IEEE P802.11
Wireless LANs

|  |
| --- |
| S1G Beacon Protection Text |
| Date: 2023-12-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Henry Ptasinski | Morse Micro |  |  | henry@e78com.com |
| David Goodall | Morse Micro |  |  | dave@morsemicro.com |
| David Halasz | Morse Micro |  |  | dave.halasz@ieee.org |

Abstract

Enhance broadcast/multicast integrity protocol (BIP) to support protection of S1G Beacon frames.

This addresses SB1 CID 6054.

R0: Initial draft

R1: Fix test vector labels

R2: Switch to RSN element bit 12

R3: Update abstract

R4: Fix doc header, fix figure 12-24 and 12-24a labeling, fix dot11BIPCompactEncapsulation definition and usage, misc. editorial

R5: Revise changes to Clause 12.5.3.2

R6: Revise changes to Clause 12.5.3.2

R7: Revise changes to Clause 12.5.3.2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 6054 | 11.52 | 2784 | 31 | There is no beacon protection for the S1G beacon, which is an extension frame. | Add protection to the S1G beacon. |

***Proposed resolution for CID 6054:***

Accepted. Request the REVme Editor to apply the changes below:

3.2 Definitions specific to IEEE Std 802.11

***Change the following definition as shown:***

**medium access control (MAC) management protocol data unit:** [MMPDU] The unit of data exchanged between two peer MAC entities, using services of the physical layer (PHY), to implement the MAC management protocol. The MMPDU is transported in one or more Management frames. The MMPDU might include a Mesh Control field, ~~or~~a management message integrity code (MIC) element (MME), or a MIC element, but does not include a MAC header, a frame check sequence (FCS), or any other security encapsulation overhead.

3.4 Acronyms and abbreviations

***Add the following acrynym in alphabetical order:***

BCE broadcast/multicast integrity protocol (BIP) compact encapsulation

6.5.14.1 MLME-SETKEYS.request

6.5.14.1.2 Semantics of the service primitive

**Add the following parameter to the end of the parameter table:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| Encapsulation Mode | Enumeration | Normal, BCE | This parameter is valid only when the Key Type value is BIGTK. |

6.5.14.1.4 Effect of receipt

**Change the last bullet as shown:**

— When the Key Type parameter is Pairwise or PeerKey, and the Key, Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize the transmitter TSC/PN counter and the receiver replay counter(s) to 0. When the Key Type parameter is not Pairwise, ~~or~~ PeerKey, or BIGTK, and the Key, Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the traffic, the transmitter TSC/PN/IPN/ ~~BIPN/~~WIPN counter to 0 or 1 (see Clause 12 (Security) and Clause 29 (Wake-Up Radio (WUR) MAC specification)) or the receiver replay counter(s) to the value in the Receive Sequence Count parameter. When the Key Type parameter is BIGTK, and the Key and Key ID parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the traffic, the transmitter BIPN counter as specified in 12.5.3.4 (BIP replay counters and packet numbers) or the receiver replay counter to the value in the Receive Sequence Count parameter. When the Key Type, Key, Key ID, and Address (where valid) parameters identify an existing key, the MAC shall not change the transmitter TSC/PN/IPN/BIPN/WIPN counter or the receiver replay counter(s) associated with that key.

9.3.4.3 S1G Beacon frame format

***Change the last two entries in Table 9-80—Minimum and full set of optional elements, and add a new last entry as shown:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Last–~~1~~2 | One or more elements can appear in this frame. | Optionally, element(s) that are not listed in this table, but are allowed in Beacon frame, in the order they appear in the Beacon frame (seeTable 9-60 (Beacon frame body)). | No | Yes |
| Last-1 | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. | No | Yes |
| Last | MME or MIC element | The MIC element is present if dot11BIPCompactEncapsulation is true.The MME is present if dot11BIPCompactEncapsulation is false and dot11BeaconProtectionEnabled is true.Otherwise neither is present. | Yes | Yes |

9.4.2.23 RSNE

9.4.2.23.4 RSN capabilities

***Change B12 in Figure 9-345 from “Reserved” to “BIP Compact Encapsulation/Reserved”***

***Change the last line of the clause as shown:***

— Bit 12: BIP Compact Encapsulation/Reserved. An S1G AP sets this bit to 1 to indicate that it supports transmission of S1G Beacon frames protected using BCE and, if bit 7 (MFPC) is set to 1, that S1G Beacons will be protected using BCE. An S1G non-AP STA sets this bit to 1 to indicate that it supports reception of S1G Beacon frames protected using BCE. For non-S1G STAs, this bit is reserved.

9.4.2.53 MME

***Change the first paragraph as shown:***

The management MIC element (MME) provides message integrity and protects group addressed robust Management frames and protected Beacon frames which are not protected with BCE from forgery and replay. Figure 9-443 (MME format) shows the MME format.

9.4.2.195 S1G Beacon Compatibility element

**Change the third paragraph as shown and add the NOTE:**

The Compatibility Information field contains all the subfields defined in 9.4.1.4 (Capability Information field) except for the subfields located in B6 and B7 of the field.~~, which~~B6 is defined as the TSF Rollover Flag subfield. An S1G AP sets the TSF Rollover Flag subfield to the value of the most significant bit of the 4 least significant octets of the TSF timer at the time the TSF timer is read for the purpose of creating the element carrying the Compatibility Information field. B7 is defined as the BIGTK Key ID Index subfield. When the S1G Beacon frame is protected with BCE, the S1G AP sets the field to 0 when the key ID used to protect the frame is 6, and sets the field to 1 when the key ID used to protect the frame is 7, i.e. *BIGTK Key ID Index = key ID + 6.*

Note 1: Valid values for the BIGTK Key ID are 6 or 7 (see 6.5.14.1 (MLME-SETKEYS.request)).

12.5.3.1 BIP overview

***Change the first paragraph as shown:***

BIP provides data integrity and replay protection for group addressed robust Management frames after establishment of an IGTKSA (see 12.6.1.1.9 (IGTKSA)) ~~and f~~. For non-S1G STAs, BIP provides data integrity and replay protection for Beacon frames after establishment of a BIGTKSA (see 12.6.1.1.11 (BIGTKSA)). For S1G STAs, BIP provides data integrity and replay protection for S1G Beacon frames after establishment of a BIGTKSA (see 12.6.1.1.11 (BIGTKSA)). BIP also provides integrity and replay protection for individually addressed and group addressed WUR frames (see 29.10 (WUR frame protection)).

***Change the last paragraph as shown:***

BIP uses the IGTK or BIGTK to compute the MMPDU MIC, uses the WTK to compute the MIC for protecting individually addressed WUR Wake-up frames, and uses the WIGTK to compute the MIC for protecting broadcast or group addressed WUR Wake-up frames. The Authenticator shall, if management frame protection is negotiated, distribute one new IGTK and IGTK PN (IPN) whenever it distributes a new GTK. The IGTK is identified by the MAC address of the transmitting STA plus an IGTK key ID that is encoded in the MME Key ID field. If beacon protection is enabled, the Authenticator may distribute one new BIGTK and BIPN when it distributes a new GTK. The BIGTK is identified by the MAC address of the transmitting STA plus:

* a BIGTK key ID that is encoded in the S1G Beacon Compatibility element, in S1G Beacon frames that use BCE or
* a BIGTK key ID that is encoded in the MME Key ID field~~.~~, in Beacon frames and S1G Beacon frames that do not use BCE.

If WUR frame protection is negotiated, the Authenticator may distribute one new WIGTK and WIPN when it distributes a new GTK. The WIGTK is identified by the MAC address of the transmitting STA plus the WIGTK key ID that is encoded in the Key ID field (see Figure 12-47 (WIGTK KDE format), Figure 9-1231 (Miscellaneous subfield format), 9.4.2.295 (WUR PN Update element) and 9.4.2.46 (FTE)) .

***Change clause 12.5.3.2 as shown:***

12.5.3.2 BIP ~~MMPDU~~encapsulation format

The MME shall follow all of the other elements in the management frame body but precede the FCS. See 9.4.2.53 (MME) for the format of the MME. The frame format for a protected Management frame is shown in Figure 12-23 (BIP encapsulation) ~~shows the BIP MMPDU~~.

|  |  |  |
| --- | --- | --- |
| ~~IEEE 802.11 H~~MAC header | Management ~~F~~frame ~~B~~body with MME as last element | FCS |
| Figure 12-23—BIP encapsulation |

For S1G Beacon frames using BCE, the MIC element shall follow all of the other elements in the frame body but precede the FCS. See 9.4.2.117 (MIC element) for the format of the MIC element. The frame format for an S1G Beacon frame using BCE is shown in Figure 12-23a (BIP compact encapsulation).

|  |  |  |
| --- | --- | --- |
| MAC header | S1G Beacon frame body with MIC element as last element | FCS |
| Figure 12-23a—BIP compact encapsulation |

12.5.3.3 BIP AAD construction

***Change the text as shown:***

For MPDUs that are not S1G Beacon frames, ~~T~~he BIP Additional Authentication Data (AAD) is constructed from the MPDU header. AAD construction is performed as follows:

1. FC—MPDU Frame Control field, with:
	1. Retry subfield (bit 11) masked out
	2. Power Management subfield (bit 12) masked out
	3. More Data subfield (bit 13) masked out
	4. No modifications to other subfields
2. A1—MPDU Address 1 field.
3. A2—MPDU Address 2 field.
4. A3—MPDU Address 3 field.

Figure 12-24 (BIP AAD construction) depicts the format of the AAD. The length of the AAD is 20 octets.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | FC | A1 | A2 | A3 |
| Octets: | 2 | 6 | 6 | 6 |
| Figure 12-24—BIP AAD construction |

For S1G Beacon frames when BCE is not in use, the BIP Additional Authentication Data (AAD) is constructed from the MPDU header. AAD construction is performed as follows:

1. FC—MPDU Frame Control field.
2. SA—address of the STA transmitting the S1G Beacon frame.
3. Change Sequence.
4. Next TBTT (if present).
5. Compressed SSID (if present).
6. Access Network Options (if present).

NOTE 1: S1G APs with dot11APPMActivated equal to true may enter Power Save mode. To prevent disruption of BSS traffic by an attacker setting the AP PM subfield (bit 15) in modified beacons, the AP PM subfield in S1G Beacon frames is protected by inclusion in the AAD.

NOTE 2: The Frame Control field in S1G Beacons does not contain Retry or More Data subfields.

Figure 12-24a (BIP AAD construction for S1G Beacon frames without BCE) depicts the format of the AAD. The length of the AAD is 9-17 octets.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | FC | SA | Change Sequence | Next TBTT | Compressed SSID | Access Network Options |
| Octets: | 2 | 6 | 1 | 0 or 3 | 0 or 4 | 0 or 1 |
| Figure 12-24a—BIP AAD construction for S1G Beacon frames without BCE |

For S1G Beacon frames when BCE is in use, the BIP Additional Authentication Data (AAD) is constructed from the MPDU header and the BIPN. AAD construction is performed as follows:

1. FC—MPDU Frame Control field.
2. SA—address of the STA transmitting the S1G Beacon frame.
3. Change Sequence.
4. Next TBTT (if present).
5. Compressed SSID (if present).
6. Access Network Options (if present).
7. BIPN.

Figure 12-24b (BIP AAD construction for S1G Beacon frames with BCE) depicts the format of the AAD. The length of the AAD is 15-23 octets.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | FC | SA | Change Sequence | Next TBTT | Compressed SSID | Access Network Options | BIPN |
| Octets: | 2 | 6 | 1 | 0 or 3 | 0 or 4 | 0 or 1 | 6 |
| Figure 12-24b—BIP AAD construction for S1G Beacon frames with BCE |

12.5.3.4 BIP replay counters and packet numbers

***Change the second paragraph as shown:***

When beacon protection is enabled at the non-~~S~~AP STA, the receiver shall maintain a 48-bit replay counter for each BIGTK. The receiver shall set the replay counter to the value of the BIPN in the BIGTK key data encapsulation (KDE) (see 12.7.2 (EAPOL-Key frames)) provided by the Authenticator in the 4-way handshake, FT 4-way handshake, FT handshake, group key handshake, or FILS authentication. The transmitter shall maintain a single BIPN for each BIGTK. When beacon protection is enabled at an S1G AP and BCE is enabled, the BIPN shall be implemented as a 48-bit representation of the number of TSBTTs or TBTTs since TSF time 0. If dot11ShortBeaconInterval is true, the BIPN shall be initialized using Equation (12-0a):

 BIPN = Floor*(TSF* / (1024 × *dot11ShortBeaconPeriod*)) (12-0a)

If dot11ShortBeaconInterval is false, the BIPN shall be initialized using Equation (12-0b):

 BIPN = Floor*(TSF* / (1024 × *dot11BeaconPeriod*)) (12-0b)

When adding protection to, or checking protection on, an S1G Beacon frame, if dot11ShortBeaconInterval is true, the BIPN shall be calculated using Equation (12-0c):

 BIPN = *CurrentTSBTT* / (1024 × *dot11ShortBeaconPeriod*) (12-0c)

where

 *CurrentTSBTT* is the TSBTT of the S1G Beacon frame that is being protected, in µs.

When adding protection to, or checking protection on, an S1G Beacon frame, if dot11ShortBeaconInterval is false, the BIPN shall be calculated using Equation (12-0d):

 BIPN = *CurrentTBTT* / (1024 × *dot11BeaconPeriod*) (12-0d)

where

 *CurrentTBTT* is the TBTT of the S1G Beacon frame that is being protected, in µs.

NOTE 1: Calculation of CurrentTBTT or CurrentTSBTT is implementation dependent. One possible implementation is the transmitter could use Ceil(TSF/(1024 x dot11ShortBeaconPeriod)) and Ceil(TSF/(1024 x dot11BeaconPeriod)), and the receiver could use Floor(TSF/(1024 x dot11ShortBeaconPeriod)) and Floor(TSF/(1024 x dot11BeaconPeriod)).

When beacon protection is enabled at an S1G AP and BCE is disabled, the BIPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding BIGTK is initialized. For non-S1G STAs, t~~T~~he BIPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding BIGTK is initialized.

***Change NOTE 1 as shown and renumber subsequent NOTEs:***

NOTE ~~1~~2—When the IPN ~~or BIPN~~ space is exhausted, the choices available to an implementation are to replace the corresponding key or to end communications. When the BIPN space is exhausted and BCE is not in use, the choices available to an implementation are to replace the corresponding key or to end communications. When the BIPN space is exhausted and BCE is in use, the choices available to an implementation are to replace the corresponding key and reset the TSF to 0 or to end communications (and the AP may restart the BSS).

12.5.3.5 BIP transmission

***Change the first paragraph as shown:***

When a STA transmits a protected group addressed robust Management frame that is not an S1G Beacon using BCE, it shall:

1. Select the IGTK or BIGTK currently active for transmission of frames to the intended group of receivers and construct the MME (see 9.4.2.53 (MME)) with the MIC field masked out and the Key ID field set to the corresponding IGTK key ID. If the frame is not a GQMF, the transmitting STA shall insert a strictly increasing integer into the MME IPN/BIPN field. If the frame is a GQMF, then the transmitting STA shall maintain a 48-bit counter for use as the IPN, the counter shall be incremented for each GQMF until the two least significant bits of the counter match the ACI of the AC that is used to transmit the frame, and the counter value shall be inserted into the MME IPN/BIPN field of the frame. For BIP-GMAC-128 and BIP-GMAC-256, the initialization vector passed to GMAC shall be ~~a concatenation of Address 2 from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.~~:
	1. For S1G Beacons: a concatenation of the SA field from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.
	2. For all other frames: a concatenation of Address 2 from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.

NOTE 1—QMF is not supported for PV1 Management frames (see 11.24.1.1 (Overview)).

1. Compute AAD as specified in 12.5.3.3 (BIP AAD construction).
2. Compute an integrity value over the concatenation of AAD and the management frame body including MME, ~~and the Timestamp field masked out if it is a protected Beacon frame, and insert~~with:
	1. For protected Beacon frames: the Timestamp field masked out.
	2. For S1G Beacon Frames: the TSF Completion field of the S1G Beacon Compatibility element masked out, if the element is present.

Insert the output into the MME MIC field. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC.

1. Compose the frame as the ~~IEEE 802.11~~MAC header, management frame body, including MME, and FCS. The MME shall appear last in the frame body.
2. Transmit the frame.

When an S1G STA transmits a protected S1G Beacon frame using BCE, it shall:

1. Select the BIGTK currently active for transmission of frames to the intended group of receivers.
2. Set the BIGTK Key ID Index subfield in the S1G Beacon Compatibility element, if present, to the value that corresponds to the BIGTK key ID (see 9.4.2.195 (S1G Beacon Compatibility element)). If the S1G Beacon Compatibility element is not present, the BIGTK used to protect the frame shall be the same BIGTK used in the most recently transmitted protected S1G Beacon frame that contained an S1G Beacon Compatibility element. If that BIGTK is not available for use, or no previous protected S1G Beacon frame containing an S1G Beacon Compatibility element has been transmitted, then the frame shall be sent without BIP encapsulation.
3. Construct the MIC element (see 9.4.2.117 (MIC element)) with the MIC field masked out.
4. Derive the BIPN using Equation (12-0c) if dot11ShortBeaconInterval is true, or Equation (12-0d) if dot11ShortBeaconInterval is false. For BIP-GMAC-128 and BIP-GMAC-256, the initialization vector passed to GMAC shall be a concatenation of the SA field from the MAC header of the MPDU and the BIPN.
5. Compute AAD as specified in 12.5.3.3 (BIP AAD construction).
6. Compute an integrity value over the concatenation of AAD and the management frame body including MIC element, with the TSF Completion field of the S1G Beacon Compatibility element masked out if the element is present.
7. Insert the output into the MIC field of the MIC element. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC.
8. Compose the frame as the MAC header, management frame body, including MIC element, and FCS. The MIC element shall appear last in the frame body.
9. Transmit the frame.

***Change the last paragraph as shown:***

Once a STA transmits a protected Beacon frame or a protected S1G Beacon frame using a new BIGTK, the STA shall not transmit protected Beacon frames or protected S1G Beacon frames using the previous BIGTK. Once a STA transmits a protected group addressed robust Management frame using a new IGTK, the STA shall not transmit protected group addressed robust Management frames using the previously used IGTK.

12.5.3.6 BIP reception

***Change the text as shown:***

When a STA with management frame protection negotiated receives a group addressed robust Management frame ~~or~~, a protected Beacon frame, or a protected S1G Beacon frame that is not using BCE~~protected by BIP-CMAC-128, BIP-CMAC-256, BIP-GMAC-128, or BIP-GMAC-256~~, it shall

1. Identify the appropriate IGTK or BIGTK and associated state based on the MME Key ID field. If the frame is a robust Management frame and no such IGTK exists, silently discard the frame and terminate BIP processing for this reception. If the frame is a protected S1G Beacon frame, and the Encapsulation Mode for the key is BCE, the receiver shall silently discard the frame and and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure. If the frame is a protected Beacon frame and no such BIGTK exists, terminate BIP processing for this reception, and
	1. If beacon protection is enabled at the non-AP STA, silently discard the frame and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure.
	2. Otherwise, process the frame.
2. Perform replay protection on the received frame. The receiver shall interpret the MME IPN/BIPN field as a 48-bit unsigned integer.
	1. If the frame is a robust Management frame but not a GQMF, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the IGTK identified by the MME Key ID field. If the value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this IGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

NOTE 1—QMF is not supported for PV1 Management frames (see 11.24.1.1 (Overview)).

* 1. If the frame is a robust Management frame and also a GQMF, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame. If the value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this IGTK and AC, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.
	2. If the frame is a protected Beacon frame or a protected S1G Beacon frame, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the BIGTK identified by the MME Key ID field. If the integer value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this BIGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.
1. Compute AAD for this Management frame, as specified in 12.5.3.3 (BIP AAD construction). For BIP-GMAC-128 and BIP-GMAC-256, an initialization vector for GMAC is constructed as: ~~the concatenation of Address 2 from the MAC header of the MPDU and the 48-bit unsigned integer from the MME IPN/BIPN field.~~
	1. For S1G Beacons: a concatenation of the SA field from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.
	2. For all other frames: a concatenation of Address 2 from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.
2. Extract and save the received MIC value, and compute a verifier over the concatenation of AAD, the management frame body, with: ~~the Timestamp field masked out if it is a protected Beacon frame,~~
	1. For protected Beacon frames: the Timestamp field masked out
	2. For S1G Beacon Frames: the TSF Completion field of the S1G Beacon Compatibility element masked out if the element is present,

and MME, with the MIC field masked out in the MME. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC. If the result does not match the received MIC value, then the receiver shall discard the frame, increment the dot11RSNAStatsBIPMICErrors counter by 1, and terminate BIP processing for this reception.

1. If the frame is a robust Management frame but not a GQMF, update the replay counter for the IGTK identified by the MME Key ID field with the value of the MME IPN/BIPN field.
2. If the frame is a robust Management frame and also a GQMF, update the replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame with the value of the MME IPN/BIPN field.
3. If the frame is a protected Beacon frame or a protected S1G Beacon frame, update the replay counter for the BIGTK identified by the MME Key ID field with the value of the MME IPN/BIPN field.

When an S1G STA with management frame protection negotiated receives a protected S1G Beacon frame that is using BCE, it shall

1. Identify the appropriate BIGTK and associated state based on the BIGTK Key ID Index subfield in the S1G Beacon Compatibility element, if present (see 9.4.2.195 (S1G Beacon Compatibility element)). If the S1G Beacon Compatibility element is not present, the BIGTK used to check the frame shall be the same BIGTK used in the most recently received protected S1G Beacon frame that contained an S1G Beacon Compatibility element. If the Encapsulation Mode for the key is Normal, the receiver shall silently discard the frame and and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure.
2. If no such BIGTK exists, terminate BIP processing for this reception, and
	1. If beacon protection is enabled at the non-AP STA, silently discard the frame and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure.
	2. Otherwise, process the frame.
3. Derive the BIPN using Equation (12-0c) if dot11ShortBeaconInterval is true, or Equation (12-0d) if dot11ShortBeaconInterval is false. For BIP-GMAC-128 and BIP-GMAC-256, the initialization vector passed to GMAC shall be a concatenation of the SA field from the MAC header of the MPDU and the BIPN.
4. Perform replay protection on the received frame. The receiver shall compare the derived BIPN to the value of the replay counter for the identified BIGTK. If the integer value from the derived BIPN is less than or equal to the replay counter value for this BIGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

NOTE 2: A STA should synchronize to the TSF prior to processing the first protected S1G Beacon frame using BCE.

1. Compute AAD for this Management frame, as specified in 12.5.3.3 (BIP AAD construction).
2. Extract and save the received MIC value, and compute a verifier over the concatenation of AAD, the management frame body, with the TSF Completion field of the S1G Beacon Compatibility element masked out if the element is present, and MIC element, with the MIC field masked out in the MIC element. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC. If the result does not match the received MIC value, then the receiver shall discard the frame, increment the dot11RSNAStatsBIPMICErrors counter by 1, and terminate BIP processing for this reception.

12.6.21 Protection of Beacon frames

***Change the first paragraph as shown:***

An AP shall transmit protected Beacon frames if beacon protection is enabled. Protected Beacon frames cannot be validated until a BIGTKSA has been established. If a BIGTKSA exists, the non-AP STA shall validate the MME or MIC element in received Beacon frames.

12.7.2 EAPOL-Key frames

***Change the BIGTK KDE description as shown:***

The Key ID field contains the BIGTK key ID.

The BIPN field contains the BIPN that was ~~carried in the MME of~~used to protect the last protected Beacon frame and it is used by the receiver as the initial value for the BIP replay counter for the BIGTK.

The BIGTK field contains the BIGTK.

B.4.4.1 MAC protocol capabilities

***Add two new entries to the MAC Protocol Capabilities table as shown:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \*PC34.1.10 | Management frame protection | 9.2.4.1.10 (+HTC subfield), 9.4.1.11 (Action field), 9.4.2.23.4 (RSN capabilities), 9.6.3 (QoS Action frame details), 12.3.4.1.2 (TKIP cryptographic encapsulation), 12.3.4.1.3 (TKIP decapsulation), 12.3.4.2 (TKIP MPDU formats), 12.5.2.3.3 (Construct AAD), 12.5.2.3.7 (CCM originator processing), 12.5.2.4.2 (CCM recipient processing), 12.5.2.4.4 (PN and replay detection), 12.5.4.4.4 (PN and replay detection), 12.6.3 (RSNA policy selection in an infrastructure BSS) | PC34:O | Yes o No o N/A o |
| \*PC34.1.10.1 | BIP | Clause 11 (MLME), 12.5.3 (Broadcast/multicast integrity protocol (BIP)) | PC34.1.10:M | Yes o No o N/A o |
| PC34.1.10.1.1 | MME | 9.4.2.53 (MME) | PC34.1.10.1:M | Yes o No o N/A o |
| PC 34.1.10.1.2 | Beacon protection | 11.52 (Beacon frame protection procedures); 12.6.21 (Protection of Beacon frames) | PC34.1.10.1 AND (CFAP OR CFSTAofAP):O | Yes o No o N/A o |
| PC 34.1.10.1.2.1 | BIP compact encapsulation | 12.5.3 Broadcast/multicast integrity protocol (BIP) | PC 34.1.10.1.2 AND CFS1G: O | Yes o No o N/A o |
| PC 34.1.10.1.2.1.1 | MIC element | 9.4.2.117 (MIC element) | PC 34.1.10.1.2.1: M | Yes o No o N/A o |
| PC34.1.11 | AKM: IEEE 802.1X authentication with SHA-256 PRF | 9.4.2.23 (RSNE), 12.7 (Keys and key distribution) | PC34:O | Yes o No o N/A o |
| PC34.1.12 | AKM: PSK with SHA-256 PRF | 9.4.2.23 (RSNE), 12.7 (Keys and key distribution) | PC34:O | Yes o No o N/A o |

C.3 MIB detail

**Change the Dot11S1GStationConfigEntry SEQUENCE as shown:**

 dot11S1GDACTImin Unsigned32,

 dot11S1GDACTImax Unsigned32,

 dot11ProtectedTWTOperationsImplemented TruthValue,

 dot11ExtendedS1GActionProtectionOperationsImplemented TruthValue,

 dot11BIPCompactEncapsulation TruthValue

 }

**Add the following new entry at the end of dot11S1GStationConfigTable TABLE:**

dot11BIPCompactEncapsulation OBJECT-TYPE

 SYNTAX TruthValue

 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 attribute, when true indicates the station supports the use of BIP compact encapsulation of protected S1G Beacon frames. The attribute is set to true only if dot11BeaconProtectionEnabled is true."

 DEFVAL { false }

 ::= { dot11S1GStationConfigEntry 59 }

***Add a new subclause after J.9.1, and renumber the following subclause(s):***

J.9.2 BIP with S1G Beacon Frames

==== S1G Beacon frame with BIP-CMAC-128, no optional header fields, S1G Beacon Compatibility element in body ====

Unprotected S1G Beacon frame (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-CMAC-128 AAD|Body(masked): 1c 40 02 00 00 00 00 00 00 d5 08 80 00 00 00 00 00 00 00 4c 10 07 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-CMAC-128 MIC: 6b f6 47 29 3f 14 5b bc

Protected MPDU (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78 4c 10 07 00 04 00 00 00 00 00 6b f6 47 29 3f 14 5b bc

==== S1G Beacon frame with BIP-CMAC-128, all optional header fields, no body elements ====

Unprotected S1G Beacon frame (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-CMAC-128 AAD|Body(masked): 1c 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 10 06 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-CMAC-128 MIC: 3c 58 b6 bd 3b da 56 c3

Protected MPDU (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 10 06 00 04 00 00 00 00 00 3c 58 b6 bd 3b da 56 c3

==== S1G Beacon frame with BIP-CMAC-128 using BCE, no optional header fields, S1G Beacon Compatibility element in body ====

Unprotected S1G Beacon frame (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-CMAC-128 AAD|Body(masked): 1c 40 02 00 00 00 00 00 00 04 00 00 00 00 00 d5 08 80 00 00 00 00 00 00 00 8c 08 00 00 00 00 00 00 00 00

S1G BIP-CMAC-128 MIC: bf d5 09 15 39 04 ef 3c

Protected MPDU (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78 8c 08 bf d5 09 15 39 04 ef 3c

==== S1G Beacon frame with BIP-CMAC-128 using BCE, all optional header fields, no body elements ====

Unprotected S1G Beacon frame (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-CMAC-128 AAD|Body(masked): 1c 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 8c 08 00 00 00 00 00 00 00 00

S1G BIP-CMAC-128 MIC: c1 1e d2 f4 23 34 40 15

Protected MPDU (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8c 08 c1 1e d2 f4 23 34 40 15

==== S1G Beacon frame with BIP-GMAC-128, no optional header fields, S1G Beacon Compatibility element in body ====

Unprotected S1G Beacon frame (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 00 00 00 00 12 34 56 78

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-128 AAD|Body(masked): 1c 40 02 00 00 00 00 00 00 d5 08 00 00 00 00 00 00 00 00 4c 18 06 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-128 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-128 MIC: a5 b2 42 c1 c1 1e ab 10 c5 a4 e8 b9 53 66 19 38

Protected MPDU (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 00 00 00 00 12 34 56 78 4c 18 06 00 04 00 00 00 00 00 a5 b2 42 c1 c1 1e ab 10 c5 a4 e8 b9 53 66 19 38

==== S1G Beacon frame with BIP-GMAC-128, all optional header fields, no body elements ====

Unprotected S1G Beacon frame (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-128 AAD|Body(masked): 1c 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 18 07 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-128 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-128 MIC: 39 d0 0c c2 ee d7 4c 2a b7 41 cc f8 08 9b 5b 08

Protected MPDU (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 18 07 00 04 00 00 00 00 00 39 d0 0c c2 ee d7 4c 2a b7 41 cc f8 08 9b 5b 08

==== S1G Beacon frame with BIP-GMAC-128 using BCE, no optional header fields, S1G Beacon Compatibility element in body ====

Unprotected S1G Beacon frame (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 00 00 00 00 12 34 56 78

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-128 AAD|Body(masked): 1c 40 02 00 00 00 00 00 00 04 00 00 00 00 00 d5 08 00 00 00 00 00 00 00 00 8c 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-128 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-128 MIC: a2 5b 7e 67 76 f0 11 57 a4 fb 4a 2d 66 d0 17 66

Protected MPDU (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 00 00 00 00 12 34 56 78 8c 10 a2 5b 7e 67 76 f0 11 57 a4 fb 4a 2d 66 d0 17 66

==== S1G Beacon frame with BIP-GMAC-128 using BCE, all optional header fields, no body elements ====

Unprotected S1G Beacon frame (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-128 AAD|Body(masked): 1c 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 8c 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-128 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-128 MIC: 86 dd b6 c0 56 21 30 9d 3e bd 25 96 67 5b dd c3

Protected MPDU (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8c 10 86 dd b6 c0 56 21 30 9d 3e bd 25 96 67 5b dd c3

==== S1G Beacon frame with BIP-GMAC-256, no optional header fields, S1G Beacon Compatibility element in body ====

Unprotected S1G Beacon frame (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-256 AAD|Body(masked): 1c 40 02 00 00 00 00 00 00 d5 08 80 00 00 00 00 00 00 00 4c 18 07 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-256 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-256 MIC: 33 a2 6f c6 7e bf fd a0 ac 9b 29 aa 70 da 3f 51

Protected MPDU (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78 4c 18 07 00 04 00 00 00 00 00 33 a2 6f c6 7e bf fd a0 ac 9b 29 aa 70 da 3f 51

==== S1G Beacon frame with BIP-GMAC-256, all optional header fields, no body elements ====

Unprotected S1G Beacon frame (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-256 AAD|Body(masked): 1c 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 18 06 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-256 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-256 MIC: 0a 5f a0 f4 71 df 73 9e 61 4d cf 5d bb 36 f9 65

Protected MPDU (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 18 06 00 04 00 00 00 00 00 0a 5f a0 f4 71 df 73 9e 61 4d cf 5d bb 36 f9 65

==== S1G Beacon frame with BIP-GMAC-256 using BCE, no optional header fields, S1G Beacon Compatibility element in body ====

Unprotected S1G Beacon frame (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-256 AAD|Body(masked): 1c 40 02 00 00 00 00 00 00 04 00 00 00 00 00 d5 08 80 00 00 00 00 00 00 00 8c 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-256 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-256 MIC: f8 76 22 80 3d 9c 22 8a cb 3c 55 8a 33 2e 94 13

Protected MPDU (without FCS): 1c 40 00 00 02 00 00 00 00 00 00 00 00 00 00 d5 08 80 00 00 00 12 34 56 78 8c 10 f8 76 22 80 3d 9c 22 8a cb 3c 55 8a 33 2e 94 13

==== S1G Beacon frame with BIP-GMAC-256 using BCE, all optional header fields, no body elements ====

Unprotected S1G Beacon frame (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

BIGTK: 4e a9 54 3e 09 cf 2b 1e ca 66 ff c5 8b de cb cf 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

BIPN: 04 00 00 00 00 00

S1G BIP-GMAC-256 AAD|Body(masked): 1c 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 8c 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

S1G BIP-GMAC-256 Nonce: 02 00 00 00 00 00 00 00 00 00 00 04

S1G BIP-GMAC-256 MIC: 3c 80 49 be 8c 23 34 1f 5c 2f 9c d6 03 e3 7a 5b

Protected MPDU (without FCS): 1c 47 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8c 10 3c 80 49 be 8c 23 34 1f 5c 2f 9c d6 03 e3 7a 5b

**References:**

[**Draft P80211REVme\_D4.1.pdf**](https://grouper.ieee.org/groups/802/11/private/Draft_Standards/11me/Draft%20P802.11REVme_D4.0.pdf)