IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution Text for Clause 9 | | | | |
| Date: 2022-01-04 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes the resolutions for CID 2085 on LB257.

**The baseline is D2.0.**

# Suggested resolution

### 9.6.7.54 EBCS Info frame format

***Replace Figure 9-909an at P64L1 as follows:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Content ID | Content Authentication Algorithm | Content Information Control | Content Address Type | Content Address | Title Length | Title |
| Octets: | 1 | 1 | 1 | 1 | variable | 1 | variable |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Negotiation Info | Time Of Termination (optional) | Next TX Schedule (optional) | Service URL Length (optional) | Service URL (optional) | Vendor Specific Data Length (optional) | Vendor Specific Data (optional) |
| Octets: | variable | 0 or 2 | 0 or 2 | 0 or 1 | variable | 0 or 1 | variable |

|  |  |
| --- | --- |
|  | Content Authentication Parameters  (optional) |
| Octets: | variable |

Figure 9-909an---Content Information field format

***Remove P66L25-P67L14:***

~~The Allowable Time Difference subfield is present if the Content Authentication Algorithm indicates PKFA~~

~~or HCFA and is not present otherwise. The value indicates 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 Content~~

~~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 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.~~

~~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 the EBCS HCFA key change interval in units of 10~~

~~milliseconds (see dot11eBCSHCFAKeyChangeInterval).~~

~~The Number Of Instant Authenticators subfield and the Instant Authenticators subfield are present if the~~

~~Content Authentication Algorithm field indicates HCFA with instant authentication, and are not present~~

~~otherwise.~~

~~The Number Of Instant Authenticators subfield, if present, indicates the number of the Instant~~

~~Authenticators contained in the Instant Authenticator List.~~

~~The Instant Authenticator List subfield, if present, contains one or more Instant Authenticators.~~

~~The format of each Instant Authenticator is shown in Figure 9-909ar (Instant Authenticator format).~~

~~Figure 9-909ar---Instant Authenticator format~~

~~The Hash Distance subfield indicates the hash distance of the instant authenticator. The Hash Value subfield~~

~~contains the instant authenticator of the following EBCS Data frame of the hash distance that is indicated in~~

~~the Hash Distance subfield.~~

***Insert the following text at P67L30:***

The Content Authentication Parameters subfield depends on the content authentication algorithm.

In case of PKFA, the Content Authentication Parameters subfield is present and its format is shown in Figure 9-909xa (Content Authentication Parameters subfield format for PKFA).

|  |  |
| --- | --- |
|  | Allowable Time Difference |
| Octets: | 2 |

Figure 9-909xa---Content Authentication Parameters subfield format for PKFA

The Allowable Time Difference subfield indicates the allowable time difference between the clock of the EBCS transmitter and the clock of the EBCS receivers in milliseconds.

In case of HCFA, the Content Authentication Parameters subfield is present and its format is shown in Figure 9-909xb (Content Authentication Parameters subfield format for HCFA).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 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: | 2 | 32 | 1 | 32 | 1 | 32 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | HCFA Key Change Interval | Number Of Instant Authenticators (optional) | Instant Authenticator List (optional) |
| Octets: | 1 | 0 or 1 | *n* x 33 |

Figure 9-909xb---Content Authentication Parameters subfield format for HCFA

The Allowable Time Difference subfield indicates 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 contains the first HCFA base key of the HCFA period that starts from this

EBCS Info frame.

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.

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 the EBCS HCFA key change interval in units of 10

milliseconds (see dot11eBCSHCFAKeyChangeInterval).

The Number Of Instant Authenticators subfield and the Instant Authenticator List subfield are present if the

Content Authentication Algorithm field indicates HCFA with instant authentication, and are not present

otherwise.

The Number Of Instant Authenticators subfield, if present, indicates the number of Instant

Authenticator subfields contained in the Instant Authenticator List.

The Instant Authenticator List subfield, if present, contains one or more Instant Authenticator subfields.

The format of each Instant Authenticator subfield is shown in Figure 9-909ar (Instant Authenticator subfield format).

|  |  |  |
| --- | --- | --- |
|  | Hash Distance | Hash Value |
| Octets: | 1 | 32 |

Figure 9-909ar---Instant Authenticator subfield format

The Hash Distance subfield indicates the hash distance of the instant authenticator. The Hash Value subfield

contains the instant authenticator of the following EBCS Data frame of the hash distance that is indicated in

the Hash Distance subfield.

In case of HLSA, the Content Authentication Parameters subfield is not present.