xIEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution Regarding CID 1209 |
| Date: 2022-07-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes the text proposal addressing CID 1209.

# Comment

**Original comment**

HCFA seems to be defining a mechanism to protect "HCFA MPDUs". The introduction to HCFA seems to imply that these are Data frames and 12.100.3.3 has a figure defining "HCFA MPDU format". However, it is not clear what exactly is an HCFA MPDU. How would a received of a Data frame know that the received frame was an HCFA MPDU? And shouldn't that frame format definition be in Clause 9 instead of Clause 12?

**Proposed Change**

Move the HCFA MPDU format description into Clause 9 and clearly define what the HCFA MPDU is (i.e., what in the frame header makes an MPDU be an HCFA MPDU).

**Original Resolution for CID 1209 (information only)**

"Revised.

TGbc discussed the alternative location of the text and agrees the clause 12 is more suitable location.

Incorporate the changes in https://mentor.ieee.org/802.11/dcn/21/11-21-0239-20-00bc-resolutions-for-clause-11-100-2.docx tagged 1209.

HCFA MPDU is used only in the newly defined EBCS Data frame that is idetified by the Type and the Subtype subfield in the MAC header. The MPDU type in an EBCS Data frame is identified by the Content ID field.

"

**Additional comment**

It looks like other than one exception, my comments have been satisfied. The remaining unsatisfied comment is CID 1209. It is unsatisfied for the following reasons:

The format of HCFA MPDU is defined in 12.14.3.3 (HCFA MPDU generation) which seems incorrect or at least confusing. This should be defined in Clause 9 and if the group does not want to move it into Clause 9, it

should at minimum be moved to a subclause that includes also reception instead of just generation. This issue shows up also in PICS EBCS3.2.1 referencing the "generation" subclause, not reception, while it should either be split into a separate generation and reception entries or modified to point to a subclause that covers both cases.

# Discussion

In the baseline, MPDU formats are defined in clause 12, e.g. 12.5.3.2 CCMP MPDU format.

Agree to move the format definition to a separate subclause.

# Proposed text

**The baseline is D3.0.**

***Modify 12.14.3.3 as follows:***

### 12.14.3.3 HCFA MPDU ~~generation~~

EBCS Data frames sent under HCFA use the HCFA MPDU format. The frame body of an HCFA MPDU is shown in Figure 12-55i (HCFA MPDU format).

*(snip)*

**Figure 12-55i—HCFA MPDU format**

The MAC Header field and the FCS field are defined in 9.2.1.

The Timestamp field indicates the elapsed time from 2020-01-01 00:00 UTC in milliseconds until the time at which the MPDU was generated.

The HCFA Sequence field indicates the HCFA sequence number of the MPDU.

The Key Sequence field indicates the key sequence number of the MPDU.

The Data Sequence field indicates the data sequence number of the MPDU.

The Data Length field indicates the length of the Data field.

The Data (PDU) field contains an MSDU.

The Disclosed Key field contains the HCFA base key to be disclosed.

The Instant Authenticator field contains instant authenticator(s) for the MPDU(s) that will be transmitted later.

The HCFA Authenticator field contains the HCFA authenticator of the MPDU.

The HCFA authenticator is the HMAC-SHA-256 value of the MPDU with the HCFA authentication key.

HCFA Authenticator = HMAC-SHA-256 (*A(s, c, k)*, transmitter’s MAC address || HCFA MPDU fields from the beginning of the Timestamp field to the end of the Instant Authenticator field)

where

*A(s, c, k)* indicates the HCFA authentication key for the HCFA sequence *s*, the content ID *c* and the key sequence *k*.

The instant authenticator is the hash value of the MPDU to be transmitted later that is specified by dot11EBCSHCFAHashDistance, generated as follows:

Instant Authenticator = SHA-256 (transmitter’s MAC address || HCFA MPDU fields from the beginning of the Timestamp field to the end of the Disclosed Key field)

***Increment subclause number as follows:***

### 12.14.3.5 HCFA MPDU reception

HCFA MPDUs shall be discarded until an EBCS Info frame from the BSS is received.

An HCFA MDPU, EBCSData(s, c, k, d), is processed as follows.

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 HCFA MPDU shall be discarded.

2) If instant authentication is used and the

~~3)~~ instant authenticator of the EBCSData(s, c, k, d), IAuth(s, c, k, d) (12.14.3.3 (HCFA MPDU)), 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 HCFA MPDU shall be discarded.

~~4~~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 HCFA MPDU may be cached until the HCFA base key for the key period is received, or the HCFA MPDU may be discarded.

~~5~~4) If instant authentication is not used, the HCFA MPDU shall be cached until the HCFA base key for the key period is received.

~~6~~5) If prior HCFA MPDU(s) using the HCFA authentication key derived from the HCFA base key included in the present HCFA MPDU, EBCSData(s,c,k-2,\*), are cached,

i) Derive the HCFA authentication key, A(s, c, k-2), from the HCFA base key, B(s, c, k-2).

ii) Compute HCFA authenticator (12.14.3.3 (HCFA MPDU)) for the cached

~~iii)~~ HCFA MPDU(s) by using the HCFA authentication key.

~~iv~~iii) If the computed HCFA authenticator is different from the HCFA authenticator in the cached

~~v)~~ HCFA MPDU, the cached HCFA MPDU shall be discarded.

### B.4.38 Enhanced Broadcast Services (EBCS) features

***Modify EBCS3.2.1 as follows:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EBCS3.2.1 | HCFA MPDU | 12.14.3.3(HCFAMPDU~~generation~~) | EBCS3.2: M | Yes  No N/A  |