Security section review comments and resolutions on draft version D1.1

Page 39, lines 14,15. Change TLS to DTLS

**7.8a.3.4 DTLS Authentication Usage**

In PKMv3, mutual DTLS authentication is required.

Page 41 line 30. Remove authentication state machine

The TEK state machine for PKMv3 is presented in a state flow diagram (Figure 7-27) and is detailed in the subclauses below.

Page 43, lines 18-21. Just clarification. The text wasn’t clear enough.

**7.8a.4.2.6 Rekey Reauth Wait State**

The TEK state machine is placed in if the Rekey Reauth Wait State if it has valid traffic keying material, has an outstanding request for the latest keying material, and the Authorization state machine initiates a reauthorization cycle. If the authorization process is completed while in this state, the SS shall Send Key Request message to BS and shall set Key Request retry timer to Rekey Wait Timeout. If the TEK key is invalidated during this state, the SS shall remove SAID keying material from its key table.

Page 44. Line 16:

AK <== HKDF-Extract (SS MAC Address | BSID | “AK”, PMK)

Page 45.

Remove line 28. It is already in line 16.

Add the following after line 15. This is to clarify the situation.

A TEK key becomes invalid if the decrypting entity (BS or SS) recognizes a loss of TEK key synchronization between itself and the encrypting entity (SS or BS). For example, if an SAID’s TEK key sequence number, contained within the received in a MAC PDU header, is out of the range of known sequence numbers for that SAID.

Page 67. (editorial changes)

lines 14 & 15 can be removed. There is no change there.

Line 20 clause should be changed:

***Instructions to the editor for Clause 11.9.6 are in the following text:***

***Modify the table as below:***

|  |  |  |
| --- | --- | --- |
| ***Type***  | ***Length*** | ***Value (string)*** |
| ***11*** | ***Variable*** | A keyed SHA hash |

Line 21 is to be removed.

Line 23 the clause should be changed:

***Instructions to the editor for Clause 11.9.29 are in the following text:***

**11.9.29 GKEK**

The ~~128-bit~~ GKEK may be randomly generated in a BS or an ASA server. The GKEK field is used to

encrypt the GTEK for the multicast service or the broadcast service.

|  |  |  |
| --- | --- | --- |
| ***Type***  | ***Length*** | ***Value (string)*** |
| ***43*** | ***Variable*** | GKEK, encrypted with the KEK derived from AK |

Line 24 is to be removed.