IEEE P802.11
Wireless LANs

|  |
| --- |
| Draft Text for 11.55 eBCS Info |
| Date: 2020-02-xx |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

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

11. MLME

11.55 Enhanced Broadcast Service (eBCS) procedures

11.55.1 General

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.

11.55.2 eBCS DL procedures

11.55.2.1 General

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

* PKFA (12.15.\* Public Key Frame Authentication)
* HCFA (12.15.\* Hash Chain Frame Authentication)

The PKFA and the HCFA use both eBCS Info frame and eBCS Data frame.

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

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



**Figure 11-\* 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 TUs.

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 AP shall transmit the eBCS Info frame periodicaly in the interval of 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
* Contents Information
* Signature

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 Numebr overflows, it is set to 0.

The Timestamp is the time of generating 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 configures in dot11EBCSInfoInterval.

The Certificate 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 Contents Information.

Each Contents Information contains the following items.

* Authentication Algorithm
* Allowable Time Difference
* Title
* Higher Layer Destination Address
* TESLA Base Key (in case of HCFA)
* Previous Period TESLA Base Keys (in case of HCFA, optinal)
* TESLA Key Change Interval (in case of HCFA)
* Instant Authenticators (in case of HCFA, optional)
* Data (in case of PKFA, optional)

The Authenticatin 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 Title is the human readable title of the contents.

The Higher Layer Destination Address is the higher layer destination address of the contents that is used for the identifier of the contents.

The TESLA Base Key, the Previous Period TESLA Base Keys and the Instant Authenticators are used only in HCFA. The details are described in 12.\* (Hash Chain Frame Authentication).

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 following.

1. Check time difference between the eBCS AP and the eBCS non-AP STA. Compare the local time of the eBCS non-AP STA with the Timestamp in the eBCS Info frame.

If the difference is greater than the Allowable Time Difference, the contents shall be ignored.

1. Verify the Certificate in the eBCS Info frame with the pre-installed certificate of the CA.

If the verification is failed, the eBCS Info frame shall be ignored.

1. Verify the Signature in the eBCS Info frame with the Certificate in the eBCS Info frame.

If the verification is failed, the eBCS Info frame shall be ignored.

If the integrity of the eBCS Info frame is verified, process each Contents Information according to the Authentication Algorithm.

* In case of PKFA,
	+ If the Data is present in the Contents 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 TESLA Base Key in the Contents Information shall be cached.
	+ If the Instant Authenticators are present in the Contents Information, the Instant Authenticators shall be cached.
	+ If the Previous Period TESLA Base Keys are present in the Contents Information, authenticate the eBCS Data frames of the previous TESLA period.

11.55.2.3 eBCS Info frame fragmentation (or 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 Fragement Hash Values, the Certificate and the Signature shall be contained in the first fragment.
6. The fragmentation number in the Fragment Contorl 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 fragnment 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-\* (eBCS Info frame fragmentation).



**Figure 11-\* eBCS Info frame fragmentation**

11.55.2.4 eBCS Info frame defragmentation (or 10.4)

When the eBCS non-AP STA receives the eBCS Info frame with the Fragmentation Number in the Fragment Control is not 0 and the Fragmentation Index is 0, the eBCS non-AP STA shall verify the signature. If the verification succeeds, the eBCS non-AP STA shall cache the eBCS Info Sequence Number, Timestamp, the Fragment Control and the Fragment Hash Values.

When the eBCS non-AP STA receives the subsequent fragments of the eBCS Info frame, the eBCS non-AP STA shall check the integrity of the fragments by the following procedure.

1. The eBCS Info Sequence Number, the Timestamp and the Fragmentation Number in the Fragment Control in the received fragment are equal to that in the first fragment. If the values are different, the received fragment shall be discarded.
2. Calculate the hash value of the received fragment and compare it with the hash value in the Fragment Hash Values in the first fragment. If the hash value is different, the received fragment shall be discarded.
3. Cache the Contents Information of the received fragment.

After all fragments are received, the eBCS non-AP STA concatenates the fragments and process the eBCS Info frame.