Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	EAP channel binding support for 802.16e
Date Submitted	**2005-05-05**
Source(s)	Jeff Mandin Runcom Hachoma 2 jeff@streetwaves-networks.com Rishon Lezion, Israel
Re:	IEEE P802.16REVe/D7 SB re circ
Abstract	EAP channel binding support for 802.16e
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>.

EAP Parameter and Channel Binding support in 802.16e

Jeff Mandin (Runcom)

1. Problem statement

As described in the EAP keying draft (draft 6 section 7.3), 802.16e - as an "EAP lower layer" - should provide a mechanism to enable the Peer and Authenticator to confirm the security parameters they have received about each other (via the EAP method and AAA protocol respectively).

These parameters would include the identity of the Authenticator, as well as the additional parameters that can be exchanged by EAP methods supporting channel binding (RFC 3748 section 7.15).

[We note parenthetically that in the case of FBSS, a single authentication entity supports multiple BS interfaces and can perform FBSS among them (ie. a single authentication suffices for all of the interfaces). This is the primary (perhaps the only) case in 802.16e where a single authenticator supports multiple instances of the 802.16 MAC/PHY.]

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 37f following the AKID attribute:]

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

[section 7.8.1 Add a new 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-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 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-Challenge. 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 11.9.31:]

EAP AuthenticatorId

Description: The Identity of the Authenticator associated with the BS. Typically this is the value that is contained in the NAS_Identifier AAA attribute

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