Host Integrity at Startup and Runtime (HIRS)

Attestation Certificate Authority (ACA) Portal and TPM Provisioner

Users Guide

Version 1.0.2

11/20/2018

Table of Contents

Introduction

Host Integrity at Runtime and Startup (HIRS) is a proof-of-concept system comprising 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 are a full suite of capabilities for processing of the Trusted Platform Module (TPM) including TPM provisioning, Endorsement Credential (EC) validation, Platform Credential (PC) validation Attestation Identity Credential (AIC) creation, and TPM Quote validation. The HIRS provisioning services comprise of an Attestation Certificate Authority (ACA) and client side provisioner application. HIRS supports an ACA Policy that is recommended for Trusted Computing based Supply Chain validation.

Background

Trusted Computing Based Supply Chain Validation Concepts

The Trusted Computing Group specifies a set of Credentials[2] that can be used for the purpose of TPM provisioning which include processes for performing Supply Chain Validation. These credentials are used to indirectly verify supply chain entities associated with the manufacturing, assembly, delivery, of the specific TPM on the device as well as and software configuration.

These credentials include:

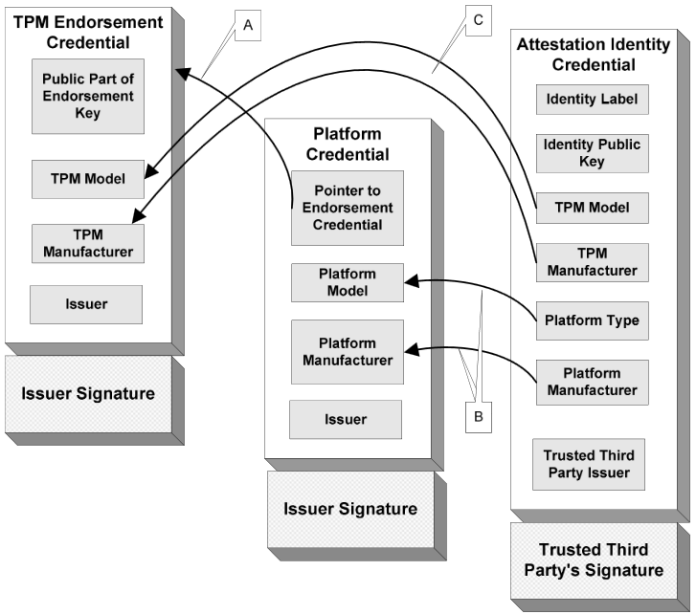
Credential	Creator	Usage
Endorsement	TPM Manufacturer	Attests that the TPM was manufactured by the TPM vendor and meets the TPM vendors documented features
Platform	Motherboard Manufacturer	Validates that the motherboard was manufactured by the specified vendor and meets their documented features
Attestation	IT departments	Used for validation of the software load

For all intents and purposes the term “Credential” is synonymous with a PKI Certificate. Specifically X.509 certificates as defined in the Trusted Computing Groups Credential Profiles Specification(s).

---

1 *www.**trustedcomputinggroup**.org*

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.

Validating the Supply Chain Sources Using TCG Credentials

Acceptance tests for TCG compliant devices may which conform to the supply chain of the device prior to initializing/provisioning/setup of the device. The credentials should be stored within the TPMs NVRAM (HIRS has support for reading the credentials from NVRAM). The validation process would consist of:

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

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

Vendor Certificate Chains

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

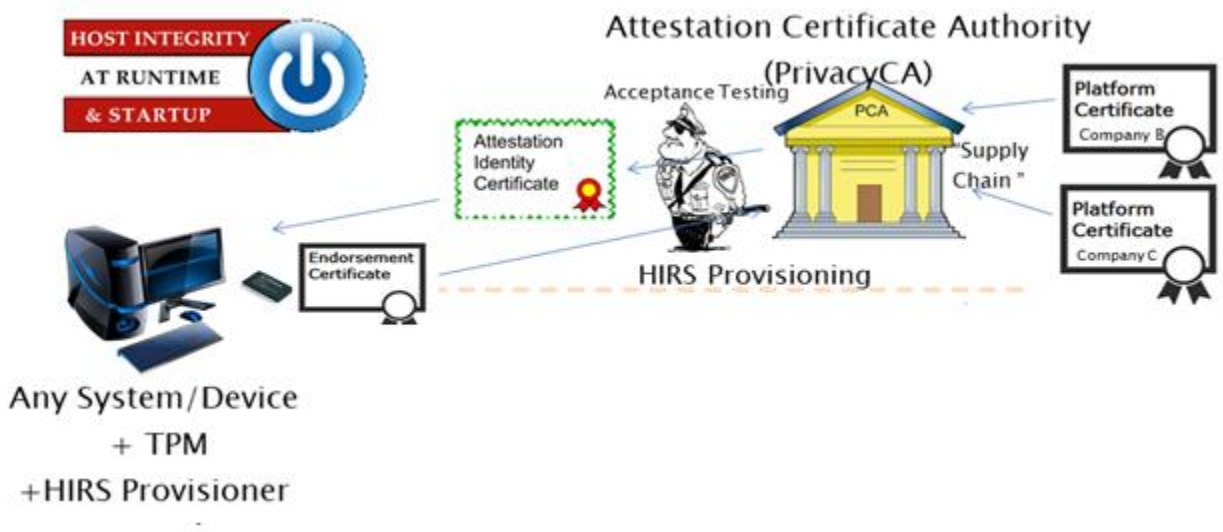
TPM vendors typically post their certificate chain on web accessible URLs. This Certificate chain can require several certificates (e.g. Root CA certificates, intermediate CA certificates, etc.). Refer to the TPM manufacturers' web site for exact location of Certificate chain URLs).

TPM Provisioning

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

HIRS Attestation Certificate Authority

The Attestation Certificate Authority (ACA) is a specialized Certificate Authority (CA) which supports the creation and issuance of an Attestation Identity Credential (AIC) per the specifications. The requirement for specialization is a result of the nature of the keys for which it is providing certificates, the formats of the requests and responses specified, 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 commercial Certificate Authority, The ability to provide revocation can be supported by a commercial CA.

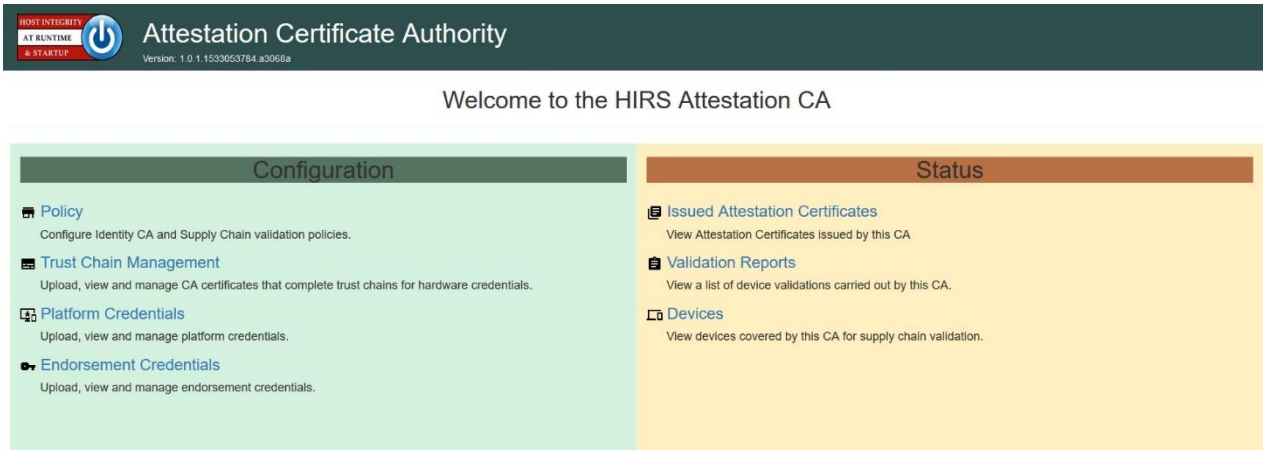
The HIRS Provisioner is a small application that installs on client systems which is used for provisioning the TPM with an Attestation Identity Credential.

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/portal/index

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



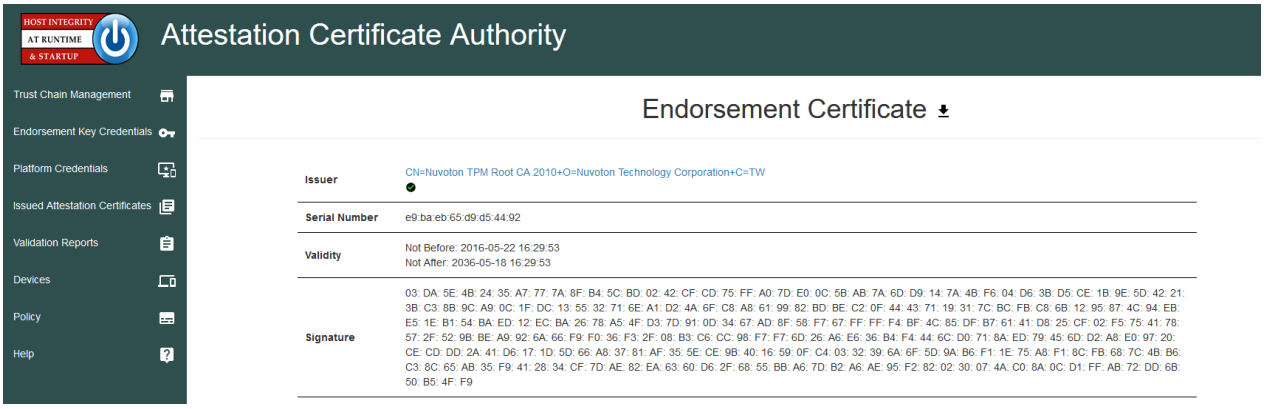
Icons used on the ACA pages generally conform to the following usage:

Located at the top of select pages, it 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.

Located under the Options column, it is used to download the certificate to your local device. A file section dialog will be shown which allows you to select the location and name of the certificate.

Located under the Options column, it is used to delete the certificates reference from the ACA.

Located under the Options column, it is used to display details about the specific certificate. The displayed certificate is tailored to the type of certificate being viewed:



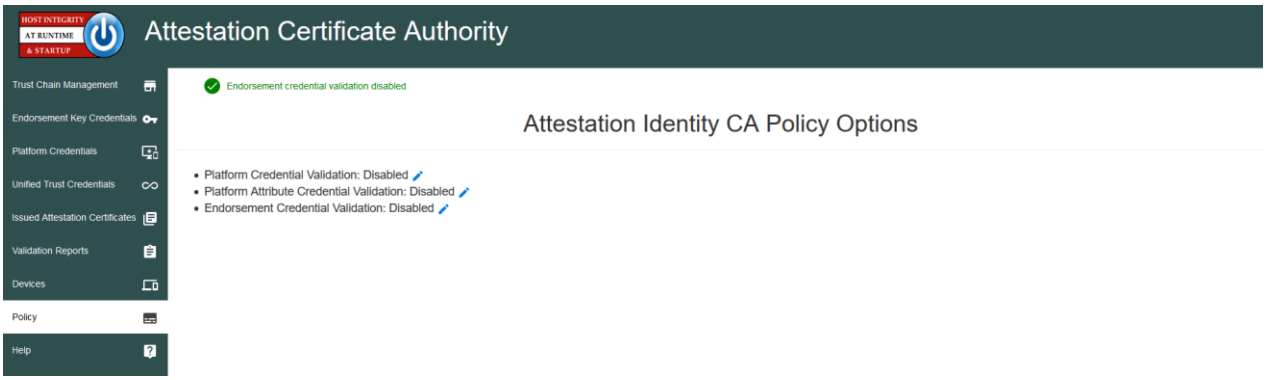
Note that the issuer field will have a blue hyperlink to the issuing cert, if the issuing cert is present in the Trust Chain Management page. The Green check under the Issuer field indicates that the entire trust chain is present and that ACA should be able to validate the signature on that particular certificate.

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 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 The Policy is set via the Policy tab on the ACA portal. Currently the options are:



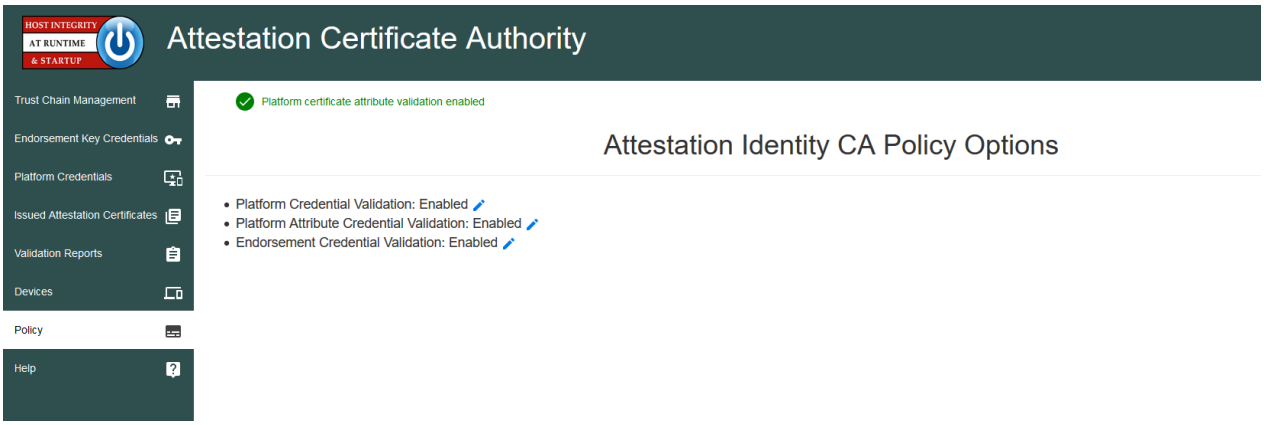
Endorsement Credential Validation: If enabled the ACA will require that the ACA validate the Endorsement Credential prior to issuing an Attestation Credential. The default is disabled.

Platform Credential Validation: If enabled 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. The Endorsement Credential Validation will be required to be checked prior to enabling this policy option. The default is disabled.

Platform Attribute Credential Validation: If enabled the ACA will require that the ACA validate all the Platform Credential Attributes prior to issuing an Attestation Credential. This

option configures the ACA to check each Component field within the certificate against information provided by the TPM provisioner. Any single discrepancy with result in a failure to issue an AIC and will be noted on the validation report page as a failure The Platform Credential Validation will be required to be checked prior to enabling this policy option. The default is disabled.

Recommended Policy Setting for Trusted Computing Based Supply Chain Validation



The recommended policy setting for Trusted Computing based Supply Chain Validation will require all current policy setting be set to true

- **Endorsement Credential Validation: Enabled**
- **Platform Credential Validation: Enabled**
- **Platform Attribute Credential Validation: Enabled**

This Policy will check for and validate:

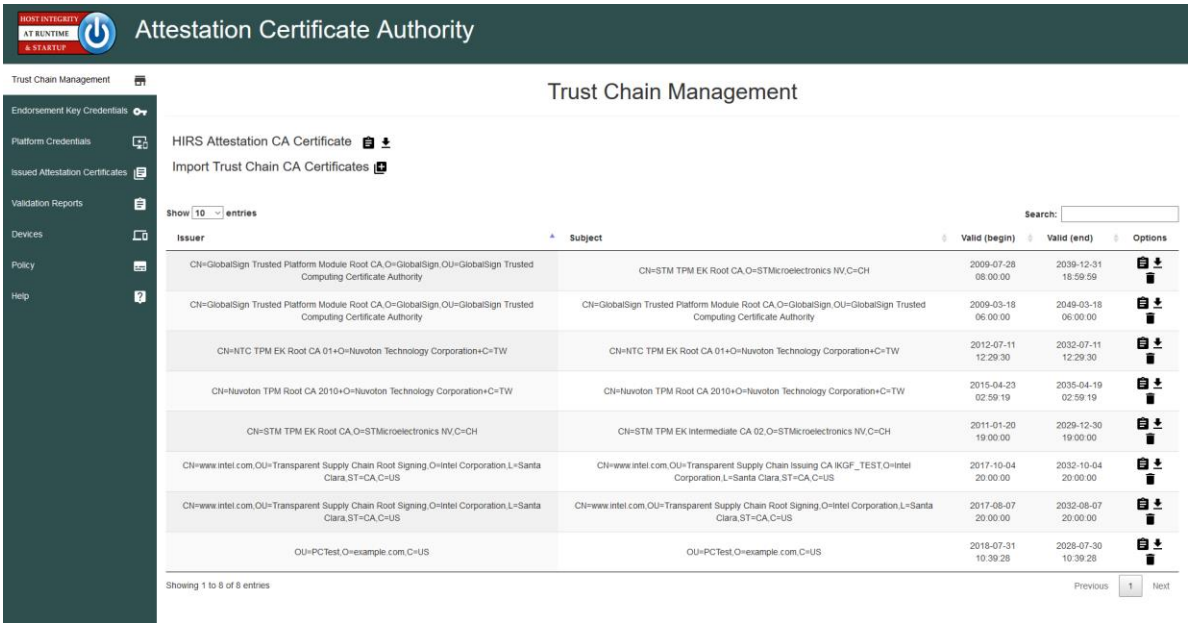
- Trust Chains belonging to all TPM manufacturers of TPM belonging to the devices that require Supply Chain Validation
- Trust Chains belonging to all Platform manufacturers of the devices that require Supply Chain Validation
    - Components defined within the Platform Credential

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 certificates) is considered a "chain: of certificates.



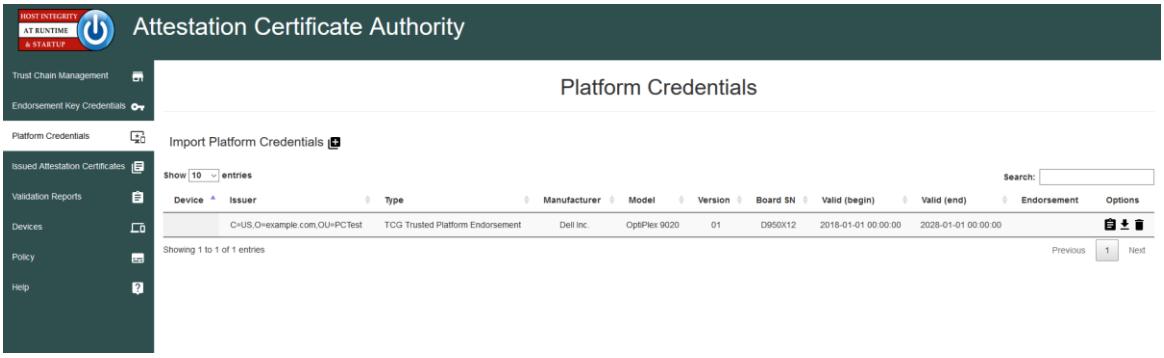
By default the ACA generates a self-signed certificate that is used as the root CA for signing all issued Attestation Certificates. An Attestation CA certificate may be signed by a Root CA and replaced (the ACA certificate would become a subordinate to the Root CA. In either case, the CA certificate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

The Platform credential 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

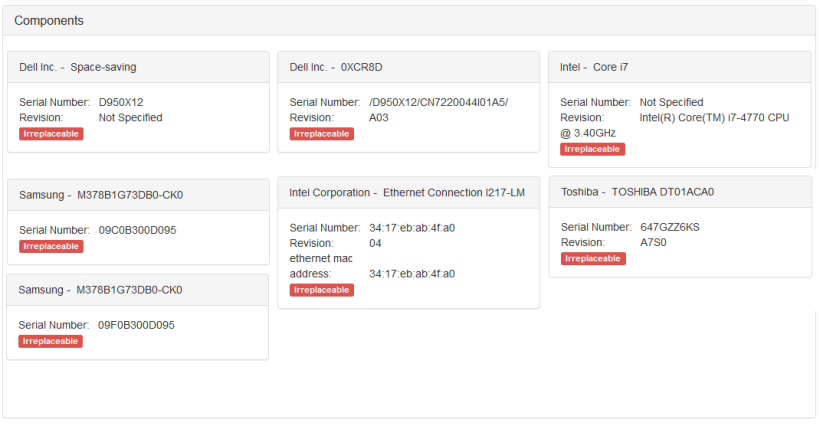
Manufacturer	Dell Inc.
Model	OptiPlex 9020
Version	01
System Serial Number	D950X12

The Platform id pertains the systems Manufacturer. The “system” information is defined by SMBIOS and adopted by most major computer manufactures.

Platform Certificate Component fields

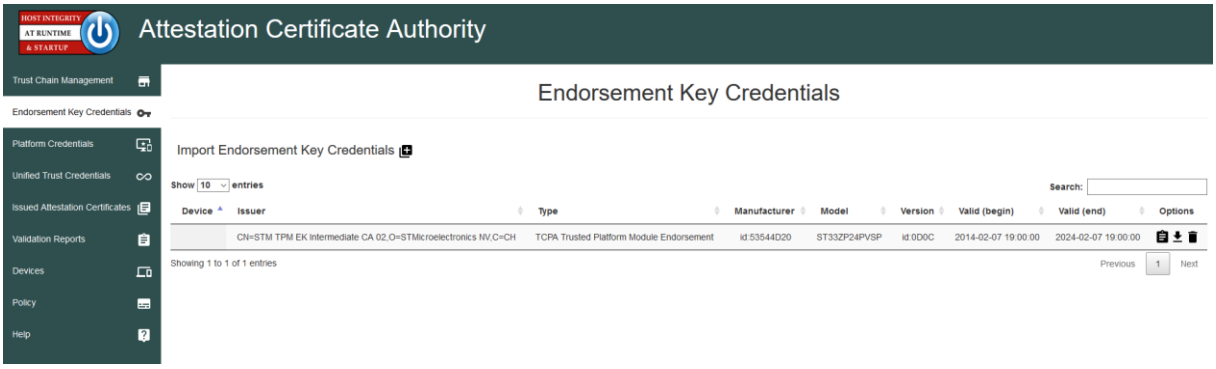
Components contain Manufacturer (first item off each component), Model, Serial Number, and Revision of components specified by the Manufacturer:

TCG Platform Configuration



The Endorsement Credential (EC) Page

The Endorsement Credential (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.



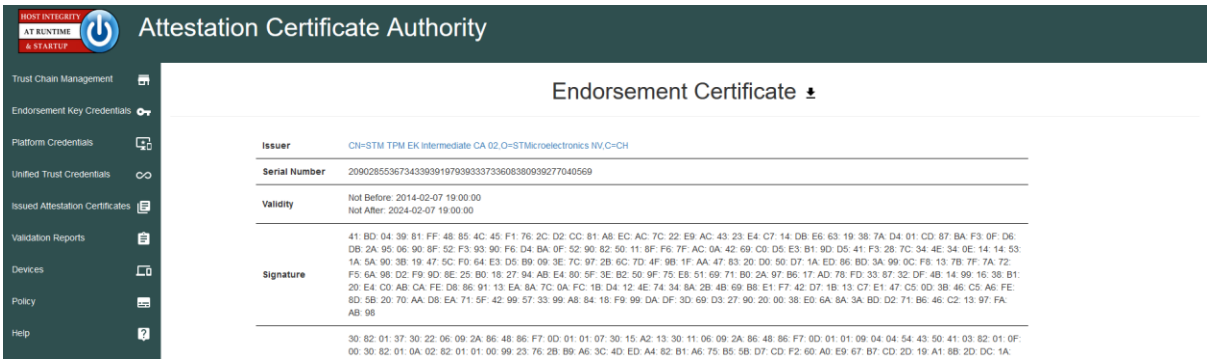
The Endorsement Key Credential must contain:

- 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 Validation. 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.

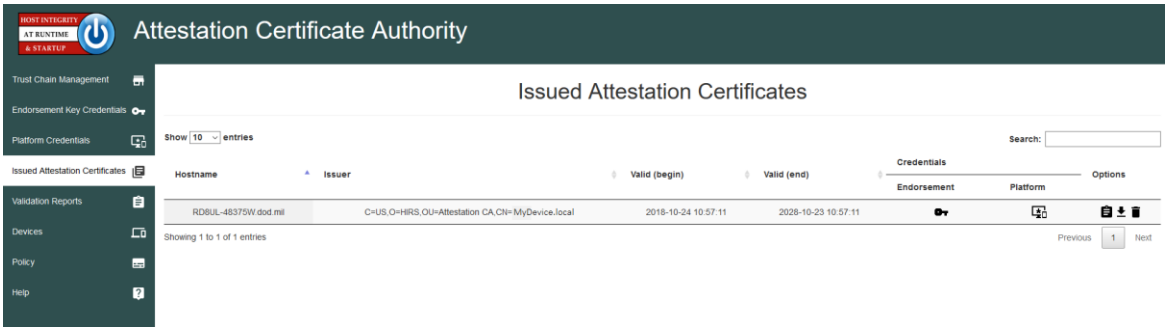


ACA Status

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

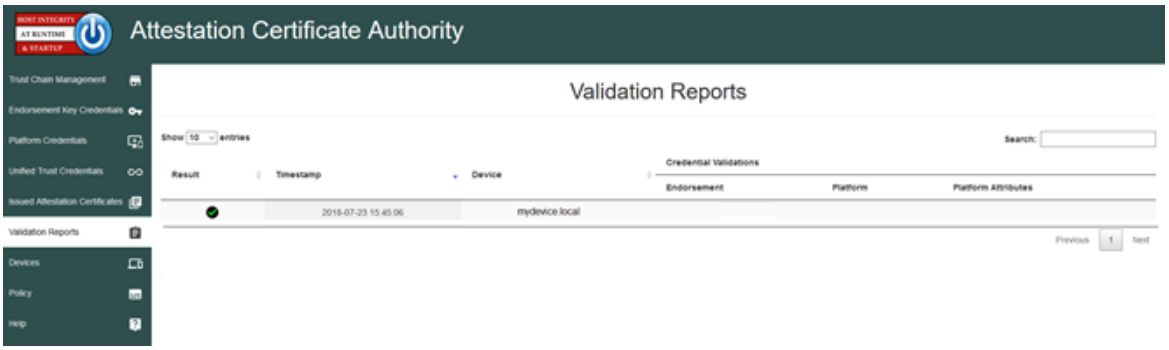
Issued Attestation Certificates page

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.

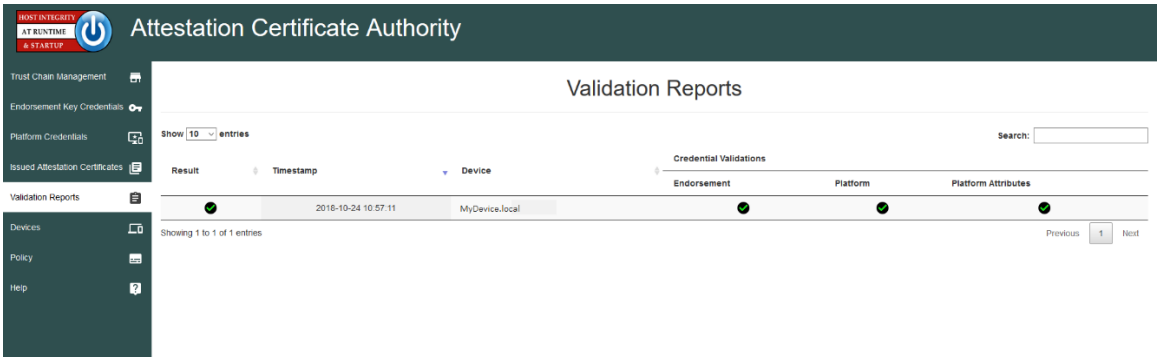


Validation Reports page

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

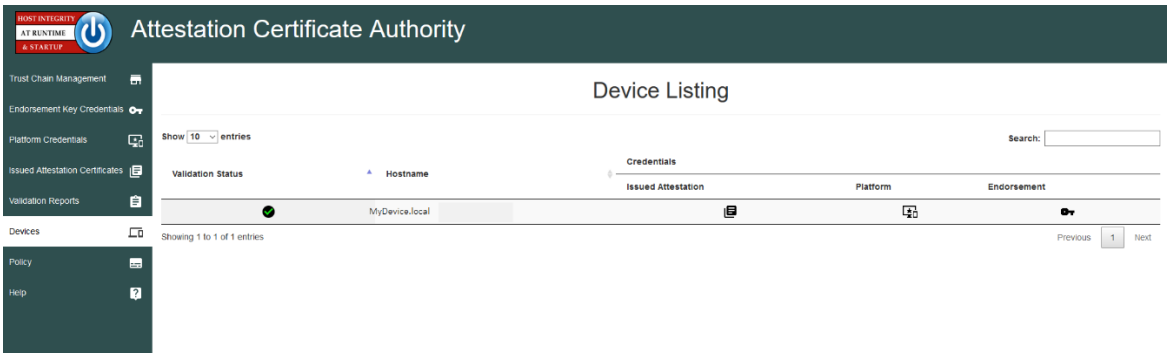


The Credential Validation Columns are only populated if the ACA Policy was set to include the particular validation at the time the request was made. The above indicates that the default policy was used and that no validation of the EK or Platform Credentials was performed. The screenshot below indicates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



Devices page

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



HIRS Provisioner

HIRS has a set of client applications used for TPM provisioning and Supply Chain Validation (one that supports TPM1.2 and one that supports TPM 2.0). The provisioner will attempt to read both Endorsement Credentials and Platform credential from the TPMS NVRAM. The TPM Provisioner performs 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 (TPM1.2).
- 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
```

This command sets 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-sit.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 on the Attestation CA 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 it 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

As well as component information (See “Recommended Policy Setting for Trusted Computing Based Supply Chain Validation” for a recommended component information to collect).

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
- Installation notes
- HIRS build guide
- Getting started guide

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

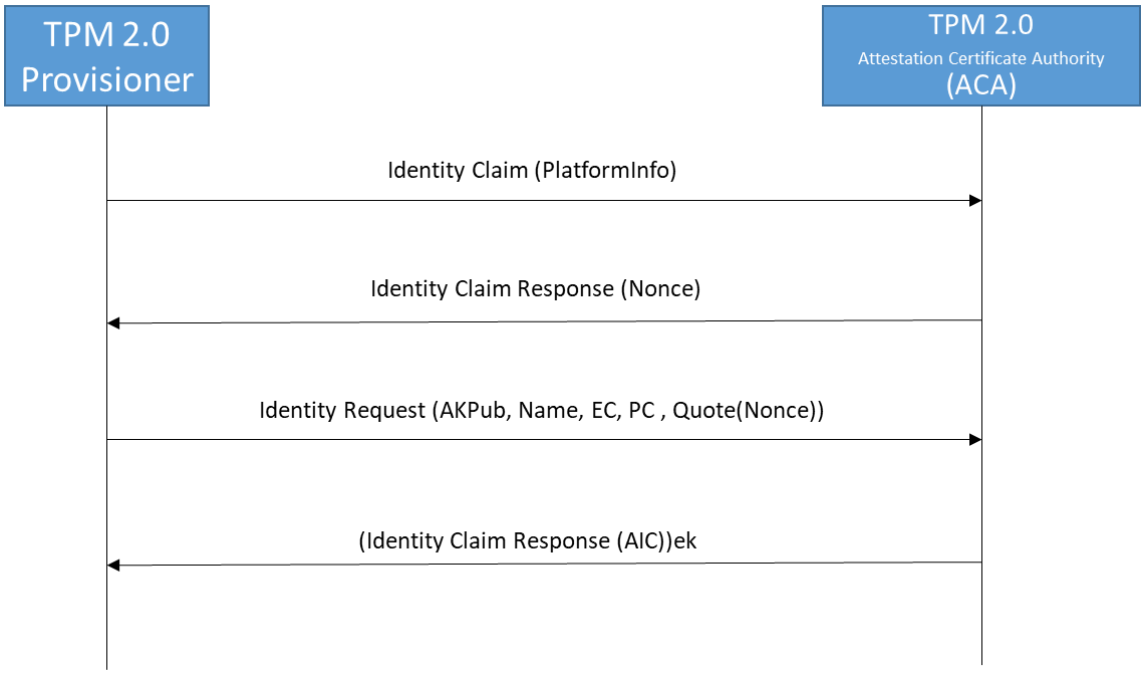
Appendix B: TPM Provisioning Details

The overall protocol for provisioning either TPM1.2 or TPM2.0 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): 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.)

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

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

This information includes the Attestation public key, a ticket which verifies the AK key usage, the Endorsement Credential (EC), the Platform credential (PC) and a TPM Quotes (which includes the nonce from the Identity Claim response and a signature using the TPM's Attestation Key.

(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 ACA implements a security protocol during provisioning in order to allow the client to utilize its TPM2_activatecredential process. The protocol will force the client to prove it possesses both the EK and AK key pairs that it claims to have. It will also ensure the ACA is communicating with a specific client. The protocol is outlined as follows:

- The client requests to authenticate with the ACA, providing the public EK (preferably in the EK certificate) and the public AK
- ACA generates the expected AK name based on ACA requirements of key generation for the AK and utilizing the given public AK
- ACA generates a seed, which are random bytes of size appropriate to the algorithm requirements
    - In our case, the seed has a length of 32 bytes
- ACA creates an AES key from the seed and the AK name according to key derivation requirements in the TPM specification
- ACA creates a HMAC key from the seed also according to key derivation requirements in the TPM specification.
- ACA encrypts the seed using the public EK retrieved from the EK cert with parameters specific to the TPM specification. This creates an asymmetrically-encrypted blob.
- ACA generates a nonce (random challenge) used to check the binding private key to the public AK. The nonce is also labeled the ‘secret’.
- ACA encrypts the secret using the AES Key, creating the encrypted secret also known as encIdentity.
- ACA creates the integrity HMAC using the HMAC key, the AK name, and the encIdentity value.
- ACA returns to the client the encIdentity value, the integrity HMAC, and the asymmetric blob, all packaged as it is expected by the TPM_activatecredential function on the client TPM.

The ACA expects the client to perform the TPM2_activatecredential function.

- TPM_activatecredential uses a private EK on the client TPM to decrypt the asymmetric blob to retrieve the seed.
- If the client possessed the expected EK, the client will recover the correct seed.
- The client uses the seed to derive the HMAC key.
- The client remembers the key handle for the AK which it sent to the ACA.
- The client TPM derives the AK name for the AK that it generated.
- The HMac key and AK name are used to validate the integrity HMac.
- If the HMac passes validation, the seed and the AK name will derive the AES key.
- The AES key is used to decrypt the encIdentity value, this recovers the secret.
- The client TPM will only recover the correct AES key to recover the expected secret if the HMac, which covers the name of the AK it created, is validated. This is proof that the AK was created by the TPM.
- The client encrypts the secret with the public key of the ACA, and sends the encrypted result to the ACA.
- ACA decrypts the encrypted blob using its private key.
- The output will only match the expected secret if all of the above steps were successful.
- In the successful case, the ACA will go forward with the generation of the AIC. Otherwise, it will deny the provisioning request with a helpful error message.