Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Definition of PMK scope via AuthenticatorId
Date Submitted	**2005-06-08**
Source(s)	Jeff Mandin Streetwaves Networking Amatzia 5 jeff@streetwaves-networks.com Jerusalem, Israel
Re:	IEEE P802.16REVe/D8 SB re circ
Abstract	Definition of PMK scope via AuthenticatorId
Purpose	Adopt changes.
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>.

Definition of PMK scope via AuthenticatorId

Jeff Mandin

1. Problem statement

From the IETF review:

Since EAP authenticators may have multiple ports, the
EAP peer needs to be aware of the authenticator identity;
this is not defined in IEEE 802.16e D8.

The BS extends the scope of the PMK by setting the
"Handover optimization flags" (section 6.3.2.5.53) to tell the
MS to reuse a PMK on a target BS.

However, this does not enable the MS to know all the BSes that
share a given PMK. Giving the MS complete knowledge of the
authenticator key scope would enable the 3-way handshake
to activate all the AKs derived from a particular PMK.

The lack of an authenticator identity also means that
IEEE 802.16e provides incomplete support for Channel
Bindings, described in [RFC3748] Section 7.15.
Lower layer support for Channel Bindings requires that the lower
layer provide the same information to the peer as the authenticator
provides to the backend authentication server.

IEEE 802.16e D8 provides the peer/BS with the Called-Station-Id (BS MAC
address), Calling-Station-ID (MS MAC Address) & SSID and these same
parameters can be provided to the AAA server in the Access-Request (assuming
that IEEE 802.16e follows the guidelines described in [RFC3580]). The
major parameter that is missing within the lower layer is the
NAS-Identifier or authenticator identity.

As described in [RFC3748] Section 7.15 verifying the authenticator
identity between the EAP peer, authenticator and server protects
against impersonation attacks. The use of an authenticator identity also
enables the MS to efficiently manage its PMK cache and to determine
whether the PMK is being used outside its authorized scope.

2. Overview of solution

We add the notion of an explicit AuthenticatorId which is used as follows:

- Each BS is associated with one or more Authenticators. The corresponding AuthenticatorId(s) is

included with the BS information in the NBR_ADV message

- An MS uses the AuthenticatorId to determine (upon entry to a particular BS) whether it can derive an AK for that particular BS from a particular Authenticator-specific PMK that it possesses.

- The MS can then perform HO among interfaces on the same authenticator without there being a need to perform the 3way handshake again. This is because accepted practice in the EAP architecture is such that performing the 3way handshake activates an AK for each port on the authenticator

3. Text changes

[Insert the following paragraph to page 230 line 56:]

The 3-way handshake demonstrates liveness of the BS and MS, proves mutual possession of the AK, and activates all of the AKs associated with the authenticator together with their AK context. When performing HO to a target BS associated with the same authenticator (as indicated in NBR_ADV) as the serving BS, no 3-way handshake is required - as all AKs on the authenticator are already active.

[Modify page 231 line 7 as follows:]

2. ~~If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover,~~ If the BS has an active AK for the MS, the BS begins the 3-way-handshake by appending the SA Challenge Tuple TLV to the RNG-RSP.

[Add the following to table 358 (DCD Channel Encoding):]

AuthenticatorId | <code> | variable | the identity of an EAP authenticator associated with the BS

[Insert new section 11.9.35:]

AuthenticatorId

Description: The Identity of the EAP Authenticator associated with the BS. This is the value that is used as the NAS_Identifier AAA attribute

Type	Length	Value
Tbd	variable	Identity of the EAP Authenticator associated with the BS

[Delete the following text from table 108f and renumber the text entries lying below it:]

~~**Bit #1: Omit PKM Authentication phase except TEK**~~
~~phase during current re-entry processing~~

[Delete the following text from page 115 line 52 and renumber the text entries lying below it:]

~~**Bit #1: Omit PKM Authentication phase except TEK phase during current re-entry processing**~~