**IEEE P802.11
Wireless LANs**

|  |
| --- |
| PDT MAC MAPC PASN part 1 |
| **Date**: June. 24, 2025.  |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **email** |
| Jay Yang | ZTE |  |  | Yang.zhijie@zte.com.cn |
| Yan Li |  |  |  |
| Yun Li |  |  |  |
| Yurong Qian |  |  |  |
| Qisheng Huang |  |  |  |
| Zisheng Wang |  |  |  |
| Bo Cao |  |  |  |
| Chun Huang |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

 **Abstract**

This submission proposes resolutions for following 4 CIDs received for TGbn CC50:

 151, 1386, 3796, 3797

**Revisions:**

Rev 0: Initial version of the document.

***TGbn editor: The baseline for this document is P802.11bn D0.3 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** |
| 151 | 9.6.10 | 63/38 | Protected MAPC Request/Response frame has been already defined, but the MAPC authentication is missing, 11bn should define a MAPC authentication procedure | the commenter will provide a solution on this. | Revised.Agree in principle.TGbn editor, please make the changes tagged by CID #151 in 11-25/1049r0. |
| 1386 | 9.6.10 | 63/38 | While protected MAPC Request/Response frames have been specified, the MAPC authentication mechanism remains undefined. The 802.11bn standard should establish a formal MAPC authentication procedure. | As it says in the comment | Revised.Agree in principle.TGbn editor, please make the changes tagged by CID #151 in 11-25/1049r0. |
| 3796 | 9.6.10 | 63/53 | Remove the MAPC Request from the Protected Dual of Public Action frame.The MAPC Request frame does not require protection.Its inclusion can introduce additional complexity, and a more fundamental security issue lies in the control frames (such as BSRP Polling and MU-RTS TXS and), which are not protected.Therefore, protecting only the negotiation process is unnecessary. | As in the comment | RejectedThe comment fails to identify a technical issue. TGbn group has already agreed to define the protected version of MAPC Negotiation request/response frame, see motion [428]. |
| 3797 | 9.6.10 | 3.57 | Remove the MAPC Response from the Protected Dual of Public Action frame.The MAPC Response frame does not require protection.Its inclusion can introduce additional complexity, and a more fundamental security issue lies in the control frames (such as BSRP Polling and MU-RTS TXS and), which are not protected.Therefore, protecting only the negotiation process is unnecessary. | As in the comment | RejectedThe comment fails to identify a technical issue. TGbn group has already agreed to define the protected version of MAPC Negotiation request/response frame, see motion [428]. |

### Relevant Passing Motions

[Motion #50]

* 11bn defines a common framework of a Multi-AP Coordination for various coordination schemes.
	+ Note - Coordination schemes such as (but not limited to): Co-SR (TXOP-based with power control), Co-BF, Co-TDMA, Co-RTWT, etc.

[Motion #51]

* 11bn defines a common framework of a Multi-AP Coordination that can enable the following procedures:
	+ Multi-AP Coordination Discovery procedure
	+ Multi-AP Coordination agreement negotiation procedure
	+ Note: Details of the procedures and whether the above procedures are mandatory/optional - TBD

[Motion #135]

* The sharing AP, that transmits a Trigger frame as part of a transmission sequence in a Multi-AP coordinated transmission scheme, identifies the shared AP via an AP ID carried in the AID12 field of the User Info field of the frame
	+ Note: the name of "sharing AP" and "shared AP" are TBD
	+ Note: Multi-AP coordinated transmission schemes are Co-SR, Co-BF and Co-TDMA

[Motion #147]

* APs that intend to participate in Multi-AP coordination can use management frames to advertise/discover the capabilities and/or parameters of individual schemes.

[Motion #148]

* APs that discovered each other and want to establish agreement(s) for Multi-AP coordination scheme(s), can use individually addressed management frames to establish the agreement(s) and negotiate parameters
	+ Note: The management frame can be a Public Action and/or new Action frames, and so on.

[Motion #265]

* As a part of M-AP coordination agreement procedure, an AP may assign an AP ID to another AP with the following constraints:
	+ The AP ID is used for the AP to identify another AP as a coordinated AP, when necessary.
	+ The AP ID field has the same size and the field value has a range as defined in AID field (see 9.4.1.8)
	+ The AP shall ensure that the AP ID value is not assigned by the AP or by its affiliated MLD to any other STA (e.g., STA is an associated non-AP STA, an unassociated non-AP STA that has been allocated a (Ranging session Identifier) RSID , or any other coordinated AP), or a non-AP MLD that is associated with the AP MLD
	+ It's TBD whether the AP ID value is greater than 2^n where n is the maximum of the value carried in the MBSSID Indicator (n) field of the Multiple BSSID element for any AP affiliated with the AP MLD that belongs to a multiple BSSID set

[Motion #342]

* Established coordination between two APs can be terminated by an explicit teardown performed by one of the two APs.

[Motion #358]

* TGbn defines new actions for Public Action frames for MAPC communications such as discovery and negotiations
	+ An action is defined for MAPC Discovery
	+ An action is defined for MAPC Negotiation Request
	+ An action is defined for MAPC Negotiation Response
	+ Others are TBD

[Motion #359]

* When an AP use Management frames to discover the capabilities and/or parameters of individual M-AP coordination schemes, the AP shall use the defined MAPC Public Action frame with the following setting:
	+ The action field is set to MAPC Discovery

[Motion #360]

* When an AP (AP1) uses an individually addressed Management frame to initiate a negotiation to establish agreements for M-AP coordination schemes (if enabled by another AP (AP2)), the AP (AP1) shall use the defined MAPC Public Action frame with the following setting:
	+ The Action field is set to MAPC Negotiation Request
	+ If new negotiations are disabled by another AP (AP2) the AP (AP1) shall not send a negotiation request to the other AP (AP2)
	+ TBD details of ‘new negotiations disabled

[Motion #361]

* When an AP (AP2) receives an individually addressed Management frame that initiates a negotiation to establish agreements for M-AP coordination schemes, the AP (AP2) shall respond by using the defined MAPC Public Action frame with the following setting, if negotiations are enabled:
	+ The Action field is set to MAPC Negotiation Response

[Motion #428]

* TGbn defines a procedure based on pre-association security negotiation (PASN) or uses PASN with necessary extensions to derive the key(s) needed for the protected version of individually addressed MAPC Negotiation Request frame and MAPC Negotiation Response frame exchanged between two APs as part of MAPC operation.

**Proposed Texts:**

***TGbn editor: please make the following change in this clause (CID #151):***

***Change the following paragraphs as shown:***

**4.5.4.2 Authentication**

***Change the third, fourth, sixth paragraph as follows:***

IEEE Std 802.11 defines the following IEEE 802.11 authentication methods:

— Open System authentication admits any STA to the DS.

— FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 13 (Fast BSS transition).

— SAE authentication uses finite field cryptography to prove knowledge of a shared password.

— IEEE 802.1X authentication uses EAP to authenticate STAs and the AS with one another.

— FILS authentication allows for faster connection to the network for FILS non-AP STAs by providing authentication, association, and key confirmation information in an efficient number of frame exchanges (see 4.10.3.6 (AKM operations using FILS authentication)).

— PASN,EDPKE and MAPC PASN authentication allows for the protection of Management frames without association by establishing a PTKSA using authentication frames. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods, or any combination of these authentication methods.

An RSNA might support one or more of the following authentication methods: SAE authentication, IEEE

802.1X authentication, FILS authentication, or PASN authentication, or EDPKE authentication. An RSNA also supports authentication based on IEEE Std 802.1X-2020, or preshared keys (PSKs) after Open System authentication. This standard does not specify an EAP method that is mandatory to implement. See 12.6.4 (RSNA policy selection in an IBSS) for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

***Add the last paragraph as follows:***

PASN authentication or EDPKE authentication is used in an RSN for an infrastructure BSS when it is based on a PMKSA established by another RSN authentication protocol. Otherwise, it does not guarantee mutual authentication, and can be used as a non-RSN protocol in an infrastructure BSS.

MAPC authentication is used in an RSN for a Multi-AP Coordination framework when it is based on a PMKSA established by another RSN authentication protocol. Otherwise, it does not guarantee mutual authentication, and can be used as a non-RSN protocol in a Multi-AP Coordination framework.

6.5.5 Authenticate

***TGbn editor: Modify 6.5.5.2, 6.5.5.3, 6.5.5.4, and 6.5.5.5 as follows (CID #151)***

6.5.5.2 MLME-AUTHENTICATE.request

##### 6.5.5.2.1 Function

This primitive requests authentication with a specified peer MAC entity.

6.5.5.2.2 Semantics of the service primitive

***TGbn editor: change the primitive parameters as follows in the .request(CID #151):***

The primitive parameters are as follows:

 MLME-AUTHENTICATE.request (

………………………….

Content of FILS Authentication frame,

Content of PASN Authentication frame,

Content of EDPKE Authentication frame,

Content of MAPC PASN Authentication frame,

VendorSpecificInfo

)

***TGbn editor: insert a new row in the following unnumbered table(CID #151):***

|  |  |  |  |
| --- | --- | --- | --- |
| Name  | Type  | Valid range  | Description |
| Content of EDPKE Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if Authentication Type indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| Content of MAPC PASN Authentication frame | Sequence of elements and fields | As defined in [12.XX.3.2](#H12o13o3o2) (MAPC PASN Frame Construction and Processing), 9.4.2.23(RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.48 (Timeout Interval element) | The set of elements and fields to be included in MAPC PASN Authentication frames. Present if Authentication Type indicates MAPC PASN authentication and dot11MAPC PASN Activated is true, otherwise not present. |
| VendorSpecificInfo  |  A set ofelements |  As defined in 9.4.2.25(Vendor Specific element) |  Zero or more elements. |

6.5.5.3 MLME-AUTHENTICATE.confirm

##### 6.5.5.3.1 Function

This primitive reports the results of an authentication attempt with a specified peer MAC entity.

6.5.5.3.2 Semantics of the service primitive

***TGbn editor: change the primitive parameters as follows in the .confirm(CID #151):***

MLME-AUTHENTICATE.confirm(

………………………….

Content of FILS Authentication frame,

Content of PASN Authentication frame,

Content of EDPKE Authentication frame,

Content of MAPC PASN Authentication frame,

VendorSpecificInfo

)

***TGbn editor: insert the following entry into the unnumbered table in this subclause maintaining the primitive order above(CID #151):***

|  |  |  |  |
| --- | --- | --- | --- |
| Name  | Type  | Valid range  | Description |
| … | … | … | … |
| AuthenticationType | Enumeration | OPEN\_SYSTEM,SHARED\_KEYFAST\_BSS\_TRANSITION,SAE, FILS\_SHAREDKEY\_WITHOUT\_PFS,FILS\_SHARED\_KEY\_WITH\_PFS,FILS\_PUBLIC\_KEY,PASN | Specifies the type of authenticationalgorithm that was used during theauthentication process. This valuematches the AuthenticationTypeparameter specified in the correspondingMLME-AUTHENTICATE.requestprimitive. |
| … | … | … | … |
| Content of EDPKE Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if Authentication Type indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| Content of MAPC PASN Authentication frame | Sequence of elements and fields | As defined in [12.XX.x.2.2](#H12o13o3o2) MAPC PASN Frame Construction and Processing. 9.4.2.23(RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.48 (Timeout Interval element) | The set of elements and fields to be included in MAPC PASN Authentication frames. Present if Authentication Type indicates MAPC PASN authentication and dot11MAPCPASNActivated is true, otherwise not present. |

6.5.5.4 MLME-AUTHENTICATE.indication

6.5.5.4.2 Semantics of the service primitive

***TGbn editor: change the primitive parameters as follows in the .indication(CID #151):***

MLME-AUTHENTICATE.indication(

………………………….

Content of FILS Authentication frame,

Content of PASN Authentication frame,

Content of EDPKE Authentication frame,

Content of MAPC PASN Authentication frame,

VendorSpecificInfo

)

***TGbn editor: insert the following entry into the unnumbered table in this subclause maintaining the primitive order above(CID #151):***

|  |  |  |  |
| --- | --- | --- | --- |
| Name  | Type  | Valid range  | Description |
| … | … | … | … |
| AuthenticationType | Enumeration | OPEN\_SYSTEM,SHARED\_KEYFAST\_BSS\_TRANSITION,SAE, FILS\_SHAREDKEY\_WITHOUT\_PFS,FILS\_SHARED\_KEY\_WITH\_PFS,FILS\_PUBLIC\_KEY,PASN | Specifies the type of authentication algorithm that was used during the authentication process. This value matches the AuthenticationTypeparameter specified in the correspondingMLME-AUTHENTICATE.request primitive. |
| … | … | … | … |
| Content of EDPKE Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if Authentication Type indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| Content of MAPC PASN Authentication frame | Sequence of elements and fields | As defined in [12.XX.3.2](#H12o13o3o2) (MAPC PASN Frame Construction and Processing), 9.4.2.23(RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.48 (Timeout Interval element) | The set of elements and fields to be included in MAPC PASN Authentication frames. Present if Authentication Type indicates MAPC PASN authentication and dot11MAPCPASNActivated is true, otherwise not present. |

6.5.5.5 MLME-AUTHENTICATE.response

6.5.5.5.2 Semantics of the service primitive

***Change the primitive parameters as follows in the .response***

 MLME-AUTHENTICATE.response(

………………………….

Content of FILS Authentication frame,

Content of PASN Authentication frame,

Content of EDPKE Authentication frame,

Content of MAPC PASN Authentication frame,

VendorSpecificInfo

)

***TGbn editor: insert the following entry into the unnumbered table in this subclause maintaining the primitive order above(CID #151):***

|  |  |  |  |
| --- | --- | --- | --- |
| Name  | Type  | Valid range  | Description |
| … | … | … | … |
| AuthenticationType | Enumeration | OPEN\_SYSTEM,SHARED\_KEYFAST\_BSS\_TRANSITION,SAE, FILS\_SHAREDKEY\_WITHOUT\_PFS,FILS\_SHARED\_KEY\_WITH\_PFS,FILS\_PUBLIC\_KEY,PASN | Specifies the type of authenticationalgorithm that was used during the authentication process. This valuematches the AuthenticationTypeparameter specified in the correspondingMLME-AUTHENTICATE.request primitive. |
| … | … | … | … |
| Content of EDPKE Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if Authentication Type indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| Content of MAPC PASN Authentication frame | Sequence of elements and fields | As defined in [12.XX.3.2](#H12o13o3o2) (MAPC PASN Frame Construction and Processing), 9.4.2.23(RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.48 (Timeout Interval element) | The set of elements and fields to be included in MAPC PASN Authentication frames. Present if Authentication Type indicates MAPC PASN authentication and dot11MAPCPASNActivated is true, otherwise not present. |

9.3.3.11 Authentication frame format

***TGbn editor: insert the new rows at the end of table 9-41(CID #151):***

1. Table 9-41—Presence of fields and elements in Authentication frames *(continued):*

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication algorithm | **Authentication transaction sequence number** | **Status code** | **Presence of fields 4 onwards** |
| MAPC PASNauthentication | 1 | Reserved | The RSNE is present. The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero. The PASN Parameters element is present. The Timeout Interval element is optionally present.The Wrapped Data element is present if the wrapped data format in the PASN Parameters element is nonzero and not reserved |
| MAPC PASNauthentication | 2 | Status | The RSNE is present and the PASN Parameters element is present if Status Code field is 0. The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero. The Timeout Interval element is optionally present. The Wrapped Data element is present if wrapped data format in the PASN Parameters element is nonzero and not reserved and the Status Code field is 0. The MIC element is present. |
| MAPC PASNauthentication | 3 | Status | The PASN Parameters element is present if Status Code field is 0. The Wrapped Data element is present if wrapped data format in the PASN Parameters element is nonzero and not reserved; and the Status Code field is 0. The MIC element is present. |

*TGbn editor: make the following change in subclause 9.4(CID #151):*

9.4 Management and Extension frame body components

9.4.1 Fields that are not elements

9.4.1.1 Authentication Algorithm Number field

Authentication algorithm number = 6: FILS Public Key authentication

Authentication algorithm number = 7: PASN authentication

Authentication algorithm number = 8: IEEE 802.1X authentication

Authentication algorithm number = 9: EDPKE authentication

Authentication algorithm number = <ANA>: MAPC PASN authentication

Authentication algorithm number = 65 535: vendor specific use

**9.4.2.23 RSNE**

**9.4.2.23.3 AKM suites**

***Modify Table 9-190 (AKM suite selectors) as follows and update reserved suite type:***

9.4.2.24 RSNE

9.4.2.24.3 AKM suites

***TGbn editor: insert the following new row (MAPC PASN) into Table 9-190 (AKM suite selectors)(CID #151):***

1. Table 9-190—AKM suite selectors

|  |  |  |
| --- | --- | --- |
| **OUI** | **Suite type** | **Meaning** |
| **Authentication type** | **Key management type** | **Key derivation****type** | **Authentication****algorithm****numbers (see****9.4.1.1****(Authentication****Algorithm****Number****field))** |
| … |  |  |  |  |  |
| 00-0F-AC | 29 | EDPKE | EDPKE | EDPKE key management defined in 12.16.9 (Enhanced Data Privacy Key Exchange) | Defined in 12.16.9.3 (Key establishment with EDPKE authentication) |
| 00-0F-AC | <ANA> | MAPC PASN | MAPC PASN | MAPC PASN key management defined in 12.xx (Multi-AP Coordination Preassociation Security Negotiation) | Defined in 12.XX.3 (Key establishment with MAPC PASN authentication) |

**9.4.2.240 RSNXE**

***TGbn editor: make the following change in Table 9-373 (Extended RSN Capabilities field)(CID #151)***.

**Table 9-373—Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| 16 | Device ID Support | A STA sets the Device ID Support field to 1 when dot11DeviceIDActivated is true to indicate that the device ID mechanism is supported. Otherwise, the STA sets the Device ID Support field to 0. |
| 17 | IRM Support | A STA sets the IRM Support field to 1 when dot11IRMActivated is true to indicate that the IRM mechanism is supported. Otherwise, the STA sets the IRM Support field to 0. |
| 18 | KEK In PASN | The field is set to 1 when dot11KEKPASNActivated is true to indicate support for deriving a KEK when using PASN or using MAPC PASN. Otherwise, the field is set to 0. |

**9.4.2.186 Wrapped Data element**

***TGbn editor: change the third paragraph as follows(CID #151):***

The Wrapped Data field is the data used by the FILS authentication algorithm (see 12.11 (Authentication for FILS)), PASN authentication algorithm (see 12.13 (Preassociation security negotiation)), EDPKE algorithm (see 12.16.9 (Enhanced Data Privacy Key Exchange)) and MAPC PASN authentication algorithm (see 12.XX (Multi-AP Coordination Preassociation Security Negotiation)).

9.6.7.64 MAPC Discovery Request frame format

***TGbn editor: make the change in clause 9.6.7.64 as follows (CID #151):***

The MAPC Discovery Request frame is used by an AP to advertise its capabilities and common parameters for MAPC. The format of the MAPC Discovery Request frame is defined in Figure 9-aa20 (MAPC Discovery Request frame format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | Dialog Token | RSNE | RSNXE | MAPC Discovery Info |
| Octets: | 1 | 1 | 1 | variable | variable | variable |

Figure 9-aa20— MAPC Discovery Request frame format

The Category field is defined in 9.4.1.11 (Action field).

The Public Action field is defined in 9.6.7.1 (Public Action field).

The Dialog Token field is set to a nonzero value chosen by the AP sending the MAPC Discovery Request frame.

The RSNE field, if present, contains the Information field of the RSNE described in 9.4.2.23 (RSNE).

The RSNXE field, if present, contains the Information field of the RSNXE described in 9.4.2.240 (RSNXE).The MAPC Discovery Info field carries a MAPC element as defined in 9.4.2.aa3.1 (MAPC element).

NOTE —When a MAPC element carrying per-scheme profiles is included in a MAPC Discovery Request frame, the MAPC Scheme Request Set field is not included in the reported per-scheme profiles.

9.6.7.65 MAPC Discovery Response frame format

The MAPC Discovery Response frame is used by an AP to respond to a MAPC Discovery Request frame. The format of the MAPC Discovery Response frame is defined in Figure 9-aa21 (MAPC Discovery Response frame format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | Dialog Token | RSNE | RSNXE | MAPC Discovery Info |
| Octets: | 1 | 1 | 1 | variable | variable | variable |

Figure 9-aa21— MAPC Discovery Response frame format

The Category field is defined in 9.4.1.11 (Action field).

The Public Action field is defined in 9.6.7.1 (Public Action field).

The Dialog Token field is set to a nonzero value chosen by the AP sending the MAPC Discovery Response frame.

The RSNE field, if present, contains the Information field of the RSNE described in 9.4.2.23 (RSNE).

The RSNXE field, if present, contains the Information field of the RSNXE described in 9.4.2.240 (RSNXE).

The MAPC Discovery Info field carries a MAPC element as defined in 9.4.2.aa3.1 (MAPC element).

NOTE —When a MAPC element carrying per-scheme profiles is included in a MAPC Discovery Response frame, the MAPC Scheme Request Set field is not included in the reported per-scheme profiles.

**11.3.4 Authentication and deauthentication**

**11.3.4.2 Authentication—originating STA or MLD**

***TGbn editor: change the second paragraph as follows(CID #151):***

Upon receipt of an MLME-AUTHENTICATE.request primitive, the originating STA shall authenticate with the indicated STA using the following procedure:

b) The STA shall execute one of the following:

…

5) For PASN authentication, the authentication mechanism described in 12.13 (Preassociation security negotiation (11az)).

6) For EDPKE authentication, the authentication mechanism described in 12.16.9 (Enhanced Data Privacy Key Exchange).

7) For MAPC PASN authentication, the authentication mechanism described in 12.XX (Multi-AP Coordination Preassociation Security Negotiation).

**11.3.4.3 Authentication—destination STA or MLD**

***TGbn editor: change the first paragraph as follows(CID #151):***

Upon receipt of an Authentication frame with authentication transaction sequence number equal to 1, the destination STA shall authenticate with the originating STA using the following procedure:

g) Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is not SUCCESS, the MLME shall transmit an Authentication frame with the corresponding status code, as defined in 9.4.1.9 (Status Code field), and the state for the originating STA or MLD shall be left unchanged. The Authentication frame is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 13.5 (FT protocol), 13.6 (FT resource request protocol), 12.13 (Preassociation security negotiation (11az)),12.16.9 (Enhanced Data Privacy Key Exchange) or 12.XX (Multi-AP Coordination Preassociation Security Negotiation).

12. Security

12.2 Framework

12.2.4 RSNA establishment

***TGbn editor:insert the following paragraph after “i)”(CID #151):***

h) If an RSNA uses PASN authentication, an RSNA capable the STA establishes an RSNA as described in 12.13 (Preassociation security negotiation (11az)).

i) If an RSNA uses EDPKE authentication, an RSNA capable STA establishes an RSNA as described in 12.16.9 (Enhanced Data Privacy Key Exchange).

j) If an RSNA uses MAPC PASN authentication, an RSNA capable STA establishes an RSNA as described in 12.XX (Multi-AP Coordination Preassociation Security Negotiation).

12.6 RSNA security association management

12.6.1 Security associations

12.6.1.1 Security association definitions

12.6.1.1.1 General

***Change the following sentence:***

***TGbn editor:modify 12.6.1.1.1 as follows(CID #151):***

PTKSA: A result of a successful 4-way handshake, FT 4-way handshake, FT authentication sequence, FILS authentication, PASN authentication, EDPKE authentication, or MAPC PASN authentication.

12.6.1.1.6 PTKSA

*Change 12.6.1.1.6 PTKSA as follows*

***TGbn editor: change first paragraph as follows(CID #151):***

The PTKSA results from a successful 4-way handshake, FT 4-way handshake, FT protocol, FT resource request protocol, FILS authentication, PASN authentication, EDPKE authentication or MAPC PASN authentication. This security association is also bidirectional. PTKSAs, except those established using PASN authentication, EDPKE authentication or MAPC PASN authentication, have the same lifetime as the PMKSA or PMK-R1 security Association, whichever comes first. PTKSAs for PASN authentication, EDPKE authentication or MAPC PASN authentication have a minimum of the lifetime of the PMKSA used and the timeout negotiated, if any, during PASN authentication or MAPC PASN authentication. Because the PTKSA is tied to the PMKSA or to a PMK-R1 security association, it only has the additional information from the 4-way handshake, FT Protocol authentication, FILS authentication, PASN authentication, EDPKE authentication or MAPC PASN authentication. There shall be only one PTKSA per key ID per band (see 12.6.20 (Multi-band RSNA)) or per MLD setup (see 35.3.5 (ML (re)setup)) with the same Supplicant and Authenticator MAC addresses.

***TGbn editor: please add the following new clause(CID #151)***

**12.XX Multi-AP Coordination Preassociation Security Negotiation**

**12.XX.1 General**

If dot11MAPC PASN is true, then dot11KEKPASNActivated is set to true.

Multi-AP Coordination Preassociation Security Negotiation (MAPC PASN) is an RSNA authentication protocol in all cases between two MAPC APs where it relies on the existence of a PMKSA for an AKMP, termed base AKMP for MAPC PASN. It is a non-RSNA protocol when there is no PMKSA and the corresponding base AKMP used with it. The protocol supports PTKSA establishment with and without mutual authentication.

MAPC PASN is initialized by the MAPC requesting AP, and has three authentication frames exchanged with MAPC responding AP to generate PTKSA, to protect the individual addressed MAPC negotiation request frame and individual addressed MAPC negotiation response frame.MAPC PASN is an either RSNA or non-RSNA authentication protocol that uses the PASN procedures (see 12.13 (Preassociation security negotiation)) with the following differences:

—The three Authentication frames are exchanged by two UHR APs.

—The entity of MAPC requesting AP is used instead of non-AP STA.

—The entity of MAPC responding AP is used instead of AP.

— The three Authentication frames have the Authentication Algorithm Number field set to <ANA> (MAPC Authentication).

**12.XX.2 Discovery of an MAPC PASN capable AP**

A UHR AP indicates it is capable of performing MAPC PASN by including the MAPC PASN AKMP as part of the RSNE included in MAPC discovery request frame or MAPC discovery response frame. When MAPC PASN AKMP is advertised, the UHR AP shall also include at least one additional AKMP in the RSNE unless it allows PTKSA derivation without authentication using the ephemeral keys exchanged during MAPC PASN authentication.

**12. XX.3 Key establishment with MAPC PASN authentication**

**12. XX.3.1 Overview**

This subclause defines the procedures for establishing a PTKSA and the corresponding shared keys between the MAPC PASN capable AP. The same procedures as specified in 12.13.1 (Overview) are used with the following differences:

— The three Authentication frames have the Authentication Algorithm Number field set to <ANA> (MAPC PASN Authentication).

— MAPC PASN AKMP is used instead of PASN AKMP.

— The RSNE indicates MAPC PASN instead of PASN.

**12. XX.3.2 MAPC PASN Frame Construction and Processing**

The same procedures as specified in 12.13.3.2 (PASN Frame Construction and Processing) are used with the following differences:

— The three Authentication frames have the Authentication Algorithm Number field set to <ANA> (MAPC PASN Authentication).

— MAPC PASN AKMP is used instead of PASN AKMP.

— The RSNE indicates MAPC PASN instead of PASN.

— The PTK is generated as specified in 12.XX.3.4 (PTKSA derivation and MIC Computation with MAPC PASN authentication).

**12. XX.3.3 PTKSA derivation** **with MAPC PASN authentication**

The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) are used.

The following modifications shall be used for PTK computation:

The Min (MAPC requesting AP MAC address, MAPC responding AP MAC address) is used instead of the BSSID.

The Max (MAPC requesting AP MAC address, MAPC responding AP MAC address) is used instead of the SPA.

**12. XX.3.4 MIC Computation with MAPC PASN authentication**

**12.XX.3.4.1 MIC computation for second PASN frame**

The MIC field of the MIC element in the second PASN frame is set by the AP to first MMM octets of:

HMAC-HASH (KCK, BSSID || SPA || RSNE || RSNXE || Frame Data)

Where

HASH is the hash algorithm used in 12.13.8 (PTKSA derivation with PASN authentication)

KCK is the key confirmation key for the PASN PTKSA

BSSID is the Min (MAPC requesting AP MAC address, MAPC responding AP MAC address)

SPA is the Max (MAPC requesting AP MAC address, MAPC responding AP MAC address)

RSNE is the Min (RSN element sent in the MAPC discovery request frame, RSN element sent in the MAPC discovery response frame) || Max (RSN element sent in the MAPC discovery request frame, RSN element sent in the MAPC discovery response frame)

RSNXE is the Min (RSNXE sent in the MAPC discovery request frame, RSNXE sent in the MAPC discovery response frame) || Max (RSNXE sent in the MAPC discovery request frame, RSNXE sent in the MAPC discovery response frame)

Frame Data is the body of the second PASN frame including the MIC element with the octets in the MIC field of the MIC element set to 0

MMM is half of the output length in octets for the hash function used, that is, 16 or 24 octets for SHA-256 and SHA-384, respectively

MAPC discovery RSNE and RSNXE are included in the MIC computation so that a downgrade attack with forged RSNE MAPC discovery will result in a MIC mismatch and thus PASN authentication failure.

**12. XX.3.4.2 MIC computation for third PASN frame**

The MIC field of the MIC element in the third PASN frame is set by the non-AP STA to first MMM octets of:

HMAC-HASH (KCK, SPA || BSSID || F1 Auth || Frame Data)

Where

HASH is the hash algorithm used in 12.13.8 (PTKSA derivation with PASN authentication)

KCK is the key confirmation key for the PASN PTKSA

SPA is the Max (MAPC requesting AP MAC address, MAPC responding AP MAC address)

BSSID is the Min (MAPC requesting AP MAC address, MAPC responding AP MAC address)

F1 Auth is the HASH of body of the first PASN frame

Frame Data is the body of the third PASN frame including the MIC element with the octets in the MIC field of the MIC element set to 0

MMM is half of the output length in octets for the hash function used, that is, 16 or 24 octets for SHA-256 and SHA-384, respectively

# Annex C

**(normative)**

1. ASN.1 encoding of the MAC and PHY MIB

## C. 3 MIB detail

***…***

***Modify “Dot11StationConfigEntry” as follows:***

Dot11StationConfigEntry ::=

SEQUENCE{

…….

dot11S1GOptionImplemented TruthValue,

dot11PASNActivated TruthValue,

dot11NoAuthPASNActivated TruthValue,

dot11EPDPKEActivated TruthValue,

dot11MAPCPASNActivated TruthValue
 }

***Insert the following object before the “End of.” as shown below:***

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11StationConfig TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

*…….*

dot11MAPCPASNActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable. It is written by an external management entity or the SME. Changes take effect for the next MLME-START.request primitive or MLME JOIN.request primitive. This attribute indicates whether or not MAPC PASN authentication is enabled."

DEFVAL {false}

::= { dot11StationConfigEntry <ANA> }

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* End of dot11StationConfig TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*