IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for Clause 9.6.7.101 |
| Date: 2021-01-12 |
| 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.

# Overview of comments

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1304 | 37.00 | 22 | 9.6.7.101 | This frame format does not account for fragmentation | Add a Fragment Hash Values field after the Certificate field, of variable length. Add a description "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." At the end of the last para of the subclause add "The Signature field is not present if the Fragment Index subfield is nonzero." | Revised.Agree with the comment.The Fragment Hash Values field is inserted in Figure 9-bc27.The proposed texts are added.Editor to incorporate changes in<https://mentor.ieee.org/802.11/dcn/21/11-21-0084-00-00bc-resolutions-for-clause-9-6-7-101.docx>. |
| 1053 | 37.00 | 25 | 9.6.7.101 | Action frames already have a sequence number and a fragment number. What is the reason for another protocol for thse two functionalities? Please remove these fields. | As in comment. | Reject.EBCS AP required to cache the Sequence Number to make authentication information for MPDUs. The Sequence Number of the MAC header is assigned in MAC layer. It is not good to treat EBCS Info frame separately. It is better to assign another Sequence Number for this purpose.Additionaly EBCS receivers require to detect loss of EBCS Info frame to authenticate EBCS Data frames correctly. The Sequence Number in MAC header is not applicable to this function.EBCS Info frame uses special fragmentation procedure to guarantee origin authenticity. The Fragment Number in MAC header is not applicable to this purpose. |
| 1117 | 37.00 | 26 | 9.6.7.101 | Definition for "Fragment Hash Values" in subclause 11.100.2.4(P53L31,...), "Fragment Hash (values)" in P54L9, "Fragment Hash Values field in eBCS Info frame" in P59L27 are unclear. I think "Fragment Hash Values field" should be defined as a field in an eBCS Info frame. | 1. Insert Fragment Hash Values field after the eBCS Info Interval field in Figure 9-bc27 eBCS Info frame Action field format.2. Add text for definition of the field.3. Add "field" or "fields" after the terms "Fragment Hash Values" in subclause 11.100.2.4.4. Replace "Fragment Hash value" with "Fragment Hash Value fields" in P54L9. | Revised.Agree with the comment.The Fragment Hash Values field is inserted in Figure 9-bc27.The definition text is added.Editor to incorporate changes in<https://mentor.ieee.org/802.11/dcn/21/11-21-0084-00-00bc-resolutions-for-clause-9-6-7-101.docx>.Defer 3 and 4 until the resolution for clause 11.100.2.4. |
| 1526 | 37.00 | 26 | 9.6.7.101 | The eBCS Info frame is rather difficult to understand as it has many subfields. I'm concerned that with several "Content Information subfields", each of which has several "InstantAuthenticators" this could become a very large frame. | It would be useful to know how many "Content Informartion" subfields can be support within an eBCS Info frame. | Reject.Each Content Information is variable length. The maximum length of MMPDU is defined in the Table 9-25 in the baseline. EBCS Info frame can be fragmented up to 8 fragments. An EBCS Info frame can contain as many as the protocol allows. |
| 1157 | 38.00 | 2 | 9.6.7.101 | Sequence number of eBCS Info frame should not be a MIB variable. | Replace "the current value of dot11eBCSInfoSequence" with "the current value of eBCS Info sequence number".Remove dot11eBCSInfoSequence from Annex C. | Revised.Replace "the current value of dot11eBCSInfoSequence" with "the current value of EBCS Info sequence number".Remove dot11eBCSInfoSequence from Annex C.Editor to incorporate changes in<https://mentor.ieee.org/802.11/dcn/21/11-21-0084-00-00bc-resolutions-for-clause-9-6-7-101.docx>. |
| 1237 | 38.00 | 2 | 9.6.7.101 | The purpose of dot11eBCSInfoSequence is not clear. The description in the MIB says it is written when a MLME-EBCSINFO.request is received. But, these seems to be a local variable used to number the eBCS Info frames. I can see no reason for this to be communicated outside the MAC, nor stored in the MIB. | Change the Sequence Number field explanation to say that each eBCS Info frame that is transmitted has a Sequence Number per 11.100.2.3 (thus implicitly creating a local variable within this context). Delete the dot11eBCSInfoSequence from the MIB. | Revised.Replace "the current value of dot11eBCSInfoSequence" with "the current value of EBCS Info sequence number".Remove dot11eBCSInfoSequence from Annex C.Editor to incorporate changes in<https://mentor.ieee.org/802.11/dcn/21/11-21-0084-00-00bc-resolutions-for-clause-9-6-7-101.docx> |
| 1105 | 38.00 | 3 | 9.6.7.101 | make the timestamp a palindrome | make it elapsed time from 2020-01-10-0202 UTC in milliseconds |  |
| 1524 | 38.00 | 8 | 9.6.7.101 | Figure 9-bc28 has an incorrect title | Change the figure title to "eBCS Info Control field format" |  |
| 1609 | 38.00 | 10 | 9.6.7.100 | the phrase "the total number of the following fragments" is not clear. Please rewrite to make the sentence clear. | as in comment |  |
| 1455 | 38.00 | 14 | 9.6.7.101 | The sentence in line 14 reads "Values of this subfield is defined ..." Since values is in plural "is" should be repolaced with "are" | As in comment |  |
| 1102 | 38.00 | 17 | 9.6.7.101 | allow for trusted raw public keys to be used in lieu of a certificate | at a minimum add a row for a raw EC public key with the algorithm being ECDSA and certificate present being "no". Say that trust is established in a manner outside the standard but describe how to use it in 12.100.2.1. Consider adding a raw RSA key too. |  |
| 1610 | 38.00 | 20 | 9.6.7.100 | No need to indicate eBCS Info frame fragmentation procedure in Clause 9 | remove this sentence or move to the appropriate section |  |
| 1075 | 38.00 | 21 | 9.6.7.101 | The paragraph "The eBCS Info Interval field indicates the eBCS Info frame transmission interval (from dot11eBCSInfoInterval), in units of 100 milliseconds. In the case of PKFA and transmitting irregular time sensitive information, the eBCS Info Interval field is set to 0", indicates the eBCS Info frame may not be periodic. I think the frame must be periodic since in general it is going to advertise multiple services which may or may not use PKFA, therefore it should be mandated periodic. | Consider making it periodic |  |
| 1135 | 38.00 | 22 | 9.6.7.101 | eBCS Info frames are transmitted periodically as described in NOTE. | Remove "In the case of PKFA and transmitting irregular time sensitive information, the eBCS Info Interval field is set to 0." |  |
| 1021 | 38.00 | 23 | 9.6.7.101 | From clause 12.100.1, it is clear that PKFA is used for time-sensitive or aperiodic (infrequent) data. Therefore the text 'and irregular time sensitive information' is not required. | Deleted the cited text |  |
| 1020 | 38.00 | 24 | 9.6.7.101 | The previous paragraph says the eBCS Info Interval field is set to 0 for PKFA. However, the note says that eBCS Info frame is sent periodically for PKFA. Please clarify the periodicity of eBCS Info frames when the for PKFA and aperiodic transmissions. | As in comment |  |
| 1136 | 38.00 | 30 | 9.6.7.101 | DER for X.509 certificate is defined in X.509. | Remove "ITU-T Recommendation X.680 (2002)" |  |
| 1528 | 39.00 | 3 | 9.6.7.101 | Regarding the "Content Information field", it would be more efficient to create a "Instant Authenticator" subframe comprising a singe "Instant Authenticator Hash Distance" and "Instant Authenticator" subfield. | Rearrange Figure 9-bc29 to group the "Instant Authenticator" sub-fields into a separate subframe. Place these subframes as a list at the end of the "Control Information" field. |  |
| 1076 | 39.00 | 4 | Figure 9-bc29 | Negotiation Method is not defined in the text | Define it as in other frames |  |
| 1527 | 39.00 | 4 | 9.6.7.101 | The subfield "Negotiation Method" in Figure 9-bc29 is not defined in the cited clause. | Either remove this subfield or add some descriptive text below the figure. |  |
| 1106 | 39.00 | 11 | 9.6.7.101 | what are the valid values for a Content ID subfield? Can all of the Content IDs be zero? Need the be unique to a transmission? Are they sequential? | define how one decides how to assign a value to this field. |  |
| 1137 | 39.00 | 15 | 9.6.7.101 | The name of Table 9-bc8, "eBCS Info frame Authentication Algorithm subfield" is confusable with Table 9-bc7, "eBCS Info Authentication Algorithm". | Replace "eBCS Info frame Authentication Algorithm subfield" with "Authentication Algorithm subfield".Same change is applied at P39L12. |  |
| 1181 | 39.00 |  | Figure 9-bc29 | Uncentered "Content" in the Figure | Center the "Content" in the Figure with the frame |  |
| 1023 | 40.00 | 8 | 9.6.7.101 | Which destination is the field referring to? In case of DL broadcast, the frames can be received by recipients in the neighborhood in range of the transmitter. Please clarify the intent of the field. | As in comment |  |
| 1022 | 40.00 | 9 | 9.6.7.101 | Doesn't apply to UL broadcast since an UL eBCS frame carries the Destination URI element to specify the remote destination. | Delete the following sentences: "UDP/hostname shall only be used for eBCS UL frames. Others are used for both eBCS DL and UL frames." and update clause 11 to specify that the eBCS Info frame does not apply to UL broadcast (forwarding service). |  |
| 1457 | 40.00 | 14 | 9.6.7.101 | The Content Destination Address Type subfield in Table 9-b9 is the same as in Table 9-bc4. Hence the explanation for the different different content destination address subfield formats is redundant between Subclause 9.4.5.100 and Subclause 9.6.7.101 | Replace "as follows" with "as in 9.5.4.100 (Enhanced Broadcast Services ANQP-element) and delete conent from line 16 page 40 to line 10 page 41. |  |
| 1506 | 40.00 | 18 | 9.6.7.101 | In Figure 9-bc31 the subfield "Destination UDP Port" is not defined in the text. | Add some text to define the "Destination UDP Port" beneath Figure 9-bc31. Alternatively the definition on P45L16 could be moved to the text beneath this figure. |  |
| 1503 | 40.00 | 18 | 9.6.7.101 | In Figure 9-bc31, the subfield "Destination IPv4 Address" is not defined in the text. | Add some text to define the "Destination IPv4 Address" beneath Figure 9-bc31. |  |
| 1507 | 40.00 | 24 | 9.6.7.101 | In Figure 9-bc32 the subfield "Destination UDP Port" is not defined in the text. | Add some text to define the "Destination UDP Port" beneath Figure 9-bc32. Alternatively the definition on P45L16 could be moved to the text beneath this figure. |  |
| 1504 | 40.00 | 24 | 9.6.7.101 | In Figure 9-bc32, the subfield "Destination IPv6 Address" is not defined in the text. | Add some text to define the "Destination IPv6 Address" beneath Figure 9-bc32. |  |
| 1508 | 41.00 | 1 | 9.6.7.101 | In Figure 9-bc33 the subfield "Destination UDP Port" is not defined in the text. | Add some text to define the "Destination UDP Port" beneath Figure 9-bc33. Alternatively the definition on P45L16 could be moved to the text beneath this figure. |  |
| 1525 | 41.00 | 8 | 9.6.7.101 | The current baseline draft 802.11REVmd D5.0 typically does not define a "MAC Address" subfield, for example P1075L58. | Remove Figure 9-bc34 as it is not required. |  |
| 1024 | 41.00 | 13 | 9.6.7.101 | Description of Negotiation Method field is missing | Add description for Negotiation Method field |  |
| 1611 | 41.00 | 19 | 9.6.7.100 | Does "is transmitted again" imply exactly the same information is transmitted? This sentence may be too restricted. In addition, the term Next Schedule is not clear, maybe change it to Next TX Schedule. | change the sentence "The Next Schedule subfield indicates the number of TBTTs until the content by the content ID contained inthe Content ID subfield is transmitted again." into " The Next TX Schedule subfield indicates the number of TBTTs until the expected broadcast of the eBCS identified by the Content ID contained in the Content ID sufield immediately following the current frame." |  |
| 1639 | 41.00 | 32 | 9.6.7.101 | There are two authentication algorithms being indicated in this frame. One is the eBCS Info Authentication Algorithm subfield in the eBCS Info Control field and is specified in Table 9-bc7 eBCS Info Authentication Algorithm subfield. The other is the Authentication Algorithm subfield in the Content Information field and is specifided in Table 9-bc8 eBCS Info frame Authentication Algorithm subfield. Regarding "The length of the HCFA Base Key subfield is determined by the authentication algorithm."on L32, and "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." on L38, it would be nice to 1) clarify which authentication algorithm is being referred here; 2) add a "Length of HCFA Base Key and Previous Period HCFA Base Key 0/1" column in the correct Authentication Algorithm Table (with modified table title and related text), to specify the length of these three Key subfields without requiring a reader to read the relevant standards. | As commended. |  |
| 1458 | 42.00 | 1 | 9.6.7.101 | End of line 1 reads "in unit of 10 milliseconds". Put "unit" in plural | As in comment |  |
| 1379 | 42.00 | 1 | 9.6.7.101 | "The HCFA Key Change Interval subfield indicates the dot11eBCSHCFAKeyChangeInterval in unit of 10 1milliseconds. " -- no, it indicates the HCFA key change interval | Change to "The HCFA Key Change Interval subfield indicates the eBCS HCFA key change interval in unit of 10 milliseconds (see dot11eBCSHCFAKeyChangeInterval). " |  |
| 1025 | 42.00 | 10 | 9.6.7.101 | The term 'Data' in the subfield name is misleading . The content of the frame does not carry broadcast data. Instead, it provides information on the how obtain credentials for the desired service. | Changing the name of the Data subfield to something appropriate that describes the intention of the subfield |  |
| 1640 | 42.00 | 10 | 9.6.7.101 | P40L7 says "The Data Present subfield indicates whether the Data Length field and the Data field are present." So, the Data Length field and the Data field are present together or not present at all, not one depending on the other. But P42L10 seems to say that the presence of the Data field depends on the presence of the Data Length field. | Please clarify. |  |
| 1641 | 42.00 | 12 | 9.6.7.101 | What unit is the value of the Data Length subfield being defined in, Octet? And, is value 0 not used for this subfield, or value 0 represents 1 octet, 1 represents 2 octets, and so on and so forth? | Please specify in a way that clearly answers these questions. |  |
| 1114 | 42.00 | 14 | 9.6.7.101 | It should add Vendor specific length so as to specify the Vendor specific filed length | as comment |  |
| 1459 | 42.00 | 32 | 9.6.7.101 | "... and its contents are outside of this standard." replace with "... and its ontents are outside of the scope of this standard." | As in comment |  |
| 1138 | 43.00 | 1 | 9.6.7.101 | Signature is not generated by the certificate. And it should refer security section. | Remove "that is generated by the certificate of theeBCS transmitter".Add "Details are described in 12.100.2.1 (Signature of the eBCS Info frame)." |  |
| 1139 | 43.00 | 2 | 9.6.7.101 | Use appropriate terminology. | Replace "the public key algorithm of the authentication algorithm" with "the eBCS Info Authentication Algorithm". |  |
| 1642 | 43.00 | 2 | 9.6.7.101 | Again, it would be nice to 1) clarify which authentication algorithm is being referred here, i.e., the one specified in Table 9-bc7 eBCS Info Authentication Algorithm subfield or in Table 9-bc8 eBCS Info frame Authentication Algorithm subfield; 2) add a "Length of Signature" column in the correct Authentication Algorithm Table (with modified Table Title and related text), to specify the length of the Signature field without requiring a reader to read the relevant standards. | As commended. |  |

# 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 | 0 or 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Certificate | Content Information Number | Content Information 1 | 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 of ~~dot11eBCSInfoSequence~~ EBCS Info sequence number [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 eBCS Info Control field format**

The Number Of Fragments subfield indicates the total number of the following fragments of the eBCS Info frame.

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 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).

The eBCS Info Interval field indicates the eBCS Info frame transmission interval (from dot11eBCSInfoInterval), in units of 100 milliseconds. In the case of PKFA and transmitting irregular time sensitive information, the eBCS Info Interval field is set to 0.

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 indicates that a certificate is present, and are not present otherwise.

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

The Certificate field is the X.509 certificate of the eBCS transmitter in the DER format (Distinguished Encoding Rules, ITU-T Recommendation X.680 (2002)).

The Content Information Number field indicates the number of Content Information fields.

…

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)*