IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11bc LB 252 resolution for CIDs assigned to Abhi (part 3) |
| Date: April 8, 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com |
| George Cherian |  |  |  |
| Jouni Malinen |  |  |  |
| Mark Rison | Samsung |  |  |  |
| Stephen McCann | Huawei |  |  |  |

 Abstract

This submission proposes resolutions for the following 26 comments submitted during LB 252 for 11bc D1.0:

1087, 1088, 1044, 1554, 1268, 1601, 1441, 1323, 1408, 1260, 1324, 1322, 1320, 1583, 1326, 1328, 1331, 1334, 1165, 1336, 1335, 1337, 1418, 1352, 1034, 1357

Revisions:

* Rev 0: Initial version of the document.
* Rev 1:
	+ Revised based on feedback from Mark Rison and Stephen McCann. Added as co­-authors
	+ Added several CIDs from clause 11 which were getting resolved anyways!

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 TGbc Draft. This introduction is not part of the adopted material.

***TGbc Editor: Editing instructions preceded by “TGbc Editor” are instructions to the TGbc editor to modify existing material in the TGbc draft. As a result of adopting the changes, the TGbc editor will execute the instructions rather than copy them to the TGbc Draft.***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 1087 | Bahareh Sadeghi | 25.00 | 7 | 9.4.2.300.2 | How is the STA is expected to use whether AP does authenticate or not... the STAs are pre-fixed on that behavior and will transmit anyways? | Add clarification -probably in clause 11- how the information about whether the AP authenticates are not may be used by the STA. | **Revised**Agree with the commenter. A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP. Such a proxy provides relaying service in which it evaluates certain criteria before relaying the contents of the HLP payload to the specified destination. The description includes discussion on performing source authentication based on client certificate signed by an entity at the specified destination. Text in clause 9 was updated to remove the field related to authentication mode from EBCS Parameter element and the structure of the element was simplified. A bit was added to Extended Capabilities element to signal if the EBCS AP is affiliated with an EBCS proxy that provides relaying service. The cited table in clause 9 was deleted and text in clause 11 was updated accordingly.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1087** |
| 1088 | Bahareh Sadeghi | 25.00 | 13 | 9.4.2.300.2 | what is the benefit of advertising this information by the AP? Whether the STA knows about throttling or not cannot impact its behavior | Please add clarification -probably in clause 11- how the information of whether the AP throttles or not is expected to or may impact STA behavior. | **Revised**Agree with the commenter. A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service. An EBCS proxy may limit the number of HLP payload it relays to the specified destination based on local policies or based on relationship with the specified destination. Advertising such information provides little value as the non-AP STA is not required to scan the WM before it transmits an EBCS UL frame (i.e., it is likely that the STA is a transmit only device). Text in clause 9 was updated to remove the field related to limiting mode from EBCS Parameter element and the structure of the element was simplified. The cited table in clause 9 was deleted and text in clause 11 was updated accordingly.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1088** |
| 1044 | Albert Petrick | 25.00 | 13 | 9.4.2.300.2 | In Table 9-bc2 for Subfield value equal to zero the Encoding column reads "allows a fix amount or frequency of uplink data..." this sentence is ambiguous. Does the frequency refer to the data rate or frequency band? | Remove ambiguity as commented | **Revised**The cited table in clause 9 was deleted as a resolution to another comment (CID 1088). A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service. Such a proxy may limit the number of HLP payload it relays to the specified destination based on local policies or based on relationship with the specified destination.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1044** |
| 1554 | Tomoko Adachi | 25.00 | 13 | 9.4.2.300.2 | "AP applies no restrictions or allows a fixed amount or frequency of uplink data from a non-AP STA to be forwarded to a remote destination." The first part looks as though there is no restriction on uplink data while the second part seems to say the amount or frequency of uplink data is fixed and there is contradiction. Looking from the definition name and the next definition and its encoding, should this just say that the AP applies no restriction to remote destinations when forwarding uplink data? | Please clarify. | **Revised**The cited table in clause 9 was deleted as a resolution to another comment (CID 1088). A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service. Such a proxy may limit the number of HLP payload it relays to the specified destination based on local policies or based on relationship with the specified destination.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1554** |
| 1268 | Mark RISON | 25.00 | 15 | 9.4.2.300.2 | "such as 15location, date/time, etc. based on the relationship with the remote destination" is not clear. How can a location or data/time be based on some relationship? | Delete "based on the relationship with the remote destination" from the cited text | **Revised**A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service.An EBCS proxy that supports relaying of HLP payload to a specified destination is expected to have a relationship with an entity at the specified destination. Based on the agreement, the proxy will embed information such as location, data/time etc, in the correct format before forwarding the HLP payload to the destination. Different destination may require the AP to embed different type of information in a specific format. This is out of scope of the TGbc standard. Text in clause 9 (9.4.2.300 (EBCS Parameters element) and 9.6.7.100 (EBCS UL frame)) was updated to remove any description and signaling related to appending metadata. Clause 11 was updated accordingly.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1268** |
| 1601 | Xiaofei Wang | 26.00 | 9 | 9.4.2.300.3 | it may be better to specify which metadata is included, particularly in the case when an AP just forward the data, without necessarily having agreements with remote server. | consider to add specifications which kind of metadata is reqeusted to be added. | **Revised**A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service.An EBCS proxy that supports relaying of HLP payload to a specified destination is expected to have a relationship with an entity at the specified destination. Based on the agreement, the proxy will embed information such as location, data/time etc, in the correct format before forwarding the HLP payload to the destination. Different destination may require the AP to embed different type of information in a specific format. This is out of scope of the TGbc standard. Text in clause 9 (9.4.2.300 (EBCS Parameters element) and 9.6.7.100 (EBCS UL frame)) was updated to remove any description and signaling related to appending metadata. Clause 11 was updated accordingly.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1601** |
| 1441 | Osama Aboulmagd | 26.00 | 5 | 9.4.2.300.3 | Figure 9-bc5 "Embedding What" | Define what is embedding and embedding what | **Revised**A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service.An EBCS proxy that supports relaying of HLP payload to a specified destination is expected to have a relationship with an entity at the specified destination. Based on the agreement, the proxy will embed information such as location, data/time etc, in the correct format before forwarding the HLP payload to the destination. Different destination may require the AP to embed different type of information in a specific format. This is out of scope of the TGbc standard. Text in clause 9 (9.4.2.300 (EBCS Parameters element) and 9.6.7.100 (EBCS UL frame)) was updated to remove any description and signaling related to appending metadata. Clause 11 was updated accordingly.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1441** |
| 1323 | Mark RISON | 54 | 26 | 11.100.3.1 | What if two APs forward, but one appends metadata and the other not? | As it says in the comment | **Revised**A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP and provides relaying service.An EBCS proxy that supports relaying of HLP payload to a specified destination is expected to have a relationship with an entity at the specified destination. Based on the agreement, the proxy will embed information such as location, data/time etc, in the correct format before forwarding the HLP payload to the destination. Different destination may require the AP to embed different type of information in a specific format. This is out of scope of the TGbc standard. Text in clause 9 (9.4.2.300 (EBCS Parameters element) and 9.6.7.100 (EBCS UL frame)) was updated to remove any description and signaling related to appending metadata. Clause 11 was updated accordingly.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1323** |
| 1408 | Michael Montemurro | 35.00 | 35 | 9.6.7.100 | I don't understand why the same eBCS action frame cannot be used for either an UL or a DL eBCS transmission. Since the traffic is proxied by the AP, the same frame can be used for either UL or DL. | Change "UL eBCS frame" to "eBCS frame" and adjust the requirements to allow the frame to be used for either DL or UL. | **Rejected**It is easier and cleaner to describe the operation with respect to a particular frame type and its content. |
| 1260 | Mark RISON |  |  | 9.4.2.300.1 | There are references to "the packet" but it is not clear what this is referring to | Change "the packet" to "a frame" at 24.8, "the packet" to "the frame" at 26.15, "packet" to "frame" at 37.12, 37.14, 55.24, 56.7 | **Revised**Most references to packet were fixed in D1.02. There wer two remaining references to ‘packet’. Both instances are fixed (a NOTE containing one of them is deleted while the other instance is fixed as EBCS UL frame).**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1260** |
| 1324 | Mark RISON | 54 | 26 | 11.100.3.1 | Per the previous sentence, >1 AP might forward | Change "forwarding AP" to "forwarding AP(s)" | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441, 1323). No further changes are needed to resolve this comment. |
| 1322 | Mark RISON | 54 | 26 | 11.100.3.1 | This is more of a "can", not a "may", here | As it says in the comment | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441, 1323). No further changes are needed to resolve this comment. |
| 1320 | Mark RISON | 54 | 29 | 11.100.3.1 | "embed metadata" is a new concept | Change to "append additional information" | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441). No further changes are needed to resolve this comment. |
| 1583 | Tomoko Adachi | 54 | 29 | 11.100.3.1 | "Furthermore, a STA's request to embed metadata might not be fulfilled by a forwarding AP." Can't it be more reliable? Say, if the AP declares the capability that it can embed metadata, the AP shall be responsible when the STA requests to do so. Or, is this covered in the third para in 11.100.3.2? If so, the sentence should be revisited to avoid misunderstanding. | As in comment. | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441). No further changes are needed to resolve this comment. |
| 1326 | Mark RISON | 55 | 1 | 11.100.3.2 | What is the difference between "supporting" a forwarding service and "providing" this service? Oh, and "ability to support [embedding]" at 55.7 is confusing too. Oh, and is "capable of embedding" different from supporting/providing? | As it says in the comment | **Revised**The cited sentences were either deleted or updated as a resolution to other CIDs (1087, 1088, 1044, 1544, 1268, 1601, 1441). A new sentence was added to say that an EBCS AP sets the EBCS Relaying Supported subfield of the Extended Capabilities element to 1 if it is affiliated with an EBCS proxy that provides relaying service.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1326** |
| 1328 | Mark RISON | 55 | 7 | 11.100.3.2 | As importantly, if an AP does not support metadata forwarding, the bit shall be set to 0 | As it says in the comment | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441). No further changes are needed to resolve this comment. |
| 1331 | Mark RISON | 55 | 18 | 11.100.3.2 | "Otherwise, the AP shall forward the frame to the remote destination identified in the frame." is obvious and isn't stated in similar contexts elsewhere. In addition, it contradicts the NOTE at the end of the subclause | Delete the cited text | **Revised**The cited sentence was deleted as a resolution to other CIDs and does not appear in D1.02. No further changes are needed to resolve this comment. |
| 1334 | Mark RISON | 55 | 21 | 11.100.3.2 | "should perform source authentication and validate the frame signature" -- surely the signature should always be checked? | Change to "should perform source authentication and shall validate the frame signature" | **Revised**The cited sentence was deleted as a resolution to another CID (1087). A new subclause was added to clause 4.5 to describe the behavior of an EBCS proxy that sits behind an EBCS AP. Such a proxy provides relaying service in which it evaluates certain criteria before relaying the contents of the HLP payload to the specified destination. The description includes discussion on performing source authentication based on client certificate signed by an entity at the specified destination. Clause 12.100.2.6 was updated to describe the authentication operation performed at the EBCS proxy.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1334** |
| 1165 | James Yee | 55 | 22 | 11.100.3.2 | It is not very reassuring to leave throttling of excessive forwarding to a simple 'should'. It is possible that an authenticated source can intentionally initiate a DoS attack, right? | Define a parameter to limit the frequency of forwarding or other stronger mechanism to protect against attacks. | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441). No further changes are needed to resolve this comment. |
| 1336 | Mark RISON | 55 | 22 | 11.100.3.2 | It is not clear how limiting the number of forwarded frames differs from limiting their frequency | As it says in the comment | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441). No further changes are needed to resolve this comment. |
| 1335 | Mark RISON | 55 | 29 | 11.100.3.2 | It is not clear why the Timestamp field is relevant here. And too many "or"s | Delete " or the Timestamp field" | **Revised**The cited NOTE was deleted as a resolution to other CIDs (1087, 1334). No further changes are needed to resolve this comment. |
| 1337 | Mark RISON | 55 |  | 11.100.3.2 | Even if one AP does rate-limiting, if there are lots of APs the aggregate could still overwhelm the remote destination | Add a mechanism so that only one AP actually forwards | **Revised**The cited sentence was deleted as a resolution to other CIDs (1268, 1601, 1441). No further changes are needed to resolve this comment. |
| 1418 | Michael Montemurro | 56 | 2 | 11.100.3.3 | Please use a standard format for a timestamp and provide a reference. | Pick a format from RFC 8877 and use the RFC as a reference. | **Revised**The name Timestamp was causing an ambiguity. The field was renamed to Replay Protection to avoid ambiguity with the commonly known field name. The change appears in D1.02. The Replay Protection field consists of a Time field and a Frame Count field. No further changes are needed to resolve this comment. |
| 1352 | Mark RISON | 56 | 6 | 11.100.3.3 | Should specify whether the Counter subfield is initialised to any value, and if so to what value and when | As it says in the comment | **Revised**Agree with the comment. The sentence was updated to clarify that the Frame Count subfield is initialize to 0 when the EBCS non-AP STA transmits the first EBCS UL frame and it is increment for each subsequent transmission of the frame.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1352** |
| 1034 | Abhishek Patil | 56 | 6 | 11.100.3.3 | The Counter subfield is 4-bits long and can carry up to 16 values. Therefore the calculation should be 2^16 | replace 2^32 with 2^16 | **Revised**The Frame Count subfield is 4 octets long and therefore 2^32 is accurate. Updated the description in clause 12.100.2.6 to provide more details for reducing the possibility of a replay attack.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1034** |
| 1357 | Mark RISON | 56 | 6 | 11.100.3.3 | "a numeric value which is incremented for each 6 packet transmission. When the STA has transmitted 2 32 - 1 frames" is imprecise. What is a "packet"? What kind of "frames"? | Change to "a numeric value which is incremented for each UL eBCS frametransmission. When the STA has transmitted 2 32 - 1 UL eBCS frames" | **Revised**Agree with the comment. The text was updated to clarify that the Frame Count subfield is increment for each transmission of an EBCS UL frame.**TGbc editor, please make changes as shown in <https://mentor.ieee.org/802.11/dcn/21/11-21-0305-01-00bc-lb252-resolutions-for-cids-assigned-to-abhi-part-3.docx> tagged as 1357** |

***TGbc Editor: The baseline for the proposed changes is 802.11bc D1.02***

**9.4.2.296 EBCS Parameters element**

***TGbc Editor: please make changes to this clause as shown below:***

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]An EBCS AP advertises its EBCS operational parameters in the EBCS Parameters element.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension |  | EBCS Info Frame Tx Countdown (optional) |
| Octets: | 1 | 1 | 1 |  | 2 |

**Figure 9-bc1 - EBCS Parameters element format**[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]

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

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

[CID 1087][CID 1087]

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

[CID 1088, 1044, 1554][CID 1088, 1044, 1554][CID 1268, 1601, 1441][CID 1087]The EBCS Info Frame Tx Countdown subfield in the element indicates the number of TBTTs until the transmission of the next EBCS Info frame. The value 1 indicates that the frame is transmitted following the next TBTT. The value 0 is reserved.

**9.3.3.2 Beacon frame format**

***TGbc Editor: please make changes to the following row in Table 9-32 as shown below:***

**Table 9-32**—**Beacon frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 93 | EBCS Parameters element | [CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]This element is optionally present if dot11EBCSSupportActivated is true. |

**9.3.3.10 Probe Response frame format**

***TGbc Editor: please make changes to the following row in Table 9-41 as shown below:***

**Table 9-41**—**Probe Response frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 113 | EBCS Parameters element | [CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]This element is optionally present if dot11EBCSSupportActivated is true. |

**9.4.2.26 Extended Capabilities element**

***TGbc Editor: please insert a new row to Table 9-153 as shown below:***

**Table 9-153—Extended Capabilities field**[CID 1087]

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | EBCS Relaying Supported | An EBCS AP sets the EBCS Relaying Supported to 1 when dot11EBCSSupportActivated is true and dot11EBCSRelayingServiceSupported is true. Otherwise the AP sets the field to 0. A non-AP STA sets the field to 0. |

**9.6.7.100 EBCS UL frame format**

The EBCS UL frame is transmitted by an EBCS non-AP STA and carries higher layer payload intended for a destination specified within the frame.

The format of the EBCS UL frame Action field is defined in Figure 9-bc24 (EBCS UL frame Action field format).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | Control | Destination URI | HLP Container | STA Certificate Container (optional) | Replay Protection (optional) | Frame Signature (optional) |
| Octets: | 1 | 1 | 1 | variable | variable | variable | 0 or 8 | variable |

 **Figure 9-bc24 - EBCS UL frame Action field 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 frames).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | B0 | B1 | B2 B4 | B5 B7 |
|  |  |  | STACertificate Present | Replay Protection Present | Frame Signature Type  | Reserved |
| Bits: |  |  | 1 | 1 | 3 | 3 |

 **Figure 9-bc25 - Control field format**[CID 1268, 1601, 1441]

The format of the Control field is shown in Figure 9-bc25 (Control field format).

[CID 1268, 1601, 1441][CID 1268, 1601, 1441]The STA Certificate Present subfield is set to 1 when the STA Certificate Container field is carried in the frame. Otherwise, the subfield is set to 0.

The Replay Protection Present subfield is set to 1 when the Replay Protection field is carried in the frame. Otherwise, the subfield is set to 0.

The encoding of the Frame Signature Type subfield is shown in Table 9-bc6 (Encoding of Frame Signature Type subfield).

 **Table 9-bc6 - Encoding of Frame Signature Type subfield**

|  |  |  |
| --- | --- | --- |
| **Subfield value** | **Algorithm** | **Encoding** |
| 0 | HLSA | The authentication of HLP payload is provided by higher layer and is included in the HLP Payload field |
| 1 | RSA-2048 | See 12.100.2.5 (Signature of the EBCS UL frame)[CID 1087] |
| 2 | ECDSA-P256 |
| 3 | Ed25519 |
| 4-7 | Reserved |  |

The Destination URI field contains a Destination URI element as defined in 9.4.2.89 (Destination URI element) that specifies the destination to which the HLP payload needs to be relayed.

The format of the HLP Container field is shown in Figure 9-bcxx (HLP Container field format).

|  |  |  |
| --- | --- | --- |
|  | HLP Payload Length | HLP Payload |
| Octets: | 2 | variable |

**Figure 9-bcxx – HLP Container field format**

The HLP Payload Length subfield indicates the length of the HLP Payload subfield in octets.

The HLP Payload subfield carries the HLP payload.

The format of the STA Certificate Container field is shown in Figure 9-bcxx (STA Certificate Container field format).

|  |  |  |
| --- | --- | --- |
|  | STA Certificate Length | STA Certificate |
| Octets: | 2 | variable |

**Figure 9-bcxx – STA Certificate Container field format**

The STA Certificate Length subfield carries a nonzero value that indicates the length of the STA Certificate subfield in octets.

The STA Certificate subfield carries the X.509v3 certificate of the STA encoded according to IETF RFC 5280.

The format of the Replay Protection field, if present, is shown in Figure 9-bc26 (Replay Protection field format).

|  |  |  |
| --- | --- | --- |
|  | Time | Frame Count |

Octets: 4 4

 **Figure 9-bc26 - Replay Protection** **field format**

The Time subfield is either set to 0 or carries the time, expressed as number of seconds since 2020-01-01 00:00:00 UTC, when the frame is queued for transmission.

The Frame Count subfield carries a numeric value that is incremented for each EBCS UL frame transmission.

The Frame Signature field is not present if the Frame Signature Type is set to 0 (HLSA). Otherwise, the field is present and carries a signature of the EBCS UL frame [CID 1087]computed as defined in 12.100.2.5 (Signature of the EBCS UL frame).

##### 11.100.3.1 General

***TGbc Editor: please make changes to this clause as shown below:***

[CID 1087]The EBCS UL Service procedure allows a non-AP STA to transmit an EBCS UL frame with the expectation that one or more EBCS proxies that are affiliated with one or more EBCS APs in the neighborhood would relay the HLP payload carried in the frame to a destination specified in the frame. [CID 1268, 1601, 1441, 1323]The relaying service is best effort with no guarantee that the HLP payload will be delivered to the destination specified in the STA’s frame [CID 1268, 1601, 1441]

##### 11.100.3.2 EBCS UL operation at an EBCS AP

***TGbc Editor: please make changes to this clause as shown below:***

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]An EBCS AP that is affiliated with an EBCS proxy (see 4.5.xx (EBCS relaying service)) provides access to a relaying service in which the HLP payload carried in an EBCS UL frame received from an EBCS non-AP STA is relayed to a destination specified in the frame. Among all APs in a multiple BSSID set, only the AP corresponding to the transmitted BSSID shall be affiliated with an EBCS proxy. Among all APs in a co-hosted BSSID set, only one AP shall be affiliated with an EBCS proxy.

[CID 1087, 1326]An EBCS AP sets the EBCS Relaying Supported subfield of the Extended Capabilities element to 1 if it is affiliated with an EBCS proxy that provides the relaying service. Otherwise the subfield is set to 0. [CID 1268, 1601, 1441][CID 1268, 1601, 1441][CID 1087]

[CID 1268, 1601, 1441]An EBCS proxy evaluates various criteria such as the ones described in 12.100.2.6 (Authentication of an EBCS UL frame) to decide whether to relay the HLP payload to the specified destination. An EBCS proxy may limit the amount or frequency of HLP payloads that are relayed to the specified destination. An EBCS proxy may append additional information before relaying the HLP payload to the specified destination. The evaluation of criteria, the decision to limit the amount or frequency of relaying, and the decision to append addition information can be based on local policies or based on a relationship established with the specified destination.

NOTE 1 – The establishment of such a relationship is out of scope of this standard.

NOTE 2 – An EBCS proxy can decide to not relay the HLP payload for any reason such as not having a relationship with the specified destination, the implemented criteria for relaying not being satisfied or for any other reason.

[CID 1087, 1334]

[CID 1087][CID 1088, 1044, 1554][CID 1087, 1088, 1044, 1554]

* + - 1. **EBCS UL operation at an EBCS non-AP STA**

***TGbc Editor: please make changes to this clause as shown below:***

An EBCS non-AP STA may request relaying of an HLP payload to a specific destination by transmitting an EBCS UL frame. The frame carries the URI of the intended destination.[CID 1087, 1268, 1601, 1441] The Address 1 and Address 3 fields of the frame shall be set to the broadcast address.

[CID 1087]An EBCS non-AP STA should include a STA certificate in an EBCS UL frame to help authenticate the transmitter of the frame (see 12.100.2.6 (Authentication of an EBCS UL frame)).

[CID 1352]An EBCS non-AP STA should include the Replay Protection field in an EBCS UL frame that it transmits to reduce the possibility of a successful replay attack. set to 0 in the first EBCS UL frame that the STA transmits and subsequent of the frame[CID 1260, 1357]

NOTE—How a STA obtains time information is out of scope of this standard.

[CID 1268, 1601, 1441][CID 1087]An EBCS non-AP STA should include the Frame Signature field in the EBCS UL frame to protect the contents of the frame (see 12.100.2.5 (Signature of the EBCS UL frame)).

[CID 1087]An EBCS non-AP STA is not required to monitor the WM and may transmit an EBCS UL frame without discovering nearby EBCS APs that provide access to the relaying service.

**12.100.2.6 Authentication of an EBCS UL frame**[CID 1334, 1034]

***TGbc Editor: please make changes to this clause as shown below:***

An EBCS proxy shall discard the EBCS UL frame if either of the following conditions are met:

1. The STA Certificate subfield is present and any of the following is true:
	1. The certificate of the specified destination or the CA that signed the STA’s certificate is not installed
	2. The verification of the STA’s certificate using the installed certificate of the specified destination or CA fails.
	3. The Frame Signature Type subfield is not HLSA and the verification of the signature of the frame using the STA’s certificate fails
2. The Replay Protection field is present and any of the following is true:
	1. The Time subfield is set to a nonzero value and the difference between that value and the time the EBCS UL frame is received is greater than a configured value.
	2. The Frame Count subfield is nonzero and is less than or equal to the value in the previously received EBCS UL frame (if any).
	3. The Frame Count subfield is 0 and the value in the previously received EBCS UL frame (if any) is not equal to 232 – 1 or less within an acceptable range.

NOTE – The acceptable time difference at an EBCS proxy can be configured based on local policies or based on relationship with the specified destination. In addition, an EBCS proxy must account for packet-loss when it performs a replay check and can have an expiration time after which the last seen Frame Count value for a certain transmitter can be deleted.

If the authentication succeeds, the EBCS proxy relays the HLP payload to the specified destination.

**6.3.201.2.2 Semantics of the service primitive**[CID 1268, 1601, 1441]

***TGbc Editor: please make changes to this clause as shown below:***

The primitive parameters are as follows:

 MLME-EBCSUL.request(

DestinationURI,

HLPPayload,

STACertificate,

ReplayProtection,

PrivateKey

 )

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
|  |  |  |  |
|  |  |  |  |
| DestinationURI | Destination URI element | As defined in 9.4.2.89(Destination URI element). | Specifies the destination to which the HLP payload is to be relayed. |
| HLPPayload | Sequence of octets | N/A | Specifies the HLP payload to be relayed to the specified destination. |
| STACertificate | Sequence of octets | N/A | When present, specifies the certificate for the STA. |
| ReplayProtection | Replay Protection field as defined in 9.6.7.100 | As defined in 9.6.7.100 | When present, specifies the time (if available) when an EBCS UL frame is queued for transmission and a count of the number of EBCS UL frame transmissions. |
| PrivateKey | Sequence of octets | N/A | When present, specifies the private key for signature generation. |

**6.3.201.3.2 Semantics of the service primitive**[CID 1268, 1601, 1441]

***TGbc Editor: please make changes to this clause as shown below:***

The primitive parameters are as follows:

 MLME-EBCSUL.indication(

DestinationURI,

HLPPayload,

ReplayProtection,

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
|  |  |  |  |
|  |  |  |  |
| DestinationURI | Destination URI element | As defined in9.4.2.89 (Destination URI element). | Specifies the destination to which the HLP payload is to be relayed. |
| HLPPayload | Sequence of octets | N/A | Specifies the HLP payload to be relayed to the specified destination. |
| ReplayProtection | Replay Protection field as defined in 9.6.7.100 | As defined in 9.6.7.100 | When present, specifies the time (if available) when an EBCS UL frame is queued for transmission and a count of the number of EBCS UL frame transmissions. |

***TGbc Editor: please insert the following subclause at the end of clause 4.5 [text based on doc 11-21/0568r4]:***

[CID 1087, 1088, 1044, 1554, 1268, 1601, 1441]

**4.5.xx EBCS relaying service**

**4.5.xx.1 General**

The EBCS relaying service provides a mechanism for an EBCS non-AP STA to send an HLP payload to a specified destination.

**4.5.xx.2 EBCS proxy operation**

An EBCS proxy is a logical component affiliated with an EBCS AP, and which might be collocated with the EBCS AP, that can relay an HLP payload carried in an EBCS UL frame received by an EBCS AP to a destination specified in the frame, typically within an external network.

An EBCS proxy that provides the relaying service evaluates certain criteria before relaying the HLP payload carried in an EBCS UL frame to the destination specified in the frame. Such criteria can include, but are not limited to, verifying the STA certificate, if present, to determine whether the STA transmitting the frame is authorized to send an HLP payload to the specified destination, performing replay checking, and limiting the amount or frequency of HLP payload that is relayed to the specified destination. The evaluation of the criteria can be based on local policies installed at the EBCS proxy and/or based on a relationship established with the specified destination. The establishment of such a relationship is out of scope of this standard.

An EBCS proxy can establish more than one relationship, each with a different destination and potentially different criteria. An EBCS proxy can also append additional information before it relays the HLP payload. The format and content of the information appended are based on the agreement with the specified destination. The relaying service is best effort and the EBCS proxy can decide not to relay the HLP payload if any of the implemented criteria for relaying are not satisfied or for any other reason.

NOTE 1 – The communication between an EBCS AP and an EBCS proxy and the communication between an EBCS proxy and a specified destination are out of scope of this standard.

NOTE 2 – An EBCS proxy evaluating various criteria before it relays an HLP payload helps reduce the likelihood of a DoS attack on the specified destination.

**4.5.xx.3 Example configurations for EBCS proxy**

Figure 4-20a (Illustration of relaying operation at an EBCS AP with collocated EBCS proxy) provides an example of the relaying service based on a relationship with a specified destination. In the figure, EBCS proxy P1 and EBCS proxy P3 have established a relationship with a destination (D). An EBCS non-AP STA (S) transmits an EBCS UL frame that is received by EBCS APs in the neighborhood (i.e., AP1, AP2 and AP3). The EBCS UL frame carries the HLP payload, a field carrying the address of D and other fields for security. P1 and P3 verify the certificate of S based on their agreement with D and perform a replay check, to determine whether the criteria for relaying the HLP payload to D are met. If the local policy or the agreement with D requires limiting the amount or frequency of HLP payloads being sent to D, then each of P1 and P3 does not send an HLP payload to D, if it determines that a limit was reached. If the agreement with D requires the inclusion of additional information, P1 and P3 append appropriate information, before relaying the HLP payload. In the figure, EBCS AP2 discards the EBCS UL frame. This could be for any number of reasons such as it not providing a relaying service, its collocated proxy not having established a relationship with D, or one or more criteria for relaying not having been satisfied.

**Figure 4-20a: Illustration of relaying operation at an EBCS AP with collocated EBCS proxy**

In another example, depicted in Figure 4-20b (Illustration of relaying when EBCS proxy is not collocated within an EBCS AP), the EBCS proxy (P) is not collocated with either EBCS AP1 or EBCS AP3, but resides on an entity in the LAN that AP1 and AP3 belong to. EBCS AP1 and EBCS AP3 send the contents of the EBCS UL frame to P, which evaluates whether the criteria for relaying are met before it relays the HLP payload to the specified destination.

**Figure 4-20b: Illustration of relaying when EBCS proxy is not collocated within an EBCS AP**

The configuration shown in Figure 4-20b (Illustration of relaying when EBCS proxy is not collocated within an EBCS AP) could be prevalent in commercial deployments, such as airports, train stations, malls, or a warehouse, where multiple EBCS APs are likely to be connected to a single entity on a common LAN (such as a network controller) which provides access to destinations outside the LAN. In such a configuration, the EBCS proxy resides on an entity in the LAN. On the other hand, the configuration shown in Figure 4-20a (Illustration of relaying operation at an EBCS AP with collocated EBCS proxy) could be prevalent in residential deployments where an EBCS AP has direct connectivity to destinations outside the LAN.

**C.3 MIB Detail**

***TGbc Editor: please insert a new entry to the following paragraph:***

***Change the end of the “Dot11StationConfigEntry” of the “dot11StationConfig TABLE” as follows:***

 …

 dot11EBCSTerminationNoticeMaximumInterval, Unsigned32,

 dot11EBCSRelayingServiceSupport, TruthValue

 }

***TGbc Editor: please insert a new entry to the following paragraph:***

***Insert the following elements at the end of the dot11StationConfigTable element definitions:***

dot11EBCSRelayingServiceSupport 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 as soon as practical in the implementation.

This attribute when true, indicates that the EBCS AP is affiliated with an EBCS proxy that provides relaying service. The capability is disabled otherwise."

DEFVAL {false}

::= { dot11StationConfigEntry <ANA> }

***TGbc Editor: please insert a new entry to the following paragraph:***

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

-- \* Compliance Statements - EBCS

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

dot11EBCSComplianceGroup OBJECT-GROUP

OBJECTS {

 …

 dot11EBCSTerminationNoticeMaximumInterval,

 dot11EBCSRelayingServiceSupported

 }

 STATUS current