

Attestation Certificate Authority Installation Notes

Version 1.0.0

This paper describes downloading, installing, setting up, and using the open source elements of the HIRS framework.

Supported Platforms

The HIRS Attestation Certificate Authority (ACA) supports installation on CentOS 6 and 7 instances.

This HIRS Provisioner supports installation on CentOS 6 and 7 with support for Ubuntu 16 planned for the future.

Before You Begin

Confirm that the target environments for both the ACA and the Provisioner (which may be the same) meet the below requirements:

1. The OS must be installed and configured for networking prior to installation. This should include:
 1. An administrative account that will be used for installing HIRS.
 2. A Fully Qualified Domain Name (FQDN) be assigned to the server running the ACA and that the DNS system will resolve the name to an address. This is important for the certificate verification that FQDN be used and the name is resolvable by DNS.
2. The hardware must meet the HIRS minimum requirements.
 1. HIRS ACA may be a virtual machine or physical device
 1. Centos 6 or 7 OS
 2. 50GB HD space
 3. 6GB RAM
 2. The Client device must have a TPM 1.2, and the TPM must be cleared and enabled in the BIOS. The settings for the TPM are generally found in the BIOS/UEFI setup application which is specific the platform hosting the TPM. Refer to the server/desktop user manuals for instruction on how to enable/clear the TPM.
3. The Provisioner will need connectivity to the ACA. Check that any firewalls between the ACA server and Provisioner have port 8443 enabled.
4. Setup an OS repository for the device. The HIRS installation package will attempt to install its dependencies for the system local software repository if they are not currently

installed. It is highly suggested that an repository be setup prior to avoid dependency issues. Dependencies for the HIRS-Provisioner include:

5. Java 1.8 (latest version)
6. gcc
7. TrouSerS
8. tpm-tools

Dependencies for the HIRS Attestation CA include

1. Java 1.8 (latest version)
2. Tomcat (latest version)

Getting the HIRS ACA and Provisioner

Currently, the HIRS ACA and Provisioner are provided as a set of CentOS 6 and 7 RPMs. In the future, the full source of these packages will be released along with documentation for building these packages. To get the currently released packages, clone the repo with:

```
$ git clone <path_to_repo> <directory>
```

This will clone the RPMs into which will contain six RPMs: HIRS_AttestationCA*.rpm, HIRS_Provisioner*.rpm, and tpm_module*.rpm for both CentOS 6 and 7.

Installing the ACA

To install the ACA, navigate to the directory where the HIRS repo was cloned and:

```
yum install HIRS_AttestationCA*.rpm
```

Installing the Provisioner

The Provisioner is intended to be run on a host device with a TPM. It does not have to be installed on the HIRS ACA, but can be if the HIRS ACA is on a device with a TPM.

To install the Provisioner, navigate to the directory where the HIRS repo was cloned and:

```
yum install tpm_module*.rpm  
yum install HIRS_Provisioner*.rpm
```

Provisioner Setup

After installing the Provisioner, it is necessary to perform a few configuration steps:

```
$ hirs-provisioner -c
```

This produces a default hirs-site.config in /etc/hirs. This default setup must be edited. The file should look like the following:

```
*****
#* HIRS site configuration properties file
*****
# Client configuration
TPM_ENABLED=
IMA_ENABLED=
CLIENT_HOSTNAME=$HOSTNAME
# Site-specific configuration
ATTESTATION_CA_FQDN=
ATTESTATION_CA_PORT=8443
BROKER_FQDN=
BROKER_PORT=61616
PORTAL_FQDN=
PORTAL_PORT=8443
```

The ATTESTATION_CA_FQDN and ATTESTATION_CA_PORT keys should be set to the hostname of the server running the ACA and the port on that server the ACA is configured to listen on (8443 by default), respectively. The BROKER_FQDN and PORTAL_FQDN should also be set to the hostname of the server running the ACA. TPM_ENABLED should be set to true.

Testing the install:

After the ACA is installed, the The HIRS Portal should be up and running

HIRS_Server package. Portal URL:

https://ACAserveraddress:8443/HIRS_AttestationCAPortal/

Provisioning

To provision the provisioning process use the following command on the TPM enabled device on which the HIRS_Provisoner was installed:

```
$ hirs-provisioner -p
```

If successful the HIRS provisioner should have provided status indicating success.

Check the HIRS_AttestationCA portals validation report page for a status successful entry from the provisioner. Note that the default setting is for the AttestationCA Policy is to not check Endorsement or Platform credentials. This requires import of the Certificate Trust Chains (PKI Certificates used to validate Endorsement or Platform Certs) via the HIRS_AttestationCA portal.