Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	Binding of PMK to EAP channel parameters	
Date Submitted	**2005-6-8**	
Source(s)	Jeff Mandin Streetwaves Networking Amatzia 5 Jerusalem, Israel	jeff@streetwaves-networks.com
Re:	IEEE P802.16REVe/D8 SB re circ	
Abstract	Binding of PMK to EAP channel parameters	
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>.	

Binding of PMK to EAP channel parameters

Jeff Mandin

1. Problem statement

From the IETF review:

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]). ….

As described in [RFC3748] Section 7.15 verifying the authenticator
identity between the EAP peer, authenticator and server protects
against impersonation attacks. …..

In order to bind identities to the keying material,
the lower layer authenticator and peer identities need
to be explicitly stated within the 3-way handshake,
and bound to PMK.

2. Overview of solution

We add fields to the SA-TEK-Challenge, SA-TEK-Request, and SA-Challenge tuple TLV so as to enable bidirectional confirmation of identities and additonal parameters that are communicated via "channel binding" methods.

3. Text changes

[Add the following to table 37g following the AKID attribute:]

AuthenticatorId | the identity of the EAP authenticator associated with the BS

[Add the following to 11.7.23 following the AKID attribute:]

AuthenticatorId | the identity of the EAP authenticator associated with the BS

[Add the following to table 37h following the AKID attribute:]

PeerId | the MAC Address of the MS

[section 7.8.1 Add a new numbered item in between 2 and 3:]

3. If the MS received the AuthenticatorId and other channel parameters via the EAP method, it shall check whether BS supplied these same parameters in the SA-TEK-Challenge. If the AuthenticatorId or parameters do not match or were not supplied, the MS SHOULD log the event as a possible security breach and the MS MAY elect to terminate communications with the BS.

[section 7.8.1 Add a new numbered item in between 4 and 5:]

5. If the BS received channel parameters (such as AAA attributes) via the EAP method, it shall check whether MS supplied these same parameters in the SA-TEK-Request. If the channel parameters do not match or were not supplied, the BS SHOULD log the event as a possible security breach and the BS MAY elect to terminate communications with the MS.

[Add the following to page 528, line 62 following the AKID attribute:]

AuthenticatorId | code | variable | the identity of the 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 sent in the NAS_Identifier AAA attribute

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

[insert new section 11.9.36:]

PeerId

Description: The MAC address of the SS. This is the value that is sent in the Calling-Station-Id AAA attribute

Type	Length	Value
Tbd	6	MAC address of the SS