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	
Release	
Patent Policy and Procedures	

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)