IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | SB1 CR for CID 6020 | | | | | | Date: 2023-10-11 | | | | | | Author(s): | | | | | | Name | Affiliation | Address | Phone | email | | Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVme D4.0:

6020

**Revision History:**

R0: Initial version. Difference with 11-23-0945r0 are marked with green.

# CID 6020

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID**  **Clause**  **Page.Line** |  |  | **Comment** | **Proposed Change** |
| 6020 |  |  | There are 51 instances of "group cipher suite" in the spec. However, group cipher suite is not a precise term. Specifically, we have group cipher suite for Data frame or group data cipher suite and group cipher suite for management frame or group management cipher suite. In some places, we specifically differentiate the difference. In some places, we just say group cipher suite, and it leaves confusions on whether we mean both group data cipher suite and group management cipher suite. In some places for GTKSA, it actually also just means Group data cipher suite. | Examine the instances of “group cipher” and clarify whether it means both group data cipher suite and group management cipher suite or just group data cipher. Author of 11-23/945r0 will continue to present the proposals. |

## Discussion:

There are many instances of “group cipher” in the baseline.

Case 1:

Sometimes there are additional context for the usage of group cipher suite like “group cipher suite for Data frames” or “group cipher suite for Management frames*”* as shown below. In these cases, there is no ambiguity.

*In non-DMG RSNA, the cipher suite selector 00-0F-AC:4 (CCMP-128) is the default group cipher suite for Data frames when the Group Data Cipher Suite field is not included in the RSNE(#1776).*

*In an RSNA with management frame protection enabled, the cipher suite selector 00-0F-AC:6 (BIP-CMAC- 128) is the default group cipher suite for Management frames when the Group Management Cipher Suite field is not included in the RSNE.*

Note that there are also usages like “group data cipher suite” or “group management cipher suite”. In these caes, there are no ambiguity as well.

In sum, instead of “group cipher suite for Data frame”, we propose an editorial change to use “group data cipher suite”. Instead of “group cipher suite for Management frame”, we propose an editorial change to use “group management cipher suite”. This will unify the usage of term. No proposed change beyond the editorial suggestion.

Case 2:

There are also cases where there are no additional texts like “for Data frames” or “for Management frames” for group cipher suite. However, the context is enough to determine that “group cipher suite” means only group data cipher suite.

For example, the below context talks about usage for pairwise cipher suite selector. Since we do not use BIP-CMAC or BIP-GMAC (used by group management cipher suite) for pairwise cipher, “Use group cipher suite” below must mean the “group data cipher suite”.

*A STA that has associated with management frame protection enabled shall not use pairwise cipher suite selectors (#3056)TKIP or “Use group cipher suite.”*

In sum, change “group cipher suite” to “group data cipher suite” based on the context.

Case 3:

Finally, there are caes where there are no additional texts and the context is not enough to definitely figure out whether “group cipher suite” means only “group data cipher suite” or only “group management cipher suite”. In this case, the interpretation is that group cipher suite will mean both group data cipher suite and group management cipher suite.

*It shall also specify the group cipher suite specified by the targeted AP.*

In sum, change “group cipher suite” to “group data cipher suite and group management cipher suite” in this case.

## Proposed Resolution: CID 6020

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for CID 6020 in 11-23/1745r0

## Proposed Text Update: CID 6020

*Instruction to TGme Editor: Update REVme D4.0 9.4.2.23.2 as shown below (track change on).*

**9.4.2.23.2 Cipher suites**

(…existing texts….)

|  |  |  |
| --- | --- | --- |
| * **Cipher suite selectors** | | |
| **OUI** | **Suite type** | **Meaning** |
| 00-0F-AC | 0 | Use group data cipher suite |
| 00-0F-AC | 1 | (#3056)Reserved |
| 00-0F-AC | 2 | TKIP |
| 00-0F-AC | 3 | Reserved |
| 00-0F-AC | 4 | CCMP-128 |
| 00-0F-AC | 5 | (#3056)Reserved |
| 00-0F-AC | 6 | BIP-CMAC-128 |
| 00-0F-AC | 7 | Group addressed traffic not allowed |
| 00-0F-AC | 8 | GCMP-128 |
| 00-0F-AC | 9 | GCMP-256 |
| 00-0F-AC | 10 | CCMP-256 |
| 00-0F-AC | 11 | BIP-GMAC-128 |
| 00-0F-AC | 12 | BIP-GMAC-256 |
| 00-0F-AC | 13 | BIP-CMAC-256 |
| 00-0F-AC | 14–255 | Reserved |
| Other OUI or CID | Any | Vendor-specific |

(…existing texts….)

In non-DMG RSNA, the cipher suite selector 00-0F-AC:4 (CCMP-128) is the default group data cipher suite when the Group Data Cipher Suite field is not included in the RSNE(#1776).

(…existing texts….)

In DMG RSNA, the cipher suite selector 00-0F-AC:8 (GCMP-128) is the default group data cipher suite when the Group Data Cipher Suite field is not included in the RSNE(#1776).

(…existing texts….)

In an RSNA with management frame protection enabled, the cipher suite selector 00-0F-AC:6 (BIP-CMAC- 128) is the default group management cipher suite when the Group Management Cipher Suite field is not included in the RSNE(#1776).

(…existing texts….)

Use of any group data cipher suite other than TKIP with TKIP as the pairwise cipher suite is not supported.

The cipher suite selector 00-0F-AC:0 (Use group data cipher suite) is valid only as the pairwise cipher suite. An AP specifies the selector 00-0F-AC:0 (Use group data cipher suite) for a pairwise cipher suite if it does not support any pairwise cipher suites. If an AP specifies 00-0F-AC:0 (Use group data cipher suite) as the pairwise cipher selection, this is the only pairwise cipher selection the AP advertises.

(#387)If an AP advertises a group data cipher suite other than TKIP(#3056), then the AP supports pairwise keys, and thus the pairwise suite selector 00-0F-AC:0 (Use group data cipher suite) is not a valid option.

(…existing texts….)

|  |  |  |  |
| --- | --- | --- | --- |
| * **Cipher suite usage** | | | |
| **Cipher suite selector** | **GTK** | **PTK** | **IGTK or BIGTK** |
| Use group data cipher suite | No | Yes | No |
| (#3056)TKIP | Yes | Yes | No |
| CCMP-128 | Yes | Yes | No |
| BIP-CMAC-128 | No | No | Yes |
| GCMP-128 | Yes | Yes | No |
| GCMP-256 | Yes | Yes | No |
| CCMP-256 | Yes | Yes | No |
| BIP-GMAC-128 | No | No | Yes |
| BIP-GMAC-256 | No | No | Yes |
| BIP-CMAC-256 | No | No | Yes |

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 11.12 as shown below (track change on).*

**11.12 Group addressed management frame protection procedures**

When management frame protection is negotiated, the MLME shall provide an encapsulation service for group addressed robust Management frames. All group addressed robust Management frames shall be submitted to this service for encapsulation and transmission.

(#1980)(#162)In an MBSS, for group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), the group addressed frame protection service shall take the following actions:

— The frames shall be encapsulated and protected with the MGTK using the group data cipher negotiated during the AMPE exchange.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.2.5 as shown below (track change on).*

**12.2.5 RSNA assumptions and constraints**

(…existing texts….)

An HT STA shall not use either of the pairwise cipher suite selectors: “Use group data cipher suite” or TKIP to communicate with another HT STA.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.3.4.4.2 as shown below (track change on).*

**12.3.4.4.2 TKIP countermeasures for an Authenticator**

(…existing texts….)

The requirement to deauthenticate all STAs using TKIP includes those using other pairwise ciphers if they are using TKIP as the group data cipher.

*Instruction to TGme Editor: Update REVme D4.0 12.3.4.4.3 as shown below (track change on).*

**12.3.4.4.3 TKIP countermeasures for a Supplicant**

(…existing texts….)

3) If less than 60 s have passed since the most recent previous MIC failure, delete the PTKSA and

GTKSA. Deauthenticate from the AP and wait for 60 s before (re)establishing a TKIP

association with the same AP. A TKIP association is any IEEE 802.11 association that uses

TKIP for its pairwise or group data cipher suite.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.6.1.1.8 as shown below (track change on).*

**12.6.1.1.8 GTKSA**

(…existing texts….)

A GTKSA consists of the following:

— Direction vector (whether the GTK is used for transmit or receive).

— Group data cipher suite selector

(…existing texts….)

When the GTK is used to encrypt individually addressed traffic (the selectable cipher suite is “Use group data cipher suite”), the GTKSA is bidirectional.

*Instruction to TGme Editor: Update REVme D4.0 12.6.1.1.10 as shown below (track change on).*

**12.6.1.1.10 Mesh GTKSA**

(…existing texts….)

The mesh GTKSA contains the following:

— MGTK

— MGTK source mesh STA MAC address (mesh STA that uses this GTK to encrypt transmissions)

— Group data cipher suite selector

— Direction vector (whether this is a receive mesh GTKSA or transmit mesh GTKSA)

— Key Index

*Instruction to TGme Editor: Update REVme D4.0 12.6.3 as shown below (track change on).*

**12.6.3 RSNA policy selection in an infrastructure BSS**

(…existing texts….)

It shall also specify the group data cipher suite and group management cipher suite (if present) specified by the targeted AP.

(…existing texts….)

In order to accommodate local security policy, a STA may choose not to associate with an AP that does not support any pairwise cipher suites. An AP may indicate that it does not support any pairwise keys by advertising 00-0F-AC:0 (Use group data cipher suite) as the pairwise cipher suite selector.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.6.4 as shown below (track change on).*

**12.6.4 RSNA policy selection in an IBSS**

In an IBSS all STAs use a single group data cipher suite and group management cipher suite (if management frame protection is enabled), and all STAs support a common subset of pairwise cipher suites. However, the SMEs of any pair of non-HT STAs may negotiate to use any common pairwise cipher suite they both support. Each STA shall include the group data cipher suite, the group management cipher suite (if management frame protection is enabled) and its list of pairwise cipher suites in its Beacon and Probe Response frames. Two STAs shall not establish a PMKSA unless they have advertised the same group data cipher suite and group management cipher suite (if management frame protection is enabled). Similarly, the two STAs shall not establish a PMKSA if the STAs have advertised disjoint sets of pairwise cipher suites.

(…existing texts….)

The SME shall check that the group data cipher suite, group management cipher suite (if management frame protection is enabled), and AKMP match those in the Beacon and Probe Response frames for the IBSS.

NOTE 2—The RSNEs in message 2 and message 3 are not the same as in the Beacon frame. The group data cipher, group management cipher (if management frame protection is enabled), and AKMP are the same, but the pairwise ciphers might differ because Beacon frames from different STAs might advertise different pairwise ciphers. Thus, IBSS STAs use the same (#3266)AKMP, group data cipher, and group management cipher (if management frame protection is enabled), while different pairwise ciphers might be used between STA pairs.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.6.5 as shown below (track change on).*

**12.6.5 RSNA policy selection in an MBSS**

(…existing texts….)

All mesh STAs in an MBSS use the same group data cipher suite and group management cipher suite (if management frame protection is enabled). Mesh STAs establish authenticated peerings with each other using the AMPE protocol (see 14.6 (Authenticated mesh peering exchange (AMPE))). In AMPE, mesh STAs negotiate a pairwise cipher suite, and establish a mesh PTKSA(#240), to protect individually addressed frames and state a group data cipher suite and establish a mesh GTKSA to process incoming group addressed frames from a peer.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.6.13 as shown below (track change on).*

**12.6.13 RSNA key management in an IBSS**

(…existing texts….)

A STA joining an IBSS shall support and advertise in the Beacon frame the security configuration of the IBSS, which includes the group data cipher suite, advertised pairwise cipher suite, AKMP, and if management frame protection is enabled, group management cipher suite (see 12.6.4 (RSNA policy selection in an IBSS)). The STA may use the Probe Request frame to discover the security policy of a STA, including additional individual cipher suites the STA supports.(#199)

NOTE—Because of the requirement for a STA joining an IBSS to support the security configuration of the IBSS, all Beacon frames transmitted in an IBSS have the same security policy.

*Instruction to TGme Editor: Update REVme D4.0 12.6.20.1 as shown below (track change on).*

**12.6.20.1 General**

(…existing texts….)

If the pairwise, group data cipher suite, and group management cipher suite used by a pair of multi-band capable devices to communicate with each other in the current operating band/channel (#1733)are also supported after the transfer to another band/channel that was performed using transparent FST, the devices shall continue using the same cipher suites to communicate with each other after the transfer. In all other cases, a separate RSNA has to be established for the other band/channel (see 12.6.20.2 (Nontransparent multi-band RSNA) and 12.6.20.4 (Multiband RSNA with TDLS in a non-DMG BSS)).

*Instruction to TGme Editor: Update REVme D4.0 12.7.2 as shown below (track change on).*

**12.7.2 EAPOL-Key frames**

(…existing texts….)

i) The value 1 shall be used for all (#1836)EAPOL-Key PDUs to a STA when the negotiated

AKM is 00-0F-AC:1 or 00-0F-AC:2 and the pairwise cipher is TKIP or “Use group data cipher suite”. In this case, the “Deprecated” row in Table 12-11 (Integrity and key wrap algorithms(#3244)) is used

ii) (#432)The value 2 shall be used for all (#1836)EAPOL-Key PDUs to a STA when the

negotiated AKM is 00-0F-AC:1 or 00-0F-AC:2 and either the pairwise or the group data cipher

is an RSNA mechanism other than TKIP. In this case, the matching row in Table 12-11 (Integrity and key wrap algorithms(#3244)) is used.

(…existing texts….)

(#1843)The following (#1836)EAPOL-Key PDUs are used to implement the (#3416)handshakes:

— 4-way handshake message 1 is an (#1836)EAPOL-Key PDU with the Key Type subfield equal to

1. The fields and their values in the EAPOL-Key PDU are described in 12.7.2 (EAPOL-Key frames). (#3638)Use of the Key Data field to indicate a PMKID when a cached PMKSA is being

used in this key derivation is defined in 12.6.8.3 (Cached PMKSAs and RSNA key management).(#589)(#190)

— 4-way handshake message 2 is an (#1836)EAPOL-Key PDU with the Key Type subfield equal to 1.(#589-Ed1)(#190)

An ESS Supplicant’s SME shall insert the RSNE it sent in its (Re)Association Request frame, and shall insert the RSNXE it sent in its (Re)Association Request frame if the RSNXE is present in the (Re)Association Request frame it sent. The RSNE and the RSNXE are included as transmitted in the Management frame. On receipt of message 2, the Authenticator’s SME shall validate the selected security configuration against the RSNE received in the (Re)Association Request frame, and shall validate the RSNXE included in message 2 against the RSNXE received in the (Re)Association Request frame from the Supplicant.

An IBSS Supplicant’s SME shall insert an RSNE containing a selected pairwise cipher suite. The Authenticator’s SME shall validate that the pairwise cipher suite selected is one of its configured cipher suites and that the group data cipher suite, group management cipher suite (if management frame protection is enabled), and AKM are consistent.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D3.0 12.7.3 as shown below (track change on).*

**12.7.3 EAPOL-Key PDU construction and processing**

(…existing texts….)

Table 12-11 (Integrity and key wrap algorithms(#3244)) indicates the particular algorithms to use when constructing and processing EAPOL-Key frames and FT authentication sequence. The AKM of “Deprecated” indicates (#3266)AKM 00-0F-AC:1 or 00-0F-AC:2 when either TKIP or “Use group data cipher suite” is the negotiated pairwise cipher.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.7.6.4 as shown below (track change on).*

**12.7.6.4 4-way handshake message 3**

(…existing texts….)

Key Data =

— For PTK generation for the current operating band, the AP’s Beacon/Probe Response

frame’s RSNE for the current operating band, and, optionally, a second RSNE that is the Authenticator’s pairwise cipher suite assignment for the current operating band, and, if a group data cipher has been negotiated, the GTK and the GTK’s (#3493)key ID (see 12.7.2 (EAPOL-Key frames)) for the current operating band, and if management frame protection is negotiated, the IGTK KDE, and if beacon protection is enabled, the BIGTK KDE(11ba), and if WUR frame protection is negotiated, the WIGTK KDE, and when this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated according to the procedures of 12.7.1.6.4 (PMK-R1) in the PMKID List field of the RSNE and the FTE with the same contents as in the (Re)Association Response frame, the MDE with the same contents as in the (Re)Association Response frame, the reassociation deadline timeout set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime]; or

— For PTK generation for a supported band other than the current operating band, the

Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s Multi-band element associated with the supported band, and optionally a second Multi-band element that indicates the Authenticator’s pairwise cipher suite assignment for the supported band, and, if group data cipher for the supported band is negotiated, the Multiband GTK KDE for the supported band if dot11MultibandImplemented is true, or

— For generating a single PTK for all involved bands, the Authenticator’s Beacon/DMG

Beacon/Announce/Probe Response/Information Response frame’s RSNE and Multi-band element(s), and optionally, additional RSNE and Multi-band element(s) that indicate the Authenticator’s assignment of one pairwise cipher suite for all involved bands; if a group data cipher for all involved bands is negotiated, the GTK and the GTK’s (#3493)key ID for all involved bands, if dot11MultibandImplemented is true and both the Authenticator and the Supplicant use the same MAC address in the current operating band and the other supported band(s), or

— For generating different PTKs for the current operating band and other supported band(s),

the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s RSNE and Multi-band element(s), and optionally, additional RSNE and Multi-band elements that are the Authenticator’s pairwise cipher suite assignments for one or more involved bands; if group data ciphers for the involved bands are negotiated, the Multiband GTK KDEs for the involved bands, if dot11MultibandImplemented is true and the Joint Multi-band RSNA subfield is 1 for both the Authenticator and Supplicant, and either the Authenticator or the Supplicant uses different MAC addresses for different bands.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.7.8.2 as shown below (track change on).*

**12.7.8.2 TPK handshake**

The TPK handshake occurs as part of the TDLS direct link(#1356) setup procedure. The TPKSA is the result of the successful completion of the TPK handshake protocol, which derives keys for providing confidentiality and data origin authentication.

In order to maintain TPK confidentiality, both the TDLS initiator STA and the TDLS responder STAs establish an RSNA with their common AP prior to executing the TPK handshake. To meet this criterion, a STA may refuse to initiate the TDLS direct link if:

a) The AP does not include an RSNE in its Beacon and Probe Response frames to advertise the availability of security;

b) The AP’s RSNE indicates that (#3056)TKIP (00-0F-AC:2) is enabled as either pairwise or group data cipher suites;(#223) or

c) The AP’s RSNE indicates that Use group cipher suite (00-0F-AC:0) is used as the pairwise cipher suite.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D3.0 12.12.2 as shown below (track change on).*

**12.12.2 Security constraints in the 6 GHz band**

The following apply to a STA operating in the 6 GHz band:

— The STA shall not use the following pre-RSNA security method(#3056):

— Open System authentication without encryption

— The STA shall not use the following cipher suite selectors:

— 00-0F-AC:0 (Use group data cipher suite)(#3056)

— 00-0F-AC:2 (TKIP)

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 12.12.3 as shown below (track change on).*

**12.12.3 Security constraints for HT STAs(#3133)**

An HT STA shall not use either of the pairwise cipher suite selectors “Use group data cipher suite” or TKIP to communicate with another HT STA.

*Instruction to TGme Editor: Update REVme D4.0 12.12.4 as shown below (track change on).*

**12.12.4 Security constraints for VHT STAs(#3133)**

A VHT STA shall not use either of the pairwise cipher suite selectors: “Use group data cipher suite” or TKIP to communicate with another HT STA or VHT STA.

*Instruction to TGme Editor: Update REVme D4.0 12.12.5 as shown below (track change on).*

**12.12.5 Security constraints for HE STAs(#3133)**

An HE STA shall not use either of the pairwise cipher suite selectors: “Use group data cipher suite” or TKIP to communicate with another HT STA, VHT STA, or HE STA.

*Instruction to TGme Editor: Update REVme D4.0 12.12.6 as shown below (track change on).*

**12.12.6 Security constraints for S1G STAs(#3133)**

An S1G STA shall not use the pairwise cipher suite selectors TKIP or “Use group data cipher suite”.

*Instruction to TGme Editor: Update REVme D4.0 12.12.8 as shown below (track change on).*

**12.12.8 Security constraints for STAs that support management frame protection(#3133)**

A STA that has associated with management frame protection enabled shall not use pairwise cipher suite selectors TKIP or “Use group data cipher suite”.

*Instruction to TGme Editor: Update REVme D4.0 14.6.2.2 as shown below (track change on).*

**14.6.2.2 Group data cipher suite and group management cipher suite selection**

Group data cipher suite (#3056)selector TKIP shall not be used as the group data cipher suite when dot11MeshSecurityActivated is true.

The mesh STA shall not use a different group data cipher suite or a different group management cipher suite (if management frame protection is enabled) than the one used by the peer mesh STA or candidate peer mesh STA in the same MBSS.

A mesh STA shall announce in a Mesh Peering Open frame the group data cipher suite and group management cipher suite (if management frame protection is enabled) it uses for broadcast protection. When it receives a Mesh Peering Open frame from a candidate peer, it shall verify that it supports the candidate’s announced group data cipher suite and group management cipher suite (if management frame protection is enabled). In addition, if the mesh STA receives a Mesh Peering Confirm frame, it shall verify that it supports the group data cipher suite and group management cipher suite (if management frame protection is enabled) listed in that frame. If either selection fails, the mesh STA shall issue the appropriate reply frame with the MESH-INVALID-SECURITY-CAPABILITY reason code.

*Instruction to TGme Editor: Update REVme D4.0 14.6.5.3.2 as shown below (track change on).*

**14.6.5.3.2 Processing Mesh Peering Confirm frames for AMPE**

(…existing texts….)

b) If dot11MeshSecurityActivated is true, the group data cipher suite is checked and the group management cipher suite (if management frame protection is enabled) is checked. If the received group data cipher suite or the received group management cipher suite is not supported by the mesh STA, the mesh STA shall reject the received Mesh Peering Confirm frame and the CNF\_RJCT event is invoked to the corresponding AMPE finite state machine with the failure reason code MESH-INVALID-SECURITY-CAPABILITY.

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 14.8 as shown below (track change on).*

**14.8 Mesh security**

During the AMPE, the peers negotiate, and agree upon, a pairwise (#3270)cipher suite, a group data cipher suite, and a group management cipher suite (if management frame protection is enabled). They also establish a mesh PTKSA(#240) and mesh GTKSA to be used with the pairwise cipher suite and group data cipher suite, respectively.

When dot11MeshSecurityActivated is true, (#1980)individually addressed mesh Data frames and individually addressed robust Management frames (see 12.2.7 (Requirements for management frame protection)) shall be protected by the mesh PTKSA(#240), and group addressed Data frames, and group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9- 79 (Category values), shall be protected by the MGTK.(#3393)

When dot11RSNAProtectedManagementFramesActivated is true, group addressed robust Management frames that are not protected by the MGTK(#3393) shall be protected using BIP (see 11.12 (Group addressed management frame protection procedures)).

*Instruction to TGme Editor: Update REVme D4.0 B.4.4.1 as shown below (track change on).*

**B.4.4.1 MAC protocol capabilities**

(…existing texts….)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PC34.1 | RSNE | 9.4.2.23 (RSNE) | PC34:M | Yes o No o N/A o |
| PC34.1.1 | Group data cipher suite | 9.4.2.23 (RSNE) | PC34.1:M | Yes o No o N/A o |
| PC34.1.2 | Pairwise cipher suite list | 9.4.2.23 (RSNE) | PC34.1:M | Yes o No o N/A o |
| PC34.1.2.1 | (#1912)Counter Mode with cipher-block chaining message authentication code protocol (CCMP) data confidentiality protocol using CCMP-128 | 12.5.2 (CTR with CBC-MAC protocol (CCMP)) | PC34:M | Yes o No o N/A o |
| PC34.1.2.1.1 | CCMP cryptographic encapsulation procedure using CCMP-128 | 12.5.2.3 (CCMP cryptographic encapsulation) | PC34.1.2.1:M | Yes o No o N/A o |
| PC34.1.2.1.2 | CCMP decapsulation procedure using CCMP-128 | 12.5.2.4 (CCMP decapsulation) | PC34.1.2.1:M | Yes o No o N/A o |
| PC34.1.3 | Group management cipher suite | 9.4.2.23 (RSNE) | PC34.1:O | Yes o No o N/A o |

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 C.3 as shown below (track change on).*

* **MIB detail**

Dot11RSNAConfigEntry ::=

SEQUENCE {

dot11RSNAConfigVersion Unsigned32,

dot11RSNAConfigPairwiseKeysImplemented Unsigned32,

dot11RSNAConfigGroupCipher OCTET STRING,

dot11RSNAConfigGroupRekeyMethod INTEGER,

dot11RSNAConfigGroupRekeyTime Unsigned32,

dot11RSNAConfigGroupRekeyPackets Unsigned32,

dot11RSNAConfigGroupRekeyStrict TruthValue,

dot11RSNAConfigPSKValue OCTET STRING,

dot11RSNAConfigPSKPassPhrase DisplayString,

dot11RSNAConfigGroupUpdateCount Unsigned32,

dot11RSNAConfigPairwiseUpdateCount Unsigned32,

dot11RSNAConfigGroupCipherSize Unsigned32,

dot11RSNAConfigPMKLifetime Unsigned32,

dot11RSNAConfigPMKReauthThreshold Unsigned32,

dot11RSNAConfigNumberOfPTKSAReplayCounters Unsigned32,

dot11RSNAConfigSATimeout Unsigned32,

dot11RSNAAuthenticationSuiteSelected OCTET STRING,

dot11RSNAPairwiseCipherSelected OCTET STRING,

dot11RSNAGroupCipherSelected OCTET STRING,

dot11RSNAPMKIDUsed OCTET STRING,

dot11RSNAAuthenticationSuiteRequested OCTET STRING,

dot11RSNAPairwiseCipherRequested OCTET STRING,

dot11RSNAGroupCipherRequested OCTET STRING,

dot11RSNATKIPCounterMeasuresInvoked Unsigned32,

dot11RSNA4WayHandshakeFailures Unsigned32,

dot11RSNAConfigNumberOfGTKSAReplayCounters Unsigned32,

dot11RSNAConfigSTKKeysImplemented Unsigned32,

dot11RSNAConfigSTKCipher OCTET STRING,

dot11RSNAConfigSTKRekeyTime Unsigned32,

dot11RSNAConfigSMKUpdateCount Unsigned32,

dot11RSNAConfigSTKCipherSize Unsigned32,

dot11RSNAConfigSMKLifetime Unsigned32,

dot11RSNAConfigSMKReauthThreshold Unsigned32,

dot11RSNAConfigNumberOfSTKSAReplayCounters Unsigned32,

dot11RSNAPairwiseSTKSelected OCTET STRING,

dot11RSNASMKHandshakeFailures Unsigned32,

dot11RSNASAERetransPeriod Unsigned32,

dot11RSNASAEAntiCloggingThreshold Unsigned32,

dot11RSNASAESync Unsigned32,

dot11RSNAStatsGCMPReplays Unsigned32,

dot11RSNAStatsRobustMgmtGCMPReplays Unsigned32,

dot11RSNAConfigGroupManagementCipher OCTET STRING,

dot11RSNAConfigGroupManagementCipherSize Unsigned32,

dot11RSNAGroupManagementCipherSelected OCTET STRING,

dot11RSNAGroupManagementCipherRequested OCTET STRING,

}

(…existing texts….)

dot11RSNAConfigGroupCipher OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This object indicates the group data cipher suite selector the entity uses. The group data cipher suite in the RSNE takes its value from this variable. It consists of an OUI or CID (the first 3 octets) and a cipher suite identifier (the last octet)."

::= { dot11RSNAConfigEntry 4 }

(…existing texts….)

dot11RSNAConfigGroupCipherSize OBJECT-TYPE

SYNTAX Unsigned32 (0..4294967295)

UNITS "bits"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This object indicates the length of the group data cipher key."

::= { dot11RSNAConfigEntry 15 }

(…existing texts….)

dot11RSNAGroupCipherSelected OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the RSNA Key Management entity in the SME when a security association is established.

The selector of the last group data cipher negotiated."

::= { dot11RSNAConfigEntry 22 }

(…existing texts….)

dot11RSNAGroupCipherRequested OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the RSNA Key Management entity in the SME when a security association is established.

The selector of the last group data cipher requested."

::= { dot11RSNAConfigEntry 26 }

(…existing texts….)

dot11RSNAConfigGroupManagementCipher OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This object indicates the group management cipher suite selector the entity uses. The group management cipher suite in the RSNE takes its value from this variable. It consists of an OUI or CID (the first 3 octets) and a cipher suite identifier (the last octet)."

::= { dot11RSNAConfigEntry <ANA> }

dot11RSNAConfigGroupManagementCipherSize OBJECT-TYPE

SYNTAX Unsigned32 (0..4294967295)

UNITS "bits"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This object indicates the length of the group management cipher key."

::= { dot11RSNAConfigEntry <ANA> }

dot11RSNAGroupManagementCipherSelected OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the RSNA Key Management entity in the SME when a security association is established.

The selector of the last group management cipher negotiated."

::= { dot11RSNAConfigEntry <ANA> }

dot11RSNAGroupManagementCipherRequested OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the RSNA Key Management entity in the SME when a security association is established.

The selector of the last group management cipher requested."

::= { dot11RSNAConfigEntry 26 }

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

-- \* End of dot11RSNAConfig TABLE

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

(…existing texts….)

Dot11InterworkingEntry ::=

SEQUENCE {

dot11NonAPStationMacAddress MacAddress,

dot11NonAPStationUserIdentity DisplayString,

dot11NonAPStationInterworkingCapability BITS,

dot11NonAPStationAssociatedSSID OCTET STRING,

dot11NonAPStationUnicastCipherSuite OCTET STRING,

dot11NonAPStationBroadcastCipherSuite OCTET STRING,

dot11NonAPStationAuthAccessCategories BITS,

dot11NonAPStationAuthMaxVoiceRate Unsigned32,

dot11NonAPStationAuthMaxVideoRate Unsigned32,

dot11NonAPStationAuthMaxBestEffortRate Unsigned32,

dot11NonAPStationAuthMaxBackgroundRate Unsigned32,

dot11NonAPStationAuthMaxVoiceOctets Unsigned32,

dot11NonAPStationAuthMaxVideoOctets Unsigned32,

dot11NonAPStationAuthMaxBestEffortOctets Unsigned32,

dot11NonAPStationAuthMaxBackgroundOctets Unsigned32,

dot11NonAPStationAuthMaxHCCAHEMMOctets Unsigned32,

dot11NonAPStationAuthMaxTotalOctets Unsigned32,

dot11NonAPStationAuthHCCAHEMM TruthValue,

dot11NonAPStationAuthMaxHCCAHEMMRate Unsigned32,

dot11NonAPStationAuthHCCAHEMMDelay Unsigned32,

dot11NonAPStationAuthSourceMulticast TruthValue,

dot11NonAPStationAuthMaxSourceMulticastRate Unsigned32,

dot11NonAPStationVoiceMSDUCount Counter32,

dot11NonAPStationDroppedVoiceMSDUCount Counter32,

dot11NonAPStationVoiceOctetCount Counter32,

dot11NonAPStationDroppedVoiceOctetCount Counter32,

dot11NonAPStationVideoMSDUCount Counter32,

dot11NonAPStationDroppedVideoMSDUCount Counter32,

dot11NonAPStationVideoOctetCount Counter32,

dot11NonAPStationDroppedVideoOctetCount Counter32,

dot11NonAPStationBestEffortMSDUCount Counter32,

dot11NonAPStationDroppedBestEffortMSDUCount Counter32,

dot11NonAPStationBestEffortOctetCount Counter32,

dot11NonAPStationDroppedBestEffortOctetCount Counter32,

dot11NonAPStationBackgroundMSDUCount Counter32,

dot11NonAPStationDroppedBackgroundMSDUCount Counter32,

dot11NonAPStationBackgroundOctetCount Counter32,

dot11NonAPStationDroppedBackgroundOctetCount Counter32,

dot11NonAPStationHCCAHEMMMSDUCount Counter32,

dot11NonAPStationDroppedHCCAHEMMMSDUCount Counter32,

dot11NonAPStationHCCAHEMMOctetCount Counter32,

dot11NonAPStationDroppedHCCAHEMMOctetCount Counter32,

dot11NonAPStationMulticastMSDUCount Counter32,

dot11NonAPStationDroppedMulticastMSDUCount Counter32,

dot11NonAPStationMulticastOctetCount Counter32,

dot11NonAPStationDroppedMulticastOctetCount Counter32,

dot11NonAPStationPowerManagementMode INTEGER,

dot11NonAPStationAuthDls TruthValue,

dot11NonAPStationVLANId Unsigned32,

dot11NonAPStationVLANName DisplayString,

dot11NonAPStationAddtsResultCode INTEGER}

(…existing texts….)

dot11NonAPStationBroadcastCipherSuite OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-only

STATUS deprecated(#3271)

DESCRIPTION

"(#3271)Deprecated as this is not required for interworking.

This is a status variable.

It is written by the SME after a non-AP STA authenticates with the BSS.

(#3256)The selector of the group cipher suite that is currently in use by the non-AP STA for Data frames.(#1649) It consists of an OUI or CID (the first 3 octets) and a cipher suite identifier the last octet)."

::= { dot11InterworkingEntry 6 }

(…existing texts….)

*Instruction to TGme Editor: Update REVme D4.0 R.2.4 as shown below (track change on).*

**R.2.4 Sales meeting**

(…existing texts….)

b) The Probe Response frame received by the laptop indicated the following capabilities:

1) Extended Capabilities element indicates: AP provides interworking service.

2) Interworking element indicates: Internet is available, venue group = 2 (Business) and venue

type = 8 (Research and Development Facility).

3) RSNE indicates: IEEE 802.1X authentication with CCMP-128 pairwise, group data cipher suite, and group management cipher suite.

(…existing texts….)