Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Resolutions to Outstanding 3way Handshake issues**
Date Submitted	**2004-07-14**
Source(s)	Jeff Mandin Streetwaves Networking Amatzia 5 Jerusalem, Israel 93148 jeff@streetwaves-networks.com
Re:	C80216e/D9 Recirc 4
Abstract	**Resolutions to Outstanding 3way Handshake issues**
Purpose	Acceptance into 802.16e text
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>.

Resolutions to Outstanding 3way Handshake issues

Jeff Mandin
Streetwaves Networking

1 Problem statement

There are some known issues to be resolved for the 802.16e 3way handshake.

Many of these derive from the IETF EAP WG review of 802.16e use of EAP (found at http://www.drizzle.com/~aboba/EAP/review.txt)

1.1 Issue 1 - The identities of the BS and MS should be explicitly included in the handshake messages.

The identities are required in the "Bellare-Rogaway 3 party" algorithm on which the 3 way handshake is based.[1] Including the identities enables the handshake to be provably correct as in the Bellare-Rogaway paper.

Omitting the identities creates the "man in the middle" vulnerability described by Jesse Walker in a review of the EAP-PSK method (which also uses Bellare-Rogaway) at http://mail.frascone.com/pipermail/eap/2005-June/003443.html (item 3).

Similarly, inclusion of the identities in the handshake was the recommendation of the IETF EAP WG review.

1.2 Issue 2 - The BS should provide the MS with notification of the authenticator (or authenticators) to which it is attached

1.3

1.4

1.5

For background, see the IETF review, and also Alper Yegin's comments at http://mail.frascone.com/pipermail/eap/2005-June/003475.html :

```
I think there is one alternative approach. Even if the NAS does not
convey the list of ports to the EAP peer, the peer may discover them as
it encounters each port. For example, when the peer moves to port Y
(from port X where it had performed the EAP authentication), if the port
Y can convey the associated NAS ID, then the peer can dynamically
discover that it is still within the same key cache boundary.
```

[1] Bellare, M. , Rogaway, P. “Entity Authentication and Key Distribution” 1993 http://www-cse.ucsd.edu/users/mihir/papers/eakd.pdf

1.6 Issue 3 - The MS should be able to perform seamless HO to when new BS on the same authenticator

MS security considerations do not appear to mandate that the MS perform a new 3way handshake when moving to a BS on the same authenticator.

If the new BS wishes to perform the 3way handshake (or full authentication for that matter), it may simply initiate it and the MS will react accordingly.

1.7 Issue 4 – It is desirable for 802.16e to support the "Channel binding" property of newer EAP methods

Though 802.11i does not support secure confirmation of parameters exchanged via "channel binding" EAP methods such as EAP-TTLSv1, this is a desirable security feature that is simple to implement.

1.8 Issue 5 - the authentication bit of the HO optimization flags is unnecessary

The authentication bit of HO optimization flags serves to inform the MS of the target BS policy.

However, the BS can always start authentication, or the 3way handshake. And the MS can begin authentication via EAP-Start. Hence the authentication bit appears to no longer be needed.

2 Changes to 802.16e D9

2.1 Remedy 1 - Include the identities in 3way handshake messages

[Add the following to table 37g (SA-TEK-Challenge) following the AKID attribute:]

AuthenticatorId | the identity of the EAP authenticator associated with the BS

[Add the following entry to the table 11.6.1 (SA Challenge tuple) following the AKID attribute:]

AuthenticatorId | the identity of the EAP authenticator associated with the BS

[Add the following to table 37h (SA-TEK-Request) following the AKID attribute:]

AuthenticatorId | the identity of the EAP authenticator associated with the BS

PeerId | the MAC Address of the MS

[Add the following to table 37i (SA-TEK-Response) following the AKID attribute:]

AuthenticatorId | the identity of the EAP authenticator associated with the BS

[insert new section 11.9.36:]

11.9.36 AuthenticatorId

Description: The Identity of the EAP Authenticator associated with the BS. This is the value that is sent in the NAS_Identifier AAA attribute

Type	Length	Value
Tbd	variable	Identity of the EAP Authenticator associated with the BS

[insert new section 11.9.37:]

11.9.37 PeerId

Description: The MAC address of the SS. This is the value that is sent in the Calling-Station-Id AAA attribute

Type	Length	Value
Tbd	6	MAC address of the SS

2.2 Remedy 2 – Enable BS to provide the MS with notification of the authenticator (or authenticators) to which it is attached

[Add the following to table 358 (DCD Channel Encoding):]

AuthenticatorId | <code> | variable | the identity of an EAP authenticator associated with the BS

2.3 Remedy 3 – Permit the MS to perform seamless HO when the target BS is on the same authenticator as the serving BS

[Modify text on page 234 line 56 as follows:]

The AK can be derived in one of three different ways depending on the authentication scheme used as documented in 7.2.2.2.3. Before the 3-way handshake begins, the BS and MS shall both derive a shared KEK and HMAC/CMAC keys as per 7.2.2.2.

The 3-way handshake demonstrates liveness of the BS and MS, proves mutual possession of the AK, and activates all of the AKs associated with the authenticator together with their AK context. When an MS performs HO to a target BS associated with the same authenticator (as indicated in NBR_ADV) as the serving BS, no 3-way handshake is required - as all AKs derived from the PMK are already active.

The PKMv2 SA-TEK 3-way handshake sequence proceeds as follows:

2.4 Remedy 4 – Enable 802.16e to support the "Channel binding" property of newer EAP methods

[section 7.8.1 Add a new numbered item in between 2 and 3:]

3. If the MS supports EAP methods with the channel binding property, and it received the AuthenticatorId via the EAP method, it shall check whether BS supplied the same AuthenticatorId in the SA-TEK-Challenge. If the AuthenticatorId does not match or was not supplied, the MS SHOULD log the event as a possible security breach and the MS may elect to terminate communication with the BS.

2.5 Remedy 5 – Eliminate the authentication bit from the HO optimization flags

[Delete the following text from table 108f and renumber the text entries lying below it:]

Bit #1: Omit PKM Authentication phase except TEK
phase during current re-entry processing

[Delete the following text from page 115 line 52 and renumber the text entries lying below it:]

Bit #1: Omit PKM Authentication phase except TEK phase during current re-entry processing