IEEE 802.16 Working Group on Broadband Wireless Access

http://WirelessMAN.org

Dr. Roger B. Marks
NIST
325 Broadway, MC 818.00
Boulder, CO 80305 USA
Tel: +1 303 497 7837
mailto:marks@nist.gov
21 July 2005

To: Bernard Aboba, IETF Liaison to IEEE 802; Co-Chair, IETF EAP Working Group

Dear Mr. Aboba,

On behalf of the 802.16 Working Group (WG) membership, I would like to thank you and the IETF EAP WG for your quick and extensive response to our request for an expert review of the use of EAP-based security in P802.16e/D8, as detailed in your liaison statement of 16 June (IEEE L802.16-05/041).

WG members have used the review to improve our draft security specifications. We invite IETF the reviewers to examine the D10 draft, to be made available soon, and we welcome your opinions.

The following is a brief summary of 802.16 WG's responses to the issues raised in the review:

1) Regarding the issues termed by the reviewers as "critical":
a. Man-in-the-middle attack on EAP-after-EAP mode
This issue has been addressed by cryptographic binding, as suggested in the review. We are very appreciative of the help provided by reviewer Yoshihiro Ohba in understanding and resolving this issue.

b. EAP method requirements
The current draft incorporates a reference to the mandatory method requirements in RFC 4017 ("EAP Method Requirements for Wireless LANs") with a caution that use of non-compliant methods could result in insecure systems. Additionally, some 802.16 members have begun work on a document for 802.16 method requirements to be submitted to an appropriate standards organization.

2) Other issues from the review that have been addressed in P802.16e/D10 include: Integrity protection of messages during reauthentication [Review Item 2], secure confirmation of insecurely negotiated parameters [Item 6], key lifetime specification [Item 7a], explicit specification of the PMK Secure Association [Item 7c], and key caching and deletion clarifications [Item 8].

3) Details of the 802.16e Task Group's deliberations on other issues are found in the comment resolution databases (IEEE 802.16-05/035r4 and IEEE 802.16-05/045r2). Jeff Mandin, the 802.16 WG's Liaison to the IETF, is available for assistance.

As always, we look forward to continued cooperation with the IETF.

Sincerely,

Roger B. Marks
Chair, IEEE 802.16 Working Group on Broadband Wireless Access

cc: Jari Arkko, Co-Chair, IETF EAP Working Group
Bert Wijnen, Co Area Director, Operations and Management Area, IETF
Lakshminath Dondeti, Co-Chair, IETF MSEC Working Group
Russ Housley, Security Area Director, IETF
Dorothy Stanley, IEEE 802.11 liaison to IETF
iab@ietf.org
iesg@ietf.org
statements@ietf.org
Jeff Mandin (802.16 Liaison to IETF)
Brian Kiernan (Chair, 802.16 Task Group e)
Phil Barber (Chair, 802.16 NetMan Task Group and 802 Architecture Group Representative)
David Johnston (802 Architecture Group Representative)
Paul Nikolich, Chair, IEEE 802 LAN/MAN Standards Committee
Paul Congdon, IEEE 802