OneSpan Authentication Server Framework

nShield® HSM Integration Guide

18 May 2022

Contents

1. Introduction

This document describes the integration of OneSpan Authentication Server Framework with the Entrust CodeSafe solution. This uses an Entrust nShield Hardware Security Module (HSM) root of trust.

CodeSafe is a runtime environment on the Entrust nShield HSM that allows third-party developers to run their own code within the secure boundary of the module.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with OneSpan Authentication Server Framework in the following configurations:

Product	Version
CodeSafe	12.80.4
Security World Compatibility Pack	1.1.0
Operating System	Red Hat Linux 8 64-bit
OneSpan ASF	3.21

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
12.80.4	12.50.11	12.80.4	✓	✓	✓

1.2.2. Connect +

Security World Software	Firmware	Image	OCS	Softcard	Module
12.80.4	12.50.8	12.80.4	✓	✓	✓

Security World ciphersuite **DLf3072s256mRijndael** is required for the integration of OneSpan ASF and nShield HSM.

1.3. Supported nShield HSM functionality

Feature	Support
Module-only key	Yes
OCS cards	Yes
Softcards	Yes
nSaaS	Yes
FIPS 140-2 Level 3	Yes

1.4. Requirements

Before installing these products, read the associated documentation:

- For the nShield HSM: *Installation Guide* and *User Guide*.
- If nShield Remote Administration is to be used: *nShield Remote Administration User Guide*.
- For CodeSafe: *CodeSafe Developer Guide for Linux*
- OneSpan documentation: *Authentication Server Framework HSM Module Management* and *Authentication Server Framework Key Management for nCipher nShield HSM*

1.5. More information

For more information about OS support, contact your OneSpan sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

2. Procedures

2.1. Prerequisites

Before you can use OneSpan Authentication Server Framework with CodeSafe and an nShield HSM, you must complete the following steps:

1. Set up the HSM. See the *Installation Guide* for your HSM.
2. Configure the HSM(s) to have the IP address of your host machine as a client.
3. Install the nShield compatibility pack:

```
% sudo mount -t iso9660 -o loop Compatibility_Package_1.1.0.iso /mnt
% cd /
% tar -zxvf /mnt/lin64/amd64/Compatibility_12.40_Lin64.tar.gz
% sudo umount /mnt
```

4. Load an existing Security World or create a new one on the HSM.

   

   The Security World **DLf3072s256mRijndael** ciphersuite is required.

   For more information on configuring and managing nShield HSMs, Security Worlds, and Remote File Systems, see the *User Guide* for your HSM(s).

5. Install CodeSafe:

```
% sudo mount -t iso9660 -o loop Codesafe_Lin64-12.80.4.iso /mnt
% cd /
% tar -xf /mnt/linux/amd64/csd.tar.gz
% tar -xf /mnt/linux/amd64/csdref.tar.gz
% sudo umount /mnt
```

2.2. Set up OneSpan ASF

The following steps to install OneSpan ASF for nShield HSM are detailed in the *Authentication Server Framework HSM Module Management* guide.

OneSpan ASF software contains an example script to set up the user data file and upload the SEE machine. See the contents of the script or refer to the OneSpan ASF documentation for the individual steps which can be tailored to your organizational needs.

1. Install the RPM package for your specific Operating System:

```
% rpm -i <OneSpan_RPM_File>.rpm
```

2. Generate the SEE code-signing key:

```
% generatekey --generate seeinteg type=rsa size=2048 pubexp= recovery=yes nvram=no plainname=seesigningkey
```

If using a FIPS 140-2 Level 3 Security World, an OCS will need to be inserted into the HSM during key generation.

3. Run the set-up script:

```
% /opt/vasco/VACMAN_Controller-HSM-3.21.0/hsm/ppc-xc/build_userdata.sh
```

The `ppc-xc` directory is required in the command if using an nShield Connect XC. The `ppc` directory is required in the command if using an nShield Connect Plus.

OneSpan Authentication Server Framework is now set up and ready to be used. Note that OneSpan ASF software contains sample programs at `/opt/vasco/VACMAN_Controller-HSM-3.21.0/sample/` that demonstrate communication between a host application and an nShield HSM.