

This is based on released TCG Specification and existing open source tools.

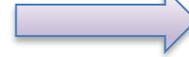
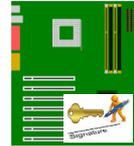
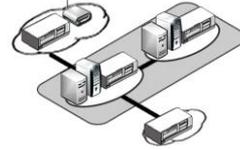
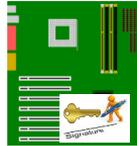
PLATFORM PROVENANCE ATTESTATION

Let's verify the hardware

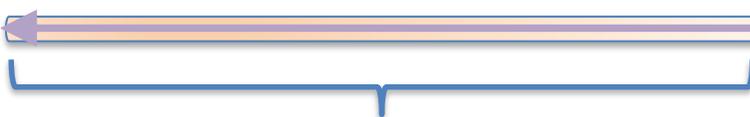
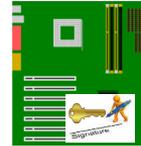
(Referred to as “Trusted Supply Chain” in previous presentations)

Value Proposition

Platform Supplier



Installer



- Counterfeit and substitution detection
- Inventory Tracking
 - Reduced cost **with**
 - Increase trust

- Attestation increases trust and capabilities of analytics

Plant Operator

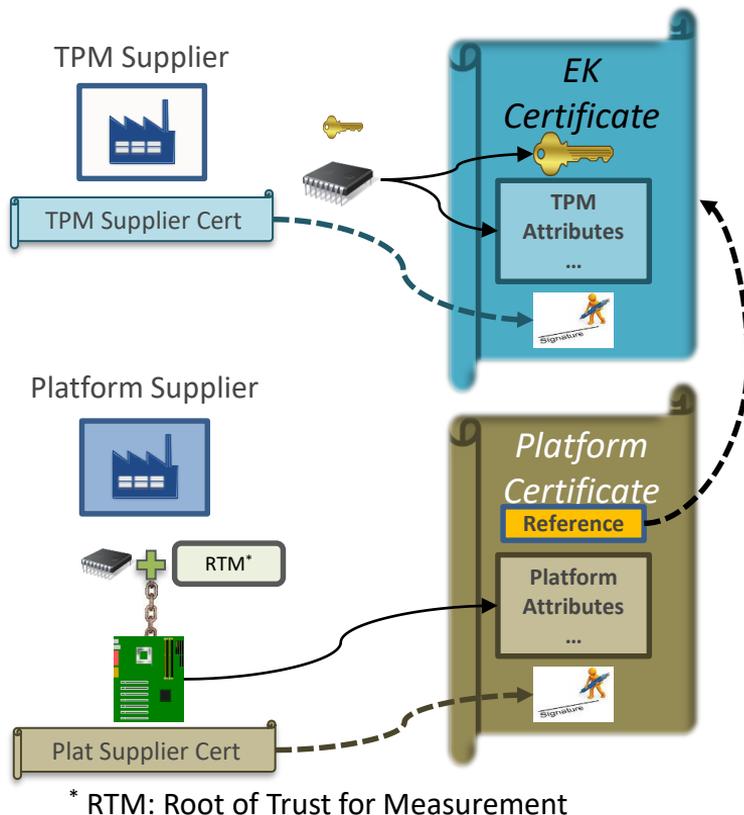


- Reduced *in situ* installation and replacement cost
- Remote proof allow remote key provisioning
- Keys allows trusted remote configuration
- Trusted channels using keys allows multiplexing connections reducing cabling costs

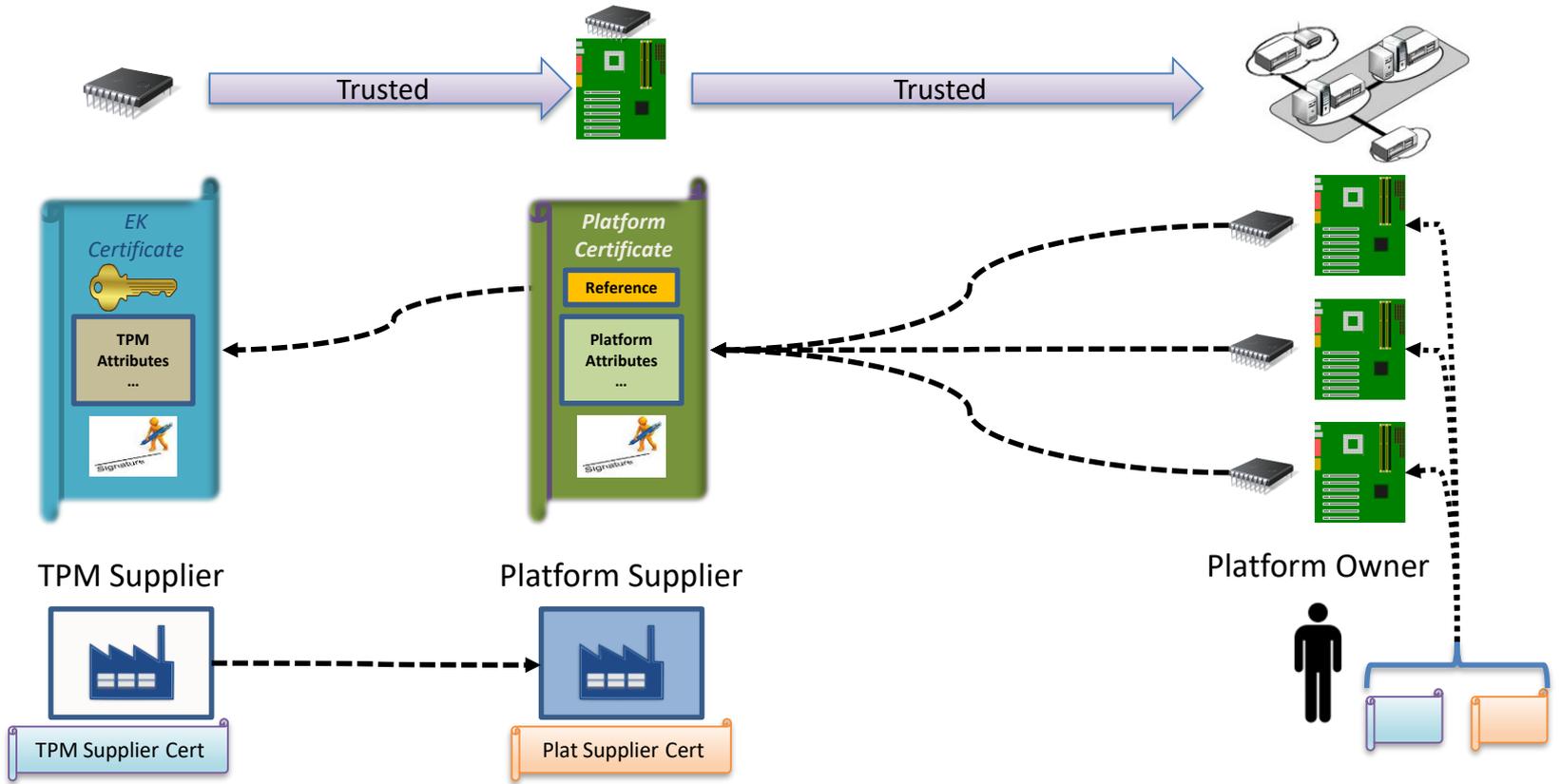


EK to Platform Certificate Binding

- TPM
 - EK Cert signed by TPM Vendor
- Platform Supplier (PM) attaches TPM
 - EK is bound to the Platform
 - Provides a platform-specific key
- Platform Certificate
 - Attributes assert platform information
 - As built data (components)
 - RTM binding to TPM
- Supply chain obtains proof of assertions
 - Verify Platform and EK Certificate signatures
 - Verify EK Certificate bound to that platform



Remote Verification of All Platforms



The RIM work described here is a “Work in Progress” within the Trusted Computing Group.

TCG Members involved with this effort are also active in various IETF forums and will continue collaborate with their relevant forums.

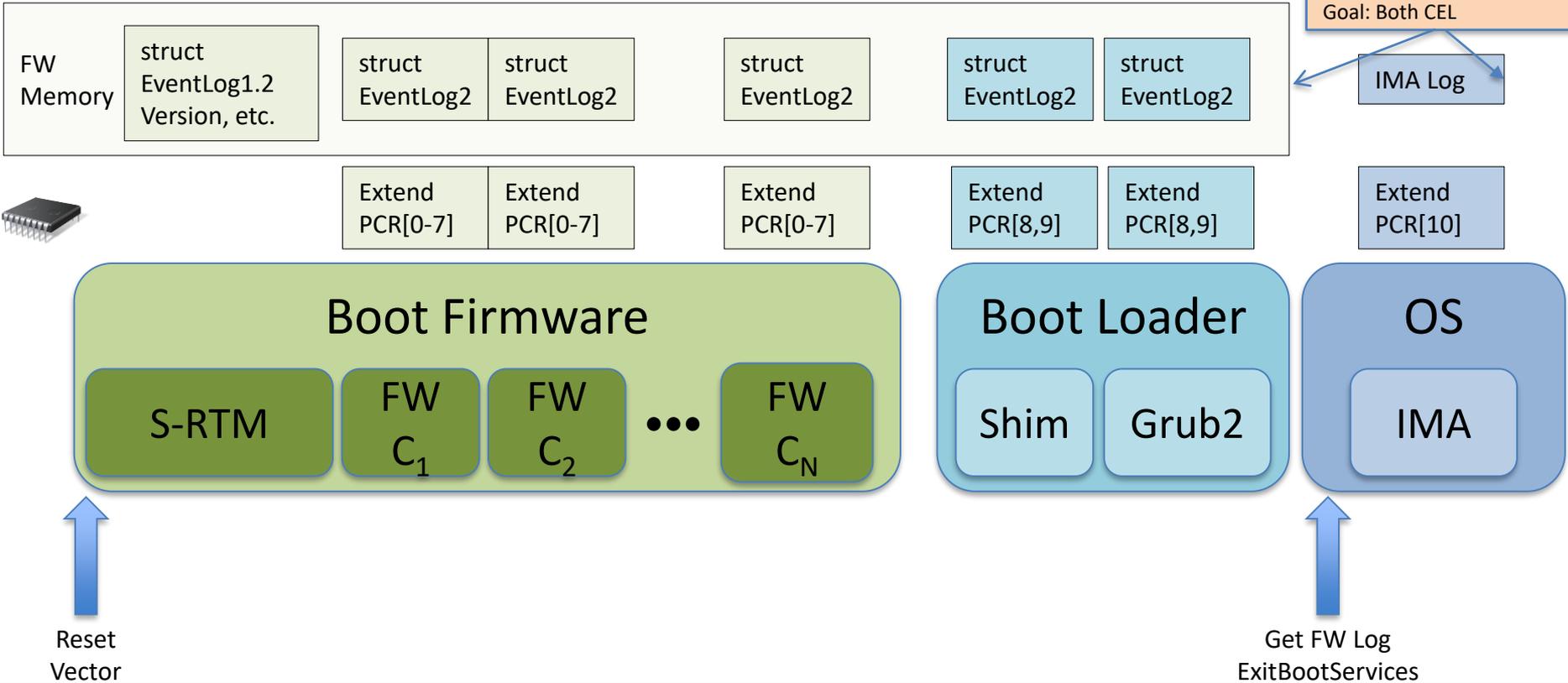
It is presented here for review and discussion only and is subject to change.

REFERENCE INTEGRITY MANIFEST (RIM)

Let's find out the what firmware *should* be there

Platform Boot Sequence (x86/UEFI/TPM2)

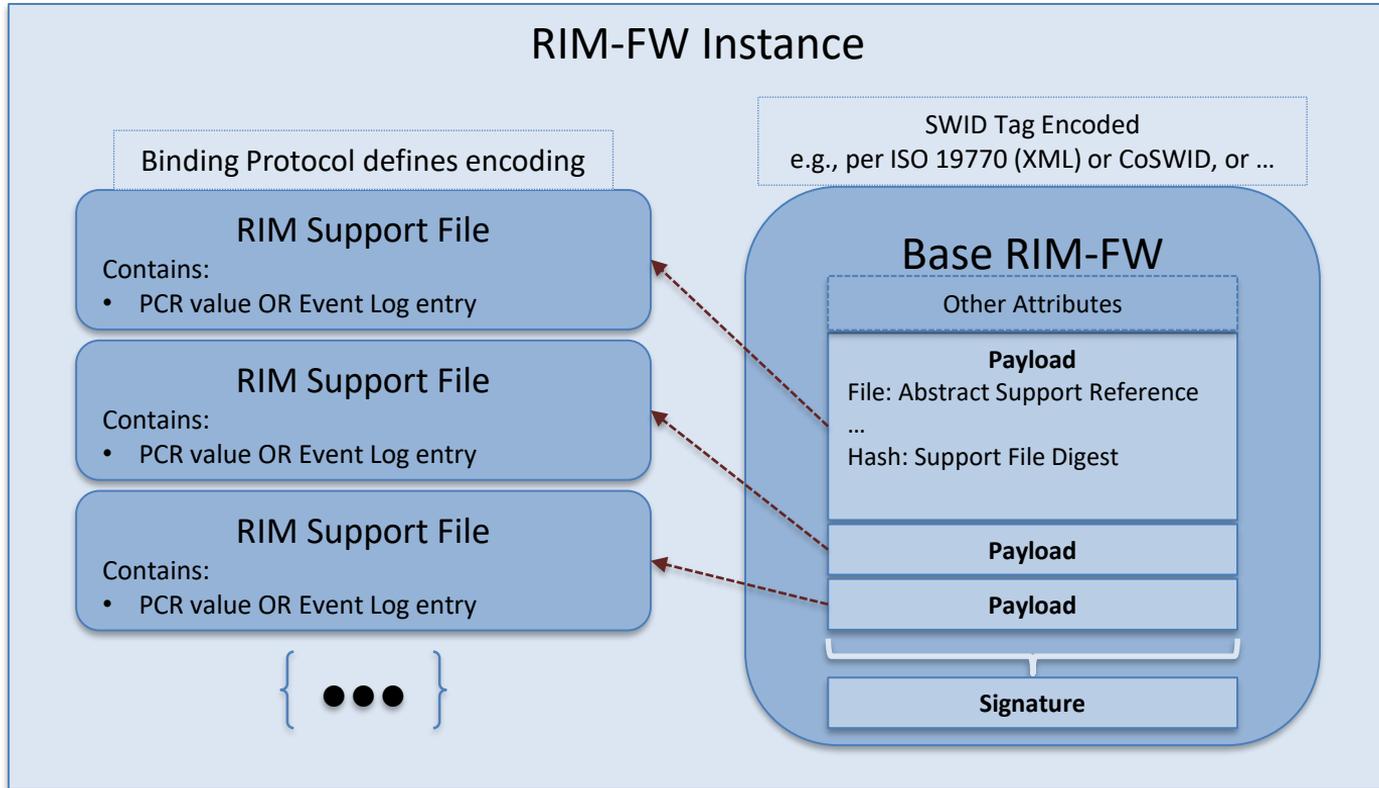
Today: Different formats
Goal: Both CEL



SWID Tag for Firmware Reference

- Problem:
 - SWID Tag (ISO-IEC 19770-2)
 - attributes scoped for files in a filesystem
 - Not Firmware measurements
 - An array of Events representing entities executed in the boot sequence
 - PCRs (I.e., an array of commonly scoped identities)
- Solution:
 - “Another level of indirection”
 - Using existing attributes to reference new and properly scoped data structures

RIM-FW

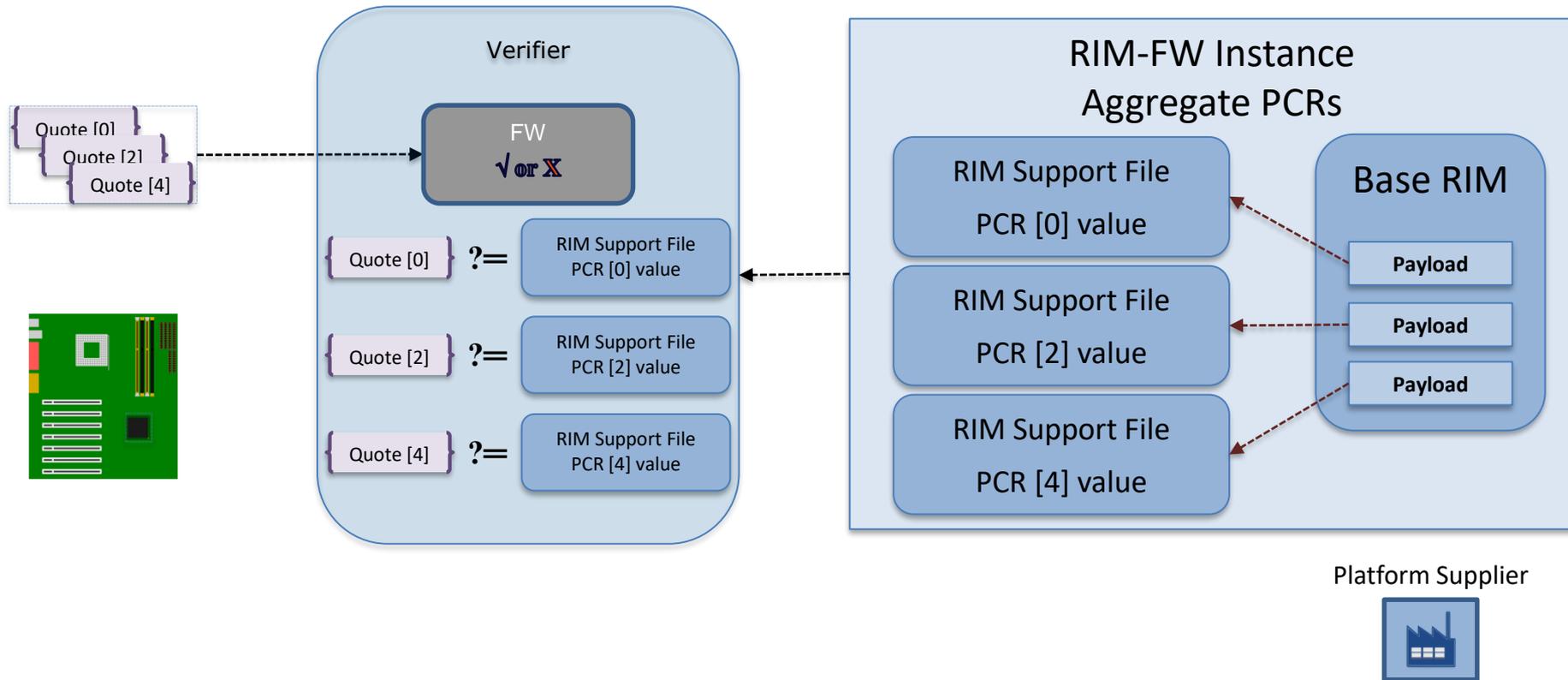


Information Model & Binding Protocols for Firmware

- Information model
 - Defines “what information” is needed to support RIM-FW
 - But not format or delivery
- PC Client RIM Binding Specification (Example)
 - Defines RIM for PC Client Systems
 - Adopts SWID Tag format for base RIM
 - Requires Signature
 - Defines 2 RIM Support Files per RIM instance
 - Snapshots TPM Event Log
 - TPM PCR Snapshot
 - E.g., Places RIM Instance in EFI System Partition (ESP)

Provides only expected "end-state"

Example RIM-FW w/ PCR Values



Thank You

Useful Links

Trusted Computing Group

<https://trustedcomputinggroup.org/>

TCG Platform Certificate Profile

https://trustedcomputinggroup.org/wp-content/uploads/IWG_Platform_Certificate_Profile_v1p1_r15_pubrev.pdf

Prototype Acceptance Test for SCRMM using Platform Certificates

<https://github.com/nsacyber/hirs>

Tools for Platform Certificates

<https://github.com/nsacyber/paccor>

https://PlatformCertTool/PCVT_TPM20