Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Outcomes of NetMan Security Problems Discussion**
Date Submitted	**2006-03-07**
Source(s)	David Johnston Intel Corporation 2111 NE 25th Ave Hillsboro, OR, 97006 USA Voice: +1 503 264 3855 Fax: +1 503 264 3483 dj.johnston@intel.com
Re:	Scheduled NetMan Security discussion
Abstract	Provides the results of the Wednesday Evening NetMan Security Discussion.
Purpose	To report out on the results of the Wednesday evening Netman security discussion.
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>.

Netman Security Discussion Report

David Johnston
Intel Corporation

The following are the conclusions resulting from the Wednesday evening NetMan Security Discussion.

1) Revisiting a BS, after losing the AK context for that BS and recomputing the old AK is a problem. The PN will restart from 0 and so PN,AK reuse will occur and so Key leakage will occur.
2) PMK Lifetimes are a problem if the 802.16 defined key lifetime conflicts with the key lifetime handed down from EAP.
3) Non defined behaviour of the BS and MS AK state machine in the face of bad CMAC/HMAC values is a potential problem. If either end uses responds to badly authenticated packets in some way other than silently discarding those messages, a DoS attack is possible.
4) Emergency Access is a problem. There is no defined mechanism for the BS to identify an MS attempting to access emergency services.