| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **Key hierarchy changes** |
| Date Submitted | **2005-03-10** |
| Source(s) | Jeff Mandin<br>Streetwaves Networking<br>Amatzia 5<br>Jerusalem, Israel<br><br>Voice: 972-50-5724-587<br>Fax: 972-50-5724-587<br>mailto:jeff@streetwaves-networks.com |
| Re: | Recirc |
| Abstract | **Key hierarchy changes for inclusion of nonces in "Authenticator Key"** |
| Purpose | Acceptance into TGe Draft document |
| 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>. |

# PKMv2 Key Hierarchy Changes

*Jeff Mandin*
*Streetwaves Networking*

## 1 Problem Statement

Currently, the PKMv2 keying material received from the AAA-Server is used directly for protecting traffic.

This causes extra rekey exchanges with the AAA server that can be avoided simply by using the nonces in the 3way handshake for the derivation of the traffic protection keys.

## 2 Specific text changes

[**Modify page 184, line 38-40**]

The PMK derivation from the AAA-key is as follows:

PMK = truncate ( Dot16KDF(AAA-key, BSRandon | SSNonce) , 160 )