Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Enhancement of 802.16e to Support EAP-based Authentication / Key Distribution Rev. 0**	
Date Submitted	**2003-12-21**	
Source(s)	Jeff Mandin Streetwaves Networking Amatzia 5 Jerusalem, Israel	Voice: 972-50-724-587 Fax: 972-50-724-587 mailto:jeff@streetwaves-networks.com
Re:	Call for contributions to 802.16e security adhoc (11/17/2003)	
Abstract	Description of requirements, mechanism, and security considerations for EAP in 802.16e	
Purpose	Provide basis for discussion and proposal of 802.16e Security Adhoc group	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Enhancement of 802.16e to Support EAP-based Authentication / Key Distribution

Jeff Mandin
Streetwaves Networking

Scope of this document

This document outlines how to incorporate Extensible Authentication[2] and key management into 802.16e on the basis of previous work in other environments (particularly 802.11[4])

For the purposes of this document, the actual EAP authentication exchange and "inner method" can be regarded as a "black box".

Background

Motivations

- To enable mobile operators to use other forms of credentials in addition to, or instead of, PKI-based device certificates (eg. Various forms of provider-supplied smartcards to be installed in an off-the-shelf device)
- facilitation of handover to other media (ie. 802.11) by providing hooks for preauthentication or other functions

Requirements

The solution must satisfy the following:

- Interoperability with non-EAP enabled 802.16/e systems
- Conformance to the standard EAP/802.1x model **so that methods and analysis pertaining to standard EAP will be applicable** (though not necessarily recommended) for 802.16e
- Support for 802.16 primary, static, and dynamic security associations. These include SAs for both unicast and non-unicast MAC-layer connections.
- Provision for ciphersuite selection and key refresh mechanisms
- Appropriate compliance with security recommendations for EAP in a wireless environment

Description of Solution

Model of operation

To describe the model of operation we must address:

- authentication flows
- key distribution and management
- coexistence with 802.16 PKM

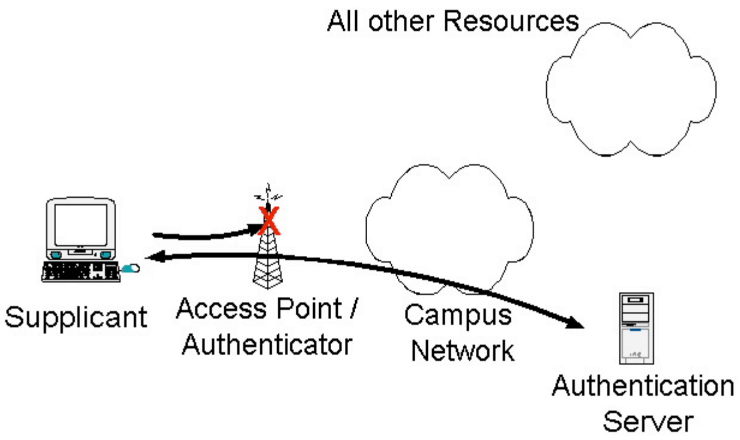
Model in Standard EAP/802.1x and 802.11i

Authentication flows in standard EAP/802.1x

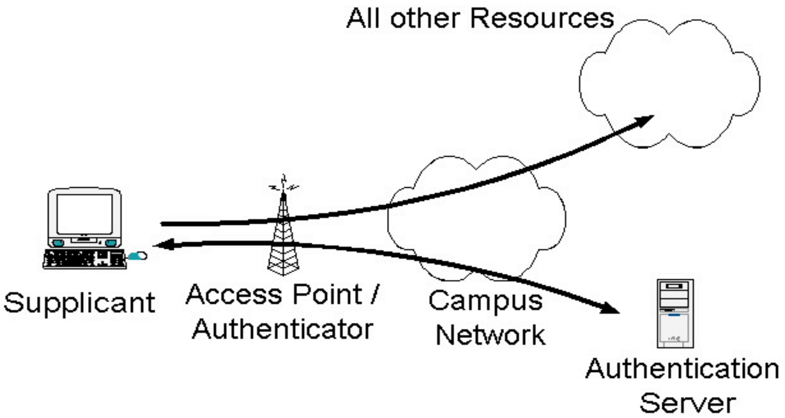
In EAP [2]/802.1x [1], authentication exchanges take place in the data plane, and *above the MAC layer*. Accordingly, the MAC layer itself must support the logical port model described in section xx of the 802.1x specification: the MAC link between the station and access point consists of two distinct **logical** links. These are termed the "controlled port" and "uncontrolled port".

<Diagram>

According to the model, EAP/802.1x packets initially flow to and from the logical uncontrolled port.



After authentication is successful, the logical "controlled port" becomes enabled – and regular data can then flow across the MAC link.



Key Distribution in 802.1xRev and 802.11i

As described in [3], successful completion of the EAP/802.1x inner method will (if desired) result in a shared-secret **AAA-Key** being exported to the Client and Authenticator from their respective EAP modules. Methods for derivation of traffic keys from the AAA-Key is ciphersuite-specific and not within the scope of the 802.1x standard.

802.11i [4] specifies mechanisms for using the AAA-Key to establish and maintain the required security associations for the 802.11 environment (including encryption key and hash derivation). Specifically, these include:

- "4-way handshake" for installing unicast session keying material
- "Group Key handshake" to "push" the data broadcast keying material to the client in EAPOL-KEY messages

Model for EAP/802.16e

The following shows the functions of PKM with the corresponding EAP/802.1x functionality:

PKM	EAP
AuthReq/Rsp	EAP Inner Method
AK transmission in AuthRsp	AAA-key derivation/export
KeyReq/Rsp	Key distribution in EAPOL-key

Note that in 802.16:

- EAP-based exchanges perform the same functions as the current PKM (ie. authentication and key/SA management).

- EAP-based functions must be separate from whatever convergence layer runs on top of the MAC layer.

Consequently:

- EAP operation and state machines will be completely contained **within** the 802.16 privacy layer.
- EAP messages will be encapsulated inside the payload of PKM MAC messages

Controlled and uncontrolled logical ports in 802.16 MAC

Our adaptation of the model into the MAC layer leads to the following assignment of the controlled/uncontrolled ports:

Uncontrolled Port	Basic and primary management connections
Controlled Port	Secondary Management connection

Format for transmission of EAP packets in 802.16 MAC Layer

<import from ETRI document>

Security Association and Key Management in EAP/802.16e

Requirements for SA establishment and key distribution correspond to those in 802.11i

- Primary SA establishment (for secondary mgt. Connection) follows 802.11i unicast session
- SA establishment for Transport connections (static or dynamic) follows the 802.11i “group key handshake”

Details are TBD.

Coexistence of EAP-based and PKM-based authentication

Each BS and SS MUST support PKM-based authentication. Support for EAP-based authentication is optional in both the BS and SS.

A particular instance of a SS’s network entry procedure will use either EAP-based or PKM-based authentication, as indicated by the SBC capabilities exchange. It will not use both EAP and PKM in the same network entry procedure, as this would require tunnelling one authentication protocol within the other.

Message sequences at network entry with EAP authentication

1. Ranging and capabilities exchange

2. multiple EAP-request/EAP-response exchanges (in PKM encapsulation, initiated by BS)
3. EAP-success (BS to SS), establishment of Primary SA (secondary management connection)
4. Establishment of transport and non-unicast Security Associations
5. Registration
6. IP address acquisition
7. connection establishment via DSx

< diagram>

Cryptographic Protection of EAP exchanges

The specific threats against EAP traffic transmitted over "insecure media" (eg. Wireless) are as follows (from [2]):

[1] An attacker may try to discover user identities by snooping authentication traffic.

[2] An attacker may try to modify or spoof EAP packets.

[3] An attacker may launch denial of service attacks by spoofing lower layer indications or Success/Failure packets; by replaying EAP packets; or by generating packets with overlapping Identifiers.

[4] An attacker may attempt to recover the pass-phrase by mounting an offline dictionary attack.

[5] An attacker may attempt to convince the peer to connect to an untrusted network, by mounting a man-in-the-middle attack.

[6] An attacker may attempt to disrupt the EAP negotiation in order cause a weak authentication method to be selected.

[7] An attacker may attempt to recover keys by taking advantage of weak key derivation techniques used within EAP methods.

[8] An attacker may attempt to take advantage of weak ciphersuites subsequently used after the EAP conversation is complete.

[9] An attacker may attempt to perform downgrading attacks on lower layer ciphersuite negotiation in order to ensure that a weaker ciphersuite is used subsequently to EAP authentication.

[10] An attacker acting as an authenticator may provide incorrect information to the EAP peer and/or server via out-of-band mechanisms (such as via a AAA or lower layer protocol). This includes impersonating another authenticator, or providing inconsistent information to the peer and EAP server.

Of the above, [3] would appear to be not relevant as DoS can be easily accomplished via interference with the RF. Whereas [4]-[10] involve using EAP to exploit weaknesses elsewhere in the security architecture which we take care to prevent.

Hence it appears acceptable to rely exclusively on the cryptographic protection provided by the EAP inner method.

Specific 802.16e text changes

<tbd>

References

[1] IEEE 802.1Xrev
[2] RFC 2284bis IETF draft
[3] EAP Keying Framework IETF draft
[4] IEEE 802.11i