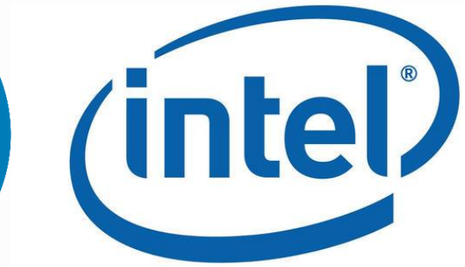
presented by



Traceable Firmware Bill of Materials Overview

UEFI 2021 Virtual Plugfest

December 8, 2021

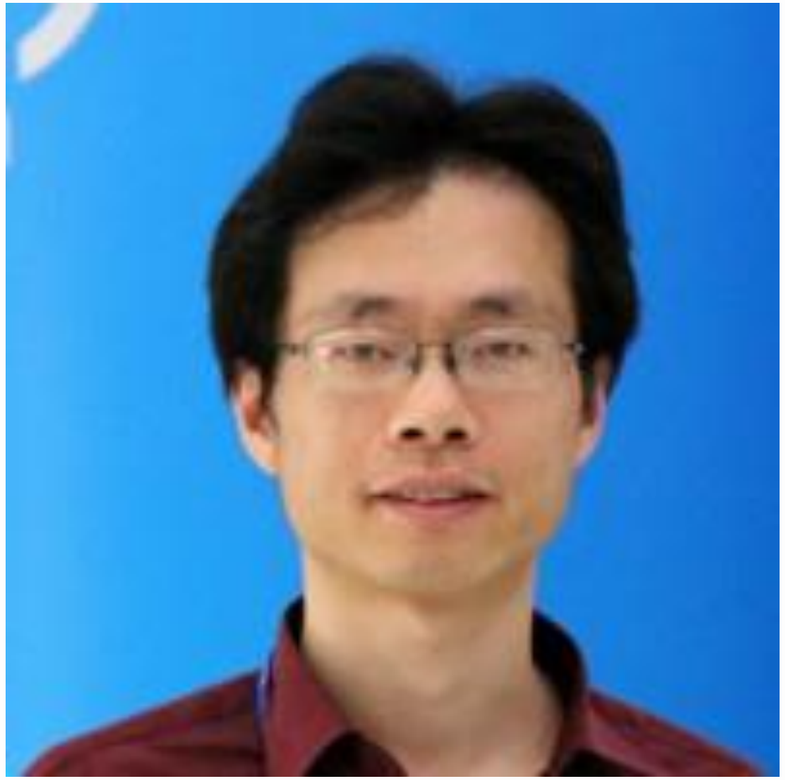
Amy Nelson, Jiewen Yao & Vincent Zimmer

Amy Nelson

- **Amy Nelson** is Distinguished Member Technical Staff, Software Engineering in Dell's Modern Computing Solutions Group. She has been a Security Architect in Dell Client Solutions Group for the last 15 years focused on hardware, firmware and software.
- Amy co-chairs the PC Client Working Group and the TCG Technical Committee. Amy is the editor of the PC Client Firmware Integrity Measurement Specification and the PC Client Platform Firmware Profile Specification.

Jiewen Yao

- **Jiewen Yao** is a principal engineer in the Intel Software and Advanced Technology Group. He has been engaged as a firmware developer for over 15 years. He is a member of the UEFI Security Sub Team and the TCG PC Client Working Group, and chairing the DMTF SPDM Code Task Force.



Vincent Zimmer

- **Vincent Zimmer** is a senior principal engineer in the Intel Software and Advanced Technology Group. He has been engaged as a firmware developer for over 25 years and leads the UEFI Security sub team.

Vincent Zimmer
Intel

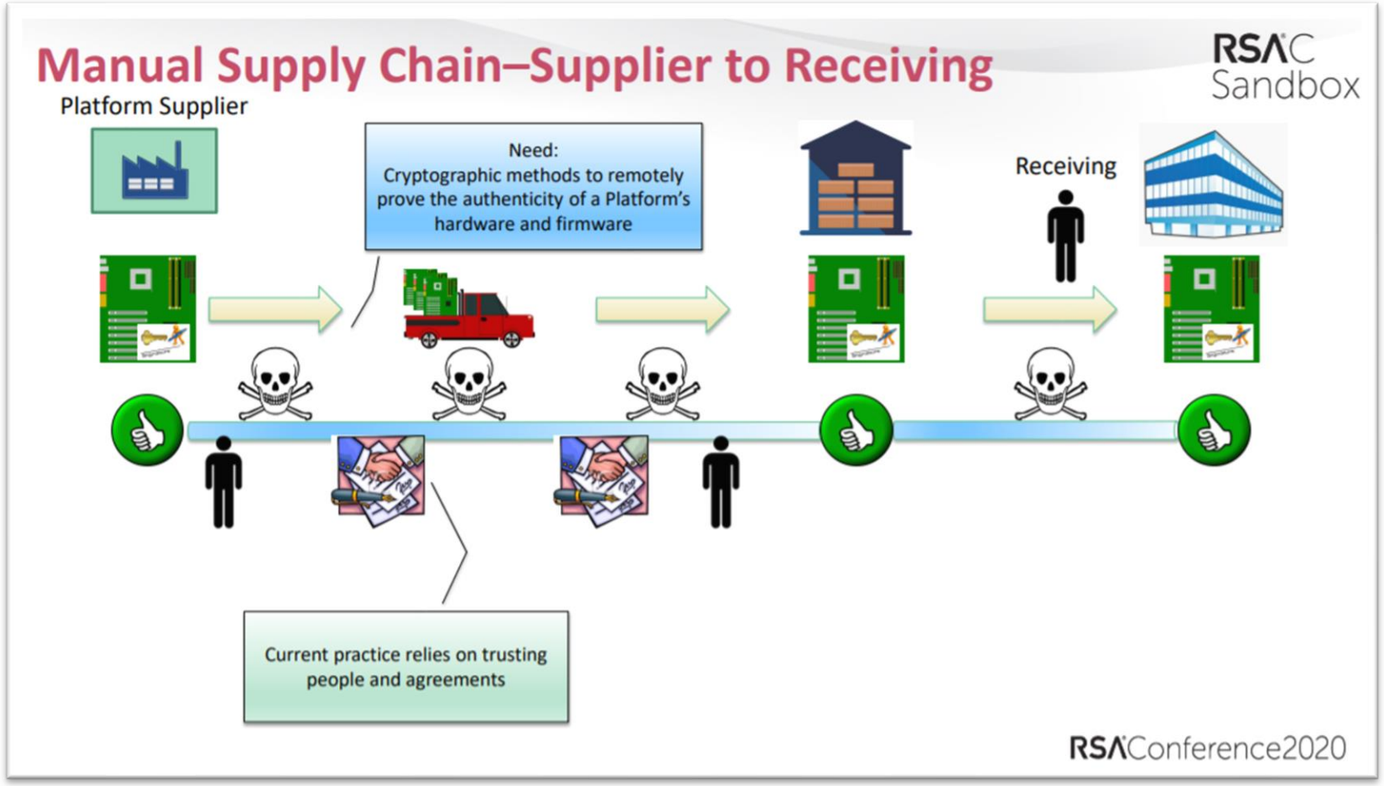
Agenda

- Background
- Firmware BOM
- Example
- Summary / Call to Action

Background – Supply Chain

Supply Chain Risk

– build tool, signing service, assembling, preinstallation, shipping



** Source: https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18108/2020_USA20_SBX1-R1_01_Industry-Standards-to-Support-Supply-Chain-Risk-Management-for-Firmware.pdf*

Software Bill of Material (BOM)

Bill of material (**BOM**): **a list of the raw materials**, sub-assemblies, intermediate assemblies, sub-components, parts, and the quantities of each needed to manufacture an end-product.

- https://en.wikipedia.org/wiki/Bill_of_materials

Software BOM Today

Software Package Data Exchange (SPDX) – Low-level details of components
Standard: ISO/IEC 5962:2021
Examples: https://github.com/swinslow/spdx-examples
Tools: https://github.com/lfscanning

Software Identification (SWID) Tag – describe Software Product
Standard: ISO/IEC 19770-2:2015, NISTIR 8060
Tools: https://pages.nist.gov/swid-tools/

Common Platform Enumeration (CPE) – Describe application, OS, hardware
Standard: https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/Specifications/cpe
Examples: https://nvd.nist.gov/products/cpe

CycloneDX Software BOM – Lightweight SBOM used in application security
Standard: https://github.com/CycloneDX/specification
Examples: https://github.com/CycloneDX/sbom-examples
Tools: https://cyclonedx.org/tool-center/

Complexity of Firmware

Quiz: How many firmware exist in this platform?

UEFI FW	ME FW	Microcode
BIOS ACM	SINIT ACM	BMC
1Gb NIC FW	PXE OROM	RST OROM
ASPEED Video	Optane DIMM	NVMe
PCIE Device	……	

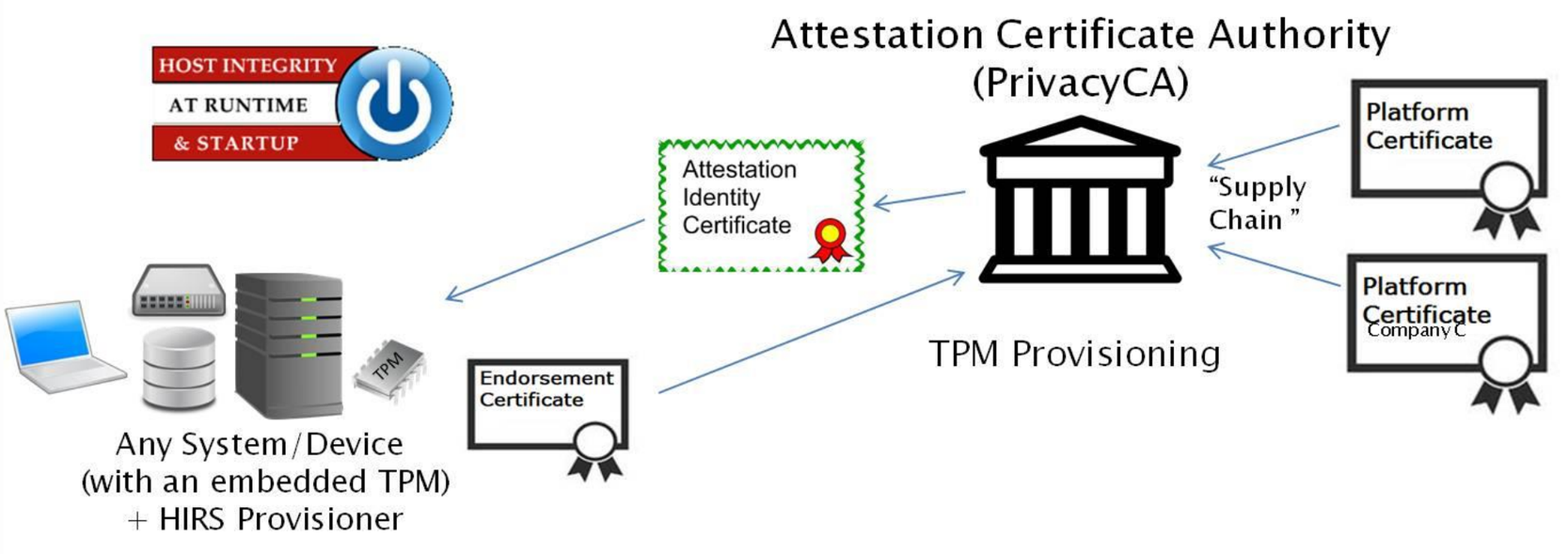
And the supply chain issue in Firmware

** Source: https://www.blackhat.com/us-21/briefings/schedule/index.html#safeguarding-uefi-ecosystem-firmware-supply-chain-is-hardcoded-23685*

Existing Tech

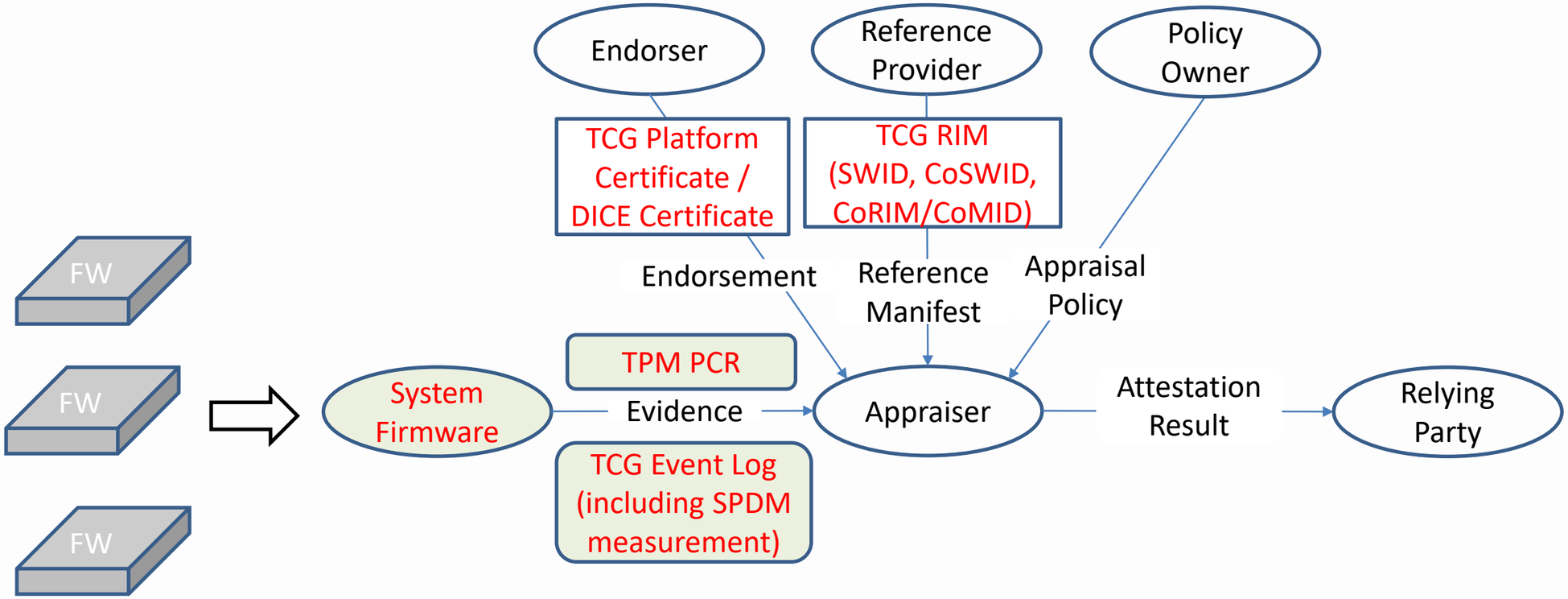
Host Integrity at Runtime and Startup (HIRS):

Source: https://github.com/nsacyber/HIRS



Version 2.0 added support for the PC Client Reference Integrity Manifest (RIM) Specification to provide firmware validation capability to the HIRS ACA. This requires that the manufacturer of a device provide a digitally signed RIM "Bundle" for each device. The HIRS ACA has a new page for uploading and viewing RIM Bundles and a policy setting for requiring Firmware validation.

Attestation for Firmware



System Firmware as Lead Attester!

What is gap today?

- BIOS is measured as a chunk.

Question: How to know info for each ***BIOS embedded component****?*

- Only BIOS and UEFI driver/application are measured.

Question: How to know info for each ***device embedded firmware****?*

Firmware Bill of Material (BOM)

- **Firmware BOM**: A list of the firmware components and their hashes which are embedded or attached to the motherboard and play roles during system boot and runtime usage.

- Firmware Related Guideline
  - NIST SP800-155 (BIOS Integrity Measurement)
  - TCG PC Client Firmware Integrity Measurement (FIM)
  - TCG PC Client Reference Integrity Measurement (RIM)
  - TCG PC Client Platform Firmware Profile (PFP)
  - IETF CoSWID
  - IETF CoMID

Firmware BOM

Firmware Classification

- Type-I firmware
  - Loaded and executed in host environment.
- Type-II firmware
  - Loaded and executed NOT in host environment.
- More detail in next page …

Firmware Classification

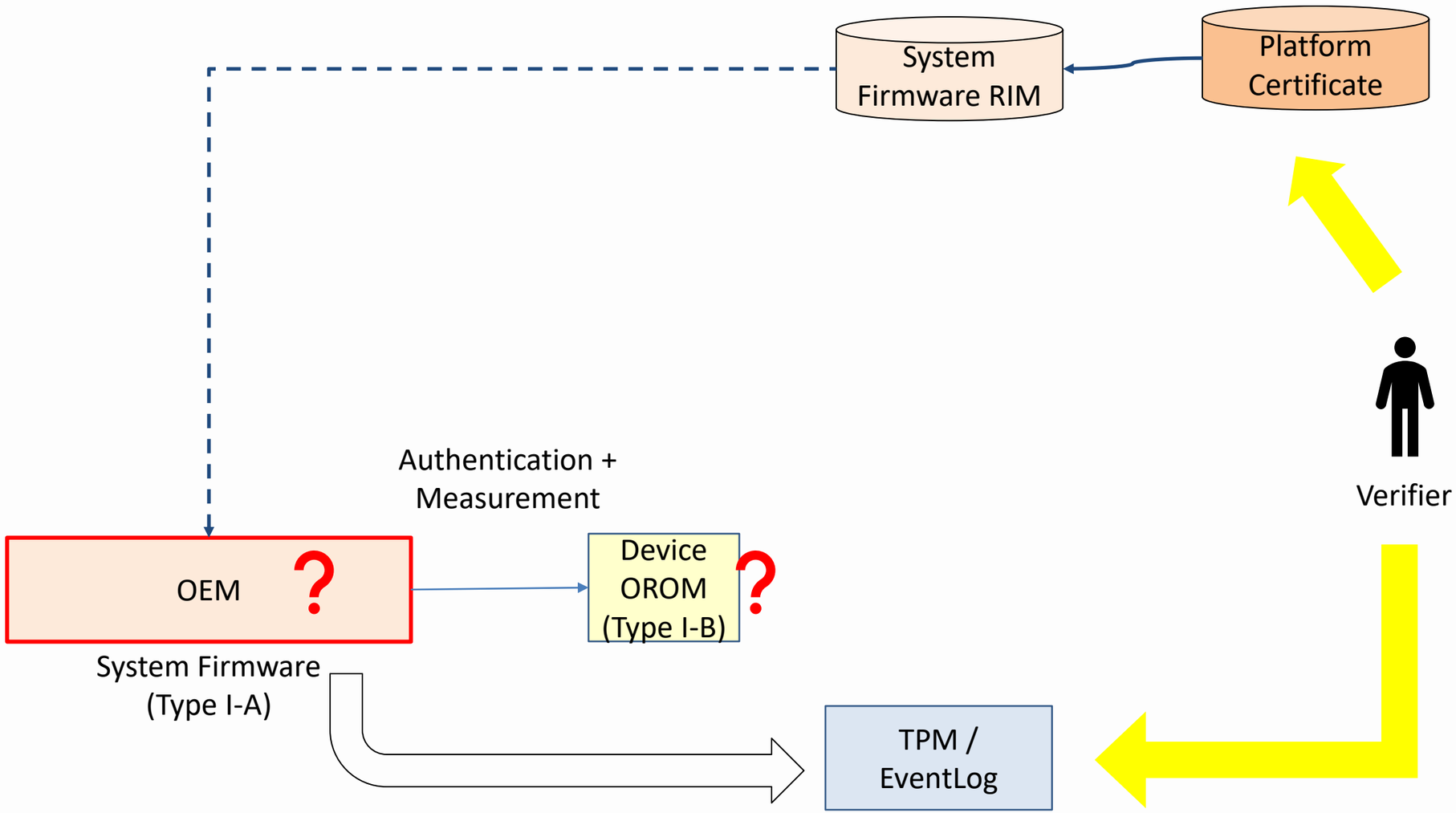
Type	SubType	Loader (Loaded by)	Location (Loaded From)	Execution Env	Example
Type-I	I-A	Host	System Firmware	Host	BIOS, Intel FSP, CPU Microcode
	I-B	Host	Peripheral Device	Host	PCI Option ROM, PXE
Type-II	II-A	Non-Host	Non-Host Firmware	Non-Host	BMC, EC, Intel CSME, PFR
	II-B	Peripheral	Peripheral Device	Peripheral Device	NIC, NVMe, NVDIMM, Graphic Card.

System Firmware's Role

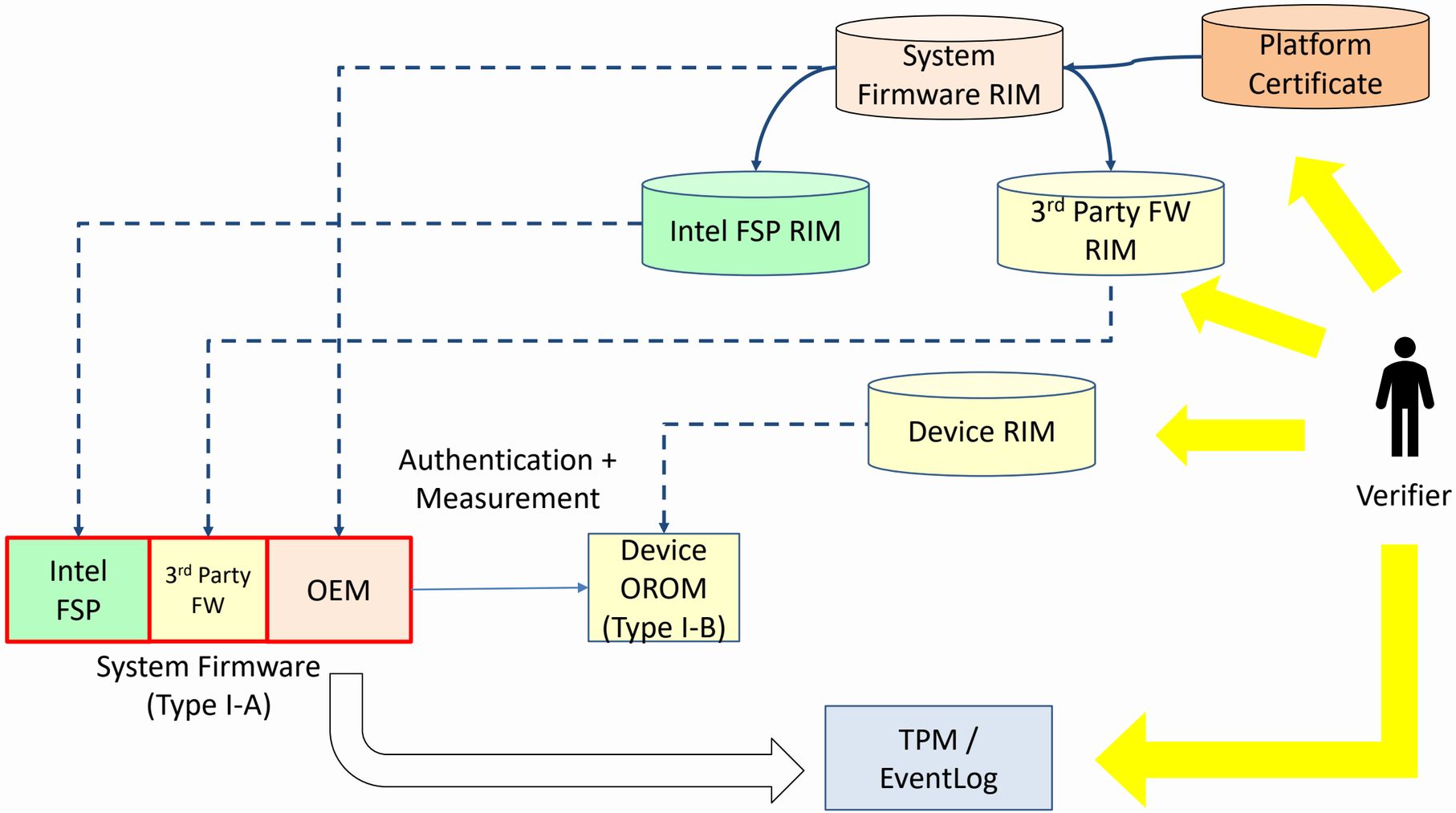
- Type-I firmware handling:
  - Load and measure other Type-I firmware.
  - Ensure each firmware component have one or more dedicated entries in the event log.

- NOTE:
  - The system firmware itself can be measured and verified by a platform RoT.

Type-I firmware (today)



Type-I firmware

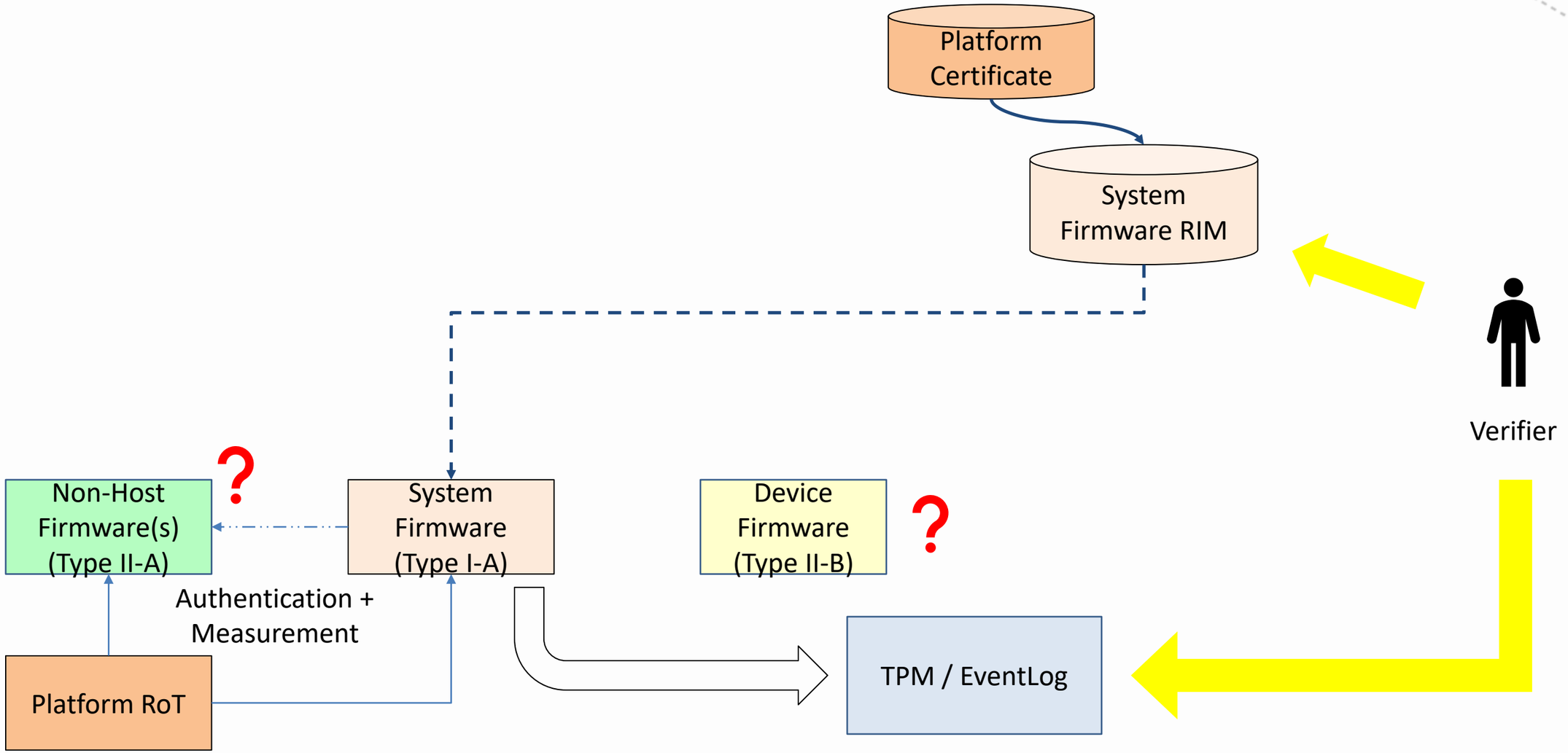


System Firmware's Role

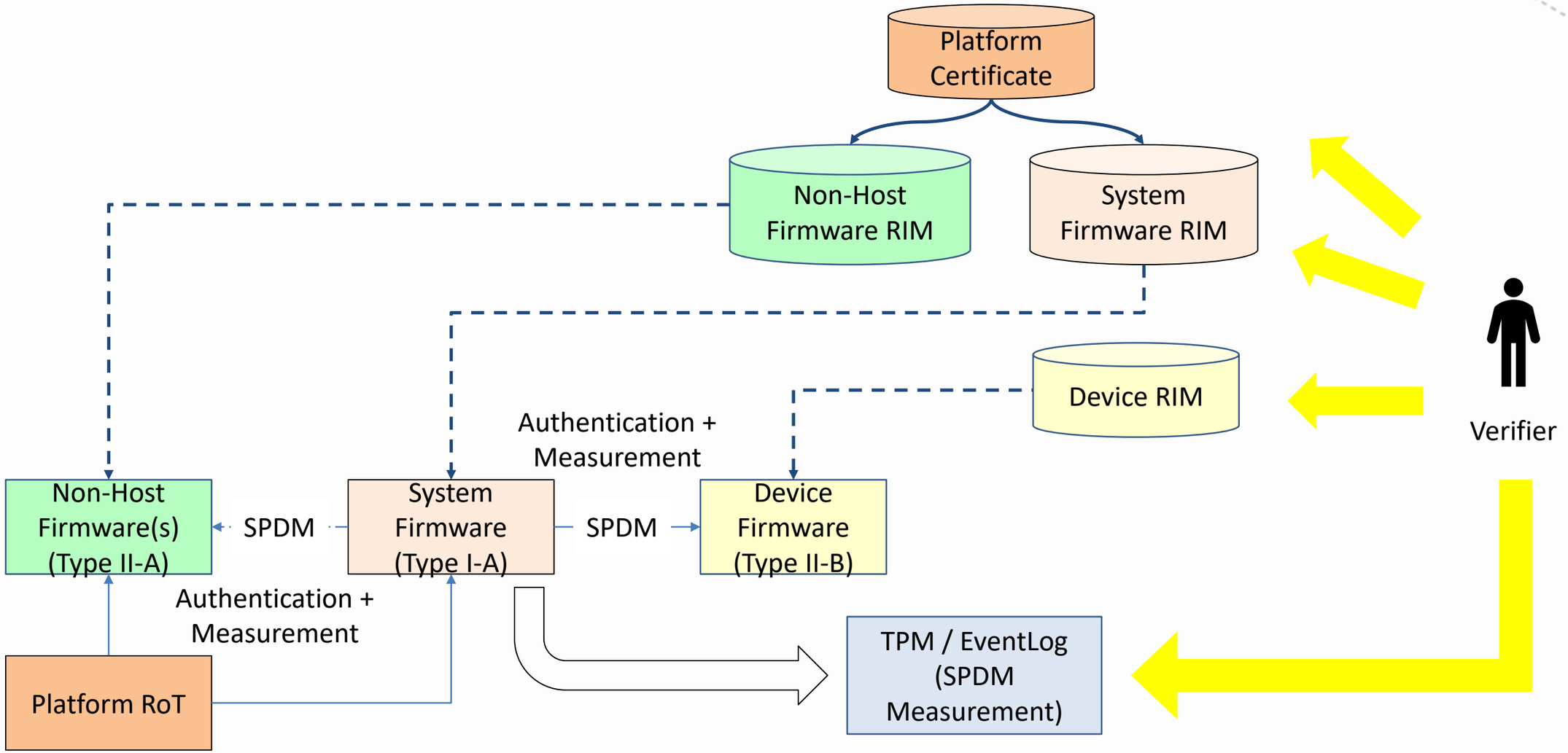
- Type-II firmware handling:
  - Collect measurement of Type-II firmware from other RoT (device or platform).
  - Ensure each firmware component have one or more dedicated entries in the event log.

- NOTE:
  - The system firmware might not have access to some device RoT directly, but may get the Type-II firmware measurement from other RoT source (device or platform).

Type-II firmware (today)



Type-II firmware



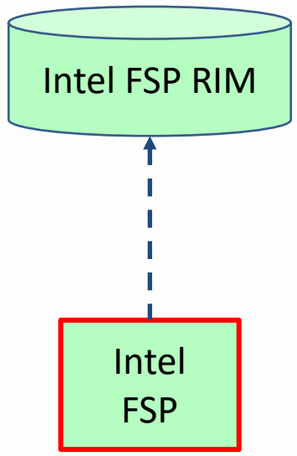
Example

Type-I Firmware - Intel FSP

- Intel Firmware Support Package (FSP)
  - **A binary** to perform silicon initialization.
  - Released by Intel.
  - Can be integrated into OEM BIOS.

- Question
  - Is the FSP binary in OEM BIOS from Intel?
  - Is it the latest FSP binary with known bug fix?

Type-I Firmware - Intel FSP



Base RIM (SWID Tag)

==========

Name: AmberLakeFspBin
version: 3.7.6
tagID: CC92BA16-8450-4C4B-8EFA-F34D5299D5E0
Link: href: http://...
Role: softwareCreator tagCreator
BindingSpec: PC Client RIM
BindingSpecVersion: 1.2
SupportRIMFormat: TCG_EventLog_Assertion
SupportRIMURL: http://...
...
DigitalSignature: XXXXXXXX

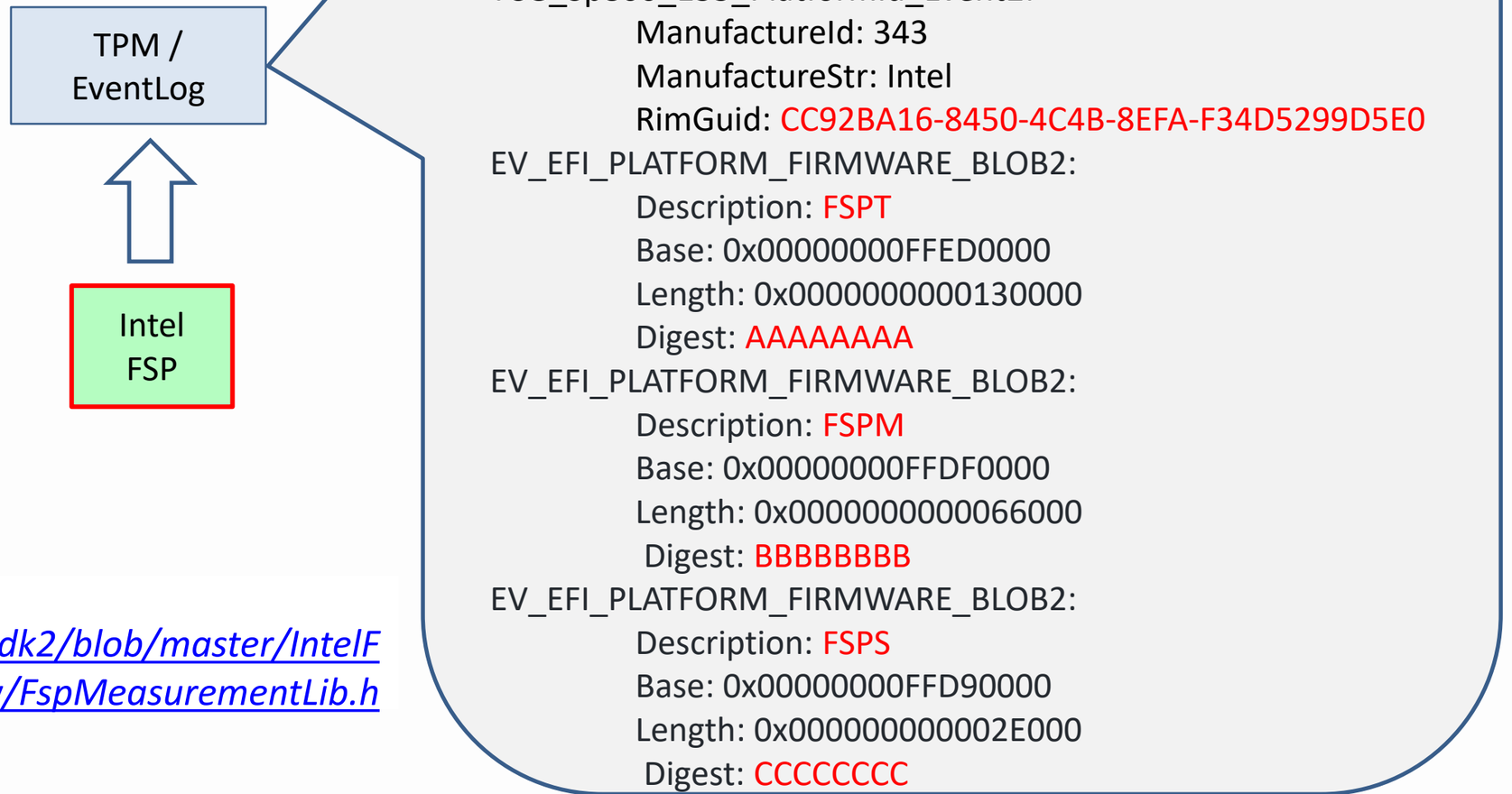
Support RIM

==========

EV_EFI_PLATFORM_FIRMWARE_BLOB2:
Description: FSPT
Base: 0x00000000FFED0000
Length: 0x0000000000130000
Digest: AAAAAAAA
EV_EFI_PLATFORM_FIRMWARE_BLOB2:
Description: FSPM
Base: 0x00000000FFDF0000
Length: 0x0000000000066000
Digest: BBBBBBBB
EV_EFI_PLATFORM_FIRMWARE_BLOB2:
Description: FSPS
Base: 0x00000000FFD90000
Length: 0x000000000002E000
Digest: CCCCCCCC

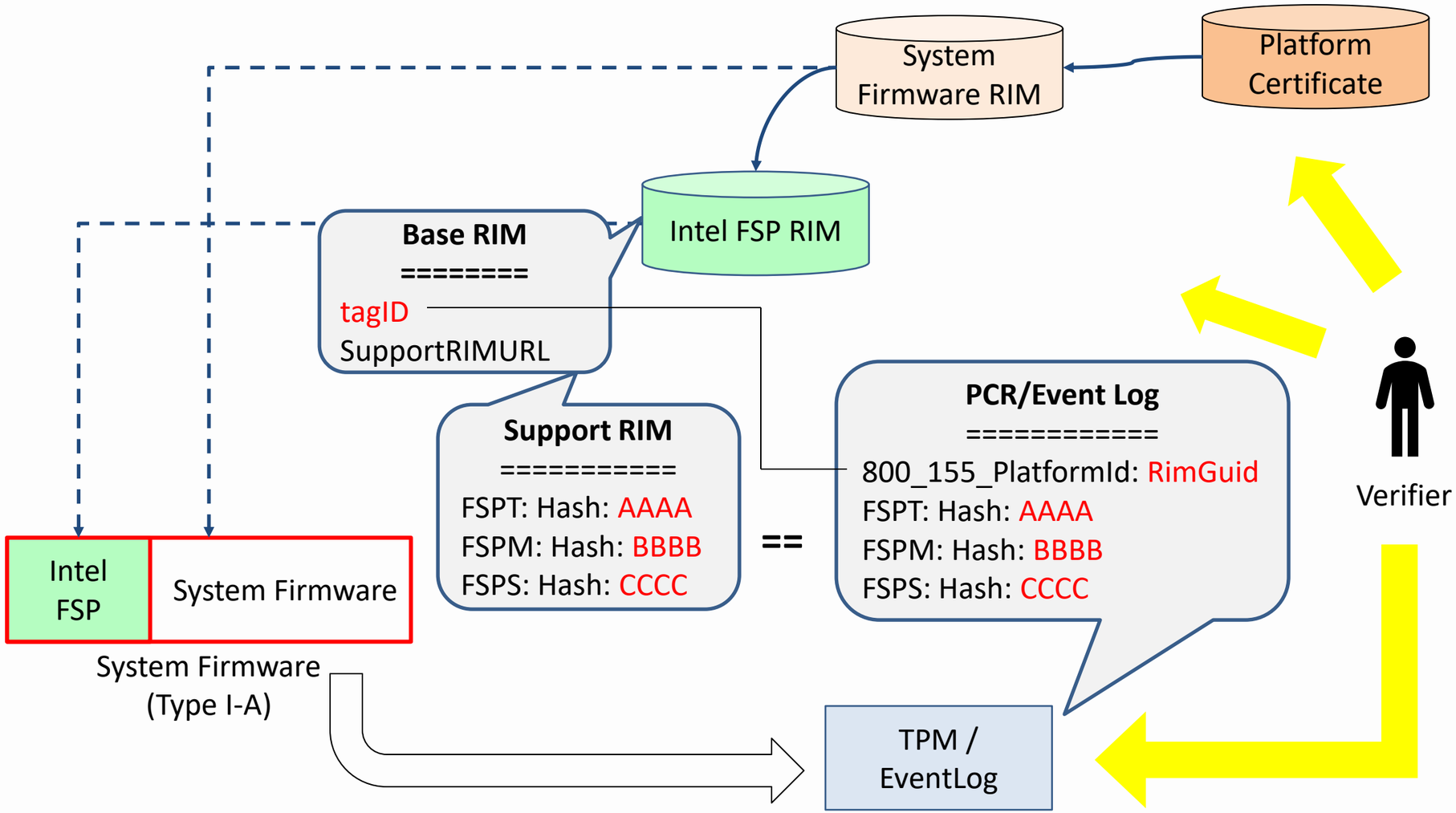
** Source: Intel FSP 2.x Measurement and Attestation,*
https://cdrdv2.intel.com/v1/dl/getContent/644001

Type-I Firmware - Intel FSP



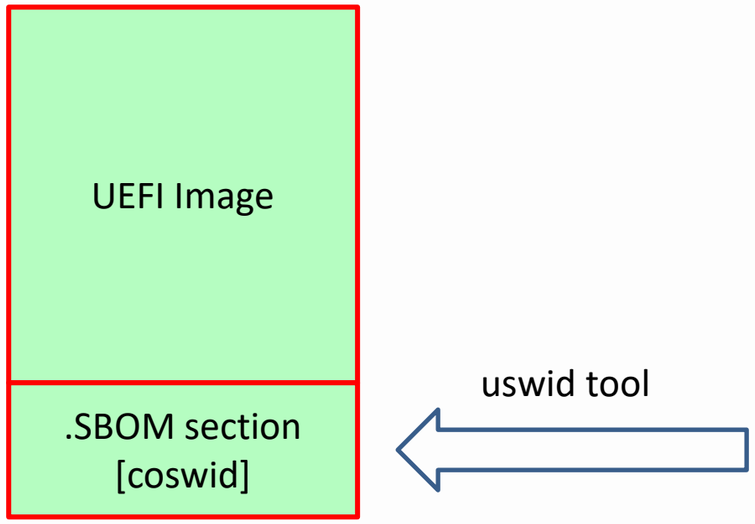
** Reference:*
https://github.com/tianocore/edk2/blob/master/IntelFsp2WrapperPkg/Include/Library/FspMeasurementLib.h

Type-I Firmware - Intel FSP



Type-I Firmware – UEFI Image

- uswid tool - https://github.com/hughsie/python-uswid
  - A tool to create CoSWID tag for **UEFI image**



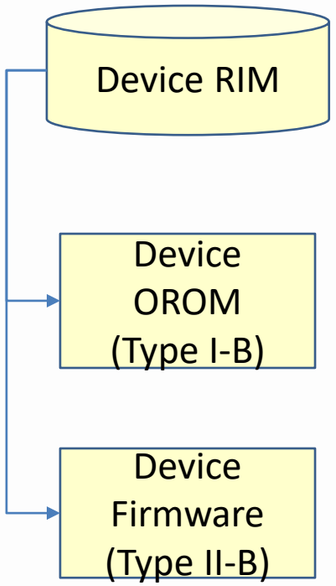

```
[uSWID]
tag-id = acbd84ff-9898-4922-8ade-dd4bbe2e40ba
software-name = HughskiColorHug.efi
software-version = 1.2.3
product = ColorHug
summary = Open Source Display Colorimeter
colloquial-version = b2ed6f1ed8587bf01a2951d74512a70f1a512d38
edition = v2021+
revision = 2

[uSWID-Entity:TagCreator]
name = Hughski Limited
regid = hughski.com
```

Type-II Firmware – Device

- Device includes
  - Firmware running in the device
  - Option ROM running in the host

- Question
  - How do we know the device firmware info?
  - How do we know the device option ROM info?

Type-II Firmware – Device



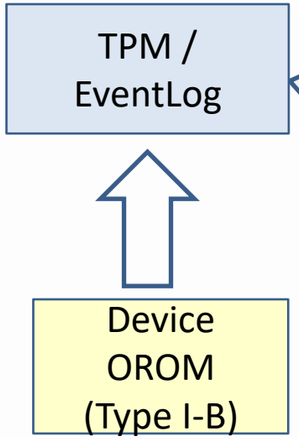
Base RIM
=========

Type: corim
Vendor: XXX
Model: A.B.C
Id: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Role: tagCreator

Tag: coswid
Payload1: Digest: EEEEEEEE

Tag: comid
Fw1:
Vendor: XXX
Digest: AAAAAAAA
Fw2:
Vendor: XXX
Digest: BBBBBBBB
fw3:
Vendor: XXX
Digest: CCCCCCCC

Type-II Firmware – Device



TCG Event Log

==========

EV_EFI_SPDM_FIRMWARE_BLOB:
- Device Path: PCI Device
- SPDM Measurement Block
  - Type 0: ImmutableROM
  - Device Measurement: AAAAAAAA
- Device Context: PCI VID/DID

EV_EFI_SPDM_FIRMWARE_BLOB:
- Device Path: PCI Device
- SPDM Measurement Block
  - Type 1: MutableFirmware
  - Device Measurement: BBBBBBBB
- Device Context: PCI VID/DID

EV_EFI_SPDM_FIRMWARE_CONFIG:
- Device Path: PCI Device
- SPDM Measurement Block
  - Type 2: HardwareConfig
  - Device Measurement: CCCCCCCC
- Device Context: PCI VID/DID

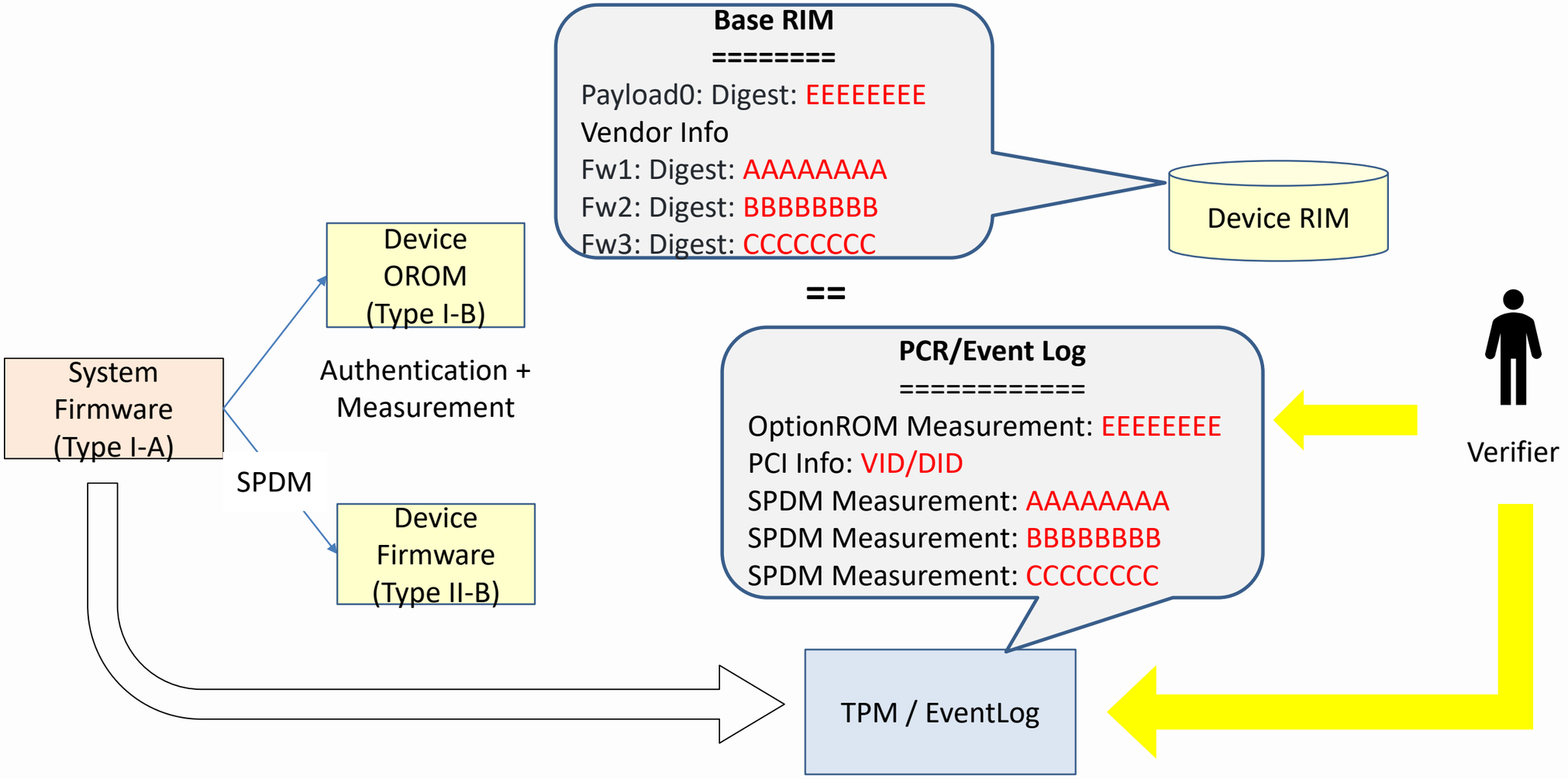
EV_EFI_BOOT_SERVICES_DRIVER:
- Image Device Path: PCI Device/Option ROM
- Digest: EEEEEEEE

** Reference:*

https://github.com/DMTF/libspdm

https://github.com/jyao1/edk2/tree/DeviceSecurity/DeviceSecurityPkg

Type-II Firmware – Device



Future items (Challenge)

- Hot Plug device
  - If we need measure/attest the hot plug device?
  - If yes, how do we notify the device hot added or removed?

- Runtime Update
  - If we need measure/attest the new runtime firmware?
  - If yes, how do we notify the runtime firmware change?

Summary & Call for Action

Summary & Call for Action

- The industry is preparing support chain identification.
- System firmware plays a role to report firmware measurement information.
- We should get our firmware prepared.

Reference

- **General Supply Chain Guideline**
  - ISO/IEC 28000:2007 - Specification for security management systems for the supply chain
  - NIST SP800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations
  - UK NCSC – Supply Chain Security Guideline
- **Standard / Guideline**
  - NIST SP800-155 (draft) – BIOS Integrity Measurement Guideline
  - TCG PC Client Platform Firmware Profile (PFP)
  - TCG PC Client Firmware Integrity Measurement (FIM)
  - TCG PC Client Reference Integrity Manifest (RIM)
  - TCG Platform Certificate Profile
  - TCG DICE Attestation Architecture
  - TCG DICE Layering Architecture
  - TCG DICE Certificate Profile
  - IETF RATS Remote Attestation Architecture
  - IETF SACM Concise SWID
  - IETF RATS Concise RIM
  - DMTF Secure Protocol and Data Model

Questions?

Thanks for attending the UEFI 2021 Virtual Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by