IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Resolution Text for CID 3084 | | | | |
| Date: 2022-06-13 | | | | |
| 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 3084.

**The baseline is D3.0.**

# Proposed text

### 12.14.3.2 Key generation

***Modify the subclause as follows:***

HCFA is a one-way key chain authentication mechanism. The EBCS transmitter generates HCFA base keys and HCFA authentication keys for each EBCS traffic stream before each EBCS Info frame generation.

SHA-256 hash function is used for HCFA key generation.

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

*Bs,0* = 256-bit random value

*key-seeds,n* = HKDF-Extract(EBCS AP MAC address, *Bs,n-1*)

*~~B~~~~s,n~~* ~~= SHA-256 (“EBCS HCFA base key” ||~~ *~~B~~~~s,n-1~~*~~) (~~*~~n~~* ~~= 1)~~

*Bs,n* = HKDF-Expand(“EBCS HCFA base key”, *key-seeds,n*) (*n* ≥ 1)

where

HKDF-Extract() and HKDF-Expand() are the functions defined in IETF RFC 5869, instantiated with SHA-256

*s* is the HCFA sequence number of the generating EBCS Info frame.

EBCS AP MAC address is an octet string that represents the MAC address of an EBCS AP

“EBCS HCFA base key” is an ASCII string.

The HCFA authentication keys (As,n) are generated as follows:

*~~A~~~~s,n~~* ~~= SHA-256 (“EBCS HCFA authentication key” ||~~ *~~B~~~~s,n~~*~~)~~

*As,n* = HKDF-Expand(“EBCS HCFA authentication key”, *key-seeds,n*)

where

HKDF-Expand() are the functions defined in IETF RFC 5869, instantiated with SHA-256

*s* is the HCFA sequence number of the generating EBCS Info frame.

“EBCS HCFA authentication key” is an ASCII string.

The number of 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 12-55h (HCFA key generation scheme).