Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Security text Corrections
Date Submitted	**2005-09-11**
Source(s)	Jeff Mandin jeff@streetwaves-networks.com
Re:	Recirc
Abstract	Security text Corrections
Purpose	Adoption
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>.

Security text Corrections

Jeff Mandin

These are fixes of mostly editorial nature from various individuals.

1. Remedy 1

- Change every instance of SSID in section 7.2.2.2 to MS MAC address
- Change SSID in table 132a to MS MAC address
- Change SS ID in table 37b to MS MAC address
- Delete SSID from the Acronyms list

2. Remedy 2

[Modify section 7.8.1 step 6. as follows:]

6. Upon receipt of PKMv2 SA-TEK-Response, an MS shall verify the HMAC/CMAC. If the HMAC/ CMAC is invalid, the MS shall ignore the message. Upon successful validation of the received PKMv2 SATEK-Response, the MS shall install the received TEKs and associated parameters appropriately. Verification of HMAC/CMAC is done as per sections 7.5.3 and 7.5.4. ~~The MS also must verify the BS's security capabilities encoded in the Security Negotiation Parameters attribute against the security capabilities provided by the BS through the SBC-RSP message. If security capabilities don't match, the MS should log the problem.~~

The MS also must verify the BS's security negotiation parameters TLV encoded in the Security Negotiation Parameters attribute against the security negotiation parameters TLV provided by the BS through the SBCRSP message. If security capabilities do not match, the MS should report the discrepancy to upper layers. The MS may choose to continue the communication with the BS. In this case, the MS may adopt the security negotiation parameters encoded in SA-TEK-Response message.

3. Remedy 3

[modify page 222, line 63 as follows:]

The product of the EAP exchange which is transferred to 802.16 layer is the Master Session Key (MSK), which is a minimum of 512-bits in length. ~~MSK. This key is derived (or may be equivalent to the 512-bits Master Session Key (MSK)).~~

4. Remedy 4

[modify page 54 line 26 as follows:]

In the case of EAP re-authentication~~, using EAP methods deriving keys,~~ "HMAC Digest/CMAC Digest" and "Key Sequence Number" attributes shall be included. At initial EAP authentication, these attributes are omitted.