Flash Memory Summit

TCG DICE Evidence and DMTF SPDM Binding Overview

Chandra Nelogal

DMTS

Dell Technologies

35 YEARS OF NAND FLASH MEMORY INNOVATION

Disclaimers

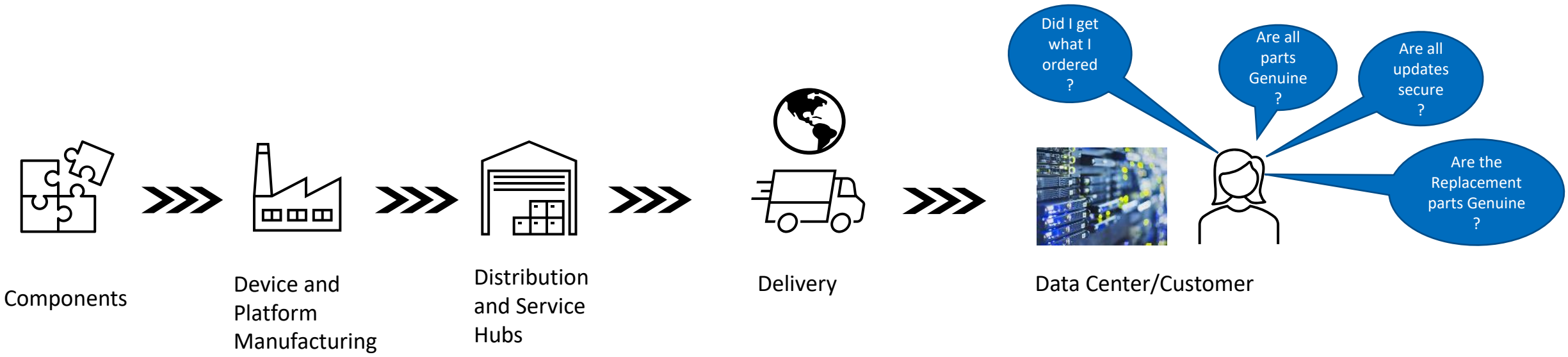
- Information shared in these slides pertain to documents developed by industry standard organizations TCG and DMTF
- There is no warranty on the information shared

Agenda

- Need for Trusted Devices and Trusted Platforms
- TCG DICE Attestation Overview
- Attestation Use Cases
- TCG DICE and DMTF SPDM Certificate Mapping
- Measurements
- SPDM Overview - brief

IS	IS-NOT
Overview of DICE-SPDM Binding work	An overview of TCG DICE nor that of DMTF SPDM
High level overview of an upcoming specification	An in-depth and a definitive description of a specification under development

Need for Trusted Devices and Trusted Platforms



- Hostile component insertion, compromised firmware(s) & Supply chain issues
- How to prevent and protect from platform component sensitive data disclosure?

DMTF Security Protocol & Data Model

- Certificate based authentication provides platform component identity assurance
- Roots of Trust measurement for firmware integrity checks
- Facilitate privacy and data security communication over the platform interfaces

TCG DICE Attestation Overview

Trusted Computing Group – DICE Work Group - Device Identifier and Composition Engine

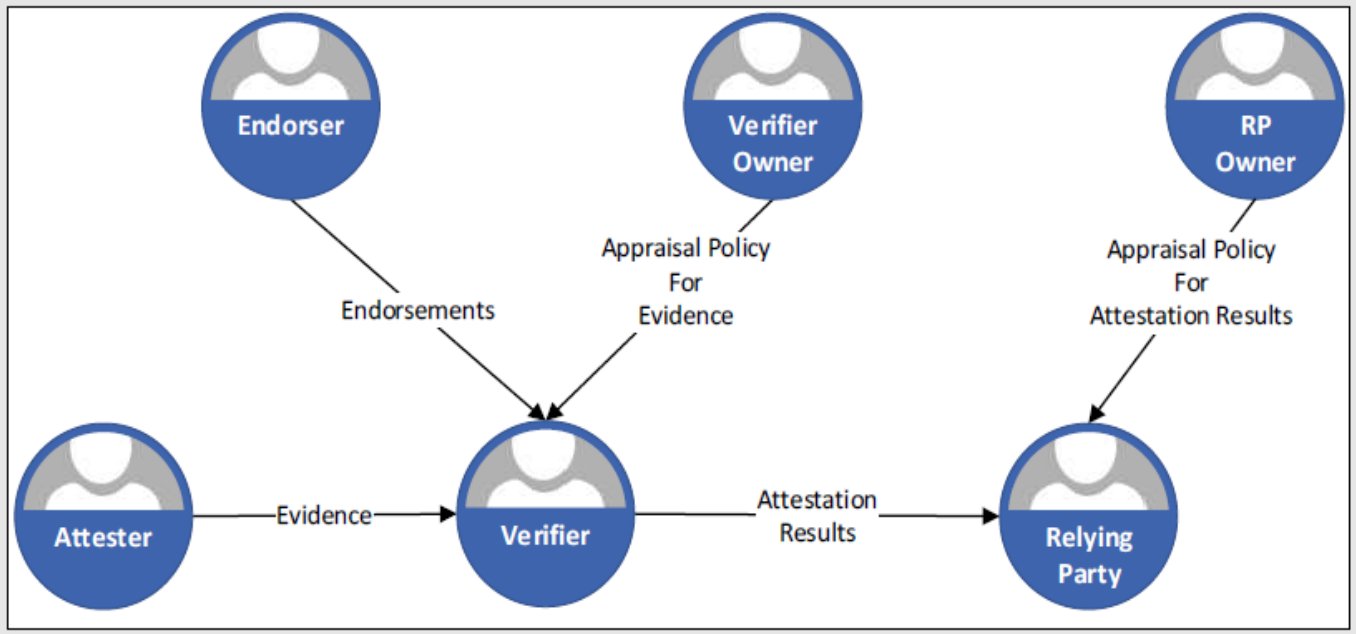


Figure 1: Attestation Roles and message flow

- The DICE attestation architecture focuses on creation, conveyance and appraisal of evidence
- An SPDM Responder device can be mapped to an attester and the
- SPDM Requestor can be a verifier
- Note that an SPDM Requestor may take on one or more roles defined in the DICE attestation architecture document

Attestation Use Cases – 1/2

Flash Memory Summit

USE CASE	EVIDENCE	VERIFIER (REQUESTER)	ATTESTOR (RESPONDER)	NOTES
Asset Tracking	Device Certificate	Request Certificate	Provide Certificate	Tracking H/W Identity. Device Certificate (stand alone or part of the Alias Certificate chain) H/W Instance specific identity
Firmware Measurement	Measurement Manifest and Alias Certificate(s)	Request Measurement(s) and Certificate(s)	Provide Measurement(s) and Certificate(s)	Measurements as well as Alias certificates
Software or Firmware Update	Measurement Manifest and Alias Certificate(s)	Request Measurement(s) and Certificate(s)	Provide Measurement(s) and Certificate(s)	Updated for f/w or s/w change detection
On Boarding	Alias Certificate(s)	Provision Cert	Add Certificate Chain or add Certificate(s)	Provision a new certificate chain*

*

The SPDM specification v1.2 requires that the public (and hence, the private) key in the leaf (end entity) certificate of any certificate slot to be the same.

35 YEARS OF NAND FLASH MEMORY INNOVATION

Attestation Use Cases – 2/2

Flash Memory Summit

USE CASE	EVIDENCE	VERIFIER (REQUESTER)	ATTESTOR (RESPONDER)	NOTES
Reprovision, Re-onboarding	Alias Certificate(s)	Provision the cert chain	Verify and store	Performed in a secure environment or at least with a secure session
Remanufacturing	Device and Alias Certificates	Provision the cert chain	Verify and store	Performed in a secure environment. Device identity will change leading to new DeviceID Key. Thus, changing all certificates that depend on it.
Decommissioning	Device and Alias Certificates	Provision	Update	Changes DeviceID Key, thus invalidating any stored and generated certificates tied to the previous DeviceID Key including Device Certificate(s) and Alias Certificate(s)

DICE Evidence and SPDM Binding

DICE and SPDM Binding

- This session focuses on TCG DICE and DMTF SPDM binding
- There is an effort underway at the TCG DICE Work Group
  - Maps DICE defined evidence types with the SPDM evidence types
- Need
  - The DMTF SPDM defines mechanisms to exchange evidence and information
  - The TCG DICE family of specifications defines different types of evidence
  - The concepts around identity and measurements used in SPDM are derived from TCG DICE
    - Not explicitly stated
  - This specification is an effort to map the aspects that are common between the standards – Certificates, Measurements

DICE Layering, TCI & CDI – Asymmetric IDs

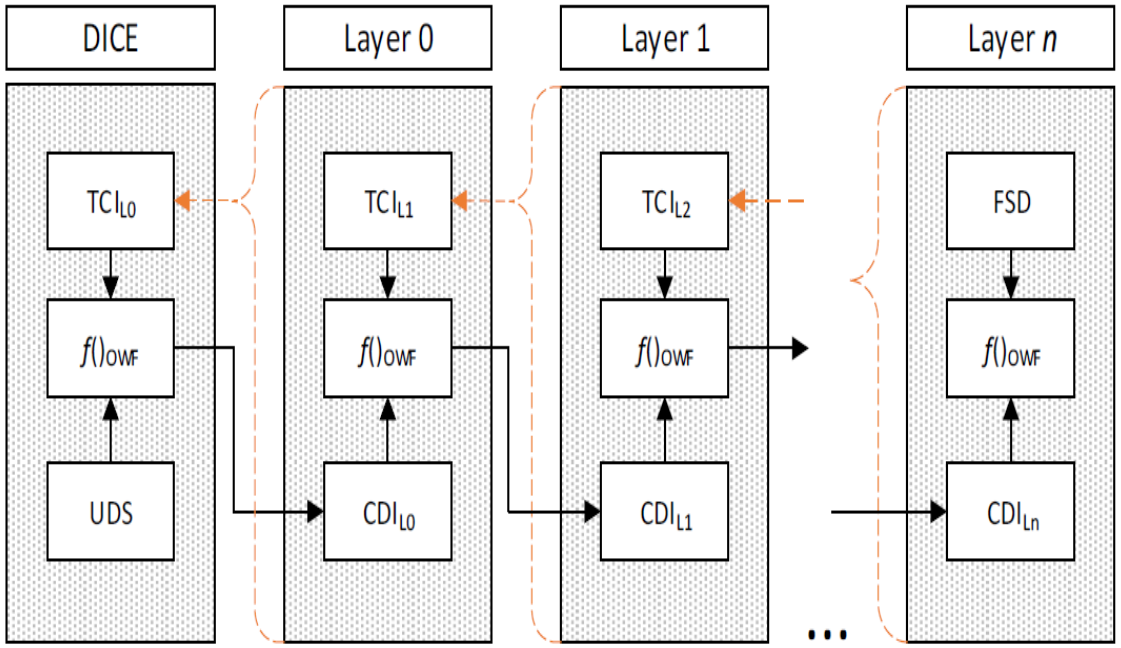


Figure 2: TCB layering architecture

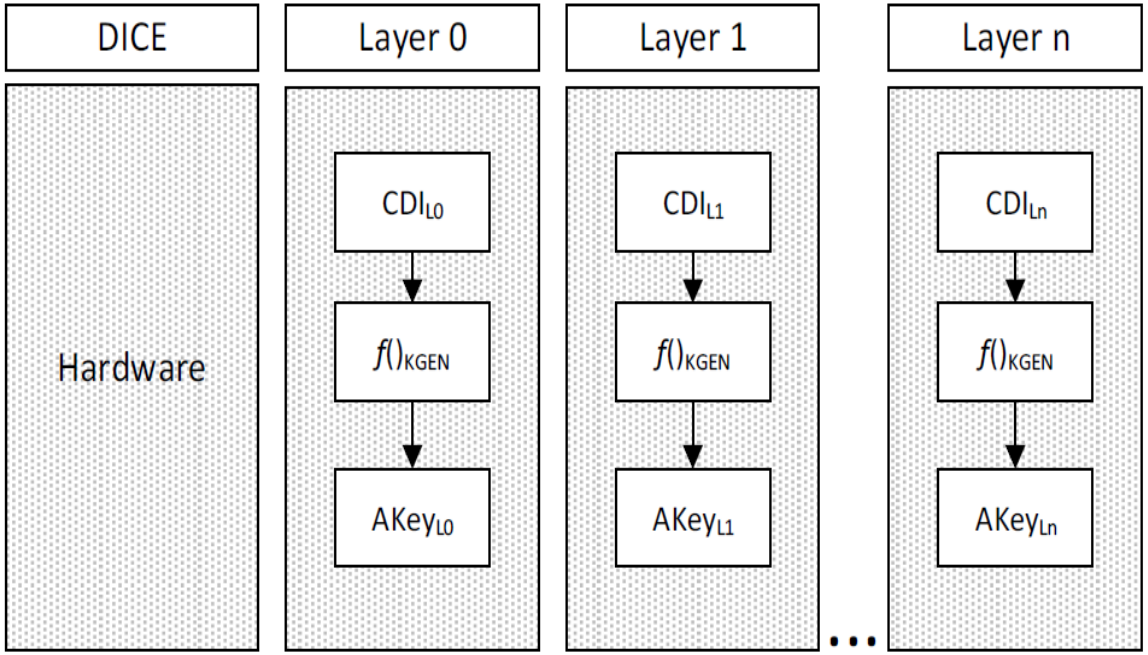
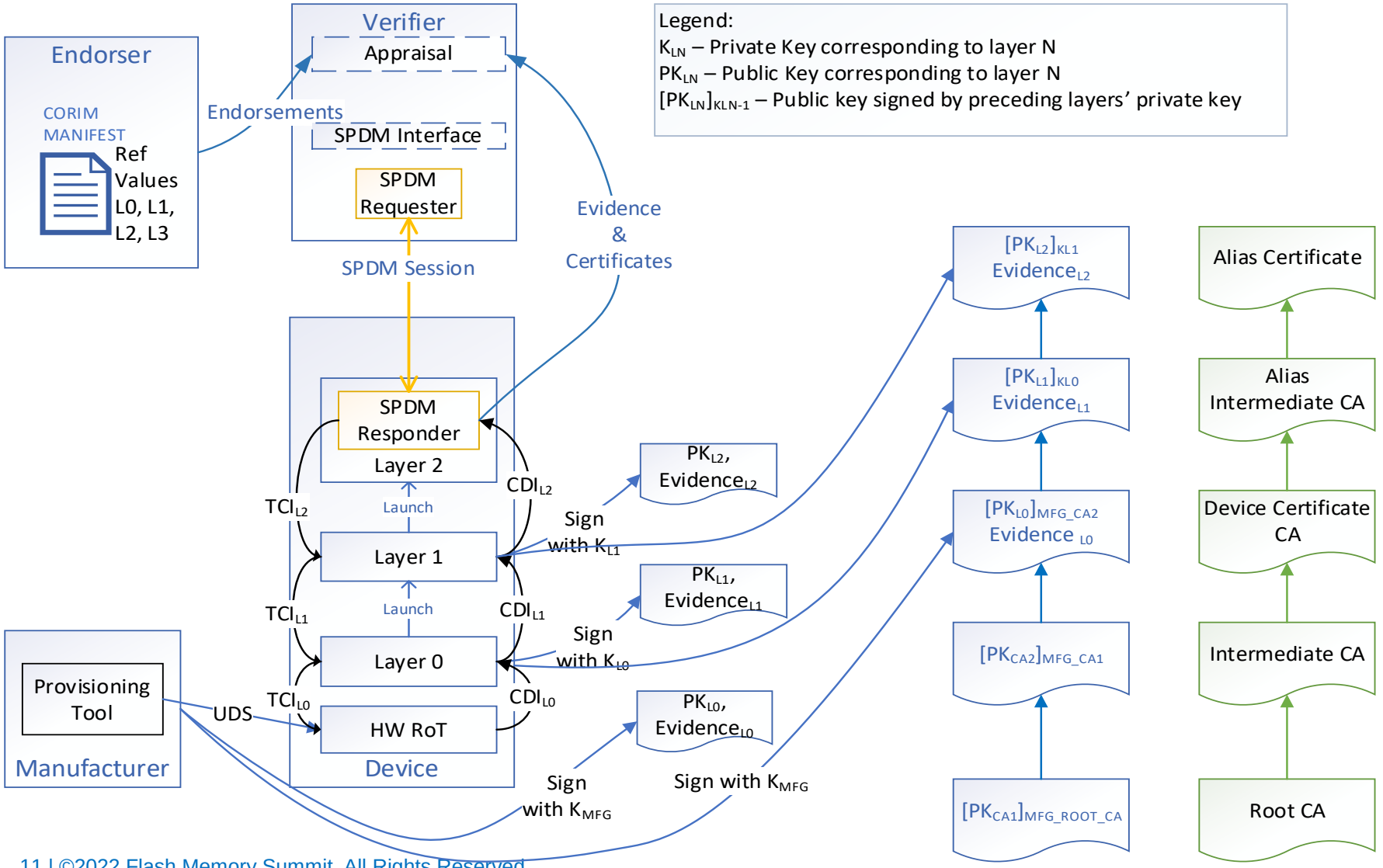


Figure 3: Asymmetric key generation example

DICE and SPDM Certificate models



1. DICE layering architecture of a device. Certificates and evidence corresponding to device layers
2. Certificate chain generation and storage on a device
3. Mapping to SPDM defined Alias Certificate Model*

*The CA terminology is used from DMTF SPDM specification.

Certificate Type Mapping

DICE Certificate Type	SPDM Certificate Type	Notes
Initial Device ID Certificate or	Device Certificate	In the Device Certificate model described by SPDM, this can map to an end-entity certificate as well.
Local Device ID Certificate	Alias Certificate	In the Alias certificate model described by SPDM, this can map to an Embedded Certificate Authority Certificate.
ECA Certificate	Device Certificate & Alias Certificate	In the SPDM Alias Certificate model, the Device Certificate maps to an ECA (embedded certificate authority) certificate. An Alias Intermediate Certificate could also be an ECA certificate
Attestation Certificate	Alias Certificate	In the SPDM Alias Certificate model, the leaf or the end entity certificate can be used for the purposes of attestation
End Entity Certificate	Alias Certificate (Leaf)	An end-entity certificate can be used for identification purposes and can sign for opaque data from an external Verifier for attestation purposes

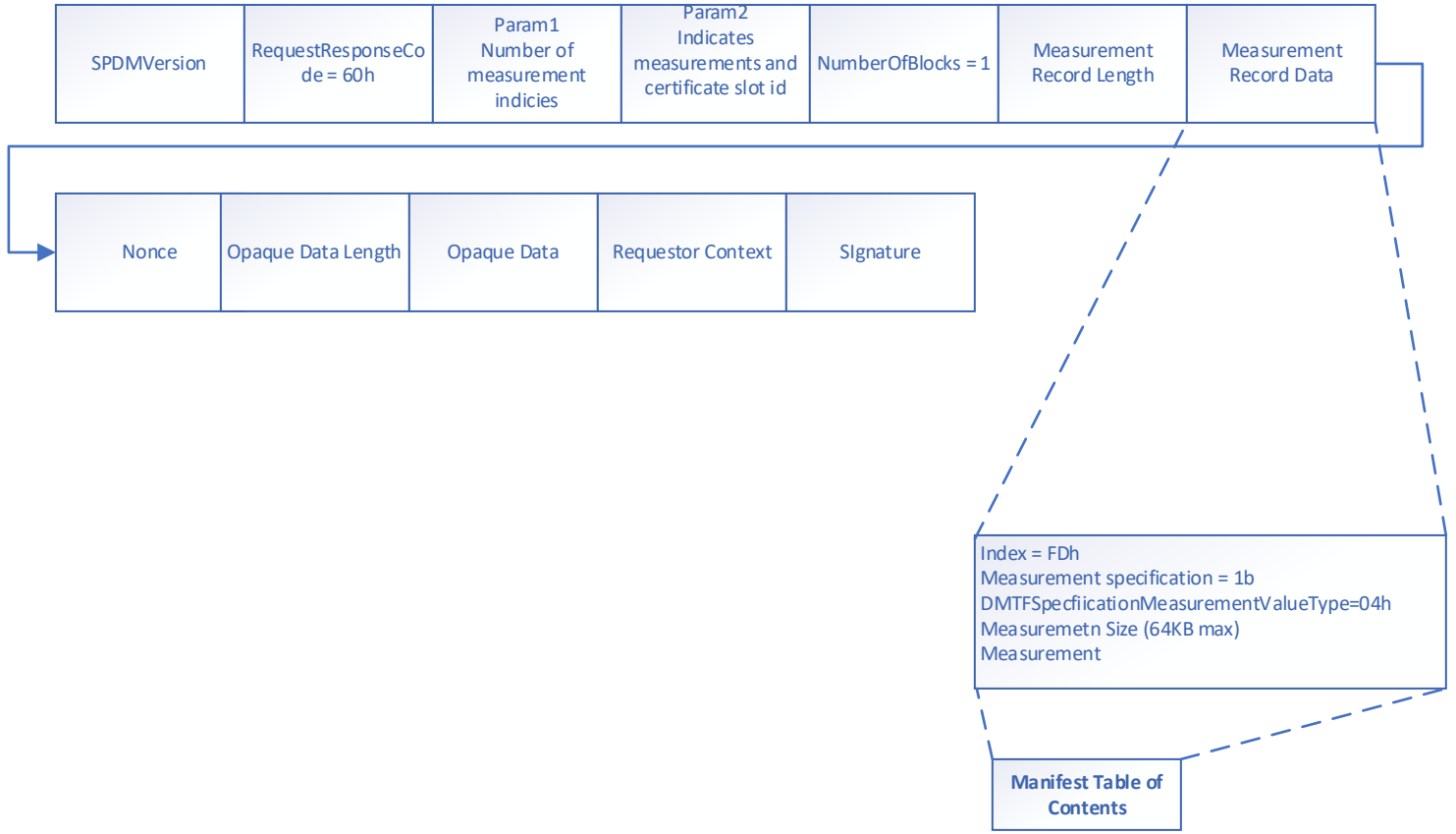
TCG DICE Certificate Profile defines specific OIDs for different certificate types. DMTF SPDM also defines OIDs.
SPDM defined Alias Certificate model is mapped. SPDM also supports the Device certificate model which is simpler

Measurements

Response to GET_MEASUREMENTS SPDM request.

The existing mechanism defined in the SPDM specification to convey measurement is leveraged to convey evidence and endorsements

A specific measurement index value is being assigned to specific evidence format which is defined using the CDDL (Common Data Definition Language), and is encoded in CBOR



Takeaways

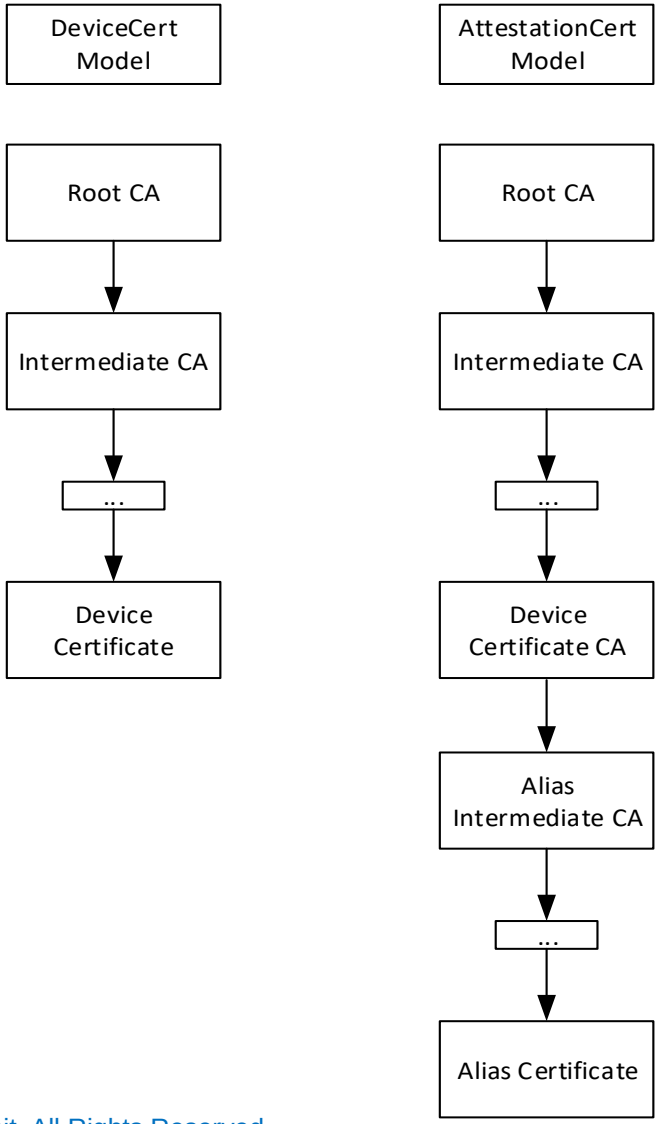
- SPDM protocol support is gaining traction
  - Device manufacturers
  - System integrators
  - DICE based implementations provide strong identities
- Participate in TCG and/or in DMTF for standards work under development

SPDM Overview

SPDM Summary

- Version 1.0
  - Measurement Support
  - Device Authentication
- Version 1.1
  - Secure Session
    - Public Key Exchange
    - Symmetric Key Exchange
  - Mutual Authentication
- Version 1.2
  - Provisioning
    - Allows installation of device certificate in manufacturing
  - Certificates
    - Allows for alias leaf certificates derived from device certificates
  - Message Fragmentation
    - Send large SPDM messages in chunks
  - Miscellaneous
    - New OIDs added

SPDM Certificate Models



Acronyms

ACRONYM	Explanation
TCI	TCB Component Identity
CDI	Compound Device Identity
DeviceID Key	An asymmetric key derived from CDI at Layer 0.
IdevID	Initial Device ID –a unique identifier provisioned during device manufacturing. Usually remains same during useful life of the device. Term defined in IEEE 802.1AR
LDevID	Local Device ID – a unique identifier associated with the IDevID. Defined in IEEE 802.1AR
ECA	Embedded Certificate Authority – a layer of a Device that can sign a certificate (usually for a subsequent layer)

References

https://trustedcomputinggroup.org/wp-content/uploads/DICE-Attestation-Architecture-r23-final.pdf
https://trustedcomputinggroup.org/wp-content/uploads/DICE-Layering-Architecture-r19_pub.pdf
https://trustedcomputinggroup.org/wp-content/uploads/Hardware-Requirements-for-Device-Identifier-Composition-Engine-r78_For-Publication.pdf
https://trustedcomputinggroup.org/wp-content/uploads/DICE-Certificate-Profiles-r01_pub.pdf
https://trustedcomputinggroup.org/wp-content/uploads/TCG_Errata_DICE_Certificate_Profiles_r02_pub.pdf
https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.2.0.pdf

Backup

DICE Layering, TCI & CDI – Symmetric IDs

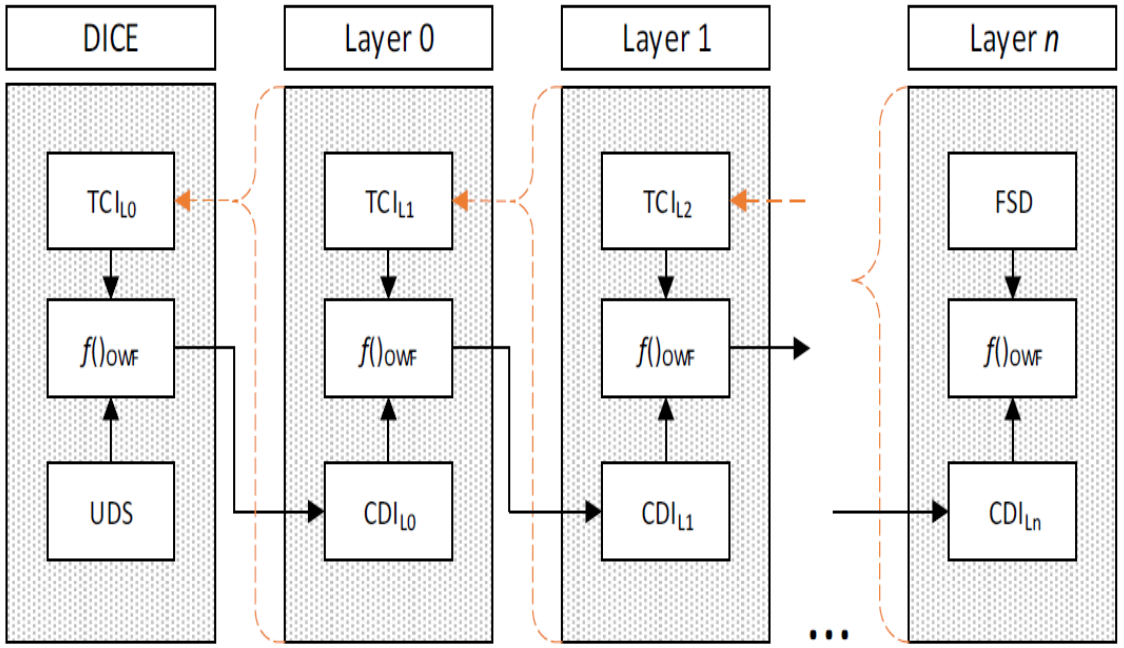


Figure 2: TCB layering architecture

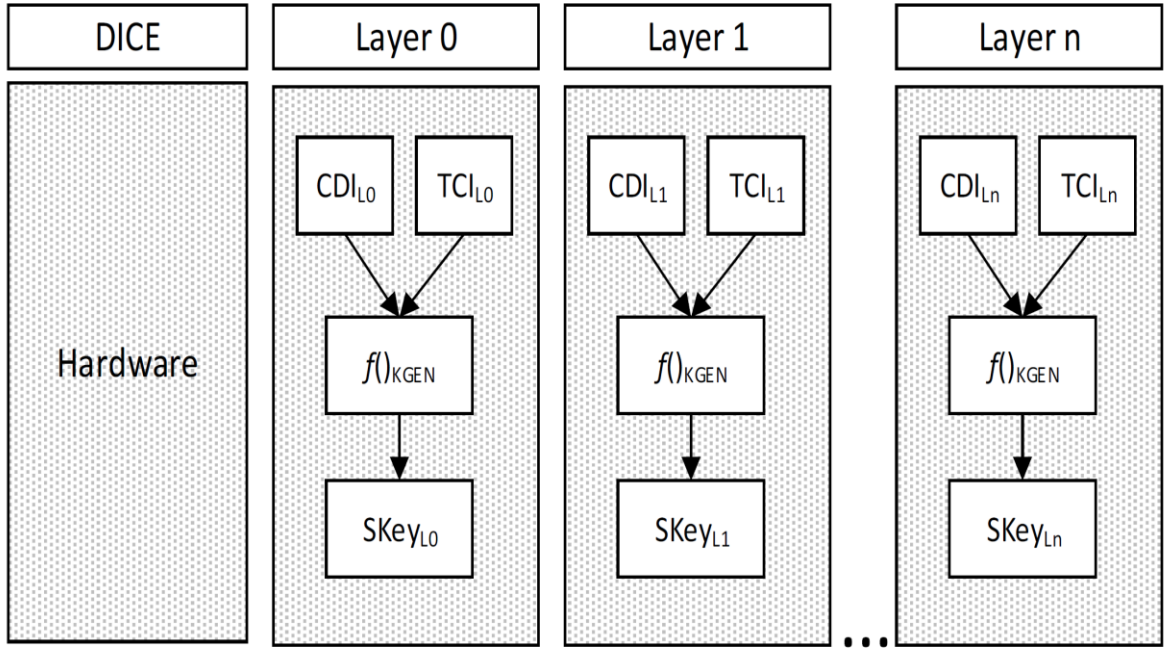


Figure 4: Symmetric key derivation example

DICE – CDI Derivation

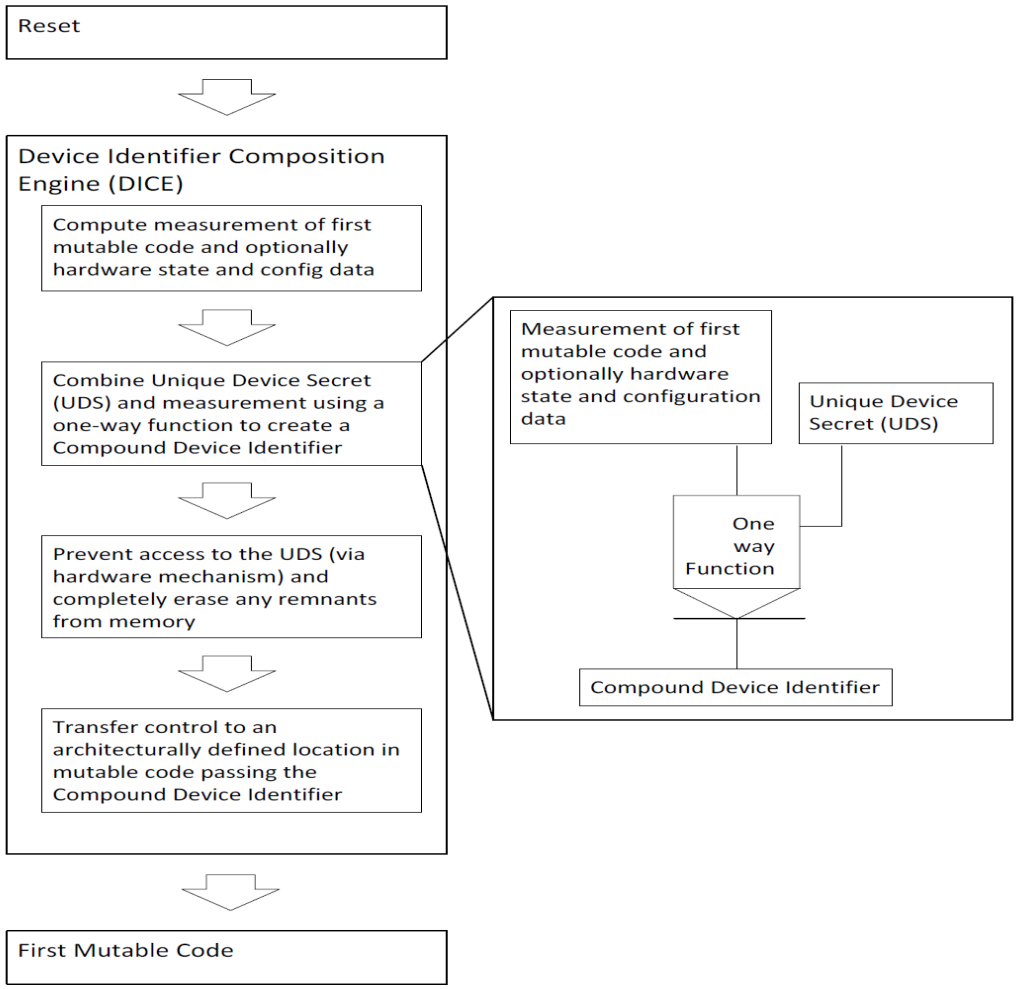


Figure 1: Compound Device Identifier Derivation Process

Note that if the “first mutable code” is immutable for the production life of the device, then the CDI for layer 0 would be same and can act as a basis for a long-lived hardware identity

CDI Derivation – multiple layers