IEEE P802.11
Wireless LANs

|  |
| --- |
| LB258 - Proposed Resolution for CID 1349  |
| Date: 2022-05-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Joseph LEVY | InterDigital Communication, Inc. | 111 W 33rd StreetNew York, NY 10120 | +1.631.622.4139 | jslevy@ieee.org  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This contribution addresses CID 1349 from LB258, providing changes that realize the agreed way forward from the TGme Ad Hoc (26-28 April 2022).

r1: Minor editorial clean up based on discussions during the 16 May TGme teleconference. (Author name in the footer is updated and the spurious highlighted symbols in the final paragraph are removed.)

This contribution proposes a resolution for LB258 CID 1349:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |  |  |  |
| 1349 | Mark Hamilton | 340 | 39 | 4.10.3.2 | The Authenticator also encrypts and sends the WIGTK in the EAPOL-Key frame | Add WIGTK to the list "GTK, IGTK, BIGTK values" |  |  |  |  |

In the minutes from the TGme Ad Hoc ([11-22/0679r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0679-00-000m-minutes-for-revme-ad-hoc-april-26-28-2022.docx)) :

* + 1. CID 1349 (SEC)
			1. Review Comment
			2. Discussion on if we have too much detail in Clause 4, and if we could simply remove figure 4-31 and 4-32.
			3. Would need more work to be able to delete the references and examples.
			4. Assign to Joseph Levy and Submission Required – put on May Agenda.
			5. Use “Group keys” in place of the lists of keys and remove the figures.
			6. **ACTION ITEM #8**; Joseph Levy include a clean-up of the related detail in clause 4 for CID 1349 (SEC).

The follow redline is based on 802.11revme D1.2

* AKM operations with AS

The following AKM operations are carried out when an IEEE 802.1X AS is used:

* Prior to any use of IEEE Std 802.1X-2010, IEEE Std 802.11 assumes that the Authenticator and AS have established a secure channel. The security of the channel between the Authenticator and the AS is outside the scope of this standard.

Authentication credentials are distributed to the Supplicant and AS prior to association.

* A STA discovers the AP’s security policy through passively monitoring Beacon frames or through active probing. If IEEE 802.1X authentication is used, the EAP authentication process starts when the Authenticator sends the EAP-Request or the Supplicant sends the EAPOL-Start frame. EAP messages pass between the Supplicant and AS via the Authenticator and Supplicant’s Uncontrolled Ports, as described in 12.7 (Keys and key distribution).
* The Supplicant and AS authenticate each other and generate a PMK. The PMK is sent from the AS to the Authenticator over the secure channel, as described in 12.7 (Keys and key distribution).

A 4-way handshake or FT 4-way handshake utilizing EAPOL-Key frames is initiated by the Authenticator to do the following:

* Confirm that a live peer holds the PMK.
* Confirm that the PMK is current.
* In the case of fast BSS transition, derive PMK-R0s and PMK-R1s.
* Derive a fresh pairwise transient key (PTK) from the PMK or, in the case of fast BSS transition, from the PMK-R1, the derived PTK including the key derivation key (KDK) if WUR frame protection is negotiated.(11ba)
* If WUR frame protection is negotiated, derive a fresh WTK from the KDK.(11ba)
* Install the pairwise encryption and integrity keys, and if WUR frame protection is negotiated, the WTK.(11ba)
* Transport the group keys and sequence numbers from Authenticator to Supplicant and install the group keys and sequence numbers in the STA and, if not already installed, in the AP.
* Verify that the RSN capabilities negotiated are valid as defined in 9.4.2.24.4 (RSN capabilities).
* Confirm the cipher suite selection.

Installing the PTK, and where applicable the group keys causes the MAC to encrypt and decrypt all subsequent MSDUs irrespective of their path through the controlled or uncontrolled ports. (11ba)Installing the WTK when WUR frame protection is negotiated causes the MAC to integrity protect subsequent individually addressed WUR Wake-up frames at the AP or to validate subsequent individually addressed WUR Wake-up frames at the non-AP STA.

Upon successful completion of the 4-way handshake, the Authenticator and Supplicant have authenticated each other; and the IEEE 802.1X Controlled Ports are unblocked to permit general data traffic, as described in 12.7 (Keys and key distribution).

If the Authenticator later changes one or more group keys, it sends the new group key(s) and sequence number(s) to the Supplicant using the group key handshake to allow the Supplicant to continue to receive group addressed frames. EAPOL-Key frames are used to carry out this exchange, as described in 12.7 (Keys and key distribution).

**References:**