securosys

SWISS SECURITY TECHNOLOGIES
FOR COMMUNICATIONS SYSTEMS

# Securing Entrust Certificate Authority

## Using Primus Hardware Security Module

## Application Note

Primus HSM or CloudsHSM Integration Guide for
Entrust Certificate Authority (Security Manager 10, 8.3)

Securosys SA, Förrlibuckstrasse 70
CH-8005 Zürich, Switzerland
Tel. +41 44 552 31 00 • www.securosys.com
info@securosys.com

## Document Information and Revision Control

| Version | Date | Author | Description, Changes |
|---|---|---|---|
| 1 | 27.10.2021 | PM | Initial document |

File: PrimusHSM_EntrustCA-Integration_AN-E01.docx

## Copyright Notice

# Table of Contents

# 1 Introduction

This document describes how to integrate Securosys Primus HSM or CloudsHSM service with Entrust Certificate Authority (Security Manager 10 or 8.3), to generate and use Security Managers key material within the protected boundary of Securosys Hardware Security Modules.

## 1.1 Target Audience

This document is intended for HSM and Security Manager administrators or integrators.

## 1.2 References and More Information

[1] Primus HSM, PKCS#11 Provider User Guide, Edition 15 or newer

[2] Primus HSM User Guide for v2.10/v2.8 Edition 10 or later

[3] Entrust Certificate Authority, Security Manager documentation, multiple documents downloadable from your Entrust TrustedCare account https://trustedcare.entrust.com

[4] Securosys CloudsHSM Service
https://www.securosys.com/en/product/cloudshsm

All Securosys documentation is downloadable from the Securosys Support Portal.
All Entrust documentation is downloadable from your Entrust TrustedCare account.

## 1.3 Requirements

- Supported Software platform:
  All current Windows and Linux operating systems supported by Entrust Security Manager and Primus PKCS# Provider, see latest [1] Primus HSM, PKCS#11 Provider User Guide and Entrust documentation for details.
- Securosys Primus PKCS#11 Provider v1.7.36 or newer.
- Hardware Security Modules:
  Primus HSM or CloudsHSM Service (HSM as a Service), firmware v2.8.21, v2.9.2 or newer with PKCS#11 API and Session Object support enabled.

As of writing this application note, following algorithms were not supported by the HSM:

- CAST5
- All **twisted** Elliptic Curves (e.g. EC-prainpoolP256t1, …)

Please consult the latest PKCS#11 and HSM User Guides for algorithm updates.

### 1.4 Notations and Symbols

Configuration files, command lines and their output are boxed using `Consolas` font. Commands are printed **bold**, values to adapt by the user are marked in **`bold blue`**, and comments are marked in *`italic brown`*, e.g.

```
ppin -u -e HSM_USERNAME
…
Provide setup password for 'HSM_USERNAME':  <enter User Setup Password, no echo>
…
```

The appended plus sign in version references (e.g. v2.9+) indicates that described functionality or behavior applies from this version onwards (including newer versions).

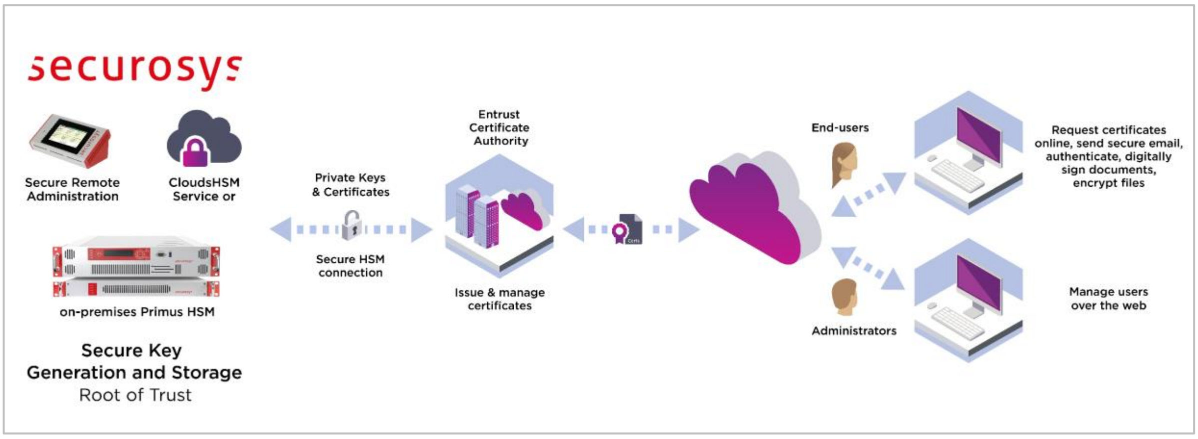
### 1.5 Support Contact

If you encounter a problem while installing/configuring the provider or integrating the HSM into the Entrust Security Manager, make sure that you have read the referenced documentation. If you cannot resolve the issue, contact your supplier or Securosys Customer Support. The Securosys Support Portal for registered users is reachable under https://support.securosys.ch .

### 1.6 Glossary

| Acronym | Definition |
|---|---|
| HSM | Hardware Security Module (physical or as a service) |
| CloudsHSM | HSM as a service, operated by Securosys |
| PKCS#11 | Public-Key Cryptography Standard #11 – API to cryptographic tokens |
| ECC | Elliptic-Curve Cryptography |
| AN | Securosys Application Note |
| UG | Securosys User Guide |
| PKI | Public Key Infrastructure |
| LDAP | Lightweight Directory Access Protocol |
| CA | Certification Authority |
| CRL | Certificate Revocation List |
| FIPS | Federal Information Processing Standard |
| CC | Common Criteria for IT Security Evaluation |
| ECASM | Entrust Certificate Authority Security Manager |

## 2 Architecture Overview


securosys
Secure Remote Administration
CloudsHSM Service or
on-premises Primus HSM
Secure Key Generation and Storage
Root of Trust
Private Keys & Certificates
Secure HSM connection
Entrust Certificate Authority
Issue & manage certificates
End-users
Administrators
Request certificates online, send secure email, authenticate, digitally sign documents, encrypt files
Manage users over the web

Entrust Certificate Authority (Security Manager), one of the leading public key infrastructures, allows organizations to easily manage the digital keys and certificates that secure user and device entities. Securosys Primus HSMs or CloudsHSM integrate easily with Entrust PKI to protect the confidentiality and integrity of sensitive keys. Organizations looking to extend the security of on-premises or hosted PKIs can deploy Entrust solutions in conjunction with on-premises Securosys Primus HSMs, or the ready-to-go CloudsHSM service via the Primus PKCS#11 provider. Securosys HSMs securely generate, store and manage CA private keys, ensure that critical keys are never exposed to unauthorized entities, and are required in case of strong compliance regulations.

Securosys provides affordable network Hardware Security Modules, up to highest requirements in performance, availability, and safety. Start your integration today using the CloudsHSM service, not having to care about setup or operation, and the possibility of later migration to on-site infrastructure.

Benefit from fast regional access, load-balancing, and automatic redundancy failover, thanks to built-in large geo-redundant HA cluster mechanisms.

Multi-tenancy and large built-in storage allow separation of different instances, and usage for future applications.

Minimize risk of exposure and operational failures by taking Root CA partitions off-line, and additional Security Officer intervention for key deletion.

Ease CA key ceremonies and automate audit procedures using Securosys Key Attestation and Audit features, proofing all keys and relevant parameters with a chain of trust originating from our Securosys root certificate.

All HSMs are developed and manufactured in Switzerland using a trusted supply chain and are certified according FIPS140-2 level 3 and CC EAL4+ (EN419221-5) to fulfill strongest compliance regulations.

Decanus allows for easy and cost-efficient remote management of HSM clusters and CloudsHSM partitions (2-of-n, 2FA) without compromising security.

# 3 Integration Procedures

This document refers to Entrust Security Manager 10 integrations. Nevertheless, most of the steps are analogously applicable for Security Manager 8.3 integration.

## 3.1 Securosys CloudsHSM or Primus HSM Setup and Configuration

Securosys CloudsHSM allows almost instant HSM operation by selecting and contracting the different services and options for your PKI project:

- Standard or certified operation (CC EAL4+, FIPS 140-2 level 3)
- Shared or dedicated HSM
- Preferred datacenter region(s)
- Required integration API: PKCS#11
- Optional: Decanus remote management, up to full control (configuration, backup/restore, key attestation and audit for regulatory requirements, offline partition)

For available service packages and options consult our website [4] Securosys CloudsHSM Service and contact Securosys sales.

For on-premises Primus HSM hardware, HA Cluster setup and operation in FIPS or Common Criteria certified modes, refer to the corresponding [2] Primus HSM User Guide for details.
Check also [1] Primus HSM, PKCS#11 Provider User Guide, chapter 2, on how to enable PKCS#11 API, configuring the PKCS# Password/PIN, and enabling session objects and further settings.

## 3.2 Securosys Primus PKCS#11 Provider Installation and Configuration

The [1] Primus HSM, PKCS#11 Provider User Guide, downloadable from the Securosys Support Portal, describes in detail the installation and configuration of the provider for the different operating system platforms. The examples below refer to a Windows Server platform.

### 3.2.1 Installing the Primus HSM PKCS#11 Provider

Install the latest version of Primus PKCS#11 provider on the Security Manager server, according [1] Primus HSM, PKCS#11 Provider User Guide chapter 3, depending on the used platform (Linux, Windows).

### 3.2.2 Configuring the Primus PKCS#11 Provider

Configure the Primus PKCS#11 provider by adapting the configuration file `primus.cfg` according your setup. Depending on your platform, the configuration file is located under

- Windows: `C:\Program Files\Securosys\Primus P11\primus.cfg`
- Linux: `/etc/primus/primus.cfg`

The following example shows the configuration file `primus.cfg` on Windows Server 2019 platform for a redundant partition named DEMO-ESM1 residing on CloudsHSM service.
The SERVICE_USER name depends on your CloudsHSM details:

```
#-----------------------------
# Primus PKCS#11 configuration
#-----------------------------
version = "1.0";

/*--- GLOBAL CONFIGURATION SECTION ---------------------------------------*/
primus:
{
  wait_delay = 250; /* in ms*/
  wait_max_tries = 5;

  /*--- HSM CONFIGURATION SECTION ----------------------------------------*/
  hsms:
  {
     hsm0:
     {
        host = "a-api.cloudshsm.com";
        port = "2310";
        slots:
        {
           slot0:
           {
             client_id  = "Entrust_Server ";
             user_name  = "DEMO-ESM1";
             proxy_user = "SERVICE_USER";            /* if proxy in use */
             id = 0;
           }; /* end slot0 */
        }; /* end slots */
     }; /* end hsm0 */

     hsm1:
     {
        host = "b-api.cloudshsm.com";
        port = "2310";
        priority = 1; /* Optional priority. Default 0 = highest priority */
        slots:
        {
           slot0:
           {
             client_id  = "Entrust_Server ";
             user_name  = "DEMO-ESM1";
             proxy_user = "SERVICE_USER";            /* if proxy in use */
             id = 0;
           }; /* end slot0 */
        }; /* end slots */
     }; /* end hsm1 */
  }; /* end hsms */

  /*--- LOG CONFIGURATION SECTION ----------------------------------------*/
  log:
  {
    file = "%PUBLIC%\Securosys\Primus P11\primus.log";  /* for windows */
    trace_linenumber    = false;     /* true or false */
    trace_timestamp     = true;     /* true or false */
    trace_function      = true;     /* true or false */
    trace_inout         = false;    /* true or false */
    trace_pid           = true;     /* true or false */
    trace_filename      = false;    /* true or false */
    trace_mask          = 0x00;
    trace_level         = 4;        /* 0-7 log level details */
  }; /* end log */
}; /* end primus */
```

For configuration value details or variants consult the [1] Primus HSM, PKCS#11 Provider User Guide, chapter 4.

### 3.2.3 Establishing HSM Connectivity

On initial setup and configuration of an HSM partition, the installation process (Security Officer of the HSMs) generates a partition **setup password** for a given user. The setup password is a 29-alphanumeric dash separated string in the form of "`FXAJX-XWVQ3-DC0O5-3SLQF-LJ9L3`" with **limited time validity** (HSM default: 3 days; CloudsHSM default: 1 week; developer account: 1 year).

This initial partition setup password is used to obtain or update a permanent secret stored in a ciphered form in the '`.secrets.cfg`' file using the '`ppin`' command line utility. From then on, the permanent secret is used to establish the secure connection between the PKCS#11 Provider and the user's HSM partition.

The PKCS#11 standard defines additionally a **PKCS#11 User PIN/Password** to perform certain operations (key usage, write, …).

In case of CloudsHMS, an additional **Service Proxy password**, an alphanumeric string in the form of "`ur7CUS3…9niuFP4m`" must be configured, before fetching the HSM permanent secret.

The `ppin` command line tool allows

- to manage the connection credentials for secure HSM communication (including service proxies)
- to show the installed provider version
- to fetch the partition log from configured HSMs

Use `ppin -h` for an overview of the different command parameters.

For details consult the [1] Primus HSM, PKCS#11 Provider User Guide chapter 5.

In case of CloudsHSM (using a Service Proxy) the **Service Proxy password** must be configured before fetching the HSM permanent secret, by using the `ppin` tool:

```
ppin -pe SERVICE_USER

*******************
Primus Permanent PIN
*******************
Provide proxy password for 'SERVICE_USER' : <enter Service Proxy Password, no echo>

*******************
Primus Permanent PIN
*******************
[01] slot-id 0:    user 'DEMO-ESM1'    permanent secret: MISSING
[02] slot-id 0:    user 'DEMO-ESM1'    permanent secret: MISSING
[01] service/proxy user 'SERVICE_USER' permanent secret: Configured
[02] service/proxy user 'SERVICE_USER' permanent secret: Configured
```

Now retrieve the permanent secret for 'DEMO-ESM1' via the service proxy, by using the ppin tool with User Setup password and PKCS#11 password:

```
ppin -ae DEMO-ESM1

*******************
Primus Permanent PIN
*******************
Provide setup password for 'DEMO-ESM1':  <enter User Setup Password, no echo>
Provide PKCS11 password for 'DEMO-ESM1': <enter PKCS#11 PIN/Password, no echo>
*******************
Primus Permanent PIN
*******************
[01] slot-id 0:     user 'DEMO-ESM1'    permanent secret: Configured
[02] slot-id 0:     user 'DEMO-ESM1'    permanent secret: Configured
[01] service/proxy user 'SERVICE_USER' permanent secret: Configured
[02] service/proxy user 'SERVICE_USER' permanent secret: Configured
```

Multiple different partitions are assigned to PKCS#11 slot ids and can be listed by the ppin tool:

```
ppin -l

*******************
Primus Permanent PIN
*******************
[01] slot-id 0:     user 'DEMO-ESM1'     permanent secret: Configured
[02] slot-id 1:     user 'DEMO-ESM2'     permanent secret: Configured
[03] slot-id 5:     user 'CLOUDSHSMPAR'  permanent secret: MISSING
[01] service/proxy user 'eqabxrfnqqos'  permanent secret: MISSING
```

Ensure that you have HSM connectivity to the necessary partitions using the following command[1]:

```
ppin --test
Load config file: '/etc/primus/primus.cfg'

hsm0: Connect to a-api.cloudshsm.com 2310, firmware: RX-2.10.0-T
          slot0 (id=0), user=DEMO-ESM1: OK
          slot1 (id=1), user=DEMO-ESM2: CKR_TOKEN_NOT_PRESENT
…
```

## 4 Installing Entrust Security Manager

Download the [3] Entrust Certificate Authority, Security Manager documentation package and software components. During the installation you may need to refer to the different guides contained in the documentation package.

For evaluations, Entrust provides a "Quick Start Installation Guide for Entrust PKI Certification Authority 10".

The following components are required for Entrust Security Manager according [3] Entrust Certificate Authority, Security Manager documentation, and your infrastructure and design requirements:

- Server infrastructure (Windows Server 2016 or 2019 fully licensed, or Linux Server)
- Database (e.g. PostgreSQL), see "Database Configuration Guide" for the list of SQL databases supported and their installation/configuration steps
- LDAP compliant Directory (e.g. AD LDS), see "Directory Configuration Guide" for the list of LDAP directories supported and their installation/configuration steps.

[1] ppin --test requires PKCS#11 provider v1.8+

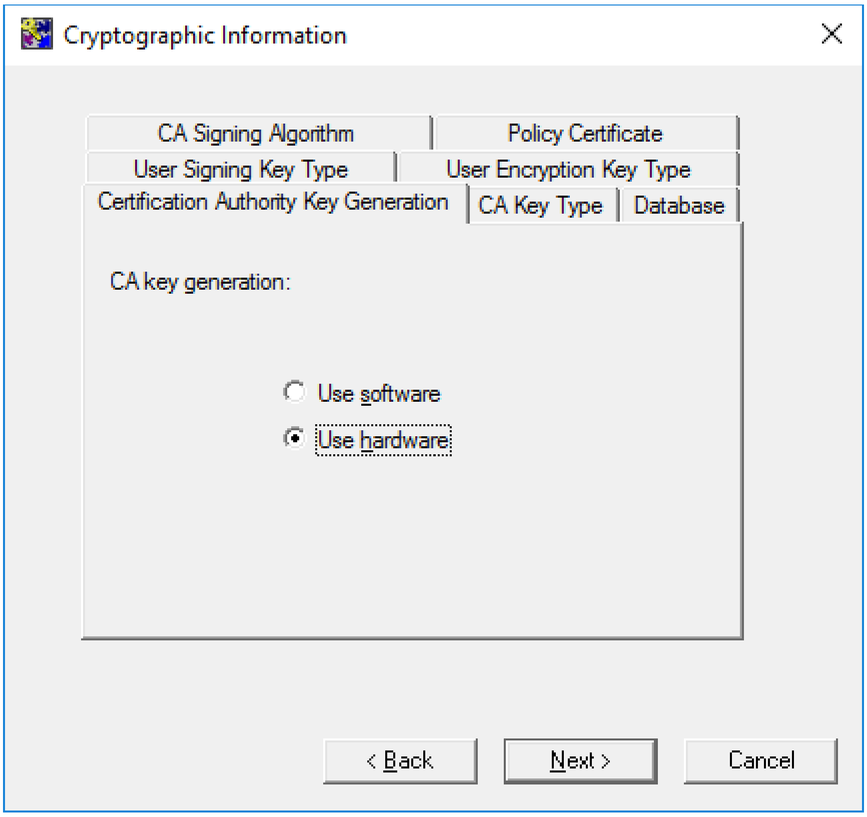
- Security Manager 10, see "Security Manager Installation Guide".
- Security Manager Administration 10, see "Security Manager Administration User Guide".

The following steps are an extract of the Security Manager Installation Guide.

- Plan for the Security Manager installation.  
  Plan and organize for a new Security Manager installation. Collect the installation and configuration data needed to install and configure the Security Manager infrastructure.
- Disable any anti-virus software to prevent conflicts for the duration of the installation process.
- Configure the operating system for Security Manager.
- Install and configure a supported **LDAP-compliant directory** as the Security Manager directory.
- Install a **supported database** as the Security Manager database.
- Install the **Primus PKCS#11 provider** to access Primus HSM or CloudsHSM (service) for storing cryptographic keys. Security Manager supports storing keys on a PKCS #11 version 2 HSM. Security Manager is a 64-bit application and requires 64-bit HSM drivers.  
  For details refer to chapter 3.1.
- (Linux only) Create groups and users for the Security Manager installation and your Master User accounts.  
  Security Manager requires a non-root user account to own the Security Manager installation. It is recommended that you also create groups and user accounts for your Master Users. The user accounts allow Master Users to log in to the server hosting Security Manager and use the software.
- Install the Security Manager software including patches.
- (Linux only) Configure directories used by Security Manager with the proper ownership and permissions so that you can configure Security Manager.
- Configure Security Manager (entConfig.exe) for the use with HSM/CloudsHSM (see chapter 4.1)
- (Optional.) Customize Security Manager files.  
  This is an optional step. You may want to configure some important settings before you initialize Security Manager.
- Initialize Security Manager.  
  You must initialize Security Manager before you can start using the PKI system.
- (Optional.) Distribute Security Manager Administration.  
  Security Manager Administration is the graphical interface for Security Manager.  
  You can distribute Security Manager Administration to your administrative users.  
  For information about installing Security Manager Administration, see the "Security Manager Administration User Guide".

## 4.1 Configure Security Manager to use the HSM (Windows Platform)

Run the Entrust Security Manager Configuration Utility with **administrator privileges**.  
At the point where you choose whether to store keys in software or hardware, select "Use hardware" and click [Next].

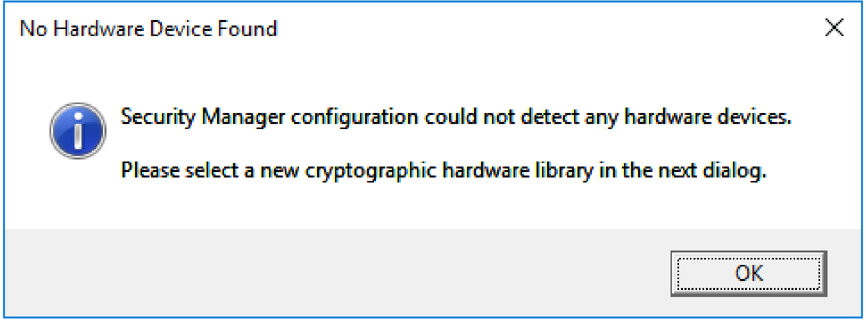


Cryptographic Information

CA key generation:

○ Use software
● Use hardware

Configure all the other settings (CA Key Type and sizes etc.) according your requirements until you get the following informational pop-up box:

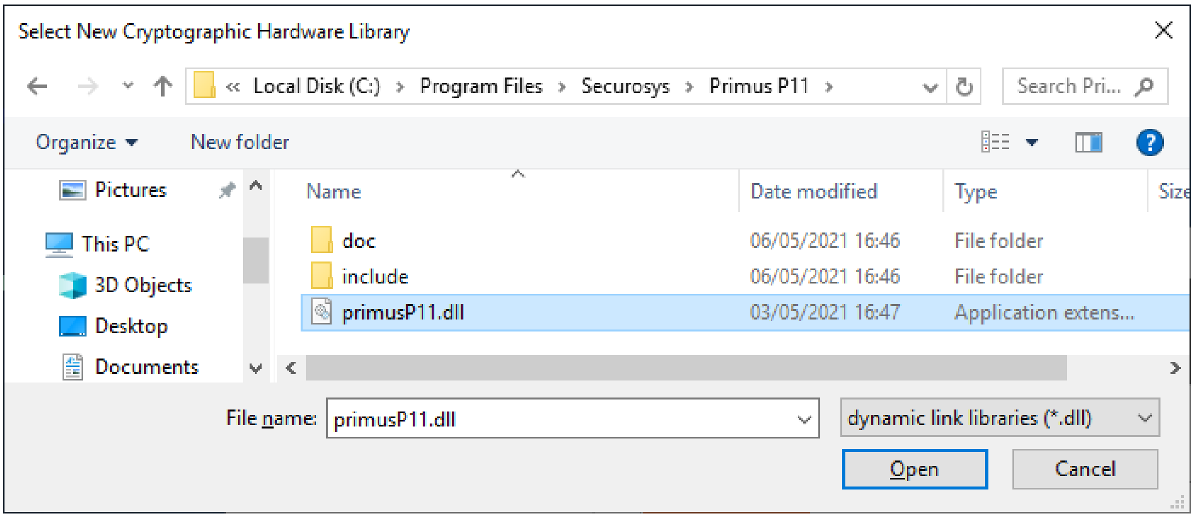


No Hardware Device Found

Security Manager configuration could not detect any hardware devices.

Please select a new cryptographic hardware library in the next dialog.

Click [OK] and point the file selector dialog to Primus HSM library path **C:\Program Files\Securosys\Primus P11\primusP11.dll** (on Windows).

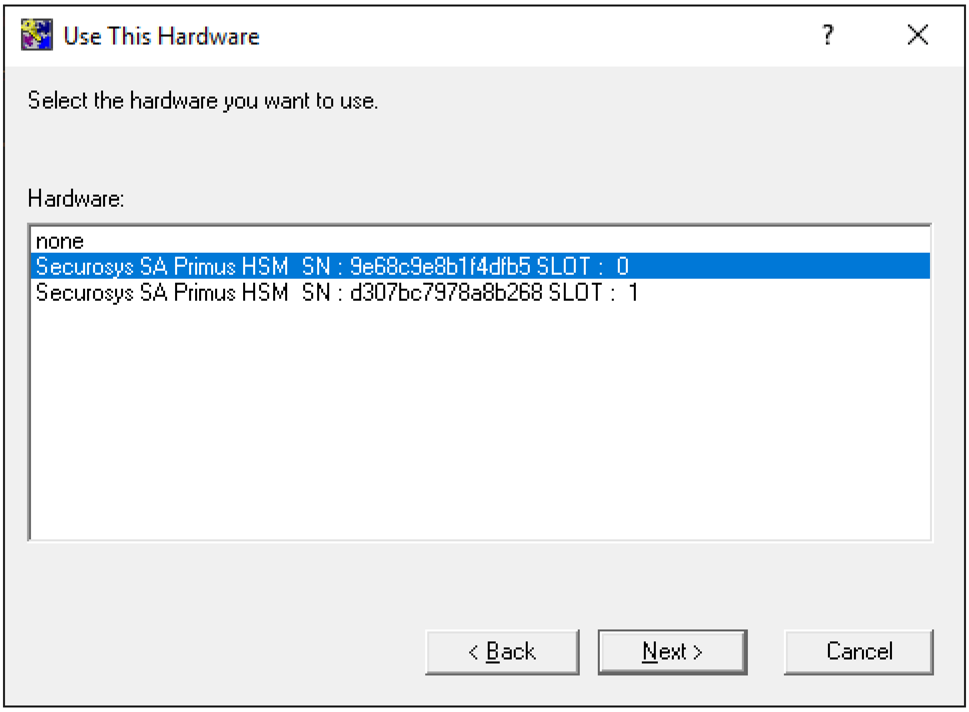


Select New Cryptographic Hardware Library

| Name | Date modified | Type | Size |
|---|---|---|---|
| doc | 06/05/2021 16:46 | File folder | |
| include | 06/05/2021 16:46 | File folder | |
| primusP11.dll | 03/05/2021 16:47 | Application extens... | |

File name: primusP11.dll

dynamic link libraries (*.dll)



Use This Hardware

Select the hardware you want to use.

Hardware:

none
Securosys SA Primus HSM SN : 9e68c9e8b1f4dfb5 SLOT : 0
Securosys SA Primus HSM SN : d307bc7978a8b268 SLOT : 1

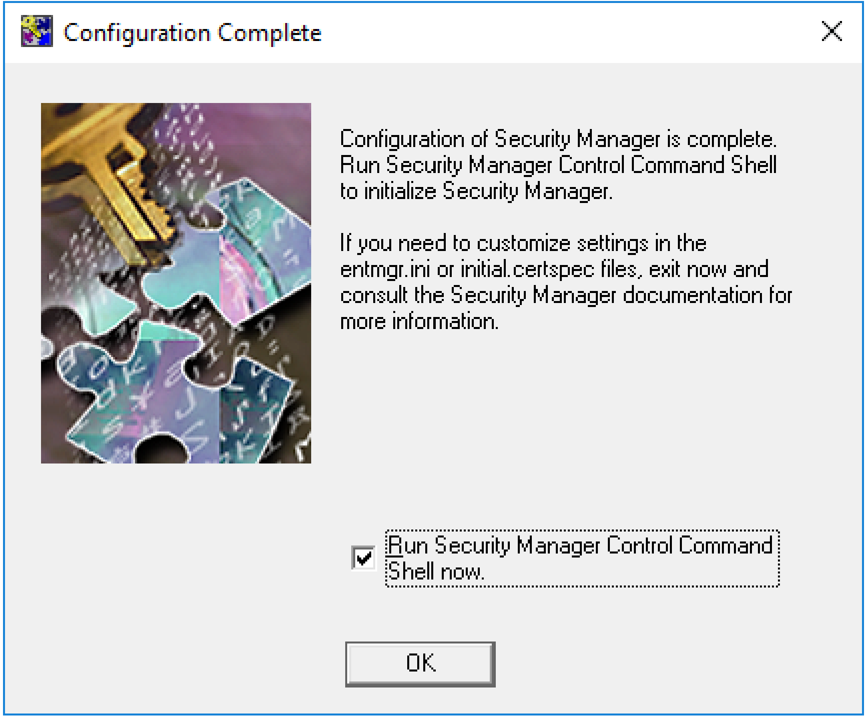
If you are not sure which partition is configured on which slot, use the ppin utility to list them:

```
C:\>"\Program Files\Securosys\Primus P11\ppin.exe" -l

*******************
Primus Permanent PIN
*******************
[01] slot-id 0: user 'DEMO-ESM1' permanent secret: Configured
[02] slot-id 1: user 'DEMO-ESM2' permanent secret: Configured
```

Continue the Entrust Security Manager Configuration utility following the Entrust documentation.

At the end activate the tick "Run Security Manager Control Command shell now."



Configuration Complete

Configuration of Security Manager is complete. Run Security Manager Control Command Shell to initialize Security Manager.

If you need to customize settings in the entmgr.ini or initial.certspec files, exit now and consult the Security Manager documentation for more information.

☑ Run Security Manager Control Command Shell now.

Or run initialization from the command line after applying customizations to your configuration (administrator privileges required):

```
C:\>"\Program Files\Entrust\Security Manager\bin\Init.cmd"

Starting First-Time Initialization...

A Hardware Security Module (HSM) will be used for the CA key:
    Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5
    The HSM requires a password.

Enter password for CA hardware security module (HSM):  <PKCS#11 password>
Enter new password for Master1:                         <password of Master1>
Confirm new password for Master1:                       <password of Master1>
Enter new password for Master2:                         <password of Master2>
Confirm new password for Master2:                       <password of Master2>
Enter new password for Master3:                         <password of Master3>
Confirm new password for Master3:                       <password of Master3>
Enter new password for First Officer:                   <password of First Officer>
Confirm new password for First Officer:                 <password of First Officer>

Initialization starting; creating ca keys...
Initialization complete.
Starting the services...
Creating CA profile...
Creating First Officer profile...
You are logged in to Security Manager Control Command Shell.
Performing database backup...
NOTICE:  pg_stop_backup complete, all required WAL segments have been archived
SUCCESS: Full backup completed successfully.
Press return to exit
```

During the above initialization procedure Security Manager requests the HSMs PKCS#11 password, definition of the other Security Manager users, and initializes the CA key on the HSM partition:

```
CA Signing Key RSA 2048
sensitive,nonextractable,modifiable,noncopyable,token,nonindestructible,private,nonpubli
c,neverextractable,alwayssensitive,local,notdecrypt,sign,notunwrap,notderive,notintegrit
y,notsignrecover
```

Start the Security Manager Control Command Shell, login as Master, and check the ca key location with the command `ca key show-cache`:

```
Entrust Authority (TM) Security Manager Control Command Shell 10.0.1(4)
Copyright 1994-2020 Entrust. All rights reserved.

Type 'help' or '?' for help on commands
entsh$ login
Master User Name: Master1
Password:
You are logged in to Security Manager Control Command Shell.
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ ca key show-cache
**** In Memory CA cache ****
Record Status Legend:
  C = current key
  H = key on hold
  A = non-current key
  X = revoked or expired non-current key has been obsoleted
  HWV1 = hardware key PKCS11 V1 *** NOT SUPPORTED ***
  HWV2 = hardware key PKCS11 V2
  SW = software key

------------------------------------------------
```

```
Internal key index:          1
CA certificate issued by:    cn=myCA,cn=ESM10,o=SECUROSYS,c=CH
serial number:               00E9B0EC89BF1797EA43378777500487A0
current CA certificate:      Y
CA certificate issue date:   Tue Jun 22 09:18:30 2021
CA certificate expire date:  Sun Jun 22 09:48:30 2031
subject key identifier:      176B0A1AEBBA3E5A736E09C5ECAC9E5B0FD570F0
private key active:          Y
private key expired:         N
certificate expired:         N
certificate revoked:         N
revocation details:          N/A
key:                         RSA-2048
global signing policy:       RSA-SHA256 (sha256WithRSAEncryption)
record status in database:   C HWV2
migrated:                    N
hardware load error:         N
hardware CKA_ID:             uCf0zZdQ+Vw4lhPlC2Z7NBC+DFg=
hardware status: Loaded >> 'Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5 SLOT :  0'.

---------------------------------------------------
**** End of In Memory CA cache ****
```

And the command `ca key show-cahw -type all`:

```
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ ca key show-cahw -type all

EAC is not enabled. There is no associated cryptographic hardware for EAC.


**** Hardware Information ****

---------------------------------------------------

Name:
Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5 SLOT :  0

Has current X.509 CA key: Y
Load Status:              hardware loaded ok
Uses Password:            Y
DB protection HW:         N
In use for X.509 CA keys: Y
In use for EAC keys:      N
ECDSA style:              2 (use minimal left-padded truncated digest)

---------------------------------------------------
**** End of Hardware Information ****
```

## 4.2 Configure Security Manager to use the HSM (Linux Platform)

Create the user who will own the Entrust Security Manager installation and add it to the primus HSM user group (or vice versa).

Install the database according the Entrust documentation.

Run the Entrust Security Manager Configuration Utility. At the point where the system asks you if you would like to use a hardware device for the CA keys, type **Yes**.

Point to the Primus HSM library path (or according your installation):
`/usr/local/primus/lib/libprimusP11.so`

The Security Manager Configuration Utility presents the option to use a PKCS#11 slot with a given serial number. Select the correct slot for your CA keys.

Complete Security Manager Configuration Utility according Entrust documentation.

Initialize the Security Manager for the first time, using the Security Manager Master Control Command Shell. After requesting the HSM partitions PKCS#11 password, add the passwords for Master1, Master2, Master3 and the First Officer user. The Security Manager generates the CA keys on the Primus HSM partition.

Start the Security Manager Control Command Shell, login as Master user and check the keys with the following command:

```
ca key show-cache
```

### 4.3 Apply Database Encryption with Keys on the HSM

Enabling database hardware encryption with keys on the HSM provides another layer of security.

**Caution:** the following procedure invalidates any previous database backups!

Start the Security Manager Control Command Shell, login as Master user, stop the services and apply the command `db hw-protection enable -alg <algorithm to use>` and restart the service:

```
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ service stop
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ db hw-protection enable -alg AES-CBC-256
Checking cluster status...

When you enable hardware-based database protection, Security Manager generates a new key
on the hardware device and
uses the new key to secure sensitive information in the database. Security Manager uses
a new hardware key even if
hardware-based database protection was previously enabled and an associated hardware key
exists on the hardware device.
As a result, enabling hardware-based database protection invalidates existing backups of
your hardware device. After
enabling hardware-based database protection, you will need to make a new backup of your
hardware device. Proceed (y/n) ? [n] y
Select the destination for the database key.
Choose one of:
1. Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5 SLOT :  0
2. Securosys SA Primus HSM  SN : d307bc7978a8b268 SLOT :  1
3. Cancel operation
> 1
Hardware-based protection for database enabled.
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ service start
```

Database hardware encryption generates a new key on the HSM partition:

```
dbprotkeyLgj3Kx56mfHxGr6c AES 256
sensitive,nonextractable,modifiable,noncopyable,token,nonindestructible,private,nonpubli
c,neverextractable,alwayssensitive,local,encrypt,decrypt,sign,verify,wrap,unwrap,derive
```

At the next login, the HSM partition PKCS#11 password will be requested:

```
entsh$ login
Enter password for: 'Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5'.
Password: <PKCS#11 password>
Master User Name: Master1
Password:
You are logged in to Security Manager Control Command Shell.
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $
```

You can also check with the following commands where the database key is stored:

```
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ db hw-protection query
Hardware-based Database Protection:  ON
Hardware Protection Mode:            CLASSIC
Hardware Description:                Securosys SA Primus HSM
Hardware Serial Number:              9e68c9e8b1f4dfb5
Encryption Algorithm:                AES-CBC-256
```

```
cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ ca key show-cahw -type all

EAC is not enabled. There is no associated cryptographic hardware for EAC.


**** Hardware Information ****

----------------------------------------------------

Name:
Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5 SLOT :  0

Has current X.509 CA key: Y
Load Status:              hardware loaded ok
Uses Password:            Y
DB protection HW:         Y
In use for X.509 CA keys: Y
In use for EAC keys:      N
ECDSA style:              2 (use minimal left-padded truncated digest)

----------------------------------------------------
**** End of Hardware Information ****
```

# 5 Add Primus HSM or CloudsHSM to an existing Security Manager Installation

To add Primus HSM or CloudsHSM to an existing Security Manager installation, perform the following steps:

- Install and configure the Primus PKCS#11 provider according to chapter 3.1.
- Adapt the file authstartup.ini and add the following settings to the configuration file (default location: C:\authdata\manager; SM8.3 the file is called entmgr.ini):
  - For Windows:

    ```
    [Entrust Settings]
    CryptokiV2LibraryNT=C:\Program Files\Securosys\Primus P11\primusP11.dll
    ```

  - For Linux

    ```
    [Entrust Settings]
    CryptokiLibrary=/usr/local/primus/lib/libprimusP11.so
    ```

- Restart the Security Manager Control Command Shell and check that the Securosys HSM is seen
  - Start a new Security Manager Control Command Shell, login as Master user, and run

    ```
    cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ util hwinfo
    Attempting to load C:\Program Files\Securosys\Primus P11\primusP11.dll
    C:\Program Files\Securosys\Primus P11\primusP11.dll: Version reported is 2.40
    ```

- Consider a CA key update (refer to the Entrust documentation for CA key update impacts)
  - Login to Security Manager Control Command Shell as Master user and perform `CA Key Update`, and select the Primus HSM partition to generate and store the new CA key:

    ```
    cn=myCA,cn=ESM10,o=SECUROSYS,c=CH.Master1 $ ca key update

    Select the destination for the new CA key.
    Choose one of:
    1. Software
    2. Securosys SA Primus HSM  SN : 9e68c9e8b1f4dfb5 SLOT :  0
    3. Cancel operation
    > 2
    Enter password for CA hardware security module (HSM): <PKCS#11 password>
    Checking cluster status...

    The cluster will be stopped and the CA key updated.
    Do you wish to continue (y/n) ? [y] y
    Stopping cluster...

    100% complete. Estimated time remaining -:-:- |

    CA key and certificate successfully updated.
    Recovering CA profile...
    Starting cluster...

    CA profile successfully recovered.

    It is recommended that all revocation lists be re-issued. This can be done later
    with the 'rl issue' command. Re-issue revocation lists now (y/n) ? [y]

    Issuing CRLs, please wait ...

    1 CRL(s) were issued.
    1 ARL(s) were issued.
    1 combined CRL(s) were issued.

    Publishing CRLs, please wait ...
    ```

- Apply database encryption with keys on HSM according chapter 4.3.