General Rules for Handling NAI Construction

The exchange of WiMAX AAA information is based on suffix-routing, also referred to as domain based routing, of a FQDN contained in the RADIUS User-Name attribute as determined by the Identity Response of the MS/SS. There are no routing precedence rules that must be followed.

The WiMAX visited CSN, acting as a RADIUS proxy, determines whether it is processing an AAA request from a roaming terminal by investigating if the received NAI is to be routed to another operator's AAA Proxy. When the received AAA RADIUS Authentication Request does not match the realm of the visited domain (e.g., NAI is user@home.com), the AAA request is recommended to be processed, forwarded, or rejected as described in IETF RFC 4282 Section 2.7 [12] and [3].

If the AAA Proxy receives an end-to-end decorated NAI from the roaming terminal, the visited AAA-Proxy forwards the RADIUS AAA request to the RADIUS host responsible for the trailing domain suffix (e.g. @fqdn.com up to the first @ delimiter, read right-to-left). It should be noted that the AAA Proxies listed in the NAI must receive the AAA messages. This does not preclude that other AAA Proxies from forwarding these AAA messages. If the visited AAA Proxy receives the NAI without an end-to-end route from the roaming terminal, the AAA Proxy needs to determine the route to the home AAA. In this case, the AAA Proxy must be configured in such a way that AAA traffic can be routed directly or via intermediate WRXs from the visited to the home domain based on realm. Any proprietary NAI decoration method must not take precedence over the procedures in [3].

RADIUS Accounting messages normally follow the same NAI routing procedures as the RADIUS Authentication request messages transmitted from the visited to the home domain. It is possible that the Authentication request messages and RADIUS Accounting messages from the visited to the home domain are routed to different AAA servers as determined by configuration or agreements. In this case, the home AAA server performs the relevant authentication while a third party, i.e. a roaming exchange, performs the accounting procedures on behalf of the home domain. When the Authentication and Accounting messages take separate RADIUS paths from the ASN Gateway, it is critical that the same NAI routing rules are applied to the different proxy paths.

Note: In WiMAX Forum NWG Network Architecture [2] [3], there is no mechanism defined to select an alternate WRX based on the fact that there is no response received.

6.2.4 EAP Authentication Methods

The WiMAX Forum NWG Network Architecture specifications, [2] and [3], specify several EAP Authentication methods that are suitable for network access including EAP-AKA, EAP-TLS and EAP-TTLS.

It should be noted that authentication is performed end-to-end, i.e. it involves the MS/SS and the Home WiMAX Network ONLY: hence, it is totally transparent to the Visited WiMAX Network.

EAP-TTLS is the recommended Authentication method for WiMAX roaming when using Digital Certificate credentials and User-Name/Password based authentications. This "Tunneled" EAP Authentication method establishes an EAP-TLS tunnel which secures the "inner" authentication containing the actual H-NSP Account Username and its corresponding credential. The Transport Layer Security (TLS)-secured Inner Authentication Methods within Tunneled Transport Layer Security (TTLS) MAY be of any type including EAP and non-EAP based methods.

When using EAP-TTLS, three instances of security credentials can be specified. When establishing the outer tunnel the AAA server must provide its server certificate to MS/SS and the MS/SS may provide its device certificate to the AAA server. In the secured inner tunnel, the MS/SS provides its subscription credential to the home AAA server

6.2.4.1 TLS Fragmentation over RADIUS

When using TTLS over RADIUS, the TLS fragmentation size is commonly set by default to 1400 bytes by most TLS libraries and is sized specifically to communicate over an Ethernet Maximum Transmission Unit (MTU) of 1500 bytes to comply with the maximum RADIUS packet length. However, when exchanging RADIUS packets peered over Generic Routing Encapsulation (GRE)/IPsec for private transport, a smaller RADIUS MTU is required (typically 1400 bytes maximum) which will fail during a TTLS exchange. It is recommended that TTLS Servers limit the TLS Fragment in order to fit the size to exactly five (5) EAP-Messages or 1265 bytes in order to fit within a 1400 byte RADIUS MTU size or Secure Socket Layer (SSL) handshake failure may occur when using IPv4. It is assumed that the each EAP message size is 253 bytes in length as per IETF RFC 2869 [10]. Further analysis is needed when IPv6 is used as transport protocol.

TTLS Home Authentication Servers must size their RADIUS packets (and the TLS fragment size being transported by them accordingly) to conform to the RADIUS Access-Request Attribute Framed-MTU should it be present in the request.

Note: This section is specific to RADIUS.

6.2.5 RADIUS Proxy Forwarding

In WiMAX Roaming Guideline Release 1.0, static routing configuration is recommended to be used to support the following scenarios:

1. Direct connection between home and visited domain (Figure 11)
2. One WRX between Home and Visited Domain (Figure 12)

Figure 12 depicts the scenario of one NSP using a WRX and the second NSP not using a WRX. The WRX may be providing service to either the visited or the home network.

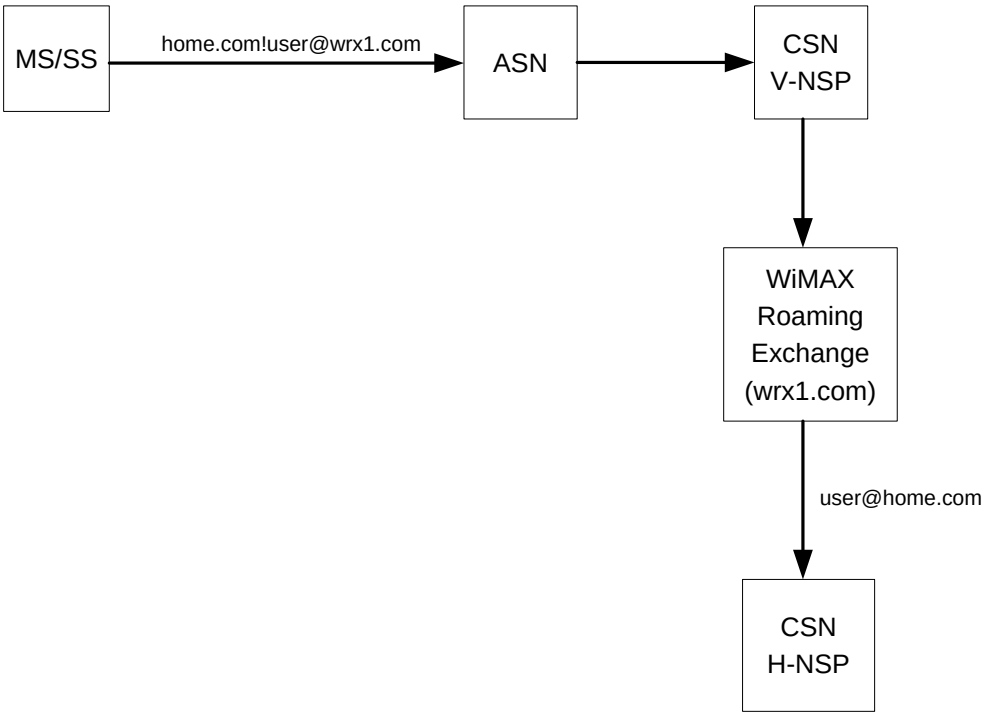

Figure 12 One WRX between two NSPs

3. Home and Visited domain connected via an interconnected WRX network

The following figure depicts the scenario of each NSP using WRX.

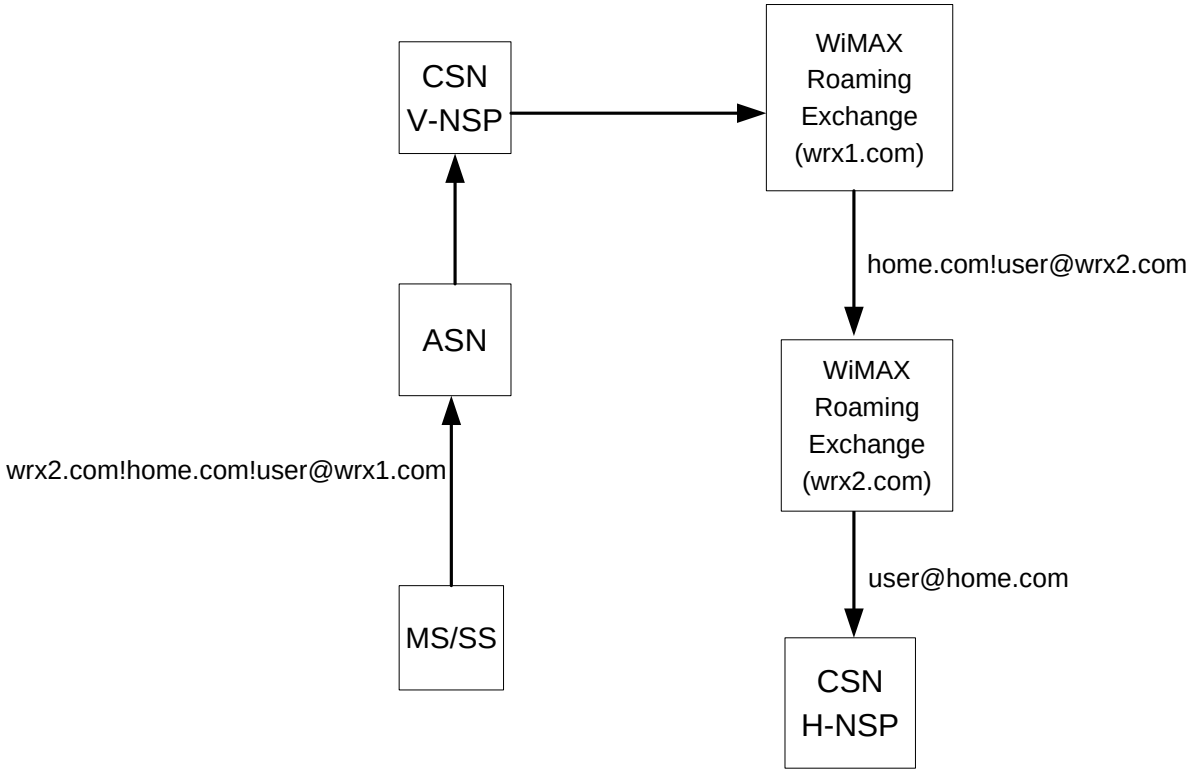

Figure 13 Two WRXs between NSPs

The information in this section is provided as a tutorial for informational purposes. For more information, see IETF RFC 4282 [12] and [3].

In WiMAX networks, the incoming Authentication Request NAI will always contain the suffix used to route the request to the current operating proxy by the upstream peer. In legacy RADIUS, this would normally indicate a Local Request arriving at the Home AAA for user authentication. In WiMAX networks, an additional check of the NAI must be performed to verify if this request is Local or decorated with an NAI Prefix for proxy. As stated in IETF RFC 4282 [12], on receiving RADIUS Access-Request with a non-local prefix contained in the NAI delimited with a "!" (read left-to-right), the message must be operated on and transformed in order to qualify it for proxy to the appropriate realm.

Incoming NAI: knownrealm.com!username@myrealm.com

Transformed NAI: username@knownrealm.com

Once the NAI has been logically transformed, the suffix is used to determine the route to the appropriate realm. Should the suffix match an existing RADIUS route, it is transmitted in its transformed syntax to its destination. All subsequent messages for the current RADIUS proxy sequence must operate on the NAI in the same manner until the sequence is complete.

Transmitted NAI: username@knownrealm.com

The Prefix Decoration of a roaming identity may occur recursively, meaning that even after transformation the NAI may still have one or more prefixes delimited with a "!" contained in the username. For example,

Incoming NAI = knownrealm!anotherrealm!username@myrealm.com

Only the first prefix from the left delimited with an "!" may be considered for proxy and therefore only a single transformation of the NAI for suffix-based forwarding is allowed during the proxy operation.

In cases where both the Decorated Prefix and Suffix realms are considered Local (e.g. myrealm.com!user@myrealm.com), the remainder is considered to be the Username of the account to be authenticated locally and is not subject to proxy. This might occur if the MS/SS always decorates its NAI when attaching to an NSP-ID in a NAP Sharing scenario even for its own Home NSP-ID.

In order to prevent the attempted re-direction of RADIUS authentication through unauthorized RADIUS peers, it is recommended that no additional decorations or modifications in the proxy operation as described above be performed on the NAI unless routing changes are required beyond the next hop. For a roaming MS/SS, it is recommended that the RADIUS Proxy not forward an NAI without the valid realm to the next hop. Only the H-NSP may determine if the undecorated Account Name is acceptable for direct access to the home network by its users.

It is recommended that the User-Name value of the Access-Request or Accounting-Request not, at any time, be modified during proxy beyond the proxy handling rules outlined herein.

Should "Stripping" of any Alternate Identity NAI decorations be necessary, the procedure must only occur at the RADIUS destination of included in the NAI; where the realm is considered "Local" and must not occur prior to the RADIUS Access-Request transmission during proxy.

6.2.6 RADIUS Authorization

RADIUS Access-Accept messages must carry the necessary per-authentication keying material necessary to secure the MS/SS Radio link as specified in [2] and [3].

Should any NAI which excludes the actual identity of the subscriber (e.g. identity hiding) be used, the H-NSP AAA must provide the RADIUS Reply Attribute "Chargeable-User-Id" in its RADIUS Access-Accept message containing a unique handle per authenticating domain representing the user identity to be

billed for the authenticated session. This identity will be changed periodically by the Home AAA to protect the true identity of the user. See IETF RFC 4372 [13] for additional information.

6.2.7 Functional Recommendations

- The Network Access Identifier (NAI) used in WiMAX networks must conform to IETF RFC 4282 [12] and [3]. It is used as an identifier within EAP-based user and MS/SS network access authentication.
- It is recommended that the outer-identity be used primarily to route the packet and act as a hint in helping the EAP Authentication Server select the appropriate EAP method. The inner-identity must be used to identify the user, or authenticated credentials. EAP methods that provide identity hiding will transmit the inner-identity within an encrypted tunnel created using the EAP method.
- In order to support identity hiding, it must be possible to carry the real identity of the MS/SS in the inner-identity only. For the outer-identity, a pseudonym is used that can be resolved to the real user identity only by the MS/SS itself and the home CSN.
- A V-NSP must be able to resolve an NAI to a valid IP address of the next valid destination for routing of RADIUS packets based on the suffix of the NAI.
- It is recommended that the AAA server authenticate the proxy AAA server to verify it is a valid roaming partner.
- The mobile device may have to authenticate itself using the device certificate to the AAA server, hence confirming the Medium Access Control (MAC) address. The mobile device may have to use other credentials as well.
- The AAA server may execute local policy rules. These local policies must not interfere with features already defined in the WiMAX Forum NWG Network Architecture specifications [2] and [3] and have to be verified between the roaming partners prior to commercial launch of roaming services. Note that AAA local policies are beyond the scope of the Roaming Guidelines.

6.3 Service Flows and QoS

In WiMAX Forum NWG Network Architecture [2] and [3], QoS is over-the-air only. WiMAX systems support the concept of pre-provisioned Service Flow, i.e. QoS is statically configured (pre-provisioned) on a per-user basis and is not dynamically negotiable. It is recommended that roaming partners agree in advance on basic QoS profiles and related parameters available to their roaming users.

6.3.1 Description

The scope of the QoS framework in WiMAX Forum NWG Network Architecture [2] and [3] is focused on the WiMAX radio link connection. QoS specific treatment in the fixed part of the access and core networks is implementation specific and is not described in this document. As a result, the WiMAX Forum NWG Network Architecture, [2] and [3], does not guarantee end-to-end QoS. The provisioning of QoS in the access and core networks is the responsibility of V-NSP.

Pursuant to the IEEE 802.16 specification, a subscription may be associated with a number of service flows characterized by QoS parameters (e.g., Unsolicited Grant Service (UGS), Real Time Variable Rate (RT-VR), Extended Real Time Variable Rate (ERT-VR), Near Real Time Variable Rate (NRT-VR) and Best Effort (BE)). This information must be provisioned in a subscriber management system (e.g., H-AAA server) or a policy server.

Each service flow represents a single unidirectional WiMAX radio interface connection with guaranteed QoS parameters. The subscriber station is not permitted to change the parameters of provisioned service flows or create new service flows dynamically.

Service flows are activated at network entry after successful MS/SS access authentication.

At the completion of authentication and registration, an Initial Service flow (ISF) is established for the MS/SS within the ASN. The ISF can be used for IP configuration of the host. Dynamic Host Configuration Protocol (DHCP) messages can be transported over the ISF associated with the MS/SS.

WiMAX Forum NWG Network Architecture [2] and [3] defines detailed procedures to create, modify and delete subscriber service flows ([3]).

6.3.2 Logical Entities

Logical entities associated with service flows and QoS are defined in [2] and [3]. A summary is provided below:

- The H-AAA server holds the user's QoS profile and associated policy rules. This information can be downloaded to the Service Flow Authorization (SFA) at the time of network entry as part of the authentication and authorization procedure.
- The Service Flow Authorization (SFA) is a logical entity in the ASN. In case the user QoS profile is downloaded from the AAA into the SFA at network entry phase, the SFA is responsible for evaluating any service request against the user's QoS profile.
- The Service Flow Management (SFM) is a logical entity in the ASN. The SFM entity is responsible for the creation, admission, activation, modification and deletion of the IEEE 802.16 service flows. The SFM entity is always located in the BS and hence falls under responsibility of V-NSP.

6.3.3 Recommendations

Listed below are recommendations to support multiple "QoS profiles" on a best efforts basis:

1. Provision "QoS profiles" on a subscriber-basis in the home AAA.
2. Default roaming profile. It is recommended that the V-NSP and H-NSP agree in advance, through a roaming agreement, on a minimum "QoS profile" which will be granted to roaming users in case the requested QoS profile cannot be provided.
3. Common "QoS profiles" for roaming users. Common QoS profiles are needed because the support of all H-NSP QoS profiles by a v-NSP may not be practical.

For example, "Best Effort Internet services" may include several best effort QoS options. If NSP A is providing a tiered best effort service (different maximum transfer rates), when NSP A users roam onto NSP B's network, applicable parameters must be provided by NSP A to NSP B.

7 IP Address Management

This section provides a high level description of the procedures for IP address allocation for IPv4 in roaming. IPv6 procedures will be addressed in a future release of this document. IPv4 addressing procedures are discussed in detail in Section 4.8 in [3].

7.1 MS and Network IP Capabilities

IP address assignment strictly depends on the mobility scheme deployed in both Home and Visited network and on MS capabilities.

Two IP mobility protocols for IPv4, as defined in [2] and [3], are:

- Proxy MIP (PMIP): The MS/SS does not implement a Mobile IP client. It obtains an IP address by using DHCP protocol. The mobility binding in this case is done transparently for the terminal between the PMIP client in the ASN and the HA.
- Client MIP (CMIP): The MS implements a Mobile IP client. It contacts the ASN-GW, functioning as Foreign Agent, which, in turn, creates a mobility binding on-behalf of the MS with the Home Agent and sets up a GRE or an IP-in-IP tunnel for MS traffic which is terminated at the HA. For MIP enabled terminals, MIP based addressing is used instead of DHCP.

Both PMIP and CMIP are optional from a terminal point of view and mandatory from a network point of view WiMAX Forum NWG Network Architecture [2] and [3].

7.2 MIP Mode Selection

Prior to an intra-ASN data path establishment, the network is unaware of the MS IP capabilities. Thus, immediately after the data path between ASN-located FA and MS is established, the FA entity will send an FA advertisement to the terminal over this newly established data path. If the terminal is MIP enabled, it will perform a MIP registration using the Care of Address (CoA) advertised in the FA advertisement. The MIP registration originated from the MS will force the network into CMIP mode.

A MS/SS without MIP functionality (Simple IP terminal) will discard the FA advertisement and send a DHCP request to get an IP address. The DHCP request will trigger the PMIP Mobility Manager to perform mobile IP on behalf of the MS/SS.

For networks that support both CMIP and PMIP the selection is straightforward and is driven by the terminal. Network capability discovery is based on MIP agent advertisement messages sent just after connection setup. The mobility scheme selection is determined by the ASN, based on the type of message received from the terminal and can be either a DHCP request or a MIP Registration Request (RRQ).

7.3 IP Address Allocation Procedures and Scenarios

After successful access level authentication, IP address allocation procedure is performed. Different scenarios are possible depending on:

- The MS/SS IP capabilities (MIP or non MIP-enabled)
- The anchoring preference (HA in H-CSN or HA in V-CSN). In WiMAX Forum NWG Network Architecture [2] and [3], the Home Agent, for a given MS, can be dynamically allocated in the H-NSP or in the V-NSP. This preference depends on the agreement between V-NSP and H-NSP and is used at the time the mobility binding is initially set-up for a MS.

Figure 14 and Figure 15 depict the two anchoring scenarios.

It is assumed that both CMIP and PMIP are mandatory in the network at least for the current release of this document.

The table below summarizes different IP allocation scenarios:

Table 2 IP allocation scenarios

MS capabilities	HA in the H-CSN	HA in V-CSN
Simple IP	Supported with PMIP	Supported with PMIP
CMIP	Supported	Supported

These procedures and scenarios are detailed in Section 4.8 in [3].

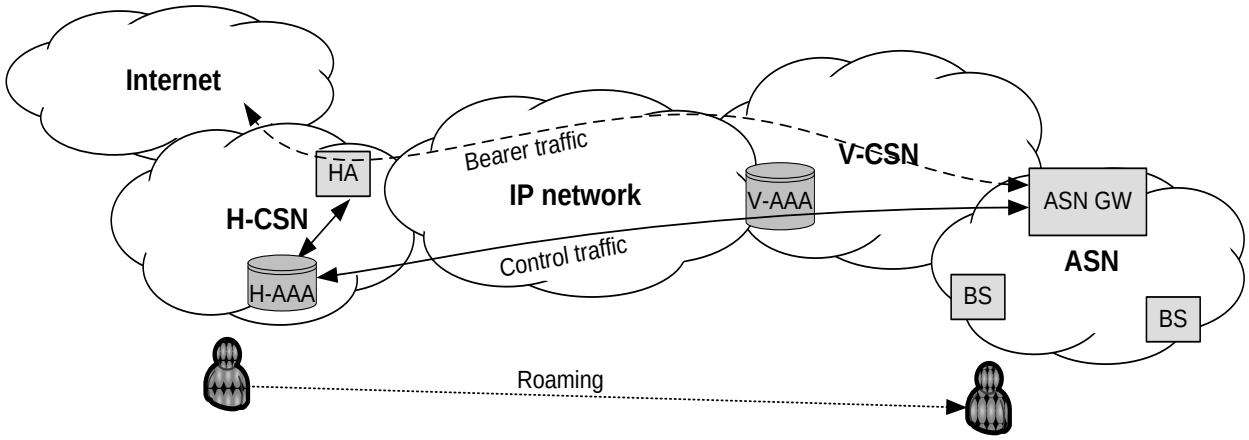

Figure 14 Roaming with HA in the Home Network

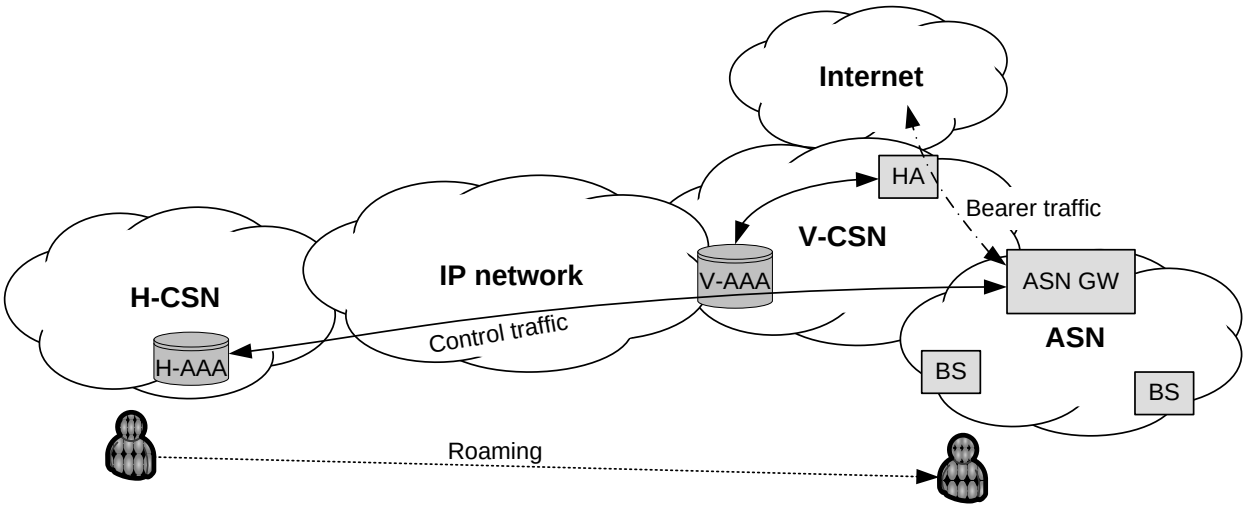

Figure 15 Roaming with HA in the Visited Network

It is recommended that the interconnection between H-CSN and V-CSN be accomplished following the guidelines in Section 8 of this document.

The uplink and downlink MS traffic is anchored to the HA as follows:

- If the HA is located in the V-CSN, traffic directed towards the Internet flows directly out of the V-CSN. In case it is required that traffic be forwarded to the H-NSP, for all or some services, the roaming partners must agree and define a suitable IP routing/tunnel configuration, which is out of the scope of WiMAX Forum NWG Network Architecture [2] and [3].
- If the HA is located in the H-CSN, all the MS traffic will be delivered to the H-CSN. For example, Internet will be accessed through the H-CSN.

7.4 Recommendations

H-NSP and V-NSP must agree on location preference for the HA (in the V-CSN or in the H-CSN). If the HA is in the V-CSN, the V-NSP must verify that sufficient IP addresses are available to accommodate roaming MSs.

H-CSN or V-CSN must be able to allocate IP addresses to roaming MS/SSs. Moreover, it is recommended that assigned IP addresses not overlap with the address space in the H-CSN or in V-CSN. For example, overlapping of private addressing spaces assigned to MS of different H-NSPs, must be avoided.

In case HA is in the H-CSN, both MIP signaling and user traffic (encapsulated in GRE or in IP-in-IP) must be transported to the Home Network.

The following table lists the possible combinations of MS/SS mobility and network mobility support. Note that not all scenarios are supported. The Roaming partners must verify coexistence.

Table 3 IP Coexistence Scenarios

MS support	Network Support	Decision
MIP	CMIP	CMIP
Simple-IP	PMIP	PMIP
MIP	CMIP + PMIP	CMIP
Simple IP	CMIP + PMIP	PMIP
MIP	PMIP	PMIP
Simple-IP	CMIP	No CSN-anchored mobility. Mobility is still possible among ASN-GWs that support R4.

8 WiMAX™ Roaming Interconnection

Data roaming requires interconnections between V-NSP and H-NSP to transport traffic used for billing and settlement as well as AAA and bearer traffic. Billing, Settlement, and Clearing require consistent regular exchanges of files by FTP or other methods. Real-time RADIUS records exchanged between AAA Proxies in the visited domain and AAA servers in the home domain must be transported over a secure or direct connection. Bearer Traffic can be best supported by high bandwidth secure circuits. Bearer Traffic interconnection is not needed when the data service is provided by the V-NSP.

Interconnections can be achieved via Internet VPN, dedicated direct circuits, or managed IP networks. If the visited or home NSP chooses to route traffic through a WRX, the interconnections to the WRX can be achieved via the aforementioned connection options.

Internet VPN:

Internet VPN has traditionally been a method of establishing roaming between two service providers. Internet VPN may also be suitable for Billing and Settlement and AAA traffic, as long as it logically segregated from data traffic.

VPNs are commonly implemented via IPsec tunnels. IPsec is a standardized, well-established, interoperable and largely implemented technology, used to build secure connections, with features such as confidentiality, integrity, and authentication. Roaming partners willing to implement interconnection through IPsec VPNs, must agree on a IPsec profile. Section 8.1 contains a recommended set of VPN parameters.

Dedicated Direct Circuits:

Two service providers may use dedicated direct point-to-point private lines to provide roaming services. Although this solution meets the requirements of AAA Traffic and Bearer Traffic, it may be expensive to create and operate direct connections with each roaming partner.

WiMAX Roaming Exchange (WRX):

WRX is a roaming intermediary that may provide:

- Dedicated IP Hub services for interconnections among multiple service providers.
- AAA Proxy and inter-networking service.
- Billing, settlement and clearinghouse services.
- Repository for NSP information required for roaming.
- Peering with other WRX providers.

A WRX may act as a single point of interface for interconnections with many service providers. A service provider can establish dedicated point-to-point circuits with one or more WRXs to connect other NSPs who also use WRXs. WRX providers must peer with each other to extend the reachability.

8.1 Recommendations

Table 4 contains the recommended IPsec profile. For some parameters, both a "minimum-to-implement" value and a recommended value have been provided, as specified in [11], [14] and [15]. For a complete list of relevant acronyms used in the tables below, see Section 2.

Table 4 Recommended IPsec profile[1]

Internet Key Exchange version 1 (IKEv1) settings		
	Minimum	*Recommended*
Diffie-Hellman Group	2 (1024-bit)	14 (2048-bit)
Protocol	Encapsulating Security Payload (ESP)	
Identification	IP address and FQDN	
ISAKMP Mode	Main	
Authentication mode	Pre-shared secrets	
Authentication algorithm	HMAC-SHA1	AES-128 in XCBC mode
Encryption Algorithm	TripleDES in CBC Mode	AES-128 in CBC mode
Lifetime	86400 seconds (24 hours)*	

Internet Key Exchange version 2 (IKEv2) settings		
	Minimum	*Recommended*
Diffie-Hellman Group	2 (1024-bit)	14 (2048-bit)
Protocol	Encapsulating Security Payload (ESP)	
Identification	IP address and FQDN	
Authentication mode	Pre-shared secrets	
Re-keying of IPsec Security Assocations (SAs) and IKE SAs	Yes	
Pseudo Random Function	HMAC-SHA1	AES-128 in CBC mode
Integrity	HMAC-SHA1-96	AES-XCBC-96
Confidentiality	TripleDES in CBC mode	AES-128 in CBC mode
Lifetime	86400 seconds (24 hours)*	

[1] See Section 2 or the relevant references for the abbreviations or acronyms used in this table.

IPsec settings		
	Minimum	*Recommended*
Protocol	ESP, Tunnel Mode	
Authentication algorithm	HMAC-SHA1-96	AES-XCBC-MAC-96
Encryption Algorithm	TripleDES in CBC mode	AES-128 in CBC mode
Perfect Forward Secrecy	No	Yes
Lifetime	28800 seconds (8 hours)*	

(*) The value of these timers is subject to Security Association agreements between the involved entities.

Note: IKEv2 has advantages over IKEv1 in terms of reducing network traffic and less complexity and is expected to replace IKEv1 in the future. Operators and WRX providers:

1) Should note that IKEv2 is not interoperable with IKEv1.

2) May implement IKEv2, however all parties must implement IKEv1 as well to ensure interoperability.

3) Must avoid falling back to less than the minimum requirements listed in Table 4.

9 WiMAX™ Roaming Accounting and Settlement

9.1 Introduction and Scope

The purpose of this section is to provide recommendations for accounting, clearing, and settlement procedures for WiMAX roaming.

It is worth noting that WiMAX accounting information is used by operators both for retail billing and for wholesale billing and settlement, which are defined as follows:

- Retail billing: The billing of a service provider's own customers for roaming services. This is the domain of each individual NSP and is dependent on the retail pricing plans NSPs provide their customers.
- Wholesale billing: The clearing and settlement process by which a V-NSP invoices the H-NSP for the usage of its network by the H-NSP's roaming users.

Retail billing is not within the scope of this document. Retail billing is based on accounting information contained in the H-AAA.

The Wholesale billing process can be divided in the following logical functions listed below:

- AAA Proxy
- Wholesale Rating
- Clearing
- Financial Settlement
- Fraud Management

Each of these functions can be performed directly by home and visited NSP, or by a third party on behalf of a NSP. The WRI specification [5] defines standard reference points between each logical function and represents the reference architecture for wholesale billing between WiMAX Roaming partners.

9.2 Accounting

Accounting is the creation and transmission of information related to a WiMAX user chargeable event occurring in a defined period of time. RADIUS ([9]) is used in [2] and [3] to generate and collect accounting information. For roaming users, accounting events used for wholesale billing are generated by the network elements in the V-NSP and then transmitted to the H-NSP. Both H-AAA and V-AAA receive the same RADIUS accounting packets.

9.2.1 WiMAX™ Network ([2] and [3]) Accounting Description

Accounting modes and terminology are detailed in Section 4.4.3.2 of [3]. Online (pre-paid) and offline (post-paid) accounting procedures are detailed in Sections 4.4.3.3 and 4.4.3.4 of [3], respectively. The Wholesale billing process depends on RADIUS messages generated by off-line or on-line accounting.

Note that the process for wholesale billing is the same irrespective of the accounting mode used (i.e. on-line or off-line).

9.2.2 Billing Attributes

The WiMAX Forum NWG Network Architecture [3] defines a number of RADIUS attributes and Vendor Specific Attributes (VSA), used both for authentication and for subsequent accounting. This document describes the recommended attributes which must be included in accounting messages to ensure accurate wholesale billing.

The billing attributes provide information required to account and bill for roaming services. This includes identification of the home network and visited network service providers, subscriber and device identification, date of service, start and stop time by session, throughput as measured in bytes and rate as determined between the two network operators. The WiMAX™ Billing Attributes are detailed in Appendix E.

9.3 AAA Proxy

The AAA Proxy takes raw usage records and performs basic transformations to construct representations of complete events. This process includes the aggregation of partial and interim records. A record is generated on either a per session per record basis based on the applicable business rules. Minimal checks are performed on the format of the records provided to ensure that they can be meaningfully dealt with; most checks are deferred until the Data Clearing process.

9.4 Wholesale Rating

Rating is a function whereby information related to a chargeable event is formatted and a rate is applied based on a tariff per unit.

Once the aggregated usage data is computed, the aggregated/correlated usage information is rated; that is, the rates agreed to by the NSPs and recorded in their roaming agreements are applied. This may be the straight-forward process of applying per-minute or per-byte charges to the usage numbers or may involve more complex rating rules, including volume discounts. With the completion of this process, the usage records are now in complete and (syntactically) valid records in the WiMAX™ specific format that be forwarded downstream.

An additional round of rating (re-rating) may also occur after the Data Clearing process. Re-rating typically occurs to implement more complex discounting rules.

Rating methods of wholesale accounting may include:

- Volume or throughput based on bytes (uplink and downlink)
- Time based
- Per session
- Flat rate for a fixed period of time.

Note: In WRI Release 1.0 flat rate is NOT supported.

9.5 Clearing

Clearing is the process of extracting and validating accounting data to enable financial settlement between a H-NSP and a V-NSP. Validation includes the creation and exchange of summary usage and accounting information between a V-NSP and a H-NSP for reconciliation.

It is recommended that the exchange of clearing information be done on a daily basis. Daily exchange facilitates reconciliation and provides an accurate forecast of in collects and out collects figures during the entire billing cycle. A separate monthly summary is also created for the financial settlement process.

9.6 Fraud Management

Fraud is the illegal use of services on a network by a user and can occur in many forms. Fraud management is the process of gathering, analyzing, and acting on information to eliminate fraudulent activity. Tools, such as, high usage reports and near real-time usage reports help an NSP to detect and take action to curtail fraudulent activity. Records provided by the AAA in near real-time can be used by NSPs to counter fraud.

As RADIUS messages become available in the H-AAA, the home network can start detecting fraudulent activities using correlation of data. It is the responsibility of the home network to take any corrective action when it detects fraudulent activity.

The first release of the WiMAX Roaming Interface will not specifically include Fraud Management.

9.7 Financial Settlement

Financial settlement is the process of settling accounts payable and receivable between an H-NSP and a V-NSP. Net financial positions are established, electronic and machine readable invoices are created and financial settlement between an H-NSP and a V-NSP occurs with the exchange of money.

9.7.1 Netting

For each bilateral roaming agreement between two NSPs, netting occurs by subtracting NSP A's payable position to NSP B from NSP B's payable position to NSP A to determine each NSP's net payable or net receivable position with NSP B (or a zero balance). NSP B follows the same process with NSP A. This results in a simple cash flow management optimization for the NSPs which results in minimizing the transfer of cash between NSPs.

Netting is performed in the currency agreed to in each roaming agreement at the charged rate. In either case, the netted position must be made available by an NSP to its roaming partners. Since this position will change as data becomes available until settlement occurs, it is expected that the most useful form of making this information available will be through an interactive interface as well as a static report generated when the position is passed to Foreign Exchange and Financial Settlement.

The first release of the WiMAX Roaming Interface will not specify any Netting procedures.

9.7.2 Invoicing

Once the positions have been calculated, invoices will be sent to each H-NSP with a payable position. Electronic invoicing files will be sent in all cases, and will be the authoritative reference for any disputes.

Where required, a paper invoice will be sent to satisfy statutory requirements.

9.7.3 Fund Transfer

Once the netted positions are calculated, payment must be sent directly to the V-NSP, or to an escrow account managed by a 3rd party, i.e. a financial clearinghouse.

9.8 Recommendations

The following recommendations are recommended to be followed to facilitate wholesale rating, clearing, and settlement:

- The ability to exchange RADIUS Accounting records with its roaming partners is to be provided.
- All recommended RADIUS attributes as per Appendix E are to be included in RADIUS records exchanged between the visited, home domain or exchange providers.
- The ability to aggregate and correlate RADIUS packets related to users sessions is to be provided.
- The ability to exchange and validate daily summarized rated usage is to be provided.
- The ability to exchange invoices and settle on monthly basis is to be provided.

It is recommended that NSPs use the WiMAX Roaming Interface (WRI) specifications [5] [6] to meet these recommendations.

10 RF and Devices Recommendations

It is recommended that devices support one or more of the WiMAX Forum approved certification profiles. The choice of profiles supported in the device is vendor specific, based on availability of certified profiles and operator requirements.

Devices must support the capability to indicate to users that a device is roaming, e.g. through displaying a roaming icon.

It is recommended that operator supported devices used by roaming subscribers be pre-configured with Operator Preferred NAP list and Operator Preferred NSP list, in order to facilitate automatic Network Discovery & Selection (ND&S) process.

Devices must display all NSPs discovered during manual ND&S to the user.

11 Inter WiMAX Roaming – Pre-Commercial Testing Recommendations

11.1 Introduction and Scope

The WiMAX Forum Network Interoperability Task Group (NWIOT), Technical Working Group (TWG) and the Evolutionary Technology Working Group (ETWG) are responsible for developing test specifications for end-to-end network level interoperability across all the normative reference points as applied across network profiles defined in WiMAX Forum network specifications [2] and [3]. The purpose of the testing is to ensure successful interworking of WiMAX network elements. TWG and ETWG are responsible for developing test specifications for the MAC, PHY and RF layers, TWG for mobile and ETWG for fixed. The goal of the NWIOT, ETWG and TWG testing is for vendors to ensure that their equipment is WiMAX compliant and to ensure interoperability between vendors.

The WiMAX Forum Global Roaming Working Group (GRWG) is developing plans for testing information passed through the WRI reference points. The purpose of the WRI tests is to ensure that information is properly exchanged to track usage and for wholesale clearing, billing and financial settlement between NSPs.

The purpose of this section is to provide a high level overview of pre-commercial roaming testing on live networks. Pre-commercial roaming testing is the testing of devices and services on a visited network and the data exchange and signaling between the visited and home network.

This Section encompasses testing all phases of roaming in a live network environment. As a part of implementing roaming, two NSPs establishing roaming services with each other typically test roaming between their networks. The purpose of these tests is to ensure that all phases of roaming are functioning properly including network discovery and selection, authentication, authorization and access to services as well as billing, clearing and financial settlement. These tests are performed on the NSPs live networks typically using devices that have been exchanged. Section 11.2 describes prerequisites for pre-commercial roaming testing and Sections 11.3 provides a high-level description of the pre-commercial roaming tests.

11.2 Base Line Prerequisites for Pre-Commercial Roaming Testing

11.2.1 Roaming Partners

Prior to executing roaming tests, roaming partners must deploy their WiMAX networks in accordance with technical specifications as defined by [2] and [3], TWG Mobile Profile Release and ETWG.. All relevant network components, including HA, FA, firewalls, routers, AAA, MIP devices, etc, must be properly implemented and configured. NSPs must have test devices that have been validated on the home network and configured for roaming.

11.2.2 WiMAX Terminal Devices

The WiMAX terminal must be able to access the RF frequencies in use by the roaming partner network.

11.2.3 Network Entry

The WiMAX terminal must be able to download and analyze the NSP data presented in the visited network and execute logic to allow a network entry on a NSP that has a connection to the H-NSP. This logic must be able to correctly deal with a shared NAP environment where multiple NSP values will be transferred to

the mobile terminal. Further, it is recommended that the network be able to support the IP connectivity required by the terminal (CMIP, PMIP).

11.2.4 Accounting

The visited Network must be connected with the H-AAA, either directly or indirectly.

The visited Network must be able to route based on realm from the V-AAA to the H-AAA, although this may use an interconnect network.

11.2.5 Regulatory Compliance

There may be differences in regulations which impact the types of services each roaming partner provides on its network. For example, one network may allow mobility, while the other may allow access only on a fixed or nomadic basis. It is expected that the roaming terminal will conform to the local regulatory rules, which must be enforced by the visited network.

11.3 Pre-Commercial Test Scenarios

It is recommended that performance criteria as defined in a roaming agreement or WRI documents be tested. This includes such areas as delay in record transmission and throughput. For a list of recommended pre-Commercial Roaming test scenarios, see [7].

Appendix A – Recommendations Summary Table (Informative)

Table 5 summarizes all recommendations contained in the previous sections of this document. It is worth noting that these recommendations should be interpreted only as "operational" requirements to be met to enable two WiMAX Forum Network compliant operators (see [2] and [3]) to successfully implement roaming with each other.

Table 5 Recommendations Summary

ID	*Description*	*Area*
R-[RG-1]	The roaming partners must use a public Operator ID (OID), as per Section 4.1.2.2 of [3] for NAP-ID and NSP-ID. Use of a public OID ensures its uniqueness and is used for both network entry and identification of the home and the visited NSP to which the AAA accounting messages exchanged via the R5 reference relate to.	ND&S (Section 6.1)
R-[RG-2]	The advertised NSP-ID list must contain only the NSPs that are directly connected to the NAP's network and with which the NAP has a direct business relationship.	ND&S
R-[RG-3]	The valid formats for NAP-ID and NSP-ID are defined in Section 4.1.2.2 of [3]. For example, an operator, which already operates a cellular network (e.g. GSM), is likely to have a NSP-ID that contains MNC and MCC code. If a terminal is allowed to roam from the home operator's network to another operator's network, the home operator must configure the terminal with the other operator's NSP-ID. The format of the NSP-ID in the terminal's roaming list is dictated by the other operator.	ND&S
R-[RG-4]	The list of NSP-IDs presented through the over the air interface (as part of SII-ADV and/or SBC-RSP) must be uniform across all Base Stations of the same NAP ID. (per Section 4.1.2.2 of [3]).	ND&S
R-[RG-5]	A Verbose NSP Names list may be needed if the network transmits a list of Verbose NSP Names through the over the air interface (as part of SII-ADV and/or SBC-RSP), along with the list of NSP-IDs.	ND&S
R-[RG-6]	Configuration needed on the MS/SS:	ND&S
	1. NAP-ID of roaming partners in the 'Operator Preferred NAP' list. List controlled by H-CSN. 2. User Controlled NAP list. List controlled by User, not under the control of any network operator. 3. NSP-ID of roaming partners in the 'Operator Preferred NSP' list. List controlled by H-CSN. 4. User Controlled NSP list. List controlled by User, not under the control of any operator 5. It is recommended that verbose names of roaming partners be available in a pre-configured list (NAP/NSP mapping list).	

ID	*Description*	*Area*
	6. If information useful in MS/SS discovery of NAP, including previously detected and retained values, stored information such as channel, center frequency, and PHY profile is available in configuration information, it is recommended that it be used to improve efficiency of NAP discovery. 7. Mapping Table to map the V-NSP-ID to a realm if needed..	
R-[RG-7]	The network access identifier (NAI) used in WiMAX networks must conform to IETF RFC 4282 [12] and [3]. It is used as an identifier within EAP-based user and MS/SS network access authentication.	AAA (Section 6.2)
R-[RG-8]	It is recommended that the outer-identity be used primarily to route the packet and act as a hint helping the EAP Authentication Server select the appropriate EAP method. The inner-identity must be used to identify the user, or authenticated credentials. EAP methods that provide identity hiding will transmit the inner-identity within an encrypted tunnel created by the EAP method.	AAA
R-[RG-9]	In order to support identity hiding, it must be possible to carry the real identity of the MS/SS in the inner-identity only. For the outer-identity, a psusedonym is used that can be resolved to the real user identity only by the MS/SS itself and the home CSN.	AAA
R-[RG-10]	A V-NSP must be able to resolve an NAI to a valid IP address of the next valid destination for routing of RADIUS packets based on the suffix of the NAI.	AAA
R-[RG-11]	It is recommended that the AAA server authenticate the proxy AAA server to verify it is a valid roaming partner.	AAA
R-[RG-12]	The mobile device may have to authenticate itself using the device certificate to the AAA server, hence confirming the MAC address. The mobile device may have to use other credentials as well.	AAA
R-[RG-13]	The AAA server may execute local policies. These local policies must not interfere with features already defined in the WiMAX Forum NWG specifications [2] and [3] and have to be verified between the roaming partners prior to the commercial launch of roaming services. Note that AAA local policies are beyond the scope of the Roaming Guideline.	AAA
R-[RG-14]	QoS profiles must be provided on a subscriber-basis in the home AAA.	QoS (Section 6.3)
R-[RG-15]	It is recommended that the V-NSP and H-NSP agree in advance, through a roaming agreement, on a minimum QoS profile which will be granted to roaming users in case the requested QoS profile cannot be provided..	QoS
R-[RG-16]	It is recommended that common QoS profiles for roaming users be agreed between roaming partners. Common QoS profiles for roaming users. Common QoS profiles are needed because the support of all H-NSP QoS profiles by a v-NSP may not be practical. For example, “Best Effort Internet services” may include several best effort QoS options, If NSP A is providing a tiered best effort service (different maximum transfer rates), when NSP A users roam onto NSP B’s network, applicable parameters must be provided by NSP A to NSP B.	QoS

ID	*Description*	*Area*
R-[RG-17]	H-NSP and V-NSP must agree on location preference for the HA (in the V-CSN or in the H-CSN). If the HA is in the V-CSN, the V-NSP must verify that sufficient IP addresses are available to accommodate roaming MSs.	IP address management and Mobility (Section 7)
R-[RG-18]	H-CSN or V-CSN must be able to allocate IP addresses to roaming MSs. Moreover, it is recommended that assigned IP addresses not overlap with the address space in the H-CSN or in V-CSN. If the HA is in the V-CSN, the V-NSP must verify that sufficient IP addresses are available to accommodate roaming MSs.	IP address management and Mobility
R-[RG-19]	In case HA is in the H-CSN, both MIP signaling and user traffic (encapsulated in GRE or in IP-in-IP) must be transported to the Home Network.	IP address management and Mobility
R-[RG-20]	Visited and home WiMAX Networks must be able to exchange RADIUS Accounting records with its roaming partners.	Accounting and Settlement (Section 9)
R-[RG-21]	Visited and home WiMAX Networks must be able to include all mandatory RADIUS accounting attributes.	Accounting and Settlement
R-[RG-22]	Visited and home WiMAX Networks must be able to aggregate and correlate RADIUS packets related to users sessions.	Accounting and Settlement
R-[RG-23]	Visited and home WiMAX Networks must be able to exchange and validate daily summarized rated usage.	Accounting and Settlement
R-[RG-24]	Visited and home WiMAX Networks must be able to exchange invoices and settle on monthly basis.	Accounting and Settlement
R-[RG-25]	Devices must support one or more of the WiMAX Forum approved certification profiles. Choice of profiles supported in the device is vendor specific, based on availability of certified profiles and operator requirements.	Devices (Section 10)
R-[RG-26]	Devices must support the capability to indicate to users that a device is roaming, e.g.by displaying a roaming icon.	Devices
R-[RG-27]	It is recommended that operator supported devices used by roaming subscribers be pre-configured with Operator Preferred NAP list and Operator Preferred NSP list in order to facilitate automatic Network Discovery & Selection (ND&S) process.	Devices
R-[RG-28]	If manual ND&S is supported, devices must display all NSPs discovered during manual ND&S to the user.	Devices

Appendix B – Implementation Options - Summary Table (Informative)

As a first step to enable roaming, two NSPs which desire to provide roaming service on each others' networks must share information about their specific requirements and capabilities. This is an important step in determining whether their networks will support roaming services for each other's subscribers. This includes information regarding frequency bands, devices, services and protocols. For example, devices of an H-NSP must be capable of operating on the frequencies and within the channel bands of the V-NSP. Also, devices of an H-NSP must be able to operate using an internet protocol supported by the V-NSP. Two operators must agree on services to be provided, IP address assignment mechanism, method of interconnection, and the format and method for sharing information to track subscriber usage and to exchange information required for billing and settlement.

WiMAX Forum "WiMAX Roaming Agreement 2 (WRA2)" [8] can be used to exchange technical information between roaming NSPs.

The purpose of Table 6 is to summarize specific available deployment options in the various functional areas, to enable WiMAX roaming.

Table 6 Deployment Options

Item	Available Deployment Options	Recommendations covered in Section
Technologies and Spectrum Band:		10
Technologies	Orthogonal Frequency Division Multiplexing Access (OFDMA), Time Division Duplex (TDD), Wireless Metropolitan Area Network (WMAN)	
Specifications	IEEE 802.16-2004, IEEE 802.16-2005 IEEE 802.16-2004/Cor2/D3	
Spectrum Bands	2.3-2.4 GHz, 2.305-2.360 GHz, 2.496-2.690 GHz, 3.3-3.4 and 3.4-3.8 GHz	
Channel Bands	5/10 MHz, 4/7/8.75/10 MHz	
Devices:		
Certification	Certified WiMAX Devices	10
Device Types	Personal Computer Memory Card International Association (PCMCIA), Universal Serial Bus (USB) Dongle, Embedded Devices, Personal Digital Assistants (PDAs), Phones, other	10
MIP / Simple IP	CMIP (optional), Proxy MIP (optional)	7
NAI	Unique NAI	6
IP Assignment – PoA supported	MS obtains the Point of Attachment (PoA) either from a DHCP/AAA server or a HA	7
Services:		
Services Supported	Internet Access	5
QoS	Best efforts, pre-configured on ASN-GW or provisioned by AAA based on user-profile	5, 6

Item	Available Deployment Options	Recommendations covered in Section
Interconnection and Data Path		
Interconnection	VPN, Direct, or via third party exchange	8
Data Path	Established in home or visited network	4
Network Selection and Authentication:		4, 6
Network Selection	Automatic Selection, Manual Selection	
Authentication	EAP-AKA, EAP-TLS, EAP-TTLS	
	Single EAP	
Authentication supported in:	H-NSP	
Network / Infrastructure:		
AAA	RADIUS,	4, 6, 16
Timer	Default Interim Timer	
Tunneling	Reverse Tunneling	
Intra/Inter-ASN Control Plane Protocol and Port	GRE tunneling between FA and HA	
IP address	Public or Private IP address	7
SS/MS – ASN Convergence Sub layer	IPv4, IPv6 (optional)	4, 7
Network Identification	NSP-ID, NAP-ID	4, 6
IP	Proxy MIP, MIP (optional)	7
Realms and NAIs:		
	Include Internatiol Standard Organization (ISO)	6
NAI	and/or ITU Country Code, NSP	
Security		4
	Control-path/data-path encryption/decryption	
	Ipsec[1]	

[1] IPsec is the recommended option: it is not needed when direct connection which are inherently secure are deployed. Other security mechanism as per roaming agreement between the involved parties.

Item	Available Deployment Options	Recommendations covered in Section
Accounting: Basis for Billing	Time based, Usage Based (Kbytes)	9
Format – sharing of billing information	Extensible Markup Language (XML) format	8
Other Time Zone Fraud	Greenwich Mean Time (GMT) time zone offset	16 9

Appendix C – Relation with SPWG recommendations and requirements for Networks based on WiMAX Forum Certified™ Products (Informative)

SPWG maintains the complete list of system and network requirements for WiMAX Forum Networks [2] and [3]. In Section 10 of [1], a list of scenarios and recommendations for roaming and interworking aspects is provided.

Appendix D – NAP Sharing (Informative)

NAP sharing refers to a particular type of deployment of a WiMAX network, in which a single NAP, which owns and operates an ASN, connects to multiple NSPs, which share the radio infrastructure of the NAP to provide network access to their subscriber. A business relationship exists between the NAP and the NSP.

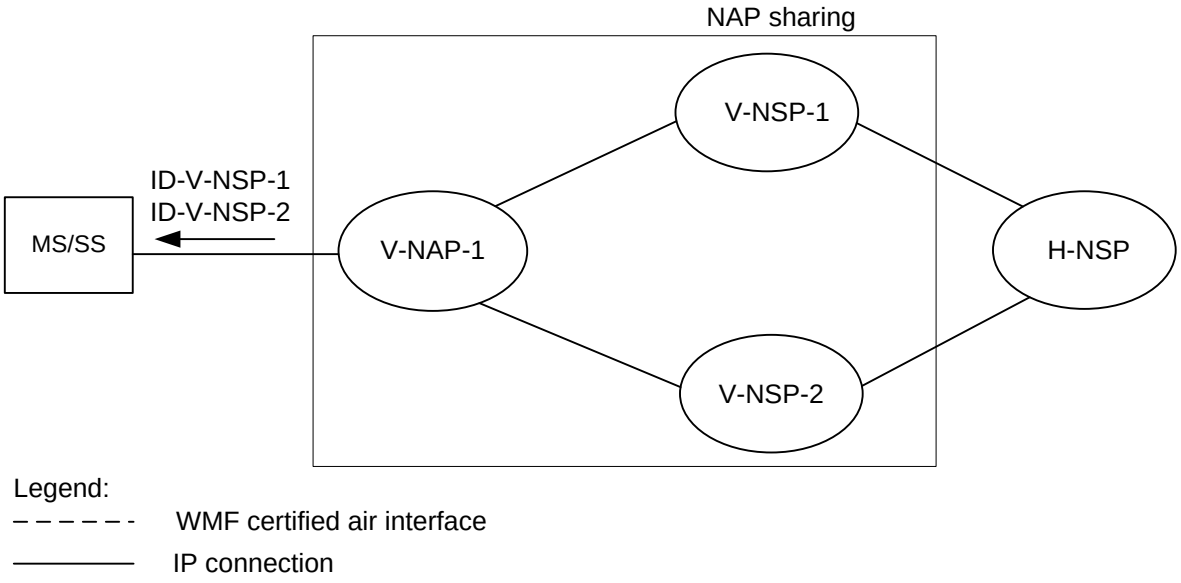

Figure 16 NAP sharing deployment

In case of roaming, NAP sharing enables multiple V-NSP sharing a single ASN to provide access to the H-NSP, with which they have a roaming agreement, as depicted in the following picture:

When the NSP Identifier Flag is set to a value of "1", i.e., NAP-Sharing, the MS/SS must use its NAI with additional information when presented, also known as "decorated NAI", to influence the routing choice of the next AAA hop when the home NSP realm is only reachable via another mediating realm (e.g., a visited NSP). The NAI only needs to be decorated with the routing information when roaming onto a NAP which is shared by multiple NSPs, which provide access to the home NSP.

An example of decorated NAI, constructed as described in [3], is:

homerealm.com!user@visitedrealm.com

Figure 17 shows an example of NAI decoration in a complex roaming environment, where H-NSP is reachable through more NAPs and NSPs. In this case, MS/SS chooses V-NSP-3 and indicates its choice to the V-NAP-2 decorating NAI accordingly.

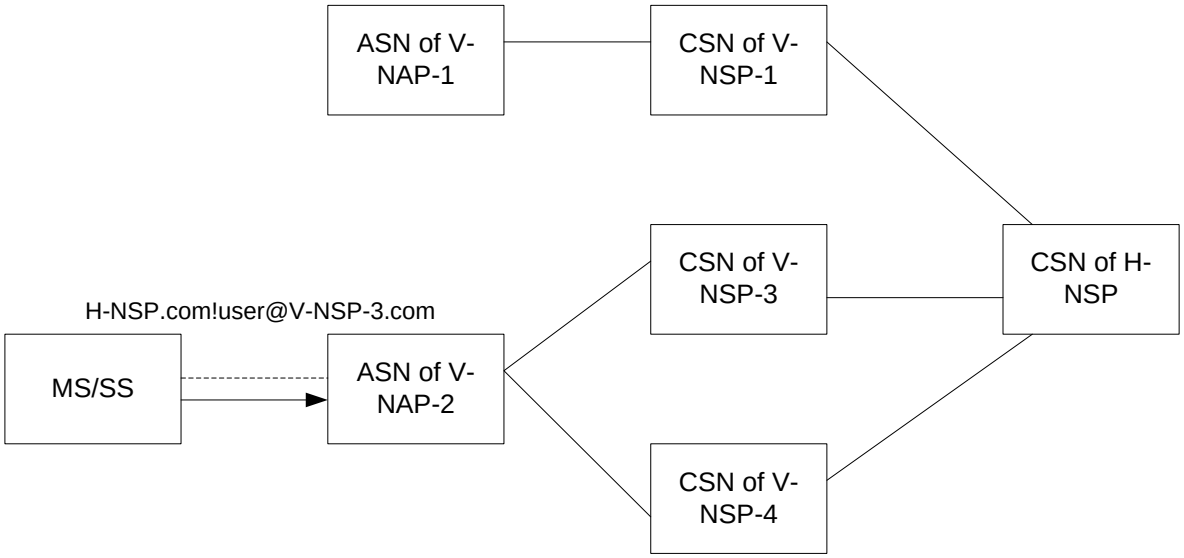

Figure 17 NAI decoration in NAP sharing

The NAI decoration will be handled automatically by the MS/SS either with pre-provisioned roaming partner information or based on user selection.

Functional Recommendations

Additional functional recommendations for NAP-sharing are:

- It is recommended that ASN-GW in the V-NAP maintains AAA and bearer traffic, belonging to the different connected V-NSP, logically separated.
- ASN-GW must be able to route AAA flow on the basis of MS/SS's choice of the V-NSP.

Appendix E – Mandatory RADIUS Attributes For Billing (Informative)

Table 7 Mandatory RADIUS attributes for billing

RADIUS Attribute Name	Number	Description
User-Name	1	The identity and realm of the user used in the outer NAI during network access authentication and authorization
Class	25	Opaque value set by the Server used to bind authentication to accounting.
Calling-Station-Id	31	The MAC address in binary format of the MS
NAS-ID	32	The identifiers of the NAS generating this record.
Acct-Status-Type	40	Indicates the record type: Start, Stop, Interim
Acct-Input-Octets	42	The total number of octets in IP packets sent by the user, as received at the accounting agent from the IP network (i.e. prior to any compression and/or fragmentation).
Acct-Output-Octets	43	The total number of octets in IP packets sent to the user. Counted after de-compression and de-fragmentation at the accounting agent.
Acct-Session-Id	44	Used to match Starts, Stop, and Interim. It is generated by the accounting client and is unique per start/stop pair.
Acct-Session-Time	46	The number of seconds the flow or session was active.
Acct-Terminate-Cause	49	Indicates why the session stopped.
Acct-Multi-Session-Id	50	This identifier is set to the value of WiMAX-Session-ID which is generated by AAA after successful initial network entry with authentication. It is delivered to the NAS in an Access-Accept message. It is unique per CSN and is used to match all accounting records within a session.
Acct-Input-Gigawords	52	Incremented when attribute 42 overflows
Acct-Output-Gigawords	53	Incremented when attribute 43 overflows
Event-Timestamp	55	Indicates the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 Coordinated Universal Time (UTC).
CUI	89	Chargeable User Identity (CUI). It is a unique temporary handle to the user responsible for paying the bill.
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the NAS or HA.
Session-Continue	26/21	True indicates that the stop is immediately followed by a start. If the attribute is missing or FALSE it means that this is the final stop.
IP technology	26/23	Proxy CMIP4, PMIP4
Active-Time	26/39	The time in which the MS is active as opposed to idle mode. Account-Session-Time minus Idle
NAP-ID	26/45	An octet string that uniquely identifies the operator that generated this User Data Record (UDR). This value is configured at the Accounting Client and can be used for charging settlement between NSP and NAP.
BS-ID	26/46	An octet string that uniquely identifies a NAP-ID and a Base Station that is serving the MS at the time the UDR is generated.

RADIUS Attribute Name	Number	Description
Location	26/47	TBD
NSP-ID	26/57	The operator ID identifying the NSP operator at the time the message was delivered

Revision History

Revision	Changes	Date
1	Initial Publication	October 17, 2008
2	Made the following modifications 1) Reference Section a) Added TCC document numbers to WiMAX Forum document b) Added References WRI Stage 2, WRI Stage 3, Pre-Commercial Testing and IETF RFC 4372. c) Organized WiMAX Documents and IETF RFCs in numeric order d) Renumbered the references 2) Made Trademark changes throughout the document including the header 3) Removed Pre-commercial test cases and sections and referred to Pre-Commercial Tesing document. 4) Modifications to Figures a) Figure 4. In WRX drawing, changed AAA to AAA Proxy b) Figures 5, 6, 9, 10, 11, 12, 13, 16, 17: Changed 'MS' to 'MS/SS' or 'Mobile Station' to 'Mobile Station/Subscriber Station' 5) CRs: a) As per WRI Stage 3 AAA Proxy Comment Resolution – Comment 1594, changed AAA-Session-ID to WiMAX-Session-ID b) To address WRI Stage 3 AAA proxy comment resolution 1591: Changed homerealm to home c) As per Roaming Guideline Release 1.0 Comment 753, the text in Section 6.1.2 needs to be updated once the RG is to be aligned with a later version of NWG Network Architecture Release 1.0 version 1.2.2. The text should read: "The list of NSP IDs and verbose NSP names presented over the air interface as part of SII-ADV and/or SBC-RSP and all NSP realms that can be obtained using SBC-REQ/RSP SHALL be uniform across all Base Stations of the same NAP ID." c) Added the following sentence to Section 9.7.1 Netting: "The first release of the WiMAX Roaming Interface will not specify any Netting procedures". 6) Editorial changes: a) NAP ID is changed to NAP-ID b) NSP ID is changed to NSP-ID c) Changed MS to MS/SS were appropriate d) Changed WiMAX to WiMAX networks or WiMAX System e) Section 16 to Appendix E f) AAA proxy to AAA Proxy	April 28, 2009
2	Made the following modifications: 1) Reference Section a) Introduced WRI Code document and renumbered the references. The text was updated. b) Changed FROM: Use of a public OID ensures its uniqueness and is also used for both network entry and wholesale billing procedures. TO: Use of a public OID ensures its uniqueness and is used for both network entry and identification of the home and the visited NSP to which the AAA accounting messages exchanged via the R5 reference relate to. In the WiMAX™ Roaming Interface	May 10, 2009

Revision	Changes	Date
	Architecture [5] [6], the WiMAX™ Roaming Interface (WRI) Code is included in information exchanged between WRI logical entities to uniquely identify the home NSPs, visited NSPs, and the sending and the receiving WRXs. The first three characters of the WRI Code represent the country the operator or the WRX is operating in or are assigned by WiMAX Forum while the remaining three characters identify the operator or the WRX. The WiMAX Forum administers and issues the WRI Code. Additional information on the detailed use of WRI code and application procedures are detailed in [2][3] and [4] respectively.	
2	Changes include: a) Editorial recommended during May 11, 2009 Dublin Meeting b) A Note that Flat Rate is NOT supported in WRI Release 1.0 c) Removed CMIP6 from IP Technology in Table 7 to align with [3] d) Added UTC to the list of Abbreviations e) Aligned Acct-Multi-Session-Id with description in [3]	May 11, 2009
2	Approved by WiMAX Forum Board of Directors	June 24, 2009