**IEEE P802.11
Wireless LANs**

|  |
| --- |
| CC50 CR for CID3866 |
| **Date**: Apr. 14, 2025.  |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **email** |
| Bo Cao | ZTE |  |  | cao.bo4@zte.com.cn |
| Jay Yang |  |  | Yang.zhijie@zte.com.cn |
| Yun Li |  |  |  |
| Yan Li |  |  |  |
| Yurong Qian |  |  |  |
| Qisheng Huang |  |  |  |
| Zisheng Wang |  |  |  |
| Chun Huang |  |  |  |

 **Abstract**

This submission proposes resolutions for following CID received for TGbn CC50:

3866

**Revisions:**

Rev 0: Initial version of the document.

Rev 1: Modified as suggested by Duncan, add relevant passed motions.

***TGbn editor: The baseline for this document is P802.11bn D0.2 and P802.11REVmeD7.0***

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbn Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbn Draft (i.e., they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbn Editor: Editing instructions preceded by “TGbn Editor” are instructions to the TGbn editor to modify existing material in the TGbn draft. As a result of adopting the changes, the TGbn editor will execute the instructions rather than copy them to the TGbn Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Pg/Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 3866 | 12 | 66/01 | Under seamless roaming, the security keys will be derived using the SMD MAC Address, established with respect to the SMD, and the security context maintained with respect to the SMD. Please investigate and update relevant sections under clause 12 to fit with the roaming architecture. | As in comment | Revised.Agree in principle.TGbn editor, please make the changes tagged by #3866 in 25/676r0. |

**Relevant passed motions:**

[Motion #279, [2]]

Move to add to the TGbn SFD the following:

* 11bn defines a Seamless Mobility Domain (SMD, exact name TBD) that covers multiple AP MLDs, where a non-AP MLD can use the UHR seamless roaming procedure to roam between the AP MLDs of the SMD
	+ A logical SMD Management Entity (SMD-ME, exact name TBD) provides association, IEEE 802.1X Authenticator (except for the management of 802.1X control ports which is TBD) and RSNA Key management for non-AP MLDs across all AP MLDs of the SMD.
	+ A non-AP MLD transitions between AP MLDs within the SMD while maintaining its association and security association with the SMD-ME.
	+ The non-AP MLD can transition from one SMD to another SMD that are part of the same MD (Mobility Domain) using FT with improvements

[Motion #285, [2]]

Move to add to the TGbn SFD the following:

* For security in seamless roaming, when a non-AP MLD is in the process of roaming from the current AP MLD to a target AP MLD within the SMD, the same PMKSA, established with the SMD-ME, shall be used to protect communications with the current AP MLD and the target AP MLD.

[Motion #286, [2]]

Move to add to the TGbn SFD the following:

* For security in seamless roaming, when a non-AP MLD is in the process of roaming from the current AP MLD to a target AP MLD within the SMD, the same PTKSA, established with the SMD-ME, shall be used to protect communications with the current AP MLD and the target AP MLD.

[Motion #348, [3]]

Move to add to the TGbn SFD the following:

* TGbn allows a second mode for security in roaming (in addition to the first mode with single TK used across all AP MLDs of the SMD) where a non-AP MLD can derive a new TK under the same PTKSA with the target AP MLD
	+ The new TK is derived as part of the single PTKSA
	+ The PN is maintained per PTKSA: The new TK negotiated with the target AP MLD shares the same PN space with the TK of the current AP MLD (PN is monotonically increasing)

[Motion #369, [3]]

**Move to add to the TGbn SFD the following:**

* For a Seamless Mobility Domain (SMD), the SMD and the 802.1X Authenticator component in the corresponding SMD-ME are uniquely identified by an SMD identifier
	+ The SMD identifier is in the format of a 48-bit MAC address
	+ The SMD identifier is used in establishing single PMKSA and PTKSA for a non-AP MLD that associates with the SMD-ME

[Motion #378, [3]]

**Move to add to the TGbn SFD the following:**

* If the SMD is part of an FT mobility domain the following applies
	+ The single PMKSA to be used in the SMD is the PMK-R1 SA and is bound to the SMD-ME, when the non-AP MLD initially associates with the SMD ME using FT initial MD association.

**Proposed Texts:**

TGbn editor: please insert the following proposed changes (#3866).

**12.2.4 RSNA establishment**

***Insert the following paragraphs and NOTE at the end of the subclause:***

(#3866)When an RSNA is established between a non-AP MLD and an SMD-ME, the SMD element shall be included in the frame body of authentication and association frames (see 9.4.2.xxx (SMD element)) and within EAPOL-Key frames (see 12.7.2 (EAPOL-Key frames)).

For SMD operation, when Supplicant is a non-AP MLD and Authenticator is an SMD-ME and when an EAPOL PDU is sent from a Supplicant to an Authenticator, the SA shall be the MLD MAC address of the Supplicant, and the DA shall be the SMD Identifier of the Authenticator. Conversely, when an EAPOL PDU is sent from an Authenticator to a Supplicant, the SA shall be the SMD Identifier of the Authenticator, and the DA shall be the MLD MAC address of the Supplicant.

**12.6 RSNA security association management**

**12.6.1 Security associations**

**12.6.1.1 Security association definitions**

**12.6.1.1.2 PMKSA**

*Change the third paragraph as follows:*

A PMKSA association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is used to create the PTKSA. PMKSAs have a certain lifetime. For a non-AP MLD that is associated with an AP MLD, the PMKSA association is between the AP MLD and the non-AP MLD. (#3866)For a non-AP MLD that is associated with an SMD-ME, the PMKSA association is between the SMD-ME and the non-AP MLD. The PMKSA consists of the following:

— PMKID, as defined in 12.7.1.3 (Pairwise key hierarchy) or 12.7.1.6.3 (PMK-R0). The PMKID identifies the security association.

— Authenticator’s or peer’s MAC address. For multi-band RSNA, the MAC address is associated with the operating band in use when the PMKSA is established. For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD. (#3866)For SMD operation, the Authenticator’s MAC address is the SMD Identifier of the SMD.

— PMK; or if the PMKSA was established with an AKMP for which the Authentication type column includes FT authentication (see Table 9-190 (AKM suite selectors)), MPMK (see 12.7.1.6.3 (PMKR0)).

— Lifetime, as defined in 12.7.1.3 (Pairwise key hierarchy) or 12.7.1.6 (FT key hierarchy).

— AKMP.

— All authorization parameters specified by the AS or local configuration. This might include parameters such as the STA’s authorized SSID.

— Cache Identifier, if advertised by the AP in FILS Indication element.

**12.6.1.1.6 PTKSA**

*Change the third paragraph as follows:*

The PTKSA consists of the following:

— PTK, where the PTK includes the KDK when WUR frame protection is negotiated

— Pairwise cipher suite selector, and when WUR frame protection is negotiated, the cipher suite selector 00-0F-AC:6 (BIP- CMAC-128) for individually addressed WUR Wake-up frames

— Supplicant MAC address, depending on the negotiated AKMP. For MLO, the Supplicant’s MAC address is the MLD MAC address of the non-AP MLD.

— Authenticator MAC address, depending on the negotiated AKMP. For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD. (#3866)For SMD operation, the Authenticator’s MAC address is the SMD Identifier of the SMD.

— Key ID

— If FT key hierarchy is used,

— R1KH-ID

— S1KH-ID

— PTKName

— If WUR frame protection is negotiated

— WTK

**12.7 Keys and key distribution**

**12.7.1 Key hierarchy**

**12.7.1.1 General**

*Change the third paragraph as follows:*

In an infrastructure BSS, the IEEE 802.1X Authenticator MAC address (AA) and the AP’s MAC address are the same, and the Supplicant’s MAC address (SPA) and the STA’s MAC address are equal. Between an AP MLD and a non-AP MLD, the IEEE 802.1X Authenticator MAC address (AA) shall be set to the MLD MAC address of the AP MLD, and the Supplicant’s MAC address (SPA) shall be set to the MLD MAC address of the non-AP MLD. (#3866)Between a non-AP MLD and an SMD-ME, the IEEE 802.1X Authenticator MAC address (AA) shall be set to the SMD Identifier of the SMD, and the Supplicant’s MAC address (SPA) shall be set to the MLD MAC address of the non-AP MLD. For the purposes of comparison in this standard, the MAC address is encoded as 6 octets, taken to represent an unsigned integer. The first octet of the MAC address shall be used as the most significant octet. The bit numbering conventions in 9.2.2 (Conventions) shall be used within each octet. This results in a sequence of 48 bits represented such that bit 0 is the first transmitted bit (Individual/Group bit) and bit 47 is the last transmitted bit.

**12.7.2 EAPOL-Key frames**

*Insert the following NOTE as the fourth paragraph after the third paragraph (“The bit and octet convention...”):*

(#3866)NOTE 1—For SMD, when Supplicant is a non-AP MLD and Authenticator is an SMD-ME and when an EAPOL PDU is sent from a Supplicant to an Authenticator, the SA shall be the MLD MAC address of the Supplicant, and the DA shall be the SMD Identifier of the Authenticator. Conversely, when an EAPOL PDU is sent from an Authenticator to a Supplicant, the SA shall be the SMD Identifier of the Authenticator, and the DA shall be the MLD MAC address of the Supplicant. See 12.2.4 (RSNA establishment).

**12.7.5 Nonce generation**

*Change the third paragraph as follows:*

The local MAC address should be AA on the Authenticator and SPA on the Supplicant. When the Authenticator is an AP MLD and the Supplicant is a non-AP MLD, the AA shall be the MLD MAC address of the AP MLD and the SPA shall be the MLD MAC address of the non-AP MLD. (#3866)When the Authenticator is an SMD-ME and the Supplicant is a non-AP MLD, the AA shall be the SMD Identifier of the SMD and the SPA shall be the MLD MAC address of the non-AP MLD.