IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 802.11bc LB 257 resolution for CIDs assigned to Abhi (part 1) | | | | |
| Date: November 6, 2021 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com |
| George Cherian |  |  |  |
| Jouni Malinen |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following 23 comments submitted during LB 257 for 11bc D2.0:

2043, 2154, 2155, 2156, 2133, 2042, 2157, 2158, 2134, 2048, 2001, 2108, 2105, 2215, 2110, 2233, 2234, 2003, 2111, 2112, 2161, 2055, 2174

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Minor updates and re-organization of content.

***TGbc Editor: The baseline for the proposed changes is 802.11bc D2.0***

**11.55.3.2** **EBCS UL operation at an EBCS AP**

***TGbc Editor: please add the following NOTE at the end of this subclause as shown below:***

NOTE – An EBCS AP that relays HLP payload to the specified destination via its EBCS proxy can be in unassociated state with the non-AP STA that transmitted the EBCS UL frame carrying the HLP payload.[2043]

**11.55.3.3** **EBCS UL operation at an EBCS non-AP STA**

***TGbc Editor: please update the following paragraphs in this subclause as shown below:***

[2154, 2155]receiving a Beacon frame or a Probe Response frame with EBCS Relaying Supported field of the Extended Capabilities element set to 1 The EBCS UL frame shall carry the HLP payload and the URI of the intended destination. The Address 1 and Address 3 fields of the frame shall be set to the broadcast address.

[2156, 2133]An EBCS non-AP STA should include its certificate in an EBCS UL frame to allow the EBCS Proxy to authenticate the EBCS non-AP STA (see [12.14.2.6 (Authentication of an EBCS UL frame)](#_bookmark239)).

[2042, 2157][2158]When an EBCS non-AP STA has time information, the Frame Tx Time field shall indicate the time when the EBCS UL frame is queued for transmission. [2157]

[2158]NOTE—An EBCS STA that transmits an EBCS UL frame can be in unassociated state. How an EBCS non-AP STA obtains time information is out of scope of this standard.

[2042, 2157]is

The Frame Signature field, if present in the EBCS UL frame, shall [2134]be computed as defined in [12.14.2.5](#_bookmark237) [(Signature of the EBCS UL frame)](#_bookmark237).

**12.14.2.5** **Signature of the EBCS UL frame**[2048]

Annon-AP STA (HLP payload) to a specified destination

If the Frame Signature Type subfield of the EBCS UL frame is set to a nonzero value, then one of the following public key algorithms is used for generating the frame signature.

— RSASSA-PSS

— ECDSA

— Ed25519

For RSASSA-PSS, the length of the modulus shall be 2048 bits or 4096 bits. SHA-256 for 2048 bits modulus or SHA-512 for 4096 bits modulus shall be used as the mask generation function and as the hash function during signature generation.

For ECDSA, the domain parameters shall be P-256 or P-521. SHA-256 for P-256 or SHA-512 for P-521 shall be used as the hash function during signature generation.

For Ed25519, SHA-512 shall be used as the hash function during signature generation.

The signature is generated as follows:

Signature = Sign (transmitter’s private key, transmitter’s MAC address || EBCS UL frame fields from the beginning of the Control field to the last field before the Frame Signature

field)

where

Sign (*k, m*) indicates a digital signature for the message *m* using the private key *k*.

* + - 1. **EBCS UL frame format**[2048]

***TGbc Editor: please update the following paragraph in this subclause as shown below:***

The Frame Signature field is not present if the Frame Signature Type subfield indicates HLSA. Otherwise, the Frame Signature field carries a signature of the EBCS UL frame (generated as described in [12.14.2.5 (Signature of the EBCS UL frame)](#_bookmark237)). The length of the Frame Signature field is determined as defined in [Table 9-397a (Encoding of Frame Signature Type subfield](#_bookmark144)). In case of ECDSA, the Signature field contains the value r and s encoded in DER-encoded ASN.1 structure (a SEQUENCE of two INTEGERS, for r and s, in that order) that includes the length.

**4.3.31 Enhanced broadcast services**

***TGbc Editor: please update the following paragraph in this subclause as shown below:***

Enhanced broadcast services (EBCS) provides enhanced transmission and reception of broadcast data, both where there is an association between the transmitter and the receiver(s) in an infrastructure BSS and in cases where there is no association between transmitter and receiver(s). Further, EBCS provides a service in which an EBCS proxy affiliated with an EBCS AP can relay the contents of a higher layer payload, received from an EBCS non-AP STA to a destination typically within an external network. The relaying EBCS proxy can embed additional information.[2001]

**4.5.12.2** **EBCS proxy operation**[2108]

***TGbc Editor: please split the following paragraph in this subclause as shown below:***

An EBCS proxy can establish more than one relationship, each with a different destination and potentially different criteria.

An EBCS proxy can also embed additional information before it relays the HLP payload. The format and content of the information embedded 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.

**4.5.12.3 Example configurations for EBCS proxy**

***TGbc Editor: please update the caption for Figure 4-20a as shown below:***

**Figure 4-20a—Illustration of relaying operation at EBCS APs with collocated EBCS proxy**[2110]

***TGbc Editor: please update the following paragraph in this subclause as shown below:***

[2003]In the figure, EBCS proxies P1, P2 and P3 are collocated with EBCS APs A1, A2 and A3 respectively. 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. [2111]If the local policy or the agreement with D requires limiting the amount or frequency of HLP payloads being sent to D, then P1 and P3 determine whether or not to relay their received HLP payload to D, based on whether or not prior transmissions have reached the limit. If the agreement with D requires the inclusion of additional information, P1 and P3 embed appropriate information, before relaying the HLP payload. In the figure, EBCS AP2 discards the EBCS UL frame. [2112]This could be for any number of reasons such as the AP does not provide a relaying service, the AP’s collocated proxy (P2) has not established a relationship with D, or that one or more criteria for relaying have not been satisfied.

***TGbc Editor: please move the NOTE from the end of this subclause to after the 2nd paragraph in this subclause:***

[2111]NOTE—Where a destination has relationships with multiple EBCS proxies, it might, as part of the agreement with each proxy, set a relaying limit (e.g., amount or frequency of relaying per proxy) so that the aggregate from all the proxies is below a certain threshold. In addition, EBCS proxies might collaborate to limit the aggregate payload being relayed to the specified destination. Such mechanisms are out of scope of this standard.

* + - 1. **EBCS UL frame format**[2161]

***TGbc Editor: please update the following paragraph in this subclause as shown below:***

The format of the Destination URI field is shown in [Figure 9-909xx (Destination URI field format](#_bookmark145)).

Destination URI Length

URI

Octets: 1 variable

##### Figure 9-909xx—Destination URI field format

The Destination URI Length subfield indicates the length of the URI subfield in octets.

The URI subfield specifies the destination URI using the format defined in IETF RFC 3986.

**9.4.2.89** **Destination URI element**[2161]

***TGbc Editor: please revert all changes to clause 9.4.2.89 (Destination URI element) from TGbc draft***

**6.3.127.2.2 Semantics of the service primitive**[2161]

***TGbc Editor: please update the first row in the table in this subclause as shown below:***

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| DestinationURI | Destination URI field as defined in 9.6.7.53 (EBCS UL frame format) | As defined in  [9.6.7.53 (EBCS UL](#_bookmark141) [frame format)](#_bookmark141) | Specifies the destination to which the HLP payload is to be relayed. |

**6.3.127.3.2 Semantics of the service primitive**[2161]

***TGbc Editor: please update the first row in the table in this subclause as shown below:***

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| DestinationURI | Destination URI field as defined in 9.6.7.53 (EBCS UL frame format) | As defined in  [9.6.7.53 (EBCS UL](#_bookmark141) [frame format)](#_bookmark141) | Specifies the destination to which the HLP payload is to be relayed. |

* + - 1. **EBCS UL frame format**

***TGbc Editor: please update Figure 9-909ai as shown below:***

B0 B1 B2 B3 B5 B6 B7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STA  Certificate Present | Frame Tx Time Present | Frame Count Present | Frame SignatureType | Reserved |

Bits: 1 1 1 3 2

**Figure 9-909ai—Control field format**[2174]

***TGbc Editor: please update the following paragraph in this subclause as shown below:***

The Frame Tx Time Present subfield is set to 1 when the Frame Tx Time [2055]field is carried in the frame. Otherwise, the subfield is set to 0.