Mobile WiMAX Network Security

Rainer Falk[1], Christian Günther[2], Dirk Kröselberg[2], and Avi Lior[3]

[1] Siemens Corporate Technology
rainer.falk@siemens.com
[2] Nokia Siemens Networks
{christian.1.guenther,dirk.kroeselberg}@nsn.com
[3] Bridgewater Systems
avi@bridgewatersystems.com

Abstract. WiMAX networks provide broadband data access to mobile as well as stationary users. While the wireless link is based on the 802.16e-2005 specification developed by IEEE, a complete network architecture "behind the base station" with global roaming support has been specified by the WiMAX forum. The security architecture for these networks covers EAP/AAA-based secure network access, secure bootstrapping of macro mobility based on Mobile IP, and secure over-the-air provisioning. Specific solutions have been standardized to support combined or separate device and user authentication.

1 Introduction

WiMAX is a technology providing mobile and stationary broadband wireless access to IP-based services through a common radio technology, providing support for quality-of-service, roaming of mobile users, and strong security. The wireless link has been specified by as IEEE 802.16e-2005 [1]. WiMAX comprises a wireless interface that is sometimes hyped as the next technology disruption after IEEE 802.11 wireless LAN. In reality, much more is covered than the pure radio interface. The WiMAX forum [2] has developed a complete network architecture [11] for 802.16-2005 wireless access that supports IP mobility and global roaming. It has similarities with cellular wireless standards such as 3GPP and 3GPP2 as well as with IEEE 802.11.

After giving an overview of the WiMAX network architecture in Section 2, its security architecture is described, highlighting the specific security solutions. Section 3 focuses on network access authentication, whereas Section 4 describes the WiMAX security and key management solution for mobility. Section 5 concludes with a summary and outlook.

2 WiMAX Network Architecture

The WiMAX network architecture complements the IEEE 802.16e-2005 wireless link with a network architecture partially based on IETF protocols. It supports mobility and global roaming, i.e. subscribers can get serviced by any visited operator that maintains a business and roaming relationship with their home operator. A mobile WiMAX-capable device is denoted as mobile station (MS). On the network side,

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 253 – 264, 2009.

WiMAX introduces two logical sets of network functions that can be mapped to corresponding business entities, or network operators, see Fig. 1.

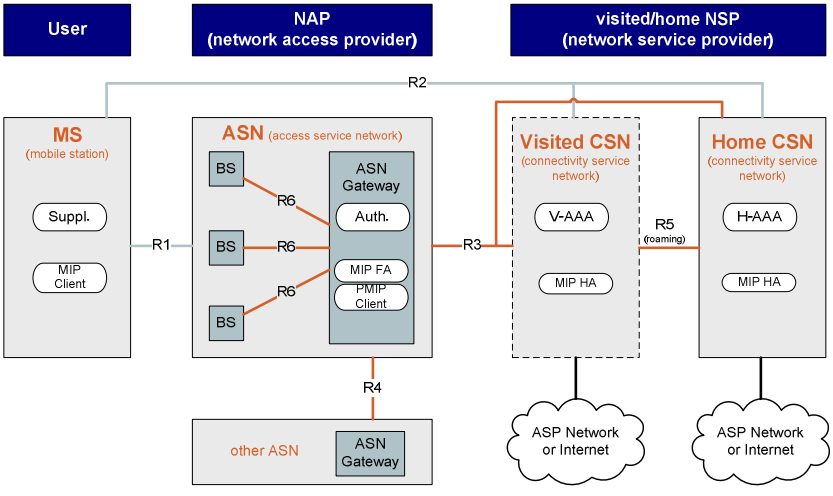

Fig. 1. WiMAX Network Architecture

- The access service network (ASN), which provides network access, comprises WiMAX base stations (BS) and introduces the ASN Gateway as a central controller. The ASN loosely corresponds to the radio access network of cellular systems.
- The connectivity service network (CSN), which corresponds rather to the core network of cellular systems, provides IP connectivity and comprises network entities like IP mobility anchor, DHCP server, AAA infrastructure, and subscriber management functions.

Reference points define the interfaces and group the different protocols between the entities of a WiMAX network. Some of these reference points connect different networks or business entities (shown at the top of Fig. 1). R3 connects ASN and CSN, or a network access provider (NAP) that is operating one or more ASNs to a network service provider (NSP) that is operating a CSN. Others, like R6, are internal to the ASN and connect one or more base stations to an ASN gateway. For roaming scenarios where a user gets WiMAX service through a different operator's network, two types of CSNs are involved, namely the visited (local) CSN and the home CSN the WiMAX user is subscribed to.

For protecting network access, access authentication in WiMAX builds on the IETF EAP (extensible authentication protocol) framework [3] and the RADIUS [8] or Diameter [10] protocol. It uses the common three-party EAP/AAA model for authentication and authorization, involving the supplicant (Suppl) on the mobile station MS, the authenticator (Auth) in the ASN, AAA proxies in the visited CSN (V-AAA) and the AAA server in the home CSN (H-AAA).

EAP itself provides a generic "container" and a well-defined state machine for carrying authentication protocols. Instances of authentication protocols are called

EAP methods. Depending on the EAP method, authentication can be unilateral, i.e. server-only authentication that is similar to common SSL or TLS usage in the Internet, or mutual. It can be based on either shared secrets (including passwords) or public/private key pairs and certificates. WiMAX supports cryptographic authentication of both the device and the subscriber (user) as one major difference to WLAN or mobile cellular network deployments. It defines, but is clearly not limited to, a set of default methods that comprise EAP-TLS [4], EAP-TTLS and EAP-AKA [5]. Any other EAP method matching WiMAX security requirements can be used when supported by the device and the CSN operator at the same time.

WiMAX defines two levels of mobility management, CSN anchored mobility that is based on Mobile IP, and ASN-anchored mobility:

- In the case of CSN anchored mobility or R3 mobility, the handoff takes place between administrative domains. Such R3 mobility can be handled by Mobile IP (MIP), see e.g. [9]. Two variants of MIP are supported: In the case of standard MIP (called CMIP or client-MIP in the WiMAX architecture), the MS itself performs mobility signaling, while in the case of proxy MIP (PMIP), a proxy mobile node (PMIP client) located within the ASN performs MIP signaling on behalf of the MS. So with PMIP, R3 mobility is possible even for MSs that do not support MIP. PMIP does not affect network access security, but has a certain impact on the required key distribution scheme, as – compared with CMIP – the PMIP client is part of a different entity having different security properties.
- Local handoffs in ASN-anchored mobility are handled by a single ASN gateway or between ASN gateways of the same administrative domain, without requiring any Mobile IP signaling towards the CSN. As the local handoff is realized on link layer, it does not affect the IP configuration of the MS.

3 Network Access Authentication

For fixed wireless access, IEEE 802.16-2004 [6] has a single network access authentication and authorization key establishment protocol Privacy Key Management (PKM). This protocol authenticates the MS using a public/private key pair. 802.16e-2005 [1] has adopted PKM for legacy reasons, but also introduced PKMv2 supporting EAP. Also, it allows for mutual authentication between MS and the backend AAA server instead of just the local BS.

For mobile WiMAX networks following the WiMAX Forum network specifications [11], security for the wireless link relies on the security measures provided by 802.16e-2005 [1]. These are profiled to limit the number of supported security options of the PKMv2 protocol, while not continuing support for the former PKM that is used by fixed WiMAX deployments. For authentication of WiMAX subscribers, mobile WiMAX networks build on EAP/AAA-based authentication. This allows for a large set of available EAP authentication methods to give each operator a maximum flexibility to match specific security needs. This section gives an overview of the mobile WiMAX network authentication.

3.1 Authentication Scenarios

For secure access to network resources a separation between authentication of the subscription and authentication of a mobile WiMAX device is introduced.

The former in the most common example maps to a human user. Subscription authentication typically ensures – from the operator's perspective – that the mobile user accessing network resources and mobile services can be uniquely and securely associated with a subscription. In contrast, different reasons may require authentication of the device itself, like for instance the protection of initial over-the-air subscription provisioning using long-term device credentials or verification that the device is not a stolen one.

Current examples of network access authentication are:

- *3GPP networks:* Subscription authentication is based on the tamper-resistant and removable SIM/USIM card that holds the subscription data and cryptographic keys. Device authentication happens only implicitly by verification of the mobile terminal's IMEI number. A USIM card and subscription can easily move between different different mobile terminals, so the subscriber's identity is not necessarily bound to any device identity.
- *WLAN networks:* Only a single EAP authentication is supported for WPA/WPA2 (Wi-Fi Protected Access). Authentication is performed using the EAP protocol towards an AAA server, or using a pre-shared key shared between WLAN devices, e.g. within a WLAN home network. Depending on the deployment, a user/subscriber or a device can be authenticated.
- *DSL or fixed WiMAX access [6]:* Here the device is authenticated. Subscription authentication is typically performed after the device is being connected, e.g. based on username/password credentials.

Device authentication becomes more important in mobile WiMAX networks. Off-the-shelf devices like standard notebooks - in contrast to today's mobile phones that are often sold and subsidized by cellular operators - cannot be expected to be under operator control. Hence, it makes much sense to introduce cryptographically strong device authentication based on certificates imprinted into the device or wireless interface card upon manufacturing. This will enable operators to control that only approved WiMAX equipment can access the operator's network resources and it especially will help to simplify the process of secure device provisioning. Another valid scenario for device authentication is based on the fact that in a roaming situation, the visited network may be subject to country-specific regulations that mandate cryptographic authentication of the device.

Certainly, the overall security level achieved by this depends on a number of challenging factors, like secure storage of keys and trusted certificates in the device, and the PKI (public-key infrastructure) system's responsibility to efficiently handle aspects like certificate revocation.

To cover all these scenarios, the WiMAX Forum defines means for performing both device and user authentication based on EAP methods, single or combined. Device certificates are pre-installed in all WiMAX-Forum compliant devices upon manufacturing, and a PKI including top-level certificate authorities to make those certificates work between different operators is made available through the WiMAX Forum. Detailed considerations related to this PKI system are provided by [12].

3.2 Subscription Authentication

Mobile WiMAX networks require secure access to their resources with authentication based on the EAP/AAA model. In principle, the same three-party authentication model of 802.1X access to WLAN networks is used.

There are a number of technical differences between WLAN and WiMAX like state machines or key derivation for the involved entities. Also, a major new aspect for mobile WiMAX is a central controller for a set of base stations which also handles authentication. With such a controller the Authenticator is not directly located in the base station any more, but is handled centrally by the ASN Gateway which may cover a large number of base stations at the same time. The base station itself only acts as a simple relay for EAP in this scenario, and is only provided with the keys required for protecting the wireless link after successful EAP authentication. One main advantage of this architecture is that during handover, the number of re-authentications can be reduced significantly, thereby avoiding delays.

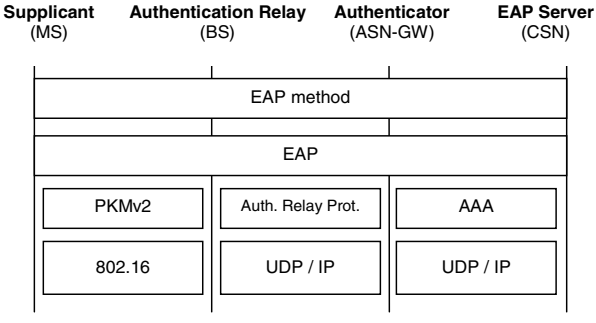

Fig. 2. WiMAX Protocol Layering for Network Access Authorization

An EAP method runs end-to-end between the supplicant in the MS and the EAP/AAA server. It is transparent to the Authenticator in the access network and to any intermediate RADIUS proxy or Diameter agent in the AAA path. Only MS and AAA server run the required security algorithms and possess the required security credentials. Hence, a decision on the EAP method to be used is up to the operator of the AAA server (as long as device vendors support the selected method). Subscription authentication in WiMAX always terminates in the AAA server of the subscriber's home network.

The roaming considerations shown in Fig. 1 also apply here. If the subscriber attaches to an ASN connected to a visited CSN operator, EAP authentication is routed based on the home domain indicated in the network access identifier NAI [7] provided by the MS. This passes through an AAA proxy in the visited CSN and is routed to the home CSN AAA server, where the subscription is actually authenticated.

The NAI for subscription authentication serves as the common identity for the EAP and Mobile IP session in the WiMAX system. It consists of a username part and a realm part identifying the subscriber's home network ("`username@realm`"). For supporting identity privacy, the NAI is allowed to carry a pseudonym as the username part instead of the real identity of the subscription. Hence, it is mainly used for AAA

routing and binding different sessions related to the same network entry of the subscriber in the WiMAX network. This pseudo-identity can also be changed with each new authentication.

On the wireless link between MS and BS, EAP payloads are encapsulated in PKMv2 messages as defined by 802.16e-2005 [1] and are transferred over the 802.16 physical link (see Fig. 2). The authentication relay function (see section 4.4.2 of [11]) in the BS and the authenticator in the ASN-GW exchange EAP payloads by encapsulating them within WiMAX-specific protocol messages across the R6 reference point.

3.3 Device Authentication and Subscription Provisioning

WiMAX client devices are shipped with a device certificate that is securely imprinted by the device vendor upon manufacturing. These certificates are verified using a common root authority hosted by the WiMAX Forum [13]. This public-key infrastructure including root certificate authorities for both WiMAX server and device certificates enables certificate-based device authentication. Conceptually, the AAA server for device authentication is always located in the home CSN and in fact in most cases it will just be the same entity as the one being responsible for subscription authentication. However, the major use case for device authentication is currently to support the process of over-the-air self-provisioning of new subscriptions where the user looking for a WiMAX subscription does not yet have any "home" operator because no subscription has been established yet. This is especially important for devices like notebooks that are bought through common retail channels that are not related to any specific operator. In such cases, one of the WiMAX NSPs locally advertised through the radio channel during initial network attachment will be selected either manually by the user or automatically based on some policy preconfigured by the operator or device manufacturer in the MS. After successful initial provisioning of subscription data the selected NSP will become the home CSN operator for this new subscriber.

The limitation of terminating subscription and device authentication in the same operator's network currently reduces complexity and therefore interoperability issues due to unclear policies between the potentially different involved ASN and CSN operators. Future extensions may support terminating device authentication also locally in the access network.

If both device and subscription authentication are to be performed for the same network entry, the technical choice is to use a tunneled EAP method with the default one being EAP-TTLS [14]. This makes use of the device certificate for setting up a TLS-based secure tunnel first and then runs the subscription authentication inside the tunnel. Options for the so-called "inner authentication" are either an MS-CHAPv2 based challenge-response authentication of the subscription credentials or any suitable EAP method that is forwarded through the outer TLS tunnel.

A different technical approach would have been to perform two subsequent but otherwise independent EAP protocol runs with cryptographically binding the two authentication exchanges in the access network ('double-EAP'). Besides improved flexibility like support for the AAA servers being located in different locations and belonging to different operators or fewer limitations regarding the choice of EAP

methods, this approach would have offered slightly advanced access security due to a cryptographic binding of the two authentication phases that is not available for the EAP-TTLS version currently used by the WiMAX Forum. However, due to a higher complexity in the wireless access this solution has been deprecated by both IEEE 802.16 and the WiMAX Forum NWG.

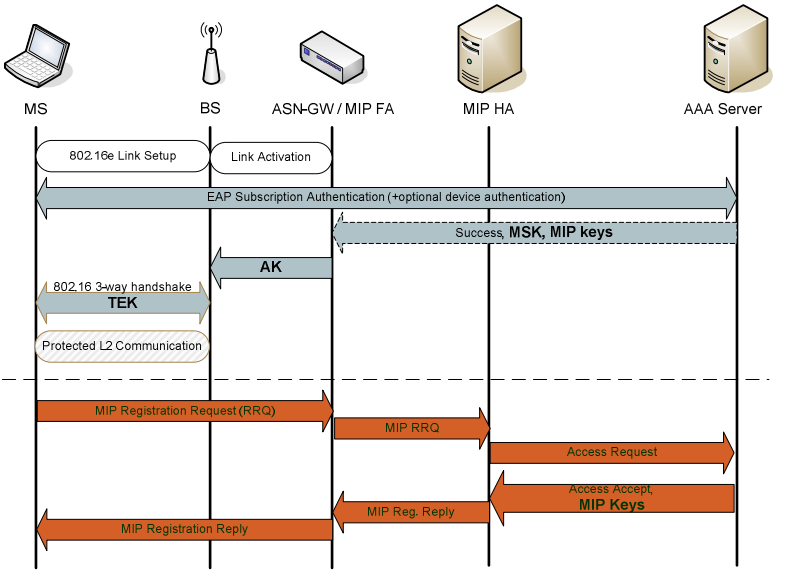

Fig. 3. WiMAX Network Access with Device and Subscriber Authentication

Figure 3 provides a high-level overview of the security-related steps that are performed in a mobile WiMAX network as part of successful network entry. Network access starts with activating the wireless link and selecting the desired NAP. The first EAP run after attaching to a BS of the NAP will be routed through the ASN's authenticator being in charge of this BS to the subscriber's home operator's AAA server. The latter is identified by the realm information of the NAI provided by the attaching MS. After successful EAP method termination the subscriber and the network are authenticated, and optionally the device itself is authenticated based on the device certificate. RADIUS or Diameter will deliver the resulting master session key MSK (see also Section 4) to the authenticator in the ASN Gateway (ASN-GW). A base station specific key AK and related security context information is derived and passed to the respective base station for securing the wireless link (see also Fig. 4 for the WiMAX key hierarchy). This key is used in the 802.16e-2005 3-way handshake authentication between MS and BS and to establish further traffic encryption keys (TEK). After successful authentication, the MS registers with its assigned Mobile IP home agent in case IP mobility service based on MIP is used. Mobility keys for protecting the Mobile IP signaling are also distributed during network access authentication (see Section 4).

Let us take a further look at device authentication in WiMAX network access for the purpose of setting up a new subscription, that is, the dynamic self-provisioning [15] after an un-provisioned device retrieves information about the locally advertised WiMAX CSN operators from the selected ASN and the user selects one for creating a new subscription. The MS enters the network using the EAP-TLS authentication method and the device certificate as the client-side security credential. Certificate-based server-authentication is also performed in EAP-TLS and a WiMAX device is expected to be shipped with pre-installed trusted root certificates to be able to verify the operator's AAA server certificate that is subject to the WiMAX Forum PKI.

After successful network entry, the user will start setting up the new subscription (typically by accessing a Web portal page) and the newly generated subscription data including security credentials and identity information has to be securely transmitted over-the-air to the WiMAX device.

This initial provisioning is based on specifications developed either by the Open Mobile Alliance (OMA) for management of mobile devices or by the Broadband Forum for CPE devices targeted for the fixed-line and DSL market. Both are extended and profiled by the WiMAX Forum [15] to cover the specifics of WiMAX devices. Security keys to enable the security mechanisms in both protocols between MS and provisioning server are derived from the EAP-TLS based device authentication procedure as subordinate keys generated from EMSK. While the MS is able to generate those keys internally, the provisioning server will receive them from the AAA server. So after network access authentication, a shared secret derived from the device authentication is established between the MS and the provisioning server to protect the communication for setting up the subscription.

4 Key Management for Mobility Support

Two levels of mobility management are supported by WiMAX: CSN anchored mobility that is e.g. based on Mobile IP, and local ASN-anchored mobility. In the latter case, the traffic is redirected towards the new BS after hand-off, but the MIP Foreign Agent (FA) location or MS IP address do not change. In the case when the new BS is controlled by the same ASN Gateway as the previous BS, the authenticator in the same ASN Gateway is still in charge for securing the new wireless link after handover and will provide appropriate key material to the new BS over the WiMAX-defined R6 reference point. This key material is still derived from the original EAP authentication session key MSK. For hand-off to a base station controlled by a new ASN Gateway, the Authenticator in the new ASN Gateway may take over security control. This requires an EAP re-authentication to be performed and fresh keys to be generated to protect the new wireless link. Alternatively, the authenticator of the old ASN Gateway can be kept to avoid re-authentication and related delays. EAP exchanges go all the way between the MS and the home operator's AAA server. In this case it will remain the "anchor" authenticator and provide appropriate keys for the new BS to the new ASN Gateway, across the R4 interface.

When CSN-anchored mobility handover via Mobile IP takes place, the MS gets assigned a different local IP address after hand-off. Although both Mobile IP v4 and v6 can be supported, this section will focus on the Mobile IPv4 [9] aspects for the

sake of brevity. The MS's local IP address called care-of-address (CoA) is registered with the MIP home agent (HA) that resides in the CSN (see Fig. 1). The HA handles the MS's long-term home IP address, which remains unchanged and tunnels data traffic destined to the MS to its current care-of address. The MS communicates using its home address. In WiMAX MIPv4, a foreign agent (FA) in the ASN gateway is the tunnel endpoint for all user traffic in the access network. WiMAX allows for a dynamic assignment of the HA and the MS' home address. The HA may, depending on operator policies, be assigned and located on a per-subscriber basis either in the home CSN or in a visited CSN. The network elements and interfaces relevant for Mobile IP and AAA interaction are shown in Fig. 1.

Two variants of MIP are supported: Either the MS performs MIP signaling itself (CMIP), or a PMIP client in the ASN-Gateway performs MIP signaling on behalf of the MS. As described above, it is possible to keep the anchor authenticator after handover. This means that the FA functionality moves to a new ASN Gateway, but no EAP re-authentication needs to be performed. The anchor authenticator is still in charge of providing keys for securing the wireless link. If PMIP is used in this scenario, the PMIP client also stays with the anchor authenticator and does not move to the new ASN Gateway.

Mobility signaling has to be protected, as it controls all the user traffic. Hence, Mobile IP requires a security association between the Mobile IP client and the HA (MN-HA) for protecting MIP signaling. Also, MIP signaling between FA and HA (FA-HA) is protected by a security association.

In WiMAX, the architectural approach was chosen to dynamically derive the mobility keys from the EAP-based network access authentication that has been described in Section 3. The resulting key hierarchy is illustrated in Fig. 4. Initially based on long-term credentials for secure authentication of the subscription for

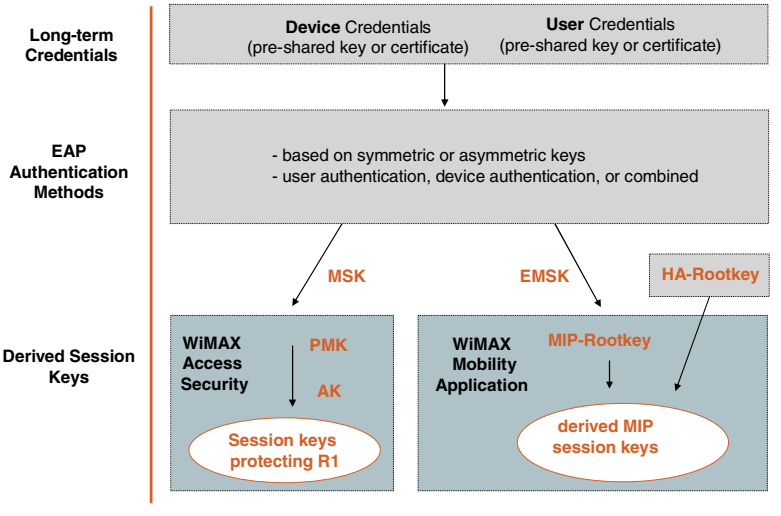

Fig. 4. The WiMAX Key Hierarchy

network entry, EAP authentication creates two session keys MSK (master session key) and EMSK (extended MSK) that are known by the EAP peer (client) and the AAA server. The EMSK key is not used for securing the wireless link and is reserved to serve as master key for derivation of further application-specific session keys. Such applications rather include those integral to the network architecture design and network operation instead of being general third-party applications that are typically independent of the WiMAX network.

The MSK key forms the basis for derivation of all session keys for protecting the 802.16e-2005 wireless link. It is generated as a result of the EAP method based authentication in the MS and the AAA server terminating EAP in the CSN. As highlighted in Fig. 3, it is delivered via the RADIUS or Diameter protocol from the AAA server to the authenticator in the ASN Gateway. Further information on the key hierarchy for the wireless link can be found in [1].

From the second key EMSK, a Mobile IP root key MIP-RK is generated in the AAA server and the EAP peer, and all user-related session keys for the MN-HA security association for a CMIP or PMIP session are derived from the root key. Although for PMIP such user-related keys would not be required (instead, a PMIP client could use the same MN-HA key for all active user sessions), CMIP and PMIP is actually using the same scheme in WiMAX. This allows to simplify the network signalling by only defining a single mechanism for keying the different R3 mobility schemes. In addition, the AAA server generates an independent root key HA-RK for protecting signaling between a specific HA and connected FAs.

The MIP session keys related to a specific user session are distributed to the authenticator in the ASN Gateway already as part of the RADIUS or Diameter message that the AAA server sends to the authenticator as shown in Fig. 3, to indicate successful authentication of the user. The HA also requires the MN-HA security association for protecting and verifying MIP messages. It requests keys, if not yet available, from the AAA server when receiving a MIP registration message. In contrast, the MS generates all keys on its own if CMIP is used. For PMIP, no Mobile IP related keys are required in the MS.

In the ASN, the authenticator is responsible for further distributing the appropriate MIP keys to the FA and the PMIP client for PMIP. This is especially the case for an FA being located in a different ASN Gateway. HA-RK is used in the authenticator and HA to derive fresh FA-HA keys. It is only distributed as required, and is not specific to a single MS or subscriber.

An important aspect from the security point-of-view is the secure binding between two otherwise independent procedures of authenticating network access and securing mobility service. WiMAX achieves this by using the NAI identity provided during network access authentication also in Mobile IP registration. This is sent by the HA together with a unique key identifier, the MIP security parameters index (MIP-SPI), to the AAA server and is subsequently used there to select the correct set of mobility keys. By this, the network ensures that the session created during network access authentication and the MIP session belong to the same user. For MIP-SPI creation, it is important to avoid collisions of SPI values for MN-HA security across the network. Such collisions would result in ambiguities for selecting the subscriber session's related MIP keys, leading to dropped sessions. Hence, WiMAX networks implement a specific procedure to ensure that such collisions cannot happen (see section 4.3.5 of [11]).

The WiMAX approach of binding key management and distribution for Mobile IP to the EAP-based network access authentication has been an important step for the WiMAX network security architecture, compared to any approach based on static pre-configuration of shared MIP keys between a subscriber's WiMAX device and the home network. Such binding, however, also creates a need for synchronization of key lifetimes between the different EAP and MIP sessions and correct removal of session state when the devices log off. In an environment supporting fully mobile devices and globally roaming users, the benefits like increased security through dynamically provisioned mobility keys and reduced administrative complexity justifies the effort.

5 Summary and Outlook

The overall goal of the WiMAX security architecture is to create an interoperable security solution that covers all relevant aspects of WiMAX networks based on commonly accepted security protocols like EAP and RADIUS/Diameter. One major objective is to minimize administrative effort and therefore reduce operational expenses by designing dynamic mechanisms for distributing configuration data in the system. Looking at security, full support for dynamic over-the-air provisioning and dynamic generation and distribution of security associations fall into this category. This holds for the provisioning based on device authentication as well as for network services like IP mobility.

WiMAX is designed with the clear goal of being extensible in the future. In particular, the security concepts are not strictly limited to the WiMAX environment, but can be expanded to leverage integration with other mobile communication technologies like those developed by 3GPP or 3GPP2. Inter-technology interworking has been an important factor in the design of the WiMAX security architecture and as one example the dynamic keying approach developed for Mobile IP is also followed by 3GPP in their specifications describing how to interwork with other access technologies like WiMAX.

The WiMAX security architecture comes with similarities to WLAN (EAP) and 3GPP2 (Mobile-IP/AAA), but also with a number of new approaches: For network access, it supports EAP-based authentication of both the user's device and the subscription. Integral support for over-the-air provisioning combined with dynamic network selection support allow users of any type of WiMAX device to flexibly create a subscription with one of the available network service providers. Mobile IP security is dynamically bootstrapped. Furthermore, the real user identity can be hidden from the wireless link and from local access networks by using a pseudo-identity mechanism.

Certainly, the WiMAX network specifications are evolving, and ongoing work related to the next releases of the WiMAX network architecture will also further extend the security architecture. Besides obvious and already available enhancements like including full support for Diameter [10] as AAA protocol in addition to the initial RADIUS-only specifications, or support for WiMAX-specific SIM cards, improvements like a cryptographically protected rejection cause indication in cases where a WiMAX device is denied network entry, or advanced access scenarios like the support for Femto cells are being worked on in the WiMAX Forum.

References

1. IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, IEEE 802.16e-2005 and 802.16/COR1, http://www.ieee802.org/16/
2. WiMAX Forum, http://www.wimaxforum.org/
3. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP), RFC 3748 (June 2004), http://www.ietf.org/rfc/rfc3748.txt
4. Aboba, B., Simon, D.: PPP EAP TLS Authentication Protocol, RFC 2716 (October 1999), http://www.ietf.org/rfc/rfc2716.txt
5. Arkko, J., Haverinen, H.: Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA), RFC 4187 (January 2006), http://www.ietf.org/rfc/rfc4187.txt
6. IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE 802.16-2004, http://www.ieee802.org/16/
7. Adoba, B., Beadless, M., Arkko, J., Eronen, P.: The Network Access Identifier, RFC 4282 (December 2005), http://www.ietf.org/rfc/rfc4282.txt
8. Rigney, C., Willens, S., Rubens, A., Simpson, W.: Remote Authentication DiaI In User Service (RADIUS) (June 2000), http://www.ietf.org/rfc/rfc2865.txt
9. Perkins, C. (ed.): IP Mobility Support for IPv4, RFC 3344 (August 2002), http://www.ietf.org/rfc/rfc3344.txt
10. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: Diameter Base Protocol, RFC 3588 (September 2003), http://www.ietf.org/rfc/rfc3588.txt
11. WiMAX Forum: WiMAX Forum Network Architecture (Stage-3: Detailed Protocols and Procedures), Release 1 Version 4, (February 2009), http://www.wimaxforum.org/sites/wimaxforum.org/files/documentation/2009/WMF-T33-001-R010v04_Network-Stage3-Base.pdf
12. WiMAX Forum: WiMAX Forum Network Architecture – WiMAX Forum Device PKI Certificate Policy Draft Specification, Version 1.0.3 (April 2008), http://www.wimaxforum.org/certification/x509_certificates/pdfs/wimax_forum_device_public_key_infrastructure_certificate_policy.pdf
13. WiMAX Forum: X.509 ordering process, http://www.wimaxforum.org/certification/x509_certificates/
14. Funk, P., Blake-Wilson, S.: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC5281 (August 2008), http://www.ietf.org/rfc/rfc5281.txt
15. WiMAX Forum: WiMAX Forum Network Architecture - WiMAX Over-The-Air General Provisioning System Specifications, Release 1.5 Version 1.0.2 (September 2008)