IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Speculative Edits to 802.11bc SFD | | | | |
| Date: 2020-06-05 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Carol Ansley | CommScope | 3871 Lakefield Dr. Suwanee, GA 30024 US | +1 678 473 8630 | carol.ansley@commscope.com |
| Stephen McCann | BlackBerry Ltd | The Pearce Building, West Street, Maidenhead, SL6 1RL, UK | +44 1753 667099 | smccann@blackberry.com |

Abstract

This document contains speculative edits to the r3 version of the Specification Framework Document for 802.11 TGbc.

R0 – document created and updated based on 11-20-0025r4.

R1 – updated based on doc 18/2123r12 motion booklet with Straw Polls #11-#15.

R2 – some editorial corrections and Straw polls #17-#19.

1. Overview

1.3 Supplementary information on purpose

***Insert the following to the end of the list:***

Specifically, in the context of IEEE 802.11™-compliant devices, this standard

....

——Defines a mechanism to enable IEEE 802.11 stations to enable enhanced transmission and reception of broadcast data both in an infrastructure BSS where there is an association between the transmitter and the receiver(s) and in cases where there is no association between transmitter(s) and receiver(s).

1. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

1. Definitions

For the purposes of this document, the following terms and definitions apply. The IEEE Standards Dictionary Online should be consulted for terms not defined in this clause. [[1]](#footnote-1)

**3.2 Definitions specific to IEEE Std 802.11**

**Enhanced Broadcast Service (eBCS) receiver:** An STA that receives Enhanced Broadcast Services (eBCS) frames.

**Enhanced Broadcast Service (eBCS) transmitter:** An STA that transmits Enhanced Broadcast Services (eBCS) frames.

## 3.4 Abbreviations and acronyms

***Insert the following acronym definitions (maintaining alphabetical order):***

**eBCS** Enhanced Broadcast Service

# 4 General Description

## 4.3 Components of the IEEE Std 802.11 architecture

***Insert a new subclause after subclause 4.3.30 as follows:***

### **4.3.31 Enhanced Broadcast Service**

[Motion #62] Enhanced Broadcast Service (eBCS) enables efficient distribution of local information. eBCS provides enhanced transmission and reception of broadcast data both in an infrastructure BSS where there is an association between the transmitter and the receiver(s) and in cases where there is no association between transmitter(s) and receiver(s).

eBCS provides additional means for protecting broadcast traffic and the privacy of the stations receiving that traffic, including protection of origin authenticity between STAs that use a group temporal key security association (GTKSA) for broadcast transmissions.

The main features of eBCS are the following:

-TBD

4.5 Overview of the services

4.5.4 Access control and data confidentiality services

*Change the nth paragraphs as follows:*

*<The current IEEE Std. 802.11 has a group temporal key security association (GTKSA) security framework for multicast that does not protect origin authenticity between devices having that GTKSA. Such protection is needed in some broadcast use cases.>*

# **6 Layer Management**

## **MLME SAP interface**

**6.3.<ANA1> eBCS Info transmission**

*Describe MLME SAP for eBCS Info frame transmission.*

6.3.<ANA2> eBCS Info reception

*Describe MLME SAP for eBCS Info frame reception.*

# 9 Frame Formats

* **Beacon frame format**

|  |  |  |
| --- | --- | --- |
| * **Beacon frame body** | | |
| **Order** | **Information** | **Notes** |
| <ANA> | E-BCS UL Capabilities | This element is optionally present if dot11eBCSSupportImplemented is true. |

* **Probe Response frame format**

|  |  |  |  |
| --- | --- | --- | --- |
| * **Probe Response frame body** | | | |
| **Order** | **Information** | **Notes** |
| <ANA> | E-BCS UL Capabilities | This element is optionally present within a broadcast Probe Response frame if dot11eBCSSupportImplemented is true. |

## 9.4.2 Elements

#### 9.4.2.1 General

***Insert the following new rows into Table 9-77 (Element IDs) (header row shown for convenience):***

Table 9-77 -- Element IDs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| eBCS Parameters | 255 | <ANA> | Yes |  |
| E-BCS UL Capabilities | 255 | <ANA> | Yes | No |
| E-BCS Container | 255 | <ANA> | Yes |  |
|  |  |  |  |  |

#### 9.4.2.27 Extended Capabilities element

**Table 9-134—Extended Capabilities element**

|  |  |  |
| --- | --- | --- |
| **Bits** | **Information** | **Notes** |
| <ANA> | eBCS Support | A STA sets the eBCS Support field to 1 when dot11eBCSSupportImplemented is true. Otherwise, the STA sets the eBCS Support field to 0. |

***Insert the following subclauses:***

**9.4.2.X E-BCS UL Capabilities element**

**9.4.2.X.1 General**

The E-BCS UL Capabilities element contains fields that are used to advertise the capabilities of an eBCS STA related to forwarding service to a remote destination.

An eBCS AP declares support for forwarding service and related capabilities by including the E-BCS UL Capabilities element in a Beacon and broadcast Probe Response frame.

An eBCS non-AP STA can include the E-BCS UL Capabilities element in an E-BCS UL frame if it intends to provide its capabilities to an AP that forwards its data to a remote destination.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | E-BCS UL Capabilities |
| Octets: | 1 | 1 | 1 | variable |

**Figure 9-<BC-1> - E-BCS UL Capabilities element format**

The format of E-BCS UL Capabilities element is shown in Figure 9-<BC-1> (E-BCS UL Capabilities element format).

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The contents of an E-BCS UL Capabilities field is defined in 9.4.2.X.2 when the element is transmitted by an eBCS AP and defined in 9.4.2.X.3 when the element is transmitted by an eBCS non-AP STA.

**9.4.2.<ANA>.2 E-BCS AP UL Capabilities**

The format of an E-BCS UL Capabilities field when transmitted by an eBCS AP is shown in Figure 9-<BC-2> (Format of E-BCS UL Capabilities field for an AP).

|  |  |
| --- | --- |
|  | UL AP Control |
| Octet: | 2 |

**9-<BC-2> - Format of E-BCS UL Capabilities field for an AP**

The format of UL AP Control is shown in Figure 9-<BC-3> (UL AP Control field format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | B0 B1 | B2 B3 | B4 | B5 | B6 | B7 B15 |
|  | Authentication Mode | Limiting Mode | Location Embedding Supported | Data-Time Embedding Supported | IP Address Embedding Supported | Reserved |
| Bits: | 2 | 2 | 1 | 1 | 1 | 9 |

**9-<BC-3> - UL AP Control field format**

The encoding of Authentication Mode subfield is shown in Table 9-<BC-4> (Encoding of Authentication Mode subfield).

**Table 9-<BC-4> - Encoding of Authentication Mode subfield**

|  |  |  |
| --- | --- | --- |
| Subfield value | Definition | Encoding |
| 0 | No Authentication | AP forwards contents of an E-BCS UL frame to the remote destination identified in the frame without authenticating the transmitter of the frame. |
| 1 | Per Destination | AP forwards contents of an E-BCS UL frame only if it is able to successfully able to authenticate the transmitter of the frame based on an established relationship with the remote destination identified in the frame. |
| 2 – 3 | Reserved |  |

The encoding of Limiting Mode subfield is shown in Table 9-<BC-5> (Encoding of Limiting Mode subfield).

**Table 9-<BC-5> - Encoding of Limiting Mode subfield**

|  |  |  |
| --- | --- | --- |
| Subfield value | Definition | Encoding |
| 0 | No Throttling | AP applies no restrictions on the amount/frequency of ULs from a non-AP STA destined to a remote destination. |
| 1 | Per Destination | AP applies forwarding limits as specified by the remote destination with whom it has established a relationship. |
| 2 – 3 | Reserved |  |

Location Embedding Supported subfield is set to 1 if the AP supports embedding of location information, based on a non-AP STA’s request, before forwarding the HLP payload carried in an E-BCS UL frame to the remote destination. Otherwise, the subfield is set to 0.

Date-Time Embedding Supported subfield is set to 1 if the AP supports embedding of date and time information, based on a non-AP STA’s request, before forwarding the HLP payload carried in an E-BCS UL frame to the remote destination. Otherwise, the subfield is set to 0.

IP Address Embedding Supported subfield is set to 1 if the AP supports embedding of IP address information, based on a non-AP STA’s request, before forwarding the HLP payload carried in an E-BCS UL frame to the remote destination. Otherwise, the subfield is set to 0.

**9.4.2.X.3 E-BCS Non-AP UL Capabilities**

The format of an E-BCS UL Capabilities field when transmitted by an eBCS non-AP STA is shown in Figure 9-<BC-6> (Format of E-BCS UL Capabilities field for a non-AP STA).

|  |  |
| --- | --- |
|  | UL Non-AP STA Control |
| Octets: | 1 |

**9-<BC-6> - Format of E-BCS UL Capabilities field for a non-AP STA**

The format of UL Non-AP STA Control is shown in Figure 9-<BC-7> (UL Non-AP STA Control field format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 B7 |
|  | No forwarding Without Embedding | Location Embedding Requested | Date-Time Embedding Requested | IP Address Embedding Requested | Reserved |
| Bits: | 1 | 1 | 1 | 1 | 4 |

**9-<BC-7> - UL Non-AP STA Control field format**

The No Forwarding Without Embedding subfield is set to 1 to indicate that the AP is not required to forward the contents of the frame transmitted by non-AP STA to the remote destination if it cannot append the requested information before forwarding. Otherwise the subfield is set to 0.

The Location Embedding Requested subfield is set to 1 to indicate that the non-AP STA transmitting the element is requesting an eBCS AP that will forward its content to the remote to append location information before forwarding. Otherwise the subfield is set to 0.

The Date-Time Embedding Requested subfield is set to 1 to indicate that the non-AP STA transmitting the element is requesting an eBCS AP that will forward its content to the remote to append date and time information before forwarding. Otherwise the subfield is set to 0.

The IP Address Embedding Requested subfield is set to 1 to indicate that the non-AP STA transmitting the element is requesting an eBCS AP that will forward its content to the remote to append AP’s IP address information before forwarding. Otherwise the subfield is set to 0.

**9.4.2.<ANA> E-BCS Container [Motion #49]**

The element carries:

* A field for carrying higher layer data
  + Can carries the ID of the transmitting STA
* Other fields TBD

9.4.2.248 eBCS Parameters

The enhanced Broadcast Services (eBCS) Parameters element contains:

* A list of one or more eBCS services offered by the AP
* Indication whether one or more eBCS services requires association
* Indication of negotiation method for eBCS services: e.g., through eBCS Request/Response frames (e.g., for associated STAs), or through ANQP exchanges (e.g., for unassociated STAs) [Motion 48]

**9.4.5 Access network query protocol (ANQP) elements: [Motion #38]**

Add the following elements:

* Define a new “Broadcast Capability” ANQP-element for eBCS services advertisement
  + ANQP-element should indicate 0, 1, or multiple eBCS services
  + This element could contain broadcast channel and timing information (e.g. time of transmission)
  + Note: Since ANQP uses GAS, this provides both an unassociated and an association query/response mechanism (protected using Protected Dual of Public Action frames)
  + Note: GAS is bi-directional between two STAs and hence works on both the uplink and downlink.
  + The typical operation for a device would be to transmit a Broadcast Capability ANQP-element request to another device, and then the other device would respond with a Broadcast Capability ANQP-element response containing the required information, if the other device supports a broadcast capability.

* Define a new “Broadcast Switching” ANQP-element for requesting and reporting about switching broadcast channels on and off.
  + ANQP-element could request switching broadcast channels on and off.
  + Note: Since ANQP uses GAS, this provides both an unassociated and an association query/response mechanism (protected using Protected Dual of Public Action frames)
  + Note: GAS is bi-directional between two STAs and hence works on both the uplink and downlink.
  + The typical operation for a device would be to transmit a Broadcast Switching ANQP-element request to another device, with appropriate sub-fields set for the required action, and then the other device would respond with a Broadcast Switching ANQP-element response containing the required information, including error codes.

**9.4.5.1 General** (Straw Poll #12)

**Add the following three new entries at the base of Table 9-330, before the Vendor Specific entry.**

Table 9-330— ANQP-element definitions

|  |  |  |
| --- | --- | --- |
| ANQP-element name | InfoID | ANQP-element (subclause) |
| Enhanced Broadcast Services | <ANA> | 9.4.5.bc |
| Enhanced Broadcast Request | <ANA+1> | 9.4.5.bc1 |
| Enhanced Broadcast Response | <ANA+2> | 9.4.5.bc2 |

***Add the following three new clauses after 9.4.5.29.***

**9.4.5.bc. Enhanced Broadcast Services ANQP-element**

The Enhanced Broadcast Services ANQP-element provides a list of one or more enhanced broadcast services that are available from a peer STA. The format of the Enhanced Broadcast Services ANQP-element is defined in Figure 9-828bc (Enhanced Broadcast Services ANQP-element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | Info ID | Length | Broadcast | Enhanced Broadcast Services  Tuples |
| Octets: | | 2 | 2 | 1 | variable |
|  | **Figure 9-838bc Enhanced Broadcast Services ANQP-element format** | | | | |

The Info ID and Length fields are defined in 9.4.5.1 (General).

The Broadcast field is a 1 octet bitmap advertising information and is defined in Table 9-838bc:

**Table 9-838bc – Broadcast field values**

|  |  |
| --- | --- |
| **Bit** | **Description (when bit set to 1)** |
| 0 | No enhanced broadcast capability |
| 1 | Enhanced broadcast service indicated by each Enhanced Broadcast Services Tuple field |
| 2 | Transmit an Enhanced Broadcast Request ANQP-element to register/de-register to/from broadcast service |
| 3 | Multiple enhanced broadcast services supported, transmit an Enhanced Broadcast Request ANQP-element for more information. |
| 4 | Registration is required to received broadcast |
| 5 - 7 | Reserved |

The Enhanced Broadcast Services Tuples field contains one or more Enhanced Broadcast Services Tuple fields as shown in Figure 9-838bc1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Length | Broadcaster MAC Address  (Optional) | Broadcast Stream Information  (Optional) | BroadcastTime Length  (Optional) | Broadcast Time  (Optional) | Broadcast Duration  Length  (Optional) | Broadcast Duration  (Optional) |
| Octets: | 1 | 6 | variable | 1 | variable |  |  |

**Figure 9-838bc1 - Enhanced Broadcast Services Tuple field format**

The Length field is a 1-octet field whose value is set to the total length of the optional fields.

The Broadcaster MAC Address field optionally indicates the MAC Address of the STA broadcasting this channel, in the case of a multi STA setup.

The Broadcast Stream Information field is used to identify the source of the broadcast stream information (e.g. as a channel number, OFDMA sub-channel [TBD - check name] or URL), when the value of the Broadcast field bit 1 is true (see Table 9-838bc).

The Broadcast Time Length field is an optional 1-octet field who value is set to the length of the Broadcast Time field. If the Broadcast Time field is not used, the Broadcast Time Length field is also not used.

The Broadcast Time field contains timing information about when the broadcast (indicated by the Broadcast Stream Information field) is available, in terms of real time and whether the broadcast repeats. The format of the Broadcast Time field is TBD. If the Broadcast Time field is not present, then the receiving STA can assume that the broadcast stream is always available.

The Broadcast Duration Length field is an optional 1-octet field who value is set to the length of the Broadcast Duration field. If the Broadcast Duration field is not used, the Broadcast Time Duration field is also not used.

The Broadcast Duration filed contains information about the duration of a broadcast (indicated by the Broadcast Stream Information field) in terms of duration. The format of the Broadcast Duration field is TBD. The Broadcast Duration field is only present, when there is a Broadcast Time field also present.

[Note: the Broadcast Time and Broadcast Duration fields could be merged into a single Broadcast Schedule field]

**9.4.5.bc1. Enhanced Broadcast Request ANQP-element**

The Enhanced Broadcast Request ANQP-element provides a list of one or more enhanced broadcast services that are available from a peer STA. The format of the Enhanced Broadcast Request ANQP-element is defined in Figure 9-828bc2 (Enhanced Broadcast Request ANQP-element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Info ID | | Length | Broadcast  Action | Enhanced Broadcast Services  Tuples  (Optional) |
| Octets: | 2 | | 2 | 1 | variable |
|  | | **Figure 9-838bc2 - Enhanced Broadcast Request ANQP-element format** | | | |

The Info ID and Length fields are defined in 9.4.5.1 (General).

The Broadcast Action field is a 1 octet bitmap and is defined in Table 9-838bc1:

**Table 9-838bc1 – Broadcast Action field values**

|  |  |
| --- | --- |
| **Bit** | **Description (when bit set to 1)** |
| 0 – 1 | Reserved |
| 2 | Register to receive broadcast |
| 3 | Unregister from receiving broadcast |
| 4 | Register with Broadcast Service(s) as indicated in the Enhanced Broadcast Services Tuples field |
| 5 | Unregister Broadcast Service(s) as indicated in the Enhanced Broadcast Services Tuple field |
| 6 - 7 | Reserved |

The Enhanced Broadcast Services Tuples field is described in 9.4.5.bc.

**9.4.5.bc2. Enhanced Broadcast Response ANQP-element**

The Enhanced Broadcast Response ANQP-element provides a list of one or more enhanced broadcast services that are available from a peer STA. The format of the Enhanced Broadcast Response ANQP-element is defined in Figure 9-828bc3 (Enhanced Broadcast Response ANQP-element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | Info ID | Length | Broadcast  Action Response | Enhanced Broadcast Services  Tuples  (Optional) |
| Octets: | | 2 | 2 | 1 | variable |
|  | **Figure 9-838bc3 - Enhanced Broadcast Response ANQP-element format** | | | | |

The Info ID and Length fields are defined in 9.4.5.1 (General).

The Broadcast Action Response field is a 1 octet bitmap and is defined in Table 9-838bc2:

**Table 9-838bc2 – Broadcast Action Response field values**

|  |  |
| --- | --- |
| **Bit** | **Description (when bit set to 1)** |
| 0 | Success |
| 1 | Failure |
| 2 - 7 | Reserved |

The Enhanced Broadcast Services Tuples field is described in 9.4.5.bc.

9.6 Action frame format details

9.6.7 Public Action details

9.6.7.1 Public Action frames

*Insert the following new rows into Table 9-363 (Public Action field values) in numeric order:*

**Table 9-363 – Public Action field values**

|  |  |
| --- | --- |
| Public Action field value | Description |
| <ANA> | E-BCS UL |
| <ANA> | eBCS Termination Notice |
| <ANA> | eBCS Info |

*Add eBCS Info frame to Table 9-362.*

9.6.7.X E-BCS UL frame format

The E-BCS UL frame is transmitted by an eBCS non-AP STA carrying data intended for a remote destination identified in the frame. The format of E-BCS UL frame Action field is shown in Figure 9-<BC> (E-BCS UL frame Action field format).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | E-BCS UL Control | HLP Payload Length | HLP Payload | STA Certificate Length | STA Certificate | Timestamp |
| Octets: | 1 | 1 | 1 | 2 | variable | 0 or 2 | 0 or variable | 0 or 8 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Destination URI | E-BCS UL Capabilities | Frame Signature Length | Frame Signature |
| Octets: | variable | 0 or 4 | 0 or 2 | 0 or variable |

Figure 9-<BC-8> - E-BCS UL 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).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| B0 | B1 | B2 | B3 | B4 B6 | B7 |  |
|  | STA Certificate Present | Packet Number Present | E-BCS UL Capabilities Present | Timestamp Present | Reserved | Frame Signature Present |
| Bits: | 1 | 1 | 1 | 1 | 3 | 1 |

**9-<BC-9> - EBCS UL Control field format**

The format of E-BCS UL Control field is shown in Figure 9-<BC-9> (E-BCS UL Control field format).

The STA Certificate Present subfield is set to 1 when the STA Certificate Length and STA Certificate fields are carried in the frame. Otherwise the subfield is set to 0.

The Packet Number Present subfield is set to 1 when the Packet Number field is carried in the frame. Otherwise the subfield is set to 0.

The E-BCS UL Capabilities Present subfield is set to 1 when the E-BCS UL Capabilities element is carried in the frame. Otherwise the subfield is set to 0.

The Timestamp Present subfield is set to 1 when the Timestamp field is carried in the frame. Otherwise the subfield is set to 0.

The Frame Signature Present subfield is set to 1 when the Frame Signature Length and Frame Signature fields are carried in the element. Otherwise the subfield is set to 0.

The HLP Payload Length indicates the length of the HLP Payload field.

The HLP Payload field carries the higher layer protocol (HLP) payload.

The STA Certificate Length field indicates the length of the STA Certificate field. The presence of this field is indicated by the STA Certificate Present subfield in the E-BCS UL Control field being equal to 1.

The STA Certificate field carries the certificate of the transmitting STA. The presence of this field is indicated by the STA Certificate Present subfield in the E-BCS UL Control field being equal to 1.

The Timestamp field provides protection against replay attack. The presence of this field is indicated by the Timestamp Present subfield in the E-BCS UL Control field being equal to 1.

The format of the Timestamp field is shown in Figure 9-<BC-10> - Timestamp field format.

|  |  |  |
| --- | --- | --- |
|  | Time | Counter |
| Octets: | 4 | 4 |

**9-<BC-9> - Timestamp field format**

The 32 bit Time subfield carries time information. See clause 11.X.Y.3 (E-BCS UL operation at an eBCS non-AP STA) for details on the value carried in this subfield.

The 32 bit Counter subfield carries a numeric value which is incremented for each packet transmission.

The Destination URI element is defined in 9.4.2.89 (Destination URI element) and carries the address of the remote destination where the packet needs to be forwarded to.

Note: The length of the Destination URI element is computed based on the value carried in the Length field in the element (value in Length field + 2 octets).

The E-BCS UL Capabilities element is defined in 9.4.2.X (E-BCS UL Capabilities element). The element is optionally present and carries the capabilities of the transmitting non-AP STA. The presence of this element is indicated by the E-BCS UL Capabilities Present subfield in the E-BCS UL Control field being equal to 1.

The Frame Signature Length field indicated the length of the Frame Signature field. The presence of this field indicated by the Frame Signature Present subfield in the E-BCS UL Control field being equal to 1.

The Frame Signature field carries signature for the contents of the E-BCS UL frame Action field except the Frame Signature field. The presence of this field indicated by the Frame Signature Present subfield in the E-BCS UL Control field being equal to 1.

**9.6.7.<ANA5> 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.

**9.6.31 eBCS Service Request Frame**

This frame is used by associated STAs to request eBCS services.

TGbc shall define a mechanism for STAs to negotiate durations of services when negotiating for one or more eBCS services.

Note: The transmitter of an eBCS service is expected to have authority on the duration of the eBCS service and can respond with an eBCS Response frame (9.6.32) (Straw Poll #13)

**9.6.32 eBCS Service Response Frame**

This frame is used by an eBCS AP to respond to an eBCS services Request frame by an associated STA.

**9.6.33 eBCS Service Advertisement Frame**

This frame is used to periodically advertise the services provided by the eBCS AP.

A transmitter of an eBCS service can advertise a schedule (periodicity and duration) of one or more eBCS service. (Straw Poll #15)

**9.6.34 eBCS Termination Notice Frame**

The eBCS Termination Notice frame is transmitted by a STA that is a transmitter of eBCSs to announce the termination of one or more of the eBCSs transmitted by the STA. (Straw Poll #14) The format of the eBCS Termination Notice frame Action field is shown in Figure 9-xxx (eBCS Termination Notice frame Action field format).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Category | Public Action | eBCS Termination Information Set |
| Octets: | 1 | 1 | variable |
|  | Figure 9-xxx--eBCS Termination Notice 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 eBCS Termination Information Set field contains one or more of eBCS Termination Info subfield.

The format of the eBCS Termination Info subfield is shown in Figure 9-xxx (eBCS Termination Info subfield format.)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | eBCS  Termination Info Control | Content ID | Title  Length | Title | Time To  Termination | Request Method | Destination Address Type | Destination  Address |
| Octets: | | 1 | 1 | 0 or 1 | variable | 2 | 1 | 0 or 1 | variable |
|  | Figure 9-xxx--eBCS Termination Info subfield format | | | | | | | | | |

The format of the eBCS Termination Info Control subfield is shown in Figure 9-xxx (eBCS Termination Info Control subfield format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | B0 | B1 | B2 | B3 B7 | |
|  | | Title Presence Indicator | Destination  Address  Presence Indicator | Association Required | Reserved | |
| bits: | | 1 | 1 | 1 | 5 | |
|  | Figure 9-xxx--eBCS Termination Info Control subfield format | | | | |

The value 1 in the Title Presence Indicator subfield indicates that a Title Length subfield and a Title subfield are present in the same eBCS Termination Info subfield. The value 0 indicates that a Title Length subfield and a Title subfield are not present in the same eBCS Termination Info subfield.

The value 1 in the Destination Address Presence Indicator subfield indicates that Destination Address Type subfield and a Destination Address subfield are present in the same eBCS Termination Info subfield. The value 0 indicates that an Destination Address Type subfield and an Destination Address subfield are not present in the same eBCS Termination Info subfield.

The value 1 in the Association Required subfield indicates that association is required to consume the eBCS identified by the Content ID contained in the Content ID subfield. The value 0 indicates that association is not required to consume the eBCS identified by the Content ID ID contained in the Content ID subfield.

The Content ID subfield is 1 octet in length and indicates the ID of the eBCS to be terminated.

The Title Length subfield is 1 octet in length indicates the length of the Title subfield in octets.

The Title subfield indicates the Title in UTF-8 format of the eBCS identified by the Content ID contained in the Content ID subfield.

The Time To Termination subfield is 2 octets in lengths and indicates the number of TBTTs until the eBCS identified by the Content ID contained in the Content ID subfield is terminated. The value 0 indicates that the eBCS identified by the Content ID in the Content ID subfield will be terminated at the following TBTT. The value 65535 indicates that the eBCS identified by the Content ID in the Content ID subfield has no specific termination time.

Note – The Time To Termination subfield indicates the expected termination time for the transmitter STA of the eBCS and does not indicate the expected termination time of the content associated with the eBCS.

The Request Method subfield is 1 octet in length and indicates the request method to request extension of the eBCS identified by the Content ID contained in the Content ID subfield. The encoding of the Request Method subfield is defined in Table 9-xxx (Request Method subfield encoding).

|  |  |  |
| --- | --- | --- |
| Table 9-xxx—Request Method subfield encoding | |  |
| Negotiation Method subfield value | Meaning | Notes |
| 0 | No Negotiation |  |
| 1 | Request through eBCS Request frames | eBCS request by STAs that are associated with the broadcaster |
| 2 | Request through ANQP/GAS eBCS Request frames | eBCS request by STAs that are not associated with the broadcaster |
| 3 | Request through IP Request | Out of band IP Request |
| 4-255 | Reserved |  |

The Destination Address Type subfield is 1 octet in length and indicates the type of the address included in the Destination Address subfield. The encoding of the Destination Address Type subfield is defined in Table 9-xxx (Destination Address Type subfield encoding).

|  |  |
| --- | --- |
| Table 9-xxx—Destination Address Type subfield encoding | |
| Destination Address Type value | Meaning |
| 0 | MAC Address |
| 1 | UDP/IPv4 Address |
| 2 | UDP/IPv6 Address |
| 3 | UDP/Hostname |
| 4-255 | Reserved |

The Destination Address subfield indicates the address to be used for negotiating for the extension of the eBCS identified by the Content ID contained in the Content ID subfield. The format and the length of the Destination Address subfield depends on the value contained in the Destination Address Type subfield.

The Destination Address subfield contains a MAC address if the Destination Address Type is equal to 0.

The format of the Destination Address subfield when the Destination Address Type is equal to 1 is shown in Figure 9-xxx (Destination Address subfield format if the Destination Address Type is equal to 1).

|  |  |  |  |
| --- | --- | --- | --- |
|  | IPv4 Address | | Destination UDP Port |
| octets: | 4 | | 2 |
|  | | Figure 9-xxx—Destination Address subfield format if the Destination Address Type is equal to 1 | | |

The IPv4 Address subfield indicates an IPv4 address used for negotiating the extension of the eBCS.

The Destination UDP Port subfield indicates the UDP Port associated with the IPv4 address indicated in the IPv4 Address subfield in little endian format.

The format of the Destination Address subfield when the Destination Address Type is equal to 2 is shown in Figure 9-xxx (Destination Address subfield format if the Destination Address Type is equal to 2).

|  |  |  |
| --- | --- | --- |
|  | IPv6 Address | Destination UDP Port |
| octets: | 16 | 2 |
|  | Figure 9-xxx—Destination Address subfield format if the Destination Address Type is equal to 2 | | |

The IPv6 Address subfield indicates an IPv6 address used for negotiating the extension of the eBCS.

The Destination UDP Port subfield indicates the UDP Port associated with the IPv6 address indicated in the IPv6 Address subfield in little endian format.

The format of the Destination Address subfield when the Destination Address Type is equal to 3 is shown in Figure 9-xxx (Destination Address subfield format if the Destination Address Type is equal to 3).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hostname Length | Hostname | Destination UDP Port |
| octets: | 1 | Variable | 2 |
|  | Figure 9-xxx—Destination Address subfield format if the Destination Address Type is equal to 3 | | | |

The Hostname Length subfield indicates the length of the Hostname subfield in octets.

The Hostname subfield indicates the host name for negotiating the extension of the eBCS in UTF-8 format.

The Destination UDP Port subfield indicates the UDP Port associated with the host name indicated in the Hostname subfield in little endian format.

**10. MAC sublayer functional description**

**10.6 Multirate support**

**10.6.5 Rate selection for Data and Management frame**

***Insert the following subclauses:***

**10.6.5.3 Rate selection for eBCS frames [Motion # 51][Motion 61]**

The transmission rate for eBCS Info frames and eBCS Data frames are determined from dot11EBCSInfoTxRate and dot11EBCSDataTxRate respectively, if FMS or GCR is not used, otherwise follow clause 10.\*\*\*.

Dot11EBCSInfoTxRate and dot11EBCSDataTxRate are configurable item and the values are selected from any available rates other than DSSS.

*Renumber 10.6.5.3 to 10.6.5.4:*

**10.6.5.4 Rate selection for other group addressed Data and Management frames**

*Change the 1st paragraph as follows:*

This subclause describes the rate selection rules for group addressed Data and Management frames, excluding

the following:

— Non-STBC Beacon and non-STBC PSMP frames

— ER beacon and HE beacon

— STBC group addressed Data and Management frames

— Data frames located in an FMS stream (see 11.22.8 (FMS multicast rate processing))

— Group addressed frames transmitted to the GCR concealment address (see 11.22.16.3.5 (Concealment of GCR transmissions))

— Group addressed Data and Management frames transmitted in an HE ER SU PPDU (see 26.15.5 (Additional rules for ER beacons and group addressed frames))

— Group addressed Data and Management frames transmitted in an HE SU PPDU (see 26.15.6 (Additional rules for HE beacons and group addressed frames))

— Group addressed Data and Management frames transmitted in an HE MU PPDU (see 26.15.7 (Additional rules for group addressed frames in an HE MU PPDU))

— eBCS Info, Data and Service Discovery frames

# 11 MLME

### 11.55 Enhanced Broadcast Service (eBCS) procedures

***Insert the following subclauses:***

11.55.1 Overview

This subclause describes enhanced Broadcast Services (eBCS) procedures that are used for eBCS STAs. eBCS is only supported in a non-DMG non-S1G infrastructure BSS.

eBCS can be used for both directions, downlink (eBCS DL) and uplink (eBCS UL). eBCS DL means broadcast from an eBCS AP to eBCS non-AP STAs. eBCS UL means broadcast from an eBCS non-AP STA to eBCS APs.

**11.22.6.2 eBCS Request and Response Procedure**

The eBCS procedures allow a STA and its associated AP to negotiate eBCS service provided.

**11.22.6.3 eBCS Service Advertisement Procedure**

The eBCS Service Advertisement frame allows associated and unassociated stations to discover services provided by the eBCS AP.

11.55.2 eBCS DL procedures

11.55.2.1 General

The eBCS DL uses three types of frame authentication mechanism as following.

* PKFA (12.15.2 Public Key Frame Authentication)
* HCFA (12.15.3 Hash Chain Frame Authentication)
* HLSA (12.15.4 No frame authentication with mandatory higher layer source authentication)

eBCS DL uses both eBCS Info frames and eBCS Data frames.

In addition to these frames, Management frames are optionally used.

The frame sequence is shown in Figure 11-bc1 (eBCS DL frame sequence).

スクリーンショット が含まれている画像

自動的に生成された説明

**Figure 11-bc1 eBCS DL frame sequence**

11.55.2.2 eBCS DL capability indications

The eBCS AP shall include the eBCS Capability element (9.4.2.\* eBCS Capability element) in Beacon and Probe Response frames. The eBCS Capability element indicates the next eBCS Info transmission time in units of Beacon Interval. For example, when the next eBCS Info transmission time is 5, the eBCS Info frame will be transmitted between next 5th Beacon and 6th Beacon.

When the eBCS non-AP STA that is scanning eBCS APs receives the Beacon frame or the Probe Response frame that include the eBCS Capability element, the eBCS non-AP STA should wait for the next eBCS Info. The eBCS non-AP STA may go into power save mode or move to other channel while waiting the next eBCS Info frame.

11.55.2.3 eBCS Info frame generation and usage

The eBCS Info frame is transmitted periodically in the interval of dot11BeaconPeriod \* dot11EBCSInfoInterval.

The eBCS Info frame contains the following information.

* eBCS Info Sequence Number
* Timestamp
* Fragment Control
* Fragment Hash Values (if fragmented)
* eBCS Info Interval
* Certificate of the AP (optional if HLSA is used for all contents, otherwise mandatory)
* Content Information
* Signature (optional if HLSA is used for all contents, otherwise mandatory)

The eBCS Info Sequence Number is initialized by a 64bit unsigned integer at the time of starting eBCS AP and incremented by every eBCS Info frame generation. If the eBCS Info Sequence Number overflows, it is set to 0.

The Timestamp is the time in UTC of generating the eBCS Info frame.

The Fragment Control indicates the total number of the fragmented frames and the index of the eBCS Info frame. The fragmentation procedure is described in 11.55.2.4 (eBCS Info fragmentation).

The Fragment Hash Values are present if the eBCS Info frame is fragmented and the fragment sequence number is 0.

The eBCS Info Interval is the interval of the eBCS Info transmission configured in dot11EBCSInfoInterval.

The Certificate of the AP is the X.509 certificate of the eBCS AP.

Details of the Signature is described in 12.15 (Frame authentication for eBCS).

An eBCS Info frame may contain multiple Content Information.

Each Content Information contains the following items.

* Authentication Algorithm
* Allowable Time Difference
* Broadcast Service ID
* Title
* Negotiation method
* Higher Layer Destination Address
* Time to Termination
* Next Schedule
* HCFA Base Key (in case of HCFA)
* Previous Period HCFA Base Keys (in case of HCFA, optional)
* HCFA Key Change Interval (in case of HCFA)
* Instant Authenticators (in case of HCFA, optional)
* Data (in case of PKFA, optional)

The Authentication Algorithm is either PKFA or HCFA with the public key algorithm and hash algorithm if required.

The Allowable Time Difference is the allowable time difference between the eBCS AP and the eBCS non-AP STAs. It depends on the frame authentication algorithm.

The Broadcast Service ID is the identifier of the content.

The Title is the human readable title of the content.

The Negotiation method is used to indicate the negotiation method that should be used to negotiate for the continuation of the broadcast service beyond the time of termination.

The Higher Layer Destination Address is the higher layer destination address of the content.

The Time to Termination is used to indicate the remaining time left until the content will terminate unless additional negotiation is conducted by the initiator of the broadcast service or by other users of the content.

The Next Schedule is used to indicate the next time the content is scheduled to be transmitted.

The HCFA Base Key, the Previous Period HCFA Base Keys and the Instant Authenticators are used only in HCFA. The details are described in 12.15.3 (eBCS hash chain frame authentication (HCFA)).

The Data is the piggy-backed data. It is used only in PKFA.

On reception of the eBCS Info frame, the 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.

If the integrity of the eBCS Info frame is verified, the eBCS non-AP STA processes each Content Information according to the Authentication Algorithm.

* Common in all authentication algorithms,
  + Cache the Title, the Negotiation Method, the Higher Layer Destination Address, the Time to Termination and the Next Schedule.
  + Notify the cached information to SME through SME-MLME SAP as described in 6.3.\* (eBCS Content Information).
* In case of PKFA,
  + If the Data is present in the Content Information, forward the MSDU in the Data to higher layer. Otherwise, the Certificate in the eBCS Info frame shall be cached.
* In case of HCFA,
  + The HCFA Base Key in the Content Information shall be cached.
  + If the Instant Authenticators are present in the Content Information, the Instant Authenticators shall be cached.
  + If the Previous Period HCFA Base Keys are present in the Content Information, authenticate the eBCS Data frames of the previous HCFA period.

11.55.2.3 eBCS Info frame fragmentation (or in 10.4)

An eBCS Info frame may be fragmented into multiple MPDUs. The length of each fragment shall be equal number of octets for all fragments except the last, which may be smaller. The length of each fragment shall be an even number of octets, except for the last fragment. The length of a fragment shall never be larger than dot11FragmentationTreshold.

The fragmentation procedure is following.

1. Construct an eBCS Info frame and determine the length of fragments.
2. When the eBCS Info frame is fragmented to N MPDUs, the fragmentation number is set to N-1.
3. Insert a space for N-1 Fragment Hash Values to the eBCS Info frame.
4. Each fragment contains the eBCS Sequence Number, the Timestamp and the Fragment Control.
5. Divide the eBCS Info frame after the Fragment Hash Values into fragments.  
   The Fragment Hash Values, the Certificate and the Signature shall be contained in the first fragment.
6. The fragmentation number in the Fragment Control is set to the number of the fragments.
7. The fragmentation index in the Fragment Control is set to 0 (the first) to N-1 (the last) respectively.
8. Calculate the hash value of each fragment except the first one and put into the Fragment Hash Values.
9. Calculate and fill the signature of the first fragment.
10. Transmit the fragments consecutively.

The eBCS Info frame fragmentation is shown in Figure 11-bc2 (eBCS Info frame fragmentation).

**11.X.Y eBCS UL Service**

**11.X.Y.1 General**

The eBCS UL Service procedure allows a non-AP STA to transmit an UL frame with the expectation that one or more eBCS APs in the neighborhood might forward the contents of the frame to a remote destination specified in the frame. An eBCS non-AP STA may include a request to the forwarding AP to append additional information before forwarding to the remote destination. The forwarding service is best effort with no guarantee that the contents are delivered to the remote destination identified in the STA’s UL frame. Furthermore, a STAs request to embed metadata may not be fulfilled by a forwarding AP.

**11.X.Y.2 E-BCS UL operation at an eBCS AP**

An eBCS AP may provide forwarding service in which it can support forwarding the contents of an E-BCS UL frame received from an eBCS non-AP STA to a remote destination identified in the frame.

An eBCS AP that supports forwarding service shall declare its ability to forward by include E-BCS UL Capabilities element (see 9.4.2.xx.2 (E-BCS AP UL Capabilities)) in the Beacon and broadcast Probe Response frames that it transmits.

An eBCS AP that supports forwarding and is capable of embedding the requested metadata shall indicate its ability to support embedding by setting the corresponding subfield in the E-BCS UL Capabilities element to 1 and shall append the requested metadata to the content received from the STA before forwarding it to the remote destination. Format TBD.

An eBCS AP that supports forwarding but doesn’t support embedding of the requested metadata shall not forward the frame to the remote destination if the No Forwarding Without Embedding subfield in the E-BCS UL Capabilities element carried in the E-BCS UL frame is set to 1. Otherwise the AP shall forward the frame to the remote destination identified in the frame.

An eBCS AP may authenticate the transmitter of the packet before forwarding it to a remote destination and shall provide an indication of the authentication scheme in the E-BCS Capabilities element that it transmits. An eBCS AP that does not require authentication of the transmitter shall forward the frame to the remote destination indicated in the frame irrespective of whether the frame carries the STA Certificate field or the Packet Number field or the Frame Signature field. In order to prevent DoS or injection attacks directed towards the remote destination, it is strongly recommended that eBCS APs that support forwarding service perform source authentication and validate the frame signature.

An eBCS AP may limit the amount/frequency of ULs it forwards to a remote destination and shall provide an indication of the throttling scheme in the E-BCS UL Capabilities element that it transmits.

NOTE – Forwarding service is best effort and an eBCS AP, that supports forwarding service, is not required to forward a STA’s data to the destination identified in the STA’s E-BCS UL frame if the conditions indicated by the AP (such as authentication and/or throttling) are not satisfied or for other reasons.

**11.X.Y.3 E-BCS UL operation at an eBCS non-AP STA**

An eBCS non-AP STA that desires to send data to a remote destination may perform an unsolicited broadcast of an E-BCS UL frame carrying data intended for a remote destination. The URI to the remote destination would be carried in the frame. The frame may also carry additional request from the transmitting STA to the forwarding AP.

The format of the E-BCS UL frame is described in 9.6.7.x (E-BCS UL Frame Format).

The STA shall include the higher layer data intended for the remote destination in the HLP Payload field of the E-BCS UL frame.

The STA may include in the E-BCS UL frame fields (such as STA Certificate, Timestamp and Frame Signature) for authentication, preventing replay attack and protecting the contents of the frame.

The STA Certificate field when present in the frame shall carry the certificate of the transmitting STA.

The Timestamp field when present in the frame carries timing information to prevent reply attack.

When the STA has time information, the Time subfield of the Timestamp field shall carry the number of seconds since 2020-01-01 00:00:00 UTC; otherwise the subfield shall be set to 0.

NOTE – How a STA obtains time information is out of scope of this standard.

The Counter subfield of the Timestamp field shall carry a numeric value which is incremented for each packet transmission. In the rare scenario where the STA has transmitted 232 – 1 frames, the value in the field wraps around and starts from 0.

The STA shall include the Destination URI element in the E-BCS UL frame to provide the address of the remote destination where the packet needs to be forwarded to.

An eBCS non-AP STA may include E-BCS Capabilities element (see 9.4.2.xx.3 (E-BCS Non-AP UL Capabilities)) to request embedding of one or more metadata by the forwarding eBCS AP before forwarding the content to the remote destination identified in the frame.

The Frame Signature field when present in the frame shall carry the signature for the contents of the E-BCS UL frame Action field except for the field itself. The contents of the field provide protection against any attack that attempts to tamper the content of the frame.

An eBCS non-AP STA may monitor the WM to gather capabilities of nearby eBCS APs and may conform to the requirements indicated by neighboring eBCS AP(s) that support forwarding service. An eBCS non-AP STA may transmit an E-BCS UL frame without obtaining any information about nearby eBCS AP(s).

NOTE – Forwarding service is best effort and an eBCS non-AP STA is not required to scan or conform to the capabilities of a neighbor eBCS AP that supports forwarding service.

**11.<ANA8>.<ANA9> eBCS Info frame generation and usage**

**11.<ANA8>.<ANA9>.1 eBCS Info frame transmission**

*Describe eBCS Info frame transmission procedure.*

**11.<ANA8>.<ANA9>.2 eBCS Info frame reception**

*Describe eBCS Info frame reception procedure.*

**11.<ANA8>.<ANA10> eBCS Data frame generation and usage**

**11.<ANA8>.<ANA10>.1 eBCS Data frame transmission**

*Describe eBCS Data frame transmission procedure.*

**11.<ANA8>.<ANA10>.2 eBCS Data frame reception**

*Describe eBCS Data frame reception procedure.*

11.22.6.x eBCS Negotiation Procedure for Associated STAs

The transmitter of an eBCS determines whether it will continue broadcasting the requested eBCS service.

11.22.6.x eBCS Termination Notice Procedure

The eBCS Termination Notice Procedure allows a STA that is a broadcaster of eBCSs to indicate that one or more eBCSs that it is broadcasting is to be terminated.

An eBCS STA that is the broadcaster of one or more eBCSs shall start to transmit eBCS Termination Notice frames if one or more eBCS that it is transmitting will terminate within an interval that is equal to or shorter than dot11eBCSTerminationNoticeTime, if the STA is not periodically transmitting a schedule for the eBCSs that are to be terminated. If the eBCS STA starts to transmit eBCS Termination Notice frames, the STA shall transmit the eBCS Termination Notice frames with a period that is larger than dot11eBCSTerminationNoticeMinimumInterval and smaller than dot11eBCSTerminationNoticeMaximumInterval.

The eBCS STA transmitting an eBCS Termination Notice frame indicates in the Time To Termination subfield in a eBCS Termination Info subfield the number of TBTTs before the eBCS identified by the Content ID contained in the Content ID subfield in the same eBCS Termination Info subfield terminates.

The eBCS STA transmitting an eBCS Termination Notice frame shall indicate in the Request Method subfield in a eBCS Termination Info subfield the reqeust method that a STA should use to negotiate for the extension of the eBCS identified by the Content ID contained in the Content ID subfield in the same eBCS Termination Info subfield.

The eBCS STA transmitting an eBCS Termination Notice frame may indicate in the Destination Address subfield in a eBCS Termination Info subfield the address associated with the request method indicated in the Request Method subfield in the same eBCS Termination Info subfield that a STA should use to negotiate for the extension of the eBCS identified by the Content ID contained in the Content ID subfield in the same eBCS Termination Info subfield.

After transmitting a eBCS Termination Notice frame, a eBCS STA shall transmit an eBCS Termination Notice frame with an updated value in the Time To Termination subfield in an eBCS Termination Info subfield if the eBCS identified by the Content ID in the Content ID subfield in the same eBCS Termination Info subfield subfield has been negotiated to another duration or with a new Time To Termination value. If the negotiated duration for the eBCS is longer than the maximum Time To Termination value, the transmitting STA shall set the Time To Termination subfield to 65535.

An eBCS STA that receives an eBCS Termination Notice frame may negotiate for the extension of an eBCS if the eBCS indicated in one of the eBCS Termination Info subfield terminates earlier than desired. The eBCS STA may negotiate the extension of the eBCS using the request method as indicated in the Request Method in the eBCS Termination Info subfield and follow the procedures defined in 11.22.6.x (eBCS Negotiation Procedure for Associated STAs) and 11.23.3.3 (ANQP Procedures).

An eBCS STA shall skip the transmission of any eBCS Request frame or a frame containing an Enhanced Broadcast Request ANQP-element requesting for an eBCS if the STA receives an eBCS Termination Notice frame with an acceptable Time To Termination value contained in the eBCS Termination Info subfield containing the Content ID of the eBCS.

**11.23.3.3 ANQP procedures**

Add behavior text about the 2 new ANQP-elements suggested in clause 9.4.5

# 12 Security (Straw Poll #11)

*Add the following new subclause in clause 12.*

**12.15 Frame authentication for eBCS**

**12.15.1 General**

eBCS provides one-way frame authentication mechanisms that do not require key negotiation between a transmitter and receivers.

eBCS DL cases use one of the following four types of frame authentication.

* Public Key Frame Authentication (PKFA)
* Hash Chain Frame Authentication (HCFA) with Instant Authentication
* Hash Chain Frame Authentication (HCFA) without Instant Authentication
* No frame authentication with mandatory higher layer source authentication (HLSA)

eBCS UL cases use PKFA or HLSA.

While PKFA is suitable for occasional small data transfer or time sensitive data transfer, HCFA is suitable for continuous content distribution such as live streaming or periodic file transfer.

The following preparations are required for both PKFA and HCFA before starting eBCS.

* The certificate(s) of the CA(s) (Certificate Authority) shall be installed into the eBCS receivers.  
  Note: The certificate of the CA(s) may be installed with an application like a content browser. The installation method is out of scope of this standard.
* The eBCS transmitter generates its own private key and public key pair. The public key shall be signed by one of the CAs for which the eBCS receiver(s) have the certificate.

**12.15.2 eBCS public key frame authentication (PKFA)**

**12.15.2.1 Signature of the eBCS Info frame**

One of the following public key algorithms is used.

* RSA-2048
* ECDSA-P256
* Ed25519

The eBCS transmitter generates an eBCS Info frame when it receives data to be transmitted. The eBCS Info frame contains the following items.

* eBCS Info sequence number
* Timestamp
* Authentication algorithm
* Allowable time difference
* Length of the Certificate of the AP
* Certificate of the AP
* Content Information
* (Data)
* Signature

If the length of the eBCS Info frame is larger than the maximum MMPDU length (Table 9-25 Maximum data unit sizes (in octets) and durations (in microseconds)), the eBCS Info frame shall be fragmented as described in 11.55.\* (eBCS Info fragmentation).

If the eBCS Info frame is not fragmented, fill all the fields according to 9.6.7.52 (eBCS Info frame format) except the signature.

Generate signature as follows:

Signature = Sign(The eBCS transmitter’s private key, SHAKE128(Transmitter’s MAC address | from the Sequence Number field to the last Content Information field in the eBCS Info frame))

Otherwise, only the first fragment contains the signature.

Signature = Sign(The eBCS transmitter’s private key, SHAKE128(Transmitter’s MAC address | from the Sequence Number field to the last of the first fragment))

And compute the hash value(s) for the following fragment(s).

HashValue = SHAKE128(Transmitter’s MAC address | from the Sequence Number field to the last of the fragment) (1)

The output length of SHAKE128 is 256bit.

Then the eBCS transmitter transmits the eBCS Info frame.

**12.15.2.2 Authentication of the eBCS Info frame**

When the eBCS receiver receives the eBCS Info frame, the eBCS receiver shall authenticate it as follows:

1. If the eBCS Info frame is fragmented, the following procedures are applied only to the first fragment.
2. If the difference between the timestamp in the eBCS Info frame and the time of the eBCS receiver is greater than the allowable time difference in the eBCS Info frame, the eBCS Info frame shall be discarded.
3. Verify the certificate of the AP in the eBCS Info frame with the installed certificate of the CA. If the verification fails or the certificate of the CA that signed the certificate of the AP in the eBCS Info frame is not installed, the eBCS Info frame shall be discarded.
4. Verify the signature in the eBCS Info frame with the certificate of the AP in the eBCS Info frame. If the verification fails, the eBCS Info frame shall be discarded.

If the authentication succeeds,

* The eBCS receiver caches the certificate of the AP and the allowable time difference in the eBCS Info frame.
* If data is present in the Content Information, the eBCS receiver processes the data in the Content Information field(s) in accordance with 11.55.\* (eBCS Info frame reception).

If the eBCS Info frame is fragmented, the eBCS receiver caches the hash value(s) of the fragment(s) and the eBCS receiver shall authenticate the following fragment(s) as following.

1. Compute the hash value of the fragment as described in the formula (1) in 12.15.2.1(Signing).
2. If the computed hash value is equal to the cached hash value, the authentication succeeds. Otherwise, the fragment shall be discarded.

If the authentication succeeds, the eBCS receiver defragments the eBCS Info frame as described in 11.55.\* (eBCS Info frame defragmentation).

**12.15.2.3 Signature of the eBCS Data frame**

The eBCS Data frame contains the following items.

* Data
* Timestamp
* Signature

Each eBCS Data frame shall be signed using the certificate of the eBCS transmitter as following.

Signature = Sign(The eBCS transmitter’s private key, SHAKE128(Transmitter’s MAC address | */\* to be determined \*/*))

**12.15.2.4 Authentication of an eBCS Data frame**

When an eBCS receiver receives an eBCS Data frame, the eBCS receiver shall authenticate it as follows:

1. If the difference between the timestamp in the eBCS Data frame and the time of the eBCS receiver is greater than the cached allowable time difference, the eBCS Data frame shall be discarded.
2. Verify the signature in the eBCS Data frame using the cached certificate. If the verification fails, the eBCS Data frame shall be discarded.

If the authentication succeeds, the eBCS receiver processes the data in the eBCS Data frame.

**12.15.2.5 Signature of the eBCS UL frame**

One of the following public key algorithms is used.

* RSA-2048
* ECDSA-P256
* Ed25519

The eBCS transmitter generates an E-BCS UL frame when it receives data to be transmitted. The format of the E-BCS UL frame is described in 9.6.7.X (E-BCS UL frame format).

The signature is generated as following:

Signature = Sign(The eBCS transmitter’s private key, SHAKE128(Transmitter’s MAC address | from the Sequence Number field to the last field before the Frame Signature Length field in the E-BCS UL frame))

Then the eBCS transmitter transmits the E-BCS UL frame.

**12.15.2.2 Authentication of an eBCS UL frame**

When an eBCS receiver receives an E-BCS UL frame, the eBCS receiver shall authenticate it as follows:

1. If the Timestamp is present and the difference between the timestamp in the E-BCS UL frame and the time of the eBCS receiver is greater than the configured value, the E-BCS UL frame shall be discarded.
2. Verify the certificate of the STA in the E-BCS UL frame using the installed certificate of the CA. If the verification fails or the certificate of the CA that signed the certificate of the STA in the E-BCS UL frame is not installed, the E-BCS UL frame shall be discarded.
3. Verify the signature in the E-BCS UL frame using the certificate of the STA in the E-BCS UL frame. If the verification fails, the E-BCS UL frame shall be discarded.

If the authentication succeeds,

* The eBCS receiver processes the HLP Payload as described in 11.X.Y.2 (E-BCS UL operation at an eBCS AP).

**12.15.3 eBCS hash chain frame authentication (HCFA)**

**12.15.3.1 General**

HCFA uses a digital signature and a modified TESLA (Timed Efficient Stream Loss-Tolerant Authentication, IETF RFC4082).

HCFA is a one-way key chain authentication mechanism. The eBCS transmitter generates HCFA base keys and HCFA authentication keys for each content stream before each eBCS Info frame generation. SHAKE128 hash function is used for HCFA key generation. The output length of SHAKE128 is 256bit.

The HCFA base keys (*Bs,n*) are generated as follows:

*Bs,0* = Random value (256bit length)

*Bs,n* = SHAKE128(“eBCS HCFA base key” || *Bs,n-1*) (*n* >= 1)

where *s* is the sequence number of the generating eBCS Info frame.

The HCFA authentication keys (*A s,n*) are generated as follows:

*As,n* = SHAKE128(“eBCS HCFA authentication key” || *Bs,n*)

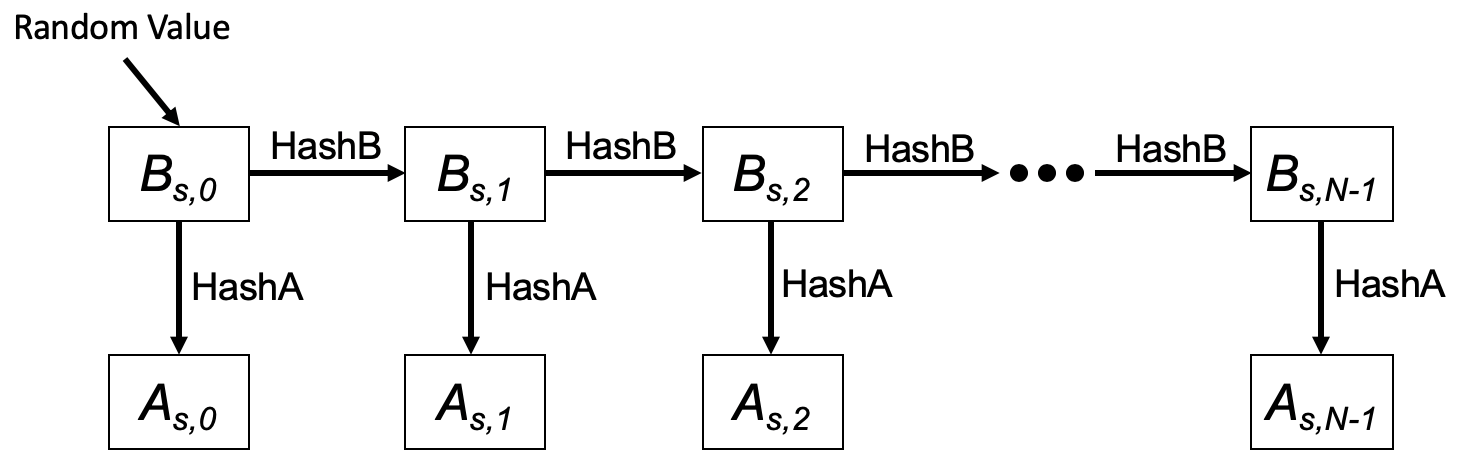
where *s* is the sequence number of the generating eBCS Info frame.

The number of the keys to be generated (*N*) is following:

*N* = *TI* / *TK* + 3

where *TI* is the eBCS Info frame transmission interval and *TK* is the HCFA key change interval.

The HCFA key generation scheme is shown in Figure 12-bc1 (HCFA key generation scheme).



**Figure 12-bc1 HCFA key generation scheme**

In this figure, HashB is the hash function to generate HCFA base keys and HashA is the hash function to generate HCFA authentication keys.

HCFA keys are generated for each content stream.

HCFA provides the following two authentication methods to authenticate each eBCS Data frame.

* HCFA authentication
* Instant authentication (optional)

Each authentication method uses a separate authenticator. HCFA authentication uses the HCFA authenticator, and the instant authentication uses the instant authenticator. The instant authenticator is optionally used to filter the malicious eBCS Data frames.

The HCFA authenticator is the KMAC128 (NIST Special Publication 800-185) value of the eBCS Data frame that contains the HCFA authenticator with HCFA authentication key.

HCFA Authenticator = KMAC128(*An*, eBCS Data frame including Instant Authenticator)

The instant authenticator is the hash value of the eBCS Data frame to be transmitted later that is generated as following:

Instant Authenticator = SHAKE128(eBCS Data frame to be transmitted later)

The HCFA uses both eBCS Info frames (9.6.7.52 eBCS Info frame format) and eBCS Data frames (/\* reference to be added \*/). The frame sequence is shown in Figure 12-bc2 (eBCS HCFA frame sequence).

文字が書かれているスクリーンショット

自動的に生成された説明

**Figure 12-bc2 eBCS HCFA frame sequence**

The eBCS Info frames are transmitted periodically in the interval of dot11EBCSInfoInteval (*TI*). *TK* is the HCFA key change interval configured as dot11EBCSHCFAKeyChangeInterval. *TI* shall be a multiple of *TK*. The period between one eBCS Info frame and the next eBCS Info frame is called the “HCFA period”. Each HCFA period is identified by the HCFA sequence number.

Each content stream has an index that is determined by the order, starting with index 0, in the Content Information field in the eBCS Info frame.

The period that uses the same HCFA authentication key is called a “Key period”. Each Key period has its sequence number, Key sequence number, starting with 0 at the beginning of each HCFA period. Note that the Key sequence number is different from HCFA key indexes.

Each eBCS Data frame has a sequence number starting from 0 at the beginning of each Key period. The eBCS Data frame is identified by the following identifiers:

* HCFA sequence number
* Content stream index
* Key sequence number
* Data sequence number

eBCSData(*s*, *c*, *k*, *d*) represents the eBCS Data frame in which the HCFA sequence number is *s*, the Content stream index is *c*, the Key sequence number is *k* and the Data sequence number is *d*. IAuth(*s*, *c*, *k*, *d*) and HAuth(*s*, *c*, *k*, *d*) represent the instant authenticator and the HCFA authenticator for the eBCSData(*s*, *c*, *k*, *d*) respectively. eBCSInfo(*s*) represents the eBCS Info frame for which the HCFA sequence number is *s*.

For example, in case of two content streams, Content A and Content B, the identifiers are shown in Figure 12-bc3 (Identifiers example).

文字と写真のスクリーンショット

自動的に生成された説明

**Figure 12-bc3 Identifiers example**

The index of the HCFA base key and the HCFA authentication key is defined as B(*s, c, k*) and A(*s, c, k*) respectively where *s* is the HCFA sequence number, *c* is the content index, *k* is the Key sequence number. The Key sequence number is different from the HCFA base/authentication key index. The HCFA base/authentication keys are used in the opposite order of the HCFA key generation. The relation between the HCFA base/authentication key index and the HCFA sequence number is shown in Table 12-bc1 (Relation between HCFA authentication key index and HCFA sequence number) where N is the number of HCFA authentication keys generated. An example of the HCFA key delivery is shown in Figure 12-bc4 (Example HCFA Key Delivery).

**Table 12-bc1 Relation between HCFA base/authentication key index and HCFA sequence number**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HCFA base/authentication key index | (N-1) | (N-2) | (N-3) | N-4 | N-5 | N-6 | … | 0 |
| HCFA sequence number | (-3) | (-2) | (-1) | 0 | 1 | 2 | … | N-4 |

Note: HCFA sequence number -3, -2 and -1 are used only for key verification.

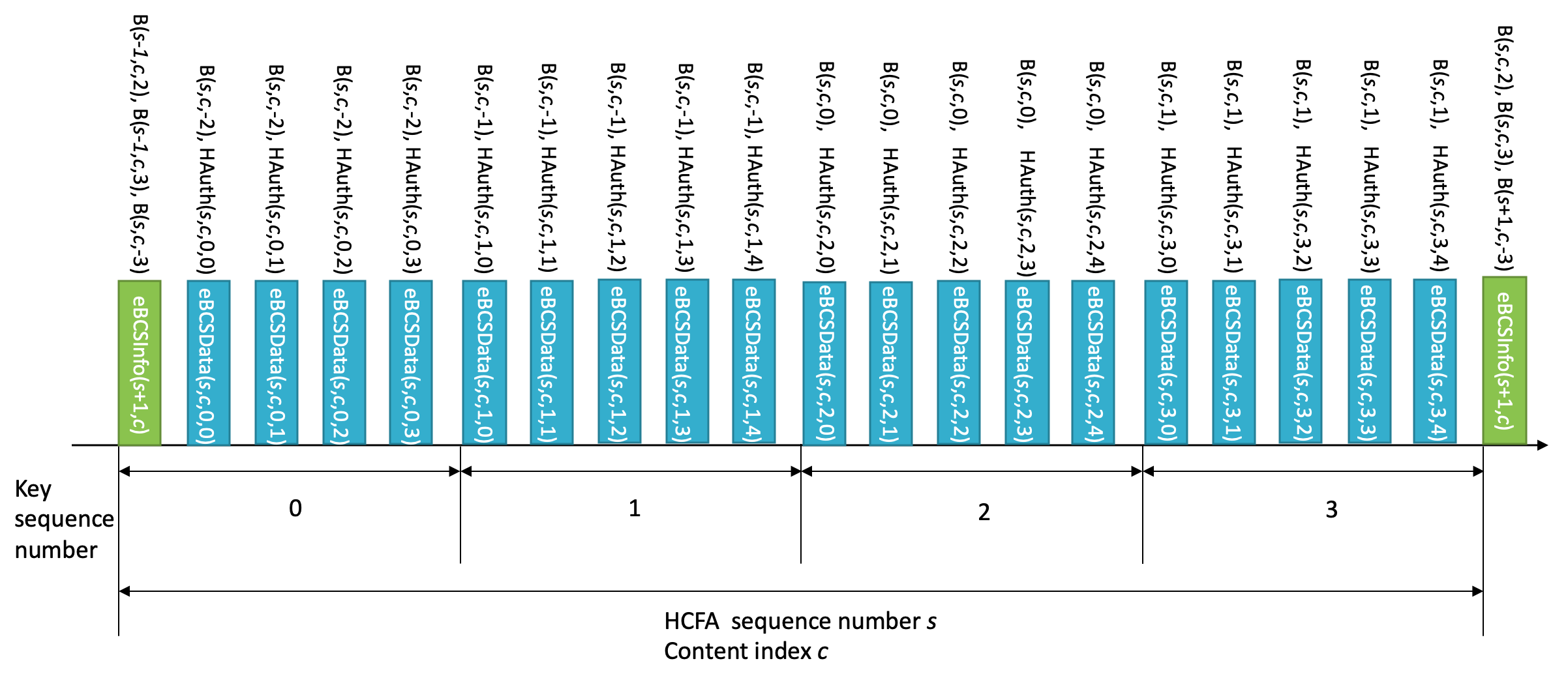


Figure 12-bc4 Example HCFA Key Delivery

An eBCS Info frame and an eBCS Data frame may contain multiple instant authenticators. For example, eBCSData(*s, c, k, d*) may contain IAuth(*s, c, k, d*+1) and IAuth(*s, c, k, d*+3). In this case, the values 1 and 3 are called Hash Distances. The Hash Distance is configured in dot11EBCSHCFAHashDistance. Each instant authenticator is delivered with the frame identifier (*s, c, k, d*). An example of the instant authenticator delivery is shown in Figure 12-bc5 (Example Instant Authenticator Delivery).

スクリーンショット が含まれている画像

自動的に生成された説明

Figure 12-bc5 Example Instant Authenticator Delivery

**12.15.3.2 eBCS Info frame generation**

An eBCS Info frame contains the following items that are related to frame authentication.

* HCFA sequence number
* Timestamp
* Certificate
* Signature
* HCFA key change interval
* Content Information
  + HCFA base key(s)
  + Instant authenticator(s) of eBCS Data frames to be transmitted (optional)

The functions of the eBCS Info sequence number, the timestamp, the certificate and the signature are same as those of PKFA.

The HCFA key change interval, HCFA base key(s) and the instant authenticator(s) are present only in HCFA.

The HCFA key change interval is *TK*.

The HCFA base keys to be included in the eBCS Info frame of sequence number *s* are B(*s*, *c*, -3), B(*s*-1, *c*, 1) and B(*s*-1, *c*, 0) for all content streams, where *c* is the content index. In case of the first eBCS Info frame, B(*s*-1, *c*, 1) and B(*s*-1, *c*, 0) are not present.

If instant authentication is used, the instant authenticator(s) with frame identifier (*s, c, k, d*) is present. In this case, the eBCS transmitter must buffer data packets to generate instant authenticators.

If the length of the eBCS Info frame is larger than the maximum MMPDU length (Table 9-25 Maximum data unit sizes (in octets) and durations (in microseconds)), the eBCS Info frame shall be fragmented as described in 11.55.\* (eBCS Info fragmentation).

**12.15.3.3 eBCS Data frame generation**

The eBCS Data frame contains the following items.

* Content data
* HCFA sequence number
* Content index
* Key sequence number
* Data sequence number
* HCFA base key
* Instant authenticator(s)
* HCFA authenticator

The HCFA sequence number, the Content index, the Key sequence number and the Data sequence number are described in 12.15.3.1 (General).

The HCFA base key contained in eBCSData(*s*, *c*, *k*, *d*) is B(*s*, *c*, *k*-2).

The instant authenticator(s) in the eBCSData(*s*, *c*, *k*, *d*) depends on the configured Hash Distance.

The HCFA authenticator in the eBCSData(*s*, *c*, *k*, *d*) is HAuth(*s*, *c*, *k*, *d*) with A(*s*, *c*, *k*).

**12.15.3.4 eBCS Info frame reception**

A received eBCS Info frame, eBCSInfo(*s*), is processed as following.

1. If the eBCS Info frame is fragmented, defragment it at first as described in 11.55.\* (eBCS Info defragmentation).
2. If the difference between the timestamp in the eBCS Info frame and the time in the eBCS receiver’s clock is greater than the HCFA key change interval in the eBCS Info frame, the eBCS Info frame shall be discarded.
3. Verify the certificate of the AP in the eBCS Info frame using the installed certificate of the CA. If the verification fails or the certificate of the CA that signed the certificate of the AP in the eBCS Info frame is not installed, the eBCS Info frame shall be discarded.
4. Verify the signature in the eBCS Info frame using the certificate of the AP in the eBCS Info frame. If the verification fails, the eBCS Info frame shall be discarded.
5. If the HCFA base key(s) of the previous HCFA period, B(*s*-1, *c*, *N*-4) and B(*s*-1, *c*, *N*-5), is included and the eBCS Data frames of the previous HCFA period to be authenticated are present, authenticate and process the eBCS Data frames as described in 12.15.3.5 (eBCS Data frame reception).
6. Cache the HCFA base key(s), B(*s*, *c*, 0), for the HCFA period of the eBCS Info frame.
7. If the instant authenticator(s) are present, cache the instant authenticators contained in the eBCS Info frame.

**12.15.3.4 eBCS Data frame reception**

eBCS Data frames shall be discarded until a eBCS Info frame from the BSS is received.

A received eBCS Data frame, eBCSData(*s*, *c*, *k*, *d*), is processed as following.

1. Compute B(*s*, *c*, *k*-3) from B(*s*, *c*, *k*-2) in the eBCSData(*s*, *c*, *k*, *d*). If the computed B(*s*, *c*, *k*-3) is different from the cached B(*s*, *c* , *k*-3), the eBCS Data frame shall be discarded.
2. If instant authentication is used and the instant authenticator of the eBCSData(*s*, *c*, *k*, *d*), IAuth(*s*, *c*, *k*, *d*), is cached, compute the hash value of the eBCSData(*s*, *c*, *k*, *d*). If the computed hash value is different from the cached instant authenticator, the eBCS Data frame shall be discarded.
3. If instant authentication is used and the instant authenticator of the eBCSData(*s*, *c*, *k*, *d*), IAuth(*s*, *c*, *k*, *d*), is not cached, the eBCS Data frame may be cached until the HCFA base key for the Key period is received, or the eBCS Data frame may be discarded.
4. If instant authentication is not used, the eBCS Data frame shall be cached until the HCFA base key for the Key period is received.
5. If eBCS Data frame(s) using the HCFA authentication key derived from the HCFA base key included in the eBCS Data frame, eBCSData(*s*,*c*,*k*-2,\*), are cached,
6. Derive the HCFA authentication key, A(*s*, *c*, *k*-2), from the HCFA base key, B(*s*, *c*, *k*-2).
7. Compute HCFA authenticator for the cached eBCS Data frame by using the HCFA authentication key.
8. If the computed HCFA authenticator is different from the HCFA authenticator in the cached eBCS Data frame, the cached eBCS Data frame shall be discarded.

Then forward the content in the eBCS Data frame to a higher layer.

Even in case of missing eBCS Data frames, the eBCS receiver recovers HCFA keys. For example, if the eBCS receiver missed all eBCS Data frames containing B(*s*, *c*, *k*) but still cached B(*s*, *c*, *k*-1) and received B(*s*, *c*, *k*+1), the eBCS receiver computes B(*s*, *c*, *k*) and B(*s*, *c*, *k*-1) as follows:

B(*s*, *c*, *k*) = SHAKE128(“eBCS base key” || B(*s*, *c*, *k*+1))

B(*s*, *c*, *k*-1) = SHAKE128(“eBCS base key” || B(*s*, *c*, *k*))

Then the eBCS receiver authenticates the HCFA base keys by comparing the computed B(*s*, *c*, *k*-1) and the cached B(*s*, *c*, *k*-1). After successful key authentication, the eBCS receiver authenticates eBCSData(*s*, *c*, *k*, \*) and eBCSData(*s*, *c*, *k*+1, \*).

**12.15.4 No frame authentication with mandatory higher layer source authentication (HLSA)**

If neither PKFA nor HCFA is used, a content source authentication mechanism shall be provided by a higher layer. The higher layer source authentication mechanism is out of scope of this standard. In this case, eBCS Info frames and eBCS Data frames for DL or E-BCS UL frames for UL are used.

Authentication of eBCS Info frames is optional if the eBCS Info frames include only HLSA content information. The eBCS AP may decide to use eBCS Info frame authentication or not.

If an eBCS Info frame includes the certificate of the AP, the eBCS receiver shall authenticate the eBCS Info frame as described in 12.15.2.2 (Authentication of the eBCS Info frame).

# (informative) Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

**Annex B**

**B.4 PICS proforma-IEEE Std 802.11-20xx**

**B.4.3 IUT configuration**

*Add description for eBCS transmitter and receiver support*

**B.4.<ANA12> eBCS features**

*Describe table that contains:*

* *eBCS Info frame transmission*
* *eBCS Info frame reception*
* *eBCS Data frame transmission*
* *eBCS Data frame reception*
* *eBCS public key frame authentication*
* *eBCS hash chain-public key frame authentication*

# Annex C (normative)

**ASN.1 encoding of the MAC and PHY MIB**

**C.3 MIB Detail**

***Insert the following entry in Annex C::***

Dot11WirelessMgmtOptionsEntry ::=

SEQUENCE {

…

dot11FineTimingMsmtRespActivated TruthValue,

dot11FineTimingMsmtInitActivated TruthValue,

dot11LciCivicInNeighborReport TruthValue,

dot11RMFineTimingMsmtRangeRepImplemented TruthValue,

dot11RMFineTimingMsmtRangeRepActivated TruthValue,

dot11RMLCIConfigured TruthValue,

dot11RMCivicConfigured TruthValue,

dot11eBCSSupportImplemented TruthValue

} …

dot11eBCSSupportImplemented OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute, when true, indicates that a eBCS protocol (see 11.22.6 (eBCS Procedures)) is implemented. The capability is disabled otherwise."

DEFVAL { false }

::= { dot11WirelessMgmtOptionsEntry <ANA>}

*Add the following line to “dot11smt”: [Motion #52]*

-- dot11eBCSConfigTable ::= { dot11smt <ANA13> }

*Add the following lines to appropriate place. [Motion #52]*

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11eBCSConfigTable TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dot11eBCSConfigTable OBJECT-TYPE

SYNTAX SEQUENCE OF Dot11eBCSConfigEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

“The table contains enhanced broadcast service configuration objects.”

::= { dot11smt <ANA13> }

*Describe “Dot11eBCSConfigEntry” according to the amendment.*

1. IEEE Standards Dictionary Online is available at: <http://dictionary.ieee.org> [↑](#footnote-ref-1)