IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for Clause 11.100.2 |
| Date: 2021-02-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | Koden-TI | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes the resolutions for clause 11.100.2 on LB252.

# To Editor: Green background means the comments finished in the previous revisions.

**The baseline is D1.01.**

# Suggested resolution

11.100.2 EBCS DL procedures

11.100.2.1 General

The EBCS DL uses three types of frame authentication mechanism as follows:

* PKFA (12.bc.2 Public Key Frame Authentication)
* HCFA (12.bc.3 Hash Chain Frame Authentication)
* HLSA (12.bc.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 for a non-AP STA without association is shown in Figure 11-bc1 (EBCS DL frame sequence for a non-AP STA without association). The frame sequence for a non-AP STA with association is shown in Figure 11-bc2 (EBCS DL frame sequence for a non-AP STA with association).

Figure 11-bc1 EBCS DL frame sequence for a non-AP STA without association

Figure 11-bc2 EBCS DL frame sequence for a non-AP STA with association

11.100.2.2 EBCS DL capability indications

The EBCS AP shall include the EBCS Capability element (9.4.2.300 EBCS Parameters element) in Beacon and Probe Response frames. The EBCS Capability element indicates the next EBCS Info transmission time in units of Beacon Interval. The EBCS Info frame is transmitted immediately after the indicated beacon.

11.100.2.3 EBCS Info frame generation and usage

The EBCS Info frame is transmitted periodically every dot11EBCSInfoInterval beacon periods. (For the APs in a multiple BSSID set, only the AP corresponding to the EBCS DL enabled BSSID may transmit an EBCS Info frame; other APs corresponding to EBCS DL disabled BSSIDs shall not transmit an EBCS Info frame.

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

If all content uses HLSA, the authentication algorithm of the EBCS Info frame may be 1 none, otherwise the EBCS Info frame shall use RSASSA-PSS, ECDSA or Ed25519.

On reception of an EBCS Info frame, an EBCS non-AP STA shall check the integrity of the EBCS Info frame as described in 12.100 (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,
	+ The non-AP STA shall cache the title, the negotiation method, the higher layer destination address, the time to termination and the next schedule.
	+ The non-AP STA shall notify the cached information to the SME through the SME-MLME SAP as described in 6.3.200 (EBCS procedures).
* In case of PKFA,
	+ If data is present in the Content Information field, the non-AP STA shall forward the MSDU in the data to a higher layer and shall cache the certificate in the EBCS Info frame to authenticate PFKA MSDUs.
* In case of HCFA,
	+ The HCFA base key in the Content Information field shall be cached.
	+ If instant authenticators are present in the content information, the instant authenticators shall be cached.
	+ If HCFA base keys from a previous period are present in the Content Informatio Information field, the non-AP STA shall authenticate the EBCS data frames of the previous HCFA period.

11.100.2.4 EBCS Info frame fragmentation

An EBCS Info frame may be fragmented into multiple MPDUs. The length of each fragment shall be an even number of octets, except for the last fragment, which may have an odd length. The length of a fragment shall not be larger than dot11FragmentationThreshold.

The fragmentation procedure is following.

1. Construct an EBCS Info frame which is not yet fragmented and determine the length of fragments.
2. When the EBCS Info frame is fragmented to N MPDUs, the Number of Fragments subfield in the EBCS Info Control field is set to N-1
3. Insert a space for N-1 Fragment Hash Values to the EBCS Info frame.
4. 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.
5. The Fragment Index subfield in the EBCS Info Control field is set to 0 (the first) to N-1 (the last) respectively.
6. Calculate the hash value of each fragment except the first one and put into the Fragment Hash Values.
7. Calculate and fill the signature of the first fragment.
8. Transmit the fragments consecutively in order of the Fragment Index. Data frames for EBCS shall not be transmitted before all of the fragments are transmitted.

The EBCS Info frame fragmentation is shown in Figure 11-bc3 (EBCS Info frame fragmentation).

Figure 11-bc3 EBCS Info frame fragmentation

11.100.2.5 EBCS Info frame defragmentation

When an EBCS non-AP STA receives an EBCS Info frame with the ~~Fragmentation Number~~ Number Of Fragments subfield in the ~~Fragment~~ EBCS Info Control field not ~~set~~ equal to 0 and the Fragment~~ation~~ Index subfield ~~set~~ equal to 0, the EBCS non-AP STA shall verify the signature. [1237] If the verification succeeds, the EBCS non-AP STA shall cache the EBCS Info frame Sequence Number, Timestamp, ~~the Fragment~~ EBCS Info Control and ~~the~~ Fragment Hash Values field values. [1237]

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. Verify that the EBCS ~~info~~ Info frame ~~sequence number~~ Sequence Number field, ~~the~~ ~~t~~Timestamp field and ~~the~~ ~~fragmentation number~~ Number Of Fragments subfield in the ~~Fragment~~ EBCS Info Control field in the received fragment are equal to those (sub)fields in the first fragment. [1237] 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 corresponding hash value in the ~~f~~Fragment ~~h~~Hash ~~v~~Values field in the first fragment. If the hash values ~~is~~ are different, the received fragment shall be discarded. [1237]
3. Cache the content information of the received fragment.

After all fragments are received, the EBCS non-AP STA concatenates the fragments and processes the EBCS Info frame as described in 11.100.2.3 (EBCS Info frame generation and usage).