Platform Security Services Overview

This emerging service accelerates industry adoption of platform trust technologies that are the building blocks of Zero Trust and supply chain security.

Authors

Eduardo Cabre
Principal Engineer
Lead Architect

Pravin Chaudhari
Security
Software Architect

Masud Chowdhury
Engineering Director

Table of Contents

Executive Summary

Platform attestation is the process of verifying and validating the integrity and security of a computing platform, such as a server, desktop, mobile, or IoT device. This process involves verifying the hardware, firmware, and software components of the platform to confirm that they have not been tampered with or compromised.

Intel's upcoming service, code-named "Platform Security Services" (PSS), is a business initiative within the Intel® Key Generation Facility (IKGF), a part of DCP LLC[1], to develop and offer services that support industry adoption of emerging platform trust technologies Device Identifier Composition Engine (DICE), Security Protocol and Data Model (SPDM), Reference Integrity Manifest (RIM), and Platform Root of Trust (PRoT). These technologies are becoming the fundamental building blocks of Zero Trust and supply chain security.

DICE creates a unique device identifier that is used to verify the authenticity of the device during the boot process. This helps prevent unauthorized modifications to the device, its firmware, or its software. In addition, SPDM is a standard developed by the Distributed Management Task Force (DMTF) used to establish secure communication between a device and a remote server, verifying the device's identity and verifying that the device has not been tampered with. SPDM helps protect against attacks such as man-in-the-middle attacks and firmware-level malware. The Reference Integrity Manifest (RIM) is the third component of the PSS. The RIM is a standard defined by the Trusted Computing Group (TCG). It is a file that contains a cryptographic hash of each file in a software package, along with other metadata such as file sizes and timestamps. RIMs are used to verify that software packages have not been modified or tampered with, as any changes to the package would result in a different hash value. RIMs can be used to verify the integrity of software packages during installation or distribution.

Industry standard organizations like TCG, DMTF, the Internet Engineering Task Force (IETF), and Open Compute Project (OCP) are driving the standardization of these technologies[2][3][4]. Intel is contributing heavily to the development of these standards. For market deployment, these standards will require support infrastructure. The goal of PSS is to facilitate implementation of these standards by providing a comprehensive portfolio of solutions, as well as the legal and governance frameworks required for their success.

PSS will also be applied to the Intel® Transparent Supply Chain service[5] to dramatically improve supply chain transparency, component and system level traceability, and tamper resistance over the entire lifecycle of the compute system.

What Problems are We Trying to Solve?

Cyber adversaries have been shifting their attacks to hardware, embedded code (firmware, BIOS), and the supply chain of hardware components. Per one estimate[6], the cost of counterfeited hardware costs the industry about $250 billion. To counter this, the industry has been adopting Zero Trust frameworks. In a Zero Trust framework, every user and device must be continuously validated and monitored to ensure trust. The validation of devices is typically done with X.509-based certificates using an attestation protocol, which verifies in real time the trustworthiness of a device. This is done through the attestation of individual components and firmware with a known reference measurement. Component suppliers are actively implementing these technologies in their products.

With sophistication and persistency of cyberattacks on rise, the President of the United States recently issued an Executive Order on Improving the Nation's Cybersecurity[7]. This Executive Order mandates adoption of Zero Trust frameworks for the Federal Government of the United States. PSS aims to accelerate industry-wide adoption of Zero Trust Framework Device Identification and Device State Verification.

To successfully implement Zero Trust technologies, component vendors are required to implement or outsource complex security and cryptography infrastructure. Manufacturers will need to provision their devices with digital certificates issued from trusted Public Key Infrastructure (PKI), which is difficult and complex to maintain. The proliferation in the number of PKI trust anchors (each vendor operating as its device root of trust) will make verifiers' job difficult, requiring them to maintain large databases of roots of trust with little infrastructure and guidance on how to determine the trustworthiness of those roots.

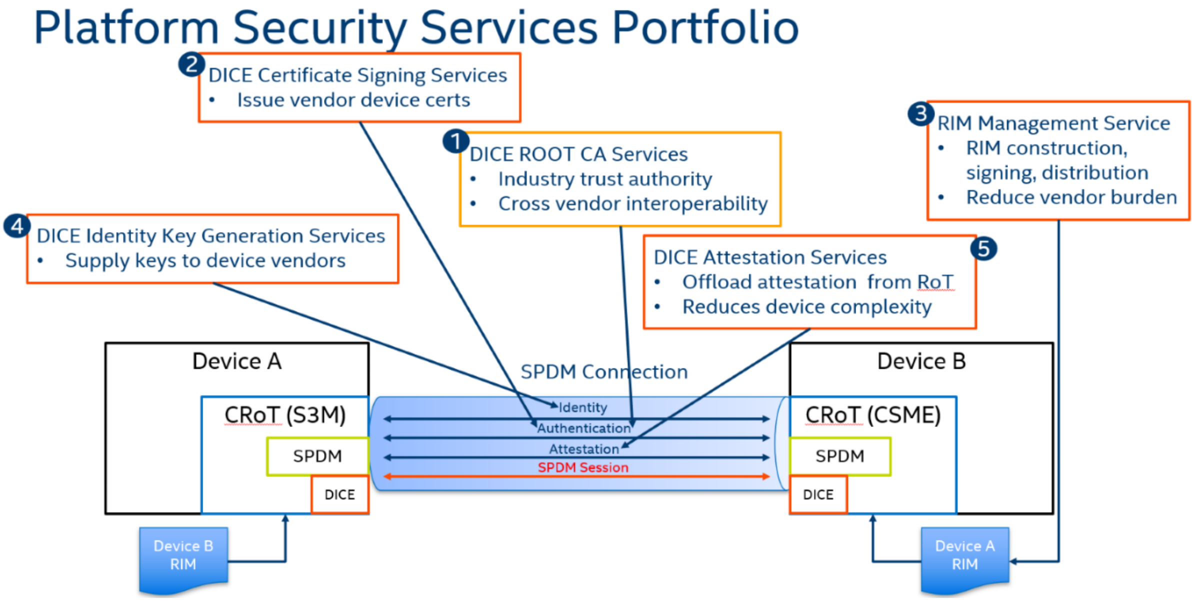
It is critical that Zero Trust solutions begin at the very earliest stages of device manufacturing. Manufacturers will need to develop and operate the facilities for issuance and provisioning of digital certificates used in the attestation protocol device identification process. These facilities require a certain level of expertise and infrastructure not inherently available to component vendors. Certificates will need to be securely issued and provisioned, and the certificate lifecycle will need to be managed for validity period and revocation. In addition, vendors will need to carefully collect, version, manage, and issue Reference Integrity Manifests containing the good known configuration (golden measurements) with which verifiers attest to their products. Complex supply chain scenarios will make the process of managing these measurements complex, requiring delegating the authority for issuing and updating Reference Integrity Manifests to downstream entities. Development of an ownership tracking and delegation facility will be necessary to address such complex supply chain scenarios.

Lastly, these technologies have little value without an end user's ability to efficiently attest to the trustworthiness of a product. Services that streamline the attestation and verification process of devices will become essential and will be made available to CSPs, enterprises, government, and other end customers to fully realize the value of Zero Trust. Attestation and verification services will be a critical piece of this infrastructure. Attestation cannot operate independently from the attestation policies that dictate what actions must be taken when the attestation is being performed. These may be, for example, not allowing a server to join a domain unless attestation is successful or forbidding a high-value compute workload to execute in a virtual machine unless it is trusted. End users will need to have the capability to dictate attestation policies in a generalized manner.

PSS has created an industry-wide Certificate Authority (CA) policy and legal framework imperative to facilitate Zero Trust frameworks. PSS, along with the CA policy and legal framework, and its application within a system-wide service such as Intel® Transparent Supply Chain are developed with the objective of addressing these technical challenges and facilitating the widespread adoption of Zero Trust.

The Intel Platform Security Service

The PSS is comprised of multiple subsystems as shown in the figure below.


Platform Security Services Portfolio
2
DICE Certificate Signing Services
• Issue vendor device certs
1
DICE ROOT CA Services
• Industry trust authority
• Cross vendor interoperability
3
RIM Management Service
• RIM construction, signing, distribution
• Reduce vendor burden
4
DICE Identity Key Generation Services
• Supply keys to device vendors
DICE Attestation Services
• Offload attestation from RoT
• Reduces device complexity
5
Device A
CRoT (S3M)
SPDM
DICE
SPDM Connection
Identity
Authentication
Attestation
SPDM Session
Device B
CRoT (CSME)
SPDM
DICE
Device B RIM
Device A RIM

DICE Root CA Services

Adoption of Platform Security technologies requires component and platform vendors to provision digital certificates. Each vendor will need to operate their own digital certificate authority or outsource to external certificate authorities the issuance of certificates. This will result in numerous trust anchors. Also, verifiers such as CSPs, Enterprise IT, or service providers will need to manage a large number of trust anchors, making the process complex. Interoperability is also a significant concern; devices must trust each other's certificates.

To address this, Intel has created and deployed the DCP DICE Global Root CA and Trust Authority policy. Intel is leading an industry-wide discussion to adopt a manageable number of Certificate Authorities under a shared Trust Authority policy. The DCP DICE Global Root CA will issue Subordinate CA certificates to component manufacturers such as Intel. Manufacturers will have the ability to issue certificates for their own devices under a common Root. The benefits of this global root CA include:

- product interoperability due to mutually trusted DICE Global Root
- trust anchor management simplified - from many anchors to one
- subordinate CA operating under policy defined by DCP DICE PKI Policy Authority
- simplifying vetting by verifiers and attestors

The DCP DICE Global Root CA ecosystem is described in diagram below:

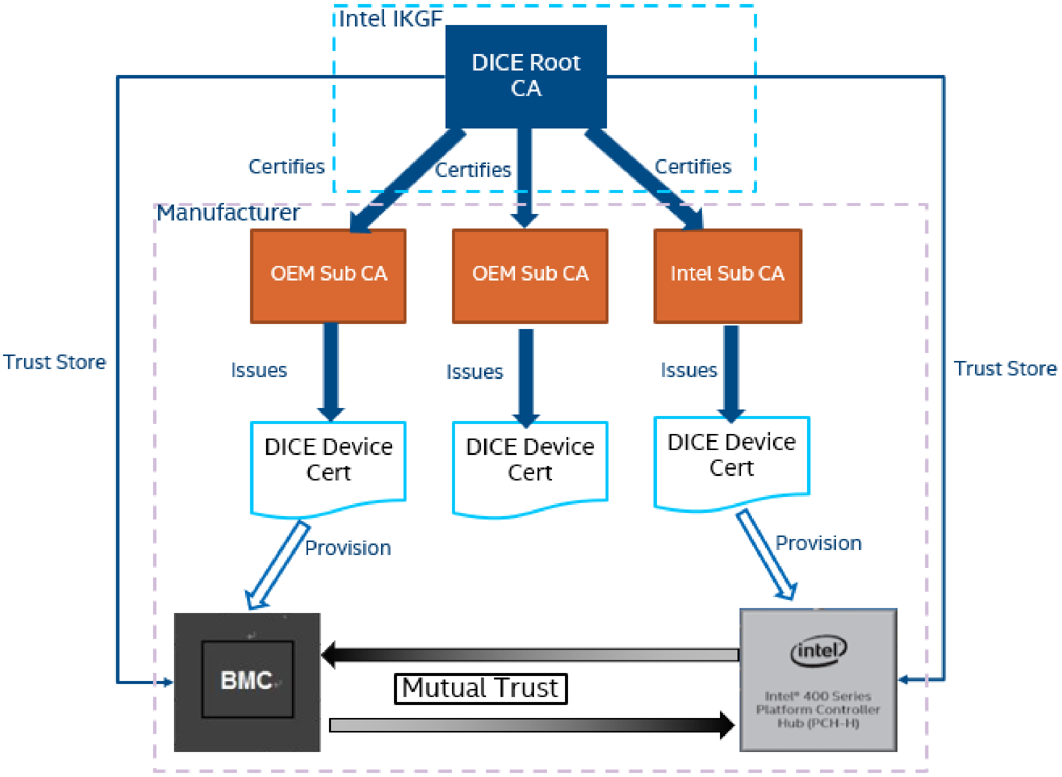
DCP Signing Service (DSS)

The fundamental block to enable Platform Security is X.509 certificates. These certificates are signed by a PKI-based CA. Intel has created a highly versatile, low cost, highly available Signing Service that implements the complete X.509 PKI specification defined in IETF RFC 5280[8]. DSS supports certificate revocation lists (CRL) and the Online Certificate Status Protocol (OCSP) for obtaining the revocation status of an X.509 digital certificate.

DSS supports flexible CA hierarchies such as hosting the Root CA, Intermediate CA in a highly secure facility, while hosting the Signing CA in the cloud, hosting the whole chain in the cloud, or any combination thereof. The DSS has numerous potential use cases such as supporting real time, geographically distributed manufacturing certificate provisioning of devices, field provisioning of device secondary identity certificates, RIM issuance, and others.

RIM Management Service (RMS)

Attestation is a critical element of establishing trustworthiness of a computing device prior to using it for processing sensitive data. The attestation process is used by a device to provide evidence of its state to a relying party. This process consists of evaluating the attestation evidence provided by the device against references provided by the manufacturer. RIM is the standard that defines how "references provided by the manufacturer" need to be collected, signed, and made available to verifiers. Device manufacturers are responsible for generating RIMs for their products. A RIM contains information such as device reference values, measurements



for installable software / firmware, embedded firmware, and digital certificates.

PSS is in process to implement the RIM Management Service to alleviate the complexities of collecting, storing, versioning, and issuing RIMs. This service supports the TCG Concise Reference Integrity Manifests (CoRIM). CoRIMs are the standardized RIM specification and the foremost mechanism for encoding reference data. The RIM Management Service will provide users the facilities to manage, update, generate, and distribute reference integrity measurements via the issuance of CoRIMs.

Key Generation Service

Device manufacturers will need to program cryptographic keys and other secrets in their products to support Zero Trust. While many devices have internal capabilities to generate keys, constrained devices (IOT, sensors, accelerometers) do not. Provisioning constrained devices with cryptographic keys requires the right infrastructure and security controls. Intel has over 20 years of experience providing a wide range of cryptographic solutions, including key and certificate generation that are secure, reliable, low-cost, and high quality. As part of PSS, Intel is creating a service to generate and distribute keys to device vendors. These keys will be generated and delivered securely to the vendors manufacturing facility for provisioning. Intel will leverage its secure facility and full disaster recovery capability to enhance the security and value of this service offering.

Attestation Service

Attestation is the process of verifying the security configuration of a device against a set of good known settings. End users would want to leverage attestation as a mechanism for confirming the trustworthiness of a component, device, or platform. In order to facilitate this process, generalized attestation services will be needed as part of ecosystem enablement. The PSS initiative is developing an attestation service for component and platform manufacturers wanting to enhance their customer's experience.

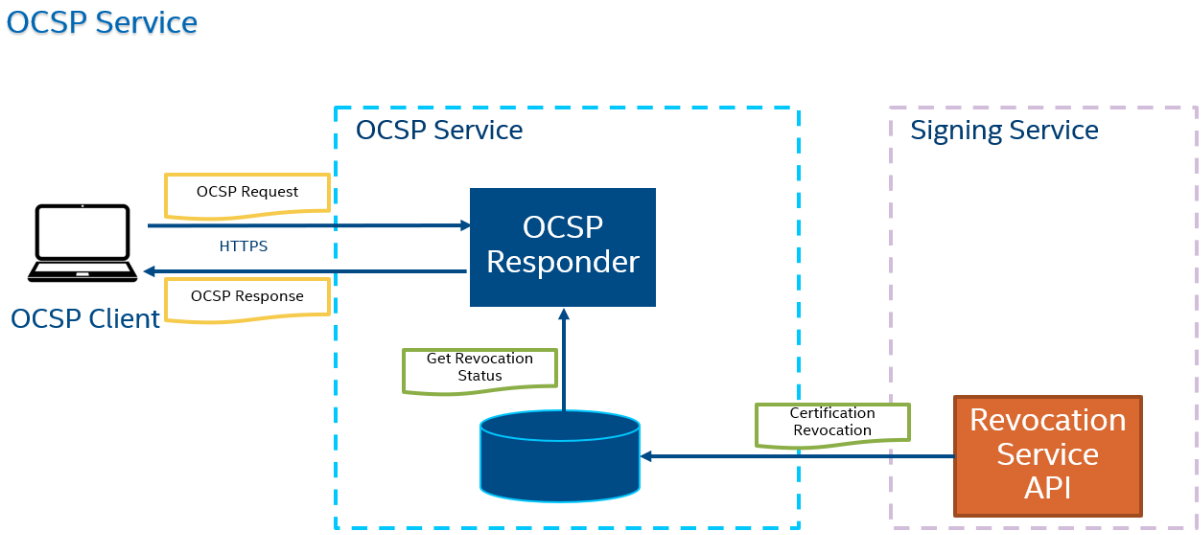
As part of onboarding a new platform, entities such as CSPs, Enterprise Data Centers, and Enterprise IT (Verifier) would collect attestation evidence and forward it to the Attestation Service. The Attestation Service will retrieve corresponding platform and device CoRIMs and appraisal policies and evaluate the reported measurements. The Attestation Service will then send the evaluation result back to the Verifier. The Verifier will decide whether to proceed with onboarding the platform based on the results obtained from the service. Other use cases such as secure boot, supply chain security, and confidential computing are also supported by the Attestation Service.

OCSP Service

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. The OCSP protocol is an Internet standards track described in RFC 6960 [9]. It was created as an alternative to CRLs, specifically addressing certain problems associated with using CRLs in a PKI system. An OCSP responder is a server typically run by the certificate issuer. It is responsible to return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'.

A perfect complement to the DCP Signing Service, the OCSP service provides real-time certificate status information. It can support any CA hosted in DSS. When a client wants to verify the status of certificate, it sends an OCSP request to the OCSP responder. The OCSP responder checks the CRL database and returns an OCSP response indicating the status of the certificate. If the certificate is still valid, the OCSP responder will return status as 'good'. If the certificate is revoked, the OCSP responder will return status as 'revoked'; otherwise, it will return 'unknown'.

The OCSP service is highly available and globally geographically distributed for low latency. The OCSP Service flow is described in the diagram below.



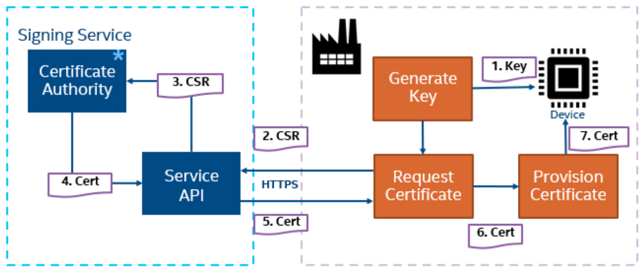
PSS Use Cases

PSS are being developed to serve multiple purposes. First, to enable Intel product groups to implement Zero Trust technologies in Intel silicon. Second, to be leveraged by other security service offerings like Project Amber, Transparent Supply Chain, and the DCAI Platform Integrity Solution. And lastly, to be offered as a revenue services portfolio directly to external customers.

Provisioning Primary Credentials for Device (During Manufacturing)

Component manufacturers will provision DICE Device Id certificates in their devices as part of their manufacturing process. The DCP Signing Service can be leveraged by manufacturers to perform this operation. The DCP Signing Service supports real time, geographically distributed certificate provisioning. Devices can generate a cryptographic key internally and send the public key to the DCP Signing Services for certification. This flow is described in the diagram below:

Primary Credential Provisioning

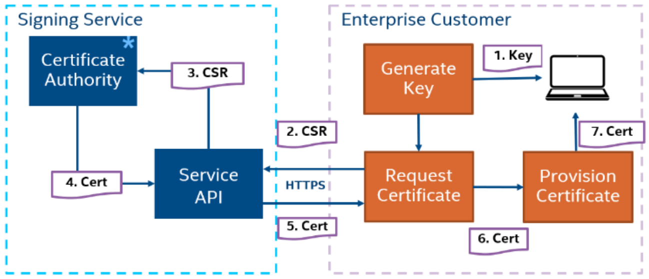


* Anchored on Root CA owned by customer

Remote Provisioning of Secondary Credentials for Device (In the Field)

When enterprise customers receive a platform, they may want to provision it and its component with certificates that they trust. Customers may leverage the DCP Signing Service to perform this operation. The DCP Signing Service can be used to generate DICE certificates from a PKI trusted by the customer. The certificates will allow the enterprise customer to perform internal onboarding, monitoring, and runtime attestation operations within their environment.

Remote Credential Provisioning



* Anchored on Root CA owned by customer

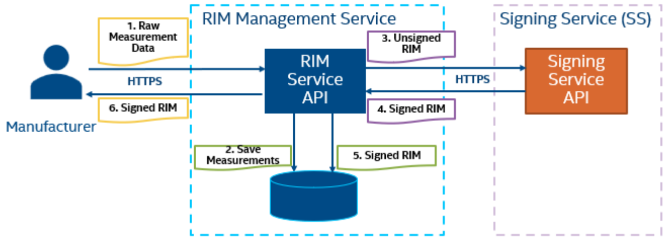
RIM Management

When component manufacturers want to enable DICE in their products, they will have to collect attestation reference measurements and issue a RIM file. This process requires expensive tooling and services to construct, sign, and distribute RIMs.

The RIM Management Service (RMS) is a fully automated system which will provide customers with the APIs necessary to efficiently manage its database of product reference measurements, as well as manage versioning of those measurements. In addition, with its integration to the DSS, the RMS will be able to construct and digitally sign CoRIMs with Certificate Authorities operated by the DSS. Customers may configure their own Certificate Authorities for issuing CoRIMs.

A high-level flow of the RIM Generation in RMS is described in the diagram below:

RIM Generation

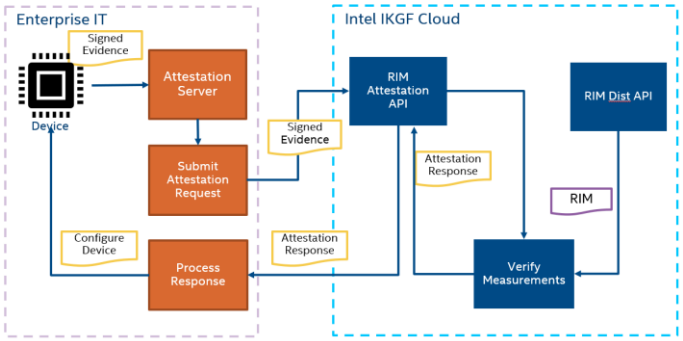


Platform Attestation

Upon acquiring a new platform, the enterprise customer would want to attest it prior to deploying into its trusted infrastructure. In addition, the enterprise customer will need to regularly verify the integrity of the platform against compromises or unauthorized configuration changes. PSS is developing a generalized attestation service to provide attestation capabilities for onboarding and runtime verification of platform and components.

A high-level flow of the platform attestation is described in the diagram below:

Platform Attestation



Key Generation Service for Component Manufacturers

Intel hosts and operates dozens of CAs that provide signing capabilities for Intel products. Successful operation of a CA requires a high level of security governance, regulation, and oversight. Intel has over 20 years of experience in PKI governance, regulatory, oversight, and cryptographic facility management. Currently, Intel generates cryptographic keys for multiple industry standard protocols and is well positioned to support any complementary key generation to proliferate the adoption of Platform Security Services.

Supply Chain Security and Platform Integrity (Application of PSS for Intel® Transparent Supply Chain)

The Intel® Transparent Supply Chain (TSC) service will be enhanced with PSS to expand the system root of trust from the TCG Trusted Platform Model (TPM) to a dynamic PRoT established via DICE and SPDM. The application of PSS to TSC will also enhance the TCG Platform Certificate v1.1 to a platform RIM enabling new protections and usages for supply chain security.

The PSS services can be used to enable the following [10]:

Supply Chain Protection

Supply chain protection is primarily about detecting a compromise and protecting the platform from the time components leave their manufacturing facilities till it arrives to end user. The buyer should be able to verify that the platform (including all its components) is authentic and is in the same state (same components in the same places, same versions of FW, same configuration values, etc.) the manufacturer shipped it.

Installation and Update Protection

The primary function of installation and update protection is to protect against and prevent a compromise; it relies heavily on PRoT enforcing authorization by checking cryptographic signatures of software and verify them against the source before any update.

In addition to protecting against compromise, installation and update mechanisms must include provisions to securely update the platform RIM because the platform state is bound to change because of update. This involves collecting the new state, creating an updated platform RIM, and cryptographically signing it.

Runtime Protection

Runtime protection of platform integrity supports both prevention and detection of compromise. Prevention of compromise is primarily accomplished by RoTs, which provide filtering functionality to prevent unauthorized runtime updates to platform/device FW images or configurations. Detection of compromise is done through attestation. In this case, the platform/device responds to attestation requests with information about its ID, FW levels, configuration, etc. Attestation requests and responses will be supported by the SPDM protocol. Attestation responses are evaluated by comparing them to the platform RIM and applying user supplied policies.

Retirement/Reassignment Protection

Retirement/reassignment protection refers to the ability to remove any sensitive data, keys, or credentials from the platform before it is retired/reassigned. This functionality is provided by HW/FW. Execution of these functions must be authorized by the platform owner.

Conclusion

PSS is a solution for establishing and verifying trust in the components in a server, desktop, mobile device, or IoT device. In this architecture, a platform (e.g., server, baseboard management controller, or trusted external service acting in this role) communicates with attester devices (e.g., RoT for subsystems and adapters) to determine whether the device is trustworthy. PSS is a portfolio of services that enable component manufacturers to successfully implement attestation technologies such SPDM, DICE, and RIM. These services have been developed to address critical use cases such as provision of credentials during manufacturing, onboarding and runtime attestation needs, management and issuance of RIMs, and a variety of supply chain scenarios.

[1] *DCP LLC., wholly owned subsidiary of Intel*
[2] *DICE Attestation Architecture, TCG, Version 1.00, Revision 23, March 2021*
[3] *TCG RIM Information Model, TCG, Version 1.00, Revision 0.16, November 2020*
[4] *Security Protocol and Data Model (SPDM) Specification, DMTF, version 1.1.1, May 2021*
[5] *https://www.intel.com/content/www/us/en/products/docs/servers/transparent-supply-chain.html, 2022*
[6] *https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/html/CHRG-112shrg72702.htm, Nov 2011*
[7] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, May 2021*
[8] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008*
[9] *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013*
[10] *Internal Whitepaper -- End-to-End Platform Integrity by Alberto Munoz, Mike Ferron-Jones, 06/15/21*

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation.
Performance varies depending on system configuration, use, and other factors. Learn more at www.Intel.com/PerformanceIndex. Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates.
No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.
Your costs and results may vary.
All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.
Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Printed in USA XXX/XXX/XXX/XXX ♻Please Recycle XXXXXX-XXX-XXXXX