ETSI The Standards People

Security Conference

TCG Standards for Zero-Trust: Ensuring Confidentiality, Integrity, and Supply Chain Trust

Presented by:

TRUSTED® COMPUTING GROUP

17/10/2023

Today's Presenter

Silviu Vlasceanu

Senior Technical Expert, Huawei

Silviu Vlasceanu is heading the Trusted Computing and System Integrity Research group at Huawei, where he has been contributing to the adoption of trusted computing solutions based on TCG technologies such as TPM, DICE and cyber-resilience building blocks to improve the system security of routers, server CPUs, BMCs or base stations, from the hardware to platform firmware and operating systems. During the last 7 years, he has been serving in the TCG Technical Committee and Board of Directors and is a co-chair of the Cyber Resilient Technologies WG.

TRUSTED® COMPUTING GROUP

Agenda

- Introduction of the TCG
- TCG standards to mitigate supply chain security risks:
  - TPM
  - DICE
  - FIM
  - RIM
  - CyRes

TRUSTED® COMPUTING GROUP

Trust in Technology

The **Trusted Computing Group (TCG)** is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry specifications and standards which form the backbone of the theory of **Trusted Computing.**

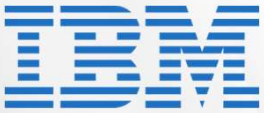
Since the first **Trusted Platform Module (TPM) specification** in 2003, TCG members have embedded the core concepts of **trust** into computers, network elements, smartphones and IoT devices and they have become fundamental to emerging trends such as supply chain security and cyber resilience. TCG **Roots of Trust** are referenced as foundational security building blocks by other standards organizations such as OCP, DMTF and ETSI.

Despite what the names may suggest, **Trusted Computing** and **Zero Trust** are interconnected concepts, providing a framework to eliminate implicit trust through key authentication, attestation, authorization and validation processes.

TRUSTED® COMPUTING GROUP

Our members include…

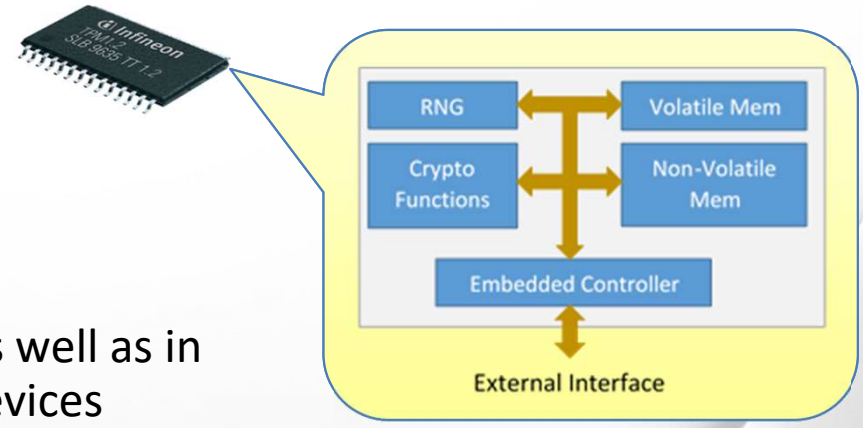
Promoters




Contributors

Trusted Platform Module (TPM)

The Standard Hardware Root of Trust from TCG



- Trusted Platform Module (TPM)
  - Self-contained security processor
  - Inexpensive & small (~0.1 watt, ~$1)
  - Connects to inexpensive processor buses
  - Commonly used in most PCs and servers, as well as in certain network equipment, cars and IoT devices
- TPM provides:
  - Secure storage of boot-time and run-time measurements (= hashes of firmware and software objects)
  - Secure storage of cryptographic secrets (e.g., private keys)
  - Cryptographic-quality Random Number Generator
  - Resistance to physical attack (i.e., reverse-engineering) to keep private keys private

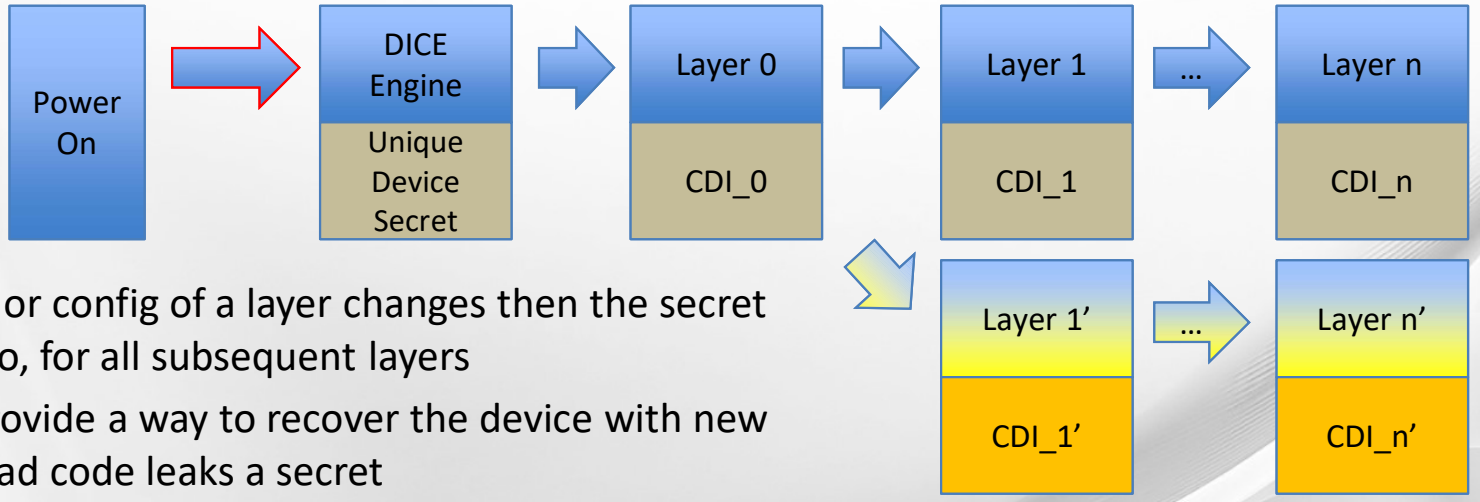
Device Identifier Composition Engine (DICE)

- New set of technology specifications in TCG
- Flexible isolated hardware Root of Trust framework
- Strong cryptographic hardware-based device identity and attestation
- Minimal requirements enable attestation very early in a device or component boot process
- Identity and attestation for any device/component:
  - Minimal (sometimes zero) additional silicon requirements
  - Hardware-based device identity, measurement, and attestation roots
  - Ideal for IoT scenarios, system components and interposers (an interposer can validate code and data loaded from components or persistent storage into a host CPU)

TRUSTED COMPUTING GROUP

The DICE Model

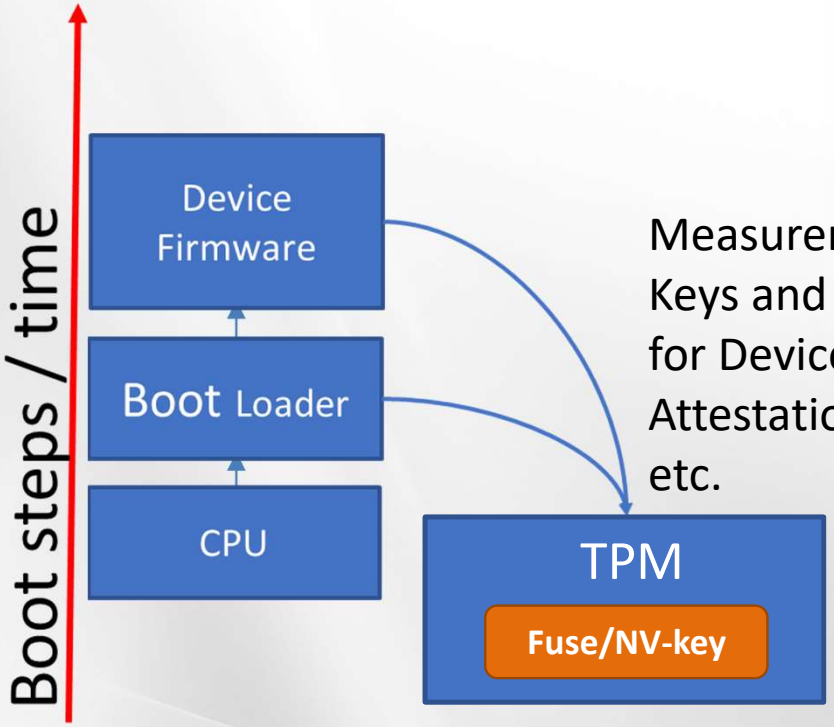
- In a DICE Architecture device startup (boot) is layered
- Beginning with a Unique Device Secret (UDS), secrets/keys called Composite Device Identifiers (CDI) are created, unique to the device and to each layer and configuration
- It means that when different code or configuration is booted, secrets are different



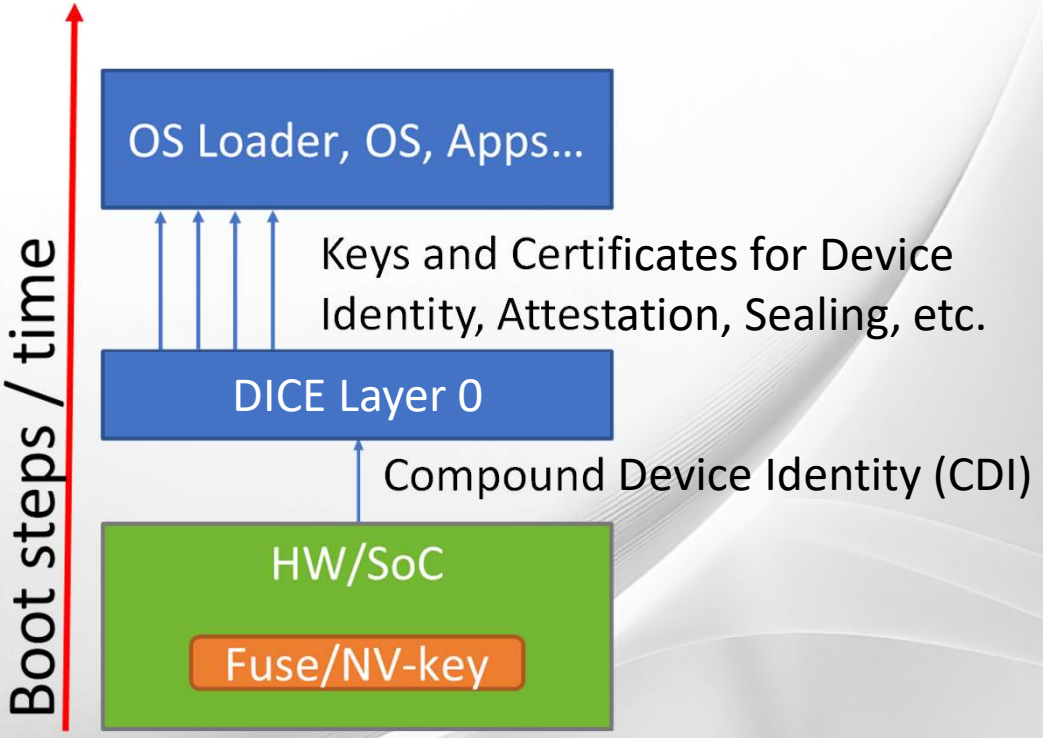
- If the code or config of a layer changes then the secret changes too, for all subsequent layers
- Updates provide a way to recover the device with new secrets if bad code leaks a secret

Chain of Trust in a DICE architecture

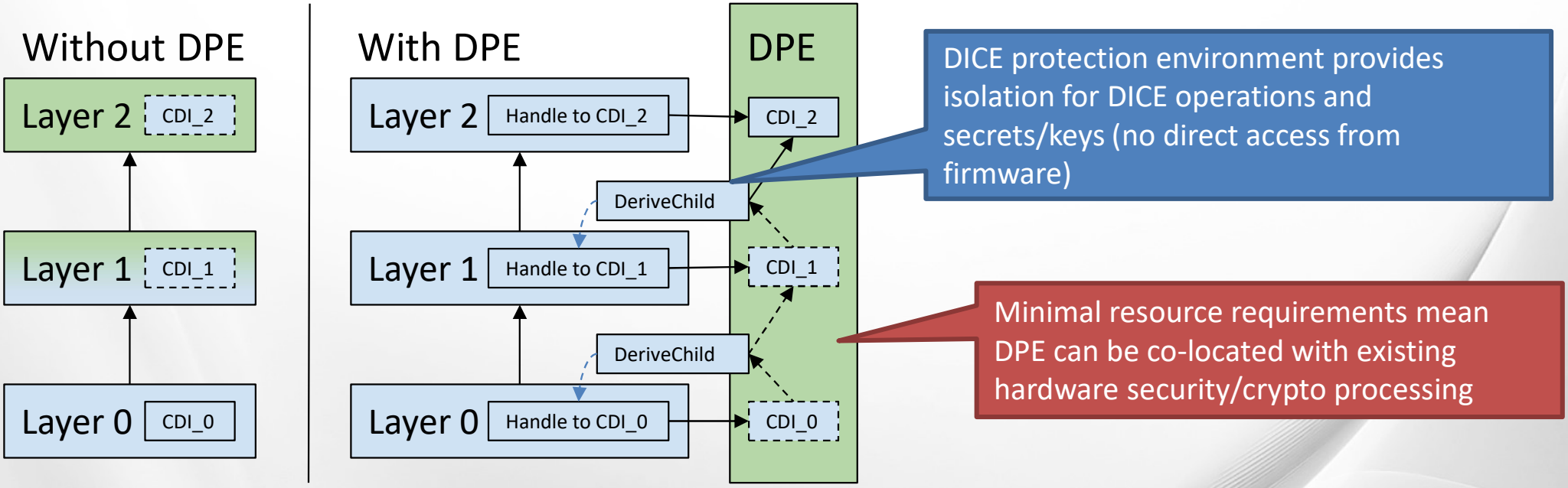
Traditional TPM-based architecture



DICE Architecture

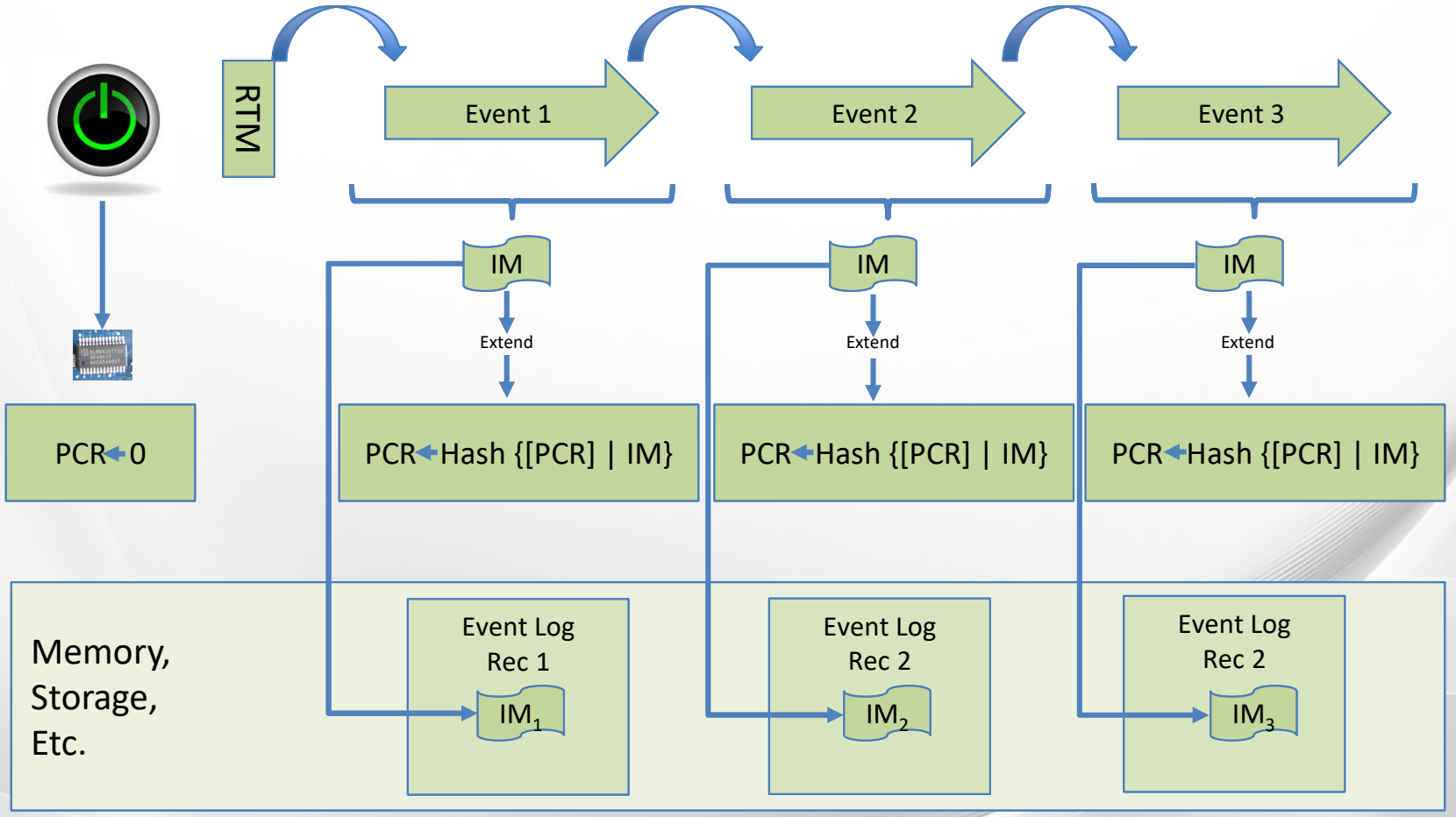


DPE – DICE Protection Environment



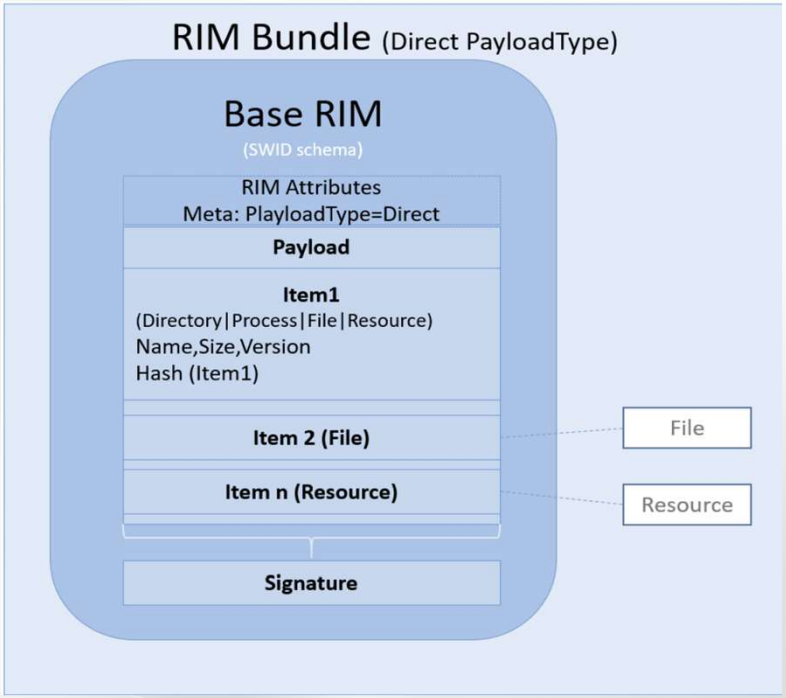
- Defines exactly how to do DICE; get both interoperability and flexibility
- Enforcement of best practices, crypto hygiene, and expensive crypto operations can be asynchronous
- Provides a single implementation for components and policy enforcement for sealing/attestation/etc.

TCG Firmware Integrity Manifest (FIM)

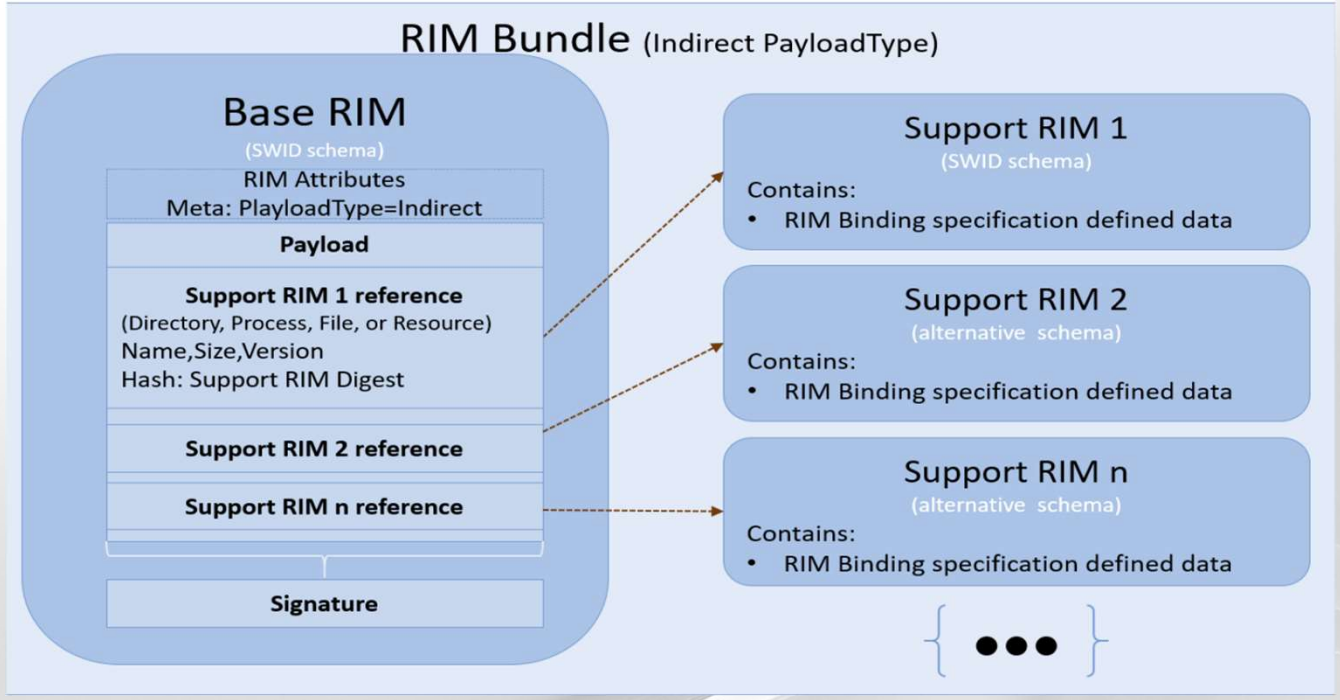


TCG Reference Integrity Manifest (RIM)

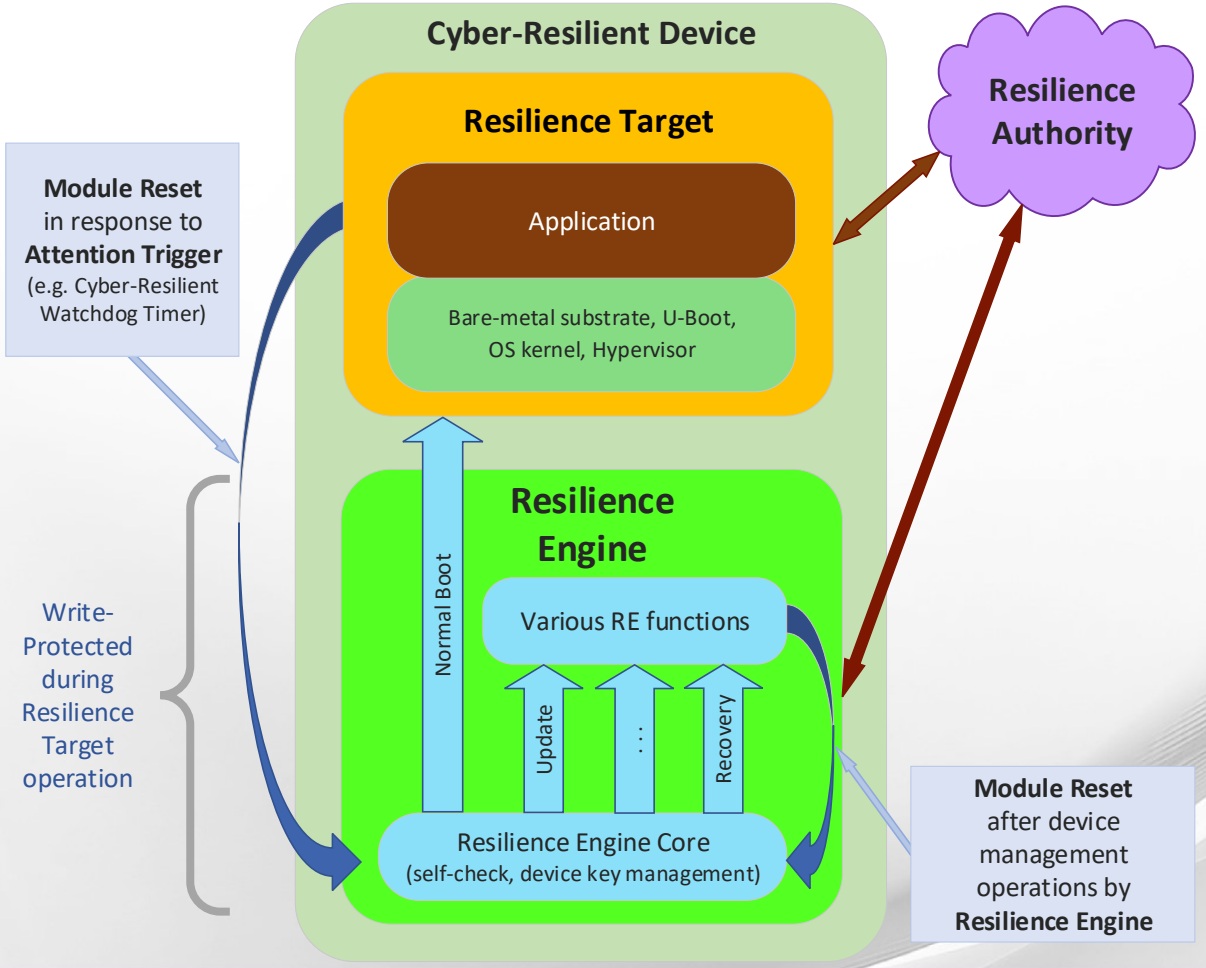
Direct



Indirect



Cyber Resilient Technologies (CyRes WG)



TRUSTED® COMPUTING GROUP

Conclusions

- TCG technologies help mitigate implicit trust in complex devices by building verifiable chains of trust from the hardware roots of trust up to software stacks, enabling network element and endpoints to become the foundation of Zero Trust architectures

- Proven TCG technologies such as TPM, as well as new TCG initiatives such as DICE and CyRes help mitigate supply chain threats such as firmware tampering or device replacement

- TCG standards RIM and FIM aim to enable the interoperable collection and publication of integrity measurements

TRUSTED® COMPUTING GROUP

Questions?

Thank You!

Contacting Trusted Computing Group

Website:
www.trustedcomputinggroup.org

Email:
admin@trustedcomputinggroup.org

LinkedIn:
https://www.linkedin.com/groups/4555624

Twitter:
@TrustedComputin