SNIA STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

DICE-SPDM Binding

TCG DICE and DMTF SPDM Binding overview

Chandra Nelogal, DMTS, Dell Technologies

A SNIA Event

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

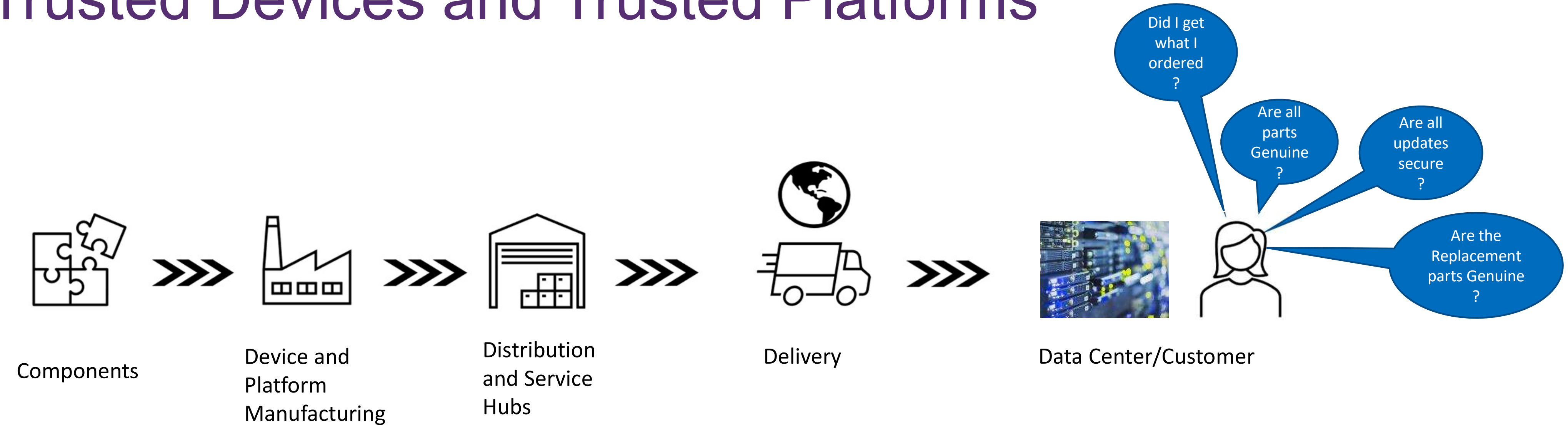
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

TCG DICE and DMTF SPDM Binding Overview - Agenda

- Trusted Devices and Trusted Platforms
- TCG DICE Attestation Overview
- TCG DICE Attestation –Use Cases
- TCG DICE and DMTF SPDM mapping - Certificates
- TCG DICE Measurements

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

Trusted Devices and Trusted Platforms


Did I get what I ordered ?
Are all parts Genuine ?
Are all updates secure ?
Are the Replacement parts Genuine ?
Components
Device and Platform Manufacturing
Distribution and Service Hubs
Delivery
Data Center/Customer

- 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

The DICE attestation architecture focuses on creation, conveyance and appraisal of evidence

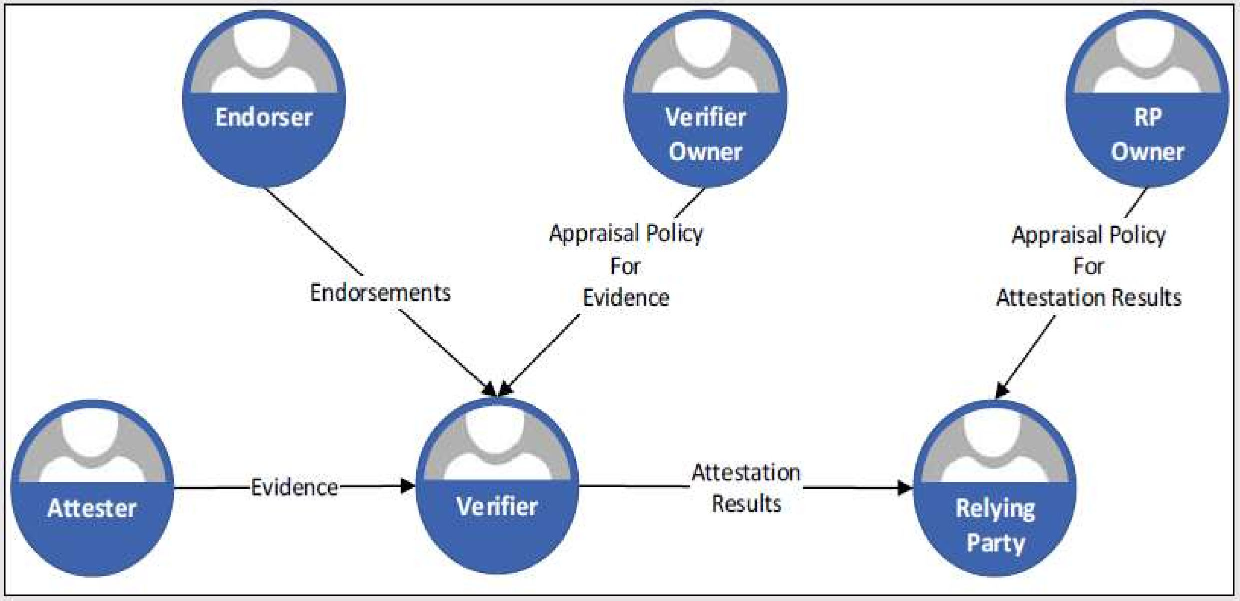


Figure 1: Attestation Roles and message flow

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

TCG DICE Attestation Use Cases (High Level)

TCG DICE Attestation Select few use cases

Use Cases – 1/2

USE CASE	EVIDENCE	VERIFIER (REQUESTER)	ATTESTOR (RESPONDER)	NOTES
Asset Tracking	Device Certificate	Request Certificate	Provide Certificate	Tracking H/W Identity. Device Certificate that's stand alone or that's part of the Alias Certificate chain can be used for hardware 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 can be used for f/w measurements an identity
On Boarding	Alias Certificate(s)	Provision Cert	Add Certificate Chain or add Certificate(s)	Provision a new certificate chain*
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

*
The SPDM specification v1.2 requires that the public (and hence private key as well) key in the leaf or the end entity certificate to be same between certificate slots

Use Cases – 2/2

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)

SNIA STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

DICE and SPDM Binding

Overview

DICE and SPDM Binding

- This session focuses on SPDM and DICE binding
- There is an effort underway at the TCG DICE Work Group to define a mechanism to map the different DICE defined evidence types with the SPDM evidence types
- Need
  - The DMTF SPDM specification – defines mechanisms to exchange 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 and Compound Device Identity (CDI)

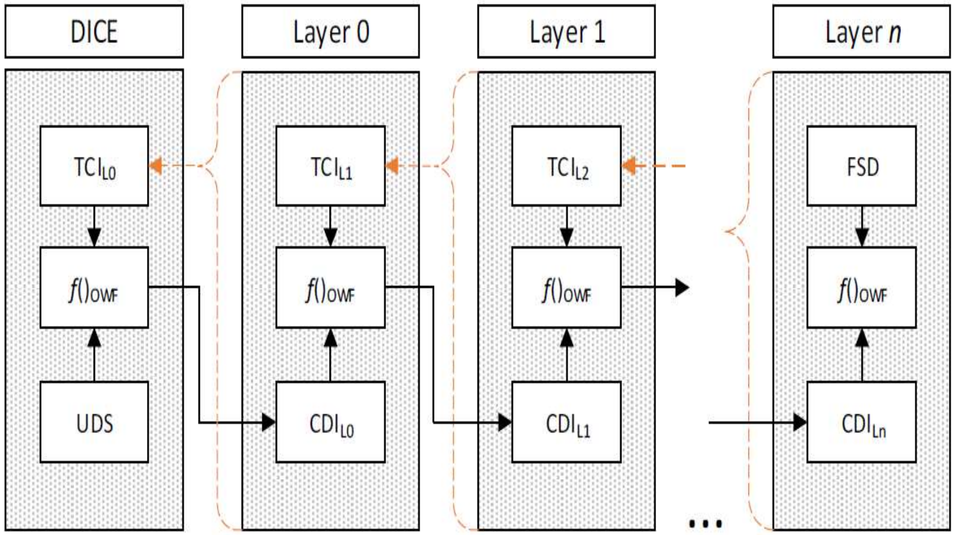


Figure 2: TCB layering architecture

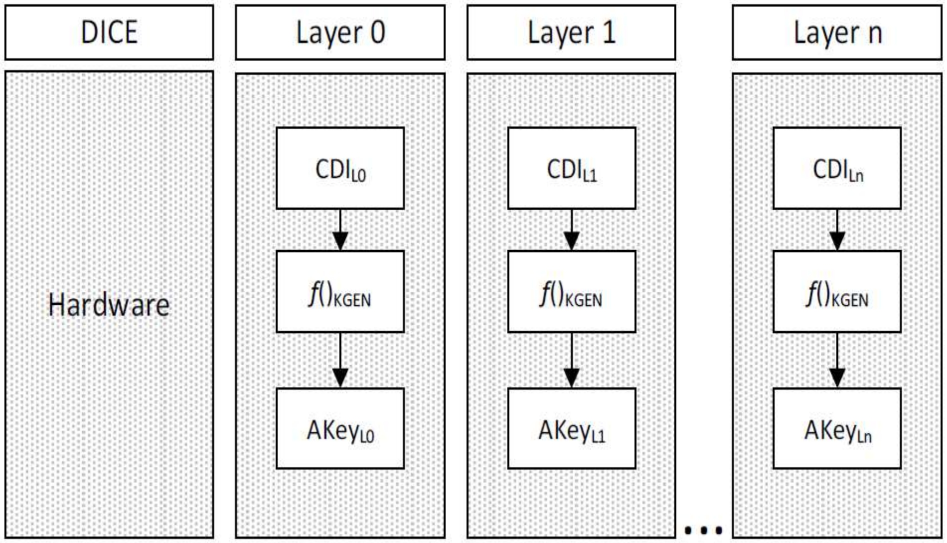
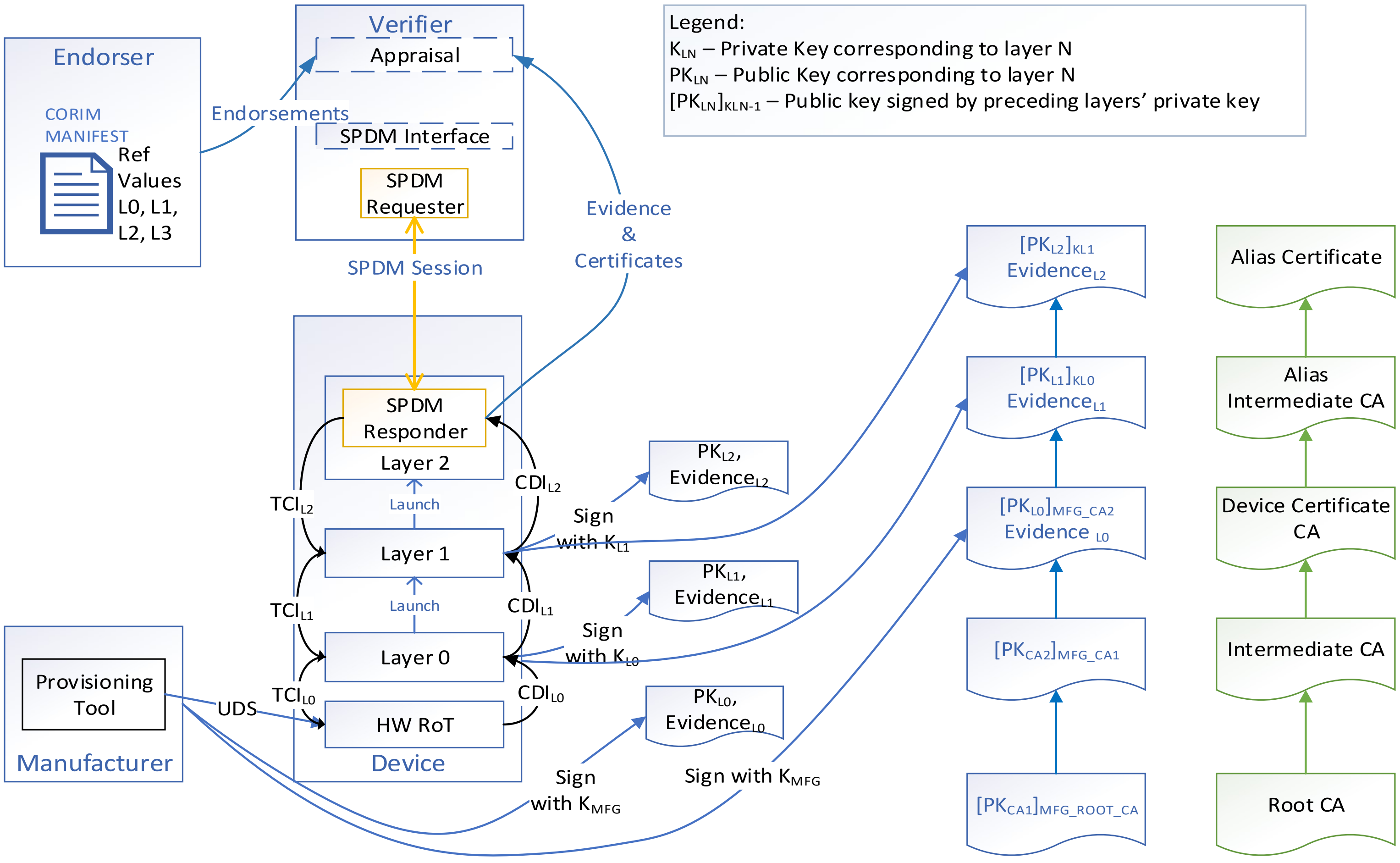


Figure 3: Asymmetric key generation example

DICE and SPDM Certificate models



Legend:

K_{LN} – Private Key corresponding to layer N

PK_{LN} – Public Key corresponding to layer N

$[PK_{LN}]_{KLN-1}$ – Public key signed by preceding layers' private key

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 Local Device ID Certificate	Device Certificate Alias Certificate	In the Device Certificate model described by SPDM, this can map to an end-entity certificate as well. 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

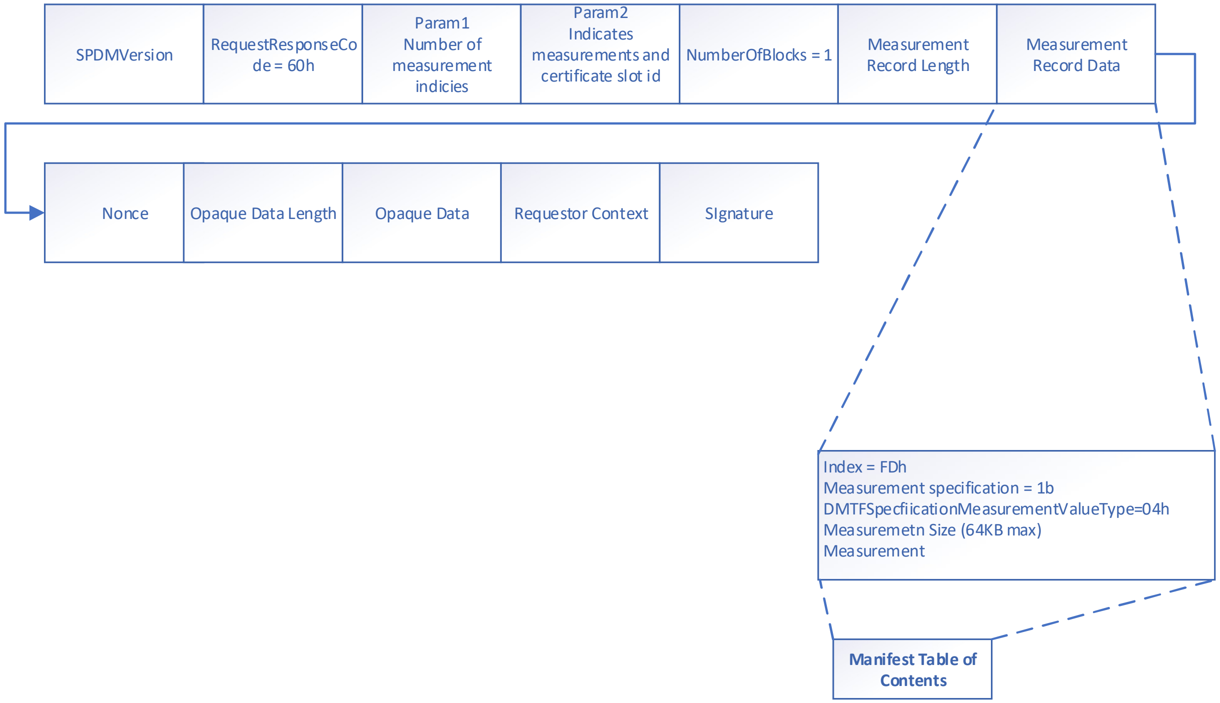
TCG DICE Certificate Profile defines specific OIDs for different certificate types.
SPDM also defines OIDs. An implementation that complies to this binding specification may contain multiple OIDs in the certificates.

Measurements – MEASUREMENTS response

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



SPDMVersion

RequestResponseCode = 60h

Param1 Number of measurement indicies

Param2 Indicates measurements and certificate slot id

NumberOfBlocks = 1

Measurement Record Length

Measurement Record Data

Nonce

Opaque Data Length

Opaque Data

Requestor Context

SIgnature

Index = FDh
Measurement specification = 1b
DMTFSpecfiicationMeasurementValueType=04h
Measuremetn Size (64KB max)
Measurement

Manifest Table of Contents

SNIA® STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Acronyms and References

Section Subtitle

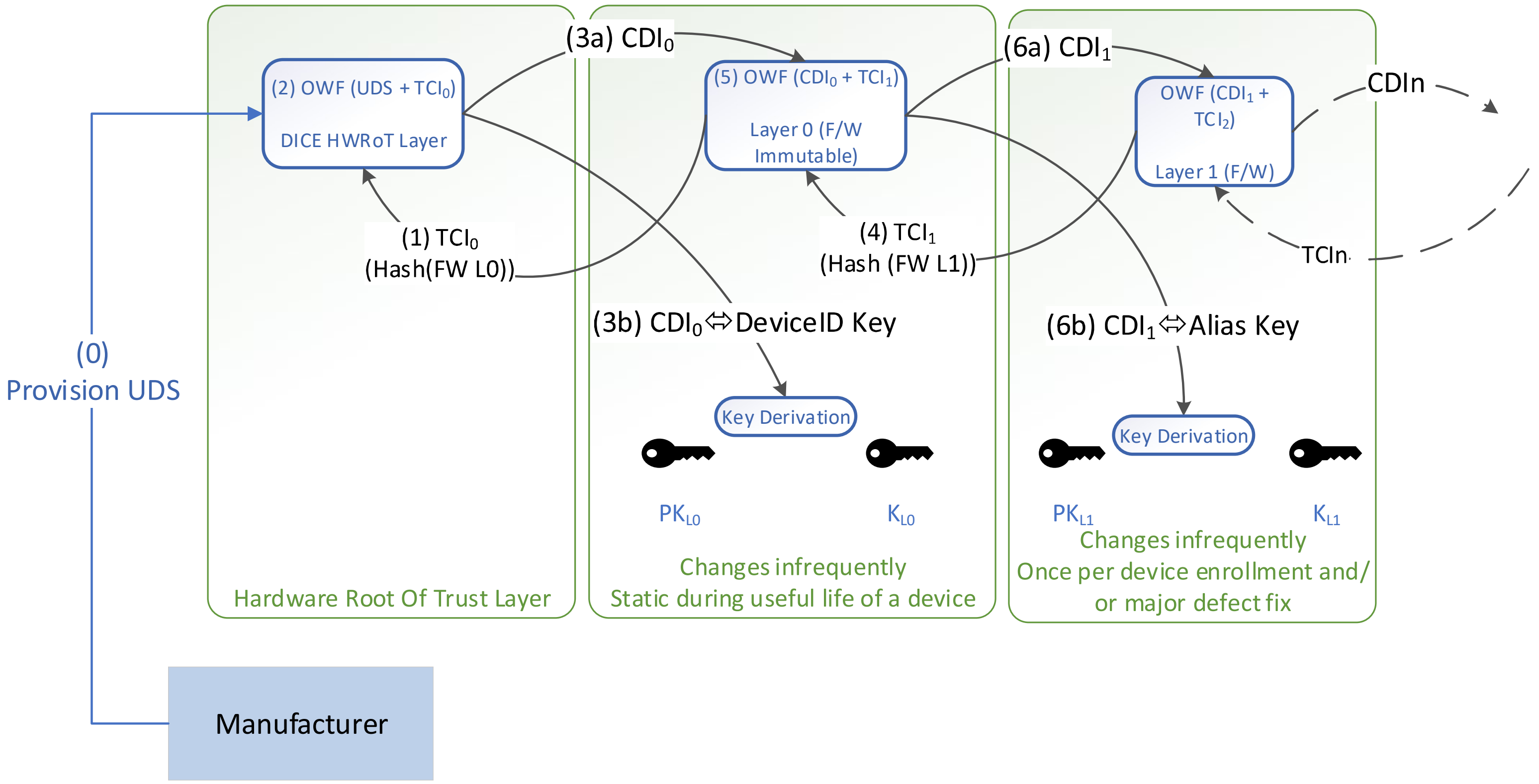
Acronyms

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

TCG DICE Identity computation flow (Detailed)



SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

Please take a moment to rate this session.

Your feedback is important to us.