IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bn PDT-CR MAC Seamless Roaming (Part 3) |
| Date: July, 2025 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Duncan Ho | Qualcomm Technologies, Inc | 5665 Morehouse Dr, San Diego CA 92131 USA | +1 (858) 845-3214 | dho@qti.qualcomm.com |
| Thomas Derham | Broadcom |  |  | thomas.derham@broadcom.com |
| Liwen Chu | NXP |  |  | liwen.chu@NXP.COM |
| Xiangxin Gu | Spreadtrum |  |  | Xiangxin.gu@unisoc.com |
| Xiandong Dong | Xiaomi |  |  | dongxiandong@xiaomi.com |
| Tuncer Baykas | Ofinno |  |  | tbaykas@ieee.org |
| Gaurav Patwardhan | HPE |  |  | gauravpatwardhan1@gmail.com |
| Ning Gao | Oppo |  |  | gaoning1@oppo.com |
| Pei Zhou | TCL |  |  | zhoupei36@gmail.com |
| Frank Hsu | Mediatek Inc. |  |  | frank.hsu@mediatek.com |
| Xuwen Zhao | TCL |  |  | zhaoxuwen123@outlook.com |
| Juseong Moon | KNUT |  |  | Jsmoon0211@a.ut.ac.kr |
| Ronny Yongho Kim | KNUT |  |  | ronnykim@ut.ac.kr |
| John Wullert | Peraton Labs |  |  | jwullert@peratonlabs.com |
| Manasi Ekkundi | Samsung Electronics |  |  | manasi.e@samsung.com |
| Jarkko Kneckt | Apple |  |  | jkneckt@apple.com |
| Pooya Monajemi | Apple |  |  | p\_monajemi@apple.com |
| Chitto Ghosh | Apple |  |  | chitto.ghosh@apple.com |
| Insun Jang | LGE |  |  | insun.jang@lge.com |
| SunHee Baek | LG Electronics |  |  | sunhee.baek@lge.com |
| Ryuichi Hirata | Sony |  |  | Ryuichi.Hirata@sony.com |
| Thomas Handte | Sony |  |  | Thomas.Handte@sony.com |
| Liangxiao Xin | Oppo |  |  | v-xinliangxiao@oppo.com |
| Liuming Lu | Oppo |  |  | luliuming@oppo.com |
| Arik Klein | Huawei |  |  | arik.klein@huawei.com |
| Zisheng Wang | ZTE |  |  | wang.zisheng@zte.com.cn |
| Prabodh Varshney | Nokia |  |  | Prabdh.varshney@nokia.com |
| Liubogoshchev | Nokia |  |  | Mikhail.Liubogoshchev@nokia.com |
| Yun Li | ZTE |  |  |  |
| Abhishek Chaturvedi | Samsung |  |  | abhi.chat@samsung.com |
| Hang Yang | Ruijie Networks Co., Ltd. |  |  | yanghang1@ruijie.com.cn |
| Alfred Asterjadhi | Qualcomm Technologies, Inc. |  |  | aasterja@qti.qualcomm.com |
| Subir Das | Peraton Labs |  |  | sdas@peratonlabs.com |
| Abhishek Patil | Qualcomm Technologies, Inc. |  |  | appatil@qti.qualcomm.com |
| Peshal Nayak | Samsung |  |  | p.nayak@samsung.com |
| Rubayet Shafin | Samsung Electronics |  |  | r.shafin@samsung.com |
| Zhenpeng Shi | Huawei |  |  | shizhenpeng1@huawei.com |
| Massinissa Lalam | Sagemcom |  |  | 00001c2d776ab802-dmarc-request@listserv.ieee.org |
| Julien Sevin | Canon |  |  | julien.sevin@crf.canon.fr |
| Yuki Fujimori | Canon |  |  | yuki.fujimori@crf.canon.fr |
| Haorui Yang | China Mobile |  |  | yanghaorui0217@163.com |
| Tomo Adachi | Toshiba |  |  | tomo.adachi@TOSHIBA.CO.JP |
| Kyosuke Inoue | Sharp Corporation |  |  | kyosuke\_inoue@sharp.co.jp |
| Stephane Baron | Canon |  |  | stephane.baron@crf.canon.fr |
| Brian Hart | Cisco |  |  | brianh@cisco.com |
| Yu Hsien Chang |  |  |  |  |
| Lei Zhou | New H3C |  |  | Zhou.leih@h3c.com |
| Gabor Bajko | Mediatek |  |  | gabor.bajko@mediatek.com |
| Lili Hervieu | CableLabs |  |  | l.hervieu@cablelabs.com |
| Hanqing Lou | InterDigital |  |  | Hanqing.lou@interdigital.com |
| Jeongki Kim | Ofinno |  |  | jkim@ofinno.com |
| Kosuke Aio | Sony Corporation |  |  | kosuke.aio@sony.com |
| Giovanni Chisci | Qualcomm Incorporated |  |  | gchisci@qti.qualcomm.com |
| Binita Gupta | Cisco |  |  | binitag@cisco.com |
| Guogang Huang | Huawei |  |  | huangguogang1@huawei.com |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
| Mike Montemurro | Huawei |  |  | montemurro.michael@gmail.com |
| Jay Yang | ZTE |  |  | yang.zhijie@zte.com.cn |
| Yelin Yoon | LGE |  |  | yl.yoon@lge.com |
| Nima Namvar | Charter Communications |  |  | Nima.namvar@charter.com |
| Ross Jian Yu | Huawei |  |  | ross.yujian@huawei.com |
| Shawn Kim | Wilus Inc. |  |  | shawn.kim@wilusgroup.com |
| Yue Zhao | Huawei |  |  | Zhaoyue122@huawei.com |
| Sungjin Park | LGE |  |  | allean.park@lge.com |
| Xiaofei Wang | InterDigital |  |  | Xiaofei.wang@interdigital.com |
| Fangxin Xu | Shenzhen Longsailing Semiconductor |  |  |  |
| Yunpeng Yang | TP-link |  |  |  |
| Yu Hsien Chang |  |  |  |  |
| Shuang Fan | Sanechips |  |  |  |

Abstract

This document contains Proposed Draft Text (PDT) for the Seamless Roaming feature of the proposed TGbn (UHR, Ultra High Reliability) amendment to the 802.11 standard.

This submission also proposes resolutions for the following CIDs received for TGbn CC50:

3915, 2543, 3760, 3941, 2403, , 274, 2716, 273, 1326, 157 (12 CIDs)

**Revision information**

The following is a summary of the important changes that occurred within each revision of this document:

|  |  |
| --- | --- |
| **Revision** | **Major changes** |
| 0 | Use 25/ 566r5 as the baseline and make changes on top of it.Summary of major technical aspects:* A per-AP MLD PTK mode can be used (TBD under what conditions it can be used).
* If a per-AP MLDP is used:
	+ The current AP and non-AP will exchange DHss to generate a new PTK.
	+ The PN for both UL and DL are not reset and they will keep increasing.
 |
| 1 | Added per-AP MLD PTK capability bit in SMD Capabilities field. If the current AP MLD supports a per-AP MLD PTK, the non-AP MLD may request to use a per-AP MLD PTK. |
| 2 | Updates:* Updated the definition of the bit in the SMD capabilities field (in the SMD Info element) to indicate same PTK vs Different PTK mode.
* Added text in section 37.9.5.3 (Per-AP MLD PTK derivation) for further discussion.
* Renamed “a per-AP MLD PTK key” to “Different PTK mode” to avoid confusion.
* Added the requirement of including the SMD Information element in the Beacon frame.
* Completed the changes for using the SMD Identifier in the PMK and PTK derivation (orthogonal to the per-AP MLD PTK discussion) in sub-sections in 12.6 and 12.7.
* Removed CIDs 2789 and updated the resolution of the other 4 CIDs.
* The Timeout value (renamed as Timeout Info) between ST prep and ST exec is now limited to max ~16 second (with 2 bits reserved) because the previous max (~65s) is probably too much.
* Added CID 164 (requiring all APs affiliated with any AP MLD that is part of the same SMD to advertise the same RSNE).
* Added CIDs 274, 2716, 273, 1326, 3914, 157 about security context
 |
| 3 | Updates:* Removed CID 3914 since further discussions are needed.
 |
| 4 | Updates:* Introduced the 2 PTK modes: 1) Per-SMD-PTK 2) Per-AP MLD PTK with 1 bit in the SMD Information element.
* Reverted back to “Per-AP MLD PTK mode”
* Added the Diffie-Hellman and the Nonce elements to ST preparation request and ST preparation response
* Added requirements to install the new Per-AP MLD PTK.
* Added PTK derivation details when Per-AP MLD PTK is used.
 |
| 5  | Updates:* Revised resolution of CID3760
 |
| 6 | Updates:* Added Per-SMD PTK derivation
* Removed CID 164
 |
| 7 | Updates:* Minor revision of the Per-SMD PTK derivation
 |
| 8 | Updates:* Residual text of CID 164 (which was removed in r6 already)
 |

**Introduction**

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. The abstract, revision information, introduction, explanation of the proposed changes and references sections are 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).***

Details of the CIDs and proposed resolution:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **Pg/Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 3915 | Binita Gupta | 37.8.2.5 | 75.36 | In 11bn for seamless roaming, two modes have been discussed for PTK generation. A shared PTK used across all AP MLDs of the SMD, and a different PTK mode generating a different PTK for each AP MLD of the SMD. The client behavior is obviously different for each of these modes. Hence we need to advertise which mode/modes are supported by the AP MLDs/SMD. This could be through defining these modes in the RSNE/RSNXE, in SMD element or via different AKMs (as is done for FT). | Define a mechanism for the AP MLD to advertise the PTK mode supported (shared PTK mode or different PTK mode) for the SMD. Make the shared PTK mode mandatory to be supported by AP MLDs and non-AP MLDs since that mode is common across both distributed and centralized SMD architectures. | **Revised**Agreed in principle.Please see the changes tagged as #3915.**TGbn editor, please incorporate the changes tagged as #3915 in document 11-25-0753-02.** |
| 2543 | Jarkko Kneckt | 37.8.2.5.1 | 75.43 | Seamlessly roaming STA should be able to rekey its PTK when is roams to a new AP MLD in SMD. The rekey should be done by using ephmeral Diffie Hellmann public keys and according to 3- frame exchange PASN protocol. | Please allow a seamlessly roaming non-AP MLD to rekey its PTKSA with the roaming target AP MLD. The PTK rekey protocol uses ephmeral Diffie Hellmann public keys and 3-frames exchange according to PASN protocol. | **Revised**The text changes in this document enables the Different PTK mode and DHss, which serves this purpose. Same resolution as #3915.**TGbn editor, please incorporate the changes tagged as #3915 in document 11-25-0753-02.** |
| 2403 | Yuki Fujimori | 37.8.2.5 | 75.36 | It's not clear whether Seamless roaming is mandatory or optional for UHR AP MLDs and UHR non-AP MLDs respectively. | Please clarify it and if it is optional, add a corresponding capability field in the UHR Capabilities element to indicate the support. | **Revised**Added the requirement that if a UHR AP MLD supports ST, the APs affiliated with the AP MLD will include the SMD Information element in its beacon. See the changes tagged as #2403 in this contribution.**TGbn editor, please incorporate the changes tagged as #2403 in document 11-25-0753-02.** |
|  |  |  |  |  |  |  |
| 274 | Xuwen Zhao | 37.8.2.5.4 | 76.32 | The roaming security context should include the security context. It should clearly describe what the security context contains and how the security context is transmitted or negotiated. | Add a description of the security context. For example, the security context may contains the PTK identifier, Snonce and Anonce required for obtaining or re-deriving the PTK. The commentor will bring a contribution to address this comment and provide more detaild solutions. | **Rejected**The security context sharing, if any, is left for implementation in the network side as there are many different types of deployments and systems hence it’s outside the scope of 802.11bn. |
| 2716 | Chittabrata Ghosh | 37.8.2.5.4 | 76.32 | Context related to security should be includedwhen exchanged during the roaming preparationphase | As in the comment | **Rejected**The security context sharing, if any, is left for implementation in the network side as there are many different types of deployments and systems hence it’s outside the scope of 802.11bn. |
| 273 | Xuwen Zhao | 37.8.2.5.2 | 75.61 | The Roaming (Preparation) Procedure lacks a description of the security process, and it needs to clarify how to transfer or renegotiate the security context. | Add a description of the security process in the Roaming Preparation Procedure. For example, the non-AP MLD and the current AP MLD generate a PTK identifier while generating the old PTK before roaming. The target AP MLD obtains the old PTK from the current AP MLD based on the PTK identifier. The non-AP MLD and the target AP MLD establish a security association based on the old PTK, or the non-AP MLD and the target AP MLD derive a new PTK based on the old PTK and establish a security association. The commentor will bring a contribution to address this comment and provide more detaild solutions. | **Revised**The text changes in this document enables the Different PTK mode and DHss, which serves this purpose. Same resolution as #3915.**TGbn editor, please incorporate the changes tagged as #3915 in document 11-25-0753-02.** |
| 1326 | Renlong Zhou | 37.8.2.5.2 | 75.47 | Define the exchange methods for sharing PMKSA and PTKSA with the AP MLDs. | Initiating the sharing operations of PMKSA and PTKSA should consider both PUSH and PULL methods between SMD and AP MLDs. | **Rejected**The commenter fails to identical a technical problem. |
|  |  |  |  |  |  |  |
| 3760 | Liuming Lu | 37.8.2.5 Seamless Roaming | 75.46 | Whether the non-AP MLD remains Single PMKSA or PTKSA during the transition is unclear. A flexible security association during the transition needs to be considered in order to adapt to different scenarios for seamless roaming. | As in the comment. | **Revised**The text changes in this document enables the Different PTK mode and DHss, which serves this purpose. Same resolution as #3915.**TGbn editor, please incorporate the changes tagged as #3915 in document 11-25-0753-02.** |

**Text to be adopted begins here.**

***TGbn editor: Note the following uses part of the SMD BSS Transition PDT Part 1 (25/566r10) as the base for making changes. Please make the changes to 25/566r10 as shown below:***

9.4.2.aa4 SMD Information element [M#352][M#369](#3920)(#3470)

The SMD Information element contains the SMD Identifier field and SMD Capabilities field for a seamless mobility domain. The format of the SMD Information element is shown in Figure 9-aa18 (SMD Information element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | SMD Identifier | SMD Capabilities | Timeout Value |

Octets: 1 1 1 6 1 2

**Figure 9-aa18—SMD Information element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The SMD Identifier field indicates a unique identifier for the SMD and is in the format of a 48-bit MAC address.

The format of the SMD Capabilities field is defined in Figure 9-aa19 (SMD Capabilities field format).

 B0 B1 B2 B7

|  |  |  |
| --- | --- | --- |
| DL Data Forwarding | (#3915)PTK Mode | Reserved |

 Bits: 1 1 6

**Figure 9-aa19—SMD Capabilities field format**

The DL Data Forwarding field is set to 1 if forwarding of buffered DL data of a non-AP MLD from the current AP MLD to a target AP MLD is supported by the SMD and is set to 0 otherwise.

(#3915)The PTK Mode field indicates the protection mode for the communications between the non-AP MLD and its current AP MLD and between the non-AP MLD and a target AP MLD. The field is set to 0 if the SMD-ME uses the Per-SMD PTK and is set to 1 if the SMD-ME uses the Per-AP MLD PTK (see (37.9.1 (General)).

The Timeout Value field is set to the timeout between the ST preparation response and ST execution request in units of TU that applies across all the AP MLDs managed by the SMD-ME of the SMD.

[TBD other fields for other SMD level capabilities]

***TGbn editor: Add the Diffie-Hellman element and Nonce element to Table 9-658bb and Table 9-658bc together with the description text shown below:***

**9.6.43.2 UHR Link Reconfiguration Request frame format**

The UHR Link Reconfiguration Request frame is used by a UHR MLD for performing SMD BSS transition (see 37.14 (SMD BSS transition)).

The Action field of a UHR Link Reconfiguration Request frame contains the information shown in 9-658bb (UHR Link Reconfiguration Request frame Action field format).

|  |
| --- |
| * **UHR Link Reconfiguration Request frame Action field format**
 |
| **Order** | **Meaning** |
| 1 | Category |
| 2 | Protected UHR Action |
| 3 | Dialog Token |
| 4 | Type |
| 5 | Reconfiguration Multi-Link element (see 9.4.2.322.4 (Reconfiguration Multi-Link element)) |
| 6 | OCI element (see 9.4.2.235 (OCI element)) (optional) |
|  | … |
| 8 | Diffie-Hellman element (see 9.4.2.312 (Diffie-Hellman Parameter element)) (optional) |
| 9 | Nonce element (see 9.4.2.188 (Nonce element)) (optional) |

The Diffie-Hellman element is defined in 9.4.2.312 (Nonce element).

The Nonce element is defined in 9.4.2.188 (Nonce element).

**9.6.43.3 UHR Link Reconfiguration Response frame format**

The UHR Link Reconfiguration Response frame is used by a UHR non-AP MLD and UHR AP MLD for performing SMD BSS transition (see 37.14 (SMD BSS transition)).

The UHR Link Reconfiguration Response frame is sent by an AP MLD in response to a UHR Link Reconfiguration Request frame received from a non-AP MLD to accept or reject a target AP MLD preparation or to accept an ST execution.

The Action field of a UHR Link Reconfiguration Response frame contains the information shown in 9-658bc (UHR Link Reconfiguration Response frame Action field format).

|  |
| --- |
| * **UHR Link Reconfiguration Response frame Action field format**
 |
| **Order** | **Meaning** |
| 1 | Category |
| 2 | Protected UHR Action |
| 3 | Dialog Token |
| 4 | Type |
| 5 | Count |
| 6 | Reconfiguration Status List |
| 7 | Group Key Data (optional) |
| 8 | OCI element (see 9.4.2.235 (OCI element)) (optional) |
| 9 | Basic Multi-Link element (see 9.4.2.322.2 (Basic Multi-Link element)) (optional) |
|  | … |
| 12 | Diffie-Hellman element (see 9.4.2.312 (Diffie-Hellman Parameter element)) (optional) |
| 13 | Nonce element (see 9.4.2.188 (Nonce element)) (optional) |

The Diffie-Hellman element is defined in 9.4.2.312 (Nonce element).

The Nonce element is defined in 9.4.2.188 (Nonce element).

***TGbn editor: The following section 12.6.2 is from 802.11be D7.0. Please modify it as follows:***

## SMD BSS transition

### General

SMD BSS transition is a mechanism for a non-AP MLD to transition from its current AP MLD to a target AP MLD (#3891)without requiring reassociation. SMD BSS transition minimizes the time during which connectivity between the non-AP MLD and the DS is lost. The non-AP MLD remains in State 4 of association with a seamless mobility domain management entity (SMD-ME) during the SMD BSS transition while preserving the context for data transmission for a seamless experience.[M#279] To support SMD BSS transition, an SMD is introduced in the IEEE 802.11 architecture. The SMD consists of multiple AP MLDs, where a non-AP MLD can use the SMD BSS transition procedure to transition between the AP MLDs within the SMD. An SMD-ME provides SMD-level authentication and association (see 11.3 (STA authentication and association)), IEEE 802.1X Authenticator functions and RSNA key management functions for non-AP MLDs across all AP MLDs within the SMD.

[M#280]Two data path models between the non-AP MLD and the DS are supported by the SMD:

* One MAC SAP for the SMD.
* Separate MAC SAP per AP MLD of the SMD.

[M#280]Only one of these data path models is used within an SMD.

[M#280](#154)In the case of a separate MAC SAP per AP MLD, the DS mapping is updated when the non-AP MLD transitions to another AP MLD within the SMD and 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.

[M#280]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.

[#369] The SMD and the 802.1X Authenticator component in the corresponding SMD-ME are uniquely identified by an SMD identifier (see 9.4.2.xxx (SMD Information element)). The SMD identifier is used in establishing a single PMKSA and PTKSA for a non-AP MLD that associates with the SMD-ME.

[M#378] [M#279] If the SMD is part of an FT mobility domain, the single PMKSA to be used in the SMD is a PMK-R1 security association that is bound to the SMD-ME (through the SMD identifier (see 9.4.2.xxx (SMD Information element)), when the non-AP MLD initially associates with the SMD-ME using FT initial MD association. [M#279] A non-AP MLD can transition from one SMD to another SMD that is part of the same mobility domain using fast BSS transition.

[M#279] A non-AP MLD performs initial association with the SMD-ME through an AP MLD within the SMD that establishes an SMD-level security association across all AP MLDs in the SMD. The non-AP MLD transitions between AP MLDs within the SMD while maintaining its association and security association with the SMD-ME. This new mobility type is called SMD BSS transition.[M#284, M#285] When a non-AP MLD is in the process of transitioning from its current AP MLD to a target AP MLD within the SMD, the same PMKSA and PTKSA created as part of RSNA security association established with the SMD-ME shall be used to protect the communications with its current AP MLD and the target AP MLD if the PTK mode is set to 0 (Per-SMD PTK mode).

If the PTK mode is set to 0 (Per-SMD PTK mode), the Per-SMD PTK is derived as defined in 37.9.5.3 (Per-SMD PKT Key derivation) and the Per-SMD PTK is then used for cryptographic encapsulation for the non-AP MLD.

[M#348]If the PTK mode is set to 1 (Per-AP MLD PTK mode), the Per-AP MLD PTK is derived as defined in 37.9.5.4 (Per-AP MLD PTK) and the Per-AP MLD PTK is then used for cryptographic encapsulation for the non-AP MLD.

SMD BSS transition includes the following procedures:

* SMD BSS transition discovery (see 37.9.2)
* Initial association to the SMD-ME (see 37.9.3)
* Target AP MLD selection recommendation (see 37.9.4)
* SMD BSS transition preparation (see 37.9.5)
* SMD BSS transition execution
	+ Through current AP MLD (see 37.9.6)
	+ Through target AP MLD (see 37.9.7)

### SMD BSS transition discovery procedure (#188)(#507)(#2000)(#2352)

A non-AP MLD can use mechanisms such as active scanning (see 11.1.4.3.2 (Active scanning procedure for a non-DMG STA) and 35.3.4.2 (Use of multi-link probe request and response)), the BSS transition management framework (see 11.21.7 (BSS transition management) and 35.3.23 (BSS transition management for MLDs)) or the neighbor report framework (see 11.10.10 (Usage of the neighbor report)) for discovery of the neighboring AP MLDs and SMD BSS transition support by those AP MLDs.

NOTE 1 – A neighboring AP MLD might or might not be part of the same SMD.

[M#344] NOTE 2 – An AP is not required to report non-collocated APs in the Reduced Neighbor Report element that is carried in its Beacon and FILS Discovery frames.

[M#352](#3912) An SMD Information element provides an SMD identifier and SMD capabilities for an SMD. (#1066)An AP MLD that is managed by an SMD shall include the SMD Information element in the (#2403)Beacon frames and Probe Response frames. The SMD Information element is provided as part of the Neighbor Report element in the BSS Transition Management Request frame and Neighbor Report Response frames for a reported AP that is part of a different SMD than the reporting AP.

[M#333] A mechanism is defined to retrieve probe response content for neighboring AP MLD(s) of the current AP MLD, through the current AP MLD.

### Initial association to the SMD-ME [M#352][M#369]

[M#352](#3912) To perform SMD-level association, a non-AP MLD shall initiate association and authentication with the SMD-ME. The SMD Information element shall be included in the Authentication frame when authenticating with the SMD-ME. The SMD Information element shall be included in the (Re)Association Request and Response frames when performing initial association with the SMD-ME.

[M#369] As part of performing authentication of a non-AP MLD with the SMD-ME, a single PMKSA shall be established between the non-AP MLD and the SMD-ME using the SMD identifier. The PMKSA includes an SMD-level PMK.

[M#369] As part of initial association of a non-AP MLD with the SMD-ME, an SMD-level PTKSA is derived between the non-AP MLD and the SMD-ME using the SMD identifier.

### Target AP MLD selection recommendation [M#364] (#188) (#2000)(#2002)(#2003)(#2004)(#2353)(#2005)

The current AP MLD may use the BSS transition management procedure (see 11.21.7 (BSS transition management) and 35.3.23 (BSS transition management for MLDs)) [TBD updates if required] to recommend one or more candidate target AP MLDs within the same SMD (or a different neighboring SMD) to the non-AP MLD, as shown in Figure 37-x2. (TBD detailed information to be carried in the BSS transition management frames).

A non-AP MLD may send a BSS Transition Management Query frame (see 11.21.7.2 (BSS transition management query)) to its current AP MLD to request recommendation for candidate target AP MLDs. The current AP MLD shall respond with a BSS Transition Management Request frame. In addition, the current AP MLD may send an unsolicited BSS Transition Management Request frame (see 11.21.7.4 (BSS transition management response)) to the non-AP MLD to indicate its recommendation for candidate target AP MLDs for SMD BSS transition. TBD – detailed information to be carried.



**Figure 37-x2— Candidate selection for target AP MLDs**

### SMD BSS transition preparation procedure

#### General

When a non-AP MLD uses SMD BSS transition to transition from its current AP MLD to a target AP MLD within an SMD, an SMD BSS transition preparation procedure as shown in Figure 37-x3 (#3004)shall be performed before performing the SMD BSS transition execution procedure that is described in 37.9.6 (SMD BSS transition execution procedure via the current AP MLD) and 37.9.7 (SMD BSS transition execution procedure via the target AP MLD) to minimize the time during which connectivity between the non-AP MLD and the DS is lost. The SMD BSS transition preparation procedure consists of (#2006)the following:

* Transfer of the context (see 37.9.7 (Context)) related to the non-AP MLD from its current AP MLD to the target AP MLD or the renegotiation of the context with the target AP MLD. (#3003)
* Setting up the link(s) with the target AP MLD as described in 37.9.5.2.



**Figure 37-x3— SMD BSS transition preparation and execution procedures**

[M#368](#3922)(#2010) A non-AP MLD prepares one or more candidate target AP MLDs within an SMD by sending a separate ST preparation request for each candidate target AP MLD. If a SMD BSS transition preparation was successful with one or more candidate target AP MLDs, then the non-AP MLD shall attempt SMD BSS transition execution with only one of those target AP MLDs at a time. If the attempted SMD BSS transition execution fails, the non-AP MLD may attempt SMD BSS transition execution with another prepared AP MLD. [TBD on policy indication from the AP on multiple target AP MLDs preparation].

#### Target links preparation

[M#283](#2715) When a non-AP MLD performs the SMD BSS transition preparation procedure to prepare a target AP MLD, the non-AP MLD shall send an ST preparation request[M#345](#493)(#2007)(#2009)(#2715)(#3457)(#3892)(#3921) to its current AP MLD.

The ST preparation request shall include the following:

* [M#345](#493)A target AP MLD MAC address.
* The Per-STA Profile subelement for each affiliated non-AP STA that the non-AP MLD is requesting to set up with the target AP MLD in the Reconfiguration Multi-link element (see 35.3.6.4 (Link reconfiguration to the setup links)) carried in the ST preparation request.
* [M#356] A Diffie-Hellman Parameter element (see 9.4.2.312 (Diffie-Hellman Parameter element)) that contains the public key generated by the non-AP MLD if the Per-AP MLD PTK mode is used.
* A Nonce element (see 9.4.2.188 (Nonce element)) that contains the nonce generated by the non-AP MLD (SNonce) if the Per-AP MLD PTK mode is used.

[M#351](#499) The non-AP MLD shall indicate in the ST preparation request whether the non-AP MLD requests part of the context not to be transferred as described in 37.9.8 (Context) (TBD actual signaling).

[M#337](#517)The non-AP MLD shall include the Listen Interval field in the ST preparation request.

After receiving the ST preparation request:

* If the target AP MLD accepts one or more links requested by the non-AP MLD in the ST preparation request:
	+ The target AP MLD shall set up the accepted links at the target AP MLD according to the procedures defined in 35.3.6.4 (Link reconfiguration to the setup links) [Editorial note: need to capture any exceptions or differences or additional rules with respect to 35.3.6.4].
	+ If a separate MAC SAP per AP MLD is used as described in 37.9.1 (General), the target AP MLD shall keep the IEEE 802.1X Controlled Port blocked so that general data traffic cannot pass directly between the non-AP MLD and the target AP MLD.
	+ The context for the non-AP MLD shall be transferred from the current AP MLD to the target AP MLD per 37.9.8 (Context).
	+ (#3927)The current AP MLD shall transfer the SCS descriptors of all the currently established SCS of that non-AP MLD to the target AP MLD.
		- The target AP MLD may accept or reject an SCS stream (e.g. based on its resource availability) and indicate that to the current AP MLD.
	+ (#3927)The current AP MLD shall transfer the MSCS Descriptor of the established MSCS with the non-AP MLD.
		- The target AP MLD may accept or reject the MSCS (e.g. based on its resource availability) in the ST preparation response and indicate that to the current AP MLD.
	+ [M#348] If the Per-AP MLD PTK mode is used, the target AP MLD shall derive a new PTK with the non-AP MLD.
* The current AP MLD shall send an ST preparation response[M#345](#493)(#2007)(#2009)(#2715) (#3457)(#3892)(#3921)to the non-AP MLD and the frame shall include the following:
	+ The status (Accept/Reject) of each requested link setup at the target AP MLD.
	+ If the status is Accept for at least one link, the frame shall include the following:
		- The AID assigned to the non-AP MLD by the target AP MLD
		- (#3927)A list of already established SCS streams that have been accepted by the target AP MLD. SCS streams that are not indicated as accepted are not setup at the target AP MLD
		- An indication of the status (accept or reject) of the transfer of MSCS context to the target AP MLD.
		- [M#356] A Diffie-Hellman Parameter element (see 9.4.2.312 (Diffie-Hellman Parameter element)) that contains the public key generated by the target AP MLD if the Per-AP MLD PTK mode is used.
		- A Nonce element (see 9.4.2.188 (Nonce element)) that contains the nonce generated by the target AP MLD (ANonce) if the Per-AP MLD PTK mode is used.
* Group keys shall not be included in the ST preparation response.
* [M#335] (#515) If an ST execution request from the non-AP MLD requesting SMD BSS transition to a target AP MLD is not received by the current AP MLD or the target AP MLD within the timeout(#515) value indicated in the SMD Information element, the following shall be deleted:
	+ The setup links at the target AP MLD.
	+ The transferred context at the target AP MLD.
	+ The newly derived PTK if the Per-AP MLD PTK mode is used.

TBD on whether/how the renegotiation of context is performed in these request/response frames.

When a non-AP MLD receives an ST preparation response from the current AP MLD indicating that the SMD BSS transition preparation was successfully completed with at least one setup link established at the target AP MLD:

* The Basic Multi-link element in the ST preparation response shall be processed by the non-AP MLD according to the procedures defined in 35.3.6.4 (Link reconfiguration to the setup links).
* [M#348] If the Per-AP MLD PTK mode is used, the non-AP MLD shall derive a new PTK with the target AP MLD.
* [M#337](#514)The non-AP MLD shall be in power save mode for all the setup links with the target AP MLD as specified in 35.3.6.4 (Link reconfiguration to the setup links).
* [M#335] (#515) The non-AP MLD may initiate the SMD BSS transition execution procedure by sending an ST execution request requesting SMD BSS transition to the same target AP MLD within the timeout value, either via the current AP MLD (see 37.9.6 (SMD BSS transition execution procedure via the current AP MLD)) or via the target AP MLD (see 37.9.7 (SMD BSS transition execution procedure via the target AP MLD)).

NOTE – The DS mapping update operation is not performed during the ST preparation procedure.

#### Per-SMD PTK Key Derivation

This subclause applies when the PTK mode is 0 (Per-SMD PTK).

If the per-SMD PTK mode is used, a PTK is derived when the non-AP MLD performs initial association to the SMD-ME (see 37.9.3 (Initial association to the SMD-ME)). This key is derived from the PMK established with the SMD-ME, using the PTK derivation formula for the corresponding AKM with the following modifications:

* The SMD Identifier is added to the end of the context of the PTK derivation formula.
* The AA or BSSID is the MLD address of the AP MLD through which association to the SMD-ME occurs.
* The PTK is a Per-SMD PTK that is used to protect the link between the non-AP MLD and AP MLDs within the SMD. If this PTK is rekeyed, the same PTK derivation as described in the above paragraph is used.

#### Per-AP MLD PTK Key Derivation

This subclause applies when the PTK mode is 1 (Per-AP MLD PTK).

If the per-AP MLD PTK mode is used, a PTK and SMD\_KDK are derived when the non-AP MLD performs initial association to the SMD-ME (see 37.9.3 (Initial association to the SMD-ME)). These keys are derived from the PMK established with the SMD-ME, using the PTK derivation formula for the corresponding AKM with the following modifications:

* The output of the PTK derivation formula is: PTK || SMD\_KDK.
* The “Length” of the KDF in the PTK derivation formula is equal to PTK\_bits + SMD\_KDK\_bits.
	+ PTK\_bits is the length of the PTK.
	+ SMD\_KDK\_bits is the length of the SMD\_KDK, which is equal to the length of the PMK.
* The SMD Identifier is added to the end of the context of the PTK derivation formula.
* The AA or BSSID is the MLD address of the AP MLD through which association to the SMD-ME occurs.

The PTK is a Per-AP MLD PTK that is used to protect the link between the non-AP MLD and current AP MLD. If this PTK is rekeyed, the regular PTK derivation formula is used and an SMD\_KDK is not rederived.

The SMD\_KDK is used to derive new Per-AP MLD PTKs when SMD BSS transition occurs; the lifetime of SMD\_KDK is equal to the lifetime of the association with the SMD-ME.

If the SMD uses Per-AP MLD PTKs and an SMD BSS transition occurs, a new Per-AP MLD PTK is derived between the non-AP MLD and the target AP MLD using the PTK derivation formula for the corresponding AKM, with the following differences:

* If the PTK derivation formula does not include DHss in its context, DHss is added at the end of the context.
* The derivation key PMK is replaced by SMD\_KDK.
* The AA or BSSID is the target AP MLD MAC address.

NOTE 2 – If the Non-AP MLD does an SMD BSS transition back to the initial AP MLD, a new Per-AP MLD PTK is derived using the SMD\_KDK as described in the previous paragraph; the SMD\_KDK is not rederived.

### SMD BSS transition execution procedure via the current AP MLD

When a non-AP MLD uses SMD BSS transition to transition from its current AP MLD to a target AP MLD within an SMD through its current AP MLD, the non-AP MLD shall send an [M#346](#511)(#2017)(#3260)(#3458)(#3929)ST execution request to its current AP MLD (#3893) (TBD if the non-AP MLD shall stop sending Data frames to its current AP MLD)[M#346] The Per-STA Profile subelement in the Reconfiguration Multi-Link element shall not be present in the ST execution request.

[M#335](#515) If the current AP MLD receives an ST execution request within the timeout value(#515) described in 37.9.5.2 (Target links preparation) and the target AP MLD has been prepared for SMD BSS transition for the non-AP MLD as described in 37.9.5 (SMD BSS transition preparation procedure), then:

* The current AP MLD shall transfer any context that is required per37.9.8 (Context) and has not already been transferred to the target AP MLD (if any).
* If a separate MAC SAP per AP MLD is used as described in 37.9.1 (General), the target AP MLD may initiate the DS mapping update for the non-AP MLD and unblock the IEEE 802.1X Controlled Port for general data traffic to pass between the non-AP MLD and the target AP MLD.
* [M#351] If the non-AP MLD had requested its current AP MLD not to transfer the next SN for existing DL block ack agreements of all TIDs (see 37.9.8 (Context)), the target AP MLD shall reset the SN to 0 for all the DL TIDs and the non-AP MLD shall initialize *WinStartB* to 0 for each DL TID with a block ack agreement, before DL traffic delivery from the target AP MLD to the non-AP MLD.
* [M#351] If the non-AP MLD had requested its current AP MLD not to transfer the latest SN that has been passed up for existing UL block ack agreement of all TIDs (see 37.9.8 (Context)), the non-AP MLD shall reset the SN to 0 for all the UL TIDs and the target AP MLD shall initialize *WinStartB* to 0 for each UL TID with a block ack agreement, before UL traffic delivery from non-AP MLD to the target AP MLD.
* Once the period of DLDrainTime has expired or terminated as described in 37.9.9 (Downlink data transmission)), the target AP MLD considers the SMD BSS transition execution procedure complete (i.e., the non-AP MLD has fully transitioned to the target AP MLD).
* The current AP MLD shall send an [M#346](#511)(#2017)(#3260)(#3458)(#3929)ST execution response with the status value set to SUCCESS to the non-AP MLD after the transfer of the context is completed(#530) (if any). The current AP MLD shall include the following in the ST execution response:
	+ [M#338] (#522)(#3590)The value of the DLDrainTime.
	+ Group keys of the successfully setup links at the target AP MLD.
* If the Per-AP MLD PTK mode is used, the target AP MLD shall not reset the PNs for either UL or DL. The PNs keep increasing monotonically when the non-AP MLD transitions to the target AP MLD even though the target AP MLD is using a new Per-AP MLD PTK for cryptographic encapsulation.
* (#154)If a separate MAC SAP per AP MLD is used as described in 37.9.1 (General) and the target AP MLD has not initiated the DS mapping update for the non-AP MLD, the target AP MLD shall initiate it for the non-AP MLD and unblock the IEEE 802.1X Controlled Port for general data traffic to pass between the non-AP MLD and the target AP MLD.

NOTE – The necessary contents of the ST execution response (e.g. security parameters) might have been provided by the target AP MLD to the current AP MLD during the SMD BSS transition preparation procedure.

[M#44] The non-AP MLD shall not transmit Class 3 frames to the target AP MLD until it has received the ST execution response with status value set to SUCCESS from the current AP MLD for at least one link.

If the Per-AP MLD PTK mode is used, the non-AP MLD shall install the Per-AP MLD PTK as the PTK in use when it receives the ST execution response with status value set to SUCCESS from the current AP MLD.

### SMD BSS transition execution procedure via the target AP MLD [M#284]

When a non-AP MLD uses SMD BSS transition to transition from its current AP MLD to a target AP MLD within an SMD through the target AP MLD, the non-AP MLD shall send an ST execution request to the target AP MLD (#3893) (TBD if the non-AP MLD shall stop sending Data frames to its current AP MLD].

[M#346] The Per-STA Profile subelement in the Reconfiguration Multi-Link element shall not be present in the ST execution request.

After the non-AP MLD transmits the ST execution request to the target AP MLD on one of the setup links with the target AP MLD, the non-AP STA corresponding to that link shall remain in awake state while the other non-AP STAs corresponding to the setup links remain in doze state as described in 35.3.6.4 (Link reconfiguration to the setup links).

The ST execution request and ST execution response for SMD BSS transition execution shall be transmitted on the same link between the non-AP MLD and the target AP MLD.

[M#335](#515) If the target AP MLD receives an ST execution request within the timeout value(#515) directly from the non-AP MLD described in 37.9.5.2 (Target links preparation) and the target AP MLD has been prepared for SMD BSS transition for that non-AP MLD, then:

* The target AP MLD shall transfer any context from the current AP MLD that is required per 37.9.8 (Context) and has not already been transferred to the target AP MLD (if any).
* If a separate MAC SAP per AP MLD is used as described in 37.9.1 (General), the target AP MLD may initiate the DS mapping update for the non-AP MLD and unblock the IEEE 802.1X Controlled Port for general data traffic to pass between the non-AP MLD and the target AP MLD.
* [M#351] If the non-AP MLD had requested its current AP MLD not to transfer the next SN for existing DL block ack agreement of all TIDs (see 37.9.8 (Context)), the target AP MLD shall reset the SN to 0 for all the DL TIDs and the non-AP MLD shall initialize *WinStartB* to 0 for each DL TID with a block ack agreement, before DL traffic delivery from the target AP MLD to the non-AP MLD.
* [M#351] If the non-AP MLD had requested its current AP MLD not to transfer the latest SN that has been passed up for existing UL block ack agreement of all TIDs (see 37.9.8 (Context)), the non-AP MLD shall reset the SN to 0 for all the UL TIDs and the target AP MLD shall initialize *WinStartB* to 0 for each UL TID with a block ack agreement, before UL traffic delivery from non-AP MLD to the target AP MLD.
* The target AP MLD shall send an ST execution response to the non-AP MLD after the transfer of the context is completed(#530) (if any). The target AP MLD shall include the following in the ST execution response:
	+ [M#338](#522)(#3590)The value of the DLDrainTime (TBD if the value of the DLDrainTime shall be set to 0).
	+ Group keys of the successfully setup links at the target AP MLD.
* (#154)If a separate MAC SAP per AP MLD is used as described in 37.9.1 (General) and the target AP MLD has not initiated the DS mapping update for the non-AP MLD, the target AP MLD shall initiate it for the non-AP MLD and unblock the IEEE 802.1X Controlled Port for general data traffic to pass between the non-AP MLD and the target AP MLD.
* [#348] If the Per-AP MLD PTK mode is used, the target AP MLD shall not reset the PNs for either UL or DL. The PNs keep increasing monotonically when the non-AP MLD transitions to the target AP MLD even though the target AP MLD is using a new Per-AP MLD PTK for cryptographic encapsulation.
* The target AP MLD shall consider the SMD BSS transition execution procedure complete (i.e., the non-AP MLD has fully transitioned to the target AP MLD).

NOTE – The necessary contents of the ST execution response (e.g. security parameters) might have been provided by the target AP MLD to the current AP MLD during the SMD BSS transition preparation procedure.

The non-AP MLD shall not transmit Class 3 frames (other than the ST execution request to the target AP MLD) until it has received the ST execution response frame with the status value set to SUCCESS from the target AP MLD for at least one link.

If the Per-AP MLD PTK mode is used, the non-AP MLD shall install the Per-AP MLD PTK as the PTK in use when it receives the ST execution response with status value set to SUCCESS from the current AP MLD.

**Text to be adopted ends here.**