SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

# How to Protect the Integrity of Electronic Components and Storage Devices from Supply Chain Attacks

**Thorsten Stremlau**, Marketing Work Group Co-Chair

**Trusted Computing Group (TCG)**

A SNIA Event

# SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containin material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

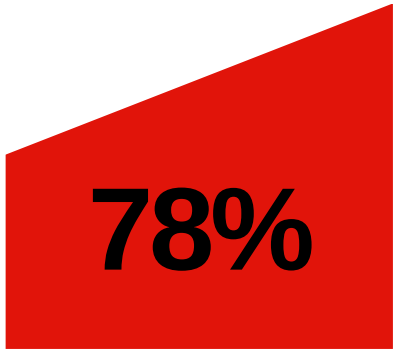
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

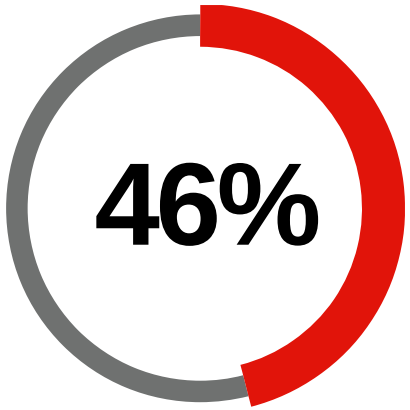
# Strategic Planning Assumptions

«Most organizations' security processes consider only the visible state of computing devices. The ***provenance*** and ***integrity*** of a delivered device and its ***components*** are typically accepted without validating through technology that there have been no unexpected modifications.»

«***Provenance*** is the comprehensive history of a device throughout the entire life cycle from creation to ownership, including changes made within the device or its components.»




year-over-year increase in supply chain attacks

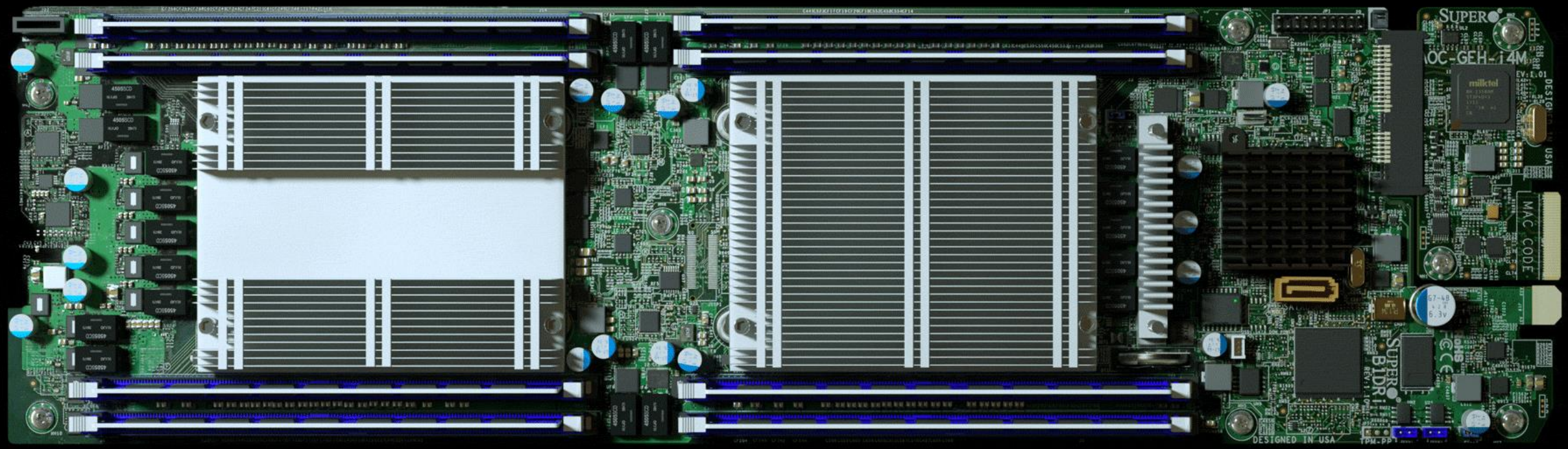



of global businesses have encountered at least one supply chain scare since shifting to a remote working model in the first quarter of 2022

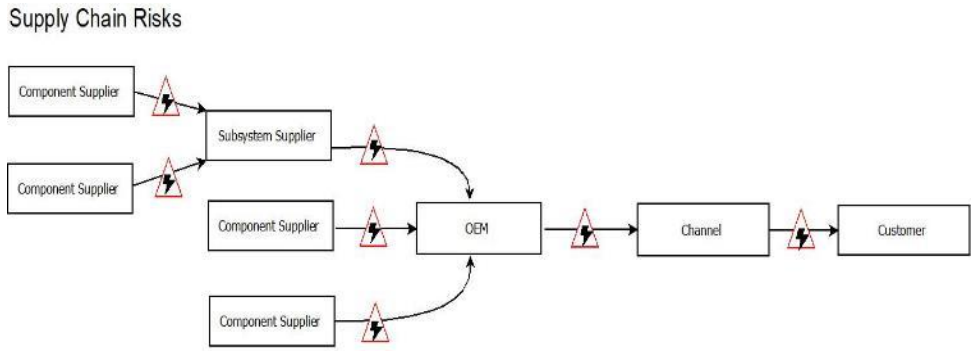
- By 2025, 60% of organizations building or procuring critical infrastructure components (SW&HW) will mandate and standardize Supply Chain Trust principles into their engineering practice, up from less than 20% in 2022
  (Gartner, Feb 2022 G00761079)

# The importance of a securing hardware in transit




https://youtu.be/C7H3V7tkxeA



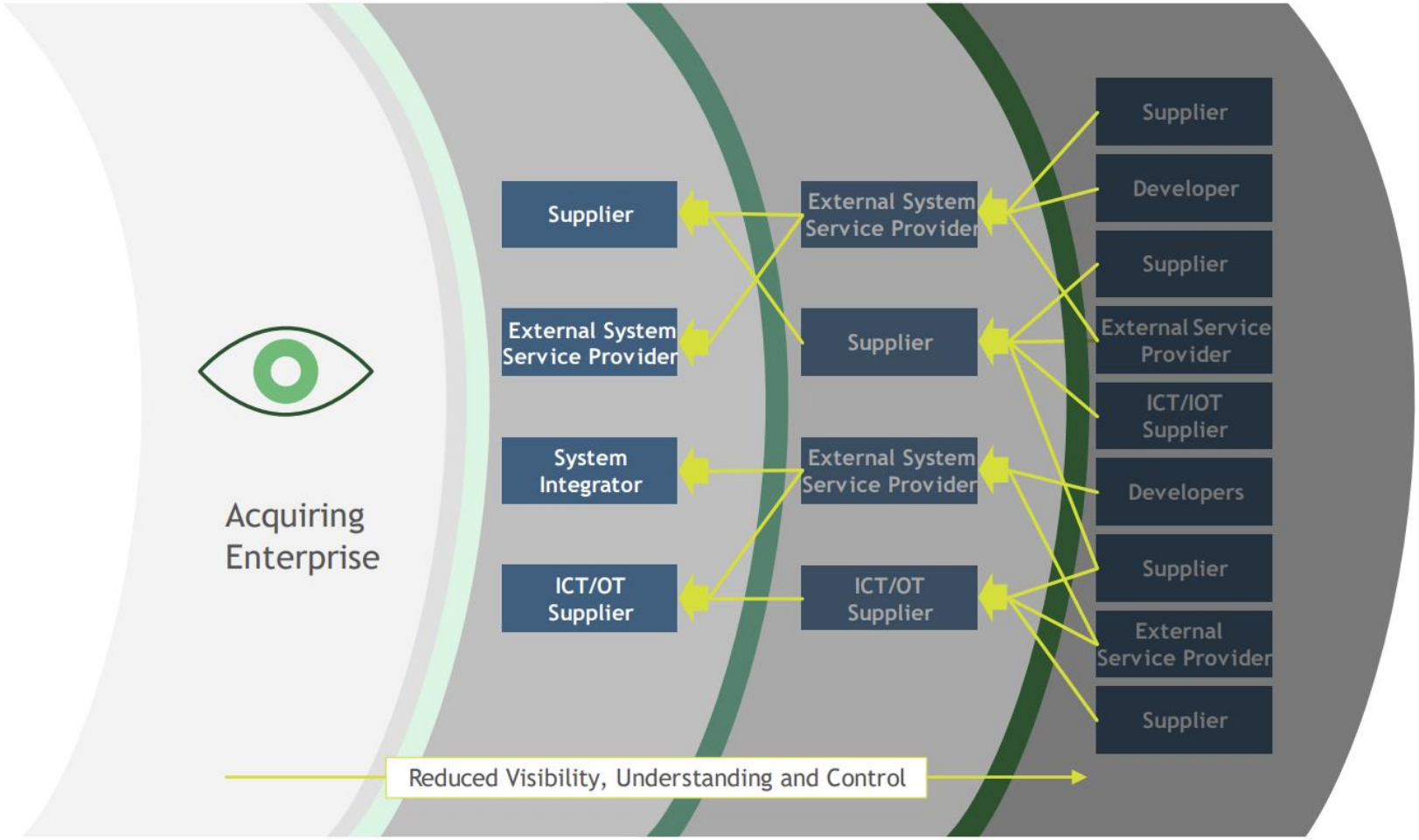
# Important Regulatory and Standards work:

- NIST SP800-161r1 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations)
- NIST SP1800-34 (Validating the Integrity of Computing Devices: Preliminary Draft)
- NIST SP800-193 (Platform Firmware Resiliency Guidelines)
- SBOM (Executive Order on Improving the Nation’s Cybersecurity)
- TCG FIM (TCG PC Client Platform Firmware Integrity Measurement)
- TCG RIM (TCG Reference Integrity Manifest (RIM) Information Model)
- EU RED (COMMISSION DELEGATED REGULATION (EU) 2022/30)

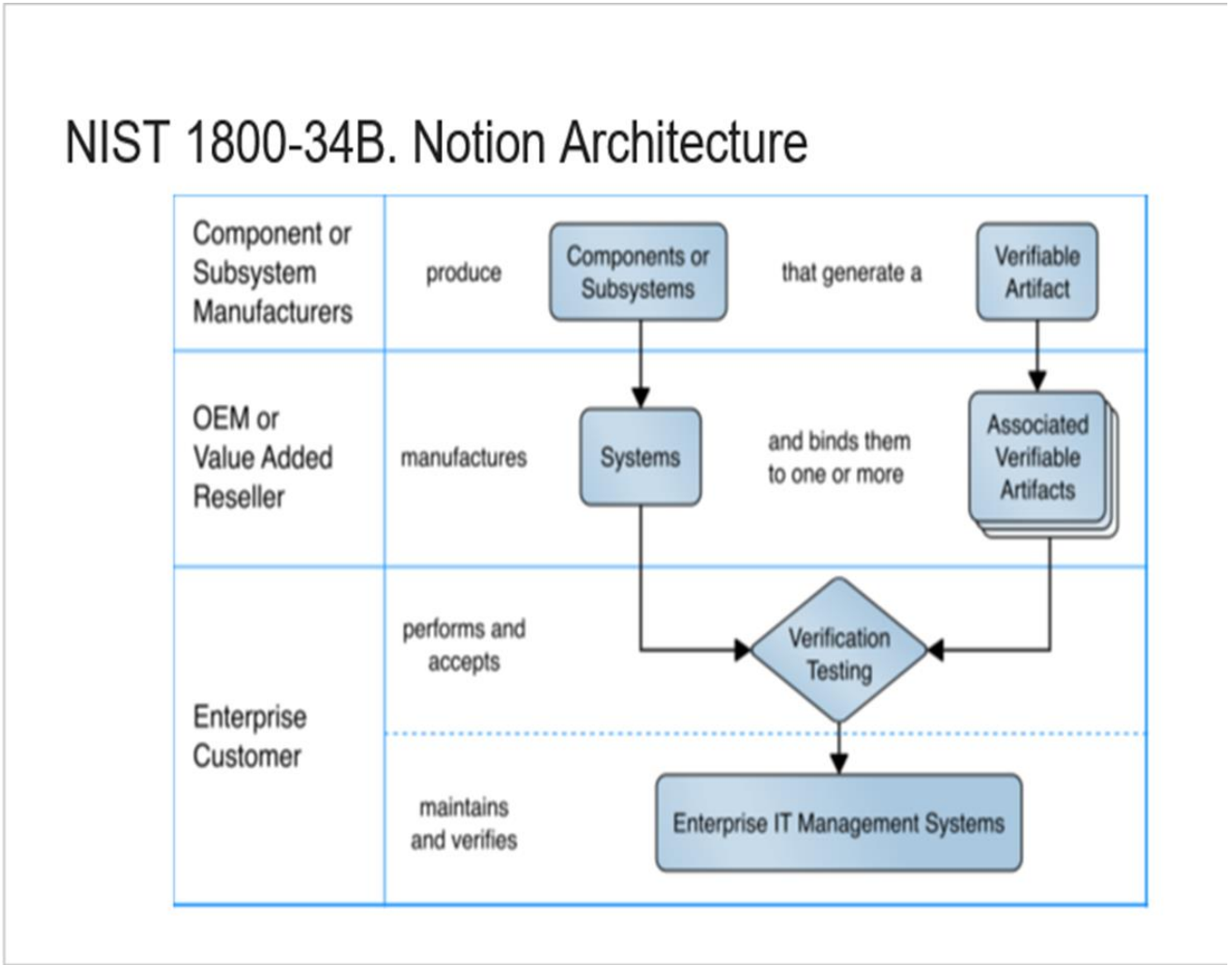
# An Enterprise's Visibility, Understanding, and Control of its Supply Chain

**NIST SP800-161r1**



# NIST SP1800-34



# SP800-193 defines Storage as critical boot device

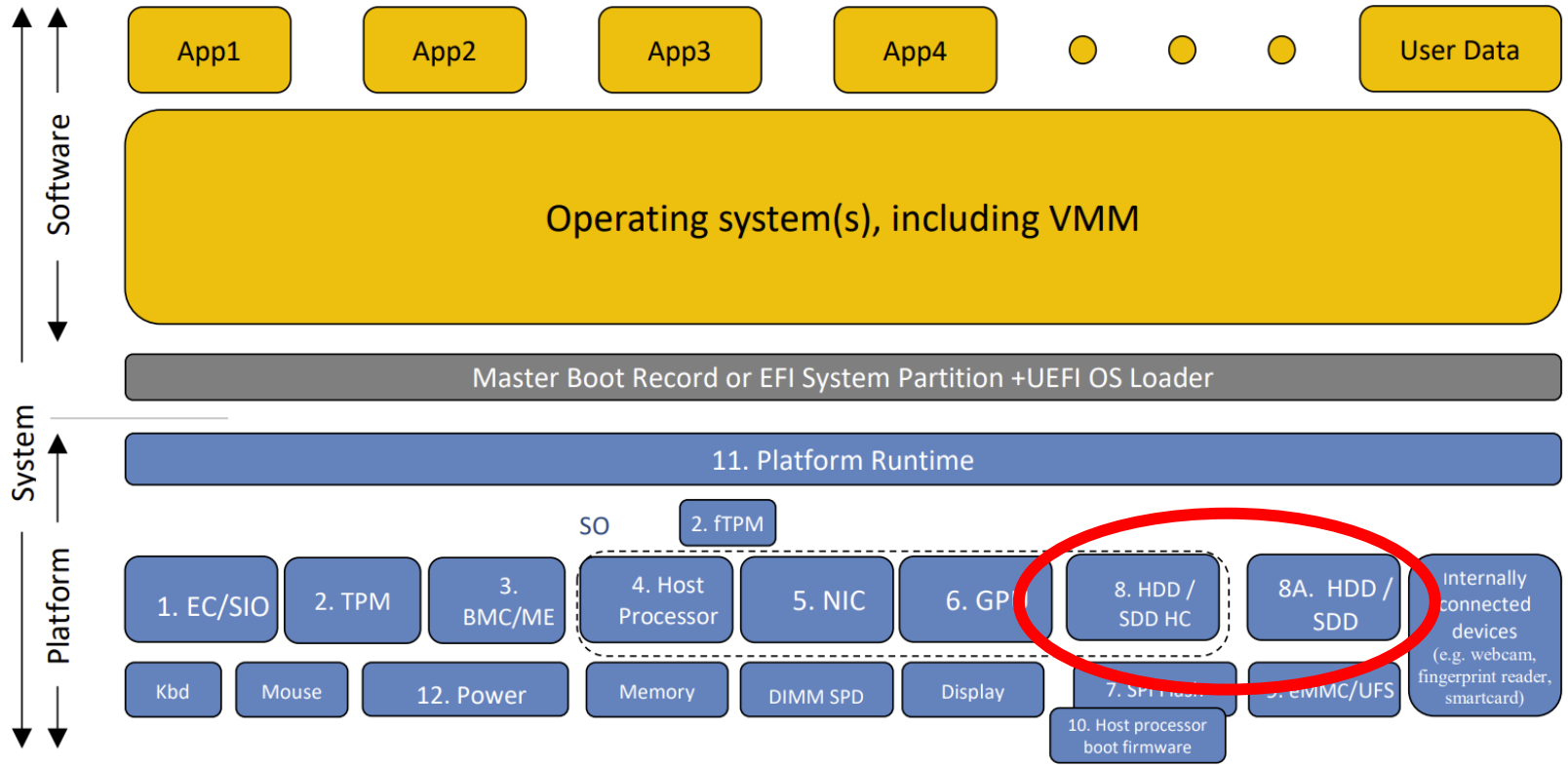



**Figure 1: High-Level System Architecture**

# Firmware Software Bill of materials

https://blogs.gnome.org/hughsie/2022/03/10/firmware-software-bill-of-materials/

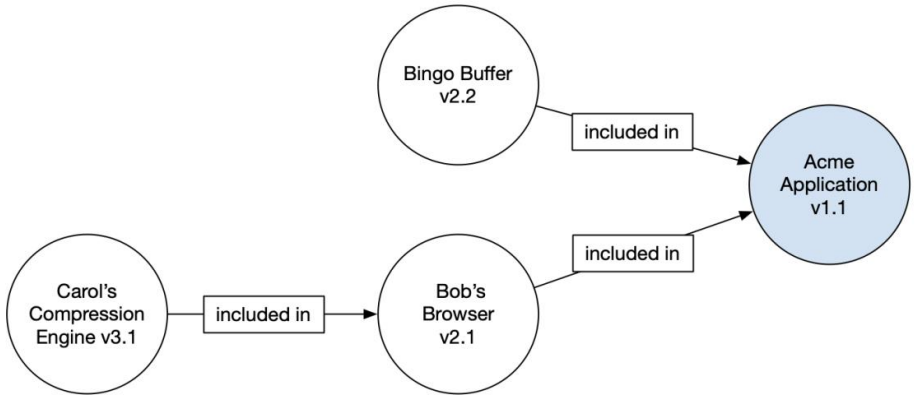
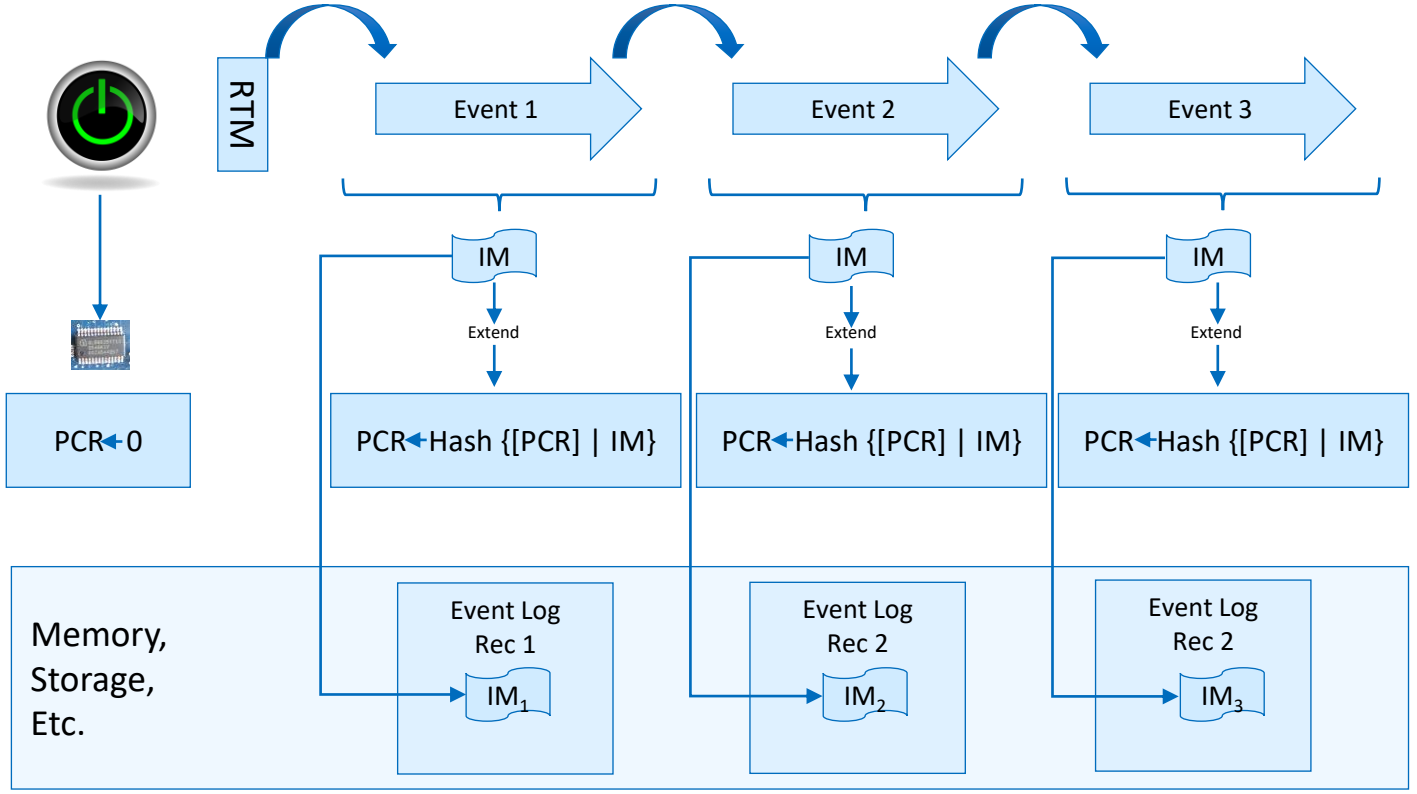



Figure 1: Conceptual SBOM graph

| Component Name | Supplier | Version | Author | Hash | UID | Relationship |
|---|---|---|---|---|---|---|
| Application | Acme | 1.1 | Acme | 0x123 | 234 | Primary |
| \|--- Browser | Bob | 2.1 | Bob | 0x223 | 334 | Included in |
| \|--- Compression Engine | Carol | 3.1 | Acme | 0x323 | 434 | Included in |
| \|--- Buffer | Bingo | 2.2 | Acme | 0x423 | 534 | Included in |

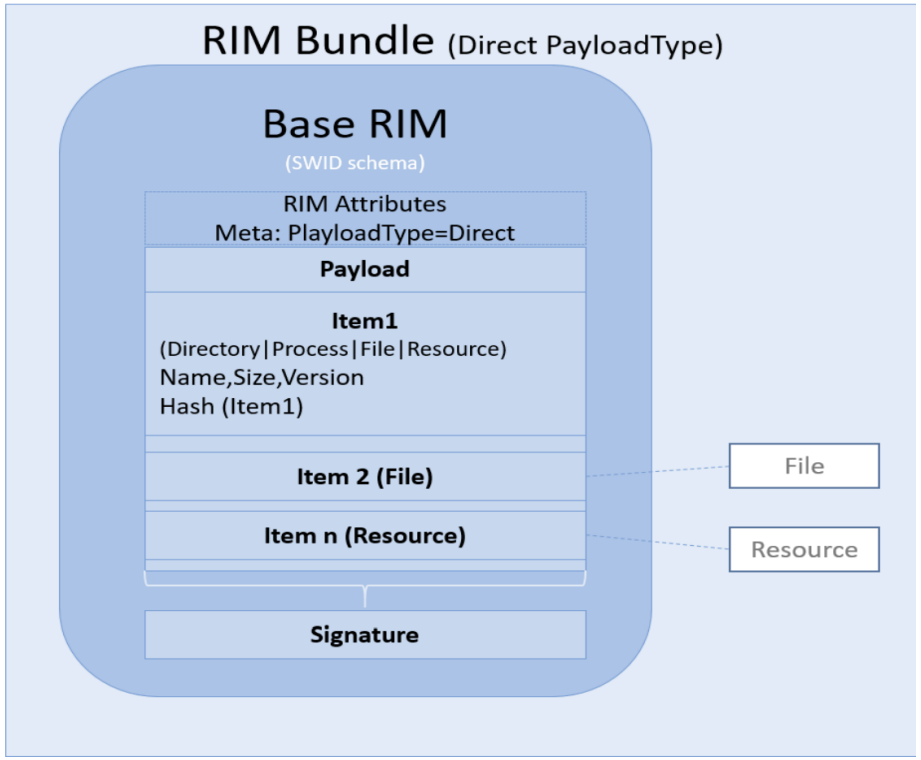
# TCG Firmware Integrity Measurement



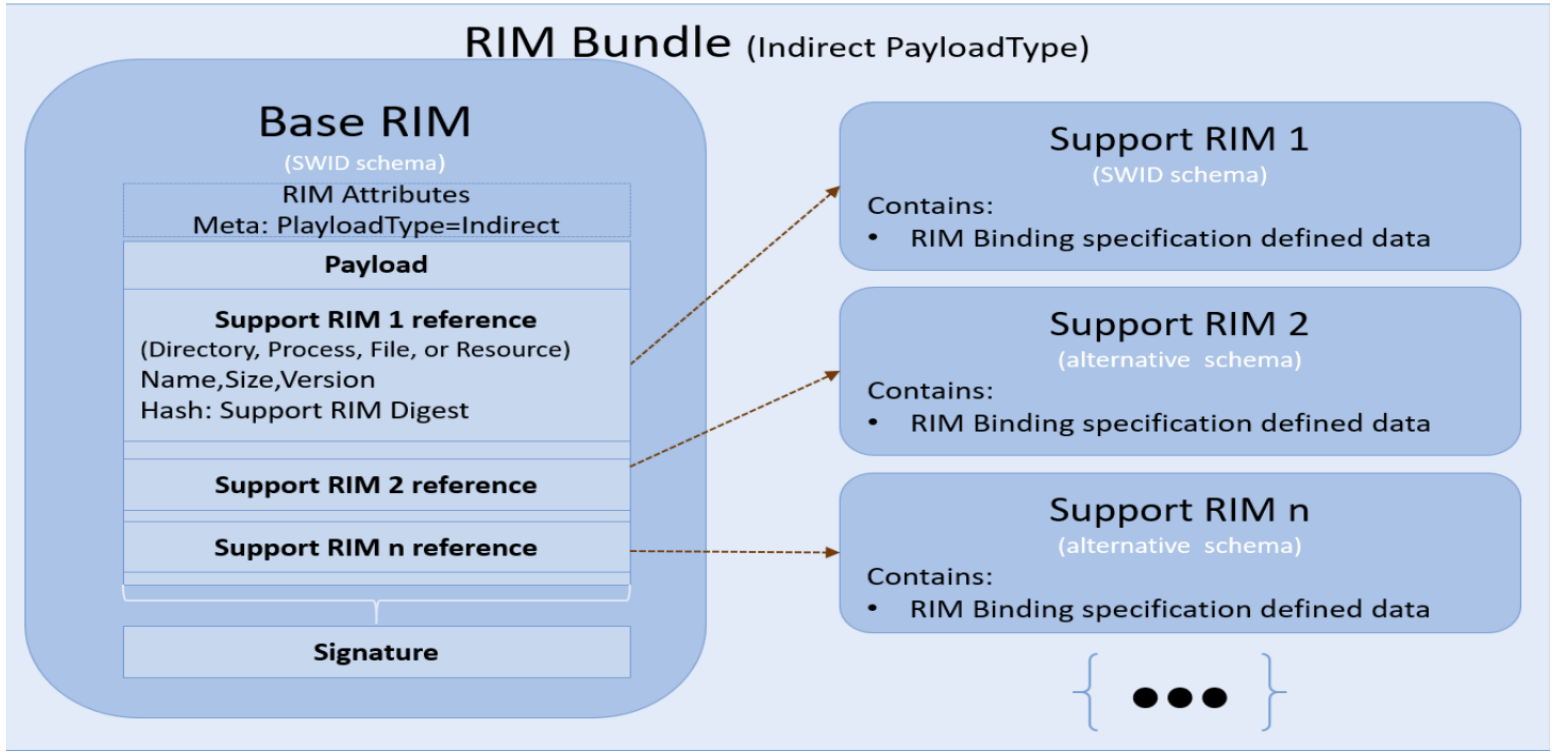

 

# TCG Reference Integrity Manifest

## Direct

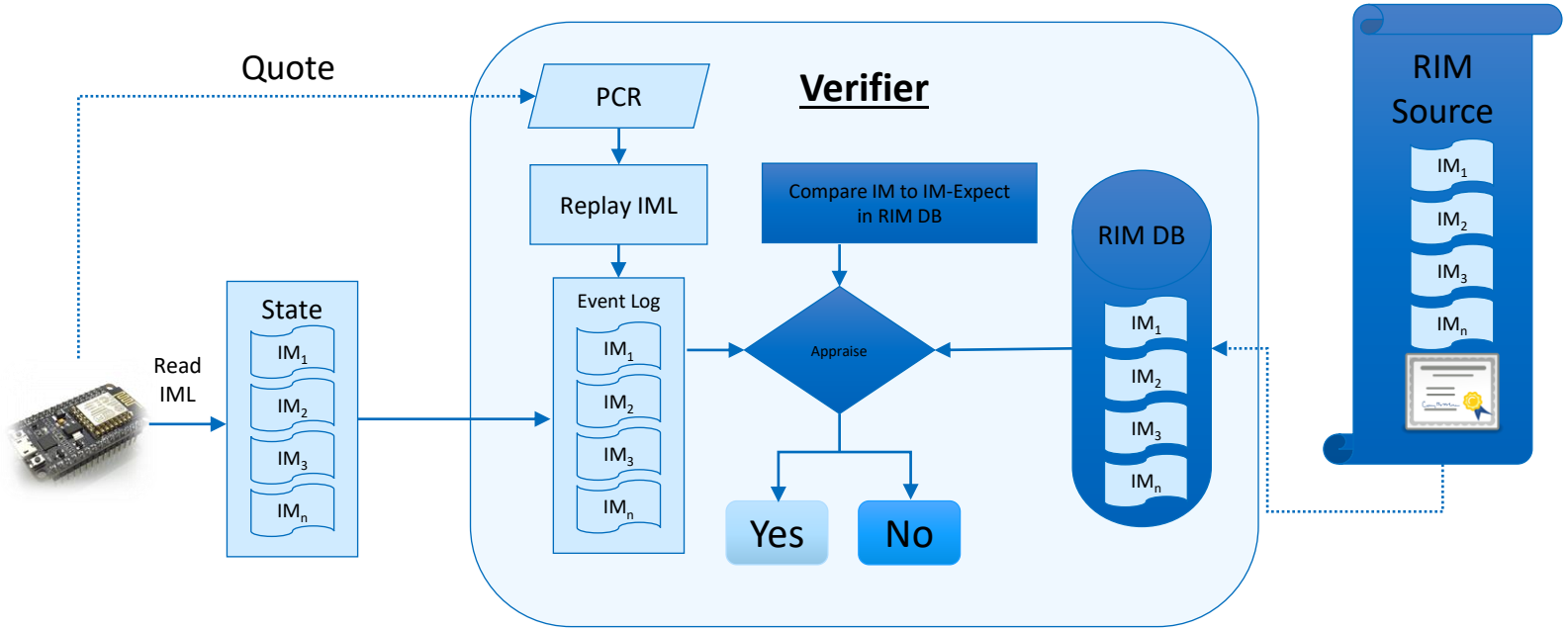



## Indirect



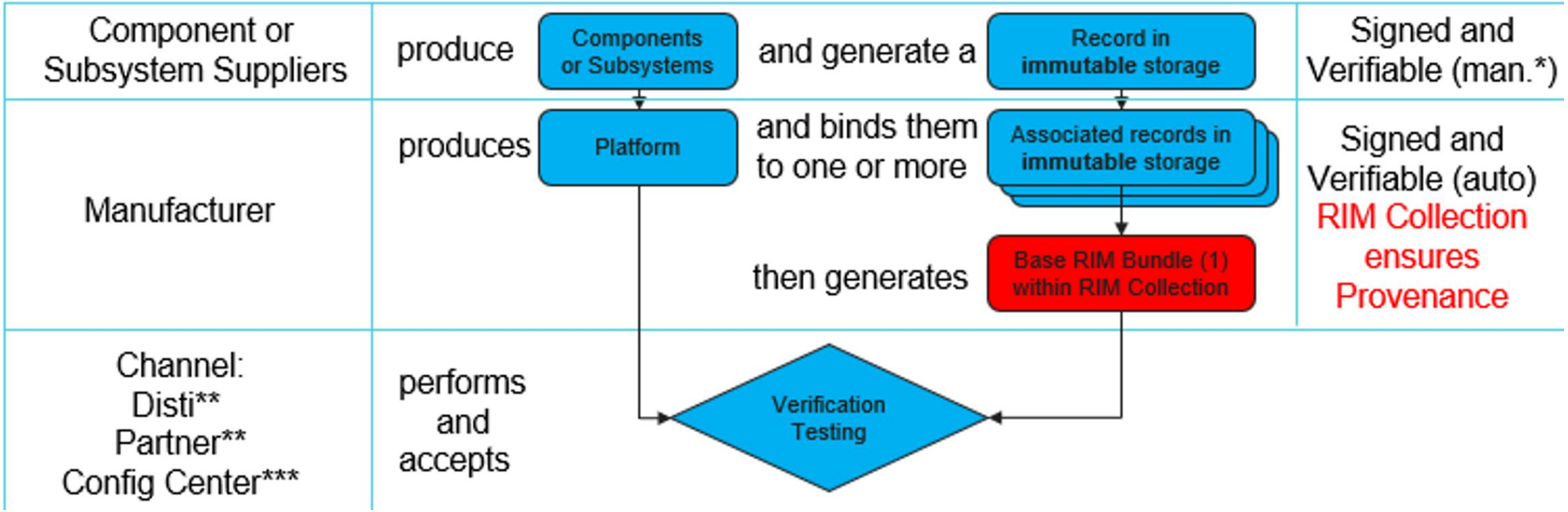

 

# How it all fits together



# Summary




# Please take a moment to rate this session.

Your feedback is important to us.