



Host Integrity at Startup and Runtime (HIRS)

**Attestation Certificate Authority (ACA)
Portal and Trusted Platform Module (TPM)
Provisioner**

10 April 2021

Users Guide

Version 2.1

Table of Contents

Introduction	1
Background	1
Trusted Computing based Supply Chain Validation Concepts	1
Reference Integrity Manifests	2
Vendor Certificate Chains	4
TPM Provisioning	4
HIRS Attestation Certificate Authority.....	4
HIRS ACA Web Portal	6
ACA Configuration	7
ACA Policy Page	7
Trust Chain Management page	10
The Platform Certificates (PC) page.....	11
Platform Certificate Holder field	11
Platform ID	11
Platform Certificate Component fields.....	11
The Endorsement Certificates (EC) Page	12
<i>Reference Integrity Manifests</i>	13
ACA Status.....	15
Issued Attestation Certificates page.....	15
Validation Reports page	15
Devices page	16
HIRS Provisioner.....	17
Provisioner commands	17
Step 1. Create and populate a hirs_site.config file.....	17
Step 2: Provision the TPM.....	18
EK certificates from TPMs.....	18
Provisioning Data Collected	19
Appendix A: Build, Installation, and Setup Guidance	20
Appendix B: TPM Provisioning Details.....	21
TPM 1.2 Provisioning	22

TPM 2.0 Provisioning24

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) to include TPM provisioning, Endorsement Credential (EC) validation, Platform Credential (PC) validation, Attestation Identity Credential (AIC) 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.

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 which include processes for performing Supply Chain Validation. 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.

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 certificates as defined in the TCG's Credential Profiles Specification(s)⁶.

¹<https://trustedcomputinggroup.org>

²<https://github.com/nsacyber/paccor>

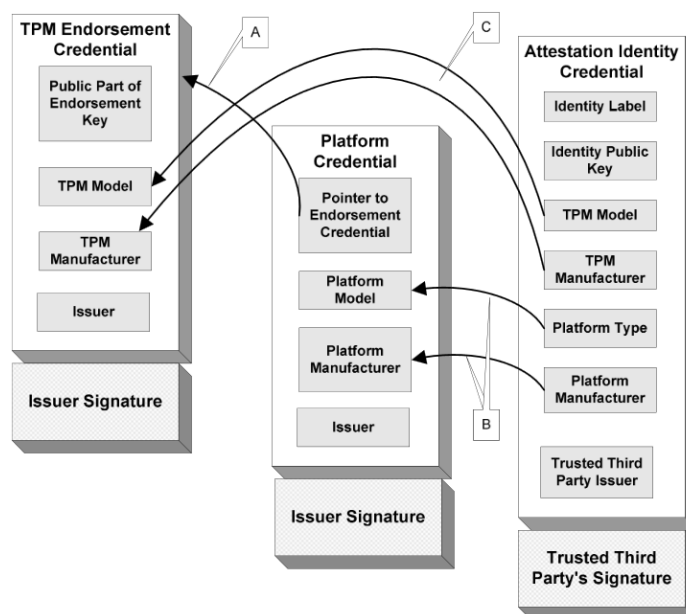
³<https://trustedcomputinggroup.org/resource/tcg-ek-credential-profile-for-tpm-family-2-0/>

⁴<https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/>

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

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

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

Reference Integrity Manifests

The Reference Integrity Information Model⁷ 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”.

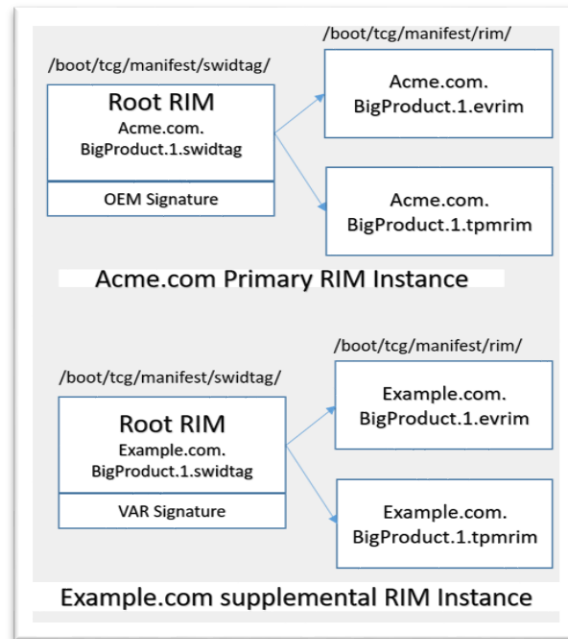
⁷ https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1p01_r0p16_pub.pdf

⁸ https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_RIM_r0p15_15june2020.pdf

The PC Client RIM defines the Base Rim as a ISO 19770-2 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 TPM Log created during the boot process. The TPM log defined by the TCG PC Client Platform Firmware Profile captures⁹ all events that extend any of the TPMs Platform Configuration Register (PCR) contents. The OEM that creates the RIM captures the 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).



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

⁹ https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client-FIM_v1r24_3feb20.pdf

Validating the Supply Chain sources using TCG Credentials

TCG compliant devices that conform to a valid supply chain must undergo acceptance/confirmation prior to initializing/provisioning/setup of the device. The credentials for these tests should be stored within the TPM's NVRAM (HIRS has support for reading the credentials 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.

Vendor Certificate Chains

Each artifact has a signature used for validation. In order to validate the credential each vendor must supply a set of intermediate and root CA certificates (the "certificate chain") that are stored by the ACA application that wishes to validate the signatures. Some vendors may post the chain to a website while others may send the chain directly to the customer.

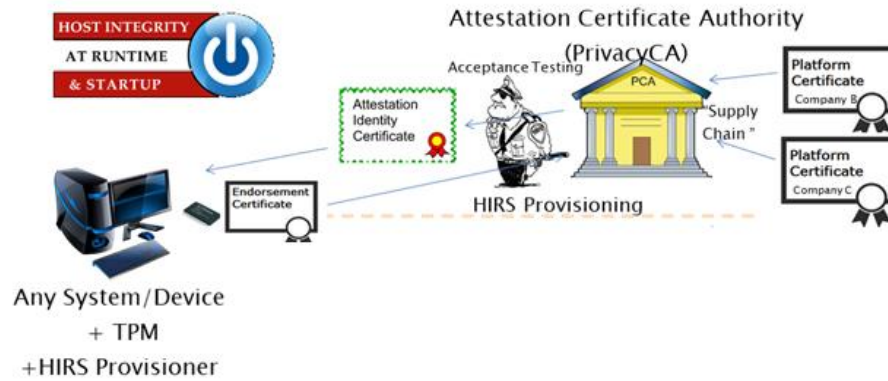
Vendors that post their certificate chain to their website will typically do so on web accessible URLs. This certificate chain can require several certificates (e.g. Root CA certificates, intermediate CA certificates, etc.). Refer to the TPM manufacturer's web site for the exact location of their certificate 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 Identity Credential (AIC) 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 Identity Keys (AIK), used by TPMs to sign quotes. It issues an Attestation Identity Certificate (AIC) 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 Certificate Authority. 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:


https://hostname:8443/HIRS_AttestationCAPortal/

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.




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 insure the certificate can be used appropriately.

The  icon under the option column will download the certificate to your local device. A file selection 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.

HOST INTEGRITY

AT RUNTIME

& STARTUP

Attestation Certificate Authority

Trust Chain Management
Endorsement Key Credentials
Platform Credentials
Issued Attestation Certificates
Validation Reports
Devices
Policy
Help

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 A0 0C 1F DC 13 55 32 71 6E A1 D2 4A 6F C8 A8 61 99 82 B0 BE C2 0F 44 43 71 19 31 7C BC FB C5 6B 12 95 87 4C 94 EB E5 1E B1 54 BA ED 12 EC BA 26 78 A5 4F 03 7D 91 0D 34 67 AD 8F 58 F7 67 FF F4 BF 4C 85 DF 87 61 41 D8 25 CF 02 F5 75 41 78 57 2F 62 9B BE A9 92 6A 66 F9 F9 36 F3 2F 08 B3 C5 CC 98 F7 F7 6D 26 A6 E6 36 B4 F4 44 6C D9 71 5A 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 6D 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.

ACA Configuration

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

ACA Policy Page

A HIRS ACA Policy provides configuration setting 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:

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

Attestation Identity CA Policy Options

- Endorsement Credential Validation: Enabled
- Platform Credential Validation: Enabled
 - Platform Attribute Credential Validation: Enabled
- Firmware Validation: Enabled
 - Ignore IMA PCR Entry: Disabled
 - Ignore TBOOT PCRs Entry: Disabled
- Generate Attestation Certificate: Enabled
 - Attestation Certificate Validity period: Disabled
 - Attestation Certificate Renewal period: Disabled

Endorsement Credential Validation: If selected, the ACA will require that the ACA validate the Endorsement Credential prior to issuing an Attestation Credential. The Default is disabled.

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

Platform Attribute Credential Validation: If selected, the ACA will require that the ACA validate the Platform Credential Attributes prior to issuing an Attestation Credential. This option only validates the credential attributes, not the platform credential. Platform Credential 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.

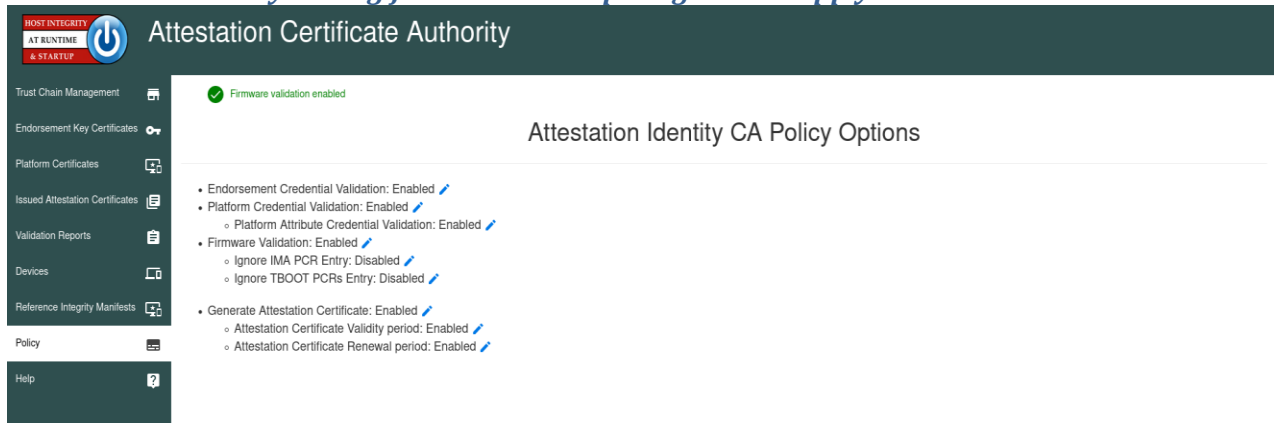
Ignore TBOOT PCRs Entry: If selected, the ACA will require that the ACA ignores the TBOOT PCRs Entry prior to issuing an Attestation Credential. Firmware Validation is required to be enabled prior to enabling this policy option.

Generate Attestation Certificate: If selected, the ACA will require that the ACA will conditionally generate an Attestation Certificate before the 'Not After' expiration date.

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.

Recommended Policy Setting for Trusted Computing Based Supply Chain Validation



The recommended policy setting for Trusted Computing based Supply Chain Validation will require these policy settings to be set to true:

- **Endorsement Credential Validation: Enabled**
- **Platform Credential Validation: Enabled**
- **Platform Attribute Credential 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+. electing this option will cause the ACA to skip evaluation of PCR17+.
- **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 TPM 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.

Attestation Certificate Authority

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=Navotek Technology Corporation+C=TW	CN=NTC TPM EK Root CA 01+O=Navotek Technology Corporation+C=TW	2012-07-11 12:29:30	2032-07-11 12:29:30	
CN=Navotek TPM Root CA 2010+O=Navotek Technology Corporation+C=TW	CN=Navotek TPM Root CA 2010+O=Navotek 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 (KGF_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

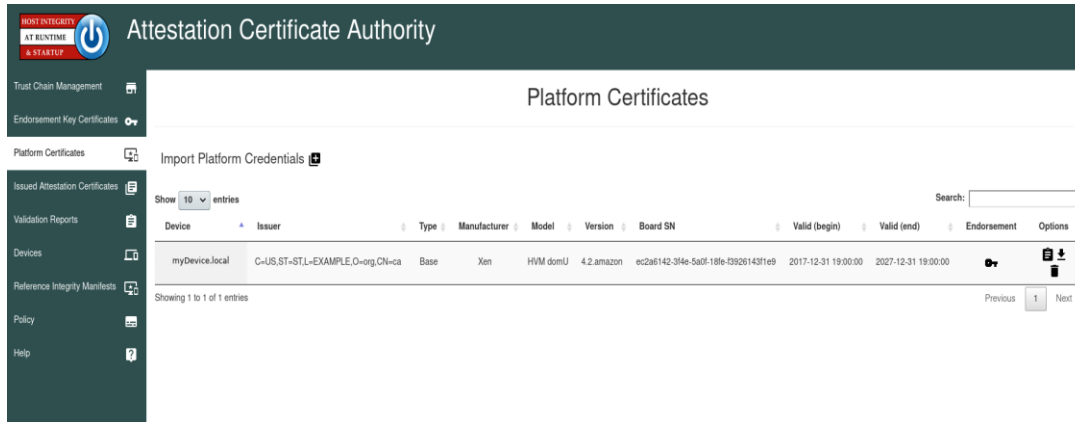
By default the ACA generates a self-signed certificate that is used as the root CA for signing all issued Attestation Certificates. An Attestation CA certificate may be signed by a Root CA and replaced (the ACA certificate would become a subordinate to the Root CA. In either case, the CA certificate 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 certificate. This certificate 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 icons selections on the page.

The Platform Certificates (PC) page

The Platform Certificates page is used to upload, download, delete, and view platform Credentials.



Viewing the individual Platform Credential 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:

Platform Certificate Holder field

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
--------	--

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.

Platform ID

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

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

Platform Certificate Component fields

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/CN722004401A5/
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

The Endorsement Certificates (EC) Page

The Endorsement Certificates (EC) asserts that the holder of the private EK is a TPM conforming to TCG specifications. Since the EK Credential 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.

Attestation Certificate Authority

Trust Chain Management

Endorsement Key Certificates

Platform Certificates

Issued Attestation Certificates

Validation Reports

Devices

Reference Integrity Manifests

Policy

Help

Endorsement Key Credentials

Import Endorsement Key Credentials

Show 10 entries

Search:

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

Previous 1 Next

The Endorsement Key Credential 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 Specification	Family: '1.2' Level: 2 Revision: 3
TPM Security Assertion	Version: 1 Field Upgradeable: true ek Generation Type: INJECTED ek Generation Location: TPM_MANUFACTURER ek Certificate Generation Location: TPM_MANUFACTURER

The Endorsement Key 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 EC credential. For further information refer to the TCG Credential Profile specification.

Attestation Certificate Authority

Trust Chain Management

Endorsement Key Certificates

Platform Certificates

Unified Trust Credentials

Issued Attestation Certificates

Validation Reports

Devices

Policy

Help

Endorsement Certificate

Issuer: CN=STM TPM EK Intermediate CA,O=STMicroelectronics NV,C=CH

Serial Number: 20902855367343393919793933733608380939277040569

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 90 D5 41 F3 28 7C 34 4E 34 0E 14 14 53 1A 5A 90 38 19 47 5C F0 64 E3 D5 89 09 3E 7C 97 2B 6C 7D 4F 98 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 3A 8A 28 48 69 B8 E1 F7 42 D7 1B 13 C7 E1 47 C5 00 38 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 A8 98 30 82 01 37 30 22 06 09 2A 86 48 B6 F7 0D 01 01 07 30 15 A2 13 30 11 06 09 2A 86 48 B6 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

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

Attestation Certificate Authority

Reference Integrity Manifests

Import RIMs

Show 10 entries

Search:

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

Previous 1 Next

When a RIM file is uploaded to the ACA, both the Base and Support files (if there are any) appear within this section.

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

Showing 1 to 2 of 2 entries

To the left of Type, Manufacturer, Model, Version and Options, are **SwidTag IDs**. These are known as "Software Identification Tags".

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.

The screenshot shows the 'Issued Attestation Certificates' page. The left sidebar contains navigation links: Trust Chain Management, Endorsement Key Credentials, Platform Credentials, Issued Attestation Certificates (selected), Validation Reports, Devices, Policy, and Help. The main content area has a title 'Issued Attestation Certificates' and a search bar. Below the search bar is a table with columns: Hostname, Issuer, Valid (begin), Valid (end), Credentials, Endorsement, Platform, and Options. A single entry is shown for Hostname 'RD8UL-48375W.dod.mil' and Issuer 'C=US,O=HIRS,OU=Attestation CA,CN=MyDevice.local'. The table shows the certificate is valid from 2018-10-24 10:57:11 to 2028-10-23 10:57:11. The bottom of the table indicates 'Showing 1 to 1 of 1 entries' and includes 'Previous' and 'Next' navigation buttons.

Hostname	Issuer	Valid (begin)	Valid (end)	Credentials	Endorsement	Platform	Options
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				

Validation Reports page

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

The screenshot shows the 'Validation Reports' page. The left sidebar is the same as the previous page, with 'Validation Reports' now selected. The main content area has a title 'Validation Reports' and a search bar. Below the search bar is a table with columns: Result, Timestamp, Device, Credential Validations, Endorsement, Platform, and Platform Attributes. A single entry is shown with a green checkmark in the Result column, a timestamp of 2018-07-23 15:45:06, and a device of 'mydevice.local'. The bottom of the table indicates 'Showing 1 to 1 of 1 entries' and includes 'Previous' and 'Next' navigation buttons.

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

The Credential 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:

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

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.

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

HIRS Provisioner

HIRS has a set of small client applications used for handling the specialized process of provisioning a TPM and performing general Supply Chain Validation with an ACA. HIRS provides TPM 1.2-compliant provisioner and another that is TPM 2.0-compliant. The provisioners will attempt to read both Endorsement Credentials and Platform credential from the TPM's NVRAM. In general, the TPM Provisioners perform the following operations.

The following steps will need to be performed prior to provisioning the TPM with HIRS:

- TPM is enabled in the UEFI/BIOS
- TPM is activated in the UEFI/BIOS
 - If TPM was previously owned, TPM is cleared, then activated again

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 TPM Provisioner takes Ownership of the TPM (TPM 1.2).
- The TPM Provisioner Retrieves the EK Certificate from the TPMs NVRAM.
- The TPM Provisioner Retrieves the Platform Certificate from the TPMs NVRAM.
- The TPM Provisioner Retrieves Component data from the device (see appendix B).
- An Attestation Identity Key is generated on the TPM, if one is not already present.
- The TPM Provisioner Creates an AIK certificate request and forwards it to the ACA.
- The ACA Optionally (Policy based) validates the Endorsement Credential.
- The ACA Optionally (Policy based) validates the Platform Credential(s).
- The performs credential validation according to its policy
- If validation is successful, the ACA issues an Attestation Identity Credential 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 CD 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 which includes the AIC ordering from the privacy CA. Trust store is established during this process even if the client does not support a TPM.

Step 1. Create and populate a `hirs_site.config` file:

For a device with TPM 1.2

```
> sudo hirs_provisioner config
```

For a device with TPM 2.0

```
> sudo hirs-provisioner-tpm2 -c
```

These commands set up the `hirs-site.config` file in the `/etc/hirs` directory (Linux). You will need to edit this file before continuing. Specifically the `Attestation_CA_FQDN` needs to be filled in. It also creates an entry for `CLIENT_HOSTNAME` and assigns the current hostname to it. This can be modified by the system before the provisioning process is the FQDN is not set up by the system. For example, edit the `/etc/hirs/hirs-site.config`

```
#*****
#* HIRS site configuration properties file
#*****
# Client configuration
TPM_ENABLED=true
IMA_ENABLED=false
CLIENT_HOSTNAME=$HOSTNAME
# Site-specific configuration
ATTESTATION_CA_FQDN=<aca_fqdn>
ATTESTATION_CA_PORT=8443
```

Step 2: Provision the TPM

Once the `hirs-site.config` file is filled in the TPM provisioning can be command on the client (works for TPM 1.2 or TPM 2.0 clients):

```
> sudo tpm_aca_provision
```

This command will take ownership of the TPM (If it is not already), create an Attestation Identity Key, and order the AIC Certificate from the Privacy CA.

These commands only need to be performed once per device. Refer to the HIRS installation guide (Please refer to appendix A) for further details on the `hirs-site.config` file and the procedure for ordering Attestation Certificates.

EK certificates from TPMs

As part of the provisioning process of taking ownership of a TPM, the TPM's EK certificate will be sent to and stored in the ACA database. The Attestation CA will need to validate this EK certificate using one or more of the Trust Chain certificates to ensure that the request is from a trusted TPM manufacturer.

Provisioning Data Collected

Device details of the target device such as the operating system, TPM specs, and networking addresses are useful for provisioning. The HIRS provisioning process first sends the details of the device and requests an Attestation Identity Credential. The ACA checks its policy and uses device details to check against the Endorsement and Platform credentials for validation.

Currently the following information is collected during the provisioning process:

- Device hostname : Fully Qualified Host Name (FQDN)
- IP Address(es)
- MAC Address(es)
- System Manufacturer
- System Product Name
- Product Version
- System Serial Number
- TPM Manufacturer
- TPM Version
- Operating System
- Kernel
- BIOS Vendor
- BIOS Version
- BIOS Release Date
- HIRS Provisioner Version

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 Provisioners. The specific wiki pages are:

- Overview <https://github.com/nsacyber/HIRS/wiki/>
- Installation notes https://github.com/nsacyber/HIRS/wiki/installation_notes
- HIRS build guide <https://github.com/nsacyber/HIRS/wiki/Hirs-build-guide>
- Getting started guide <https://github.com/nsacyber/HIRS/wiki/Gettingstarted>

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

If attempting to provision a device running an operating system that's not officially supported by the HIRS TPM 2.0 provisioner, e.g. Ubuntu, please consult the wiki page on installing a custom TPM 2.0 software stack that works for the target runtime environment before building and/or installing the TPM 2.0 provisioner. It can be found here: https://github.com/nsacyber/HIRS/wiki/custom_TPM2SoftwareStack

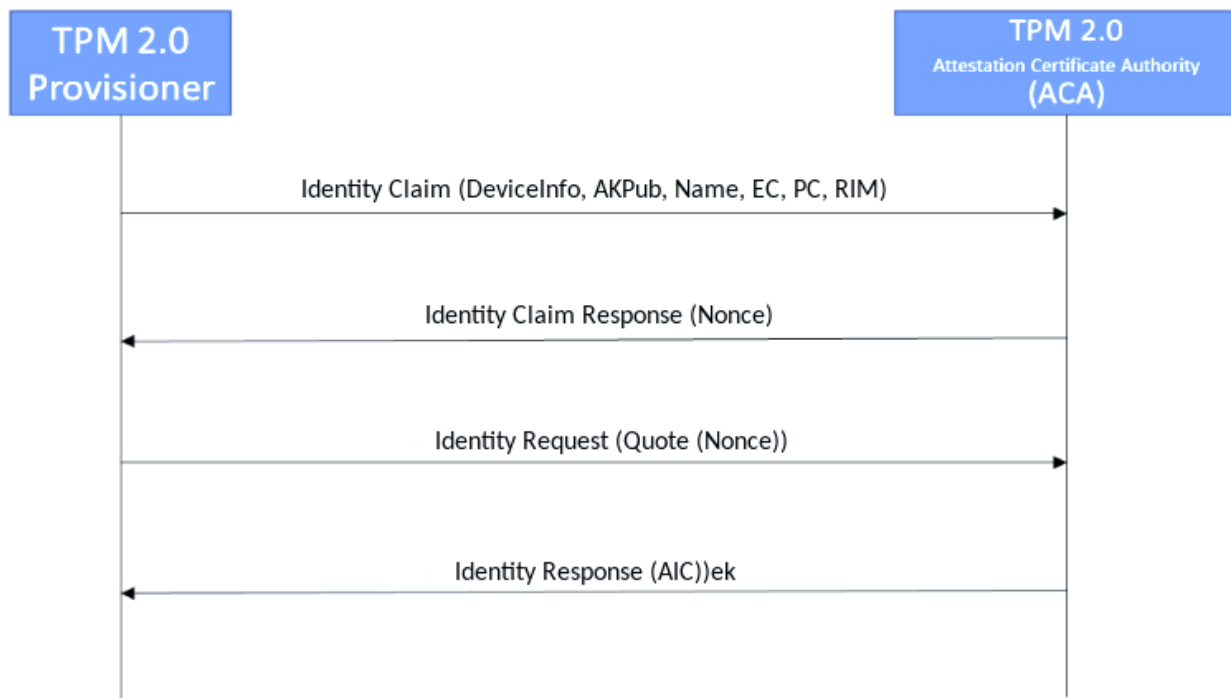
Appendix B: TPM Provisioning Details

The general protocol for provisioning either TPM 1.2 or TPM 2.0 is the same. HIRS implements a 2 pass procedure for provisioning to incorporate:

An Identity Claim from the device requesting the AIC.

An Identity Request which contains a signed challenge to bind the TPM to the EK and AIK as well as information about the device, including the EK and Platform Certs.

An Identity Response which contains the Attestation Certificate if the Identity Request information validates.



IdentityClaim (DeviceInfo, AKpub, Name, EC, PC, RIM): The Identity claim has information presented by the provisioner which includes information collected from the device (Serial Numbers, TPM info, Firmware info, OS info, Network Info, etc.). This also includes the Attestation public key, a ticket which verifies the AK key usage, the Endorsement Credential (EC), the Platform credential (PC), a RIM Bundle, and a TPM Quote, which includes the nonce from the Identity Claim response and a signature using the TPM's Attestation Key.

IdentityClaimResponse (Nonce) : The ACA does a preliminary check on the provided info and returns a challenge (nonce) if it finds the claimed identity message acceptable.

IdentityRequest (Quote (nonce)): The provisioner assembles a set of information to present as part of a request for an Attestation Identity Credential to the ACA.

(IdentityResponse (AIC)) ek: The ACA processes all the information provided by the Provisioner. If acceptable the ACA generates an AIC and sends that back to the provisioner. This response is encrypted using the public endorsement key provided by the Provisioner in the Identity Request.

The process that the ACA and provisioner (generically) perform:

- Provisioner generates an identity request from the client that includes, at a minimum public AK and the EK cert along with information about the device.
- Certificate and certificate chain validation for the EK and platform certificates. If that fails, go no further. Note that the Certificate checking at the ACA is dependent upon the ACA policy settings.
- Generate a nonce (random challenge) used to check the binding private key to the public AK.
- Return an encrypted blob to the provisioner which includes the nonce.
- The client will decrypt the blob and retrieve the nonce to send back to the ACA as proof that it holds the private key associated with the EK public.
- The ACA encrypts the devices Attestation Certificate with the EK cert and sends it back to the provisioner.
- The provisioner decrypts the Attestation Certificate and “Activates” the certificate.

TPM 1.2 Provisioning

The TSS 1.2 (a software interface to the TPM) defines two functions that directly relate to the Attestation CA for requesting an Attestation Identity Certificate (AIC):

- `Tspi_TPM_CollateIdentityRequest`: This function initiates the creation of an identity key, known specifically as an Attestation Identity Key (AIK), and produces a request for an identity credential. The request is encrypted to the Privacy CA, using the Privacy CA's public key (provided indirectly from the Privacy CA's public key certificate).
- `Tspi_TPM_ActivateIdentity`: This function takes a two-part encrypted response from the Attestation CA and extracts the identity credential.

Specifications published by the TCG define all of the details of this process. Here are the relevant details:

The identity request is in the form of a structure named `TCPA_IDENTITY_REQ` (this structure is named `TPM_IDENTITY_REQ` in some documentation). The identity request is simply an encrypted form of the identity proof. The request is a single structure that has two main parts. The first 256 bytes of the request is encrypted to the Privacy CA's public key, and contains details of the process used to perform the symmetric encryption of the second part (including the symmetric key itself). The symmetric encryption is performed using CBC, which requires the use of an initialization vector (IV). The placement of the IV is specified by the TCG, however the most widely used TSS (as of this writing), IBM's open-source `TrouSerS`, uses a different convention. A robust Attestation CA must be able to differentiate between and successfully decipher both forms.

The identity proof should contain all of the information needed for the Attestation CA to create an identity credential and return it to a TPM. Primarily, this information is the public part of the identity key (the modulus and public exponent) and the requested identity label (a string, in some form -- the standard is not explicit and consistent in this). A fully-functional Attestation CA needs to return the credential in an encrypted form to the TPM. The key to be used for this encryption should be included in the request within an endorsement credential. This credential is often not present, and not included when present, resulting in the information not being included in the identity proof. The lack of this information must result in a failure of the Attestation CA to return a credential.

The TPM_IDENTITY_REQ (The "Identity request" output of the Tspi_TSP_CollateIdentityRequest function) is created and sent to the Privacy CA.

- The Attestation CA
 - decrypts the request
 - validates the integrity of the request
 - validate the TPM (by matching to an indexed EK certificate and validating signature),
 - create an X509 AIK certificate
 - package the certificate (TCPA_IDENTITY_CREDENTIAL), encrypt (ASYM_CA_CONTENTS and SYM_CA_ATTESTATION), and send back to the TPM
- The Client/TPM takes the structures from the Privacy CA,
 - passes them to the Tspi_TPM_ActivateIdentity function, and
 - Stores the resulting AIK certificate (TCPA_IDENTITY_CREDENTIAL) in protected storage.

Note that the Identity Request should contain the EK credential, but there is no guarantee that the same TPM holds both the private AIK and private EK for the EK and AIK contained within the Identity Request. This is the purpose for the encryption of the Identity Certificate to the EK. This is also the reason an Attestation CA should never store the Identity Certificate it creates or distribute the Identity Certificate to any party other than to the requesting client, and then only encrypted to the EK. This is an important point, worth repeating as it is a different action than used by many CA's, and is core to the trustworthiness of the AIC's use for attestation.

TPM 2.0 Provisioning

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

- 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 credential with another object in a way that ensures that the TPM has validated the parameters of the credential object.

The ACA performs the TPM2_makecredential process. What it needs for the process is:

- The public EK. This can come from a variety of sources, but the EK cert is the best.
- The AK "name." This can be generated using the public AK.

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

- ACA generate 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 generate 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. The details are similar to that used in the 1.2 CA response, but with different hashing mechanism and OAEP key.
- 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.
- Return 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_activatecredential to 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. (2021). *Trusted Computing Group*. Retrieved from Trusted Computing Group: <https://trustedcomputinggroup.org>
- [2] *Platform Attribute Certificate Creator (paccor)*. (2021, February 18). Retrieved from GitHub: <https://github.com/nsacyber/paccor>
- [3] Trusted Computing Group. (2020, July 23). *TCG EK Credential 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. (2020, April 10). *TCG Platform Certificate Profile*. Retrieved from Trusted Computing Group: <https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/>
- [5] Trusted Computing Group. (2020, November 4). *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. (2020, November 12). *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. (2020, March 31). *TCG PC Client Reference Integrity Manifest Specification*. Retrieved from Trusted Computing Group: https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_RIM_r0p15_15june2020.pdf
- [9] Trusted Computing Group. (2019, 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