

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >
Title	EAP channel binding support for 802.16e
Date Submitted	2005-04-29
Source(s)	Jeff Mandin Streetwaves Networking Amatzia 5 jeff@streetwaves-networks.com Jerusalem, 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 Channel Bindings in 802.16e

Jeff Mandin (Runcom)

1. Problem statement

An EAP channel binding method will provide the MS with an identifier associated with the Authenticator. This Identifier specifies the key scope and protects against the “lying NAS” scenario.

Since we want access to the key scope information also in the case of FBSS, we do not include the Authenticator Id in the 3 way handshake. Rather we use the channel binding method.

2. Text changes

1. Add 6-byte AuthenticatorId field to the UCD message
2. Change AK derivation (page 191 line 48) to:

AK=Dot16KDF(PMK, SSID | BSID | AuthenticatorId | “AK”, 160)