**IEEE P802.11  
Wireless LANs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC50 CR for CID3866 | | | | |
| **Date**: May. 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 CIDs received for TGbn CC50:

162, 3866

**Revisions:**

Rev 0: Initial version of the document.

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

Rev 2: Add CID 162. Removed AA related text (TBD).

Rev 3: Editorial change.

***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** |
| 162 | 37.8.2.5 | 75/38 | When non-AP MLD authenticate with SMD, the authentitor MAC address shall be set to the SMD-ME MAC address | As in comment | Revised.  Agree in principle.  TGbn editor, please make the changes tagged by #3866 in 25/676r2. |
| 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 25/676r2. |

**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 #280, [2]]

* 11bn defines that within a Seamless Mobility Domain (SMD, exact name TBD) the data path includes either one MAC-SAP for the SMD or a separate MAC-SAP per AP MLD of the SMD.
  + In the case of a separate MAC-SAP per AP MLD, the DS mapping is updated when the non-AP MLD roams to another AP MLD within the SMD.
  + In the case of a separate MAC-SAP per AP MLD, the component of the 802.1X Authenticator in the SMD-ME interacts with an 802.1X Authenticator component in the AP MLD that manages the 802.1X controlled port for the non-AP MLD.
  + In the case of a single MAC-SAP for the SMD, the 802.1X Authenticator in the SMD-ME manages the 802.1X controlled port for the non-AP MLD.

[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 at the end of the subclause:***

(#3866)When an RSNA is established between a non-AP MLD and an SMD-ME, the SMD Information element (see 9.4.2.xxx (SMD Information element)) shall be included in Authentication frames and (Re)Association Request and Response frames.