IEEE P802.11
Wireless LANs

|  |
| --- |
| Draft Text for 9.6.7 eBCS Info Frame |
| Date: 2020-07-07 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
| Antonio de la Oliva | InterDigital | Madrid, Spain |  | aoliva@it.uc3m.es |

Abstract

This document describes a draft text proposal for eBCS Info frame.

*Yellow marked numbers are temporal and to be assigned by ANA.*

2. Normative references

*Add new reference*

ITU-T Recommendation X.680 (2002), Distinguished Encoding Rules

9. Frame formats

9.6 Action frame format details

9.6.7 Public Action details

9.6.7.1 Public Action frames

*Add new entry (and adjust the reserved value) to Table 9-362 as shown below.*

|  |  |
| --- | --- |
| **Public Action field value** | **Description** |
| <ANA> | eBCS Info |
| <ANA+1> - 255 | Reserved |

*Add the following new subclause under 9.6.7*

9.6.7.52 eBCS Info frame format

The format of the Action field of the eBCS Info frame is shown in Figure 9-bc1 (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-bc1 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-bc2 (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 |

**Figure 9-bc2 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 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 subfield in the eBCS Control field is set to 1 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)).

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

The format of each Content Information field is shown in Figure 9-bc3 (Content Information field format).

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

**Figure 9-bc3 Content Information field format**

The Content ID subfield indicates the identifier of the content.

The Authentication Algorithm subfield is defined in Table 9-bc1 (eBCS Info frame Authentication Algorithm field)

**Table 9-bc1 eBCS Info frame Authentication Algorithm subfield**

|  |  |
| --- | --- |
| **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 |

The Content Information Control subfield is shown in Figure 9-bc4 (Content Information Control subfield format)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 | B5 | B6 | B7 |
|  | Time Of Termination Present  | Next Schedule Present | Reserved |
| Bits: | 1 | 1 | 6 |

**Figure 9-bc4 Content Information Control subfield format**

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

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

The Content Destination Address Type subfield is defined in Table 9-bc2 (Content Destination Address Type subfield). UDP/hostname shall only be used for eBCS UL. Others are used for both eBCS DL and UL.

**Table 9-bc2 Content Destination Address subfield**

|  |  |
| --- | --- |
| **Value** | **Higher Layer Protocol** |
| 0 | UDP/IPv4 |
| 1 | UDP/IPv6 |
| 2 | UDP/hostname (UL only) |
| 3 | MPEG transport stream identifier |
| 4 | MAC address |
| 5-7 | Reserved |

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

If the Content Destination Address Type is UDP/IPv4, the format of the Content Destination Address subfield is shown in Figure 9-bc5 (Content Destination Address subfield format for UDP/IPv4).

|  |  |  |
| --- | --- | --- |
|  | Destination IPv4 Address | Destination UDP Port |
| Octets: | 4 | 2 |

**Figure 9-bc5 Content Destination Address subfield format for UDP/IPv4**

If the Content Destination Address Type is UDP/IPv6, the format of the Content Destination Address subfield is shown in Figure 9-bc6 (Content Destination Address subfield format for UDP/IPv6).

|  |  |  |
| --- | --- | --- |
|  | Destination IPv6 Address | Destination UDP Port |
| Octets: | 16 | 2 |

**Figure 9-bc6 Content Destination Address subfield format for UDP/IPv6**

If the Content Destination Address Type is UDP/hostname, the format of the Content Destination Address subfield is shown in Figure 9-bc7 (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.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hostname Length | Hostname | Destination UDP Port |
| Octets: | 1 | variable | 2 |

**Figure 9-bc7 Content Destination Address subfield format for UDP/hostname**

If the Content Destination Address Type is MPEG transport stream identifier, the format of the Content Destination Address subfield is shown in Figure 9-bc8 (Content Destination Address subfield format for MPEG transport stream). The MPEG Transport Stream Length subfield indicates the length of the MPEG Transport Stream subfield. The MPEG Transport Stream subfield is the MPEG transport stream identifier as a UTF-8 string.

|  |  |  |
| --- | --- | --- |
|  | MPEG Transport Stream Length | MPEG Transport Stream |
| Octets | 1 | Variable |

**Figure 9-bc8 Content Destination Address subfield format for MPEG transport stream**

If the Content Destination Address Type is MAC Address, the format of the Content Destination Address subfield is shown in the Figure 9-bc9 (Content Destination Address subfield format for MAC Address). The MAC Address field is the destination MAC Address of the content.

|  |  |
| --- | --- |
|  | MAC Address |
| Octets | 6 |

**Figure 9-bc9 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 Negotiation Method subfield, the Time Of Termination subfield, the Next Schedule subfield will refer the eBCS Termination Notification frame.*

The Allowable Time Difference subfield is present if the Authentication Algorithm is PKFA or HCFA. The value is 8bit unsigned integer that is 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 dot11EBCSHCFAKeyChangeInterval in unit of 10 milliseconds.

The Number Of Instant Authenticators subfield, Instant Authenticator Hash Distance *n* subfields and the Instant Authenticator *n* subfields are present if the Authentication Algorithm field indicates HCFA with instant authentication, and are not present otherwise.

The Number Of Instant Authenticators subfield indicates the number of instant authenticators to be used. 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 Data subfield is present if the Authentication Algorithm field indicates PKFA and the Data Length subfield is present, and is not present otherwise.

The Data Length subfield indicates the length of the Data subfield.

The Data subfield is shown in the Figure 9-bc10 (Data subfield format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Flags | Service URL Length(Optional) | Service URL(Optional) | Vendor specific(Optional) |
| Octets | 1 | 0 or 1 | Variable | variable |

**Figure 9-bc10 Data subfield format**

The Data Flags subfield is shown in Figure 9-bc11 (Data Flags subfield format).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 | B5 | B6 | B7 |
|  | Content With Restriction | Service URL Present | Reserved |
| Bits: | 1 | 1 | 6 |

**Figure 9-bc11 Data Flags subfield format**

The Content With Restriction subfield indicates whether the content requires offline registration to be accessed. The registration process is outside of the scope of this standard.

The Service URL Present subfield indicates that the Service URL Length subfield and the Service URL subfields are present in the Data subfield; they are not present otherwise.

The Service URL Length subfield indicates the number of octets in the Service URL field.

The Service URL field indicates the URL at which information relevant to the corresponding eBCS service might be retrieved, including negotiation or registration for the service, formatted in accordance with IETF RFC 3986.

The Vendor Specific subfield is defined by application specific requirements and its contents are outside of this standard.

The Signature field is the digital signature of the eBCS Info frame that 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.