RSAC Sandbox

RSAConference2020

HUMAN ELEMENT

SESSION ID: **SBX1-R1**

Industry Standards to Support Supply Chain Risk Management for Firmware

Lawrence Reinert

Laboratory for Advanced Cybersecurity Research
National Security Agency

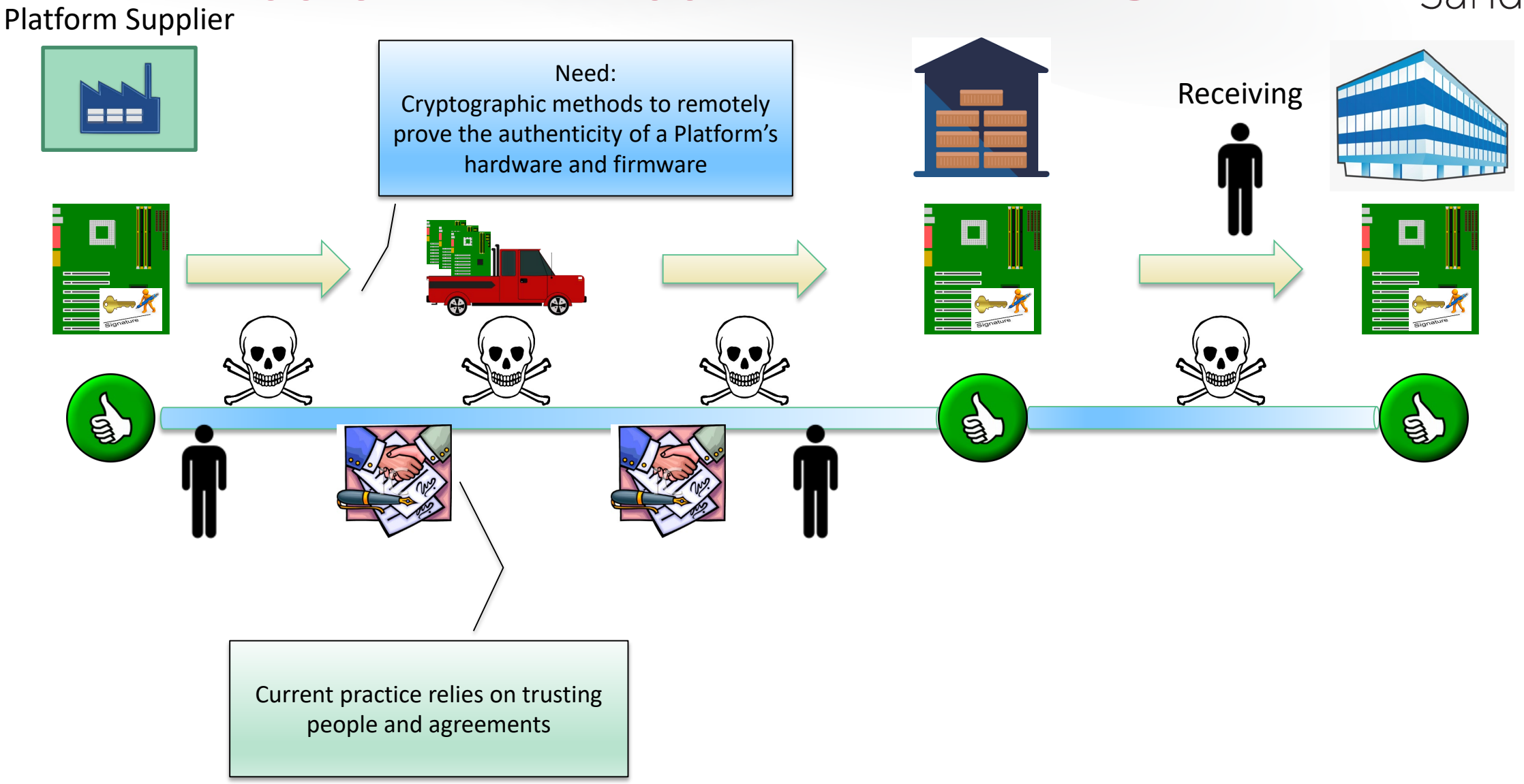
Monty Wiseman

Cybersecurity, Controls & Optimization
General Electric; GE Research Center
@montywiseman32

Problem: Trusting the Supply Chain

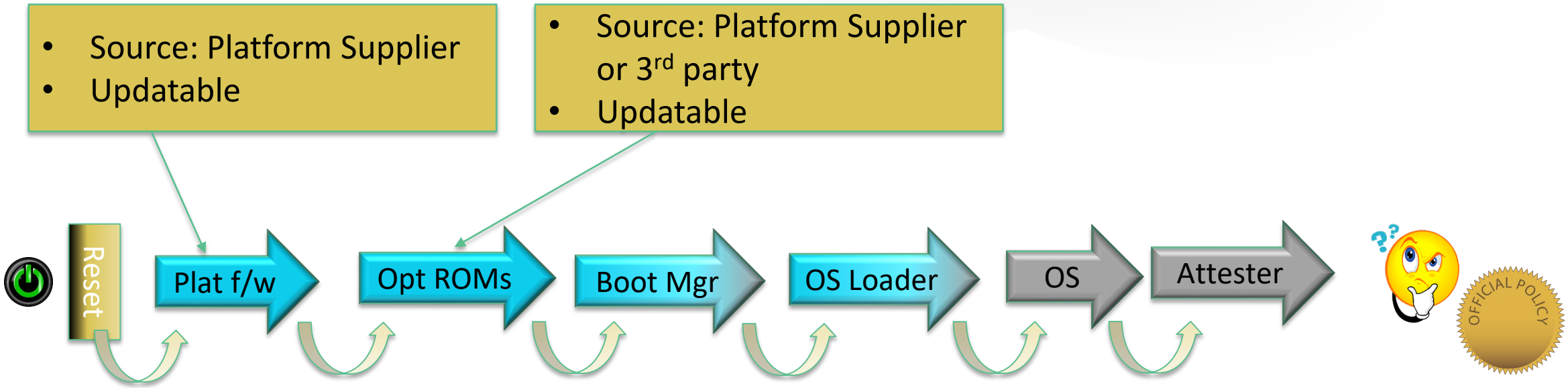
Hardware and Firmware

Manual Supply Chain–Supplier to Receiving



Inspecting Firmware at Scale

RSAC Sandbox



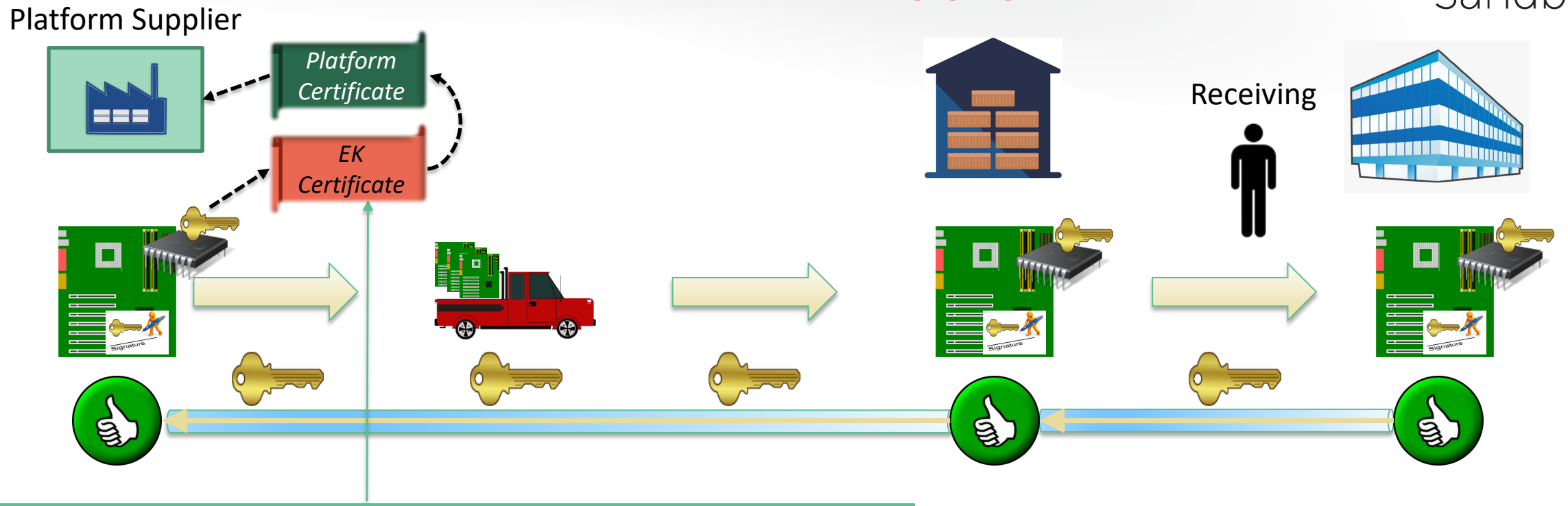
Why do we care?

- Detecting Counterfeit devices and device components
- Firmware: Malware and Vulnerable Versions of older firmware
  - Autonomous and Invisible Computing
  - Some modules run in parallel to the OS (e.g., SMI) or while the computer appears “off” (i.e., Suspend, Hibernate)
- Firmware signing necessary (e.g. via UEFI Secure Boot) but only verifies module’s source for updates
  - Verification keys are modifiable (in most configurations)
  - Does not provide explicit evidence of f/w integrity to (scalable) remote verifiers
- Plat f/w configures all components (e.g. memory, USB, wireless devices, etc.)

Solving the Problem

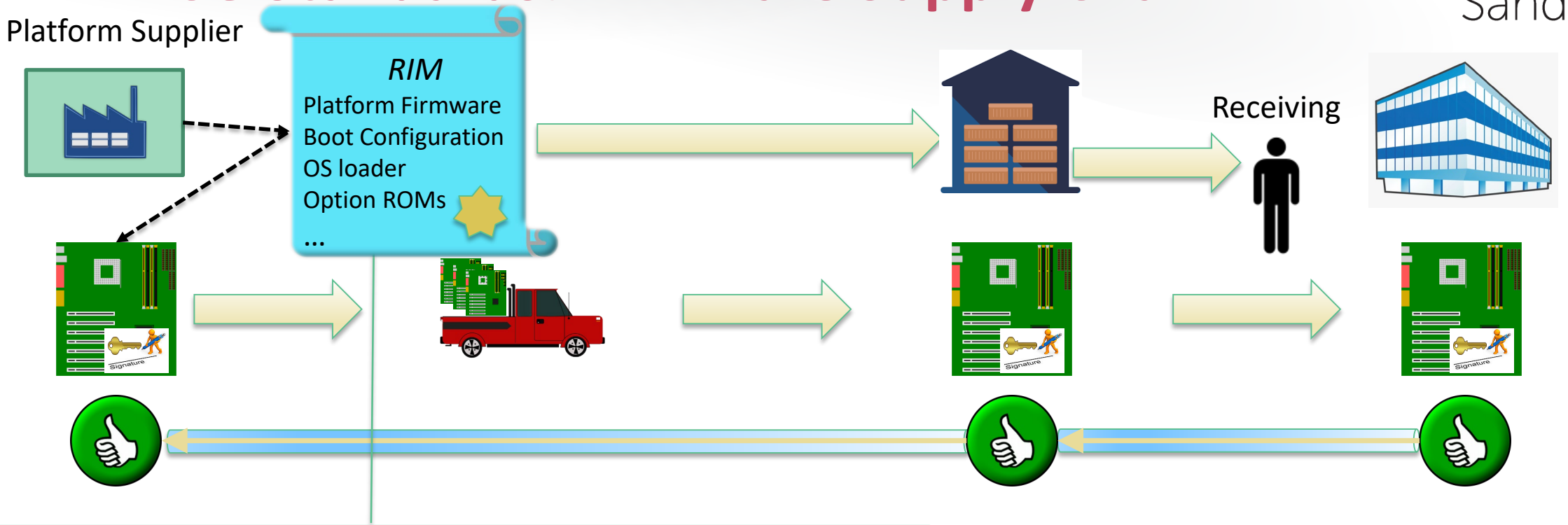
Adding Trust in the Supply Chain (Platform Hardware and FW) using TCG Standards

TCG Standards: Hardware Supply Chain



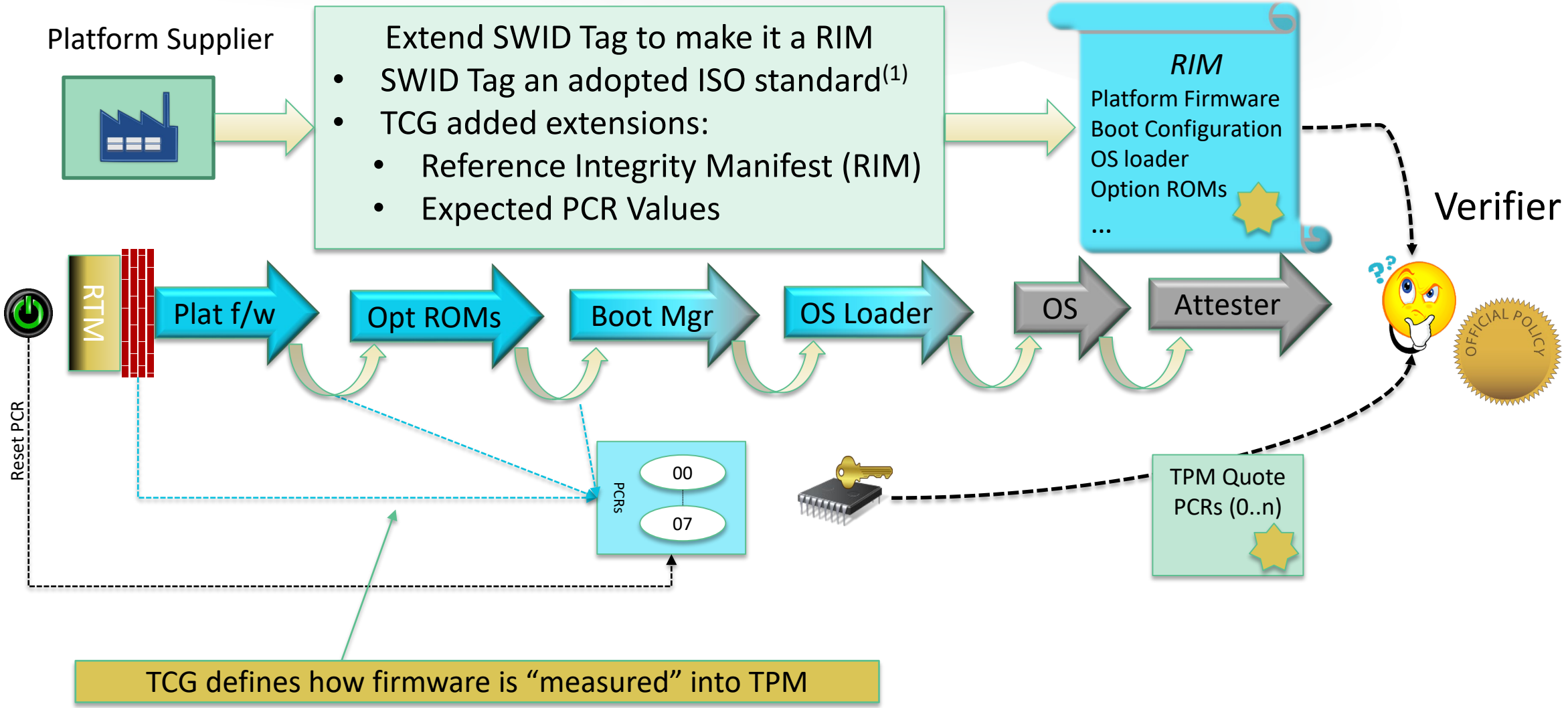
- TCG Endorsement Key & Platform Certs bind Supplier to platform
  - Provides Cryptographically bound Device Identity
  - Hardware Bill of Materials – lists components in device
  - Counterfeit detection
  - Component lists deter parts swapping

TCG Standards: Firmware Supply Chain



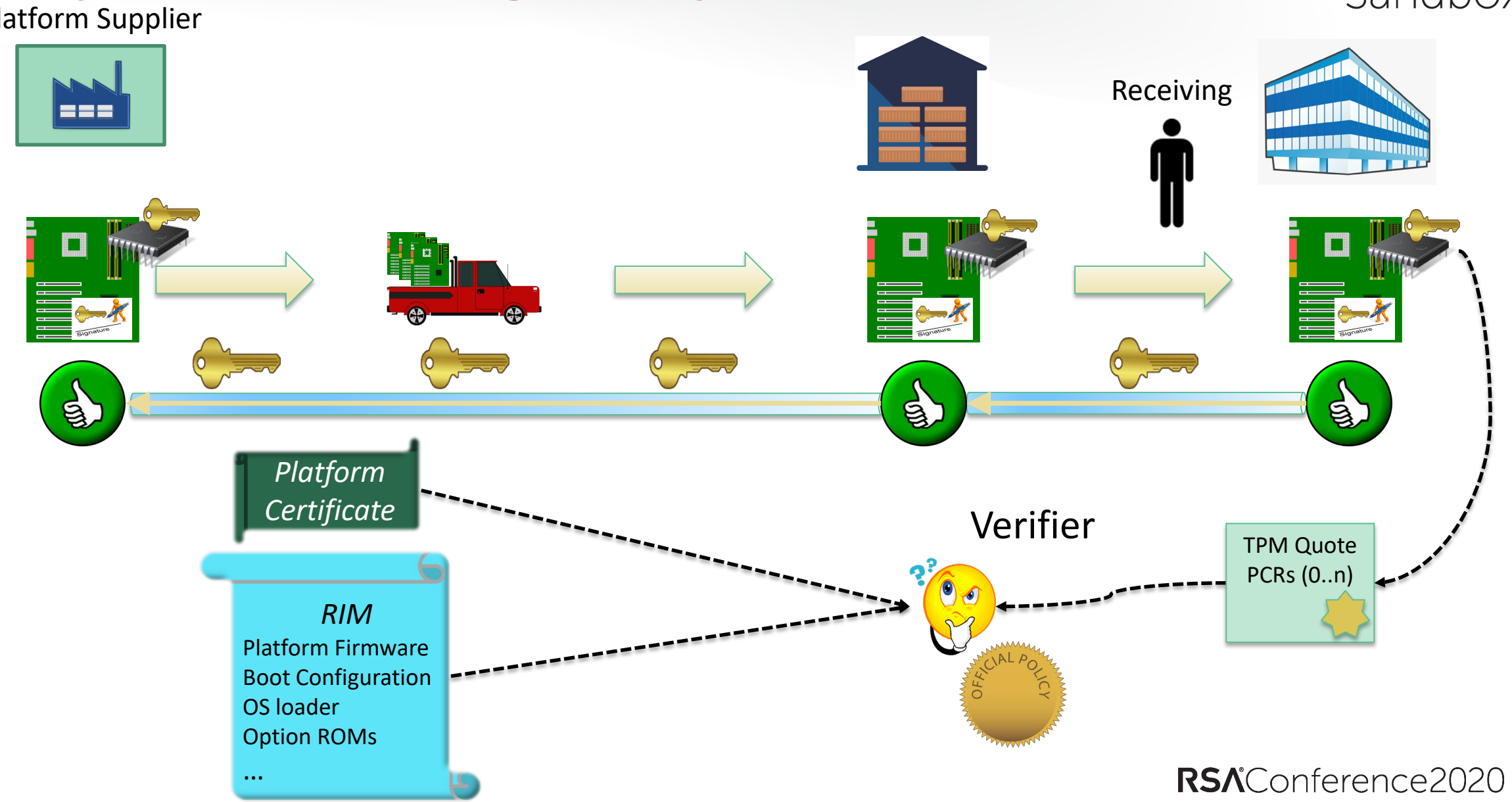
- TCG Reference Integrity Manifests (RIM)
  - (aka Golden Measurements)
  - Provides references for detecting Firmware and Boot Software modifications
  - Provides verifiable factory configuration settings

Comparing Expected (Golden) Values with Delivered



(1) ISO-IEC 19770-2 & NISTIR 8060: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

Acceptance Test Using TCG Specifications



Summary and Demo

Achieving Trusted Supply Chain

RSAC Sandbox

- Trusted Supply Chain can be achieved using open standards
  - Using Trusted Platform Modules (TPM)
  - Using TCG defined Certificates (Endorsement Key & Platform)
  - Reference (Golden) Measurements from a Trusted Source
    - E.g., the original platform supplier (OEM)
- Open source software is available

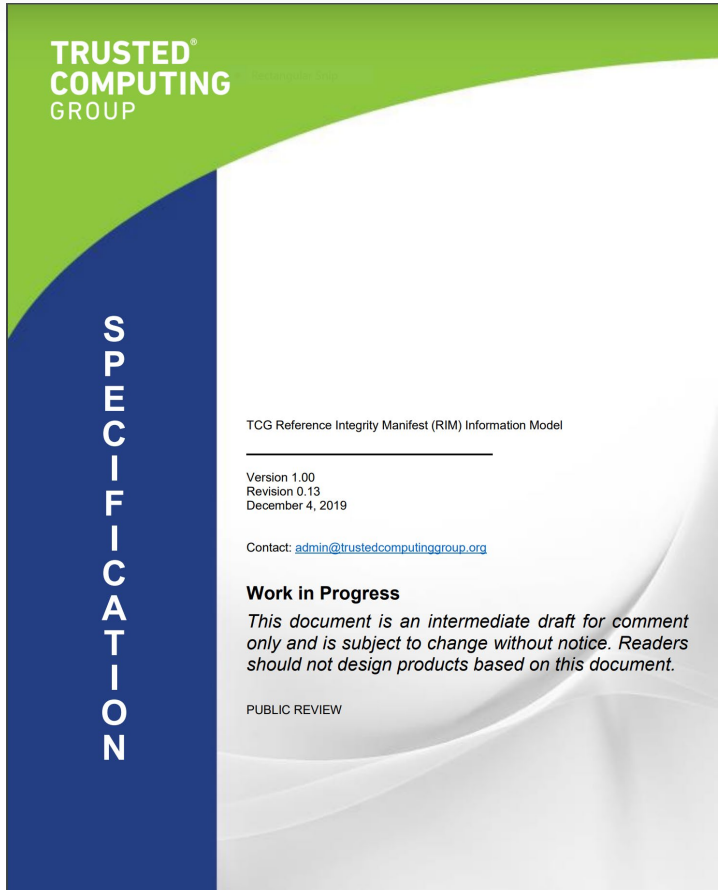
Demo

Trusted Supply Chain: Hardware and Firmware

Example RIM – Based on DRAFT TCG Specification

RSAC Sandbox

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<softwareIdentity xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" xmlns:ns3="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
    corpus="false"
    name="Example.com BIOS"
    patch="false"
    supplemental="false"
    tagId="94f6b457-9ac9-4d35-9b3f-78804173b65as"
    version="01">
  <ns3:Entity
    name="Example Inc"
    regid="http://Example.com"
    role="softwareCreator tagCreator"
    thumbprint=""/>
  <ns3:Link href="https://Example.com/support/ProductA/firmware/installfiles" rel="installationmedia"/>
  <ns3:Meta xmlns:rim="https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model"
    rim:bindingSpec="PC Client RIM"
    rim:bindingSpecVersion="1.2"
    rim:colloquialVersion="Firmware_2019"
    rim:edition="IOT"
    rim:payloadType="Indirect"
    rim:pcURIGlobal="https://Example.com/support/ProductA/firmware/rims"
    rim:pcURILocal=""
    rim:platformManufacturerId="00213022"
    rim:platformManufacturerStr="BIOSVendorA"
    rim:platformModel="AO"
    rim:platformVersion="12"
    rim:product="ProductA"
    rim:revision="r2"
    rim:rimLinkHash="88f21d8e44d4271149297404df91caf207130bfa116582408abd04ede6db7f51"/>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>uVQCImZQAW3BQqU0mq9Sa4gZxn+btddQU7K7h8Cem9E=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>pAnGOAl5x4vyegkai89gRN5olCJmNekljmVcrd7SAd51JF8ZRLfJb9OYruXOlaA32+QVsSPhRA/f
O6saSu6CmJwuEjantBFGN2TAhXZ4yWjxpEB/NAEuHfnHPoouxiZVqp8YkOQ3NC0QAI5W8dkCfqFo
XnFQHYC3c06fgaa8Q/P1gyhS3pWUZmjKytcZfjhtmNvj+URZQPVRt5PVvKuPaOklyeaxdWHngyus
aaiRhkRXesACxm+MMnXQLsqerhbWbMF2MC7oOeDzpNi3ZSFJ1JZwOFyI71UcYd52IjHFfWhGozVY
14amyx5kW1ccKK8Cm2MxyNSRGpN3uIVMZYzGBQ==</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509SubjectName>CN=example.RIM.signer,OU=PCClient,O=Example,ST=VA,C=US</X509SubjectName>
        <X509Certificate>MIIDYTCCAkmgAwIBAgIJAPB+r6VBhBn4MA0GCSqGSIb3DQEBCwUAMFMxCzAJBgNVBAYTAlVTMQsw
CQYDVQQIDAJWQTEQMA4GA1UECgwHRXhhbXBsZTERMA8GA1UECwwIUENDbGllbnQxEjAQBgNVBAMM
CUV4YW1wbGVDQTAeFw0yMDAyMTAxODE1MzRaFw0yOTEyMTkxODE1MzRaMFwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJWQTEQMA4GA1UECgwHRXhhbXBsZTERMA8GA1UECwwIUENDbGllbnQxGzAZBgNV
BAMMEmV4YW1wbGUuUklNLnNpZ25lcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKd1
lWGkSRuxAAY2wHag2GVxUk1dZx2PTpfQOflvLeccAVwa8mQhlsRERq+QK8ilj8Xfqs44/nBaccZD
OjdfIxIUCMfwhGXjxCaqZbgTucNsExDnu4arTGraoAwzHgOcVLiKT/Cxj9NL4dcMgxRXsPdHfXbO
923C7xYd2t2qfWO5umgaj7qeQl6c68CFNsGX4JA8rWFQZvvGx5DGlK4KTcjPuQQINs5fxasNKqLY
2hq+z82x/rqwr2hmyizD6FpFSyIABPEMPfBO36GEhRwu1WEMkq8yIp2jgRUoFYke9pB3ph9pVowO
Hh4mNFSKD4pP41VSKY1nus83mdkuukPy5oOCAwEAAaMvMCOwCQYDVR0TBAIwADALBgNVHQ8EBAMC
BsAwEwYDVR0lBAwwCgYIKwYBBQUHAwMwDQYJKoZIhvcNAQELBQADggEBAGuJ+dasb3/Mb7TBJ1Oe
al5ISq8d2LQD5ke5qnjgSQWKXfQ9fcUy3dWnt3Oked/i8B/Tyk3jCdTZJU3J3iRNgTqFfMLP8rU1
w2tPYBjjuPKiiK4YRBHPxtFxPdOL1BPmL4ZzNs33Lv6HOm4aff9p6QpMclX5b/CRjl+8OJWRLiLj
U3BOCejZB9dJrPr9SBaC31cDoeTpja9Cl86ip7KkqrZZIYeMuNF6ucWyWtjrW2kr3UhmEy8x/6y4
KigsK8sBwmNv4N2Pu3RppeIcpjYj5NVA1hwRA4eeMgJp2u+urm3lloo1UNX1HsSSBHp1Owc9zZLm
07Pl8T46kpIA4sroCAU=</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</softwareIdentity>
```



https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf

Action

Think

- Do you know where your hardware platform “really” came from?
  - Can you identity all computers on your network
  - If they are malicious, will the software really identify itself?
- Do you know if the firmware (or even OS, apps) is authentic?
  - Remember, the firmware’s execution is long before the OS and any anti-malware is running
- Without trusted hardware there is now way to know

Download and Review

RSAC Sandbox

- Industry Specification:
  - TCG Platform Certificate: https://trustedcomputinggroup.org/wp-content/uploads/TCG-Platform-Attribute-Credential-Profile-Version-1.0.pdf
  - TCG Reference Integrity Manifest: https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf
- Get involved with Trusted Computing Group
  - More standards being developed in this area
- Review Open Source projects
  - HIRS: https://github.com/nsacyber/HIRS
  - Go-Attestation: https://github.com/google/go-attestation

References

RSAC Sandbox

- Software Identification tags
  - SWID tags support software inventory and asset management initiatives
  - ISO-IEC 19770-2
    - Requires purchase
  - NISTIR 8060
    - Describes SWID tags in sufficient detail for our purposes
    - https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf
  - CoSWID
    - https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid
- Records unique information about an installed software application
  - Its name, edition, version, etc.
  - whether it is part of a bundle and more
- Tools:
  - https://tagvault.org/about/
  - https://github.com/strongswan/swidGenerator
- Other references:
  - https://csrc.nist.gov/Projects/Software-Identification-SWID/management