Authentication and Security in 1722.1 Draft 20

Ashley Butterworth
Apple Inc.

Overview

- Key Management
- Controller Authorization
- Transport Security Control
- Stream Encryption Control
- Entity Model Verification

Key Management

- Add, Remove and List Keys (RSA Public and Private, AES128 and AES256)
  - AUTH_ADD_KEY, AUTH_DELETE_KEY, AUTH_GET_KEY_LIST and AUTH_GET_KEY
- Add and Remove Keys from Keychains giving the keys permissions
  - AUTH_ADD_KEY_TO_CHAIN, AUTH_DELETE_KEY_FROM_CHAIN and AUTH_GET_KEYCHAIN_LIST

Keychains

- 5 keychains are defined
  - ENTITY_PUBLIC - The RSA public key of the Entity for verification of signatures
  - ENTITY_PRIVATE - The RSA private key of the Entity
  - MANUFACTURER_PUBLIC - The Entity manufacturer’s RSA public for verification of ENTITY_PUBLIC
  - CONTROLLERS - The RSA public key’s of the Controllers allowed to control the Entity
  - TRANSPORT - The keys allowed to be used for transport security

Chain of Trust

- Each key is signed by another key which is traceable to a key which is trusted by the Entity or Controller
- Entity public key is signed by Manufacturer private key
- Manufacturer public key is signed by trusted root private key
  - Controller or Entity has the trusted root public key

Key GUIDs

- Key GUID is a means of naming the keys so they can be used
- The section in the draft needs to be updated
  - There are 2 key GUID types, manufacturer generated and dynamically generated
  - Manufacturer generated use manufacturers OUI or OUI36 and allocates the lower 40 or 28 bits
  - Dynamically generated use 1722 OUI
    - 90e0f0 are management assigned
    - 91e0f0 are free-for-all unmanaged

Controller Authorization

- Restricts access to Controllers which know the token
- Off by default, enabled by sending AUTH_ADD_TOKEN
- Disabled by sending AUTH_DELETE_TOKEN
- Authentication token is binary data blob
- Authentication token is sent as plain text relying on transport security

Transport Security Control

- Turn on and off transport security (1722a and maybe MACSEC[802.1AE-2006]) for ADP, ACMP and AECP
- Note - Transport security control can cause a denial of service attack by enabling or disabling transport security when other Entities expect it to be disabled or enabled.

Stream Encryption Control

- Enables or disables encryption of streams
- Type of encryption is dependent on the key used when enabling
    - Currently support AES128, AES256 and RSA1024
- Note - Stream encryption control can cause a denial of service attack by enabling or disabling encryption when other Entities expect it to be disabled or enabled.

Entity Model Verification

- Verification that AEM Entity model hasn’t been tampered with since manufacture or firmware update
- Entity model is signed by the manufacturer’s private key during manufacture/firmware building with the signature coded into the device
- Controller verifies model with manufacturers private key