IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for Clause 9.6.7.101 |
| Date: 2021-01-26 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | Koden-TI | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes the resolutions for clause 9.6.7.101 on LB252.

# To Editor: Green background means the comments finished in the previous revisions.

**The baseline is D1.01.**

# Suggested resolution

**9.6.7.101 eBCS Info frame format**

The format of the Action field of the eBCS Info frame is shown in Figure 9-bc27 (eBCS Info frame Action field format).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | Sequence Number | Timestamp | eBCS Info Control | eBCS Info Interval | Fragment Hash Values [1304, 1117] | Certificate Length |
| Octets: | 1 | 1 | 4 | 8 | 1 | 1 | ~~variable~~*n* x 32 | 0 or 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Certificate | Content Information Number | Content Information ~~1~~ List | ~~Content Information 2~~ | ~~…~~ | ~~Content Information N~~ | Signature |
| Octets: | variable | 1 | variable | ~~variable~~ |  | ~~variable~~ | variable |

**Figure 9-bc27 eBCS Info 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 1 (Public Action frames).

The Sequence Number field contains the ~~current value~~ sequence number of ~~dot11eBCSInfoSequence~~ the EBCS Info frame [1157, 1237].

The Timestamp field is the elapsed time from 2020-01-01 00:00 UTC in milliseconds.

The eBCS Info Control field is shown in Figure 9-bc28 (eBCS Info frame eBCS Info Control field format)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 | B5 | B6 | B7 |
|  | Number Of Fragments | Fragment Index | eBCS Info Authentication Algorithm |
| Bits: | 3 | 3 | 2 |

**Figure 9-bc28 ~~eBCS Info frame~~ [1524] EBCS Info Control field format**

The Number Of Fragments subfield indicates the ~~total~~ [1609] number of the ~~following~~ [1609] fragments of the EBCS Info frame minus 1. [1609]

The Fragment Index subfield indicates the fragmentation index of the EBCS Info frame.

The EBCS Info Authentication Algorithm subfield indicates the algorithm to authenticate the EBCS Info frame. Values of this subfield ~~is~~ are [1455] defined in Table 9-bc7 (EBCS Info Authentication Algorithm subfield).

**Table 9-bc7 EBCS Info Authentication Algorithm subfield**

|  |  |  |
| --- | --- | --- |
| **Value** | **Algorithm** | **Certificate Present** |
| 0 | None | No |
| 1 | RSASSA-PSS | Yes |
| 2 | ECDSA | Yes |
| 3 | Ed25519 | Yes |

Details of each algorithm are described in 12.bc.2.1 (Signature of the EBCS Info frame).

~~The EBCS Info frame fragmentation procedure is described in 11.100.2.4 (EBCS Info frame fragmentation).~~ [1610]

The EBCS Info Interval field indicates the EBCS Info frame transmission interval (from dot11EBCSInfoInterval), in units of ~~100 milliseconds~~ a beacon interval. [w/o CID] ~~In the case of PKFA and transmitting irregular time sensitive information, the EBCS Info Interval field is set to 0.~~ [1075, 1135, 1021, 1020]

NOTE—Even if PKFA is used, the EBCS Info frames are transmitted periodically to advertise EBCS availability.

The Fragment Hash Values field is only present if the Number Of Fragments subfield N is nonzero. It contains a sequence of N 16-octet Fragment Hash Value subfields. [1304, 1117]

The Certificate Length field, the Certificate field and the Signature field are present if the EBCS Info Authentication Algorithm subfield ~~in the EBCS Control field~~ [w/o CID] indicates that a certificate is present, and ~~are~~ is [w/o CID] not present otherwise.

The Certificate Length field indicates the length of the Certificate field in octets.

The Certificate field ~~is~~ contains the X.509v3 certificate of the EBCS transmitter ~~in the DER format (Distinguished Encoding Rules, ITU-T Recommendation X.680 (2002))~~ encoded according to IETF RFC 5280. [1136]

The Content Information Number field indicates the number of Content Information included in the Content Information List field~~s~~. [w/o CID]

The Content Information List field contains multiple Content Information. [w/o CID]

The format of each Content Information ~~field~~ [w/o CID] is shown in Figure 9-bc29 (Content Information field format).At P

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | ~~Content ID~~ | ~~Authentication Algorithm~~ | ~~Content Information Control~~ | ~~Content Destination Address Type~~ | ~~Content Destination Address~~ | ~~Title Length~~ | ~~Title~~ |
| ~~Octets:~~ | ~~1~~ | ~~1~~ | ~~1~~ | ~~1~~ | ~~variable~~ | ~~1~~ | ~~variable~~ |

|  |  |  |  |
| --- | --- | --- | --- |
|  | ~~Negotiation Method~~ | ~~Time Of Termination~~ | ~~Next Schedule~~ |
| ~~Octets:~~ | ~~1~~ | ~~0 or 2~~ | ~~0 or 2~~ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | ~~Allowable Time Difference~~ | ~~HCFA Base Key~~ | ~~Previous Period HCFA Base Key 0 Sequence~~ | ~~Previous Period HCFA Base Key 0~~ | ~~Previous Period HCFA Base Key 1 Sequence~~ | ~~Previous Period HCFA Base Key 1~~ |
| ~~Octets:~~ | ~~0 or 2~~ | ~~variable~~ | ~~0 or 1~~ | ~~variable~~ | ~~0 or 1~~ | ~~variable~~ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ~~HCFA Key Change Interval~~ | ~~Number Of Instant Authenticators~~ | ~~Instant Authenticator Hash Distance 0~~ | ~~…~~ | ~~Instant Authenticator Hash Distance N-1~~ |
| ~~Octets:~~ | ~~0 or 1~~ | ~~0 or 1~~ | ~~0 or 1~~ |  | ~~0 or 1~~ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ~~Instant Authenticator 0~~ | ~~…~~ | ~~Instant Authenticator N-1~~ | ~~Data Length~~ | ~~Data~~ |
| ~~Octets:~~ | ~~variable~~ |  | ~~variable~~ | ~~0 or 1~~ | ~~variable~~ |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Content ID | Content [1137] Authentication Algorithm | Content Information Control | Content Destination Address Type | Content Destination Address | Title Length | Title |
| Octets: | 1 | 1 | 1 | 1 | variable | 1 | variable |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Negotiation Method | Time Of Termination (optional) | Next Schedule (optional) | Allowable Time Difference (optional) |
| Octets: | 1 | 0 or 2 | 0 or 2 | 0 or 2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | HCFA Base Key(optional) | Previous Period HCFA Base Key 0 Sequence (optional) | Previous Period HCFA Base Key 0 (optional) | Previous Period HCFA Base Key 1 Sequence (optional) | Previous Period HCFA Base Key 1 (optional) | HCFA Key Change Interval (optional) |
| Octets: | variable | 0 or 1 | 0 or 32 | 0 or 1 | 0 or 32 | 0 or 1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Number Of Instant Authenticators (optional) | Instant Authenticator List (optional) [1528] | Data Length (optional) | Data (optional) |
| Octets: | 0 or 1 | *n* x 33 | 0 or 1 | variable |

**Figure 9-bc29 Content Information field format**

The Content ID subfield indicates the identifier of the content.

The Content [1137] Authentication Algorithm subfield is defined in Table 9-bc8 (~~EBCS Info frame~~ Content [1137] Authentication Algorithm field)

**Table 9-bc8 ~~EBCS Info frame~~ Content [1137] Authentication Algorithm subfield**

|  |  |
| --- | --- |
| **Value** | **Content [1137] Authentication Algorithm** |
| 0 | HLSA (see 12.100.4 No frame authentication withmandatory higher layer source authentication (HLSA)) |
| 1 | PKFA (see 12.100.2 EBCS public key frameauthentication (PKFA)) |
| 2 | HCFA without instant authentication (see 12.100.3EBCS Hash chain frame authentication (HCFA)) |
| 3 | HCFA with instant authentication (see 12.100.3 EBCSHash chain frame authentication) |
| 4-255 | Reserved |

The Content Information Control subfield is shown in Figure 9-bc30 (Content Information Control subfield format)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 | B5 | B6 | B7 |
|  | Time Of Termination Present | Next Schedule Present | Data Present | Reserved |
| Bits: | 1 | 1 | 1 | 5 |

**Figure 9-bc30 Content Information Control subfield format**

The Time Of Termination Present subfield indicates whether the Time Of Termination field is present.

The Next Schedule Present subfield indicates whether the Next Schedule field is present.

The Data Present subfield indicates whether the Data Length field and the Data field are present.

The Content Destination Address Type subfield is defined in Table 9-bc9 (Content Destination Address Type subfield). UDP/hostname shall only be used for EBCS UL frames. Others are used for both EBCS DL and UL frames.

**Table 9-bc9 Content Destination Address Type subfield**

|  |  |
| --- | --- |
| **Value** | **Higher Layer Protocol** |
| 0 | UDP/IPv4 |
| 1 | UDP/IPv6 |
| ~~2~~ | ~~UDP/hostname (UL only)~~ [1022] |
| ~~3~~ 2 | MAC address |
| 4-7 | Reserved |

The Content Destination Address subfield is the destination address and port of the content encoded as follows.

If the Content Destination Address Type subfield is UDP/IPv4, the format of the Content Destination Address subfield is shown in Figure 9-bc31 (Content Destination Address subfield format for UDP/IPv4).

Figure 9-bc31 Content Destination Address subfield format for UDP/IPv4

If the Content Destination Address Type subfield is UDP/IPv6, the format of the Content Destination Address subfield is shown in Figure 9-bc32 (Content Destination Address subfield format for UDP/IPv6).

Figure 9-bc32 Content Destination Address subfield format for UDP/IPv6

If the Content Destination Address Type subfield is UDP/hostname, the format of the Content Destination Address subfield is shown in Figure 9-bc33 (Content Destination Address subfield format for UDP/hostname). The Hostname Length subfield indicates the length of the Hostname subfield. The Hostname subfield is the hostname as a UTF-8 string.

Figure 9-bc33 Content Destination Address subfield format for UDP/hostname

If the Content Destination Address Type subfield is MAC Address, the format of the Content Destination Address subfield is shown in the Figure 9-bc34 (Content Destination Address subfield format for MAC Address). The MAC Address field is the destination MAC Address of the content.

Figure 9-bc34 Content Destination Address subfield format for MAC Address

The Title Length subfield indicates the length of the following Title subfield in octets. The Title subfield is a human readable title of the content as a UTF-8 string.

The Time Of Termination subfield indicates the number of TBTTs until the content identified by the content ID contained in the Content ID subfield is terminated. A value of 0 indicates that the content identified by the content ID in the Content ID subfield will be terminated at the following TBTT. A value of 65535 indicates that the content identified by the content ID in the Content ID subfield has no specific termination time.

The Next Schedule subfield indicates the number of TBTTs until the content by the content ID contained in the Content ID subfield is transmitted again. A value of 0 indicates that the content identified by the content ID in the Content ID subfield will be started to transmit at the following TBTT. A value of 65535 indicates that the content identified by the content ID in the Content ID subfield has no specific transmission starting time.

The Allowable Time Difference subfield is present if the Authentication Algorithm is PKFA or HCFA. The value indicates the allowable time difference between the clock of the EBCS transmitter and the clock of the EBCS receivers in milliseconds.

The HCFA Base Key subfield, the Previous Period HCFA Base Key 0 Sequence subfield, the Previous Period HCFA Base Key 0 subfield, the Previous Period HCFA Base Key 1 Sequence subfield, the Previous Period HCFA Base Key 1 subfield and the HCFA Key Change Interval subfield are present if the Authentication Algorithm field indicates HCFA, and are not present otherwise.

The HCFA Base Key subfield contains the first HCFA base key of the HCFA period that starts from this EBCS Info frame. The length of the HCFA Base Key subfield is determined by the authentication algorithm.

The Previous Period HCFA Base Key 0 Sequence subfield and the Previous Period HCFA Base Key 1 Sequence subfield indicate the key sequence number of the Previous Period HCFA Base Key 0 subfield and the Previous Period HCFA Base Key 1 subfield respectively. The Previous Period HCFA Base Key 0 subfield and the Previous Period HCFA Base Key 1 subfield contain the HCFA base key to be disclosed for the previous HCFA period. The length of the Previous Period HCFA Base Key 0 subfield and the Previous Period HCFA Base Key 1 subfield is determined by the authentication algorithm.

If the previous HCFA period does not exist, e.g. at the start of the EBCS transmission, the Previous Period HCFA Base Key 0 Sequence subfield, the Previous Period HCFA Base Key 0 subfield, the Previous Period HCFA Base Key 1 Sequence subfield and the Previous Period HCFA Base Key 1 subfield are set to 0.

The HCFA Key Change Interval subfield indicates the dot11EBCSHCFAKeyChangeInterval in unit of 10 milliseconds.

*(P42 L1)*

The Number Of Instant Authenticators subfield~~, Instant Authenticator Hash 1 Distance n subfields~~ [1528] and the Instant Authenticators ~~n~~ subfield~~s~~ are present if the Content [1137] Authentication Algorithm field indicates HCFA with instant authentication, and are not present otherwise.

The Number Of Instant Authenticators subfield indicates the number of the ~~i~~Instant ~~a~~Authenticators ~~to be used~~ containd in the Instant Authenticator List.

~~The Instant Authenticator Hash Distance n subfields indicate the hash distance of each instant authenticator. The Instant Authenticator n subfields contain the instant authenticator of the following EBCS Data frame of the hash distance that is indicated by the Instant Authenticator Hash Distance n subfield.~~

The Instant Authenticator List subfield contains multiple Instant Authenticators.

The format of each Instant Authenticator is shown in the Figure 9-bc35a (Instant Authenticator format). [1528]

|  |  |  |
| --- | --- | --- |
|  | Hash Distance | Hash Value |
| Octets: | 1 | 32 |

**Figure 9-bc35a Instant Authenticator format [1528]**

The Hash Distance subfield indicate the hash distance of the instant authenticator. The Hash Value subfield contain the instant authenticator of the following EBCS Data frame of the hash distance that is indicated in the Hash Distance subfield. [1528]

The Data subfield is present if the Authentication Algorithm field indicates PKFA and the Data Length subfield is present, and is not present otherwise.

…

*(P43 L1)*

The Signature field is the digital signature of the EBCS Info frame that 1 is generated by the certificate of the EBCS transmitter. The length of the Signature field is determined from the public key algorithm of the authentication algorithm.

The Signature field is not present if the Fragment Index subfield is nonzero. [1304]

*(End of subclause 9.6.7.101)*