Supply Chain Assurance Using TCG Technology

Trusted Computing Group
2024-01-23

Joshua Schiffman, HP Inc.
Monty Wiseman, Beyond Identity

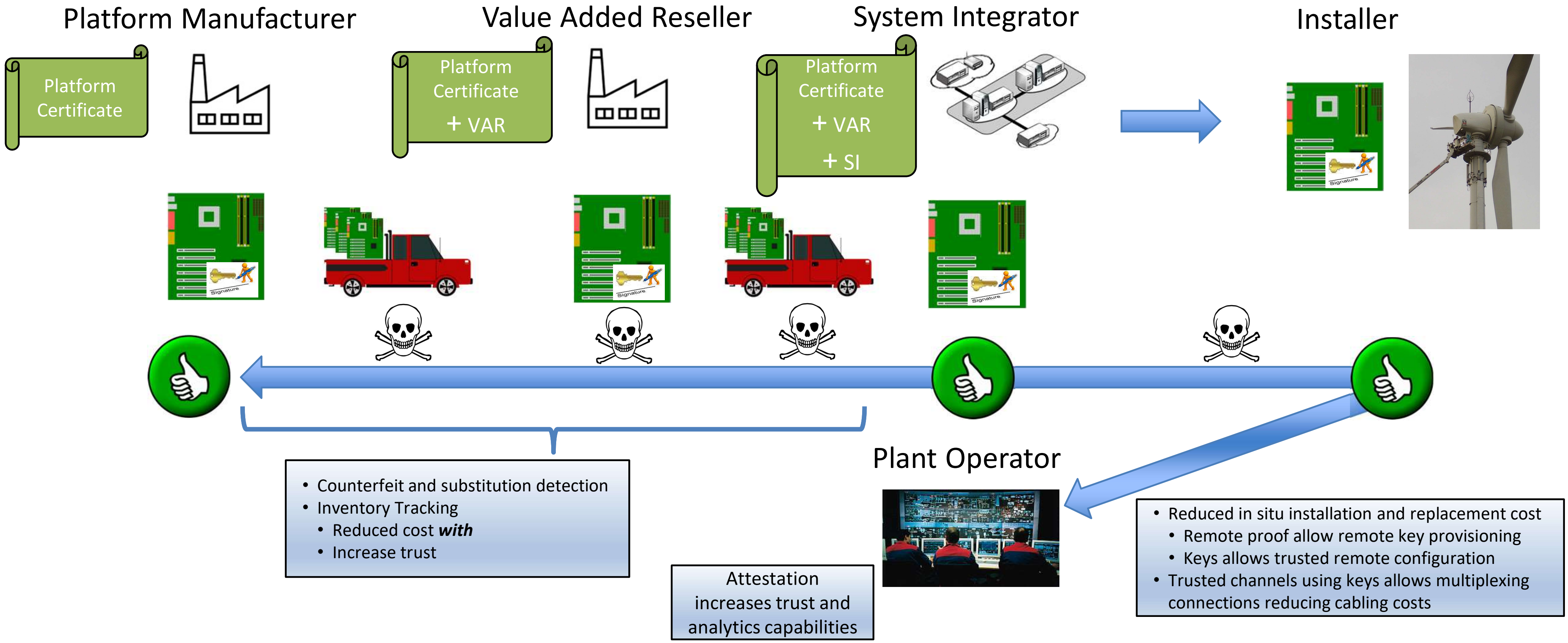
Trusted Supply Chain

- Problem
  - Assurance of a device’s origin in today’s diverse manufacturing, logistics, and just in time inventory.
  - Remote deployment and provisioning requires assurance in the Supply Chain.
    - — Reduce reliance on physically tracking devices through the Supply Chain
    - — Reduces cost, decreases service time, …
- Solution
  - Use a Root of Trust to provide assurance of a device’s origin
  - This Root of Trust establishes the foundation for a Trusted Supply Chain
- We will explain the use of a hardware Root of Trust to establish a Trusted Supply Chain

TCG Supply Chain Assurance

- Verifiable HBOM artifacts produced by each entity in the Supply Chain
  - Using interoperable signed certificates (signed X509)
- Root of trust verifiably binds BOM to platform
- Supports complex chain VAR / SI / OEM chains
- Extends into verifying boot path firmware / software
  - Software Bill of Material (including Firmware)
- NCCoE Project early work presented in May 2019
- New features: Extensible traits and assertions (more later)

Supply Chain Using TCG Technology



Platform Manufacturer

Platform Certificate

Value Added Reseller

Platform Certificate + VAR

System Integrator

Platform Certificate + VAR + SI

Installer

Plant Operator

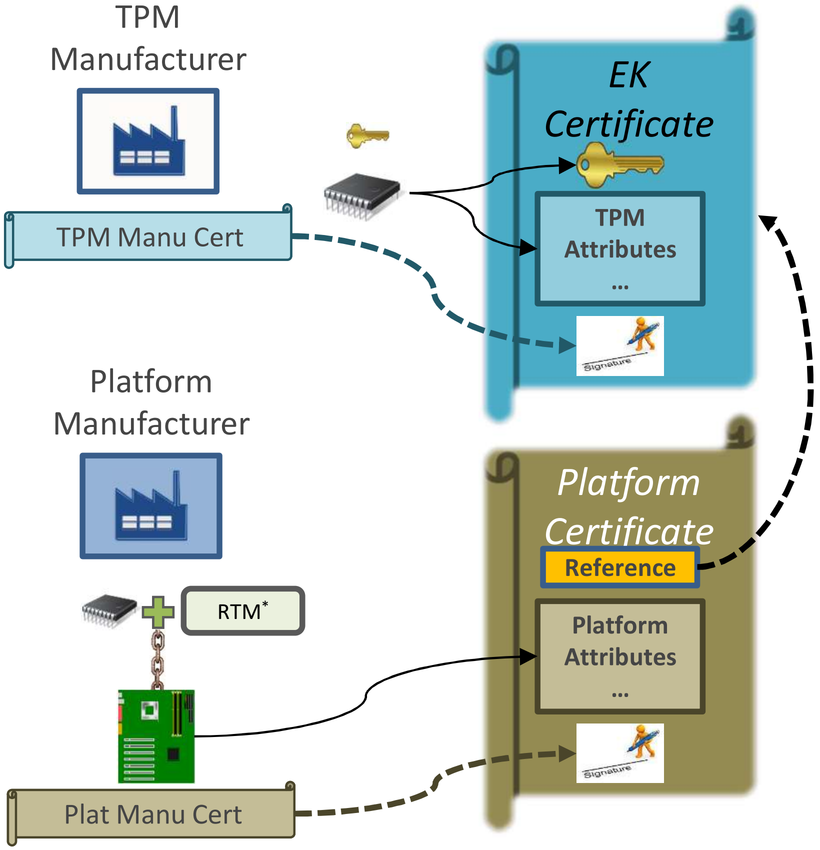
- Counterfeit and substitution detection
- Inventory Tracking
  - Reduced cost ***with***
  - Increase trust

Attestation increases trust and analytics capabilities

- 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

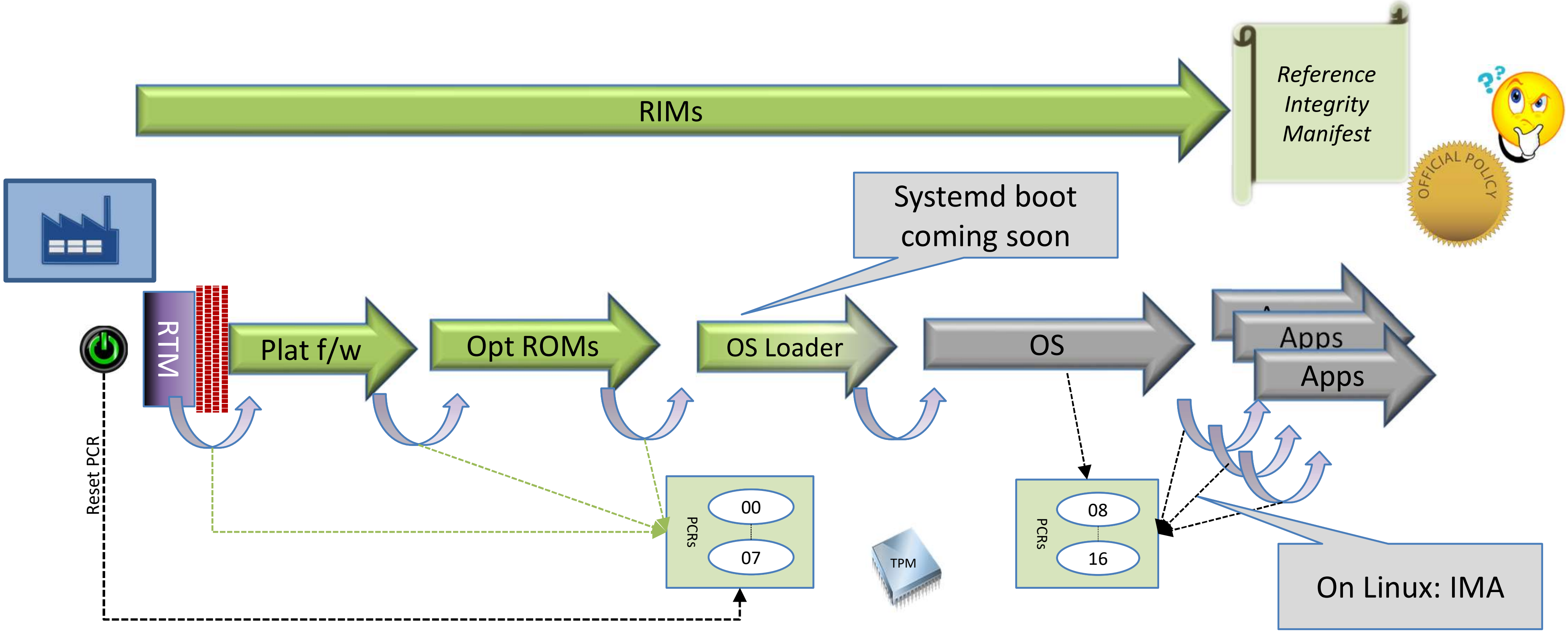
Supply Chain using TPM

- TPM
  - EK Cert signed by TPM Vendor
- Platform Manufacturer attaches TPM
  - EK is bound to the Platform
  - Provides a platform-specific key
- Platform Certificate
  - Attributes assert information about the platform
    - 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



* RTM: Root of Trust for Measurement

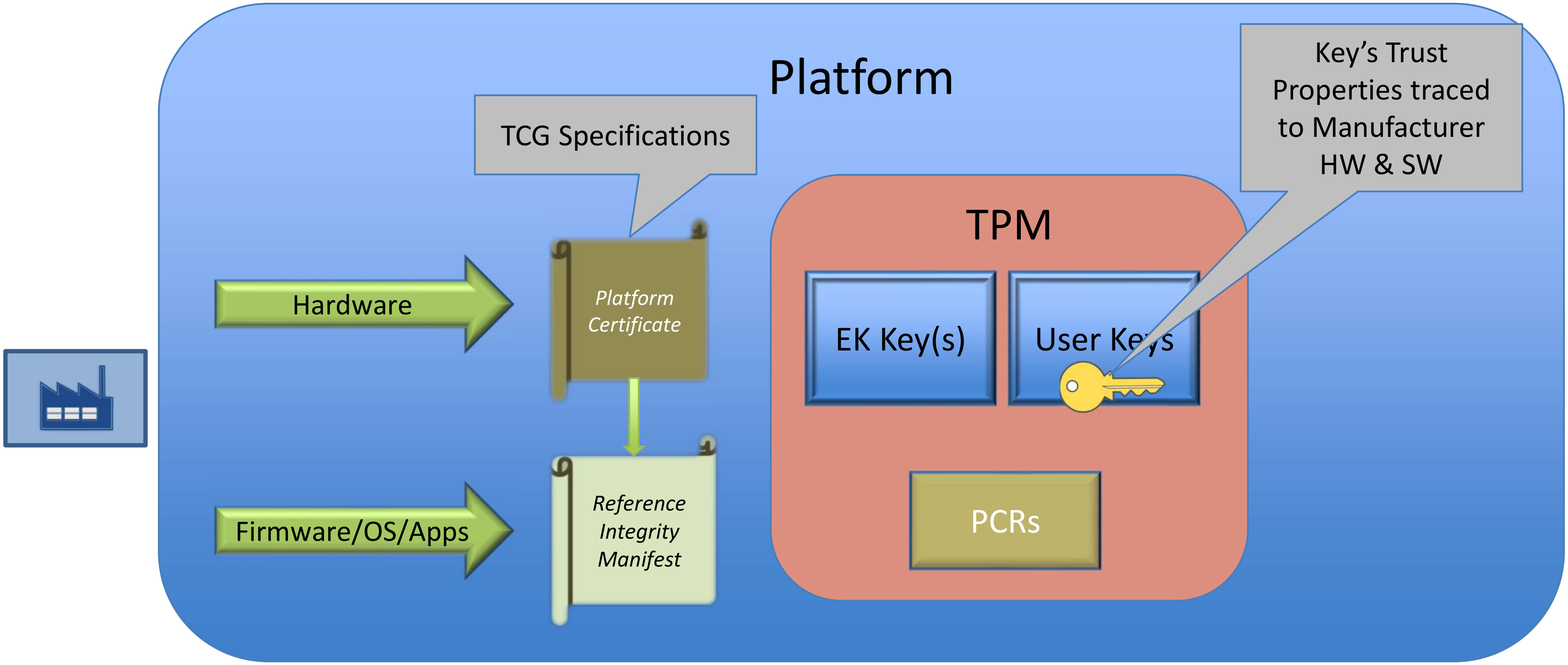
Trust Chain for Firmware



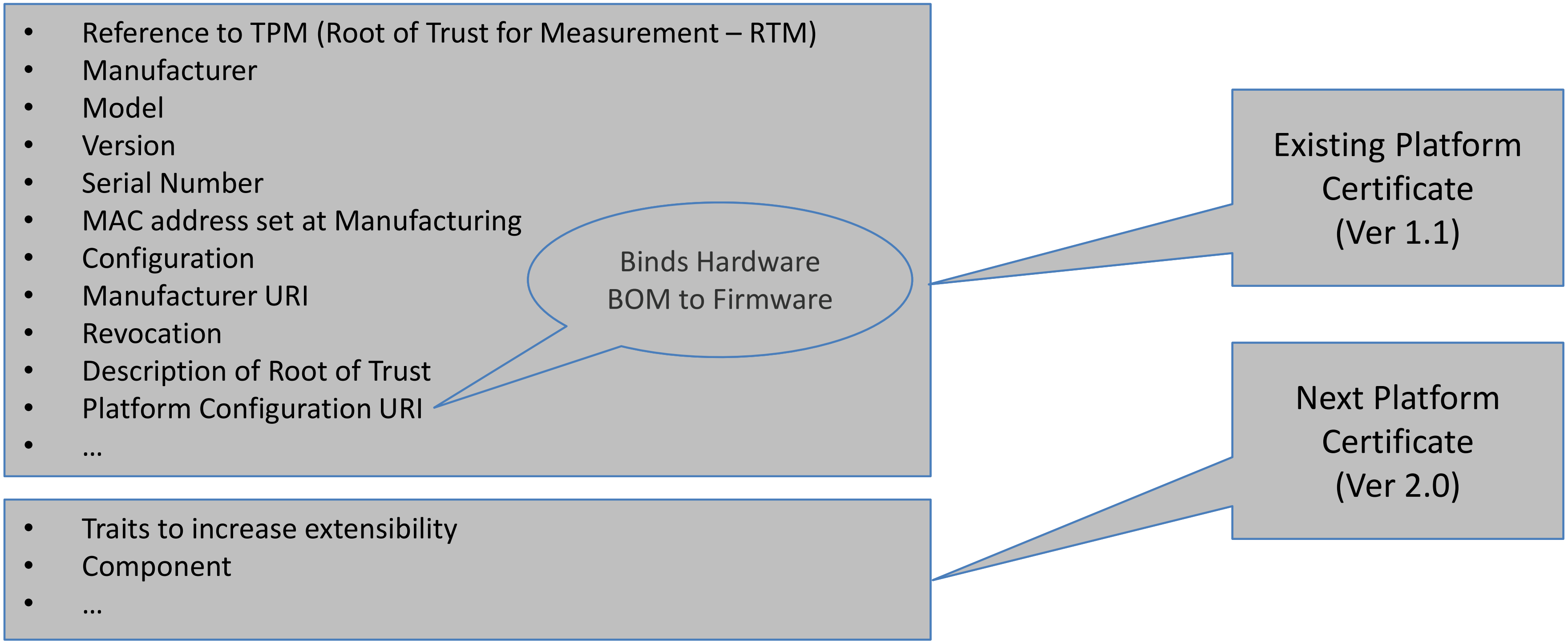
Systemd boot coming soon

On Linux: IMA

TPM General Architecture



TCG Platform Certificate, Next



- Reference to TPM (Root of Trust for Measurement – RTM)
- Manufacturer
- Model
- Version
- Serial Number
- MAC address set at Manufacturing
- Configuration
- Manufacturer URI
- Revocation
- Description of Root of Trust
- Platform Configuration URI
- …

Binds Hardware BOM to Firmware

Existing Platform Certificate (Ver 1.1)

- Traits to increase extensibility
- Component
- …

Next Platform Certificate (Ver 2.0)

TCG-Based Reference Projects

- HIRS: https://github.com/nsacyber/HIRS
- PACCOR: https://github.com/nsacyber/paccor
- HPE PCVT: https://github.com/HewlettPackard/PCVT
- Linux
  - TCG Platform Certificates supported by Fedora and other distros KVM.
    - E.g., https://github.com/stefanberger/swtpm
- Openssl support for Platform Certificates (in development):
  - https://github.com/TrustedComputingGroup/openssl
- NIST NCCoE Supply Chain Project:
  - https://www.nccoe.nist.gov/supply-chain-assurance

Some Example Implementations

- Dell Technologies – Secured Component Verification
  - https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/secured-component-verification-datasheet.pdf
- Dell Technologies – Secured Component Verification for Power Edge
  - https://www.dell.com/en-us/lp/dt/open-manage-secure-component-authentication
- HP Inc. – HP Platform Certificate
  - https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3109ENW
  - https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3108ENW
- Hewlett Packard Enterprise
  - PCVT repository: https://github.com/HewlettPackard/PCVT/
- Intel Corporation – Intel Transparent Supply Chain
  - https://www.intel.com/content/www/us/en/products/docs/servers/transparent-supply-chain.html

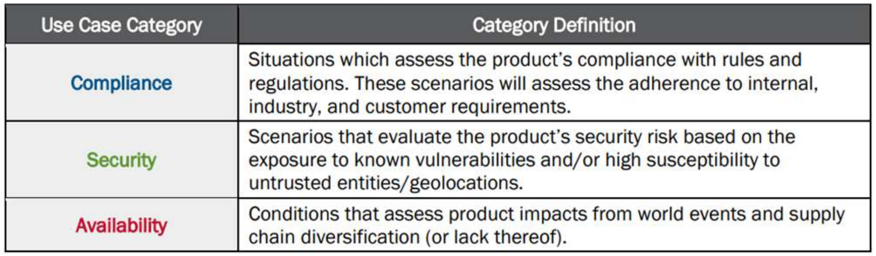
A brief description from the manufacturer of each is provided after the “Questions?” slide

CISA HBOM Framework

- CISA HBOM Framework, published Sept 2023[1], calls for HBOMs to carry data fields to address critical use cases

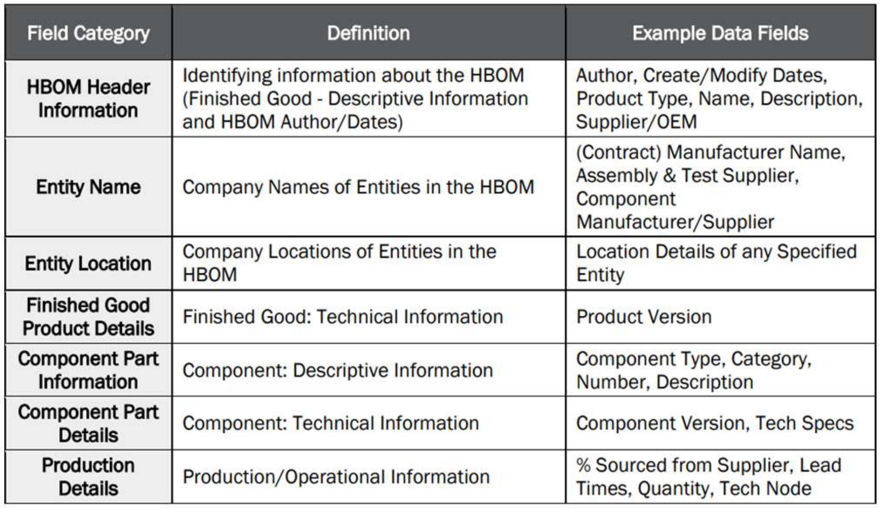
- TCG Platform Certificates support many of these fields and can be extended to remaining fields

TABLE 1: USE CASE CATEGORY DEFINITIONS



Use Case Category	Category Definition
Compliance	Situations which assess the product's compliance with rules and regulations. These scenarios will assess the adherence to internal, industry, and customer requirements.
Security	Scenarios that evaluate the product's security risk based on the exposure to known vulnerabilities and/or high susceptibility to untrusted entities/geolocations.
Availability	Conditions that assess product impacts from world events and supply chain diversification (or lack thereof).

TABLE 3: HBOM DATA FIELD CATEGORIES

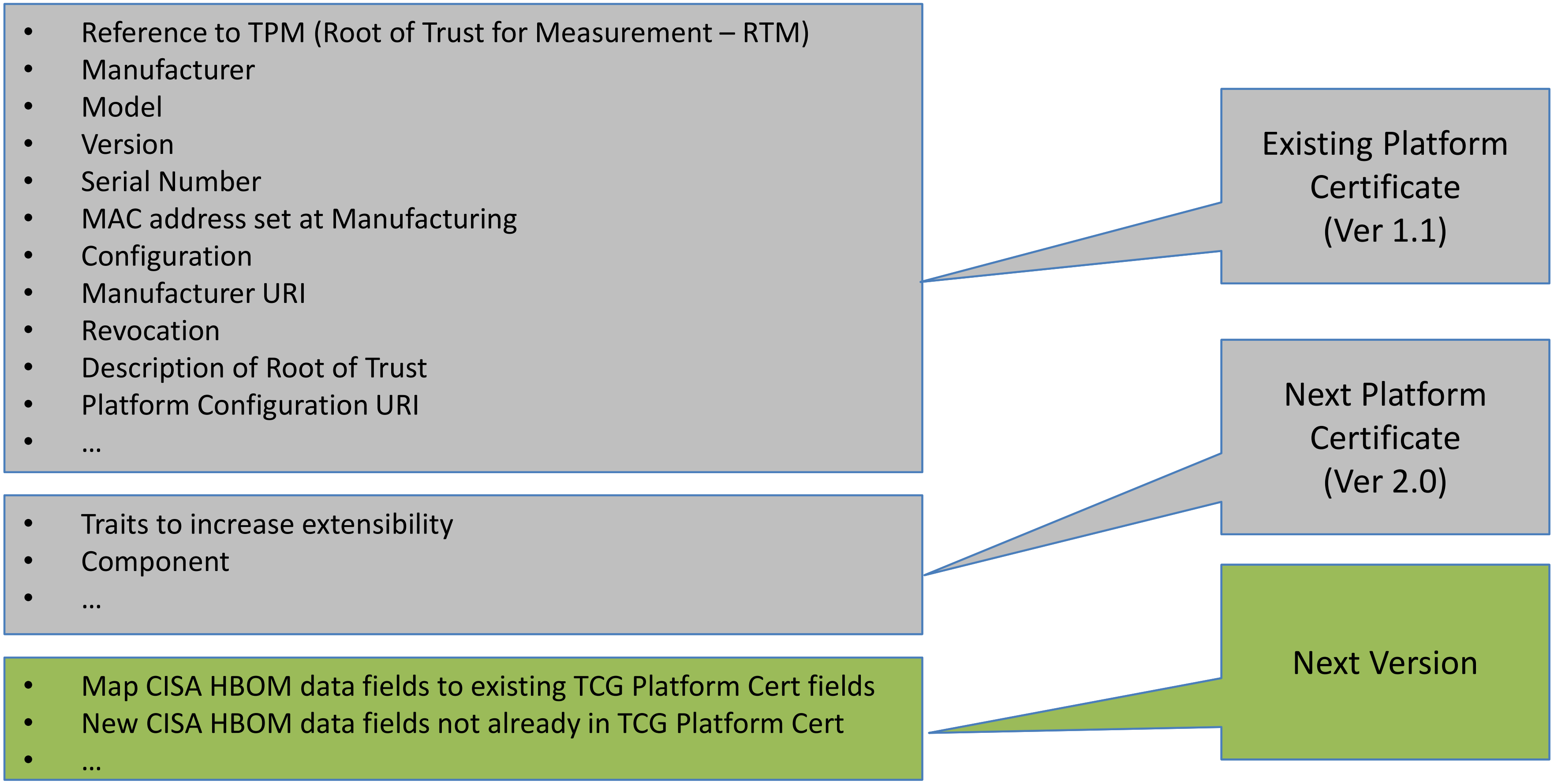


Field Category	Definition	Example Data Fields
HBOM Header Information	Identifying information about the HBOM (Finished Good - Descriptive Information and HBOM Author/Dates)	Author, Create/Modify Dates, Product Type, Name, Description, Supplier/OEM
Entity Name	Company Names of Entities in the HBOM	(Contract) Manufacturer Name, Assembly & Test Supplier, Component Manufacturer/Supplier
Entity Location	Company Locations of Entities in the HBOM	Location Details of any Specified Entity
Finished Good Product Details	Finished Good: Technical Information	Product Version
Component Part Information	Component: Descriptive Information	Component Type, Category, Number, Description
Component Part Details	Component: Technical Information	Component Version, Tech Specs
Production Details	Production/Operational Information	% Sourced from Supplier, Lead Times, Quantity, Tech Node

Source: CISA HBOM Framework [1]

[1] https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management

TCG Platform Certificate, Next



- Reference to TPM (Root of Trust for Measurement – RTM)
- Manufacturer
- Model
- Version
- Serial Number
- MAC address set at Manufacturing
- Configuration
- Manufacturer URI
- Revocation
- Description of Root of Trust
- Platform Configuration URI
- …

Existing Platform Certificate (Ver 1.1)

- Traits to increase extensibility
- Component
- …

Next Platform Certificate (Ver 2.0)

- Map CISA HBOM data fields to existing TCG Platform Cert fields
- New CISA HBOM data fields not already in TCG Platform Cert
- …

Next Version

Beyond the Initial Framework

- HBOM framework calls for future guidance on
  - Conveying and verifying BOMs (HW and SW)
  - Identifying roles for sharing and protecting BOMs
  - Operational use of HBOMs
  - Interoperability of HBOM formats
- TCG has developed substantial work in this space with Platform Certificates

Call to Action

- TCG would like to work with CISA, and the community to incorporate their requirements into the Platform Certificate Specification.
- CISA HBOM members are requested to review the TCG Platform Certificate Specification, version 2.0, in public review by end of January 2024.
- Work with TCG to develop future guidance requirements outlined in the HBOM framework.

TRUSTED® COMPUTING GROUP

Questions?

Dell Technologies
Secured Component Verification

https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/secured-component-verification-datasheet.pdf

With Secured Component Verification (SCV), organizations can confidently deploy new devices knowing that critical components are matched exactly with the configuration that left the factory. Once a customer places an order for a PC with SCV, the product is built, PC component data is collected and encrypted, and this information generates a platform certificate that is created and signed at the factory. The digital certificate is stored either on the local drive or in a secure Dell cloud for delivery to the customers. Upon receipt, the customer can validate the components delivered against the certificate. This process ensures that what the customer ordered is what they received and is free of tampering.

Dell Technologies
Secured Component Verification for Power Edge

https://www.dell.com/en-us/lp/dt/open-manage-secure-component-authentication

Dell Technologies Secured Component Verification ensures that PowerEdge servers are delivered and ready for deployment exactly as they were built by Dell manufacturing, providing an extension to Dell’s Secure Supply Chain assurance process.

HP Inc. – HP Platform Certificate

https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3109ENW

https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3108ENW

HP Platform Certificate allows Information Technology (IT) administrators to assess the authenticity and integrity of a PC and its components, helping uncover unauthorized changes that may pose a potential threat to the organization. The TCG standards compliant, signed attribute certificate can be used to verify that a PC is a legitimate HP device and whether unauthorized changes have occurred while traveling through the supply chain, creating a security risk to the customer's organization. Giving IT the ability to authenticate the integrity of a PC will help increase confidence in onboarding and connecting a remote fleet of PCs to their network by reducing the potential risk of a back door security breach.

Hewlett Packard Enterprise

PCVT repository: https://github.com/HewlettPackard/PCVT/

Through its Trusted Supply Chain program, HPE issues TCG-compliant Platform Certificates leveraging a hardware root of trust (TPM) with its ProLiant Gen10 and later servers. In addition, HPE provides the open-source Platform Certificate Verification Tool (PCVT) for customers to verify a server’s current hardware manifest against its Platform Certificate. In addition to validating the server cryptographic identity (IDevID) and Platform Certificate trust chains, PCVT can be delivered as a bootable ISO image and can run in “air-gapped” environments.

Intel Corporation
Intel Transparent Supply Chain

https://www.intel.com/content/www/us/en/products/docs/servers/transparent-supply-chain.html

Assurances of a device's origin and authenticity help establish the foundation for a trusted supply chain. The Intel Transparent Supply Chain utilizes the TCG's TPM standards and Platform Certificates to attest to the platform's origin. In particular, remote deployment and provisioning presents both challenges and opportunities for supply chain security: Intel Transparent Supply Chain customers today depend on the TCG Platform Certificates to attest to the platforms (both hardware and software) in their IT fleets as they are deployed on the networks.