Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Clarifications on key caching, activation, deletion|
Date Submitted	**2005-06-08**
Source(s)	Jeff Mandin Runcom Hachoma 2 Rishon Lezion, Israel jeff@streetwaves-networks.com
Re:	IEEE P802.16REVe/D8 SB re circ
Abstract	Clarifications on key caching, activation, deletion|
Purpose	Adopt changes.
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>.

Clarifications on key caching, activation, deletion

Jeff Mandin

1. Problem statement

From the IETF review:

```
It appears that there are circumstances where a BS could hold two
 PMKs for a given MS (such as during EAP re-authentication).  As
 part of the PMK cache definition, 802.16e should explicitly describe
 when PMKs are installed and deleted.  For example, does installation
 of a new PMK automatically destroy the old PMK?  It appears that this
 is implied by IEEE 802.16e D8, but it is not explicitly stated.

 Does failure of the 3-way handshake result in automatic deletion of
 the AK and PMK? 802.16e D8 is not explicit about this either. We would suggest
 that it is best not to delete the PMK in this case to prevent DoS
 attacks.  In situations where the MS has corrupted the PMK,
 this should not result in a deadlock as long as the MS
 can choose whether to initiate EAP re-authentication after a
 3-way handshake failure.

 Does failure of EAP authentication result in automatic deletion of the
 PMK?  802.16e is not explicit about this; we would suggest that it is
 best not to delete the PMK in this case to prevent DoS attacks.
```

2. Overview of solution

We clarify the text according to the following approach:

- The PMK cache is a logical entity maintained by BS and MS which is indexed by the Authenticator/MS MacAddr pair. Associated with each PMK is its context (as described in D8 section xx) and one or more AKs. The list of associated AKs can be viewed as indexed by BSId

- A PMK is installed upon successful EAP authentication and reception of the MSK via the AAA protocol

- Deletion of an AK by BS or MS (for example in the case of reclaiming resources) must result in deletion of the associated PMK, and all the AKs derived from the PMK

- Failure of the 3-way handshake does not (in and of itself) cause deletion of AK or PMK. After failure of the 3-way handshake the PMK and its associated AKs may be deleted due to lifetime expiration, or due to a new successful authentication (with its associated key creation).

3. Text changes

[Add the following new section 7.2.2.2.11 :]

7.2.2.2.11Maintenance of PMK and AK

The BS and MS maintain cached PMK and AK as follows:

a) PMK caching

An MS caches a PMK upon successful EAP authentication. A BS caches a PMK upon its receipt via the AAA protocol. Upon caching a new PMK, both the BS and MS MUST delete any cached PMK for the same Authenticator/Subscriber pair.

In the case of reauthentication, the older PMK and its AKs must be deleted by the MS after receipt of SA-TEK-Challenge, and by the BS after reception of SA-TEK-Request.

b) AK activation and deactivation

Successful completion of the 3-way SA-TEK handshake causes the activation of all the AKs associated with the Authenticator. If the MS moves to a different authenticator, all of the AKs then become deactivated (requiring another 3-way handshake to make them active), but the BS and MS must maintain the AK context (ie. replay counters etc.) as long as they retain the AK. If a packet counter belonging to an AK reached its maximum value, the AK becomes permanently deactivated.

c) PMK and AK deletion

The BS and MS can delete PMKs and associated AKs in various situations – including lifetime expiration, reauthentication, and reclamation of memory resources.

In any event, a PMK and its derived AKs must always be deleted together. A BS or MS must not delete an AK without deleting the associated PMK and all other associated AKs.

[Change text beginning at page 230, line 58 as follows:]

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

1. During initial network entry or reauthorization, the BS shall send SA-TEK-Challenge (including a random number RandomBS) to the MS after protecting it with the CMAC/HMAC tuple. If the BS does not receive SA-TEK-Request from the MS within SAChallengeTimer, it shall resend the previous SA-TEKChallenge. The BS may send SA-TEK-Challenge up to SAChallengeMaxResends times. If the BS reaches its maximum number of resends, it ~~shall discard the AK and~~ 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 SA-TEK-Request from the MS within SaChallenge-Timer (suggested to be several times greater than the length of SaChallengeTimer), it ~~shall discard the AK and~~ may initiate full re-authentication or drop the MS. If the BS receives RNG-REQ during the period that SA-TEK-Request is expected, it shall send a new RNG-RSP with another SaChallenge TLV.

3. The MS shall send SA-TEK-Request to the BS after protecting it with the CMAC/HMAC. If the MS does not receive SA-TEK-Response from the BS within SATEKTimer, it shall resend the request. The MS may resend the SA-TEK-Request up to SATEKRequestMaxResends times. If the MS reaches its maximum number of resends, it ~~shall discard the AK and~~ may initiate ~~do~~ full re-authentication or decide to connect to another BS or take some other action.