IEEE P802.11
Wireless LANs

|  |
| --- |
| SFD Proposal for R3.3.1 |
| Date: 2019-11-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes a frame authentication SFD proposal based on 11-19/451r5 and 11-1802r1.

# R3.3.1

**The 802.11bc amendment shall provide origin authenticity protection for broadcast data frames.**

The following SFD proposal implements this frame authentication mechanism based on Draft P802.11REVmd D3.0.

OCB related items will be added after joint session with TGbd.

# Discussion Items

**Public key only authentication**

Public key only authentication is suitable for small, time sensitive and aperiodic event based data.

**Option 1: Data piggy-backed in eBCS Info frame**



Pros: Less airtime occupancy for small data, Receiver does not need to cache public key

Cons: Data passed via MLME-SAP, More airtime for large data

**Option 2: Data transmitted in eBCS Data frame**



Pros: Data passed via MAC-SAP, Less airtime for large data

Cons: More airtime for small data, Receiver has to cache public key

**Option 3:**



**Straw poll #6**

Which option do you prefer to be supported in eBCS?

Option 1:

Option 2:

Option 3:

# SFD Proposal

**3. Definitions**

**3.2 Definitions specific to IEEE Std 802.11**

**Enhanced Broadcast Service (eBCS) receiver:** An STA that receives Enhanced Broadcast Services (eBCS) frames.

**Enhanced Broadcast Service (eBCS) transmitter:** An STA that transmits Enhanced Broadcast Services (eBCS) frames.

6. Layer management

6.3 MLME SAP interface

**6.3.<ANA1> eBCS Info transmission**

*Describe MLME SAP for eBCS Info frame transmission.*

6.3.<ANA2> eBCS Info reception

*Describe MLME SAP for eBCS Info frame reception.*

9. Frame formats

9.6 Action frame format details

9.6.7 Public Action details

9.6.7.1 Public Action frames

*Add eBCS Info frame to Table 9-362.*

9.6.7.<ANA5> eBCS Info frame format

*Describe eBCS Info frame format that contains:*

* *eBCS Info sequence number*
* *eBCS transmitter’s certificate signed by CA*
* *Timestamp*
* *Authentication algorithm identifier*
* *eBCS Info transmittion interval*
* *Contents information*
	+ *Human readable title*
	+ *Higher layer protocol type*
	+ *Destination IP address and UDP port (if UDP/IP)*
	+ *Hash chain parameters (if hash chain is used) [11-19/1802r1]*
		- *Hash chain distances*
		- *Details are future work*
* *Signature for this eBCS Info frame signed by the eBCS transmitter’s private key*
* *Contents data (optional)*
	+ *if public key authentication is used and uplink case, data can only be transmitted via this frame.*
	+ *If public key authentication is used and downlink case, field is not present (piggy-backing not allowed).*

11. MLME

11.<ANA8> Enhanced Broadcast Service (eBCS) procedures

11.<ANA8>.<ANA9> eBCS Info frame generation and usage

11.<ANA8>.<ANA9>.1 eBCS Info frame transmittion

*Describe eBCS Info frame transmission procedure.*

11.<ANA8>.<ANA9>.2 eBCS Info frame reception

*Descrive eBCS Info frame reciption procedure.*

11.<ANA8>.<ANA10> eBCS Data frame generation and usage

11.<ANA8>.<ANA10>.1 eBCS Data frame transmission

*Describe eBCS Data frame transmission procedure.*

11.<ANA8>.<ANA10>.2 eBCS Data frame reception

*Descrive eBCS Data frame reciption procedure.*

12. Security

12.<ANA11> Frame authentication for eBCS

12.<ANA11>.1 General

*Describe abstract of the eBCS frame authentication mechanism that contains:*

* *eBCS public key frame authentication that uses only public key algorithm*
* *eBCS hash chain-public key frame authentication that uses combination of hash chain and public key algorithm*

12.<ANA11>.2 eBCS public key frame authentication

*Describe eBCS public key authentication procedure.*

12.<ANA11>.3 eBCS hash chain-public key frame authentication

*Describe eBCS hash chain-public key frame authentication procedure.*

Annex B

B.4 PICS proforma-IEEE Std 802.11-20xx

B.4.3 IUT configuration

*Add description for eBCS transmitter and receiver support*

B.4.<ANA12> eBCS features

*Describe table that contains:*

* *eBCS Info frame transmission*
* *eBCS Info frame reception*
* *eBCS Data frame transmission*
* *eBCS Data frame reception*
* *eBCS public key frame authentication*
* *eBCS hash chain-public key frame authentication*

Annex C

C.3 MIB details

*Add the following line to “dot11smt”.*

-- dot11eBCSConfigTable ::= { dot11smt <ANA13> }

*Add the following lines to appropriate place.*

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11eBCSConfigTable TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dot11eBCSConfigTable OBJECT-TYPE

 SYNTAX SEQUENCE OF Dot11eBCSConfigEntry

 MAX-ACCESS not-accesible

 STATUS current

 DESCRIPTION

 “The table contains enhanced broadcast service configuration objects.”

 ::= { dot11smt <ANA13> }

*Describe “Dot11eBCSConfigEntry” according to the amendment.*