Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Comments to Security Ad Hoc Document C802.16e-03/71r2**
Date Submitted	**02-Jan-2004**
Source(s)	Vladimir Yanover Alvarion Ltd. 11/5 Shtern Str. Herzlya, Israel Voice: +972-36457834 Fax: +972-36456222 mailto:vladimir.yanover@alvarion.com
Re:	IEEE C80216e-03/71r2
Abstract	The document contains questions and comments to Security Ad Hoc Submission IEEE C80216e-03/71r2
Purpose	The document is submitted for consideration by Security Ad Hoc Group
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 text 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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Comments to Security Ad Hoc Submission C80216e-03/71r2

Vladimir Yanover

Alvarion Ltd.

This document contains certain questions and comments to Security Ad Hoc Submission C80216e-03/71r2 by Jeff Mandin. Original text appears in black; comments and questions appear in **blue**.

1.1 Motivations

To enable mobile operators to use other forms of credentials in addition to, or instead of, PKI-based device certificates (eg. various forms of provider-supplied smartcards to be installed in an off-the-shelf SS device)

1) Existing 802.16 standard does not specify where device certificate is stored, particularly it can be stored at smartcard. If so, why we need yet another auth procedure?

2) EAP ID says (3.1 Lower layer requirements): "EAP assumes that lower layers either provide physical security (e.g., wired PPP or IEEE 802 links) or support per-packet authentication, integrity and replay protection. EAP SHOULD NOT be used on physically insecure links (e.g., wireless or the Internet) where subsequent data is not protected by per-packet authentication, integrity and replay protection."

802.16 does not provide physical security and does not support per-packet authentication or integrity or replay protection [limited support of user data auth/integrity/replay protection is provided by Privacy sublayer]. So a suggestion for using EAP in 802.16 instead of Privacy sublayer must include serious analysis of applicability of EAP in this situation. In absence of such analysis, conclusion of section 4.5 "appears acceptable to rely exclusively on the cryptographic protection provided by the EAP inner method" seems unsubstantiated. I would rather summarize section 4.5 as "with EAP we don't have anything to relay on but EAP inner method".

3) It was an assumption in 802.16 development that any upper layers stuff [including security] can be launched over wireless link protected by 802.16 Privacy, above 802.16 MAC. This option is not covered by the document at all. By the way, wouldn't EAP procedures be less vulnerable if run over Privacy-protected link?

4) What about restriction of max 256 authentications per System Port [802.1X]? Is it applicable?

facilitation of handover to other media (ie. 802.11) by providing hooks for preauthentication or other functions

To consider this issue we need a model of [or assumptions on] heterogenous [e.g. 802.11-802.16] networks, otherwise any idea is good [and bad]

Interoperability with non-EAP enabled 802.16d/e systems

More precise wording is needed here. I didn't find in the document any explanation of this goal as well as whether the goal is reached.

Does it mean that there should be two modes, one limited to “Privacy sublayer” specified in REVd ? If yes, I would support that.

Compatibility with the standard EAP/802.1x model **so that methods and analysis pertaining to standard EAP will be applicable** (though not necessarily recommended) for 802.16e

802.1X defines “Devices that attach to a LAN, referred to in this standard as Systems (3.1.6), have one or more points of attachment to the LAN, referred to in this standard as Ports (3.1.3)”.

802.16 network is essentially different from LAN. So it is NOT a situation when every definition or statement from 802.1X is automatically consistent with 802.16 standard. What is Port in 802.16: one connection or all togetether or Basic + two management connections constitute one port while traffic connections another one? Port is bidirectional while connections are not. 802.1X Port can be *blocked* **while 802.16 connection can be created or deleted. EAPOL addressing [802.1X, 7.8] is not directly applicable to 802.16 etc. etc.**

Seems like many things must be re-defined and/or clarified before we can think on applying methods/analysis pertaining to standard EAP/802.1X to 802.16.

Support for 802.16 primary, static, and dynamic security associations. These include SAs for both unicast and non-unicast MAC-layer connections.

Needs clarification. In which sense they must be “supported”? To be able to establish SAs instead of legacy Privacy sublayer?

The document does not explain explicitly relation between suggested new security framework and existing Privacy stuff, so one may say that above requirement is not staisfied.

Provision for ciphersuite selection and authorization refresh

The document alternately uses terms “authorization” and “authentication”. Generally these are two different things. In 802.16 authentication is a part [step] of SS authorization [see 7.2.1 in the Std.]. Authorization includes also KEK transfer and SAs creation.

Opposite, in EAP ID "successful authentication" is defined as "an exchange of EAP messages, as a result of which the authenticator decides to allow access by the peer, and the peer decides to use this access. The authenticator's decision typically involves both authentication and authorization aspects; the peer may successfully authenticate to the authenticator but access may be denied by the authenticator due to policy reasons.”

This must be clarified.

Each BS and SS MUST support Legacy-PKM-based authentication. Support for EAP-based authentication is optional in both the BS and SS.

If sugested approach is not a superset of legacy PKM in 802.16 (seems like that), then it is rather “yet one more security scheme" than “extended PKM”, so I would recommend change misleading term “extended PKM”. Anyway there is a strong need in explanation of relationship between “extended PKM” and "legacy PKM"

Appropriate compliance with security recommendations for EAP in a wireless environment

Which? A reference is needed. See also above comment on section 4.5.

These Extended PKM Logical Control Interface will follow the logical interface definitions given in the EAP state machine draft [5] (or successor document) for the lower-layer interfaces of the supplicant [section 4.1] and authenticator [section 5.1].

1) Which model is to be supported: Switch? Passthrough?

2) [5] probably points to "State Machines for EAP Peer and Authenticator" (draft-ietf-eap-statemachine). The question is whether the state machine [that specifies behavior of unerlying layer expected by EAP] is consistent with 802.16 MAC?

3.1.1 Overview of Components of the Extended Privacy Layer

The .16e “Extended Privacy” Layer contains:

EAP methods – these are outside the scope of the current specification, and would typically include one or more strong, well-understood authentication algorithms such as EAP-TLS.

On one hand, EAP authentication is considered as a replacement [at least in some cases] of existing Privacy. On the other hand, EAP methods are out of the scope of the standard. Then, how interoperability will be achieved?

My answer to this and similar questions is that we have to decouple EAP stuff from 802.16 MAC/PHY specifications and make EAP running above MAC [e.g. through Secondary Management connection] so that 802.16 link would be transparent for EAP packets. Then MAC/PHY spec would remain a compatibility standard while EAP operations would become a recommended practice for communiation between Supplicant and Authenticator, that might be SW modules at SS and BS or at another network peers or smart card or whatever.

4.2 Link Control

The link control model is the logical entity that restricts the flow of most data packets until authentication has completed.

Probably there is no need in such entity as before auth comes to successfull end [presumably at network entry], no traffic connections were created so far. This is different from LANs which does not have procedures similar to connection setup and data packets may [and must] flow to the network each time when appear at MAC SAP.

4.2.1 Controlled/Uncontrolled Port

Associated with the link control module are the notions of a logical "controlled port" and "uncontrolled port".

The logical "uncontrolled port" carries the packets which can flow when authentication state is "not authenticated" – ie. ranging, sbc, and pkm. The logical "controlled port" carries the packet traffic which is permitted by 802.16 to flow only after authentication has completed successfully.

There are no "ports" in 802.16 MAC. New terms should be defined based on existing terms: connections etc.

4.4. Format for transmission of EAP packets in 802.16 MAC Layer

Important question: why EAP packets cannot be transferred over Secondary Management connection? If they can, we just specify formats of messages with no regard to MAC PKM messages. After all, this is exactly the role of Secondary Management connection: transport of upper layer protocols like DHCP.

4.5 Cryptographic Protection of EAP exchanges

Hence it appears acceptable to rely exclusively on the cryptographic protection provided by the EAP inner method.

I would rather summarize section 4.5 as "we don't have anything to relay on but EAP inner method".

If so, then probably certain [mandatory?] EAP method[s] should be suggested to provide some level of interoperability?

[Picture from Appendix A]

What is "802.16 Basic Setup"? One may guess that it is something related to [standing for?] Network Entry.