Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Resolutions to Outstanding 3way Handshake issues**
Date Submitted	**2005-07-21**
Source(s)	Jeff Mandin jeff@streetwaves-networks.com Streetwaves Networking Amatzia 5 Jerusalem, Israel 93148
Re:	C80216e/D9 Recirc
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 NAS (ie. Authenticator) 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).

Remedying this issue will partially satisfy IETF review item 7b:

```
In order to bind identities to the keying material,
the lower layer authenticator and peer identities need
to be explicitly stated within the 3-way handshake,
and bound to PMK.
```

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

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
```

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

```
Y can convey the associated NAS ID, then the peer can dynamically
discover that it is still within the same key cache boundary.
```

Remedying this issue will complete the resolution of item 7b from the IETF review:

```
Since EAP authenticators may have multiple ports, the
EAP peer needs to be aware of the authenticator identity;
this is not defined in IEEE 802.16e D8.
```

1.5 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.

Remedying this issue will clarify an ambiguity in the specification that was described in the IETF review:

1.6

1.7 Issue 4 - the authentication bit of the HO optimization flags needs clarification

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 possessing the AK

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

AuthenticatorId | the identity of the EAP authenticator possessing the AK

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

AuthenticatorId | the identity of the EAP authenticator possessing the AK

PeerId | the MAC Address of the MS

[insert new section 11.9.36:]

11.9.36 AuthenticatorId

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

Type | Length | Value

Tbd | variable | Identity of an 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

2.3 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

2.4 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 the serving BS (as indicated by DCD or by handover optimization flags), 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:

[Modify text in 7.8.1 as follows:]

During initial network entry or reauthorization, the BS shall send PKMv2 SA-TEK-Challenge (including a random number BS_Random) to the MS after protecting it with the CMAC/HMAC tuple. If the BS does not receive PKMv2 SA-TEK-Request from the MS within SAChallengeTimer, it shall resend the previous PKMv2 SA-TEK-Challenge.

The BS may send PKMv2 SA-TEK-Challenge up to SAChallengeMaxResends times. If the BS reaches its maximum number of resends, it may initiate full re-authentication or drop the MS.

~~2. If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, the BS begins the 3-way-handshake by appending the SA Challenge Tuple TLV to the RNG-RSP. If the BS does not receive PKMv2 SA-TEK-Request from the MS within SaChallengeTimer (suggested to be several times greater than the length of SaChallengeTimer), it may initiate~~

~~full re-authentication or drop the MS. If the BS receives an initial RNG-REQ during the period that PKMv2 SA-TEK-Request is expected, it shall send a new RNG-RSP with another SaChallenge TLV.~~

3. The MS shall send PKMv2 SA-TEK-Request to the BS after protecting it with the CMAC/HMAC. If the MS does not receive PKMv2 SA-TEK-Response from the BS within SATEKTimer, it shall resend the request. The MS may resend the PKMv2 SA-TEK-Request up to SATEKRequestMaxResends times. If the MS reaches its maximum number of resends, it may initiate full re-authentication or decide to connect to another BS or take some other action. The MS must include, through the Security Negotiation Parameters attribute, the security capabilities that it included in the SBC-REQ message during the basic capabilities negotiation phase.

[

2.5