| | | |
|---|---|---|
| Project | IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**> | |
| Title | TEK FSM Fix | |
| Date Submitted | 2006-09-22 | |
| Source(s) | Avishay Shraga<br>Intel corporation | voice: +972-3-920-5763<br>avishay.shraga@intel.com |
| Re: | TEK_Invalid bug found during TSS/TP | |
| Abstract | The contribution fixes the usage of TEK_Invalid event to close a security hole | |
| Purpose | Close a major security hole | |
| 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>. | |

# TEK FSM FIX

*Intel Corporation*

## 1. Background

The current TEK FSM as appear in the standard defines that upon TEK Invalid event (internally created or received from BS):

The MS deletes the TEKs it uses – hence stop all data exchange for this SA.
Ask BS for TEK update
Resume Data upon updated TEK reception.

There is no way to validate the source of this event because:

The event is created (in either side) by receiving data packet with unknown key sequence number in the EKS field of GMH.
If EKS is unknown – there is no way to validate message (which is done using TEK pointed by EKS)
The packet could have been send by an un-authorized source – attacker.

The problem is that this creates a security hole that allows anyone to send a forged packet with wrong EKS and cause the MS to stop sending data.

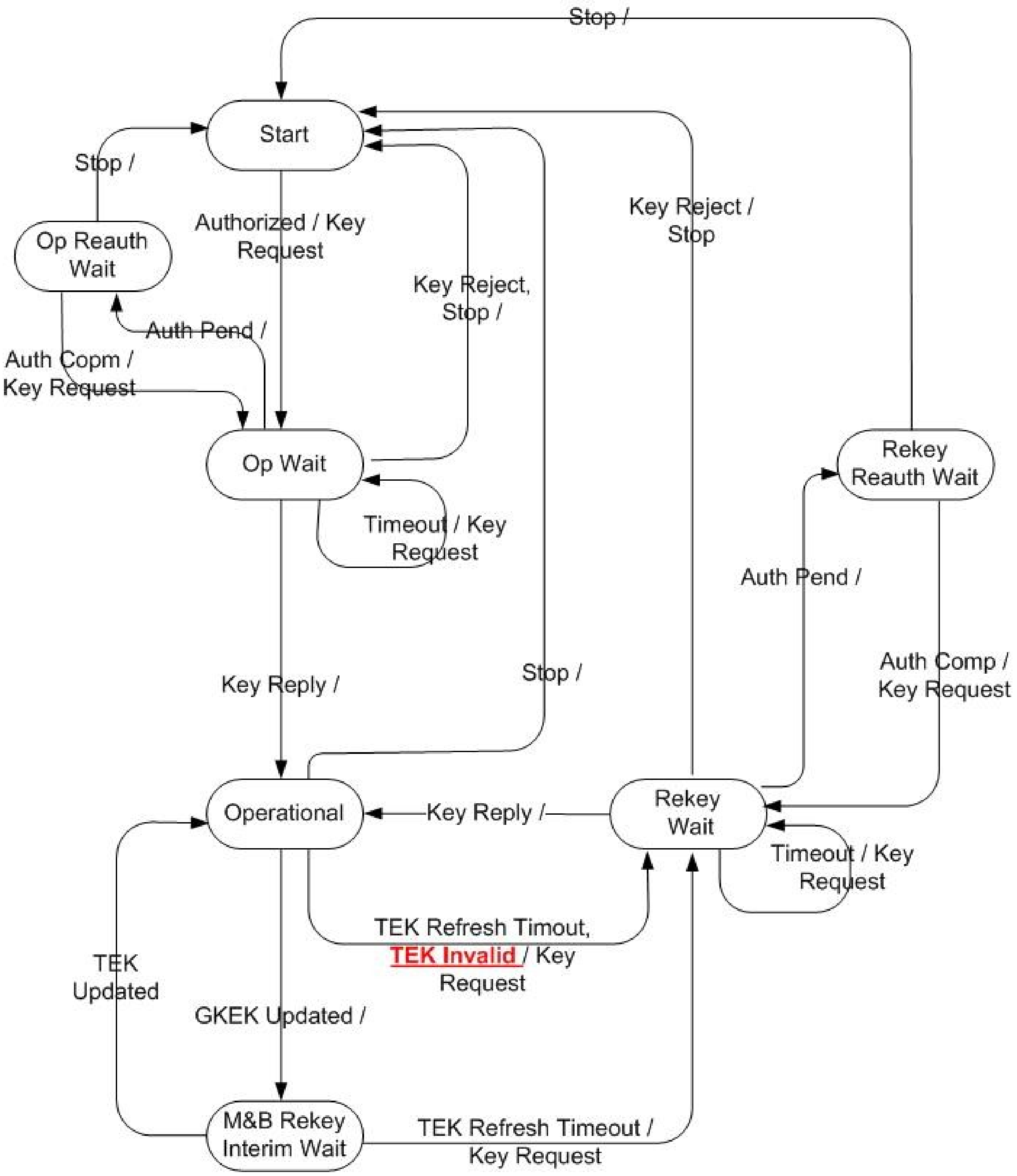
## 2. Suggested remedy

The proposed solution is to use the event as trigger to ask BS for key update but without deleting current TEKs and in parallel drop all data packets received with wrong EKS.
It means that this event causes the FSM to behave exactly like when receiving "TEK refresh timeout" which means that this solution deletes any action when receiving this event in Rekey Wait states because if the FSM already waits for new keys it doesn't have to do anything.

This remedy allows the MS to re-sync with the BS TEKs if the event was created from real reason but continue to exchange data using old keys if the event was an attack.
The MS can validate if the event was "real" by comparing the TEKs it received from BS with the TEKs it already has and may take countermeasures if the event re-occurs frequently. The countermeasures are out of scope of this standard.

## 3. Proposed Text Changes

**[Please replace "figure 131- TEK state machine flow diagram" in section 7.2.2.5 in page 290 of 802.16e-2005 with the following diagram]**



**[Please update "table 134 - TEK FSM state transition matrix" in section 7.2.2.5 in page 291 of 802.16e-2005 with the following table]**

| State Event or receive message | (A) Start | (B) Op Wait | (C) Op Reauth Wait | (D) Operational | (E) Rekey Wait | (F) Rekey Reauth Wait | (G) M&B Rekey Interim Wait |
|---|---|---|---|---|---|---|---|
| (1) Stop | | Start | Start | Start | Start | Start | |
| (2) Authorize | Op Wait | | | | | | |
| (3) Auth Pend | | Op Reauth Wait | | | Rekey Reauth Wait | | |
| (4) Auth Comp | | | Op Wait | | | Rekey Wait | |
| (5) TEK Invalid | | | | ~~Op Wait~~ Rekey Wait | ~~Op Wait~~ | ~~Op Reauth Wait~~ | |
| (6) Timeout | | Op Wait | | | Rekey Wait | | |
| (7) TEK Refresh Timeout | | | | Rekey Wait | | | Rekey Wait |
| (8) Key Reply | | Operational | | | Operational | | |
| (9) Key Reject | | Start | | | Start | | |
| (10) GKEK Update | | | | M&B Rekey Interim Wait | | | |
| (11) GTEK Update | | | | | | | Operational |
| | | | | | | | |

**[Please update section “7.2.2.5.5 Actions” in page 293 of 802.16e-2005 as follows:]**

5-D Operational (*TEK Invalid*) → ~~Op Wait~~ Rekey Wait

~~a) Clear TEK refresh timer~~

~~b) Send Key Request message to BS~~

~~c) Set Key Request retry timer to Operational Wait Timeout~~

~~d) Remove SAID keying material from key table~~

a) Silently discard the first two consecutive instances of TEK invalid; on third instance send Key Request message to BS

b) Set Key Request retry timer to Rekey Wait Timeout

~~5-E Rekey Wait (TEK Invalid) → Op Wait~~

~~a) Clear TEK refresh timer~~

~~b) Send Key Request message to BS~~

~~c) Set Key Request retry timer to Operational Wait Timeout~~

~~d) Remove SAID keying material from key table~~

~~5-F Rekey Reauth Wait (TEK Invalid) → Op Reauth Wait~~

~~a) Remove SAID keying material from key table~~