

Patterns for WiMax security

Eduardo B. Fernandez, Michael VanHilst and Juan C. Pelaez
Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL , USA

Abstract

WiMax (Worldwide Interoperability of Microwave Access), also known as the IEEE 802.16 protocol is the latest standard for wireless networks. Its purpose is to expand the range of wireless systems access. We present here two patterns for this standard: WiMax Network Architecture, which describes the structural and dynamic aspects of these networks which are relevant for security and WiMax Security, which describes its main security features.

1 Introduction

Does it make sense to have patterns for standards? We have found some resistance to this idea from pattern ‘purists’ in the past. However, we are convinced that it makes a lot of sense to define patterns for standards. A standard is a set of guidelines to be used by vendors to develop products and by users when using these products or interacting with them. Standards are the basis for interoperability and as such they have an enormous business value. For example, an architectural standard defines a generic model that describes many real architectures and as such satisfies a basic genericity requirement. The standard also solves a problem or set of problems, how to define guidelines for products, architectures, software, or hardware in a unified way that allows them to interoperate. We have produced a variety of patterns for standards, especially for web services security standards, which include patterns for XACML and WSPL [Del05], SAML [Fer06a], and Liberty Alliance [Del07]. Standards are in general complex, and described using words, or low-level languages such as XML. It is then hard for a user to understand them. We have found that describing standards as patterns makes them clearer (the power of abstraction), and allows designers to use them as guidelines for new designs as well as evaluating existing products [Fer06b]. We present here two patterns for a relatively new standard, WiMax (Worldwide Interoperability of Microwave Access), also known as the IEEE 802.16 protocol.

The current wireless standards WiFi (IEEE 902) and Bluetooth require access points at short distances of the subscriber. WiMax addresses high-bandwidth wide-area access between a service provider base station and multiple subscriber stations, often referred to as the “last mile” in reference to neighborhood connections between subscribers’ homes and a phone or cable company office. In fact, important parts of the protocol are based on the DOCSIS BPI+ (Data Over Cable Service Interface Specifications: Baseline Privacy Plus Interface Specification) [DOC00] protocol used in cable modems.

Figure 1 shows the relationships of these patterns with respect to each other and with respect to some related patterns. Their thumbnail descriptions are given below. The two new patterns are shown first.

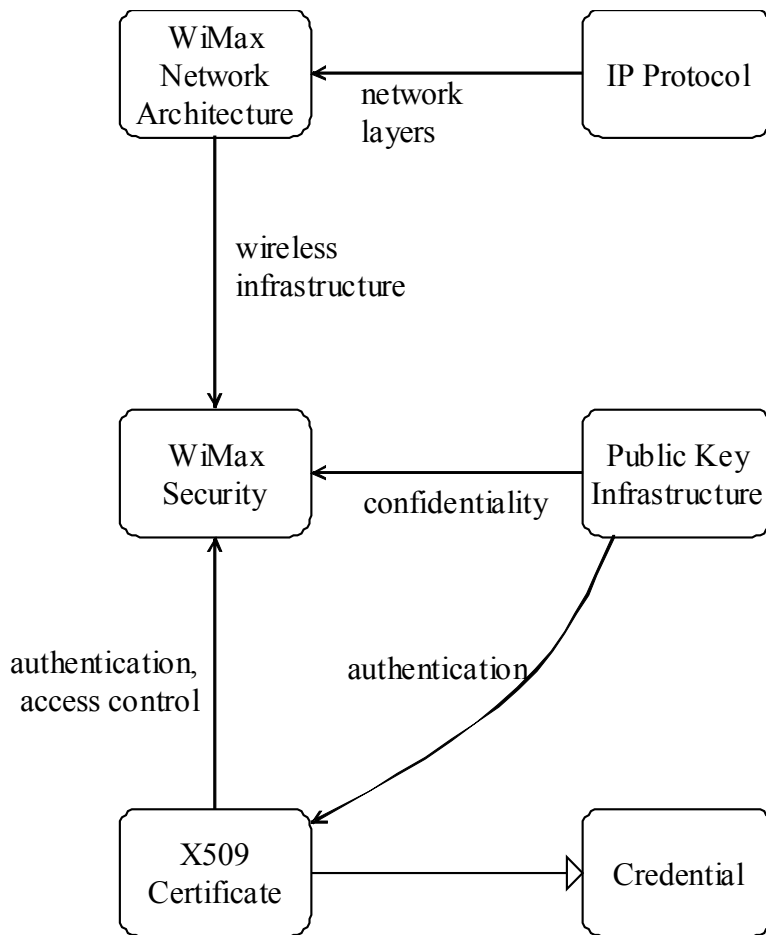


Figure 1. Pattern diagram for WiMax patterns

WiMax Network Architecture.

How do we let subscriber (user) stations communicate with each other through long distances (up to 30 miles) using wireless networks? Make *Subscriber Stations (SSs)* communicate with a *Base Station (BS)* through wireless links. The Base Station connects all subscribers. Use a layered architecture that supports different protocols in different layers. Support multiple message types and sub-layers within layers, e.g. for mapping and security.

WiMax Security.

How do we establish a security environment for the use of the network and for the messages exchanged in it? Base Stations perform authentication using credentials to control the access of users to the network. Connections use security associations to indicate the way they will protect their messages.

Public Key Infrastructure [Let01]

Provide a cryptographic framework based on public/private keys to distribute keys, exchange keys, provide digital signatures, and protect message integrity.

Credential [Mor06].

Provide secure and portable means of recording authentication and authorization information for use in distributed systems.

X.509 Certificate.

A type of Credential, defined by ISO standards.

In Figure 1, the central pattern is the WiMax Network Architecture pattern. This defines the structural aspects of WiMax networks that are relevant for security. Its layers are supported by the layers defined by the IP Protocol. The WiMax Security pattern defines the security standard for the wireless network. In turn, this standard uses X.509 certificates for authentication and access control. These certificates are a special case of the Credential pattern. X.509 certificates use a Public Key Infrastructure for authentication, signatures, and hashing.

Section 2 discusses the WiMax Network Architecture pattern while Section 3 presents the WiMax Security patterns . We end with some conclusions and some ideas for future work.

2. WiMax Network Architecture Pattern

1.1 How do we let subscriber (user) stations communicate with each other through long distances (up to 30 miles) using wireless networks? Make *Subscriber Stations (SSs)* communicate with a *Base Station (BS)* through wireless links. The Base Station connects all subscribers. Use a layered architecture that supports different protocols in different layers. Support multiple message types and sub-layers within layers, e.g. for mapping and security.

1.2 2.1 Example

Lina has a PC but lives in a rural area. She works in the city. When she goes to the city she can use the Internet but in her home she has no access. She would like to use the Internet to reach her friends and work occasionally from home but she cannot do this unless she moves to an area in the city.

1.3 2.2 Context

1.4 Fixed or mobile stations in wireless networks distributed in relatively large geographic areas, where a WiFi network cannot reach.

1.5 2.3 Problem

Many wireless subscribers live far from each other, need to be dispersed because of their functions (e.g. a deployed army battalion), or travel frequently. These users may need to talk to other subscribers with similar characteristics. The current wireless standard, WiFi, has only a limited reach.

A possible solution to this problem is constrained by the following forces:

- Wireless users want to reach other subscribers or access the Internet, regardless of their distance to access points.
- We need a common protocol and network structure to be able to interconnect a variety of products and networks together.
- Subscribers want to use their network connections for a variety of applications, involving a variety of message types and a variety of QoS and security needs. At the same time, the capacity and quality of wireless connections varies unpredictably with time. Subscribers must be able to establish, use, and dynamically adjust different kinds of connections within the common architecture.

- Base station providers want to limit services to paying customers, and to have the ability to offer different customers different combinations of services.
- Wireless bandwidth is a limited resource. The overhead for network management functions should not consume an undue portion of the connection bandwidth.

1.6 2.4 Solution

Make *Subscriber Stations (SSs)* communicate with a *Base Station (BS)* through wireless links. The Base Station connects subscribers to other networks. Use a layered architecture that supports different protocols (or sub-protocols) in different layers, with flexible mappings between the layers. Support multiple message types using the same layers on the same connection, with simple tags and IDs to differentiate the types. Support sub-layers within layers, i.e. for mapping and security.

WiMax defines two layers of the protocol stack, *Physical* and *Medium Access Control (MAC)*. The MAC layer manages connections and security. The physical layer (PHY) handles signal connectivity and error correction, as well as initial ranging, registration, bandwidth requests, and connection channels for management and data.

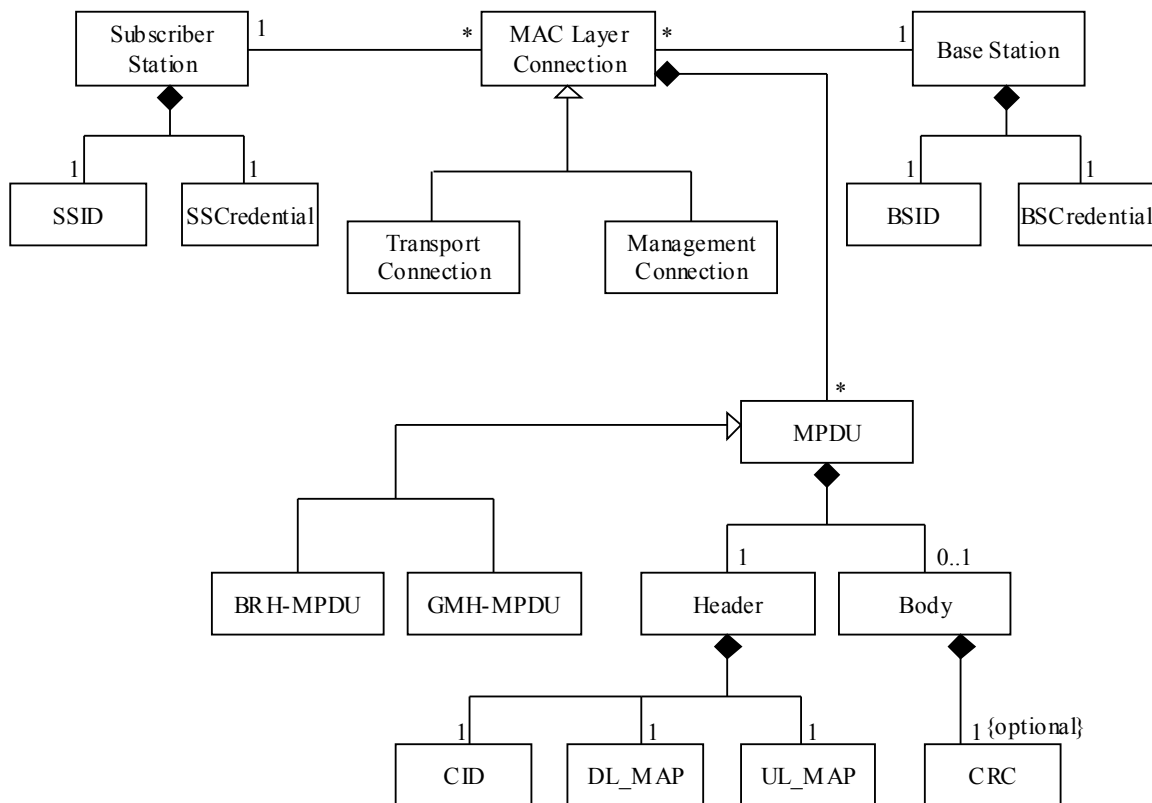


Figure 2. Class diagram of WiMax network architecture

1.7 Structure

A communication is divided into *frames*. Frames from BS to SS (*downlink frames*), and SS to BS (*uplink frames*) contain a frame header and a body (Figure 2). The header has two slot maps, a downlink map (DL_MAP) and an uplink map (UL_MAP). The maps describe the use of the slots and their location. Each slot is part of some connection, identified by a connection

ID (CID). *Management connections* are used to set up connections and contain aspects such as bandwidth requests and other administration information. On connection, an SS is assigned three management connections (basic, primary, and secondary) for management messages with different QoS needs. Short management messages needing immediate response use the basic connection, while the secondary connection handles IP management traffic such as address request (DHCP), system status (SNMP), and remote update (TFTP). User messages are sent through *transport connections*. IEEE security applies only to transport connections and the secondary management channel.

Data is moved through packets with MAC protocol data units (MPDUs). Depending on their functions there are two types of MPDUs (Figure 2): those with bandwidth request headers (BRHs) and those with generic MAC headers (GMHs) (in this case the header is followed by a body and an optional CRC). A management connection uses management packets, where each MPDU carries a single MAC management message.

1.8 Dynamics

Figure 3 is a sequence diagram describing the start of a connection. Before connecting, a subscriber station scans its frequency list to find a base station, observes base station traffic to determine parameters for timing, modulation, error correction, and power, and finally identifies time slots (“maintenance windows”) to use for an initial request. The initial sequence of packets (“ranging requests”) between the subscriber and base station are used to refine power and timing settings, and to establish connection reservations (time slot “profiles” and Connection IDs). The subscriber station obtains multiple CIDs for different management and data connections with different quality of service (QoS) criteria. .

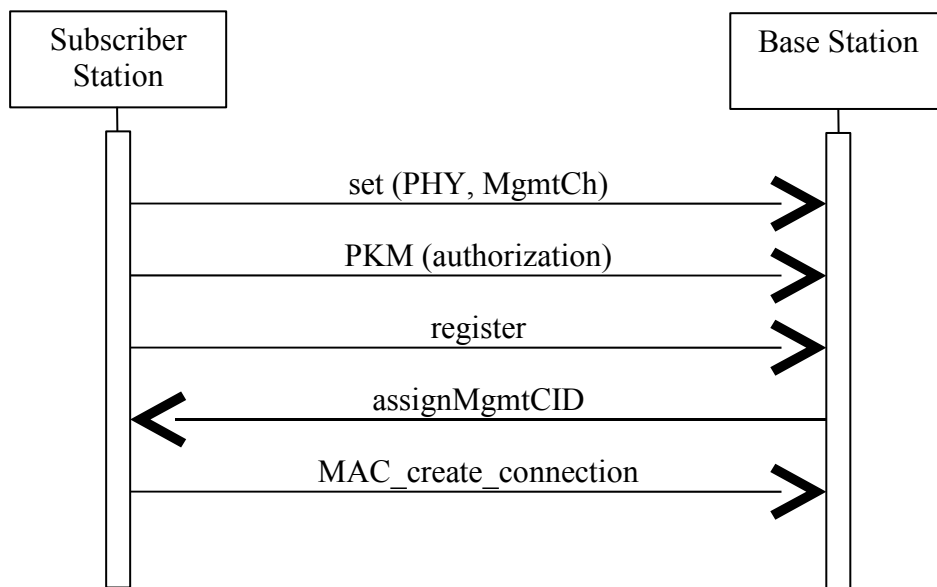


Figure 3. Starting a connection

1.9 2.5 Implementation

The original 802.16 standard covers line-of-sight connections in the 10-66 GHz range, supporting speeds up to 280 Mbps over distances up to 50 kilometers (30 miles). 802.16a covers non-line-of-sight connections in the 2-11 GHz range, supporting speeds up to 75Mbps

over distances of 5-8 kilometers (3-5 miles). 802.16a also adds features for mesh networks, while an 802.16e standard adds support for mobility (i.e. station handoff) [Eck02].

The physical layer consists of a sequence of equal-length frames transmitted through the coding and modulation of RF signals. Physical frames, and also MAC frames, do not necessarily begin or end on boundaries of higher layer frames – this is handled by intermediate mapping layers. Intermediate mapping gives 802.16 flexibility to support a wide variety of traffic types and profiles in the transport layer and above, including IP, Ethernet, and ATM, with a high level of efficiency [Eck02].

1.10 2.6 Example resolved

Lina became a WiMax subscriber and now she can work from home and has access to the Internet.

1.11 2.7 Known uses

- Intel and Fujitsu have developed WiMax chips.
- Nokia and Nortel have some WiMax networking products.
- Possible military applications are described in [Bur05].
- The use of WiMax in P2P systems is described in [Ang06].

1.12 2.8 Consequences

This pattern has the following advantages:.

- It is possible to let a subscriber stations communicate with other networks through the Base Station.
- The common protocol enables network interoperability.

This pattern has the following disadvantages:

- There is some overhead in using a Base Station to mediate accesses.
- The standard is still evolving.
- This is not the only standard for this purpose, there are also two cellular standards: Long Term Evolution (LTE), and CDMA1x EV-DO Revision C. In fact, WiMax itself has three significant versions: the original 802.16, 802.16-2004 (also called 802.16d) which adds numerous enhancement options, and 802.16e which presents alternatives for supporting mobile subscribers. This may bring confusion to the users and those developing products based on the standards..

1.13 2.9 Related patterns

- WiMax Security complements this pattern.
- As indicated in Figure 1, the IP Protocol pattern provides lower-layer support.
- Some of the patterns in [Sch00] to establish network connections are also complementary.

3 WiMax Security

How do we establish a security environment for the use of the network and for the messages exchanged in it? Base Stations perform authentication using credentials to control the access of users to the network. Connections use security associations to indicate the way they will protect their messages.

3.1 Example

Lina does a lot of Instant Messaging with her friends but there are a lot of impostors in the network, trying to get identity information. She is afraid to talk to some people because of this. She also wants to keep her messages confidential.

3.2 Context

1.14 Fixed or mobile stations in wireless networks distributed in relatively large geographic areas, where WiFi cannot reach.

3.3 Problem

How do we establish a security environment for the use of the network and for the messages exchanged in it? Subscribers need to exchange messages without exposing them to eavesdroppers. They also need to know they are talking to authentic subscribers. The network company only wants to authorize legitimate subscribers to use the links.

The possible solution is constrained by the following forces:

- We need to restrict access to the network only to registered subscribers. Otherwise it would be difficult to guarantee bandwidth and performance to legitimate users.
- Subscriber need to exchange confidential messages, authenticated messages, and messages with guarantees that they have not been modified in transit. These are important issues for business use.
- The approach should be transparent or very easy for the users.

3.4 Solution

Base Stations perform authentication using credentials to control the access of users to the network. Connections use security associations to indicate the way they will protect their messages.

Security is closely tied to connections and connection types. WiMax defines two connection types, management and data. Management connections are further subdivided into basic, primary, and secondary. Stations perform authentication using credentials, X.509 certificates in the current standard. Once authenticated, a user is given a token to access the system.

802.16 defines a *Privacy and Key Management (PKM)* protocol to address the goals of subscriber station confidentiality and preventing theft of provider services [Bur05]. The PKM uses *Security Associations (SAs)*, of which there are two types. A *data SA* specifies how messages between the base station and subscriber station are to be encrypted, which algorithms will be used, the keys to be used, and related information. By using additional SAs different methods of encryption may be used for different groups of messages. An *authorization SA* is used for management and update.

Structure

Figure 4 shows the structure of this pattern. Each data SA includes an ID (SAID), an encryption algorithm to protect the confidentiality of messages, two *traffic-encryption keys (TEKs)*, two identifiers (one for each TEK), a TEK lifetime, an initialization vector for each TEK, and an indication of the type of data SA (primary or dynamic). An *authorization SA* (not explicitly defined by the standard) includes a credential, an *authorization key (AK)* to authorize the use of the links, an identifier for the AK, a lifetime for the AK, a key-encryption key (KEK), a downlink hash-based message authentication code (DHMAC), an uplink hash

code (UHMACH), and a list of authorized data SAs. Figure 2 summarizes the information used in SAs.

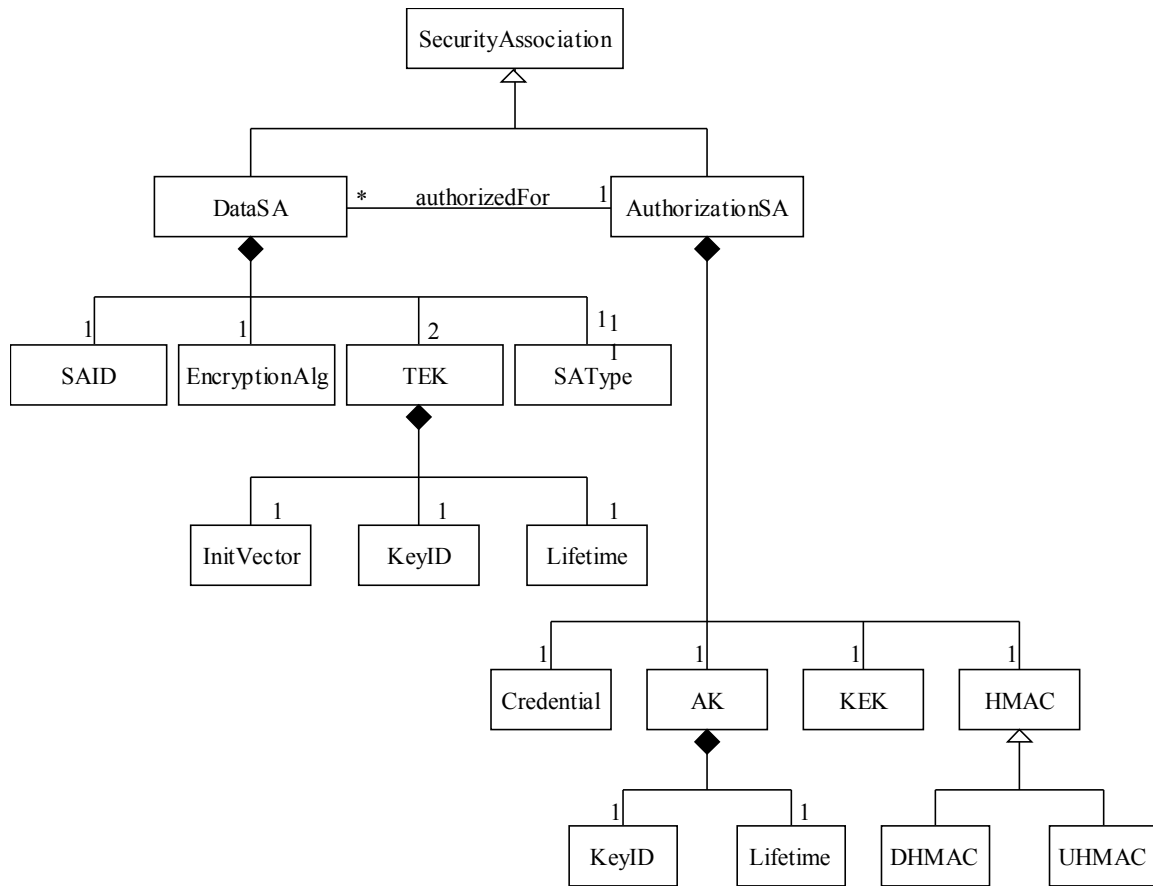


Figure 4. Class diagram of SA structure

Dynamics

Security begins with authentication in the initial “ranging request” phase. Each subscriber station has a 48 bit ID (or MAC address) and an X.509 certificate. It also possesses an X.509 certificate of its manufacturer – but this latter certificate is generally ignored by the base station and plays no role in security. The subscriber station also obtains multiple security association identifiers (SAIDs) which identify an SA which specifies both a service type and encryption parameters. Subsequent management messages can change connection profiles in response to changing QoS needs and signal quality.

Figure 5 summarizes the steps in the PKM protocol for the subscriber station (SS) to obtain authorized access to the network. The subscriber station sends two messages. The first message (Authentication Information) contains the manufacturer X.509 certificate. The second, Authorization Request, includes its own X.509 certificate and a list of its security capabilities. If the subscriber station is authenticated and authorized to join the network, the base station (BS) sends an Authorization Reply. The Authorization Reply is encrypted with the subscriber station’s public key (denoted as E(Auth, SSPK) in the figure) and includes an Authorization Key (AK), a key lifetime, a key sequence number, and a security association (SA) descriptor (the basis for the authorization SA). The 802.16e standard supports an EAP variant to verify the Base Station, shown in the section on implementation.

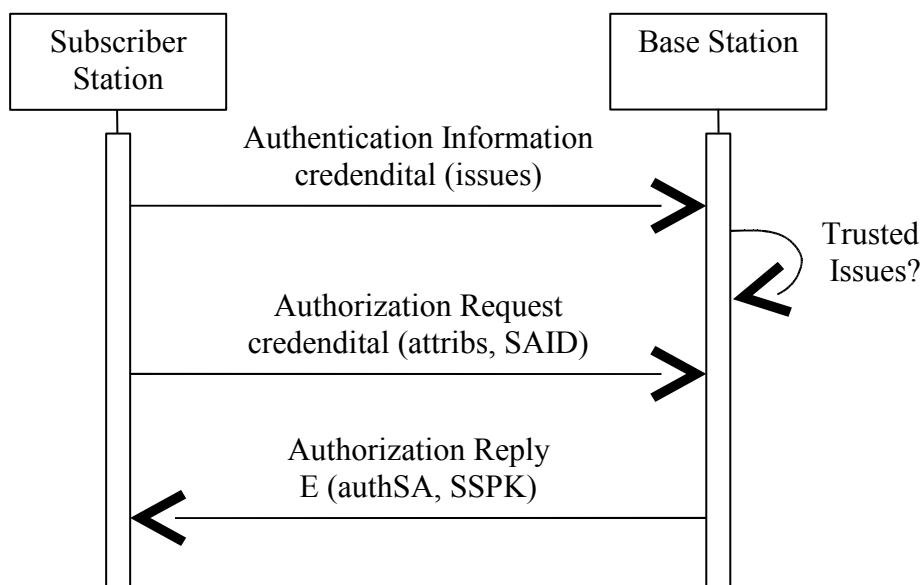


Figure 5. PKM Authorization protocol

The PKM exchange of messages establishes an authentication key (AK), and a security association (SA). The sequence numbers in the protocol represent instances of the AK. The AK is used to derive three additional keys for both encrypting and verifying the source and integrity of future messages. Message source and integrity are verified with message authentication (HMAC) keys, e.g. HMAC(1) proves the integrity of the first message from the BS to the SS. . Two separate HMAC keys are derived from the AK, for the BS-to-SS (downlink) and SS-to-BS (uplink) directions. A key encryption key (KEK) is also derived from the AK. The KEK is used for key exchange messages to obtain the traffic encryption keys (TEK) used when transmitting data.

In WiMax the Subscriber Station (SS) and Base Station (BS) exchange management messages for authentication as shown and then proceed to key management as shown in Figure 7 before transmitting data.

3.5 Implementation

The base WiMAX RSA-based authentication/authorization model (PKM), defined in the standard for fixed wireless access, is shown in Figure 5. The Subscriber Station initiates the authentication/authorization process. If authorized, the Base Station responds with an Authorization Reply which includes an Authorization Key and a Security Association. Details of the PKM exchange are described under Dynamics, above. In this model, only the Base Station authenticates the Subscriber, preventing theft of service.

The 802.16e standard for fixed and mobile broadband access [Lan06] extends the PKM model to PKMv2, based on the Extensible Authentication Protocol (EAP) [Abo04, Sta05]. PKMv2 allows alternative methods of authentication and supports mutual (two-way) authentication. The extended PKMv2 model, with new EAP messages, is shown in Figure 6. In the extended model, the Authenticator initiates authentication with a Request indicating the type of authentication to use. However, the Peer may prompt the Authenticator to begin the exchange by sending an EAP Start message. The Peer replies to the request with a Response with the same type ID, including such additional fields as are needed to satisfy the Request. The

Authenticator may perform the authentication, but more commonly will act as a “pass-through” and forward the Response to a central Authentication Server. After performing authentication, the Authenticator sends either a Success or Failure message. The Peer uses the payload included with the Success message to authenticate the Base Station. PKMv2 supports double-authentication, where the second round follows the same sequence as the first, but now encrypted with material from the first round.

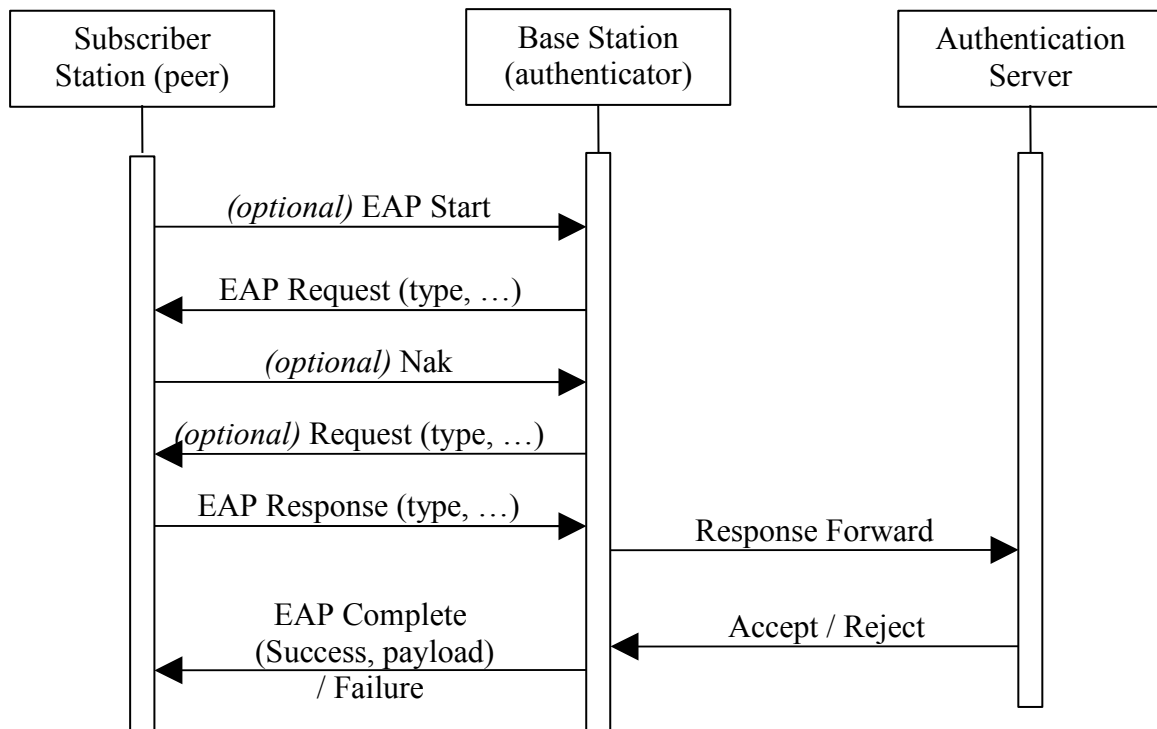


Figure 6. PKMv2 Authorization protocol

In the PKMv2 exchange, the peer may optionally reply to a Request with a Nak, indicating that it does not support the requested type of authentication and requesting an alternative. In response to a Nak, the Authenticator may reply with an alternative Request, or indicate Failure. To prevent man-in-the-middle attacks, the Authenticator ignores Naks if a Response is also received.

Each Security Association (SA) has two traffic encryption keys (TEK), shown in Figure 4. TEK0 is the current key, while TEK1 is its replacement. The lifetimes of the two keys overlap - the older key expires halfway through the life of the newer key. The newer key replaces the older key at or before its expiration, and a new replacement key is requested. To defend against statistical types of attack, keys should not be used for more than a limited period of time. The protocol assures both that keys are expired by both parties in the appropriate time window and that an active key is always available and in use, even in the presence of host or network latency. Key update is performed with Key Request and Key Reply messages, shown in Figure 7. Replay and man-in-the-middle attacks on key creation and update traffic are resisted by the use of sequence numbers and HMAC hash codes. During key exchange, the Subscriber Station encrypts uplink messages with TEK1, while the Base Station encrypts downlink messages with TEK0.

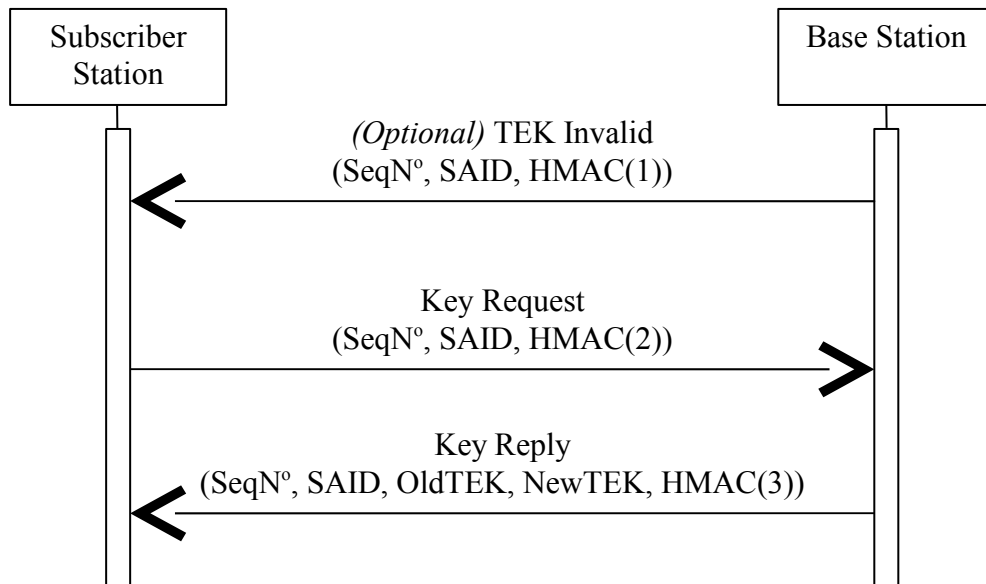


Figure 7. Creation of a Data Association Keys

3.6 Example resolved

Lisa requires her friends to use X.509 certificates and she authenticates them when they talk to her. Their communications are protected by periodically changing keys. Various other types of attack are also resisted.

1.15 3.7 Known uses

- Intel and Fujitsu have developed WiMax chips.
- Nokia and Nortel have some WiMax networking products.

3.8 Consequences

This pattern has the following advantages:

- Subscribers can authenticate the Base Station and vice versa.
- Use of the services provided by the network can be controlled.

Possible disadvantages include:

- Several flaws have been found in the basic standard. [Bar05], [Joh04], and [XuS06] discuss some of them. However, several corrections appear in later revisions of the WiMAX standard. An improved scheme for key management, based on EAP, is explained in [Yan05].
- Attacks to the application level are similar to other wireless devices [Fer05]; that is, this standard does not address issues at that level.

Related Patterns

- The WiMax Network Architecture pattern defines the infrastructure to apply security.
- Authorization [Sch06]. Defines the rights to access resources and here implies the right to use the communications links.
- Authentication and Access Control [Sch06].
- Credential [Mor06]. The use of credentials is required for authentication and access control.

Conclusions

We have distilled the fundamental aspects of the conceptual architecture of WiMax, in particular its architecture and security in the form of patterns. We have separated the conceptual architecture from implementation details, aspects which are intermingled in the standards. This separation is very important for evolving standards like this one, where the implementation is expected to change relatively frequently but the conceptual architecture should remain stable. These models can be used to understand the more complex aspects of the standard and to analyze weaknesses and improvements to the protocol. We need to write patterns for the IP Protocol and for X.509 Certificates.

Acknowledgements

Our shepherd, Markus Schumacher, provided valuable comments that improved the paper. The Secure Systems Research Group at FAU (www.cse.fau.edu/~security) provided useful discussions.

References

- [Abo04] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowitz, Ed., “Extensible Authentication Protocol (EAP)”, IETF RFC 3748, June 2004.
www.ietf.org/rfc/rfc3748.txt
- [Ang06] B. Angelov and B. Rao, “The progression of WiMAX toward a peer-to-peer paradigm shift”,
- [Bar05] M. Barbeau, “WiMax/802.16 threat analysis”, *Procs. of ACM Q2SWinet’05*, October 13, 2005, Montreal, Quebec, Canada.
- [Bur05] J.L. Burbank and W.T. Kasch, “IEEE 802.16 Broadband Wireless Technology and its application to the military problem space”, *Proceedings of the 2005 IEEE Military Communications Conference (MILCOM 2005)*, Vol. 3, 1905 – 1911, Oct. 2005
- [Del05] N. Delessy, and E. B.Fernandez, "Patterns for the eXtensible Access Control Markup Language", in *Proceedings of the 12th Pattern Languages of Programs Conference (PLoP2005)*, Monticello, Illinois, USA, 7-10 September 2005.
<http://hillside.net/plop/2005/proceedings/>
- [Del07] N. Delessy, E.B.Fernandez, and M.M. Larrondo-Petrie, "A pattern language for identity management", accepted for the *2nd IEEE Int. Multiconference on Computing in the Global Information Technology (ICCGI 2007)*, March 4-9, Guadeloupe, French Caribbean.
- [DOC00] "Data-Over-Cable Service Interface Specifications: Baseline Privacy Plus Interface Specification SP-BPI+-I05-000714", DOCSIS, July 2000,
<http://www.cablemodem.com/>.
- [Eck02] C. Ecklund, R.B. Marks, K.L. Stanwood, and S. Wang, “IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access”, *IEEE Communications Magazine*, vol. 40, No 6, 98–107, June 2002
- [Fer05] E. B. Fernandez, S. Rajput, M. VanHilst, and M. M. Larrondo-Petrie, “Some security issues of wireless systems,” in *Proceedings of IEEE Fifth International Symposium and School on Advanced Distributed Systems (ISSADS 2005)*, Guadalajara, Mexico, 24-28 January 2005, IEEE, and in F. F. Ramos et al. (Eds.)

Lecture Notes in Computer Science, LNCS Vol. 3563, Springer Verlag, Berlin Heidelberg, 2005, 388-396.

- [Fer06a] E.B.Fernandez, N.A.Delessy, and M.M. Larrondo-Petrie, "Patterns for web services security", in "*Best Practices and Methodologies in Service-Oriented Architectures*", L. A. Skar and A.A.Bjerkestrand (Eds.), 29-39, part of OOPSLA 2006, the *21st Int. Conf. on Object-Oriented Programming, Systems, Languages, and Applications*, Portland,OR, ACM, October 22-26.
- [Fer06b] E.B.Fernandez and N. Delessy, ""Using patterns to understand and compare web services security products and standards", *Proceedings of the IEEE Int. Conference on Web Applications and Services (ICIW'06)*, Guadeloupe, February 2006.
- [Joh04] D. Johnston and J. Walker, "Overview of IEEE 802.16 security", *IEEE Sec. and Privacy*, May/June 2004, 40-48.
- [Lan06] LAN/MAN Standards Committee, "IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems." February 2006, <http://ieeexplore.ieee.org/iel5/10676/33683/01603394.pdf>
- [Let01] S. Lehtonen and J. Parssinen, "A pattern language for key management", *Procs. of PLoP 2001*, http://jerry.cs.uiuc.edu/~plop/plop2001/accepted_submissions/accepted-papers.html
- [Mor06] P. Morrison and E.B.Fernandez, "The Credential pattern", *Procs. of the Conference on Pattern Languages of Programs, PLoP 2006*, Portland, OR, October 2006, <http://hillside.net/plop/2006/>
- [Sch00] D. Schmidt, M. Stal, H. Rohnert, and F. Buschmann, *Pattern-oriented software architecture, vol. 2 , Patterns for concurrent and networked objects*, J. Wiley & Sons, 2000.
- [Sch06] M. Schumacher, E.B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating security and systems engineering*, J. Wiley & Sons, 2006.
- [Sta05] D. Stanley, J. Walker, and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", IETF RFC 4017, March 2005
- [XuS06] S. Xu, M. Mathews, and C.T.Huang, "Security issues in privacy and key management protocols of IEEE 802.16", *Procs. of ACM SE '06*, Melbourne, FL, March 2006.
- [Yan05] F. Yang, H. Zhou, L. Zhang, and J. Feng, "An improved security scheme in WMAN based on IEEE Standard 802.16", IEEE Explore, <http://ieeexplore.ieee.org/iel5/10362/32965/01544255.pdf?arnumber=1544255>