Response to DCN-499 Rev1

 Comment 22

I suggest the following change:

18.4.2. 3

The DPP SS shall allow an X.509 certificate signed by a Certificate Authority to be installed

during production or later by a Certificate Authority under customer responsibility. The certificate binds the SS identity (MAC address or name) with its private-public key pair.

Comment 23

I reviewed all appearances of identity with MAC address / name. There are some inconsistencies. I suggest the following changes:

18.4.2, 4-d

SS Name (optional) – a string of up to 31 characters, provides an option to identify a DPP SS by its name rather than its MAC address.

18.4.2, 5-c

If configured for Manual Selection, a DPP SS shall support a

vendor-specific display of the identity of DPP SSs (MAC address or name) from which it has received an ASSOCIATE Request message

18.4.2, 6-b

Identity of each peer SS (MAC address or Name),

18.4.3 1-b

When configured for Manual Selection mode, the ASSOCIATE Request message transmitted by a DPP SS shall indicate the initiating DPP SS MAC Address, its Name (optional), and the initiating DPP SS CA Name, as appear in its certificate Issuer Name field.

**18.5.1 Identity filtering**

If configured to use the Automatic Selection mode, a pair of DPP SS peers shall exchange their MAC addresses and optionally, names, using ASSOCIATE Request/Response messages. The

DPP SS receiving an ASSOCIATE Request message, if not already in the association process

with the sending DPP SS, shall compare the received selection mode, and the MAC address

and optional name with its own selection mode and the MAC address(es) and the

name(s) of its configured peer DPP SS(s) and send an ASSOCIATE Response message to the

sender of the ASSOCIATE Request message if a match is found in both selection mode and MAC address or name. If there is no match, the DPP SS shall not respond to the ASSOCIATE

Request message. The identity verification process is shown in Figure 18-8.

I suggest to combine sections 2 and 4 of 18.5.1, as follow:

2. If configured to use the ‘Manual’ Selection mode, the DPP SS receiving an ASSOCIATE

Request message shall compare the selection mode and the CA Name identified in the received

ASSOCIATE Request message with its configured peer DPP SS CA name(s) and if matched

will add the SS’s Name and MAC Address, as appear in the ASSOCIATE Request message, to

the list of candidate DPP SS peers presented to the user. The DPP SS shall include a vendor-specific function to display the list of candidate DPP SS peer(Names or if absent, MAC addresses) to enable manual selection of the peer DPP SS(s). When the operator selects a DPP SS from the list of candidate DPP SS peer displayed , the DPP SS shall send an ASSOCIATE Response message to the selected DPP SS. Figure 18-9 shows the flow.

Comment 26 - TLS Client – Server

I reviewed all references. It looks well defined to me. We may think why we need the two options – pre configured sever-client and automatic.

18.4.2 4

f) TLS mode (automatic, server or client)

A DPP SS can be configured to use TLS client or TLS server mode. If configured to automatic mode, an independent TLS session starts with each association process. The server or client mode are automatically selected as explained in 18.5.1.

**18.5.1 Identity filtering**

3. A DPP SS in Client TLS mode shall respond to an ASSOCIATE Request only if the sending DPP SS is in Server TLS mode and a DPP SS in Server TLS mode shall respond to an ASSOCIATE Request only if the sending DPP SS in Client TLS mode.

**18.5.2.1 Authentication and Key management**

Upon entering the Associate Sub-state for a peer association, the DPP SS shall start a TLS session with the peer. If configured to Server TLS mode, the DPP SS shall operate as a TLS server; if configured to Client TLS mode, the DPP SS shall operate as a TLS client; Otherwise, the DPP SS shall compare its own MAC address with the peer DPP SS’s MAC address and shall operate as a TLS server if its MAC address is higher than the peer DPP SS’s MAC address, otherwise, it shall operate as a TLS client.

To compare the MAC addresses, convert the MAC address bits into a number by ordering the bits from LSB to MSB. The lower value belongs to the lower MAC address and the higher value belongs to the higher MAC address.

Comment 27 – AES

Last block padding is well explained in the standard [FIPS 197]. Added a reference. I added AES-128 because it appears in the configurable parameters (Table 18-11).

18.5.2.1

c) Encryption: if preconfigured to use encryption, a DPP SS shall support AES-128 or AES-256 [FIPS 197].

Comment 28 – TLS encapsulation

I suggest switching table 18-11 (configurable parameters) and table 18-12 (TLS message)

**18.5.2.1 Authentication and Key management**

Transport Layer Security (TLS) v1.3 handshake shall be used to mutually authenticate the communicating peers, negotiate cryptographic algorithms, and establish shared keying materials. Each DPP SS shall support both client and server TLS v1.3 handshakes.

When an SS has a TLS payload to transmit to its peer SS, it encapsulates it in a TLS Message (Table 18-12).

Comment 29

18.5.2.1

Line 28

1. Certificate Signature: verify that the certificate was signed by the private key corresponding to the peer preconfigured public key

Line 39

1. Certificate Signature: verify that the certificate was signed by the private key corresponding to the peer preconfigured CA public key. In case of certificate chain, verify the certificate is signed by the public key that is in the certificate