IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Modification of eBCS Info frame | | | | |
| Date: 2020-10-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | [hmorioka@src-soft.com](mailto:hmorioka@src-soft.com) |
|  |  |  |  |  |

Abstract

This document proposes modification of eBCS Info frame.

Discussion

Problem in eBCS Info frame

While an eBCS frame is common to all contents in the BSS, current eBCS Info frame specifies authentication type for each content as shown in the Table 9-bc5.

|  |  |
| --- | --- |
| **Value** | **Authentication Algorithm** |
| 0 | HLSA (see 12.15.4 No frame authentication with mandatory higher layer source authentication (HLSA)) |
| 1-15 | reserved |
| 16 | PKFA with RSA-2048 (see 12.15.2 eBCS public key frame authentication (PKFA)) |
| 17 | PKFA with ECDSA-P256 (see 12.15.2 eBCS public key frame authentication (PKFA)) |
| 18 | PKFA with Ed25519 (see 12.15.2 eBCS public key frame authentication (PKFA)) |
| 19-31 | Reserved |
| 32 | HCFA without instant authentication (see 12.15.3 eBCS Hash chain frame authentication (HCFA)) with RSA-2048 and SHAKE128/KMAC128 |
| 33 | HCFA without instant authentication (see 12.15.3 eBCS Hash chain frame authentication (HCFA)) with ECDSA-P256 and SHAKE128/KMAC128 |
| 34 | HCFA without instant authentication (see 12.15.3 eBCS Hash chain frame authentication (HCFA)) with Ed25519 and SHAKE128/KMAC128 |
| 35-47 | Reserved |
| 48 | HCFA with instant authentication (see 12.15.3 eBCS Hash chain frame authentication) with RSA-2048 and SHAKE128/KMAC128 |
| 49 | HCFA with instant authentication (see 12.15.3 eBCS Hash chain frame authentication (HCFA)) with ECDSA-P256 and SHAKE128/KMAC128 |
| 50 | HCFA with instant authentication (see 12.15.3 eBCS Hash chain frame authentication (HCFA)) with Ed25519 and SHAKE128/KMAC128 |
| 51-255 | Reserved |

Public key is used to verify the signature of the eBCS Info frame and PKFA MPDUs, and is delivered in eBCS Info frame.

Public key algorithm should be uniquely specified in the eBCS Info frame and the same algorithm should be used for PKFA.

Resolution

9.6.7.~~1.~~bc2 eBCS Info frame format

The format of the Action field of the eBCS Info frame is shown in Figure 9-bc22 (eBCS Info frame Action field format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | Sequence Number | Timestamp | eBCS Info Control | eBCS Info Interval | Certificate Length |
| Octets: | 1 | 1 | 8 | 8 | 1 | 1 | 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-bc22 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 (Public Action frames).

The Sequence Number field contains the current value of dot11eBCSInfoSequence.

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-bc23 (eBCS Info frame eBCS Info Control field format)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 | B5 | B6 | | B7 |
|  | Number Of Fragments | | | Fragment Index | | | ~~Certificate Present~~ | | ~~Reserved~~ |
| Bits: | 3 | | | 3 | | | ~~1~~ | ~~1~~ | |

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

Figure 9-bc23 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 Certificate Present subfield indicates whether the Certificate Length field, the Certificate field and the Signature field are present.~~

The eBCS Info Authentication Algorithm subfield indicates the algorithm to authenticate the eBCS Info frame. Values of this subfield is defined in Table 9-bc4.5 (eBCS Info Authentication Algorithm subfield).

Table 9-bc4.5 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 11.55.2.3 (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 Certificate Length field, the Certificate field and the Signature field are present if the ~~Certificate Present~~ eBCS Info Authentication Algorithm subfield in the eBCS Control field ~~set to 1~~ indicates that certificate is present, and are not present otherwise.

The Certificate Length field indicates the length of the Certificate field 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)).

(skip)

The Authentication Algorithm subfield is defined in Table 9-bc5 (eBCS Info frame Authentication Algorithm field)

Table 9-bc5 eBCS Info frame Authentication Algorithm subfield

|  |  |
| --- | --- |
| **Value** | **Authentication Algorithm** |
| 0 | HLSA (see 12.bc.4 No frame authentication with mandatory higher layer source authentication (HLSA)) |
| ~~1-15~~ | ~~reserved~~ |
| 1~~6~~ | PKFA ~~with RSA-2048~~ (see 12.bc.2 eBCS public key frame authentication (PKFA)) |
| ~~17~~ | ~~PKFA with ECDSA-P256 (see 12.bc.2 eBCS public key frame authentication (PKFA))~~ |
| ~~18~~ | ~~PKFA with Ed25519 (see 12.bc.2 eBCS public key frame authentication (PKFA))~~ |
| ~~19-31~~ | ~~Reserved~~ |
| ~~3~~2 | HCFA without instant authentication (see 12.bc.3 eBCS Hash chain frame authentication (HCFA)) ~~with RSA-2048 and SHAKE128/KMAC128~~ |
| ~~33~~ | ~~HCFA without instant authentication (see 12.bc.3 eBCS Hash chain frame authentication (HCFA)) with ECDSA-P256 and SHAKE128/KMAC128~~ |
| ~~34~~ | ~~HCFA without instant authentication (see 12.bc.3 eBCS Hash chain frame authentication (HCFA)) with Ed25519 and SHAKE128/KMAC128~~ |
| ~~35-47~~ | ~~Reserved~~ |
| ~~48~~ 3 | HCFA with instant authentication (see 12.bc.3 eBCS Hash chain frame authentication) ~~with RSA-2048 and SHAKE128/KMAC128~~ |
| ~~49~~ | ~~HCFA with instant authentication (see 12.bc.3 eBCS Hash chain frame authentication (HCFA)) with ECDSA-P256 and SHAKE128/KMAC128~~ |
| ~~50~~ | ~~HCFA with instant authentication (see 12.bc.3 eBCS Hash chain frame authentication (HCFA)) with Ed25519 and SHAKE128/KMAC128~~ |
| ~~51~~4-255 | Reserved |

11.bc.2.3 eBCS Info frame generation and usage

The Sequence Number subfield is initialized to a random number at the time of starting an eBCS and incremented by 1 for every new eBCS Info frame transmission. If the Sequence Number overflows, it is set to 0.

If all contents use HLSA, the authentication algorithm of the eBCS Info frame may be none, otherwise the eBCS Info frame shall use RSASSA-PSS, ECDSA or Ed25519.

On reception of an eBCS Info frame, an eBCS non-AP STA shall check the integrity of the eBCS Info frame as described in 12.15 (Frame authentication for eBCS) if the Certificate of the AP is included in the eBCS Info frame.