HOST INTEGRITY
AT RUNTIME
& STARTUP

Host Integrity at Startup and Runtime (HIRS)

Attestation Certificate Authority (ACA)

Portal

and

Trusted Platform Module (TPM) Provisioner

October 2024

Users Guide

Version 3.0

Table of Contents

Introduction

Host Integrity at Runtime and Startup (HIRS) is a proof-of-concept system, comprised of a collection of measurement and attestation capabilities that provide integrity analysis of a running platform. Based upon the Trusted Computing concepts defined by the Trusted Computing Group [1](TCG), HIRS provisioning services provide a full suite of capabilities for processing of the Trusted Platform Module (TPM). Capabilities include TPM provisioning, Endorsement Certificate (EC) validation, Platform Certificate (PC) validation, Attestation Certificate (AC) creation, TPM quote validation and firmware validation through the usage of the Reference Integrity Manifest (RIM). The HIRS provisioning services are comprised of an Attestation Certificate Authority (ACA) server application and a corresponding, client-side, provisioner application. HIRS supports an ACA policy that is recommended for Trusted Computing based supply chain validation. HIRS is compatible with Platform Certificates created by the Platform Attribute Certificate Creator (PACCOR)[2] and RIM Bundles created by the tcg_rim_tool[9] .

Terms

Note the following words in this document are used interchangeably:

1) Provisioner, HIRS Provisioner, TPM Provisioner, HIRS TPM Provisioner
2) Endorsement Certificate, Endorsement Credential, EC, Endorsement Key Certificate/Credential, EK Certificate/Credential
3) Platform Certificate, Platform Credential
4) Attestation Certificate, Attestation Credential, Attestation Key Certificate/Credential, AK Certificate/Credential

Background

Trusted Computing Based Supply Chain Validation Concepts

The TCG specifies a set of artifacts that can be used for the purpose of TPM provisioning and performing supply chain validation processes. These artifacts are used to indirectly verify supply chain entities associated with the manufacturing, assembly, and delivery of the device as well as verify software configuration.

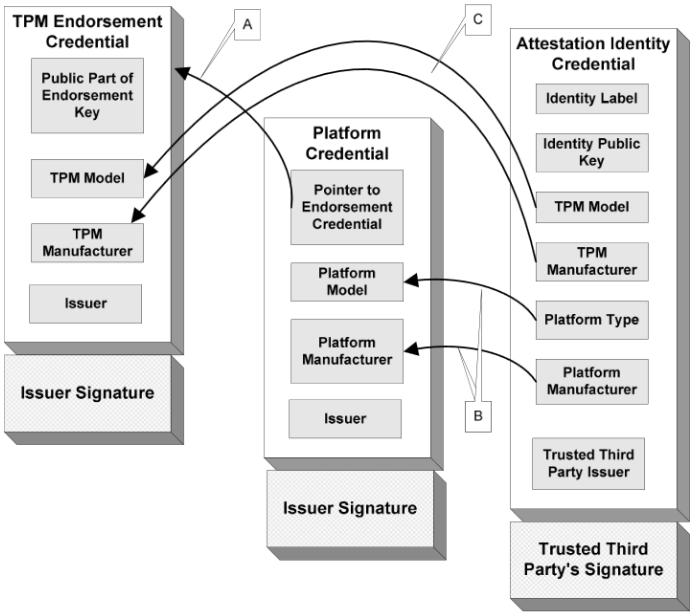
[1] https://trustedcomputinggroup.org
[2] https://github.com/nsacyber/paccor

These artifacts include:

Artifact	Creator	Usage
Endorsement Credential[3]	TPM Manufacturer	Attests that the TPM was manufactured by the TPM vendor and meets the TPM vendor's documented features
Platform Certificate[4]	Motherboard Manufacturer	Validates that the platform was manufactured by the specified vendor and meets their documented features
Attestation Certificate	IT departments	Used for device identity and validation of the software load
Reference Integrity Manifest[5]	Manufacturers, System Integrators, Value Added Resellers, Information Technology (IT) support organizations	Used for validation of the firmware

Essentially, the term "credential" is synonymous with a PKI certificate, specifically X.509 certificate as defined in the TCG's Certificate Profiles Specification(s)[6].

Note that the Platform Certificate is an X.509 Attribute Certificate that ties back to one of the public key based Endorsement Credentials using its certificate attributes:



In this context the Endorsement Certificate and the Attestation Certificate have private keys within the TPM that can be used to validate their corresponding credentials. The Platform Certificate links to the Endorsement Key/Certificate via a set of attributes within the credential. The Platform Certificate cannot be considered valid unless the Endorsement Certificate has been validated since it is linked to the Endorsement Certificate and has no private key of its own.

[3] https://trustedcomputinggroup.org/resource/tcg-ek-credential-profile-for-tpm-family-2-0/

[4] https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/

[5] https://trustedcomputinggroup.org/resource/tcg-pc-client-reference-integrity-manifest-specification/

[6] https://trustedcomputinggroup.org/wp-content/uploads/TCG_IWG_EKCredentialProfile_v2p3_r2_pub.pdf

Reference Integrity Manifests

The Reference Integrity Information Model[7] defines structures that a Verifier (i.e. a system that analyzes evidence from a platform or platform component to determine its state) uses to validate expected values (Assertions) against actual values (Evidence).

The RIM is an OEM produced artifact that can be used by the ACA when the Firmware Validation Policy option is enabled. Firmware Validation compliments the Platform Certificate for supply chain acceptance testing by providing an automated means to verify the firmware and boot software for the platform before an Attestation Certificate will be issued.

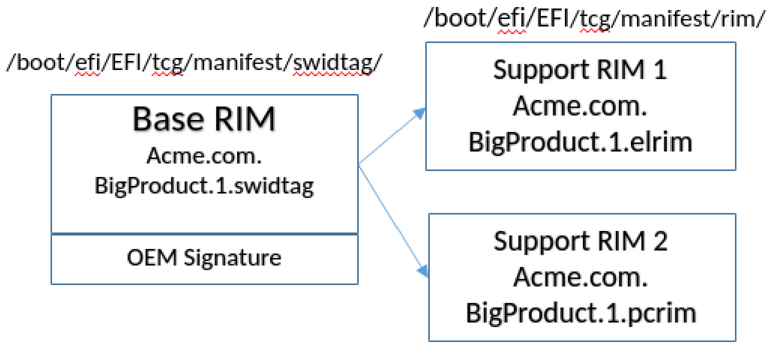
For the PC Client,[8] there are two different types of RIM files: the Base RIM and the Support RIMs. This is designated by the TCG as the “RIM Bundle”.

The PC Client RIM defines the Base Rim as an ISO 197770-2 Software Identity (SWID) standard compatible file. The Base RIM provides a verifiable identity of the RIM creator and also integrity information of Support RIMs. It contains:

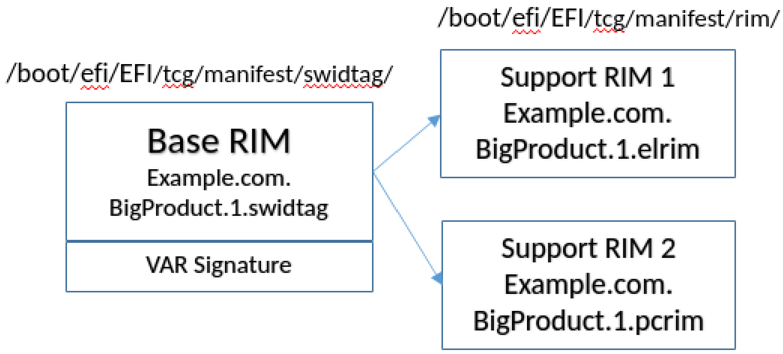
1. Cryptographically verifiable identification of the Creator of the RIM and Support RIMs.
2. A unique identifier (tagId) for a set of RIM Bundles.
3. A reference to the binding specification that defines the Support RIMs.
4. Cryptographic hashes (digests) of all Payload references including Support RIMs.
5. A digital signature of the RIM signed by the RIM’s Creator.

For PC Clients, the Support RIM utilizes the TCG Event Log created during the boot process. The TCG Event Log defined by the TCG PC Client Platform Firmware Profile[9] captures all events that extend any of the TPMs Platform Configuration Register (PCR) contents. The OEM that creates the RIM captures the TCG Event Log at the end of the production process and inserts a hash of the log into the Base RIM before the Base RIM is signed. It then stores the RIM onto the device or optionally provides a Uniform Resource Identifier (URI).

[7] https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1p01_r0p16_pub.pdf
[8] https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_RIM_r0p15_15june2020.pdf
[9] https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client-FIM_v1r24_3feb20.pdf



Acme.com Primary RIM Instance



Example.com supplemental RIM Bundle

As depicted in the image above, the RIM files can be optionally placed in the boot partition. The HIRS Provisioner will send these files to the ACA and they will be processed and stored in the database.

Validating the Supply Chain Sources Using TCG Credentials

Acceptance testing prior to initializing/provisioning/setup of a device requires valid TCG Credentials. The Endorsement credential can be found within the TPM's NVRAM (HIRS has support for reading the Endorsement credential from NVRAM). The confirmation process would consist of:

1. Validating the Endorsement Credential
2. Validating the Platform Credential
3. Validating the RIM Bundles
4. Issuing an Attestation Credential

See "Recommended Policy Setting for Trusted Computing Based Supply Chain Validation" for further details.

Each artifact has a signature used for validation. In order to trust the artifact/credential, the ACA must validate the signature via the signature's certificate chain. Each vendor must supply this certificate chain, which consists of a set of intermediate and root CA certificates. The ACA stores all of these certificates in its database. Some vendors may post the chain to a website while others may send the chain directly to the customer.

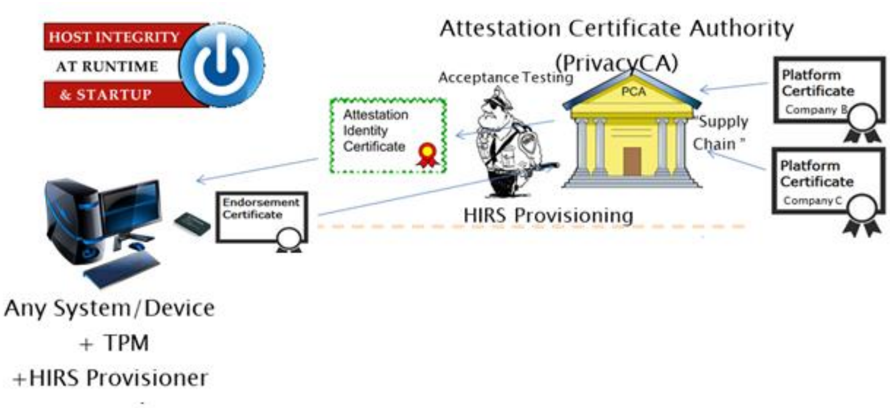
Vendors that post their certificate chain to their website will typically do so on web accessible URLs. This certificate chain can require several certificates (root CA certificates, intermediate CA certificates, etc.). Refer to the TPM manufacturer’s website for the exact location of their certificate chain URLs.

TPM Provisioning

Provisioning, in the context of this document, refers to the policies, procedures, and processes used to configure the TPM for use by an organization.

HIRS Attestation Certificate Authority

The Attestation Certificate Authority is a specialized Certificate Authority (CA) which supports the creation and issuance of an Attestation Key (AK) and/or a Device Identifier (DevID) Certificate per the TCG's specifications. The specialized nature of the ACA results from the makeup of the keys for which it is providing certificates, the formats of the requests and responses sent to/from the ACA, and the details of the identity creation process that are crucial for maintaining the "chain of trust" on which the trusted use of a TPM is based.



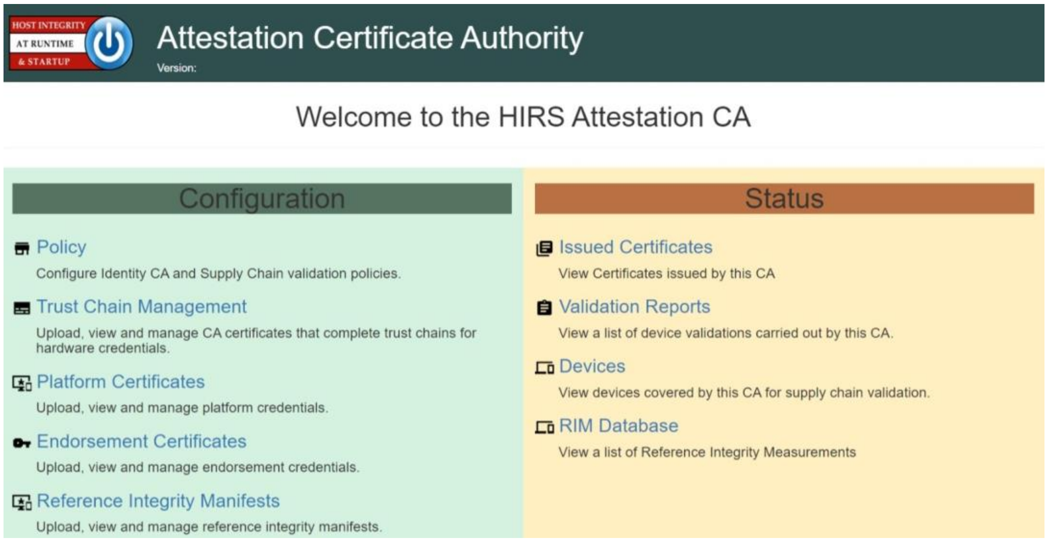
The Attestation CA is a core component of the TPM PKI architecture. Its role is certifying attestation keys, used by TPMs to sign quotes. It issues an AK Certificate to the HIRS Provisioner as part of the client provisioning process.

An Attestation CA uses a different request/response format and verification scheme than are traditionally used for PKI; however, the HIRS Attestation CA will have the option to be a subordinate to a regular, commercial CA. The ability to provide certificate revocation can be supported by a commercial CA.

HIRS ACA Web Portal

The HIRS web portal contains support for managing trust chains, setting validation policy, and viewing validation reports. After installation on a web server, the ACA portal can be accessed via a URL in a browser:

Where "hostname" is to be substituted with the name of the server that the portal is installed on. For details on the installation please refer to the HIRS ACA installation guide.



HOST INTEGRITY AT RUNTIME & STARTUP

Attestation Certificate Authority

Version:

Welcome to the HIRS Attestation CA

Configuration

Policy

Configure Identity CA and Supply Chain validation policies.

Trust Chain Management

Upload, view and manage CA certificates that complete trust chains for hardware credentials.

Platform Certificates

Upload, view and manage platform credentials.

Endorsement Certificates

Upload, view and manage endorsement credentials.

Reference Integrity Manifests

Upload, view and manage reference integrity manifests.

Status

Issued Certificates

View Certificates issued by this CA

Validation Reports

View a list of device validations carried out by this CA.

Devices

View devices covered by this CA for supply chain validation.

RIM Database

View a list of Reference Integrity Measurements

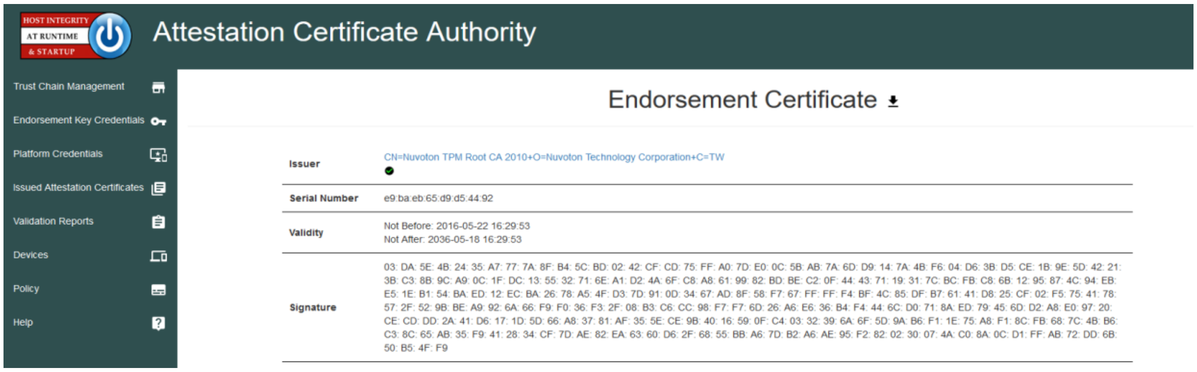
Icons used on the ACA pages generally conform to the following usage:

The ⊞ icon is used to upload certificates and other files. This will invoke a file selection dialog used to select the file to upload. The ACA will check the format of the selected file before storing it in the database, to ensure the certificate can be used appropriately.

The ⤓ icon under the option column will download the certificate to your local device. A file section dialog will be shown to allow you to select the download location.

The 🗑 icon under the option column will delete the certificate's reference from the ACA.

The 📋 icon under the options column will display details about the specific certificate. The displayed certificate is tailored to the type of certificate being viewed.



Endorsement Certificate

Issuer	CN=Nuvoton TPM Root CA 2010+O=Nuvoton Technology Corporation+C=TW ✓
Serial Number	e9:ba:eb:65:d9:d5:44:92
Validity	Not Before: 2016-05-22 16:29:53 Not After: 2036-05-18 16:29:53
Signature	03: DA: 5E: 4B: 24: 35: A7: 77: 7A: 8F: B4: 5C: BD: 02: 42: CF: CD: 75: FF: A0: 7D: E0: 0C: 5B: AB: 7A: 6D: D9: 14: 7A: 4B: F6: 04: D6: 3B: D5: CE: 1B: 9E: 5D: 42: 21: 3B: C3: 8B: 9C: A9: 0C: 1F: DC: 13: 55: 32: 71: 6E: A1: D2: 4A: 6F: C8: A8: 61: 99: 82: BD: BE: C2: 0F: 44: 43: 71: 19: 31: 7C: BC: FB: C8: 6B: 12: 95: 87: 4C: 94: EB: E5: 1E: B1: 54: BA: ED: 12: EC: BA: 26: 78: A5: 4F: D3: 7D: 91: 0D: 34: 67: AD: 8F: 58: F7: 67: FF: FF: F4: BF: 4C: 85: DF: B7: 61: 41: D8: 25: CF: 02: F5: 75: 41: 78: 57: 2F: 52: 9B: BE: A9: 92: 6A: 66: F9: F0: 36: F3: 2F: 08: B3: C6: CC: 98: F7: F7: 6D: 26: A6: E6: 36: B4: F4: 44: 6C: D0: 71: 8A: ED: 79: 45: 6D: D2: A8: E0: 97: 20: CE: CD: DD: 2A: 41: D6: 17: 1D: 5D: 66: A8: 37: 81: AF: 35: 5E: CE: 9B: 40: 16: 59: 0F: C4: 03: 32: 39: 6A: 6F: 5D: 9A: B6: F1: 1E: 75: A8: F1: 8C: FB: 68: 7C: 4B: B6: C3: 8C: 65: AB: 35: F9: 41: 28: 34: CF: 7D: AE: 82: EA: 63: 60: D6: 2F: 68: 55: BB: A6: 7D: B2: A6: AE: 95: F2: 82: 02: 30: 07: 4A: C0: 8A: 0C: D1: FF: AB: 72: DD: 6B: 50: B5: 4F: F9

Note that the issuer field will have a blue hyperlink to the issuing cert, assuming that the issuing cert is stored in the ACA. The green check under the issuer field indicates that the entire trust chain is present, and that the ACA should be able to validate the signature on that particular certificate. However, if there is a red exclamation mark instead, this means that the signature could not be validated or a certificate in the chain is missing.

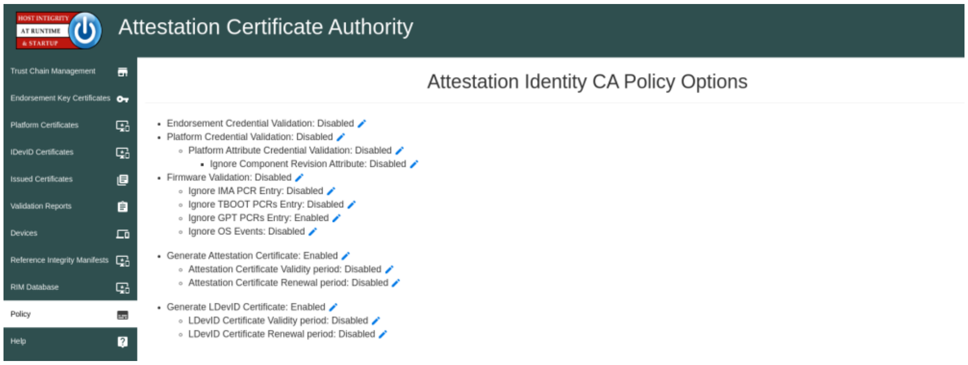
HIRS ACA Configuration

ACA configuration is a collection of pages which dictate the behavior of the ACA when it receives an Attestation Certificate Request from the HIRS TPM Provisioner.

ACA Policy Page

A HIRS ACA policy provides configuration settings for attestation provisioning for the system. The default for the ACA is to ***not*** check any credentials or attributes for TPM provisioning. This initial setting is intended to support TPM provisioning of systems that might not be delivered with supply chain credentials. This policy is set via the policy tab on the ACA portal.

Currently the options are:



Attestation Identity CA Policy Options

- Endorsement Credential Validation: Disabled
- Platform Credential Validation: Disabled
  - Platform Attribute Credential Validation: Disabled
    - Ignore Component Revision Attribute: Disabled
- Firmware Validation: Disabled
  - Ignore IMA PCR Entry: Disabled
  - Ignore TBOOT PCRs Entry: Disabled
  - Ignore GPT PCRs Entry: Enabled
  - Ignore OS Events: Disabled
- Generate Attestation Certificate: Enabled
  - Attestation Certificate Validity period: Disabled
  - Attestation Certificate Renewal period: Disabled
- Generate LDevID Certificate: Enabled
  - LDevID Certificate Validity period: Disabled
  - LDevID Certificate Renewal period: Disabled

Endorsement Certificate Validation: If selected, the ACA will require that the ACA validate the Endorsement Certificate prior to issuing an Attestation Credential. The default is ‘Disabled’.

Platform Certificate Validation: If selected, the ACA will require that the ACA validate the Platform Certificate prior to issuing an Attestation Credential. This option only validates the Certificate itself, not the attributes within the platform credential. Endorsement Certificate Validation is required to be enabled prior to enabling this policy option. The default is ‘Disabled’.

Platform Attribute Certificate Validation: If selected, the ACA will require that the ACA validate the Platform Certificate Attributes prior to issuing an Attestation Credential. This option only validates the Certificate Attributes, not the platform credential. Platform Certificate Validation is required to be enabled prior to enabling this policy option. The default is 'Disabled'.

Firmware Validation: If selected, the ACA will require that the ACA validate Firmware prior to issuing an Attestation Credential. The TCG defined artifacts necessary for this validation are: the RIM, a log file produced by UEFI, a TPM quote and PCR List, the platform certificate issued by the OEM, System Integrator or Value Added Reseller, the Endorsement Certificate to which the Platform Certificate is linked, a certificate chain of the organization that produced the Platform Certificate, and a certificate chain of the organization that produced the RIM.

Ignore IMA PCR Entry: If selected, the ACA will require that the ACA ignores the IMA PCR Entry prior to issuing an Attestation Credential. Firmware Validation is required to be enabled prior to enabling this policy option.

Ignore TBOOT PCRs Entry: If selected, the ACA will require that the ACA ignores the TBOOT PCRs Entry prior to issuing an Attestation Credential. Firmware Validation is required to be enabled prior to enabling this policy option.

Ignore GPT PCRs Entry: If selected, the ACA will require that the ACA ignores the GPT PCRs Entry prior to issuing an Attestation Credential. Firmware Validation is required to be enabled prior to enabling this policy option.

Generate Attestation Certificate: If selected, the ACA will conditionally generate an Attestation Certificate after a successful TPM provisioning.

Generate LDevID **Certificate:** If selected, the ACA will conditionally generate a Local Device ID (LDevID) certificate after a successful TPM provisioning.

Attestation Certificate Validity period: If selected, the ACA will require that the ACA will have an Attestation Certificate Validity period of the input number of days. Generate Attestation Certificate is required to be enabled prior to enabling this option. Attestation Certificate Validity period being enabled automatically causes Attestation Certificate Renewal period to become enabled. If Attestation Certificate Renewal period is disabled, this will also disable Attestation Certificate Validity period.

Attestation Certificate Renewal period: If selected, the ACA will require that the ACA will renew the input 'n' number of days before the Attestation Certificate's 'Not After' validity date which has a default of 365 days. Generate Attestation Certificate is required to be enabled prior to enabling this option. Attestation Certificate Validity period being enabled automatically causes Attestation Certificate Renewal period to become enabled. If Attestation Certificate Validity period is disabled, this will also disable Attestation Certificate Renewal period.

The recommended policy setting for Trusted Computing based supply chain validation will require these policy settings to be set to true:

- **Endorsement Certificate Validation: Enabled**
- **Platform Certificate Validation: Enabled**
- **Platform Attribute Certificate Validation: Enabled**
- **Firmware Validation: Enabled**
- **Generate Attestation Certification: Enabled**

It should be noted that:

- **Firmware Validation** should only be set to enabled if the device manufacturer supports RIMs.
- **The IMA policy option** refers to IMA which is a Linux feature that utilizes PCR10. Selecting this option will cause the ACA to skip evaluation of PCR10.
- **The TBOOT policy option** refers to the TBOOT which is a Linux feature that utilizes PCR17+. Selecting this option will cause the ACA to skip evaluation of PCR17+.
- **Selecting the GPT policy option** will cause the ACA to skip evaluation of events of type EV_EFI_GPT_EVENT.
- **The default for the Attestation Certificate Validity period policy option** should be 3651 days.
- **The default renewal for the Attestation Certificate Renewal period policy option** should be 365 days before the ‘Not After’ validity date.

This policy will check for and validate:

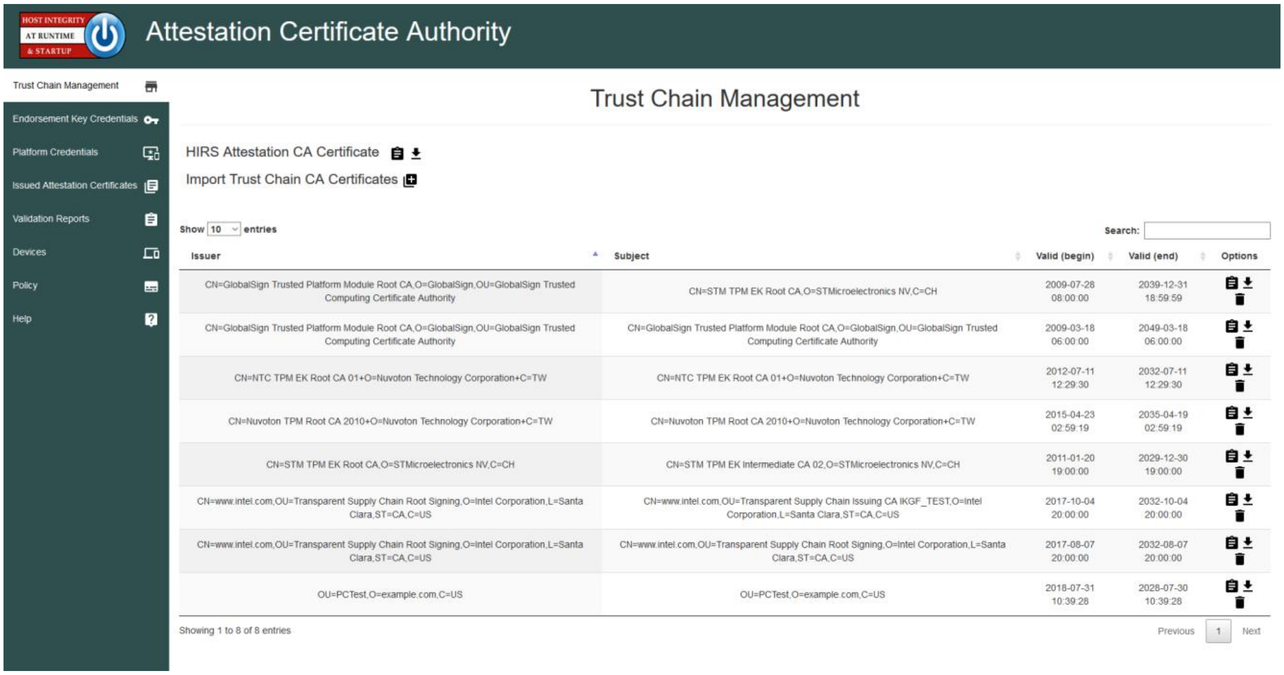
- Trust chains belonging to all TPM manufacturers of TPMs belonging to the devices that require supply chain validation
- Trust chains belonging to all platform manufacturers of the devices that require supply chain validation
    - Components defined within the Platform Credential

The recommended components initially supported by HIRS include:

- Baseboard (motherboard)
- BIOS/UEFI
- Chassis (aka the serial number typically found on a label on the back/underside of the device)
- Memory
- Disk (aka hard drive)
- Network Interface Card (NIC)
- Processor (aka the CPU)

Trust Chain Management Page

The Trust Chain Management page is intended to upload, download, and display attributes of all certificates used by the ACA for certificate validation. A set of root and intermediate CA certificates required to validate a particular certificate (Attestation, Endorsement, and/or Platform Certificate) is considered a "chain" of certificates.


HOST INTEGRITY AT RUNTIME & STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Credentials
Platform Credentials
Issued Attestation Certificates
Validation Reports
Devices
Policy
Help

Trust Chain Management

HIRS Attestation CA Certificate

Import Trust Chain CA Certificates

Show 10 entries

Search:

Issuer	Subject	Valid (begin)	Valid (end)	Options
CN=GlobalSign Trusted Platform Module Root CA,O=GlobalSign,OU=GlobalSign Trusted Computing Certificate Authority	CN=STM TPM EK Root CA,O=STMicroelectronics NV,C=CH	2009-07-28 08:00:00	2039-12-31 18:59:59	
CN=GlobalSign Trusted Platform Module Root CA,O=GlobalSign,OU=GlobalSign Trusted Computing Certificate Authority	CN=GlobalSign Trusted Platform Module Root CA,O=GlobalSign,OU=GlobalSign Trusted Computing Certificate Authority	2009-03-18 06:00:00	2049-03-18 06:00:00	
CN=NTC TPM EK Root CA 01+O=Nuvoton Technology Corporation+C=TW	CN=NTC TPM EK Root CA 01+O=Nuvoton Technology Corporation+C=TW	2012-07-11 12:29:30	2032-07-11 12:29:30	
CN=Nuvoton TPM Root CA 2010+O=Nuvoton Technology Corporation+C=TW	CN=Nuvoton TPM Root CA 2010+O=Nuvoton Technology Corporation+C=TW	2015-04-23 02:59:19	2035-04-19 02:59:19	
CN=STM TPM EK Root CA,O=STMicroelectronics NV,C=CH	CN=STM TPM EK Intermediate CA 02,O=STMicroelectronics NV,C=CH	2011-01-20 19:00:00	2029-12-30 19:00:00	
CN=www.intel.com,OU=Transparent Supply Chain Root Signing,O=Intel Corporation,L=Santa Clara,ST=CA,C=US	CN=www.intel.com,OU=Transparent Supply Chain Issuing CA IKGF_TEST,O=Intel Corporation,L=Santa Clara,ST=CA,C=US	2017-10-04 20:00:00	2032-10-04 20:00:00	
CN=www.intel.com,OU=Transparent Supply Chain Root Signing,O=Intel Corporation,L=Santa Clara,ST=CA,C=US	CN=www.intel.com,OU=Transparent Supply Chain Root Signing,O=Intel Corporation,L=Santa Clara,ST=CA,C=US	2017-08-07 20:00:00	2032-08-07 20:00:00	
OU=PCTest,O=example.com,C=US	OU=PCTest,O=example.com,C=US	2018-07-31 10:39:28	2028-07-30 10:39:28	

Showing 1 to 8 of 8 entries

Previous 1 Next

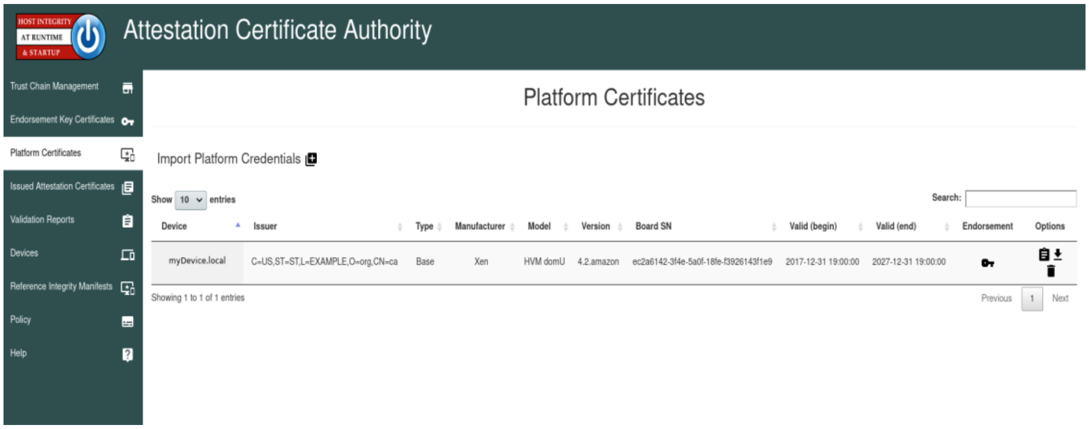
By default, the ACA generates a certificate chain that is used for verifying all issued Attestation Certificates. An Attestation CA certificate may be signed by a CA and replaced (the ACA certificate would become a subordinate to the root CA). In either case, the CA certificate must be trusted by a TPM quote appraiser.

The download icon next to the "HIRS Attestation CA Certificate" label on the Trust Chain Management page allows for a download of the ACA's certificates. These certificates will be required in future processing of TPM quotes, since TPM quotes are signed by the TPM's Attestation Key (AK).

Other CA certificates (from any organization involved with the supply chain) can be uploaded, downloaded, deleted, or viewed using the icon selections on the page.

Platform Certificates Page

The Platform Certificates (PC) page is used to upload, download, delete, and view Platform Credentials.


HOST INTEGRITY AT RUNTIME & STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help

Platform Certificates

Import Platform Credentials

Show 10 entries

Search:

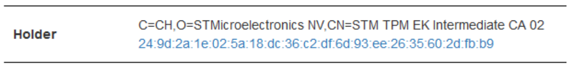
Device	Issuer	Type	Manufacturer	Model	Version	Board SN	Valid (begin)	Valid (end)	Endorsement	Options
myDevice.local	C=US,ST=ST,L=EXAMPLE,O=org,CN=ca	Base	Xen	HVM domU	4.2.amazon	ec2a6142-3f4e-5a0f-18fe-f3926143f1e9	2017-12-31 19:00:00	2027-12-31 19:00:00		

Showing 1 to 1 of 1 entries

Previous 1 Next

Viewing the individual Platform Certificate will (using the 📋 icon) provide a variety of details about the manufacturer of the device and the components contained within.

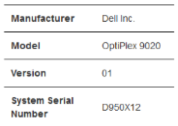
Fields of particular note when viewing a Platform Credential:



Holder	C=CH,O=STMicroelectronics NV,CN=STM TPM EK Intermediate CA 02 24:9d:2a:1e:02:5a:18:dc:36:c2:df:6d:93:ee:26:35:60:2d:fb:b9

Platform Certificate Holder field

The holder field contains the CN and Certificate Serial Number of the EK Cert. The SN will hyperlink to the EK cert, if present on the EK cert page.

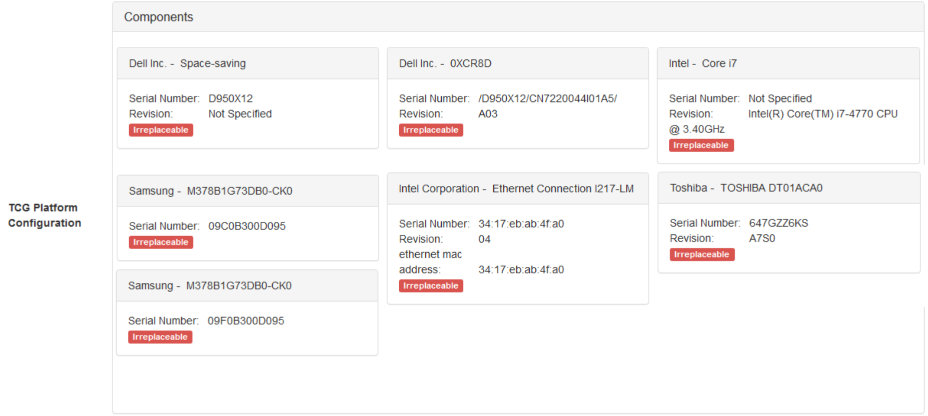


Manufacturer	Dell Inc.
Model	OptiPlex 9020
Version	01
System Serial Number	D950X12

Platform ID

The Platform ID pertains to the system's manufacturer. The "system" information is defined by SMBIOS and adopted by most major computer manufactures.

Components contain manufacturer (first item off each component), model, serial number, and revision of components specified by the manufacturer:



TCG Platform Configuration

Components

Dell Inc. - Space-saving
Serial Number: D950X12
Revision: Not Specified
Irreplaceable

Dell Inc. - 0XCR8D
Serial Number: /D950X12/CN7220044I01A5/
Revision: A03
Irreplaceable

Intel - Core i7
Serial Number: Not Specified
Revision: Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
Irreplaceable

Samsung - M378B1G73DB0-CK0
Serial Number: 09C0B300D095
Irreplaceable

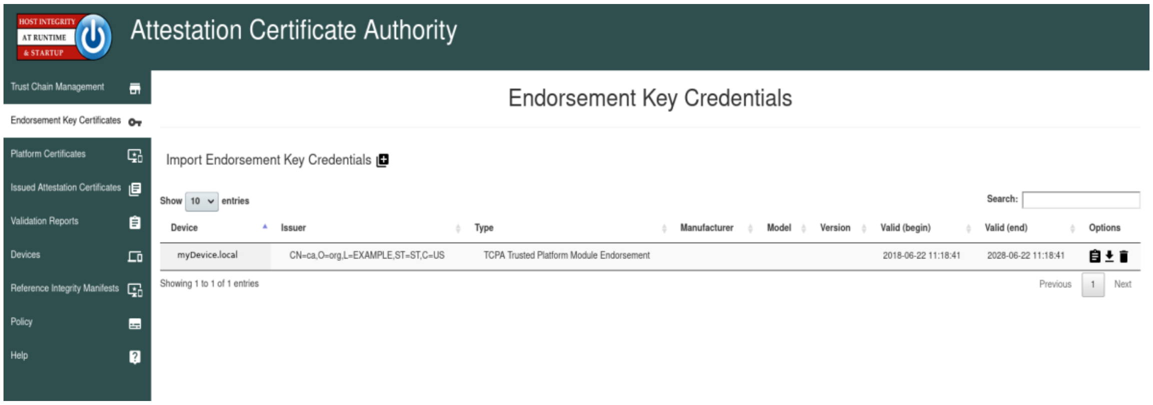
Intel Corporation - Ethernet Connection I217-LM
Serial Number: 34:17:eb:ab:4f:a0
Revision: 04
ethernet mac address: 34:17:eb:ab:4f:a0
Irreplaceable

Toshiba - TOSHIBA DT01ACA0
Serial Number: 647GZZ6KS
Revision: A7S0
Irreplaceable

Samsung - M378B1G73DB0-CK0
Serial Number: 09F0B300D095
Irreplaceable

Endorsement Certificates Page

The Endorsement Certificates (EC) asserts that the holder of the private Endorsement Key (EK) is a TPM conforming to TCG specifications. Since the EK Certificate is a public key credential, then, by definition, the signature of the issuer binds the public key material and the subject of the credential, which is a particular TPM model.


HOST INTEGRITY
AT RUNTIME
& STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help
Import Endorsement Key Credentials
Search:
Previous
1
Next

Endorsement Key Credentials

Show 10 entries

Device	Issuer	Type	Manufacturer	Model	Version	Valid (begin)	Valid (end)	Options
myDevice.local	CN=ca,O=org,L=EXAMPLE,ST=ST,C=US	TCPA Trusted Platform Module Endorsement				2018-06-22 11:18:41	2028-06-22 11:18:41	📋 ⬇ 🗑

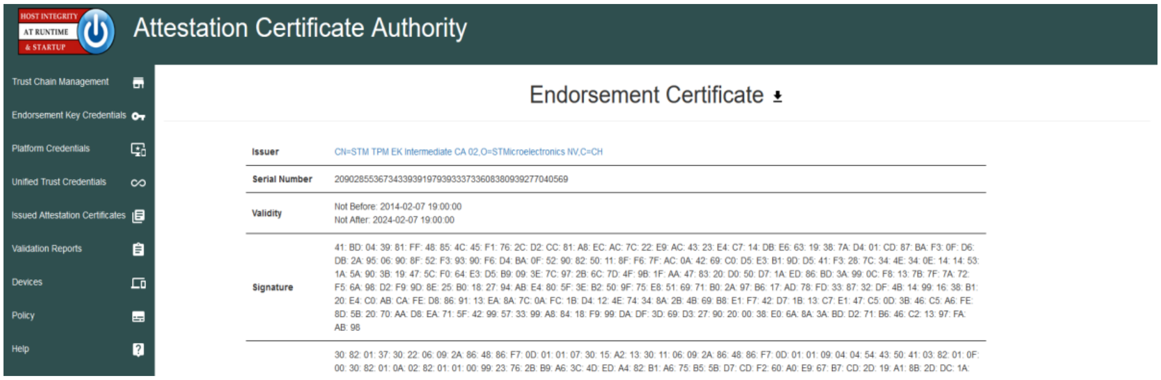
Showing 1 to 1 of 1 entries

The Endorsement Key Certificate must contain:

- The TPM public key
- The TPM model (TPM manufacturer, TPM model, and TPM version)
- Optionally the EC may contain TPM security assertions.

TPM Security Assertion	Version: 1 Field Upgradeable: true ek Generation Type: INJECTED ek Generation Location: TPM_MANUFACTURER ek Certificate Generation Location: TPM_MANUFACTURER

The EK Certificate gets used for TPM provisioning and supply chain confirmation. The ACA requires that the Trust Chain is uploaded via the Trust Chain page of the ACA prior to performing any validation of EK Credential. For further information refer to the TCG Certificate Profile specification.

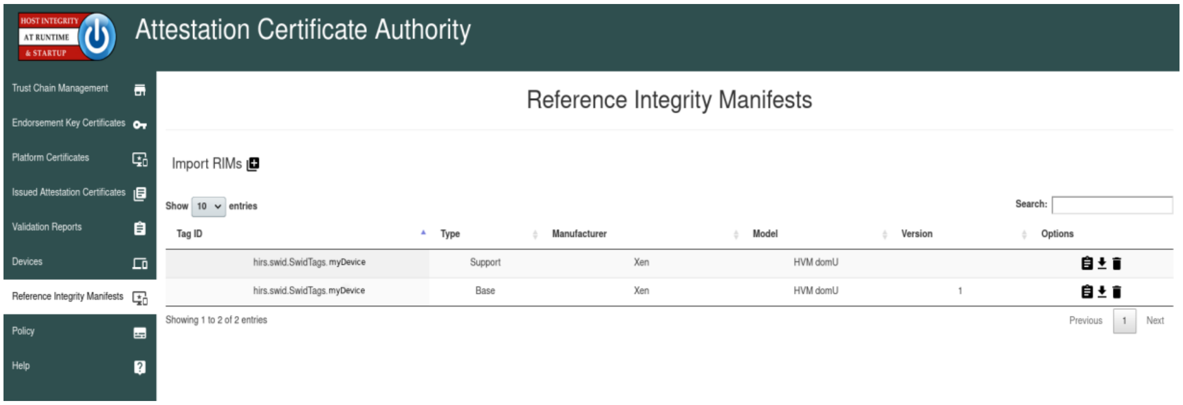

HOST INTEGRITY AT RUNTIME & STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Credentials
Platform Credentials
Unified Trust Credentials
Issued Attestation Certificates
Validation Reports
Devices
Policy
Help

Endorsement Certificate

Issuer	CN=STM TPM EK Intermediate CA 02,O=STMicroelectronics NV,C=CH
Serial Number	209028553673433939197939333733608380939277040569
Validity	Not Before: 2014-02-07 19:00:00 Not After: 2024-02-07 19:00:00
Signature	41: BD: 04: 39: 81: FF: 48: 85: 4C: 45: F1: 76: 2C: D2: CC: 81: A8: EC: AC: 7C: 22: E9: AC: 43: 23: E4: C7: 14: DB: E6: 63: 19: 38: 7A: D4: 01: CD: 87: BA: F3: 0F: D6: DB: 2A: 95: 06: 90: 8F: 52: F3: 93: 90: F6: D4: BA: 0F: 52: 90: 82: 50: 11: 8F: F6: 7F: AC: 0A: 42: 69: C0: D5: E3: B1: 9D: D5: 41: F3: 28: 7C: 34: 4E: 34: 0E: 14: 14: 53: 1A: 5A: 90: 3B: 19: 47: 5C: F0: 64: E3: D5: B9: 09: 3E: 7C: 97: 2B: 6C: 7D: 4F: 9B: 1F: AA: 47: 83: 20: D0: 50: D7: 1A: ED: 86: BD: 3A: 99: 0C: F8: 13: 7B: 7F: 7A: 72: F5: 6A: 98: D2: F9: 9D: 8E: 25: B0: 18: 27: 94: AB: E4: 80: 5F: 3E: B2: 50: 9F: 75: E8: 51: 69: 71: B0: 2A: 97: B6: 17: AD: 78: FD: 33: 87: 32: DF: 4B: 14: 99: 16: 38: B1: 20: E4: C0: AB: CA: FE: D8: 86: 91: 13: EA: 8A: 7C: 0A: FC: 1B: D4: 12: 4E: 74: 34: 8A: 2B: 4B: 69: B8: E1: F7: 42: D7: 1B: 13: C7: E1: 47: C5: 0D: 3B: 46: C5: A6: FE: 8D: 5B: 20: 70: AA: D8: EA: 71: 5F: 42: 99: 57: 33: 99: A8: 84: 18: F9: 99: DA: DF: 3D: 69: D3: 27: 90: 20: 00: 38: E0: 6A: 8A: 3A: BD: D2: 71: B6: 46: C2: 13: 97: FA: AB: 98
	30: 82: 01: 37: 30: 22: 06: 09: 2A: 86: 48: 86: F7: 0D: 01: 01: 07: 30: 15: A2: 13: 30: 11: 06: 09: 2A: 86: 48: 86: F7: 0D: 01: 01: 09: 04: 04: 54: 43: 50: 41: 03: 82: 01: 0F: 00: 30: 82: 01: 0A: 02: 82: 01: 01: 00: 99: 23: 76: 2B: B9: A6: 3C: 4D: ED: A4: 82: B1: A6: 75: B5: 5B: D7: CD: F2: 60: A0: E9: 67: B7: CD: 2D: 19: A1: 8B: 2D: DC: 1A:

Reference Integrity Manifests Page

The Reference Integrity Manifests page is used to upload, view, manage, and delete Reference Integrity Manifest files.


HOST INTEGRITY AT RUNTIME & STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help
Import RIMs
Search:
Previous
1
Next

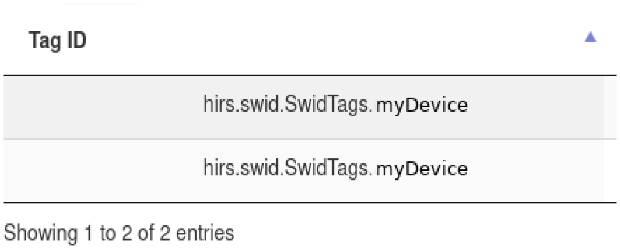
Reference Integrity Manifests

Show 10 entries

Tag ID	Type	Manufacturer	Model	Version	Options
hirs.swid.SwidTags.myDevice	Support	Xen	HVM domU		
hirs.swid.SwidTags.myDevice	Base	Xen	HVM domU	1	

Showing 1 to 2 of 2 entries

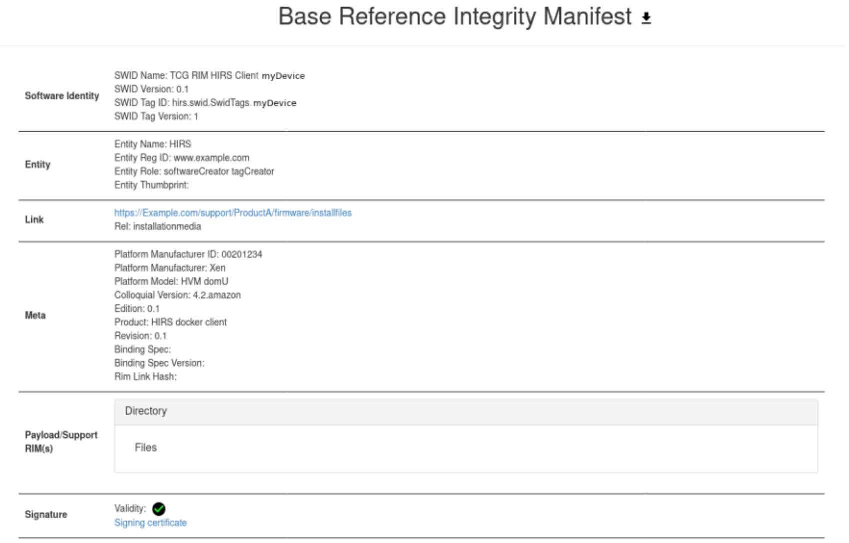
When a RIM file is uploaded to the ACA, both the Base and Support files (if there are any) appear within this section. To the left of Type, Manufacturer, Model, Version and Options, are SwidTag IDs. These are known as ”Software Identification Tags”.



Tag ID ▲
hirs.swid.SwidTags. myDevice
hirs.swid.SwidTags. myDevice

Showing 1 to 2 of 2 entries

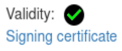
In order to view each RIM file, the 📋 icon must be clicked on. The Details page (this icon 📋) holds different information for both the Base and Support file(s). The Base RIM shows information defined by the SWID standard and other meta fields defined by the TCG:



Base Reference Integrity Manifest ⭳

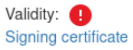
Software Identity	SWID Name: TCG RIM HIRS Client myDevice SWID Version: 0.1 SWID Tag ID: hirs.swid.SwidTags. myDevice SWID Tag Version: 1
Entity	Entity Name: HIRS Entity Reg ID: www.example.com Entity Role: softwareCreator tagCreator Entity Thumbprint:
Link	https://Example.com/support/ProductA/firmware/installfiles Rel: installationmedia
Meta	Platform Manufacturer ID: 00201234 Platform Manufacturer: Xen Platform Model: HVM domU Colloquial Version: 4.2.amazon Edition: 0.1 Product: HIRS docker client Revision: 0.1 Binding Spec: Binding Spec Version: Rim Link Hash:
Payload/Support RIM(s)	Directory Files
Signature	Validity: ✓ Signing certificate

It should be noted that when a RIM file's signature is validated, a green check mark will appear beside the Signature section within the Details page for the Base RIM:



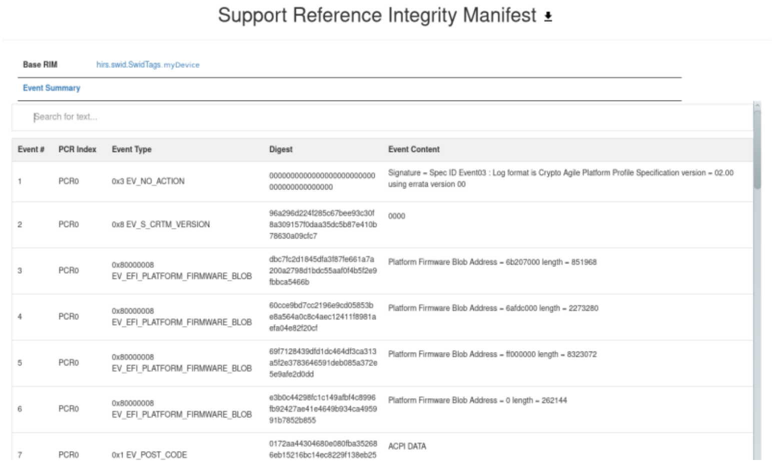
Validity: ✓
Signing certificate

However, if the signature on the RIM file does not validate or a certificate in the chain is missing, then a red exclamation mark will appear instead:



Validity: !
Signing certificate

The Support file(s) Details page contains information on all of the hashes that get extended into the TPM PCRs value during the boot cycle as well as an overall Event Summary section which lists what items the Support RIM file covers and which it does not. Should the TPM quote verification fail, this Details page will be needed to provide vital information on each PCR.



Support Reference Integrity Manifest ⭳

Base RIM hirs.swid.SwidTags.myDevice

Event Summary

Search for text...

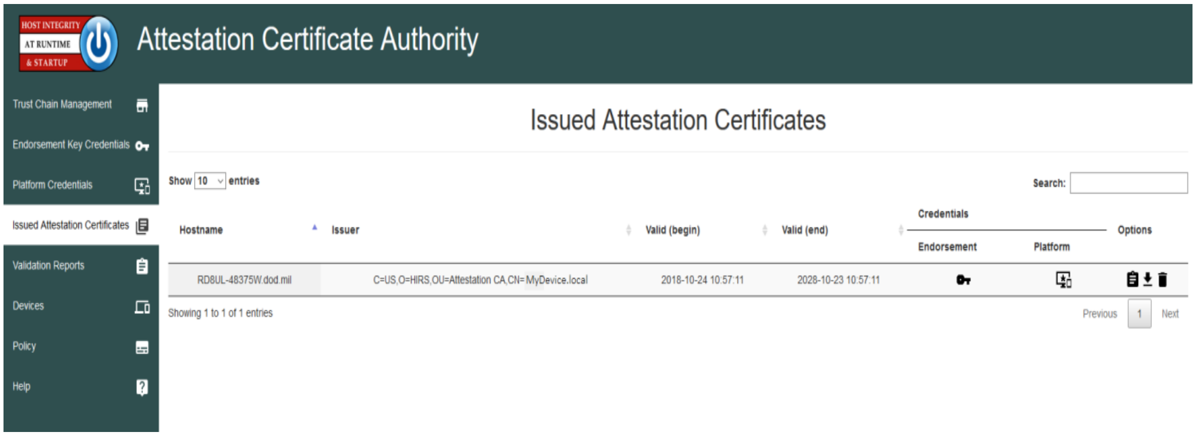
Event #	PCR Index	Event Type	Digest	Event Content
1	PCR0	0x3 EV_NO_ACTION	000000000000000000000000000000000000000	Signature = Spec ID Event03 : Log format is Crypto Agile Platform Profile Specification version = 02.00 using errata version 00
2	PCR0	0x8 EV_S_CRTM_VERSION	96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7	0000
3	PCR0	0x80000008 EV_EFI_PLATFORM_FIRMWARE_BLOB	dbc7fc2d1845dfa3f87fe661a7a200a2798d1bdc55aaf0f4b5f2e9fbbca5466b	Platform Firmware Blob Address = 6b207000 length = 851968
4	PCR0	0x80000008 EV_EFI_PLATFORM_FIRMWARE_BLOB	60cce9bd7cc2196e9cd05853be8a564a0c8c4aec12411f8981aefa04e82f20cf	Platform Firmware Blob Address = 6afdc000 length = 2273280
5	PCR0	0x80000008 EV_EFI_PLATFORM_FIRMWARE_BLOB	69f7128439dfd1dc464df3ca313a5f2e3783646591deb085a372e5e9afe2d0dd	Platform Firmware Blob Address = ff000000 length = 8323072
6	PCR0	0x80000008 EV_EFI_PLATFORM_FIRMWARE_BLOB	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	Platform Firmware Blob Address = 0 length = 262144
7	PCR0	0x1 EV_POST_CODE	0172aa44304680e080fba352686eb15216bc14ec8229f138eb25	ACPI DATA

HIRS ACA Status

ACA status is a collection of pages which report on activities performed by the ACA.

Issued Attestation Certificates Page

The Issued Attestation Certificates page provides access to the Attestation Certificates issued by the ACA. Note that there can be multiple Attestation Certificates if the TPM provisioning process is run multiple times.



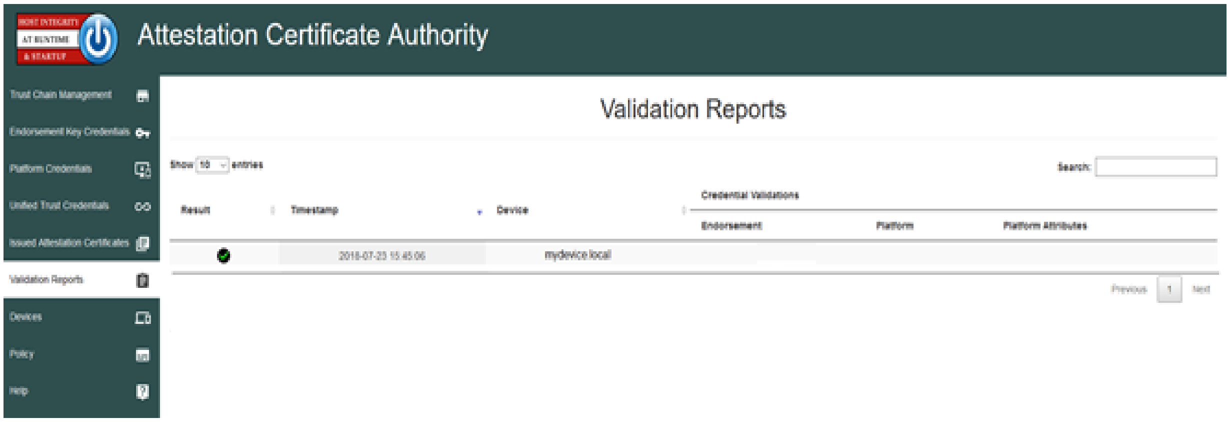
Issued Attestation Certificates

Hostname	Issuer	Valid (begin)	Valid (end)	Credentials		Options
				Endorsement	Platform	
RD8UL-48375W.dod.mil	C=US,O=HIRS,OU=Attestation CA,CN=MyDevice.local	2018-10-24 10:57:11	2028-10-23 10:57:11	🔑	🖥	📋 ⬇ 🗑

Showing 1 to 1 of 1 entries

Validation Reports Page

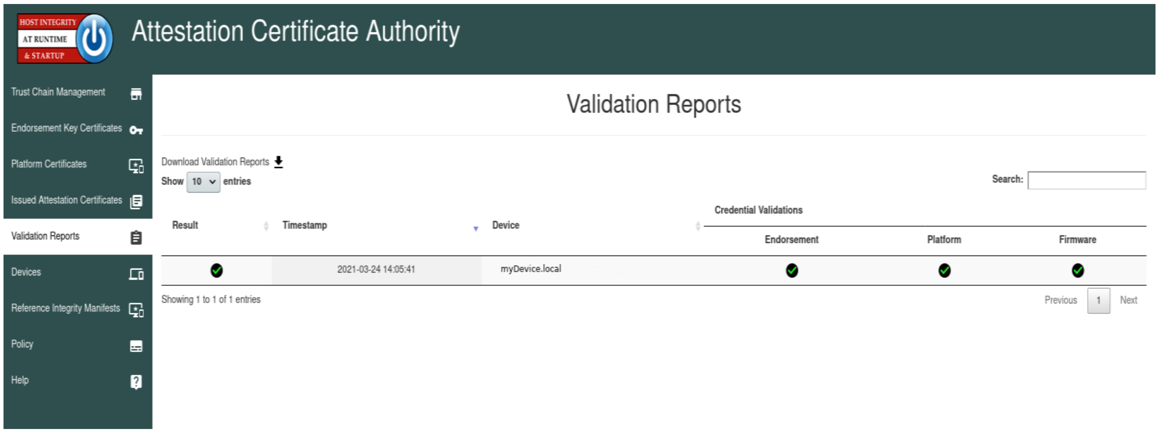
The Validation Reports page indicates the status of previous Attestation CertificateRequests from HIRS TPM Provisioners.



Validation Reports

Result	Timestamp	Device	Credential Validations		
			Endorsement	Platform	Platform Attributes
✓	2018-07-23 15:45:06	mydevice.local			

The Certificate validation columns are only populated if the ACA policy was set to include the particular validation at the time the request was made. The above indicates that the default policy was used and that no validation of the EK or Platform Credentials was performed. The screenshot below indicates the recommended report policy for supply chain validation:


HOST INTEGRITY
AT RUNTIME
& STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help

Validation Reports

Download Validation Reports

Show 10 entries

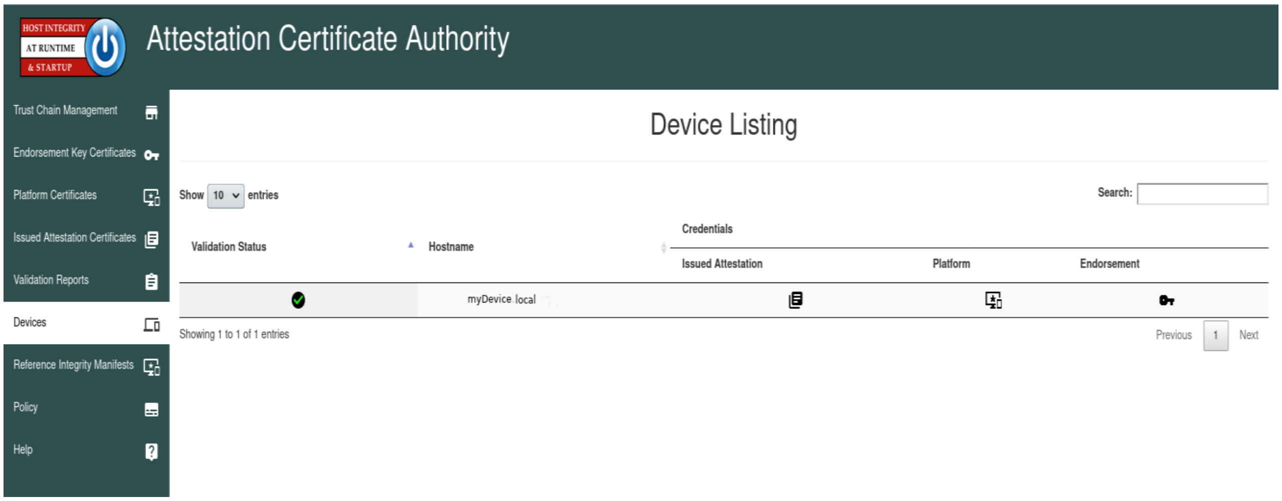
Search:

Result	Timestamp	Device	Credential Validations		
			Endorsement	Platform	Firmware
✓	2021-03-24 14:05:41	myDevice.local	✓	✓	✓

Showing 1 to 1 of 1 entries

Devices Page

The devices page is similar to the reports page but only shows one row per device, thus allowing for easier access to a particular device's status. As with the validation page, the credentials associated with the device are dictated by the ACA policy during the latest validation report.


HOST INTEGRITY
AT RUNTIME
& STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help

Device Listing

Show 10 entries

Search:

Validation Status	Hostname	Credentials		
		Issued Attestation	Platform	Endorsement
✓	myDevice.local	🗎	🖥	🔑

Showing 1 to 1 of 1 entries

HIRS Provisioner

HIRS provides a TPM 2.0-compliant Provisioner, which consists of an application for handling the specialized process of provisioning a client's TPM and performing other client-side actions required for supply chain validation. The Provisioner is run on the client computer. As part of the actions required, the Provisioner attempts to gather artifacts that reside in the TPM and are required for validation processing with an ACA. The following steps will need to be performed prior to provisioning the TPM with HIRS:

- TPM is enabled in the UEFI/BIOS (typically enabled by default)
- TPM is activated in the UEFI/BIOS (typically activated by default)
    - ○

The HIRS Provisioner application, along with the HIRS ACA, will perform the following high-level tasks during the provision process. Please refer to appendix B for further details:

- .
- The HIRS Provisioner retrieves the EK Certificate from the TPM's NVRAM.
- The HIRS Provisioner retrieves the Platform Certificates and / or RIM Bundle from the EFI partition, if present.
- The HIRS Provisioner retrieves the TCG Event Log.
- The HIRS Provisioner retrieves component data from the device (see appendix B).
- A Local Attestation Key (LAK) is generated on the TPM, if one is not already present.
- The HIRS Provisioner creates an AK Certificate request, which includes the above artifacts and data, and forwards it to the ACA.
- The HIRS ACA stores the artifacts and data in the ACA database.
- The HIRS ACA (policy based) validates the Endorsement Credential.
- The HIRS ACA (policy based) validates the Platform Credential(s).
- The HIRS ACA (policy based) validates any new RIMs.
- The HIRS ACA performs Certificate validation according to its policy.
- If validation is successful, the ACA issues an AK Certificate or LocalDevID Certificate (policy based) to the device.

Ideally the TPM provisioning tasks would be performed in a controlled environment, prior to the installation of any software to the computer. This could be done with a bootable peripheral device or PXE boot, and should be done in a read-only mode from trusted software.

Provisioner Commands

The HIRS Provisioner has a command line interface that provides a simple process for provisioning the TPM. The first step is to configure the connection between the Provisioner and the ACA.

Step 1. Edit teh appsetting.json file:

```
"auto_detect_tpm":  "TRUE",
  "aca_address_port": "https://127.0.0.1:8443",
  "efi_prefix": "/boot/efi",
  "certificate_output_directory": "/home/lareine/test2",
  "paccor_output_file": "",
  "event_log_file":  "",
  "hardware_manifest_collectors": "paccor_scripts",
```

Note efi_prefix is OS dependent (linus path shown). Windows does not expose it efi partition so it will need to be mounted first. Refer to Microsoft documentation for instructions on how to mount the efi partition.

Step 2: Provision the TPM

Once the hirs-site.config file is filled in, the TPM provisioning can be run as a command on the client:

```
> sudo tpm_aca_provision
```

This command will perform the high-level tasks listed in the previous section.

EK certificates from TPMs

As part of the provisioning process of taking ownership of a TPM, the Provisioner will send the TPM's EK Certificate to the ACA, where it will be stored in the ACA database. During validation, the ACA will need to validate this EK Certificate using one or more of the trust chain certificates to ensure that the certificate is from a trusted TPM manufacturer.

Provisioning Data Collected

As part of the provisioning process, the Provisioner will also gather and send device details of the target device to the ACA. During validation, the ACA checks its policy and uses device details to check against the Platform Credential(s).

Currently device manufacturer, model, and serial numbers are collected during the provisioning process from the following devices:

- System
- BIOS
- Baseboard (Motherboard)
- Chassis
- Storage devices
- Memory devices
- Network Cards

- Additional information regarding various physical device components is also collected. (For more information, see “Recommended Policy Setting for Trusted Computing Based Supply Chain Validation” for a current listing of component information to be collected.)

Appendix A: Build, Installation, and Setup Guidance

The HIRS GitHub wiki has specific instructions for installation, configuration, and first-time use of the ACA and TPM Provisioner. The specific wiki pages are:

- Overview https://github.com/nsacyber/HIRS/wiki/
- Getting Started Guide https://github.com/nsacyber/HIRS/wiki/Gettingstarted
- Installation Notes https://github.com/nsacyber/HIRS/wiki/installation_notes
- HIRS Build Guide https://github.com/nsacyber/HIRS/wiki/Hirs-build-guide

The Getting Started Guide is the recommended starting point for installing, running, configuring, and creating test patterns for HIRS.

Appendix B: TPM Provisioning Details

Provisioning Overview

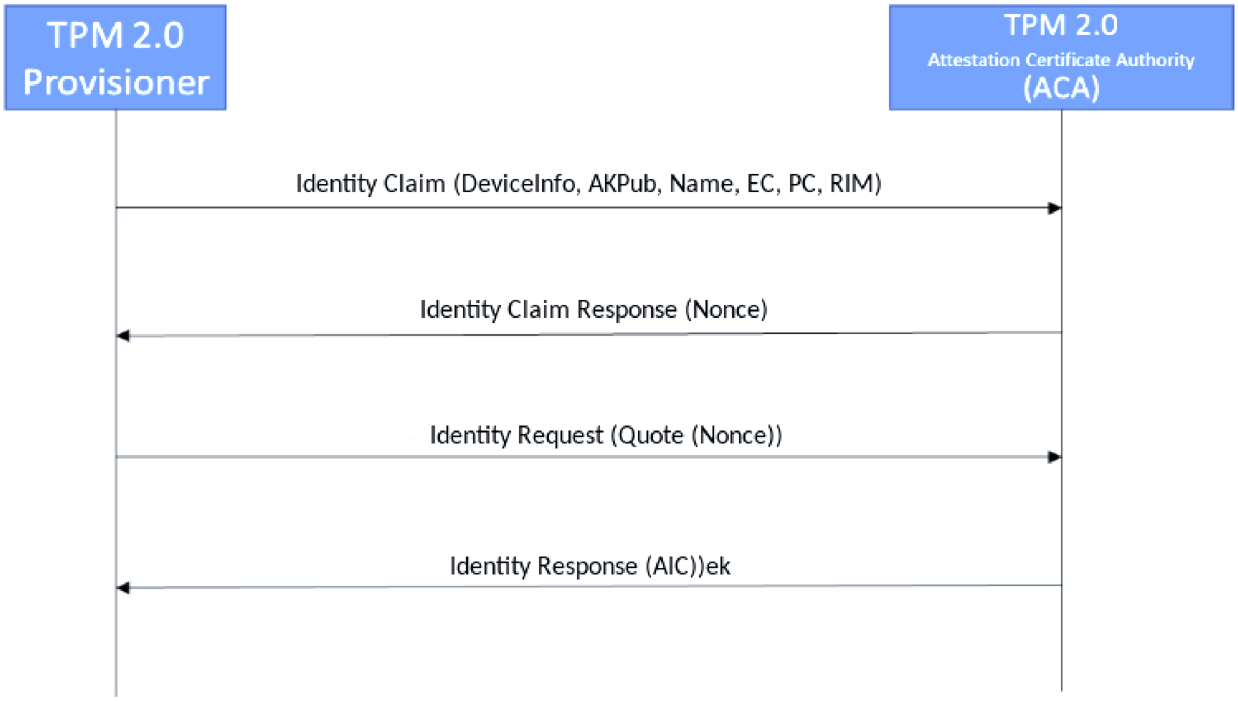
HIRS implements a 2-pass procedure for provisioning to incorporate:

Pass 1:

A. An Identity Claim from the device requesting the AK Certificate.
B. An Identity Claim Response from the ACA.

Pass 2:

A. An Identity Request from the device, which contains a signed challenge to bind the TPM to the EK and LAK as well as information about the device, including the EK and Platform Certificates.
B. An Identity Response from the ACA, which contains the AK Certificate if the Identity Request information validates.


TPM 2.0
Provisioner
TPM 2.0
Attestation Certificate Authority
(ACA)
Identity Claim (DeviceInfo, AKPub, Name, EC, PC, RIM)
Identity Claim Response (Nonce)
Identity Request (Quote (Nonce))
Identity Response (AIC))ek

IdentityClaim (DeviceInfo, AKpub, Name, EC, PC, RIM): The Provisioner collects information about the device (serial numbers, TPM info, firmware info, OS info, network info, etc.), the Endorsement Credential, the Platform Credential, and a RIM Bundle and current TCG Event Log. The Provisioner also requests a LAK or LDevID key to be made by the TPM, and the TPM gives the Provisioner the LAK public key. The Provisioner sends a request for an Attestation Certificate from the ACA, and includes the gathered info in its request.

IdentityClaimResponse (Nonce): The ACA does a preliminary check on the provided info. As part of this check, the ACA validates the EK and Platform Certificates and certificate chains. Note that the Certificate checking is dependent upon the ACA policy settings. If the check fails, the ACA will go no further and send a failed response. If the check passes, the ACA creates a request for a Quote and includes a challenge (nonce) in the request. The ACA encrypts this request with the LAK public key that it received from the Provisioner during the Identity Claim. The ACA sends this encrypted response (the “encrypted blob”) to the Provisioner. The encryption proves that the TPM holds the private key of the LAK.

IdentityRequest (Quote (Nonce)): The Provisioner decrypts the request (the “encrypted blob”) from the ACA. The Provisioner retrieves the nonce. The Provisioner requests a Quote from the TPM, along with the nonce (from the ACA) and a PCR mask. The TPM generates this Quote and signs it with the private key of the LAK. Quote includes a signed (single) composite hash of all PCRs using the PCR mask register. The Provisioner sends this TPM Quote to the ACA. The fact that the Provisioner was able to decrypt the ACA’s “encrypted blob” and retrieve the nonce proves that the TPM holds the private key associated with the LAK public key. The fact that the Provisioner returns the nonce also proves that this is a current message and not a replay attack.

(IdentityResponse (AC)) ak: The ACA processes all the information provided by the Provisioner. If verification is successful, the ACA generates an AC, encrypts this response using the public key of the LAK provided by the Provisioner in the Identity Claim, and sends the encrypted response back to the Provisioner. The Provisioner decryptes the AC and “activates” the certificate.

Provisioning Additional Details

The TPM 2.0 (a software interface to the TPM) defines two functions that directly relate to the ACA for requesting an Attestation Certificate (AC):

- TPM2_makecredential: This function performs the actions required of a Certificate Authority in creating an object containing an activation credential.
- TPM2_activatecredential: This function enables the association of a Certificate with another object in a way that ensures that the TPM has validated the parameters of the Certificate object.

The ACA performs the TPM2_makeCertificate process. What it needs for the process is:

- The public EK. t.
- The AK "name." This can be generated using the public AK.

The specific processes that the ACA and TPM 2.0 Provisioner perform to send the nonce and create to the provisioner include:

- ACA generates a nonce (random challenge) used to check the binding private key to the public AK.
- ACA generates a random AES key and IV, and use these to encrypt the nonce.
- ACA generates a random 32 byte value that we will use as a "seed."
- ACA encrypts this seed using the public EK retrieved from the EK cert.
- ACA uses a key derivation function (KDF - as specified in the TPM 2.0 specs) to generate another AES key.
- ACA uses this new AES key to encrypt the first AES key.
- ACA uses the KDF again, with different parameters to generate an HMAC secret.
- ACA wraps the encrypted AES key with some other relevant bits using the HMAC key.

- Returns the HMACed, symmetrically-encrypted blob, the asymmetrically-encrypted blob, and the symmetrically encrypted chunk of data to the client.
- The client will use this blob as an input parameter for the tpm2_activateCertificateto get the key that can be used to decrypt the original chunk. If that chunk is the AK cert, then you're done. If it's a nonce, then it should be returned to the CA as proof to go forward with the generation of the certificate.

Appendix C: References

[1] Trusted Computing Group. (2024). *Trusted Computing Group*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org

[2] *Platform Attribute Certificate Creator (paccor)*. (2024, February 18). Retrieved from GitHub: https://github.com/nsacyber/paccor

[3] Trusted Computing Group. (2023, March 15). *TCG EK Certificate Profile for TPM Family 2.0*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/resource/tcg-ek-credential-profile-for-tpm-family-2-0/

[4] Trusted Computing Group. (2023, December 4). *TCG Platform Certificate Profile*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/

[5] Trusted Computing Group. (2024 April 26). *TCG PC Client Reference Integrity Manifest Specification*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/resource/tcg-pc-client-reference-integrity-manifest-specification/

[6] Trusted Computing Group. (2020, July 23). *TCG EK Credential Profile For TPM Family 2.0; Level 0*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/wp-content/uploads/TCG_IWG_EKCredentialProfile_v2p3_r2_pub.pdf

[7] Trusted Computing Group. (2024 April 26). *TCG Reference Integrity Manifest (RIM) Information Model*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1p01_r0p16_pub.pdf

[8] Trusted Computing Group. (2023, December 4). *TCG PC Client Platform Firmware Integrity Measurement*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client-FIM_v1r24_3feb20.pdf

[9] The tcg_rim_tool . Retrieved from https://github.com/nsacyber/HIRS/tree/main/tools/tcg_rim_tool