nFinity Partner

Corda R3 Enterprise Blockchain Platform

Entrust Integration Guide

Version 1.1

Date: SEPTEMBER 1, 2021

Introduction

This guide details how to store legal identity keys for a Corda Enterprise node in an Entrust nShield HSM.

Integration configurations

Operating system	***Partner product namePartner product name***	**nShield HSM**	**nShield firmware version**	**nShield Security World version**	**Certification support**
Linux	*Corda Enterprise Node v4.4*	*nShield Connect XC*	*V12.50.11*	*12.60.2*	*FIPS 140-2 Level 2*

Supported Entrust nShield features

Corda Enterprise supports the JAVA JCE/JDK for integration with the nShield Security World Client. The Corda Enterprise HA JAR utilities leverages the use of the JAVA JCE/JDK for communication with nShield.

Requirements and prerequisites

The guide assumes users have access to the following:

- A Linux server running supported OS and JCE/JDK distribution for Corda Enterprise (see here)
- A Corda Enterprise node JAR file (version 4.4 or above)
    - A Corda Enterprise HA utilities JAR (version 4.4 or above – see here)
- The truststore of the network where the Corda node is to be registered (see here)
- Entrust nShield HSM
    - Firmware version 12.50.11
    - Entrust Security World distribution (ISO image for Linux 64-bit) including nCipherKM provider (nCipherKM.jar) version 12.60.2

The guide assumes that the Entrust nShield HSM and the Linux server are located in a secure network, and the HSM has been configured to accept connections from the Linux server.

Related documents and support

Additional Entrust related documentation for the nShield and API use can be found:
* Installation Guide and User Guide for the nShield HSM.
* User Guide for the nFinity Partner Product.

Corda R3 Product Support pages: https://www.r3.com/contact-support/

Submit a request to nshield.support@entrust.com to request access to product documentation.

Entrust Product Documentation pages are accessible via: https://ncipher.zendesk.com/hc/en-us.

Integration procedure

nShield Security World Client Install

1. Mount Security World ISO image:

   ```
   $ sudo mkdir /media/iso
   $ sudo mount -o loop ./SecWorld_Lin64-12.60.2.iso /media/iso
   ```

2. Extract archives from ISO image:

   ```
   $ for file in /media/iso/linux/amd64/*; do sudo tar zxvf "$file" -C /; done
   ```

3. Install service:

   ```
   $ sudo /opt/nfast/sbin/install
   ```

4. Check that hardserver is started

   ```
   $ /opt/nfast/bin/enquiry
   ```

5. Check access to HSM:

   ```
   $ /opt/nfast/bin/anonkneti -p 9004 {hsm_ip_address}
   ```

6. Enroll the HSM client:

   ```
   $ sudo /opt/nfast/bin/nethsmenroll -P 9004 {hsm_ip_address}
   ```

7. Check that HSM module is properly configured:

   ```
   $ /opt/nfast/bin/enquiry
   ```

8. Optional if using nSaaS:
   Copy provided module_XXXX-XXXX-XXXX and world files into /opt/nfast/kmdata/local directory.

9. Set nonpriv_port=9000 and priv_port=9001 in the hardserver configuration file

   ```
   $ sudo vi /opt/nfast/kmdata/config/config
           # The port for the hardserver to listen to for local non-privileged TCP
           # connections or 0 for none. Java clients default to connecting to 9000
           # (default=0)
           nonpriv_port=9000
           #
           # The port for the hardserver to listen to for local privileged TCP
           # connections or 0 for none. Java clients default to connecting to 9001
           # (default=0)
           priv_port=9001
   ```

10. Restart hardserver:

    ```
    $ sudo /opt/nfast/sbin/init.d-ncipher restart
    ```

11. Ensure that /opt/nfast/kmdata/local is writable for current user.

Corda node configuration

1. Create a directory called /opt/corda and a directory called /opt/corda/drivers

2. Place the Corda Enterprise JAR in /opt/corda

3. Create the following subdirectories under /opt/corda:

4. Create a node configuration file (/opt/corda/node.conf) and include the following entries:

   ```
   cryptoServiceName: "N_SHIELD"
   cryptoServiceConf: "nshield.conf"
   cryptoServiceTimeout: 10000
   ```

5. Create a CryptoService configuration file (/opt/corda/nshield.conf) with the following entries:

   ```
   keyStore: "certificates/keystore.nshield"
   password: "my-password"
   ```

6. Place provided nCipherKM.jar file in the /opt/corda/drivers folder.

Generating Corda node legal identity keys

Run node initial registration procedure by using the HA Utilities JAR:

```
$ java -jar 4.4-RC01/corda-tools-ha-utilities-4.4.jar node-registration --config-files
/path/to/node.conf --network-root-truststore /path/to/network-root-truststore.jks --
network-root-truststore-password trustpass
```

Appendix: Additional information

Provide additional details about the integration not covered within the main portion of this guide including support for High Availability, cloud support (AWS, Azure, or other), backup strategies, or other considerations.

Contact Information

To request technical support for Corda R3 reference:

Corda R3 Product Support pages: https://www.r3.com/support/.

To request technical support for Entrust nShield Products reference:

https://nshieldsupport.entrust.com/hc/en-us for technical support contact details.

Via Email, to request access to Entrust product documentation email nshield.support@entrust.com .