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
15 September 2005

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

Dear Mr. Aboba,

The 802.16 Working Group (WG) membership would once again like to thank you and the IETF EAP WG for your efforts in reviewing the security and usage of EAP in the 802.16e draft.

This process has been exceptionally productive, as is clear from the manner in which most of the original review comments have been addressed by the 802.16 Working Group. The assistance you have provided has enabled the Working Group to improve the security and robustness of the 802.16e draft.

In reference to your latest liaison statement (IEEE L802.16-05/050, dated September 12):

1. We would like to offer responses to certain of the issues listed as outstanding:

    a. Regarding the issue of explicit prohibition of AK sharing:

    The 802.16 membership understands that this is an important guideline for key management. However, some members believe that the requirements of specific operator deployment scenarios may justify relaxation of the restriction and that it is not the role of an air interface specification such as 802.16e to impose firm restrictions of this type.

    We have heard that some implementations – notably the WiMAX Forum Network Working Group's draft specification – have in fact adopted the stringent approach of prohibiting sharing of AKs between Authenticators.

    We will continue to consider the constraint as the standard progresses.

    b. Regarding the issue of binding the PMK to its scope in the 3-way handshake, including making the Authenticator identity explicit for support of Channel Binding:

    As with the issue of AK sharing, 802.16 members see a division between the MAC functions to be defined by the air interface specification and the rest of the operator's network. To accomplish this division within the EAP architecture, 802.16e defines the "handover flags" that enable the (non-MAC) entity performing the functions of the EAP authenticator (e.g. AAA-client functionality) to signal

appropriate behavior to the MAC layer. One consequence of this scheme is that 802.16e does not explicitly list rules for setting the handover flags.

Another consequence is that the scope of the PMK remains unavailable to the MAC layer, so that explicit binding of the PMK to its context in the 3-way-handshake and full support of channel binding is not possible.

We note, however, that 802.11i lacks both key context binding and full support for channel binding but has enjoyed successful deployment nonetheless. Also, our understanding is that partial support of channel binding (using parameters such as Called-Station-ID) is still possible in 802.16e.

c. Regarding the issue of "synchronization of key context and authorizations":

In 802.16, a group of data-traffic authorizations is associated with an authenticated user. These authorizations are represented by SAIDs and are included in the final message of the 3-way handshake. However, 802.16e does not include the notion of a service authorization in the manner of 802.11 (i.e., where an AP can offer a BSS ID "guest" with one set of service permissions and another BSS ID "corporate" with a different set). Consequently, it appears that authorizations (to the extent that there are any in 802.16e) are in fact synchronized between the BS and MS. Key context is addressed in item b) above.

2. There were several issues which we expect to refer to 802.16's Network Management (NetMan) Task Group. These include:

a. EAP State machine integration

b. PMK SA definition clarification

c. Random Number Generator requirements

802.16's NetMan Task Group is developing the 802.16g project, chartered to define the 802.16 management plane. The NetMan Task Group has noted these key management issues and intends to address them in the course of its work – together with the issues that you raised regarding the IPv6 management text.

3. The textual clarifications ("nits") that were suggested have all been incorporated into the 802.16e text.

We appreciate the seriousness and dedication of the reviewers and 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