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
17 March 2005

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

Dear Mr. Aboba,

Thank you for taking the time to speak with officials of the IEEE 802.16 Working Group (WG) on 9 March 2005, as recorded in IEEE L802.16-05/019, to discuss liaison communications between IETF and IEEE 802.16. During this call, you noted that your meeting with IEEE 802 in January 2004 <http://www.drizzle.com/~aboba/IEEE/coord.ppt> had led to the suggestion that draft IEEE 802 MIBs be reviewed by a "MIB Doctor" in IETF <http://ops.ietf.org/mib-doctors.html>. The second major topic of this call was the use of EAP and the possibility that the 802.16 WG might request a basic review of conformance to RFC 3748.

To place our work in context, the published IEEE Std 802.16-2004 defines a fixed broadband wireless access air interface. The 802.16 WG is currently developing several amendments to that standard. One of these amendments, P802.16e, will amend the standard to add mobility functionality to the base fixed broadband wireless access air interface. This work includes the development of security protocols that take advantage of EAP to provide an authentication mechanism. The IEEE 802.16 working group respectfully requests IETF EAP WG review of the method of EAP use employed in P802.16e. The specification details are defined in IEEE Std 802.16-2004 as well as in draft P802.16e/D7, which is presently being created by the Technical Editor following the WG's Session #36 of 14-17 March 2005.

We would like to bring particular attention to the following aspects of the defined security mechanisms:

a) To support fast handover in mobile 802.16 systems, the 802.16e PKMv2 protocol defines a key derivation algorithm based on the definition of the AAA-Key-A,B,C... keys as described in the EAP Key Framework draft draft-ietf-eap-keying-05.txt. This sort of security protocol typically requires great care in its production and great scrutiny in review to render it secure and functional. The complexity and novelty of the solution method gives us cause to solicit external expert review.

b) Another area of concern is the PKMv2 TEK transfer mechanism that securely transfers keys generated in a base station to a subscriber station. It is not clear if this mechanism meets all the requirements of the EAP key framework requirements for transient session keys.

c) Finally, the MBS (Multimedia Broadcast Service) and Multicast security mechanisms in P802.16e/D7 describe multicast rekeying mechanisms that may overlap the work of the IETF MSEC working group.

Separately, 802.16's Network Management Task Group is developing the P802.16f project, which defines a MIB to facilitate the management of fixed mode 802.16 systems based on IEEE 802.16-2004. We respectfully request an IETF MIB expert to review P802.16f/D3 for compatibility with IETF MIB-related standards. We appreciate your efforts to obtain the expeditious assignment of a MIB Doctor (Bert Wijnen) and we understand that the document has already undergone a preliminary review. The P802.16f draft is open for IEEE-SA Sponsor Ballot until 27 April 2005. I welcome your comments and will gladly submit them to Sponsor Ballot on your behalf.

Per the letter of 26 July 2004 from IEEE 802 to IETF's Bert Winjen and Bernard Aboba entitled "IEEE 802 archive access policy for IETF coordination purposes," I am authorized to grant membership in IEEE 802.16 to an IETF WG chair upon request. As a member of the IEEE 802.16 WG, the IETF WG chair will receive username/password access to IEEE 802.16's drafts. These drafts are IEEE-SA copyright controlled and shall be used by the IETF WG solely for the purposes of IETF research and standards development. They shall not be redistributed outside of the IETF WG, or made use of in IETF drafts, without prior approval.

Please provide me the name of the person most appropriate for membership in the IEEE 802.16 WG in order to expedite IETF participation in our process.

We greatly appreciate the enthusiasm that IETF members have shown in assisting the IEEE 802.16 WG on these matters and look forward to continued future cooperation.

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
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