DICE

Joakim Bech - TF TSC - 2022-11-17

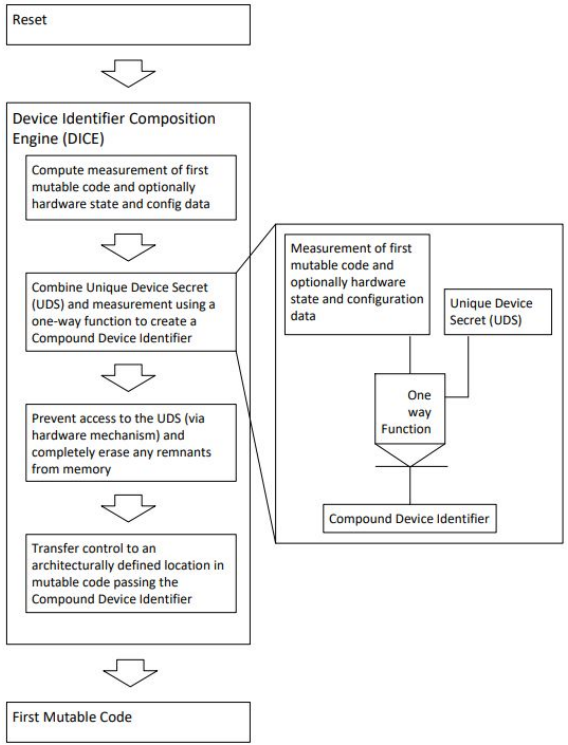
DICE - Device Identity Composition Engine

- TCG standard with industry adoption
- Small footprint and simple key derivation
- Provides a measurement chain that is rooted in the device's identity and based on measured code.
  - In short, key(s) bound to device ID and firmware IDs
- UDS needs to be programmed in fab
- UDS should only be available to ROM code or similar.

CDI = $\boldsymbol{H}_{\textbf{SHA-256}}(\textit{UDS} \mid\mid \boldsymbol{H}_{\textbf{SHA-256}}(\textit{first mutable code}))$

alt.

CDI = $\boldsymbol{HMAC}(\textit{UDS}, \boldsymbol{H}_{\textbf{SHA-256}}(\textit{first mutable code}))$



- Ilias Apalodimas proposed DICE as an improvement to the LEDGE SC earlier this year.

SRC: Hardware Requirements for Device Identifier Composition Engine Level 00, Revision 78

Linaro

Identity Based Device Identity Architecture

- TCG example

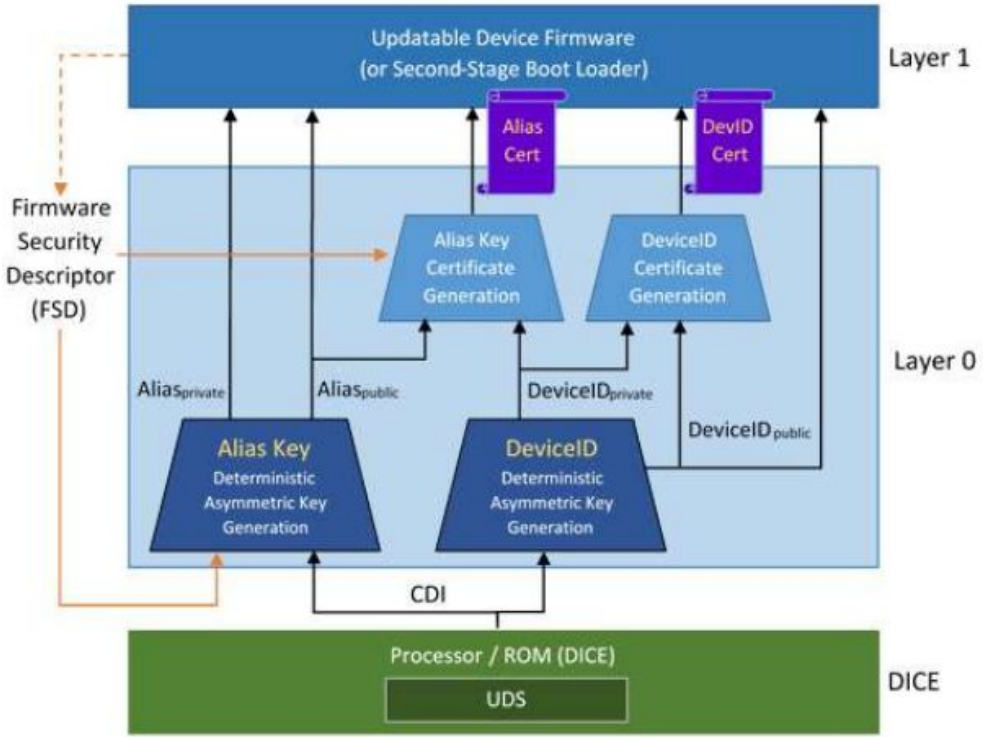
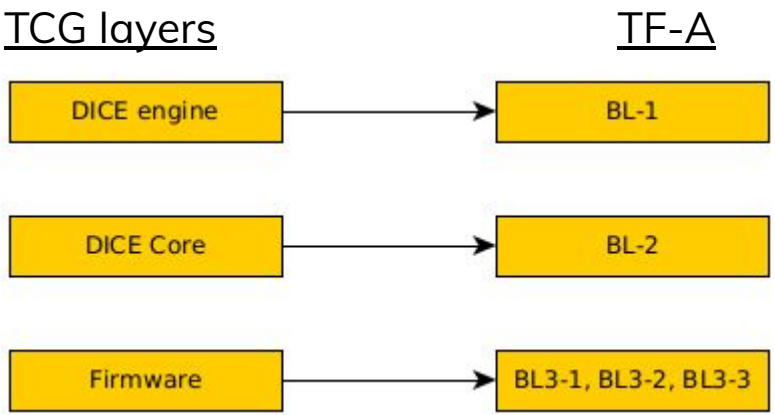


Image source: https://trustedcomputinggroup.org/wp-content/uploads/Foundational-Trust-for-IOT-and-Resource-Constrained-Devices.pdf

DICE in TF-A?

- Prototype work for TF-A proposed at Linaro Jira TS-295.
- Compile time flag, making it optional to use



- Could serve as a lightweight mechanism for attestation and measured boot when there is no TPM device to use

Links

- Hardware Requirements for a Device Identifier Composition Engine
- Microsoft blog post

DICE - Acronyms

UDS – Unique Device Secret

The UDS is a statistically unique per-device secret that is installed or created early in the life of the device and is only accessible to DICE.

CDI – Compound Device Identifier

The value created by DICE and revealed to RIoT Core that depends on the UDS and the measurement (digest) of the First Mutable Code.

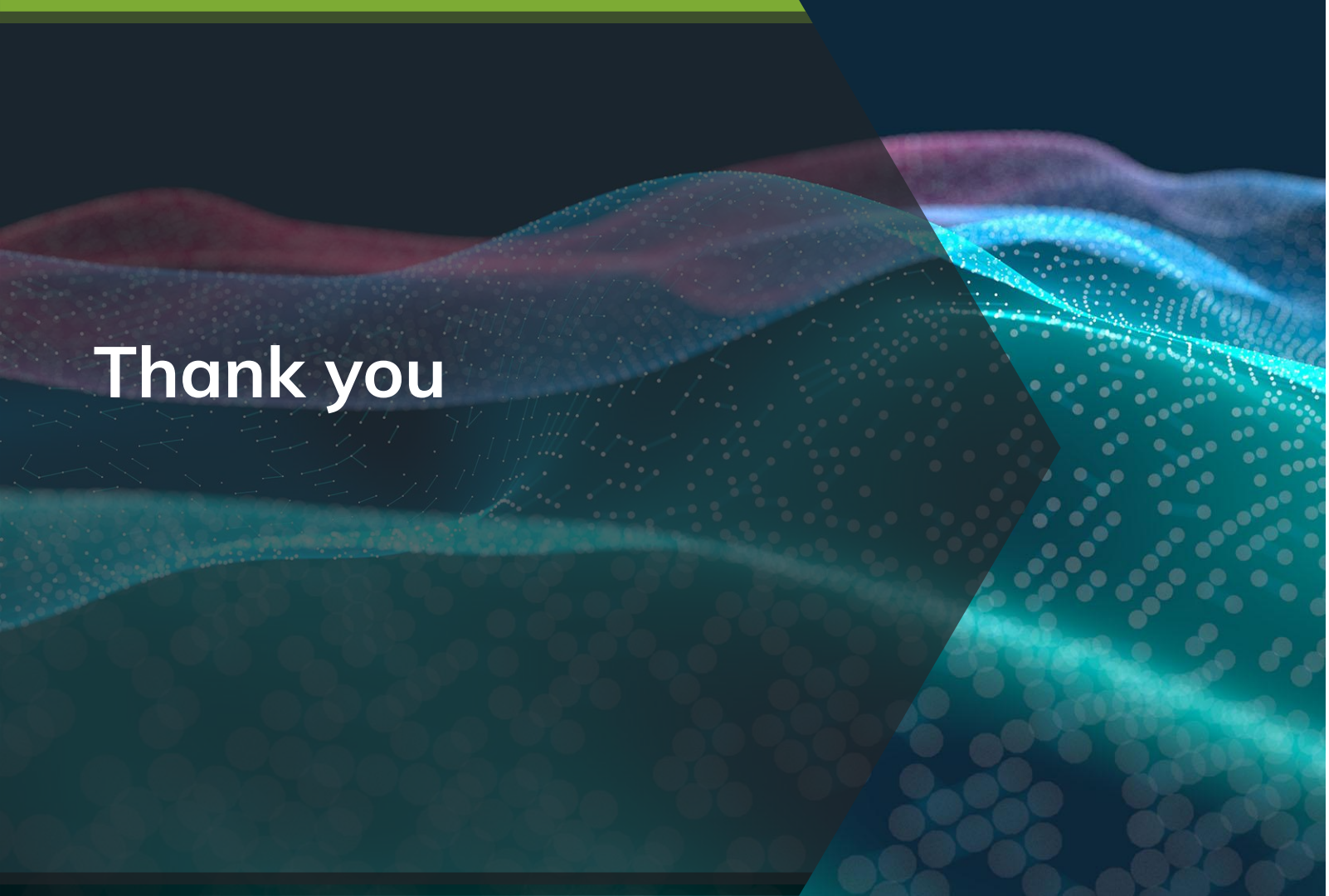
DeviceID – Device Identity Key

An asymmetric key pair (currently an ECC P256 key) that serves as a long-term identifier for the device. The DeviceID key may be self-certified or may be certified by the device vendor. The DeviceID key is created by RIoT Core, and the private key is never released from RIoT Core.

Alias Key/Alias Cert – Alias key and associated certificate

The Alias Key is an asymmetric key pair created by RIoT and provided to Device Firmware. The Alias Certificate is a DeviceID private key signature over the Alias Public Key and device attestation data.

Source: https://develop.trustedcomputinggroup.org/2018/03/20/implementing-dice/



Linaro