IEEE P802.11
Wireless LANs

|  |
| --- |
| Draft Text for 9.6.7 eBCS Info Frame |
| Date: 2020-07-XX |
| 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.*

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: | 0 | 1 | 8 | 8 | 1 | 1 | 0 or 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Certificate of the AP | 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 is a 64bit unsigned integer that is dot11EBCSInfoSequence.

The Timestamp field is a 64bit unsigned integer that is the elapsed time from 2020/1/1 0:00 UTC in units of millisecond.

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 in the eBCS Info Control field is a 3bit unsigned integer that is the total number of the fragments of the eBCS Info frame.

The Fragment Index subfield in the eBCS Info Control field is a 3bit unsigned integer that is the fragmentation index of the eBCS Info frame.

The Certificate Present bit is 1 bit in length and indicates the Certificate Length field, the Certificate field and the Signature field exist in the eBCS Info frame.

Fragmentation procedure is described in 11.55.2 (eBCS Info frame generation).

The eBCS Info Interval field is an 8bit unsigned integer that is the interval of the eBCS Info frame transmission interval configured as dot11EBCSInfoInterval in units of 100 millisecond. In case of using 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 bit in the eBCS Control field is set to 1.

The Certificate Length field is a 16bit unsigned integer that is the length of the certificate in units of octet.

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 is an 8bit unsigned integer that indicates the number of the Content Information fields.

The 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 | Next Schedule | Termination Time |
| Octets: | 1 | 0 or 4 | 0 or 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 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 is 1 octet in length and indicates the identifier of the content.

The Authentication Algorithm subfield is an 8bit unsigned integer that is show in Table 9-bc1 (eBCS Info frame Authentication Algorithm field)

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

|  |  |
| --- | --- |
| **Value** | **Authentication Algorithm** |
| 0 | HLSA (12.15.4 No frame authentication with mandatory higher layer source authentication (HLSA)) |
| 1-15 | reserved |
| 16 | PKFA with RSA-2048 (12.15.2 eBCS public key frame authentication (PKFA)) |
| 17 | PKFA with ECDSA-P256 (12.15.2 eBCS public key frame authentication (PKFA)) |
| 18 | PKFA with Ed25519 (12.15.2 eBCS public key frame authentication (PKFA)) |
| 19-31 | reserved |
| 32 | HCFA without instant authentication (12.15.3 eBCS Hash chain frame authentication (HCFA)) with RSA-2048 and SHAKE128/KMAC128 |
| 33 | HCFA without instant authentication (12.15.3 eBCS Hash chain frame authentication (HCFA)) with ECDSA-P256 and SHAKE128/KMAC128 |
| 34 | HCFA without instant authentication (12.15.3 eBCS Hash chain frame authentication (HCFA)) with Ed25519 and SHAKE128/KMAC128 |
| 35-47 | reserved |
| 48 | HCFA with instant authentication (12.15.3 eBCS Hash chain frame authentication) with RSA-2048 and SHAKE128/KMAC128 |
| 49 | HCFA with instant authentication (12.15.3 eBCS Hash chain frame authentication (HCFA)) with ECDSA-P256 and SHAKE128/KMAC128 |
| 50 | HCFA with instant authentication (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 |
|  | Termination Time Present  | Next Schedule Present | Data Present | reserved |
| Bits: | 1 | 1 | 1 | 5 |

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

Bit 0 to 2 of the Content Information Control subfield correspond to the subfields that are conditionally present in the Content Information field.

The Content Destination Address Type subfield is an 8bit unsigned integer that shown in Table 9-bc2 (Content Destination Address subfield). UDP/hostname may be used only 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 (Uplink only) |
| 3 | MPEG Transport stream identifier |
| 4 | MAC Address |
| 5-7 | Reserved |

The Content Destination Address subfield is the higher layer 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 format is shown in the Figure 9-bc5 (Content Destination Address subfield format for UDP/IPv4). The Destination UDP Port subfield is encoded in little endian.

|  |  |  |
| --- | --- | --- |
|  | 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 format is shown in the Figure 9-bc6 (Content Destination Address subfield format for UDP/IPv6). The Destination UDP Port subfield is encoded in little endian.

|  |  |  |
| --- | --- | --- |
|  | 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 format is shown in the 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 in UTF-8. The Destination UDP Port subfield is encoded in little endian.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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, the format of the Content Destination Address subfield format is shown in the 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 in UTF-8.

|  |  |  |
| --- | --- | --- |
|  | 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 format is shown in the Figure 9-bc9 (Content Destination Address subfield format for MAC Address).

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

**Figure 9-bc9 Content Destination Address subfield format for MAC Address**

The Title Length subfield is 8bit unsigned integer that is the length of the following Title subfield in units of octets. The Title subfield is human readable title of the content encoded in UTF-8.

The Negotiation Method subfield is 1 octet in length and indicates the negotiation method for starting or extending the eBCS identified by the Content ID contained in the Content ID subfield. The encoding of the Negotiation Method subfield is defined in Table 9-bc3 (Negotiation Method subfield).

The Next Schedule subfield is present if the Next Schedule Present bit in the Content Information Control subfield is set to 1. The Next Schedule subfield is 4 octets in length and indicates the time to start broadcasting the content in elapsed seconds from 2020/1/1 0:00 UTC.

The Termination Time subfield is present if the Termination Time Present bit in the Content Information Control subfield is set to 1. The Termination Time subfield is 4 octets in length and indicates the time of the content termination in elapsed seconds from 2020/1/1 0:00 UTC.

**Table 9-bc3 Negotiation Method subfield**

|  |  |  |
| --- | --- | --- |
| Negotiation Method subfield value | Meaning | Notes |
| 0 | No Negotiation |  |
| 1 | Negotiation through ANQP/GAS eBCS Request frames |  |
| 2 | Negotiation through IP Request | Out of band IP Request |
| 3-7 | Reserved |  |

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 eBCS transmitter and the eBCS receivers. The unit of the value is millisecond.

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 is HCFA.

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 contains 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 transmitter, 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 filled by 0.

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

The Number of Instant Authenticators subfield, Instant Authenticator Hash Distance *n* subfield and the Instant Authenticator *n* subfield are present if the authentication algorithm is HCFA and instant authentication is used.

The Number of Instant Authenticators subfield is 1 octet in length and indicates the number of the instant authenticators to be used. The Instant Authenticator Hash Distance *n* subfield is 1 octet in length and indicates the hash distance of each instant authenticator. The Instant Authenticator *n* subfield contains the instant authenticator of the following eBCS Data frame of the hash distance that is indicated by the Instant Authenticator Hash Distance *n*.

The Data Length subfield and the Data subfield are present if the authentication algorithm is PKFA and the Data Present bit in the Content Information subfield is set to 1.

The Data Length subfield is 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 | 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 | Vendor Specific Present | Reserved |
| Bits: | 1 | 1 | 1 | 5 |

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

The Content with restriction bit indicates if the content requires of some kind of offline registration to be accessed. The registration process is out of the scope of this document.

The Service URL Present bit indicates that the Service URL Length subfield and Service URL subfield are present in the Data subfield.

The Vendor Specific Present bit indicates that the Vendor Specific subfield is present in the Data subfield.

In the case the Data Flags indicate the Service URL subfield is present, the Service URL Length subfield is a 1octet field whose value is set to the number of octets in the Service URL field.

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

The Vendor specific subfield is to be defined by application specific requirements.

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.