4

WiMAX Network Security[1]

Luca Adamo, Romano Fantacci and Leonardo Maccari
Department of Electronics and Telecommunications – University of Florence

4.1 Introduction

The possible usage scenarios of a WiMAX service network are extremely various. The network can support static and mobile users roaming in a metropolitan area, the kind of traffic can be the typical Internet browsing or real-time traffic with stringent QoS constraints. The components of a WiMAX network must assure that all these needs are fulfilled. To reach this goal, all the layers of the OSI stack are required to co-operate in order to guarantee security, session establishment, fast handover and correct quality levels.

The IEEE 802.16 family of standards is focused on the radio and MAC layers so it doesn't give any indication on how to manage the networking back-end. Nevertheless a WiMAX network can be composed of many distinct and heterogeneous elements: mobile stations, base stations, gateways, authentication servers that need to cooperate in a multi-user, multi-terminal and even multi-operator scenario. In order to define an interoperable network organization the WiMAX Forum [1] has produced a set of documents that specify the network elements, organization and configuration that must be deployed in a WiMAX network ([2], [3]).

[1] The topic presented in this chapter has been subject of investigations partially supported by the Italian National Project *Wireless multiplatfOrm mimo active access netwoRks for QoS-demanding muLtimedia Delivery* (WORLD) and FIRB *Integrated System for Emergency* (InSyEme) under Grant 2007R989S and RBIP063BPH.

WiMAX Security and Quality of Service: An End-to-End Perspective Edited by Seok-Yee Tang, Peter Müller and Hamid Sharif
© 2010 John Wiley & Sons, Ltd. ISBN: 978-0-470-72197-1

In this chapter an overview of this organization will be given, based on the WiMAX Forum specification 1.2. The focus of our description will be the standards, the technical challenges and the solutions for mainly three issues:

- integration of authentication techniques and management of AAA (Authorization, Authentication, Accounting);
- IP addressing and networking issues;
- distribution of the QoS parameters.

These topics will be analyzed not from a MAC layer perspective but from the point of view of the network manager and of the interaction between the access network and the back-end.

4.2 WiMAX Network Reference Model

In order to understand completely the relationships between all the network components a logical representation of a WiMAX network must be introduced. Such a scheme is provided by the WiMAX Forum in [2] under the name of NRM (*Network Reference Model*) and distinguishes the *logical domains*, the *functional entities* and the *Reference Points* (RPs) as reported in Figure 4.1.

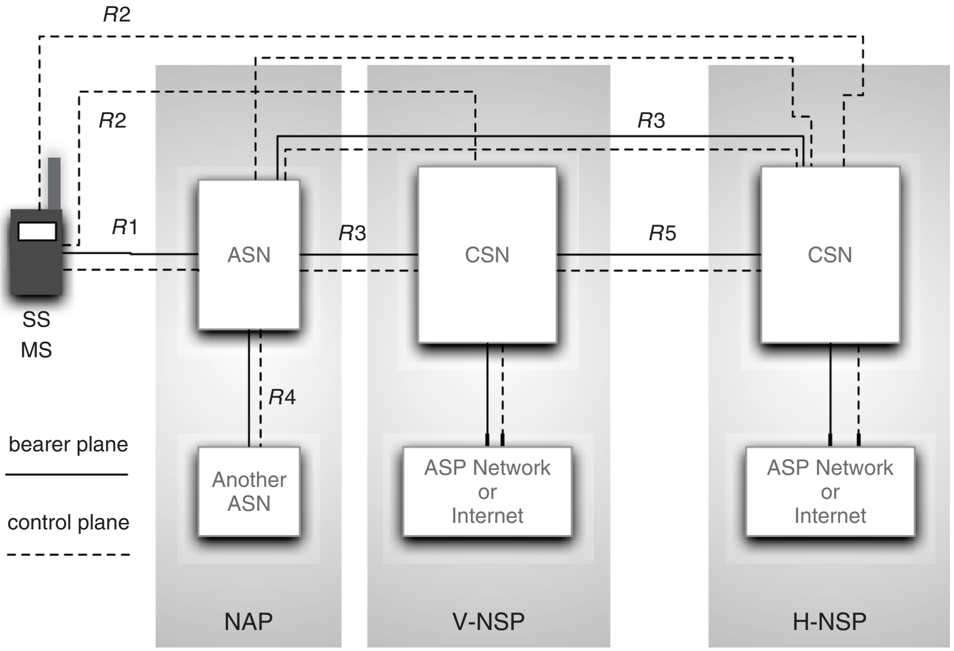

Figure 4.1 WiMAX network reference model.

The NRM is a logical model rather than a precise definition of a network architecture; the goal is to allow a variety of implementation solutions while maintaining an overall interoperability among different realizations of functional entities. For this reason no assumptions are made on the implementation of the functional entities. For some of them, however, guidance is provided through the so called *profiles* that we will describe later on. The following sections illustrate the most relevant components of the NRM.

4.2.1 Functional Entities

The main functional entities depicted in Figure 4.1 are:

- MS, *Mobile Station*. The MS is the generic device used by the subscriber to access the WiMAX network. The same device can be used by more than one user and the same user can access the network with more than one MS. Some configuration parameters can depend on the couple MS, user.
- ASN, *Access Service Network*. The ASN represents a boundary for functional interoperability with WiMAX clients and WiMAX connectivity services. It is mainly responsible for handling the layer 2 connectivity plane, forwarding all the AAA messages towards the H-NSP (Home Network Service Provider), relaying layer 3 service messages (e.g DHCP and Mobile IP). The logical decomposition of an ASN is shown in Figure 4.2. The two most relevant components of the ASN are the radio BS and the ASN-GW. The ASN-GW is the gateway to the IP network and the end-terminal of RP3 as described later on.

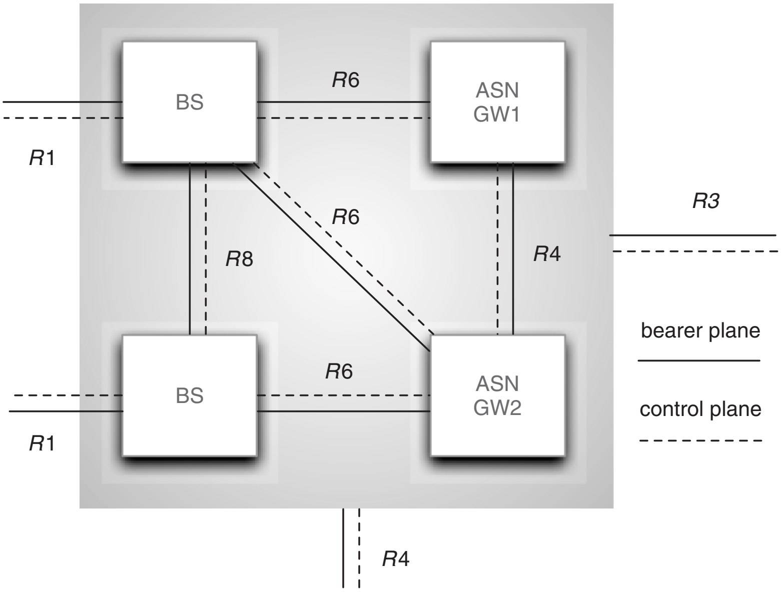

Figure 4.2 WiMAX network reference model, ASN decomposition.

- CSN *Connectivity Service Network*. The CSN is the entity entitled to the management of the IP layer 3 connectivity of the subscribers terminals. More specifically it covers the following tasks:
  - IP address provisioning;
  - gateway towards other networks;
  - performing AAA functions;
  - handling the *Inter-ASN Mobility* through the use of *Mobile IP*.

A MS, ASN or CSN are made up of logical functional entities that may be realized in a single physical host or may be distributed over multiple physical hosts.

4.2.2 Logical Domains

A logical domain can be seen as a group of functions that can be associated in a single domain. In Figure 4.1 three logical domains are presented.

- NAP, *Network Access Point*. The NAP is the physical point used by the subscriber terminal to access the network; from a logical point of view the ASN that is currently serving the MS is part of the NAP.
- H-NSP *Home Network Service Provider*. The H-NSP is the WiMAX service provider with which the WiMAX subscriber has a Service Level Agreement. This business entity authenticates and authorizes subscriber sessions and is responsible of the billing and charging procedures even in a roaming scenario where the subscriber is moving through various NSPs.
- V-NSP *Visited Network Service Provider*. A visited NSP is a WiMAX service provider that a subscriber uses to access the network in a roaming scenario even if there is no Service Level Agreements among the two parts. If the V-NSP has a roaming relationship with the H-NSP the V-NSP can be used to forward AAA messages from the subscriber to the H-NSP thus gaining access to the network on a foreign domain. The range of services provided to the subscriber by the V-NSP depends on the roaming relationship between that V-NSP and the subscriber's H-NSP.

4.2.3 Reference Points

Referring to Figure 4.1 a RP is the end-point of the communication between two functional entities and it constitutes the standard interface that must be used to achieve overall interoperability among components of different manufacturers. The WiMAX Forum specifications [2] list several RPs in the NRM and also provides three examples of implementation profiles. Each profile includes only a subset of these RP. We describe here the most relevant RPs defined in the NRM, to help the reader to understand the rest of the chapter:

- *Reference Point R1*. R1 consists of the protocols and procedures used on the air interface between MS and ASN as defined in [4], [5] and [6]. It is the radio and MAC WiMAX interface.

- *Reference Point R3*. R3 is an interface between an ASN and a CSN (operated either by a H-NSP or a V-NSP). These two functional entities use this interface to vehiculate AAA messages, policy enforcement messages and Mobile IP mobility management capabilities. This interface is in practice an IP link supporting the RADIUS protocol and the gateway for user data.
- *Reference Point R4*. R4 is responsible for the communications between two ASNs that are managed by the same CSN. For instance, when a MS performs an handover between two ASNs into the same NSP the AAA phase could be avoided using communication over this interface.
- *Reference Point R5*. R5 defines and assures inter-networking functions between CSNs operated by H-NSP and V-NSP. This interface in practice will be an IP path that could be routed across dedicated or even public networks.
- *Reference Point R8*. Within an ASN with multiple BSs, R8 is the reference point used to support fast and seamless handover of the MSs.

4.2.4 ASN Profiles

Referring to the logical architecture shown in Figure 4.2 three possible implementation options are proposed and analyzed by WiMAX Forum specifications. These options are called *Profiles* and differ for the number of RPs exposed and for the grouping of some of the logical functions. In Figures 4.3 and 4.4 we report two ASN profiles proposed by the WiMAX Forum with the intent to guide the implementation of the ASN in two of the most common configurations. In the figures we omitted some of the modules that WiMAX Forum describes but that are out of the context of this review.

Profile A, shown in Figure 4.3 will be used in a configuration where a single ASN-GW is responsible to manage multiple BSs. This configuration is suitable in scenarios where it is necessary to cover a large area or to serve a high number of users. Mobility is completely handled by the ASN-GW that controls subscribers handovers over R4 reference point (ASN-anchored mobility).

Profile B shown in Figure 4.4 describes a configuration with a physical co-location of ASN-GW and BS where all the functions of the ASN are included in a single entity with an advantage in terms of complexity reduction. The drawback is that this solution implies a 1:1 ratio between ASN-GW and BSs and for this reason is appropriate only for scenarios with a small number of users dislocated in a localized area.

The function decomposition depicted in both Figure 4.3 and Figure 4.4 evidences the presence into the ASN of the entities used to support AAA procedures, MIP (Mobile IP) compliant mobility and DHCP (Dynamic Host Confguration Protocol). The different location of these entities is the most important element to be noticed when comparing the two profiles.

The choice of a profile must be guided by the extension of the coverage area and impacts on the costs and on the software and hardware solutions. For instance, using profile A the network manager may adopt hardware and software from different vendors, and could face configuration inconsistencies or incompatibilities. Using profile B these issues are avoided (R1 and R4 are standard and widely used interfaces) but scalability is limited.

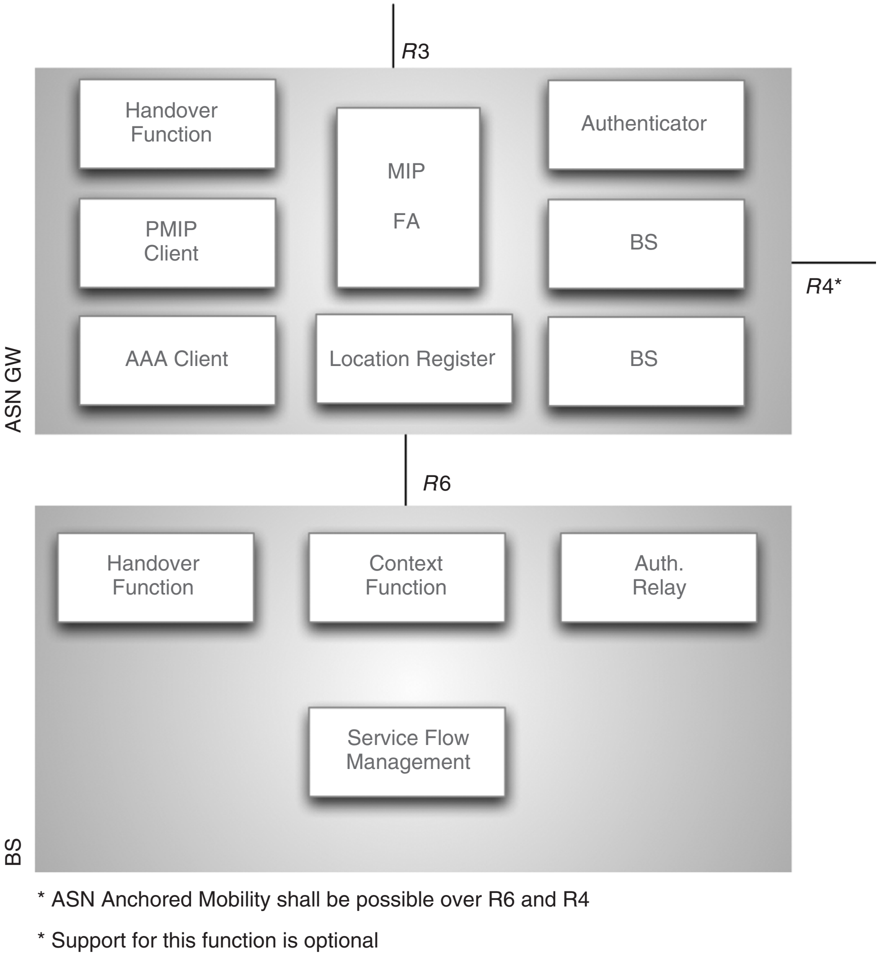

Figure 4.3 WiMAX network profile A for ASN implementation.

4.3 The RADIUS Server

In any network configuration model it is included an *AAA server* where AAA stands for *Authorization, Authentication, Accounting*. The de-facto standard protocol for AAA is RADIUS (Remote Authentication Dial-In User Service) [7]. A successor of RADIUS is the DIAMETER protocol [8] that is currently under definition and will be supported in the future by the WiMAX Forum. The AAA server is used at any user login and plays three functions:

- Authorization: in this phase the received request is parsed and its validity is checked. Possible actions that can be taken are to accept the request (that is passed to the following modules), to reject the requests or to forward it to another server. A request could be rejected because the user that generated it was not allowed to, or because

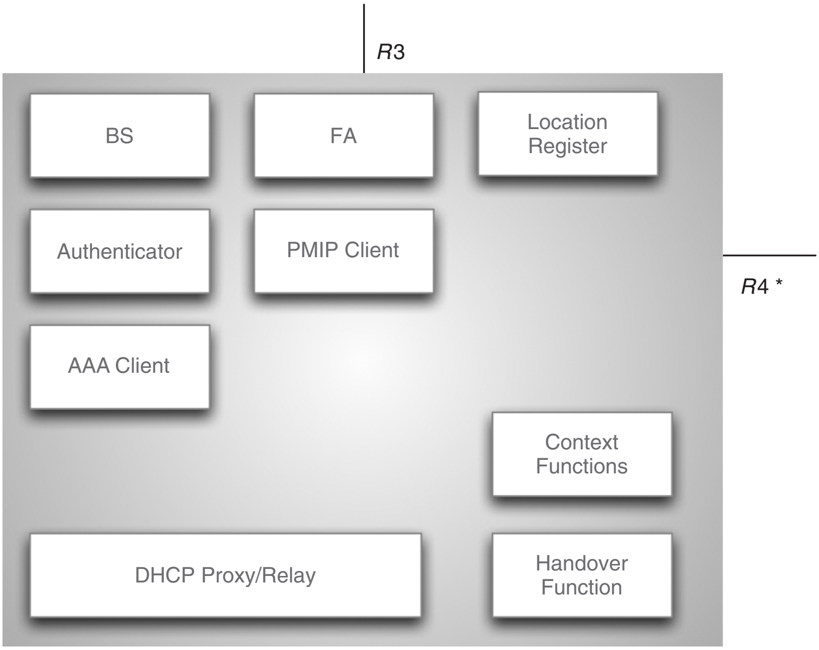

Figure 4.4 WiMAX network profile B for ASN implementation.

the ASN from which it comes has not correctly signed the packet. A request could be forwarded because the AAA server observes that it is not able to satisfy it. A request carries a username in the canonical form *user@domain*, if the server is not responsible for the specified domain it will forward the request to another authoritative server. This is particularly important in large metropolitan networks where users might be roaming from one operator to another. Since only the user's original operator owns the database containing the authentication credentials (i.e. password or certificates) the request must be forwarded to the H-NSP. The same applies to QoS parameters; the visited operator is not aware of the QoS properties that the user has negotiated with his own operator so they must be received from the H-NSP.

- Authentication: the user has to show that he is in possession of valid credentials to enter the network. At the same time the network must present valid credentials to the user in order to assure him that he is entering the correct network. This procedure is particularly delicate and will be explained more in detail.
- Accounting: this function is necessary to the manager of the network to record the activities of the users. The server receives from the ASN accounting packets that include the number of users, the start and end of user sessions or the resources occupied. All this information will end in a database that will be used mainly for billing purposes.

4.3.1 Authentication in WiMAX Infrastructure

The IEEE 802.16 standard supports two distinct authentication procedures, the first one was introduced with the *d* amendment of the standard and it is called PKMv1 (Private Key

Management version 1). Starting from IEEE 802.16e a new one has been proposed called PKMv2. PKMv1 doesn't rely on the use of an AAA server, the authentication algorithms are designed ad-hoc for WiMAX and it has been shown to be insecure [9] [10]. In PKMv1 each subscriber station is equipped with a couple of digital certificates that can be used to perform the authentication: one is inserted from the manufacturer and another that is user-dependent. The first one is signed by a CA owned by the manufacturer and is used to verify the hardware address of the device. This detail is particularly important and innovative compared to other existing standards. It is in fact very common for Ethernet or WiFi networks to perform address spoofing also at MAC layer, since most of the commercial network interfaces give to the user the possibility to change its own MAC address. As an example, most of the commercial IEEE 802.11 access points support MAC filtering and web-based authentication that binds the used credentials (username and password) with the MAC address that is accessing the network. In WiMAX this weak security measure is strengthened using digital certificates.

Nevertheless PKMv1 is subject to many insecurities, the most significant are:

- The authentication is unidirectional, meaning that the base station never authenticates itself with the client. The client could be led to enter a rogue network placed by an attacker.
- There is no form of authentication for some of the packets, this leads to the possibility for an attacker of replying authentication packets or personifying the base station.
- The lack of support for a centralized server is a great limitation to the deployment of large area networks where a set of base stations are managed by the same network administrator.

To address these issues PKMv2 has been introduced that adopts the IEEE 802.1X [11] port-based access control standard. Briefly, IEEE 802.1x determines the three roles that perform an authentication, a *supplicant* that is the client, an *authenticator* that is embedded in the access infrastructure (an ASN in WiMAX) and the *authentication server* that is the AAA server and resides in the CSN. In IEEE 802.1x the *authenticator* doesn't have any specific role into the authentication and acts as a proxy to the AAA server that owns the credentials of the clients and can verify them. No specific authentication algorithms are described in IEEE 802.1x, the EAP protocol [12] is used to transport a set of existent authentication protocols that can be password or certificate based.

The WiMAX Forum gives precise directives for the application of IEEE 802.1x standard into WiMAX networks: mandatory authentication methods are TLS [13] (Transport Layer Security), TTLS (Tunneled Transport Layer Security) [14] and AKA (Authentication and Key Agreement) [15], authentication must be bidirectional, support for OCSP (Online Certificate Status Protocol) [16] protocol is requested and keying material must be generated during the authentication to be reused in other security procedures, such as DHCP [17] or MIP [18]. Given the presence of digital certificates on the devices, user and device authentication is encouraged.

One of the turning points introduced by the WiMAX Forum architecture is the presence of the AAA server not only for authentication but for the distribution of user-based attributes to other network elements. The authentication is the only standard procedure that can be used by the client, the ASN and the CSN to negotiate parameters for MAC and IP layers. When the authentication has success the AAA server will attach to the Access-Accept RADIUS frame more RADIUS *attributes* (that's the terminology used by RADIUS protocol) that will be used by other networking elements. These attributes mostly deal with:

- QoS parameter that will be used by the BS to assure sufficient layer II resources.
- IP parameters, such as a static IP address, or the address of a DHCP server or MIP home agent address.

The possible configurations of a large area WiMAX network, and consequently the variables needed to configure an MS are many and theoretically an ASN could support them all. When a terminal enters the network the BS must be informed on which is the kind of authentication requested for the client, if it owns a static IP address or it uses DHCP, if it supports mobile IP and which in case are the addresses of its home or foreign agent. These parameters can be statically configured on each ASN with great scalability limitations. In a large network these parameters must be provided to the ASN elements when the authentication takes place, since the authentication is the only standard procedure that involves the CSN of the network. It is crucial to understand the role of an AAA server in a WiMAX network because it is responsible to distribute these pieces of information.

One more detail to focus on is that the presence of embedded digital certificates into the terminals can be used to perform a two step authentication, one for the device and another for the user. The TTLS protocol for instance is made up of two phases, the so called *outer authentication* that is certificate based and can be unidirectional or bidirectional and the *inner authentication* that is generally used to transport user/password challenges. Using TTLS the AAA server is not only authenticating an user but it is authenticating the user on a specific terminal. Some of the network parameters could be depending on the user, some other could be linked to the terminal or to the couple (user, terminal). This way the same account could be used for a home connection or for a mobile connection, with distinct quality and billing features.

4.4 WiMAX Networking Procedures and Security

This section provides an overview of the most important networking procedures used in a WiMAX architecture. First of all we discuss the handover phase, then the IP address provisioning problem is addressed presenting both DHCP and Mobile IP and the requirements that these two protocols introduce on the AAA implementation. The last part of the section is devoted to QoS considerations and to an analysis of the authentication mechanism.

4.4.1 Handover Procedure

A mobile station in WiMAX is free to change its point of attachment to the network to perform an handover. Two distinct kinds of handover can be performed by an MS: ASN-anchored or CSN-anchored. Referring to Figure 4.1, in the first case the mobile station is moving from a BS to another that resides in the same ASN. The ASN-GW to which each BS is connected is the same, so that there is no need to update routing tables or network address. In this case the handover is managed by the entities into the ASN and does not have impact on the IP layer. In the second case the MS is moving from an ASN to another. The CSN connected to both the ASNs could be the same, if the new ASN belongs to the H-NSP or another if the new ASN belongs to a V-NSP. In this second case the new CSN will behave as a proxy towards the previous one and the result will be logically the same.

Recall that an ASN is not a monolithic component but it is composed of many sub-modules. Those sub-modules can be physically placed in the same host as depicted in Figure 4.4 or separated as in Figure 4.3. Changing the point of attachment for a MS means changing the BS but depending on the chosen configuration might imply the change of other functional entities such as the authenticator or the MIP FA (Mobile IP Foreign Agent). In the following part of the chapter we will always refer to CSN-Anchored mobility since it has direct consequences on the networking layer.

A WiMAX network should be able to deal with roaming users that need to keep their sessions alive when they perform a handover. Two prerequisites to maintain the sessions active are: to keep the same IP address across handovers and to update the reverse routes from the remote destination to the MS. This tasks can be performed using the Mobile IP protocol for MSs that have support for this standard. If the MS supports only DHCP, then the same result can be obtained combining the DHCP protocol for the MS and an instance of MIP protocol that runs only on the back-end. These two options and their security implications will be described in the rest of this chapter.

WiMAX aims to be the first wireless mass technology that is targeted to mobile, IP-based, real-time application for large area networks. The WiMAX Forum addressed some networking issues using a composition of standard protocols adapted to resolve specific WiMAX problems. One of these issues is that there is no standard and commonly used way to move configuration parameters from a centralized server to a MS. In general, whenever a MS enters a network (for its first time or during an handover) the authentication procedure is the only phase in which the user, the mobile terminal, the ASN and the CSN are forced to communicate. This is the only moment in which authentication, networking and IP parameters can be moved from the management back-end to the rest of the network. In practice this happens with the following scheme:

- The parameters for a specific terminal or end-user are stored in a DB that the RADIUS server has access to.
- The parameters are moved to the authenticator using RADIUS attributes over R3 and possibly R5.
- From the authenticator, using custom protocols they are moved to other network elements, for instance, QoS parameters are moved to the BS together with the MSK key that has been negotiated during the authentication.
- If some of them must be transmitted to the MS they are inserted into DHCP extensions that will be used for the MS over R1.

Note that the RADIUS protocol is the only standard mean to move parameters from the CSN to the ASN. Into the ASN the endpoint that manages them is the IEEE 802.1x authenticator, that is encharged to dispatch them to the other entities, such as the DHCP server or the BS. This composition of protocols is completely backward compatible but has two limitations: it is quite complicate and it is fully concentrated into the authentication phase. This means that if later on in the communication some parameters need to be changed (such as QoS parameters) there is now no standard way of renegotiating them if not triggering a new authentication. Depending on the authentication protocol used, on the network configuration and on the network load the authentication can last up to a few seconds in which the MS is disconnected, since it has no valid cryptographic keys active. Summing up, the renegotiation of a parameter is a costly operation that has not been addressed in the present version of the WiMAX Forum specification. In the future version (version 2.0) higher level protocols for this task will be designed.

4.4.2 DHCP

An MS that doesn't support the MIP protocol may have a static preconfigured IP address or may use DHCP protocol to obtain a new one at each handover. Even in the first case the handover can not be transparent to the IP layer since other network parameters need be updated. In particular on the client side the MS will have to update its route to a new default gateway or the IP address of a Domain Name Server (DNS) present in the new network. There is no other standard protocol to move these parameters to the MS if not using standard DHCP protocol, so that even a MS configured to have a static IP address will need to use DHCP protocol.

At the end of a successful authentication the ASN is still not aware if the MS is MIP-compliant or not. The distinction is based on the MS actions, if the first packet sent by the MS is a DHCP DISCOVER frame, the ASN will conclude that it is a DHCP compliant station, if the frame is a MIP registration request it will conclude that it is a MIP-compliant station. In the first case it will have to activate DHCP and possibly PMIP procedures as described in the next section.

DHCP protocol can be configured in a WiMAX network in two ways, using a DHCP Relay or a DHCP proxy. In the first case the correspondent entity into the ASN doesn't act as a DHCP server but forwards the request to a remote server. In the second case it's the ASN itself that answers to the DHCP REQUEST frame and assigns the IP address to the MS. Recall that if the session must be kept active the IP of the MS must be the same before and after the handover. If the DHCP server is acting as a Relay its role will be to forward the DHCP REQUEST to another server that must be the same one that the MS used in its first authentication. The DHCP Relay may not know the IP address of this server, so this information must be included in some way into the information that the ASN receives at the end of the authentication, that is, in a RAIDUS attribute. This configuration parameter could also be pre-configured in the ASN but such a policy is not usable in multi-operator networks, in which the client may be coming from a foreign network.

Similarly, if the ASN is configured to behave as a DHCP proxy it will need to answer to the DHCP DISCOVER with the same IP address that the MS was using before the handover. A DHCP DISCOVER could be carrying a specific option that is used by the client to ask to be assigned a specific address that is already using. For security reasons this decision can not be based on the IP that the MS requests for itself since the DHCP frames are unauthenticated and an MS could be trying to achieve someone else's address.

Again, the IP address to be assigned to the MS will be included into a specific RADIUS attribute included in the Access-Accept packet coming from the CSN.

4.4.3 Security Issues

In the depicted scenario an attacker that is able to intercept and modify the DHCP packets that are forwarded from a DHCP relay to a remote DHCP server could produce severe security problems. For instance, he could change the default gateway to perform man in the middle attacks, or modify the DNS server in order to redirect the MS to fake websites. This possibility is concrete in WiMAX networks since there is no a-priori trust between the DHCP relay and server. It can not be assumed that other security measures such as virtual private networks are deployed to secure those paths.

To address this issue the DHCP protocol has a security extension that allows to authenticate the frames from a relay to a server. This security extension is based on the knowledge of a symmetric shared key called DHCP-RK. From this pre-configured key specific ones are derived to secure each single session. To be able to support dynamic redirection of the DHCP requests the DHCP-RK key must be dynamically moved into the DHCP Relay and into the DHCP server when needed. Again this is achieved using RADIUS attributes, but in a more complicated manner. The first complication resides in the fact that RADIUS is used for MS authentication but the DHCP-RK key is not MS-related. The key is related to the couple (DHCP Relay, DHCP Server) and can be used to configure more than a MS. Moreover, the remote DHCP server is not in the logical path of the authentication, so it will not receive the DHCP-RK with an AAA message during the authentication. The WiMAX Forum specifies the following behaviour, as depicted in Figure 4.5:

1. During the authentication the CSN generates a random key and internally assigns that key to the DHCP server involved into this session.
2. Together with the Access-Accept packet the ASN receives a RADIUS attribute containing the DHCP server IP, the DHCP-RK, the lifetime of the key and a unique ID.
3. The DHCP relay in the ASN will use this key to secure the DHCP DISCOVER frame that is sent to the server. The DHCP server will receive a DHCP DISCOVER including the Auth. suboption based on a key with the specified ID.
4. If it owns the key it will use it to verify the signature, otherwise it will issue a RADIUS request to the RADIUS server asking for the key. The RADIUS server will in turn respond with the DHCP-RK.
5. The DHCP server can answer to the request and the DHCP procedure be completed.

A few issues deserve to be detailed. Step 1 is performed when the RADIUS server is using a DHCP server for the first time, or when the lifetime of a previous key has expired. Similarly, step 4 is performed by the server if it has not interacted with the Relay before, or if the lifetime of the key has expired. The DHCP server has to embed a RADIUS client to be able to satisfy the request and the RADIUS protocol is used in an unconventional way. Generally an authenticator has an embedded RADIUS client to transport authentication packets that come from a supplicant. The supplicant uses an username to authenticate against the RADIUS server. In this case there is no real

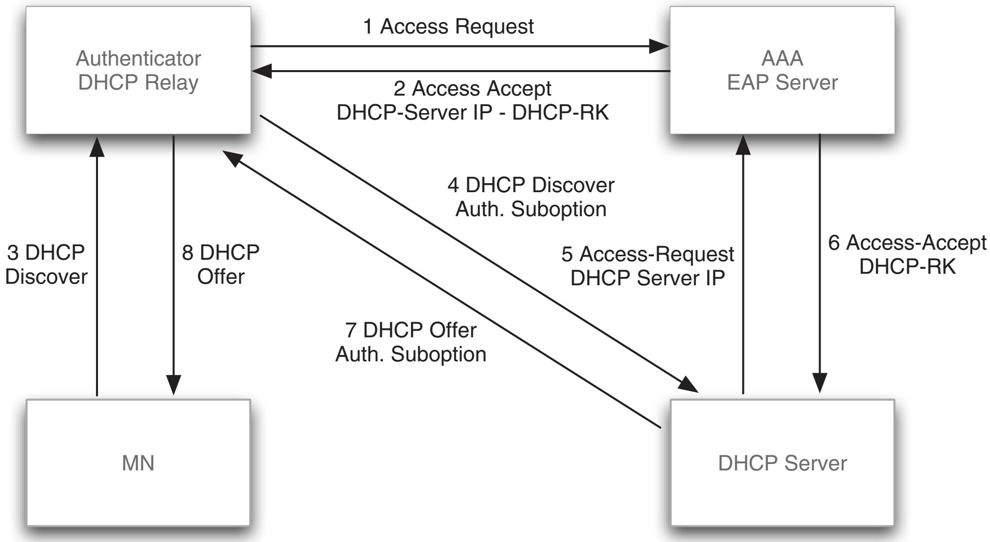

Figure 4.5 Key exchange for DHCP protocol key management.

user that has to perform any authentication, but the RADIUS frames carry requests that come directly from the a unique entity comprised of client and authenticator. This issue, together with the need for the server to store a key and redistribute it later on (recall that RADIUS is in principle a stateless protocol) has an impact on current RADIUS implementations.

4.4.4 Mobile IP Protocol

Mobile IP [18] is an Internet Engineering Task Force (IETF) standard communications protocol described in IETF RFC 3344 and IETF RFC 4721 whose main intent is to allow a user to have a permanent IP address while moving and changing his point of access to the network. This feature is highly valuable for all those connection oriented services that need a permanent connection during the user roaming through the network.

In the previous section we have explained how it is possible using DHCP to keep the same IP address during an handover. This is necessary to keep sessions active but it is not sufficient. The other end of the communication will receive IP packets but its replies will be routed to the home network of the node. The mobile IP protocol takes care of forwarding the packets from the home network to the visited network.

The Mobile IP protocol resolves the session persistence problem using two addresses for every terminal: an *home address* and a COA *Care-of-Address*. The home address is the IP address the node has got from his HA (Home Agent) on his home network; this IP address is the one that will remain fixed while roaming. The COA is the address given to the node by a FA (*Foreign Agent*), a mobility agent that has in charge the IP provisioning of the terminals attached to a V-NSP.

The way Mobile IP works can be briefly resumed as follows:

1. At the time of its first authentication an MS gets an IP address from the HA in his home network. Until it remains under the coverage of this network the datagrams to and from that node are routed simply using this address and the Mobile IP protocol is not used.
2. When a mobile terminal moves away from his home network to a different one it searches for a FA and receives a COA from this agent.
3. After the COA assignment, the MS starts a Mobile IP registration towards his HA using the Mobile IP RRQ *Registration Request* standard procedure. This registration has the intent to inform the HA about the current COA that should be used to reach the terminal on the visited network. To confirm that the registration has been received the HA sends back a RRP *Registration Reply*.
4. The path to and from the MS must be changed after the registration in the foreign domain. When the mobile terminal wants to communicate to a remote terminal it uses a direct route from its new network. When a correspondent node wants to communicate with the mobile node it has to use the *triangular routing* technique sending the IP datagram to the home address of this node. The HA will receive this packet, determine the current COA of the node from the last registration procedure, and send the packet to the right FA that finally forwards the datagram to the node.

From the security perspective Mobile IP defines an AEE *Authentication Enabling Extension* to both RRQ and RRP packets. The goal of this extension is to create secure channels between the MN and either a HA or a FA and between the FA and the HA. These three links are secured using three shared keys (MN-FA, MN-HA and FA-HA) that are generally preconfigured into the mobility agents. In WiMAX a dynamic way of generating MIP keys is introduced, that will be discussed in section 4.4.6 and 4.4.8.

The WiMAX Forum specifies that mobile user terminals IP provisioning problem should be addressed using the Mobile IP protocol to guarantee session persistence during subscriber mobility across multiple domains. Terminals are classified according to their mobile IP compliancy being divided into two groups, Proxy-MIP and Client-MIP terminals, PMIP and CMIP from now on.

4.4.5 PMIP

A Proxy-MIP terminal is a mobile terminal that completely lacks Mobile IP support but that still needs persistent connection during roaming and seamless handovers between multiple BSs like it happens for CMIP terminals. When a PMIP terminal accesses a foreign network it sends a DHCP DISCOVER in order to get an IP address of that network. To allow reverse routing the WiMAX Forum identifies a special entity called *PMIP Mobility Manager* that is in charge of handling the Mobile IP registration procedure for the user terminal. This entity intercepts the DHCP DISCOVER coming from the terminal and performs a MIP registration with the terminal HA. When this registration has been completed the PMIP mobility manager uses the DHCP protocol to assign the IP address to the mobile terminal. This procedure is transparent both for the user terminal (that simply use DHCP) and also for the HA that receives and handles normal MIP RRQ and RRP.

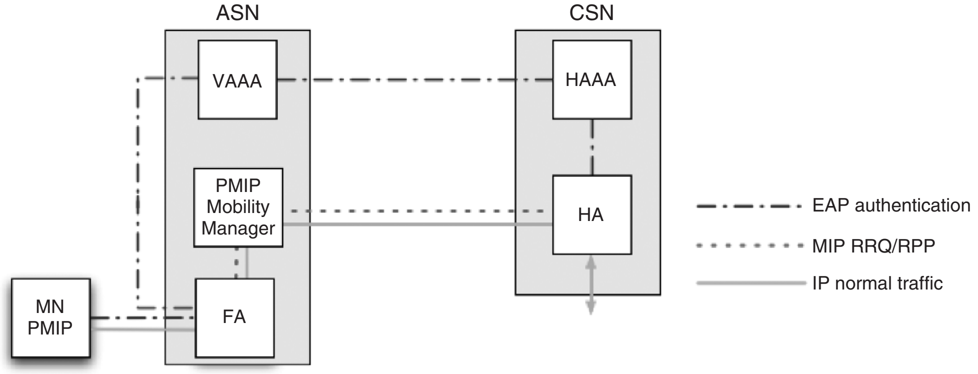

Figure 4.6 NRM and packet flows end-points, PMIP case.

The PMIP Mobility Manager receives also information about the authenticating client including its HoA *Home of Address* (address on the home network), the address of its HA and other additional details. Again, these parameters are moved to the authenticator using appropriate RADIUS attributes.

Figure 4.6 shows the different logic data-path used by MIP signalling traffic, AAA traffic and normal data traffic in a PMIP client connection scenario.

4.4.6 PMIP Security Considerations

The differences between PMIP and CMIP terminals have an impact also on the AAA authentication procedures and the security mechanism described by the WiMAX Forum. Figure 4.7 describes how the keying material needed to authenticate the MIP AEE is derived by the various entities involved.

When a terminal receives beaconing traffic that notifies the existence of a foreign network it wants to access, it will perform IEEE 802.1x authentication with its H-NSP. The RADIUS Access-Accept message carries also attributes used for MIP. Among those attributes we cited the HA address, but also an MSK key that has been produced by the authentication. The authenticator will store the MSK and share it with the co-located PMIP Mobility Manager. From that key will be generated the MIP-RK and a HA-RK key (see Figure 4.10). The PMIP Mobility Manager is now capable of generating MIP RRQ on behalf of the terminal using a MN-HA key (see Figure 4.10) to protect the request message with an AEE extension. Figure 4.7 shows what happens in the home network when a RRQ generated by the PMIP Mobility Manager is received by the HA. The HA lacks the MN-HA and HA-RK keys needed to authenticate and processes the MIP RRQ. These keys can be retrieved using a RADIUS Access-Request to the AAA. The AAA verifies if the request is correct and sends back the requested cryptographic material through a RADIUS Access Response. This procedure is basically the same with the one used by the DHCP server to retrieve the DHCP-RK. Note that with PMIP the MIP client and FA are co-located in the ASN, so that there is no need for an MN-FA key.

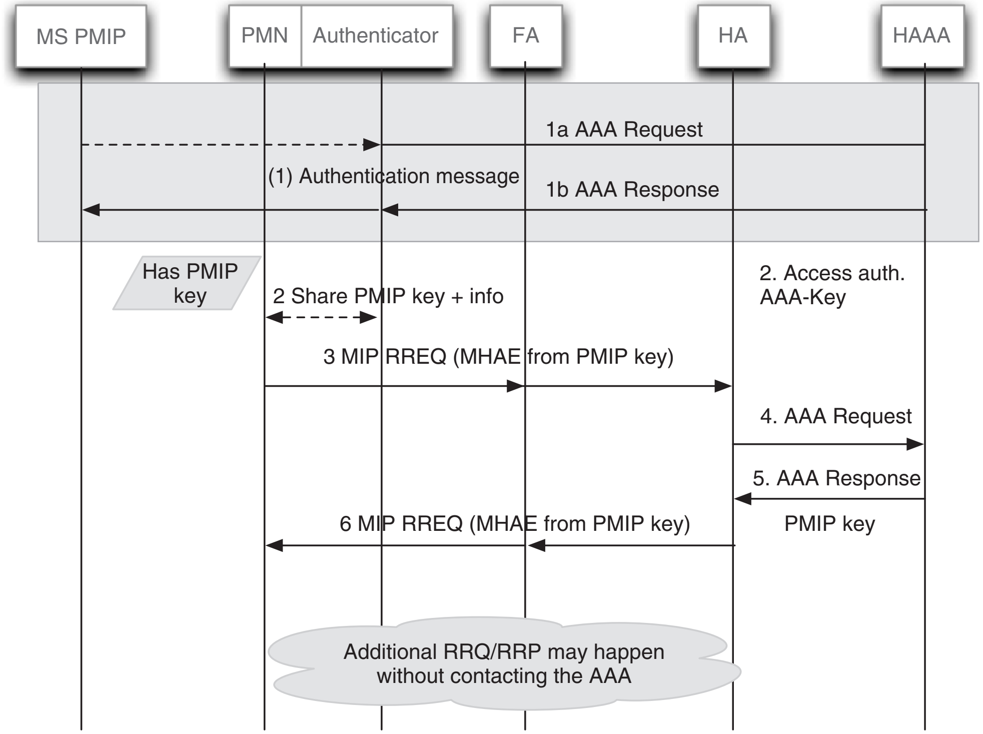

Figure 4.7 PMIP key generation and transfer – message sequence.

4.4.7 *CMIP*

A CMIP terminal is a mobile terminal RFC 3344 compliant with support for all the Mobile IP standard procedures as briefly described in 4.4.5. Figure 4.8 shows the different logic data-path used by MIP signalling traffic, AAA traffic and normal data traffic.

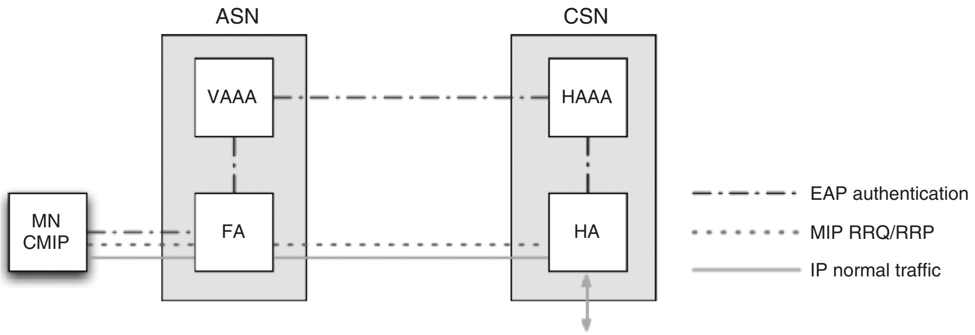

Figure 4.8 NRM and packet flows end-points, CMIP case.

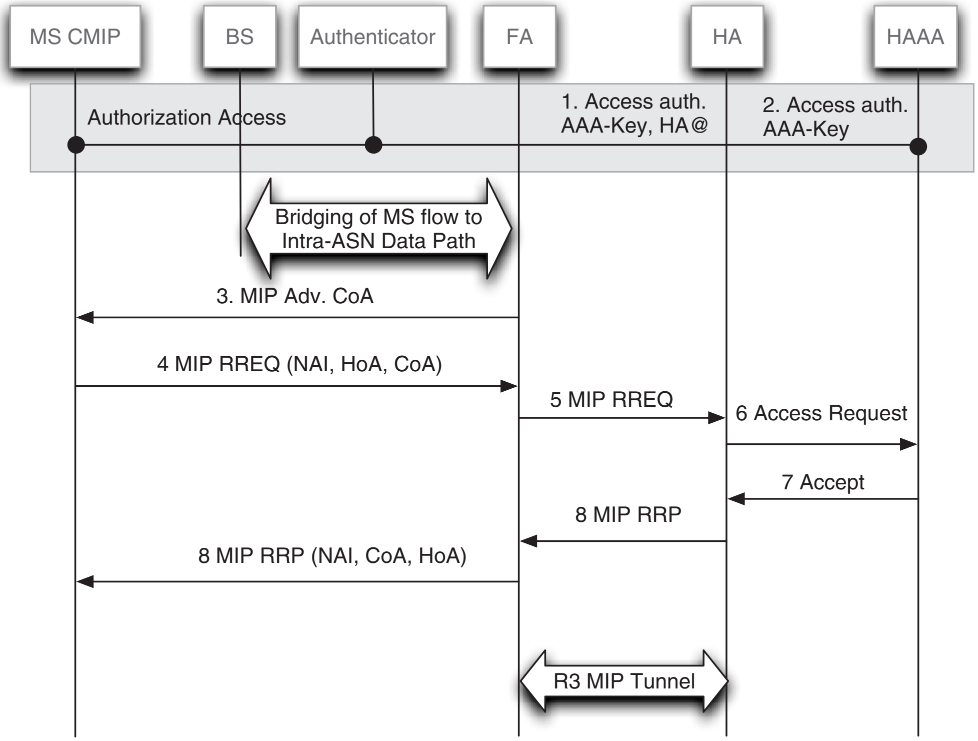

Figure 4.9 CMIP key generation and transfer – message sequence.

A FA is able to distinguish between PMIP and CMIP clients simply observing the way they start their connection setup. If a terminal is a PMIP client it uses a DHCP DISCOVER, in instead it is a CMIP it send a MIP RRQ.

4.4.8 CMIP Security Considerations

The security procedure is the same as used with PMIP but it includes the usage of a new key, a FA-RK to derive a MN-FA key to authenticate messages from the terminal to the FA. This key is generated and used into the MN and FA, the rest of the procedure is the same as the PMIP scenario.

The WiMAX Forum also suggests that for both CMIP and PMIP terminals the HA dynamic assignment should be supported. This procedure allows the user to configure the terminals without an HA IP address and to receive this parameter (and others) during the link layer authentication. More specifically during the EAP authentication phase the AAA inserts in the RADIUS Access-Accept packet some attributes about the authenticating MS configuration including HA IP address, and if needed a DHCP-Server address or a Framed-IP-Address[2]. The authenticator receives the RADIUS Access Accept packet and if the

[2] A Framed-IP-Address is an address statically bound to a MS. If this attribute is returned in the RADIUS Access Accept that address must be assigned to the MS without considering other policies.

terminal is a CMIP sends the HA configuration in the EAP success packet, otherwise if the authenticating MS is a PMIP the MS configuration attributes are shared with the PMIP Mobility Manager that handles the terminal MIP registration procedure (see Figure 4.9).

4.4.9 QoS

IEEE 802.16 defines a set of quality of service classes and the MAC layer parameters that define their quality. The WiMAX Forum addresses the management of QoS introducing the concept of *service flow*, each service flow is mapped to a set of quality parameters that are configurable from the network manager. When a node is authenticated it will be assigned a certain number of service flows of any type depending on its agreement with the operator. At least one service flow is always assigned to an MS, the *initial service flow*, that is used to move DHCP or MIP signalling. The creation and assignment of the following ones is dealt by logical entities that are described in the specification. Their interaction is quite complex and out of the scope of this chapter. The version 1.0 of the WiMAX Forum specification defines only fixed and pre-provisioned service flows. The final outcome is that the Access-Accept RADIUS packet will contain one more attribute for each service flow that must be activated for the MS. Each service flow is characterized by a set of parameters (i.e. tolerated jitter, maximum latency, etc.). The value of these fields can be moved using appropriate RADIUS attributes or they can be preconfigured in the ASN. In the most general case, the ASN will receive a set of RADIUS attributes that define the number of flows and the quality of each flow for each MS. Within the 1.0 specification, the ASN has a set of pre-configured service flows and it receives from the RADIUS server a directive to activate a subset for the current MS; service flows can not be activated or renegotiated once the MS has completed the authentication (this will be supported in the next revision).

Exactly as it happens with DHCP or MIP, the authenticator that receives the RADIUS attribute may be co-located with the BS or more likely included into the ASN-GW. In this second case it will use a custom protocol to move the QoS parameters into the BS to be associated to the corresponding MAC procedures.

4.4.10 A Complete Authentication Procedure

In Figure 4.10 is provided the complete key tree that is produced during an authentication, here we briefly summarize their functions and their usage.

After a successful EAP authentication two keys are generated into the MS and into the RADIUS server called MSK and EMSK. The first one is moved from the RADIUS server to the authenticator into the Access-Accept packet. It will be used by the MAC layer to generate the keys necessary to the cryptographic algorithms of IEEE 802.16. The second one is kept into the endpoints and will be used to generate MIP session keys: the MN-HA key and the FA-RK key. The MN-HA key is moved to the HA when the HA sends a RADIUS request to the server, the FA-RK is moved to the authenticator and will be used to generate the session key MN-FA in CMIP configuration[3] (see Figure 4.9).

[3] The MIP keys that are generated and reported in the figure are distinct for PMIP and CMIP and for IPv4 and IPv6. For simplicity we didn’t focus on this detail in the text

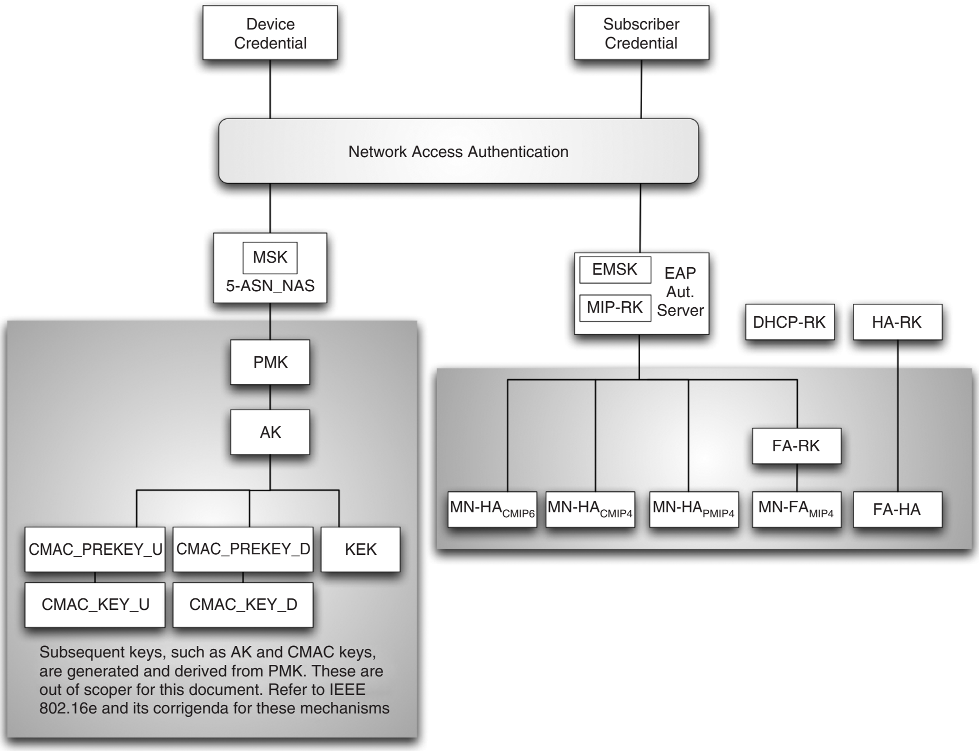
Device Credential
Subscriber Credential
Network Access Authentication
MSK
5-ASN_NAS
EMSK
MIP-RK
EAP Aut. Server
DHCP-RK
HA-RK
PMK
AK
FA-RK
MN-HA$_{CMIP6}$
MN-HA$_{CMIP4}$
MN-HA$_{PMIP4}$
MN-FA$_{MIP4}$
FA-HA
CMAC_PREKEY_U
CMAC_PREKEY_D
KEK
CMAC_KEY_U
CMAC_KEY_D
Subsequent keys, such as AK and CMAC keys, are generated and derived from PMK. These are out of scoper for this document. Refer to IEEE 802.16e and its corrigenda for these mechanisms

Figure 4.10 The global key tree of a WiMAX network.

The path from FA to HA and from DHCP relay to DHCP server does not depend on the authentication of a single MS, so that the keys used to secure those paths are independent by the MSK (Master Session Key) or EMSK. They are generated by the RADIUS server and later on moved into the ASN with the Access-Accept frame and to the HA and DHCP Server with custom requests generated directly by RADIUS clients embedded in their software.

In Figure 4.11 is shown the scheme of a complete EAP-TTLS MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2) authentication in the case of a MS that does not support MIP negotiations and triggers DHCP and PMIP procedures. The single steps have been illustrated so far and do not need further descriptions. What is evident is that in the case of CSN-Anchored mobility the procedure to perform an handover is very complex and consequently very time-consuming. Note that some of the packet exchanges are realized between hosts that do not reside in the same LAN network so that the whole procedure could need several seconds to be completed. This is the price to pay to have extreme flexibility and to support very dynamic configurations.

4.5 Further Reading

The WiMAX Forum website is a valuable resource for white papers and case studies (see [19]). In particular, industries participating in WiMAX Forum activities have released

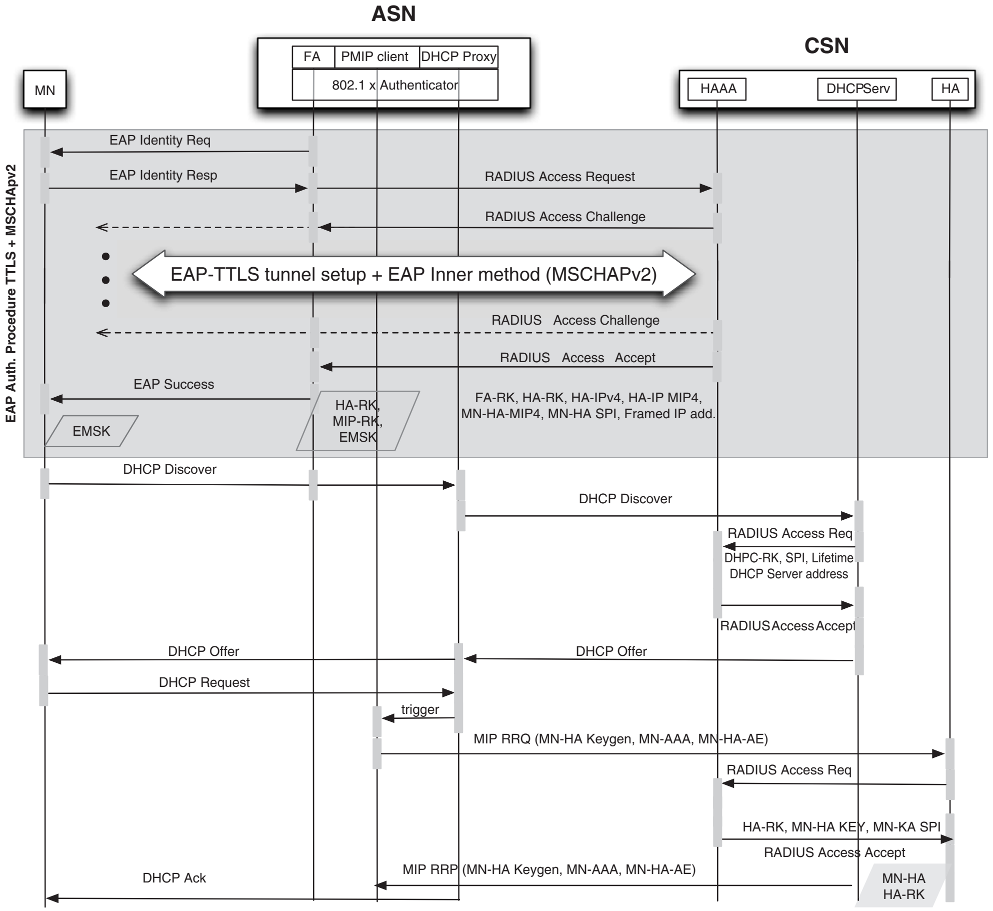

Figure 4.11 A complete WiMAX authentication and parameters exchange.

white papers on the security aspects of WiMAX networks. We suggest [20] and [21] for AAA management. In [2] the WiMAX forum released a complete overview of WiMAX deployment with a descriptive style and references to more detailed specifications. For a more in-depth view of Mobile IP features including security we recommend [22] where real-world use cases are explained and related to Cisco implementations as well as [23] that is focused on the interactions of AAA protocols with mobility management.

4.6 Summary

WiMAX is considered, among the emerging standards, the one that is more likely to be able to address all the bandwidth demands of the new-coming high-speed mobile voice and data services. For this reason there are a lot of concerns about its effective security. Even if most of the of security standards used for WiMAX are widely-trusted protocols a collection of secure technologies does not, in itself, constitute a secure end-to-end network.

Consequently, WiMAX presents a range of security design and integration challenges that are worth to be discussed.

From a security point of view the central element of a WiMAX network is the AAA Server, a functional entity responsible of essentially three main functions: authorization, authentication and accounting. The *de facto* standard for AAA servers is the RADIUS protocol even if IEEE 802.16e foresees also the support for DIAMETER, a more advanced protocol that is expected to update RADIUS. Together with Privacy and Key Management Protocol Version 2 (PKMv2) as a key management protocol both device and user authentications can be performed relying on an AAA server that stores users and devices credentials.

Within the WiMAX architecture the AAA server is used extensively also to supply user related information through specific RADIUS attributes. The AAA server has the role of moving to the ASN the network configuration and QoS parameters related to the specific user. Those attributes are included in the last Access-Accept RADIUS message that is delivered to the 802.1x authenticator in the ASN.

The rationale behind this architecture is to concentrate all the connection related parameters in a reliable central storage point (the AAA server at the H-NSP) and to define primitives and procedures that allow to move those parameters in a secure way, in order to ensure seamless handovers and reliable QoS to mobile users. A MS can freely choose its point of attachment to the network whether the selected BS belongs to its provider or not and all the QoS and IP addressing parameters are moved to the ASN that handles that point of attachment during the EAP authentication phase.

References

[1] http://www.wimaxforum.org. Last visited 04/20/2009.

[2] WiMAX Forum, WiMAX Forum Network Architecture. Stage 2: Architecture Tenets, Reference Model and Reference Points. V. 1.2, WiMAX Forum Std., 2009.

[3] WiMAX Forum, WiMAX Forum Network Architecture. Stage 3: Detailed Protocols and Procedures, WiMAX Forum Std., 2009.

[4] IEEE, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society Std., 2007.

[5] IEEE, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society Std., 2005.

[6] IEEE, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment 3: Management Plane Procedures and Services, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society Std., 2007.

[7] IETF, *RFC 2865 – Remote Authentication Dial In User Service (RADIUS)*, IETF Internet Engineering Task Force – Network Working Group Std., 2000.

[8] IETF, *RFC 3588 – Diameter Base Protocol*, IETF Internet Engineering Task Force – Network Working Group Std., 2003.

[9] D. Johnston and J. Walker, ‘Overview of ieee 802.16 security,’ *Security and Privacy, IEEE* **2**(3): 40–8, May–June 2004.

[10] R. Fantacci, L. Maccari, T. Pecorella and F. Frosali, ‘Analysis of secure handover for ieee 802.1x-based wireless ad hoc networks’ *Wireless Communications, IEEE* **14**(5): 21–9, October 2007.

[11] IEEE, 802.1X – Port Based Network Access Control, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society Std., 2001.

[12] IETF, RFC 3748 – Extensible Authentication Protocol (EAP), IETF Internet Engineering Task Force – Network Working Group Std., 2004.

[13] IETF, RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2, IETF Internet Engineering Task Force – Network Working Group Std., 2008.

[14] IETF, RFC 5281 – Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), IETF Internet Engineering Task Force – Network Working Group Std., 2008.

[15] IETF, RFC 4187 – Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), IETF Internet Engineering Task Force – Network Working Group Std., 2006.

[16] IETF, RFC 2560 – X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, IETF Internet Engineering Task Force – Network Working Group Std., 1999.

[17] IETF, RFC 2131 – Dynamic Host Configuration Protocol (DHCP), IETF Internet Engineering Task Force – Network Working Group Std., 1997.

[18] IETF, *RFC 3344 – IP Mobility Support for IPv4 (Mobile IP)*, IETF Internet Engineering Task Force – Network Working Group Std., 2002.

[19] http://www.wimaxforum.org/resources/documents/marketing/whitepapers. Last visited 04/20/2009.

[20] B. Systems, 'Is your aaa up to the wimax challenge?', 2007.

[21] M. Inc., 'WiMAX security for real-world network service provider deployments', 2007.

[22] S. Raab and M. Chandra, *Mobile IP technology and applications* Cisco Press, 2005.

[23] M. N. Madjid Nakhjiri, *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility* John Wiley & Sons, 2005.