Entrust Security Manager – Trident HSM Integration Guide

i4p Informatics Ltd.
Email: info@i4p.com
Website: http://www.i4p.com
http://support.i4p.com

[20211124-0001]

1 Introduction

The goal of this document is to describe how the Trident HSM can be used as a hardware security module (HSM) for Entrust Security Manager, to generate and maintain keys. Entrust Security Manager, from Entrust Corp., is a software product providing a Public-Key Infrastructure (PKI) that manages digital certificates and can publish Certificate Revocation Lists (CRLs). Although Entrust also has several HSM solutions as part of the nShield HSM product family, it is possible to interface it with any PKCS#11 compliant third-party HSM.

Trident HSM is a hardware security module developed by i4p-informatics, designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys and data.

Please note that the installation and configuration steps presented in this document are valid for version 10.0.1 of Entrust Security Manager, and with respect to Trident HSM, for version 0.13.0 of MPCM submodule. Later (or earlier) versions may need slightly different or even additional steps – please consult the homepage of i4p at https://www.i4p.com for up-to-date information or contact i4p support at http://support.i4p.com.

2 Requirements

This document assumes that the Trident HSM has been properly installed and set up (see the Trident HSM installation guide for details), is operational, and is accessible from the server on which the Entrust Security Manager software will be running.

You will also need the Trident HSM PKCS#11 driver files for the operating system (Windows Server, Red Hat Enterprise Linux or CentOS) on which you plan to run Entrust Security Manager. You should have received these files from i4p, along with sample configuration files, as part of Trident SDK.

3 Preparing Trident HSM

There are a few steps you have to perform to prepare Trident HSM for the integration. First, you have to create a cryptoki user which will be used by the Entrust Security Manager to connect to Trident HSM. Although you could utilize a cryptoki user already created for a different purpose, due to security reasons it is highly recommended to have a separate cryptoki user dedicated only to Entrust Security Manager. To create a cryptoki user, log in to the Trident HSM and issue the command:

```
mpcmd mpc_newusr
```

The command will ask a series of questions. You need to specify:

- the username
- the user role; enter "u" to create a key user
- the user type; enter "c" to create a cryptoki-enabled user
- the client application type; enter "e" to select External Client Application
- whether the user will be used by SAM; enter "n" to decline this option
- the authentication factor; enter "1" to select password-only authentication
- the initial password (twice)
- username of a CM administrator
- the password for the given CM administrator

In order to activate the user, its initial password should be modified by the user itself, so the command below has to be issued:

```
mpcmd mpc_passwd
```

This command will also ask a few questions, namely:

- the username; enter the same username you did for the `mpc_newuser` operation
- confirmation for the password change; enter "y"
- the new password (twice)
- username of the user on which behalf you want to perform the operation; enter again the same username you did for `mpc_newuser`
- password of the user on which behalf you want to perform the operation; enter the initial password you specified for `mpc_newuser`

Ensure that the new password is different from the initial one, and that both passwords comply with the password rules configured for Trident HSM. By default, passwords should contain at least one lower case letter, at least one upper case letter, at least one digit, at least one punctuation mark, and should be at least 10 characters long.

A PIN code has to be assigned to the cryptoki user, which will be used later by Entrust Security Manager for authenticating itself. The Trident SDK provides a Java-based tool to perform this operation, namely you have to issue the following command from any machine which has Java version 8 or later installed and can access Trident HSM:

```
java -jar cryptoki-init.jar <url> <username> <password> <pin>
```

where `<url>` represents the URL of the Trident HSM API endpoint (for example "https://192.168.1.10:2000"), `<username>` stands for the username of the newly created cryptoki user, `<password>` is the password set by the `mpc_passwd` command, and `<pin>` specifies the PIN code.

Moreover, values of a few configuration parameters need to be changed, therefore log in to the Trident HSM and, since the configuration of a running MPCM cannot be edited, shut it down first:

```
mpcmd mpc_stop
```

After the MPCM is stopped, use this command to initiate the configuration:

```
setconf -t mpcm
```

A text editor is launched with the MPCM configuration file opened in it. First, disable the timeout for user sessions, so that the session management of Trident HSM is completely aligned with how PKCS#11 operations are carried out by Entrust Security Manager. This means setting the `mpcm_createsesstmo_u` and `mpcm_lastacc2sesstmo_u` parameters to a relatively large integer, for example 31,536,000 (they specify the number of seconds after a user session times out, measured from the session creation and last operation, respectively).

In addition, instead of requiring a password for generated keys, make it optional by changing the value of the `mpcm_keyprotection` parameter from "required" to "enabled". To save the modified configuration, press Control-X and then "Y".

Now you can start MPCM again:

```
mpcmd daemon -t mpcm
```

The last step is to enable automatic key generation; if you have not done already so, enter the following command:

```
mpcmd mpc_autokeygen -auto
```

4 Installation

Log in to the server on which Entrust Security Manager will run, and uncompress the Trident SDK archive containing the Trident HSM PKCS#11 driver files and the sample configuration file in a temporary directory. In case of Windows Server, copy the driver files to a designated directory, for instance `C:\trident`, and add that directory to the `Path` system variable. One way to achieve that is to open the Control Panel, search for the "Edit the system environment variables" section, and after launching it, clicking on **Environment Variables…** under the **Advanced** tab, then simply editing the value of the `Path` variable in the lower list. If you are using Linux, copy `libmpcm-pkcs11.so` and `libcmapi.so` to `/usr/lib64`.

Copy the sample configuration file `mpcm-pkcs11.conf` to any location you prefer (in case of Windows you can put it in the same directory where the driver files are

located), and ensure that the user running the Entrust Security Manager has the necessary permissions to access it and read its content. The file looks like this:

```
url=https://192.168.1.10:2000
log_level=4
log_to_std_output=1
log_to_file=C:\trident\pkcs11.log
keytec=5
slot1=testUser
```

Modify the configuration parameters as necessary to fit the characteristics of your Trident HSM and planned Entrust Security Manager installations. The only mandatory parameter is `url`, which should refer to the URL of the Trident HSM API endpoint. For the exhaustive and detailed description of available parameters see the MPCM PKCS#11 User Guide.

Set the system environment variable `MPCM_PKCS11_CONFIG_PATH` to point to this customized configuration file. In Windows you can again use the "Edit the system environment variables" section in the Control Panel; for Linux one approach is to add a line to `/etc/environment`, which, assuming the path of the configuration file is `/etc/mpcm-pkcs11.conf`, would be:

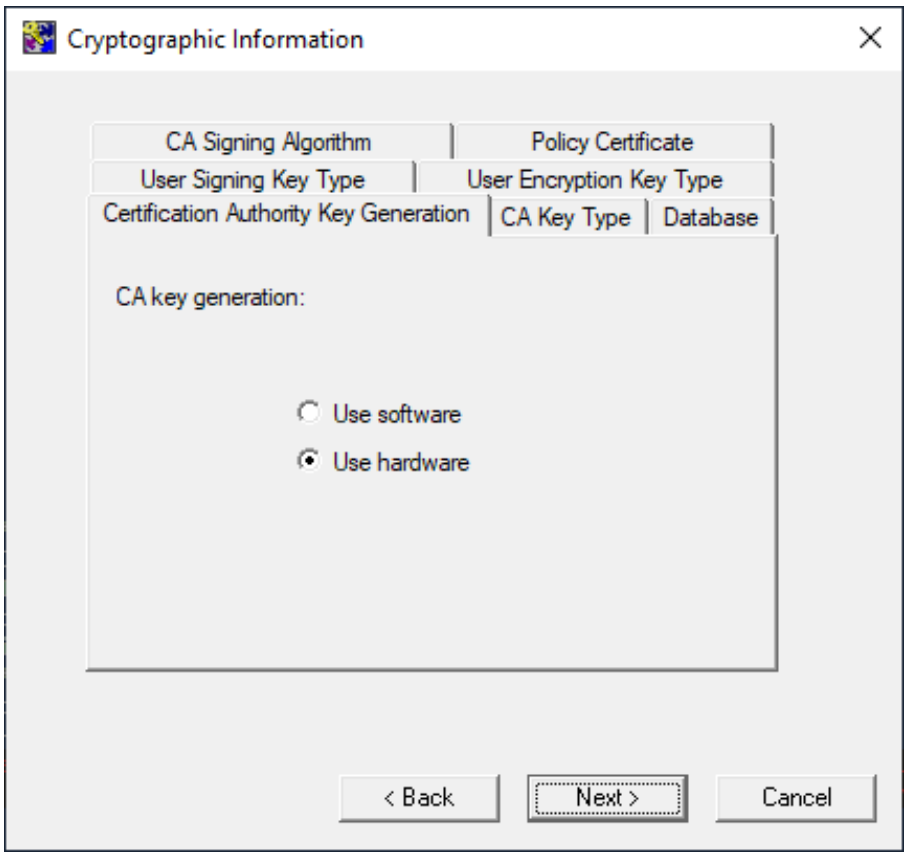
```
MPCM_PKCS11_CONFIG_PATH=/etc/mpcm-pkcs11.conf
```

assuming that the path of the configuration file is `/etc/mpcm-pkcs11.conf`.

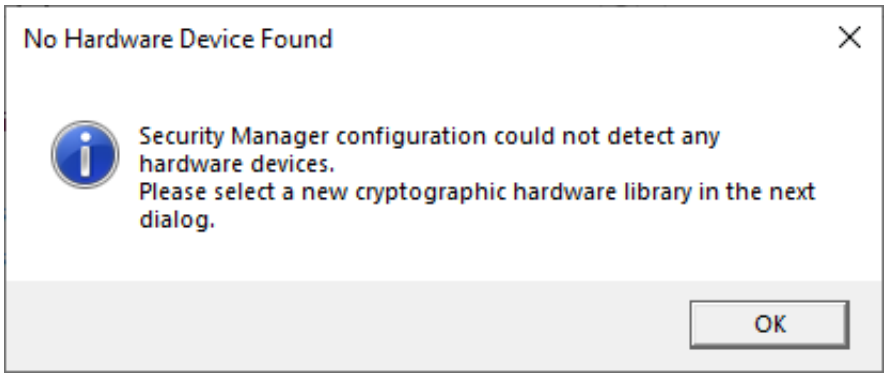
Next, install Entrust Security Manager on the server, according to the installation guide to which you should have received access from Entrust.

5 Configuration

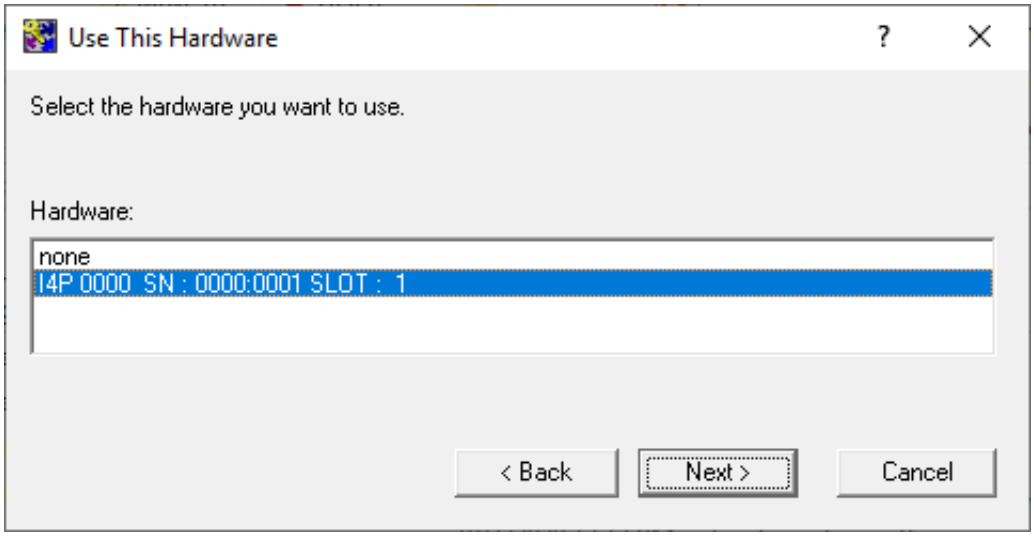
After Entrust Security Manager has been installed successfully, launch the Entrust Configuration Tool, which is available as `entConfig.exe` under the directory `C:\Program Files\Entrust\Security Manager\bin` (unless you changed the default installation settings). The tool walks you through the configuration of the Active Directory and Certification Authority integration, the database connection, and then asks you whether you want to generate the Certification Authority key using software or hardware.



Select the **Use hardware** option and click **Next**. A message will pop up telling you that no hardware device was found.



Click the **OK** button. A new dialog opens where you can select the driver file to be used to connect to the HSM – choose `mpcm-pkcs11.dll` from the directory where the Trident HSM files are located (in our example `C:\trident`). If the Entrust Configuration Tool successfully recognized the driver library, in the next step you have to select the slot you want to use.



Select the row representing the appropriate slot and click **Next**. In the following steps you have to specify the various characteristics of the Certificate Authority key and its management; see the Entrust Security Manager installation guide for the meaning and effect of these parameters. It is important to ensure that you set a key type which is compatible with Trident HSM.

Now the only task remaining is to initialize the Entrust Security Manager, which can be carried out by running the `init.cmd` script, again located in the directory `C:\Program Files\Entrust\Security Manager\bin`. The script will be run in its own terminal window, and right at the start will ask for the PIN code of the cryptoki user.

```
A Hardware Security Module (HSM) will be used for the CA key:
    I4P 0000  SN : 0000:0001
    The HSM requires a password.

Enter password for CA hardware security module (HSM): _
```

After you entered the PIN code, the script will immediately attempt to generate a Certification Authority key using Trident HSM. If you enabled logging to standard output by setting `log_to_std_output` to 1 in the Trident HSM configuration file (which is strongly recommended during the initial configuration), you can follow the various operations as they happen and their results. If you notice some error codes, you can check the MPCM Development Guide for their meanings and correct the configuration parameters accordingly.

If connecting to Trident HSM was successful, the script will prompt you for various initial passwords required for Entrust Security Manager, and then again perform several operations through the HSM. Successful completion of the script indicates that integration with Trident HSM works flawlessly, there is no need to do any additional testing in this regard. In order to improve the performance of the HSM driver, it is recommended to turn off detailed logging by changing the values of the `log_level` and `log_to_std_output` parameters in `mpcm_pkcs11.conf`.

6 Contacting i4p

If you have any questions about Trident HSM in general, encountered issues with integrating Entrust Security Manager with Trident HSM, or would like to share your ideas about how to improve this document, feel free to contact us

- via email: info@i4p.com
- via our homepage: https://www.i4p.com

In case you want to provide feedback regarding the document, please include the document title and version number (as shown in the footer).

Please use our support request form available at:

http://support.i4p.com