SafeNet Authentication Service PCE/SPE with Support for HSM PSE 2 Integration

Feature Documentation

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-013558-001, Rev. C

Release Date: February 2017

Table of Contents

1

Hardware Security Module and SafeNet Authentication Service

Introduction

A Hardware Security Module (HSM) is a physical crypto-processing device that securely manages and stores digital keys used during transactions, for identification, and applications' access. The Hardware Security Modules (HSMs) act as trust anchors protecting things such as websites, banking systems, mobile devices, smart meters, medical devices, national identity cards, credit card data, PINs, mobile payments, digital documents, and passports. It protects the cryptographic infrastructure by provisioning encryption, decryption, authentication, and digital signing services.

Gemalto's SafeNet ProtectToolkit (PTK) is a Public Key Cryptography Standards (PKCS) compliant device that incorporates features developed through extensive experience, implementing best practices in hardware, software, and operations. The PTK HSMs are easy to deploy, and adhere to rigorous design requirements, stringent product verification, and testing.

The PTK supports two hardware components:

1. ProtectServer External (PSE): Cryptographic adapter; an external network device
   [Latest, supported version of the product is version 2 (v2), and the product is usually referred to as, PSE 2]
2. ProtectServer Internal (PSI-E): Cryptographic adapter; a plug-in card

Hardware Security Module with SafeNet Authentication Service

The SafeNet Authentication Service (SAS) server uses AES encryption key of the PTK HSMs for encrypting sensitive data.

WARNING: Once an HSM is enabled, the operation cannot be undone since it is a one-way, irreversible process. Therefore, we recommend using a minimum of two HSM devices with appropriate backups.

This document provides information on the PSE 2 configuration and settings on the SAS server. The process broadly involves the following three steps:

1. Setting up PSE 2 Device
2. Setting up HSM Components

3. Configuring HSM Settings in SAS

Compatibility Information

Supported Hardware Versions

A PSE 2, with the following particulars, is compatible with the SAS solution:

Model: PSI-E2:PL1500
Firmware Version: 5.00.02

Note: Other minor firmware versions are also compatible.

Supported Software Versions

The following versions are compatible with the SAS solution:

- PTKnethsm Version 5.2.0
- PTKcpsdk Version 5.2.0

Supported Databases

This General Availability (GA) release supports the following databases:

- MySQL 5.7
- MS SQL 2012
- MS SQL 2014
- PostgreSQL 9.3

Supported Operating Systems

This GA release supports the following operating systems:

- Windows Server 2012 R2
- Windows Server 2008 R2

Setting up ProtectServer External 2 Device

The setup is a one-time activity and needs to be completed on the PSE 2 device. To set the network configurations, connect a monitor and a keyboard to the PSE device.

To set up a PSE 2 device, complete the following steps:

1. Login: Login as root with the default password (as `password`).
2. Adjust Network Configurations: Assign an IP address to ETH0 interface in `/etc/sysconfig/network-scripts/ifcfg-eth0` file.
3. Add Hostname: Add a hostname of the system to `/etc/sysconfig/network` file.
   Example: HOSTNAME=examplename
4. Add Default Gateway: Add the default gateway to `/etc/sysconfig/network` file.
   Example: GATEWAY=192.168.1.1

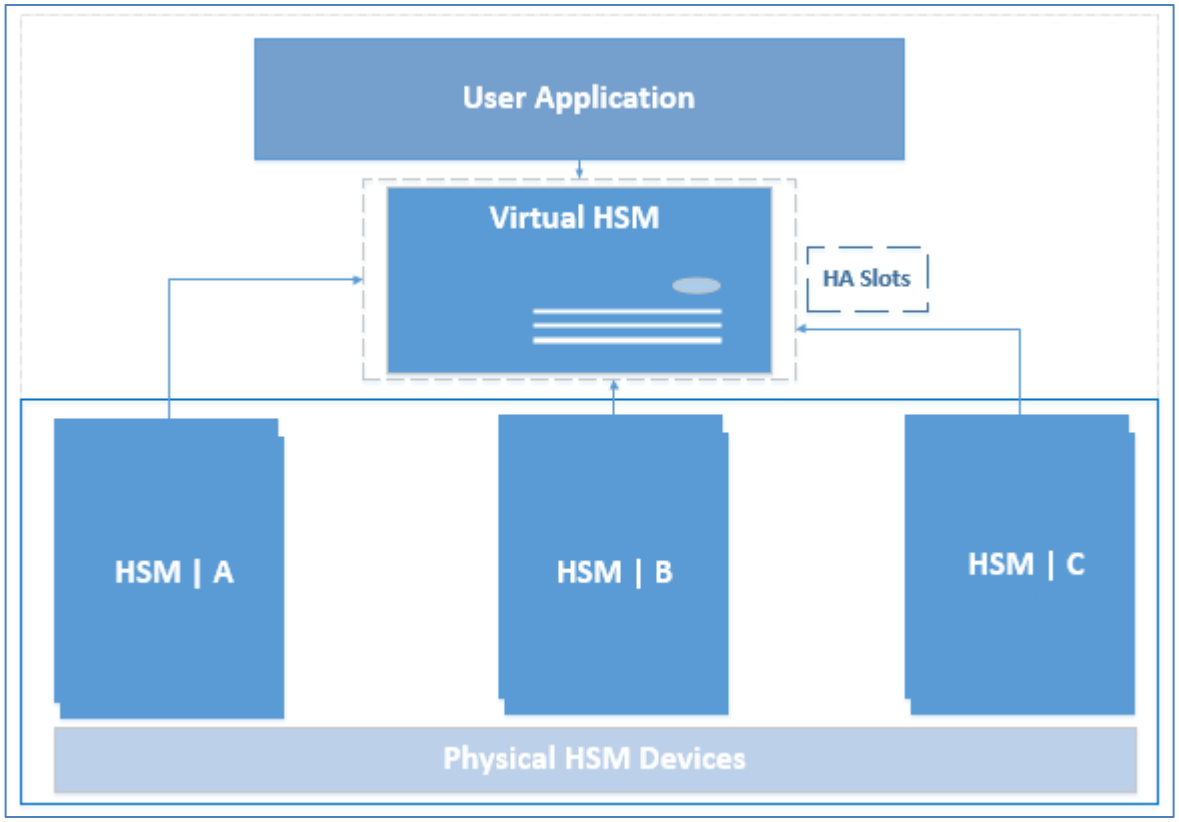
5. Add Domain Name System (DNS): Add DNS to `/etc/resolv.conf` file.
   Example: nameserver x.x.x.x
6. Add HSM: Add HSM servers to `/etc/hosts` file.
   Example: 192.168.1.x examplehost examplehost.domain.internal
7. Restart: Reboot the network (`/etc/init.d/network restart`) to set the changes.

   Note: When the machine restarts, you can connect via Secure Shell (SSH) using the Administrator login details (default password: `password`).

2
Setting up Hardware Security Module in Normal Mode

Prerequisite: This procedure assumes that the SAS server is already installed, and running on the system. If the SAS server is not installed, install it by following the instructions provided at the following link: **http://www2.gemalto.com/sas/implementation-guides.html**.

During setup, different applications and utilities must be able to access the HSM slots directly. The HSMs are initially configured to operate in the **Normal** mode. After the initial setup is complete, the utilities that need access to the system in **High Availability** (**HA**) mode must be configured.
The HA mode is required for mission-critical applications that require uninterrupted uptime. It allows multiple HSM devices to be grouped together to form a virtual device, ensuring that the service is maintained even if one or more physical devices is unavailable.
The HA slots are required since they act as virtual slots between the physical HSM(s) and the user application. An HA slot shares the same token label as the HSM slot (associated with it), and thus talks with the user application on behalf of the HSM. The following figure illustrates the schema.



Installing and Configuring Protect Toolkit C Package

To install and configure the Protect Toolkit C (PTKC) package, complete the following steps:
The steps need to be completed on the SAS server, and all other sites for that SAS instance.

Optional Step: To allow the ability to readdress PSEs in the future, add HSM entries in the `hosts` file on your machine by following the instructions:

a. Navigate to the following path: `C: > Windows > System32 > drivers > etc`

b. Locate the `hosts` file, open it using a Notepad, and add the HSM entries.

1. Install **Network HSM Access Provider** (`PTKnethsm.msi`) package version 5.2.0. To install, follow the steps:

   a. Visit Service Portal (**https://serviceportal.safenet-inc.com**).

   b. Login using your **User ID** and **Password**.
   Note: If you are not registered, register as a **New User** at the portal, using your Customer Identifier Number (CIN).

   c. Search Document ID **DOW4210** in the Knowledge Base, and download.

   d. Install the required package (`PTKnethsm.msi` package version 5.2.0) only.

   The Access Provider package enables connection to one or multiple HSMs. It acts as a data abstraction layer for which you can add multiple front-end Application Program Interfaces (APIs). To install, use the `PTKnethsm.msi` file, with default settings, and continue clicking next until the **Protect Server Setup** popup window is displayed.

Provide the HSM IP or Fully Qualified Domain Name (FQDN), and click **OK**.

Ensure that the IP address here must belong to the HSM **device 0**.
The HSM **device 0** is the first HSM machine that the Administrator is configuring.

Notes

- If the installer is executed from a Network Share, the Protect Server Toolkit 5.2 Win64 packages do not install on 2012 R2.
  Copy the installer files to the local drive first, and then install.

- For **Network HSM Access Provider** package to run, the .NET Framework 3.5 is required.
  If you do not have the framework, download it from the following link:
  https://www.microsoft.com/en-in/download/details.aspx?id=21

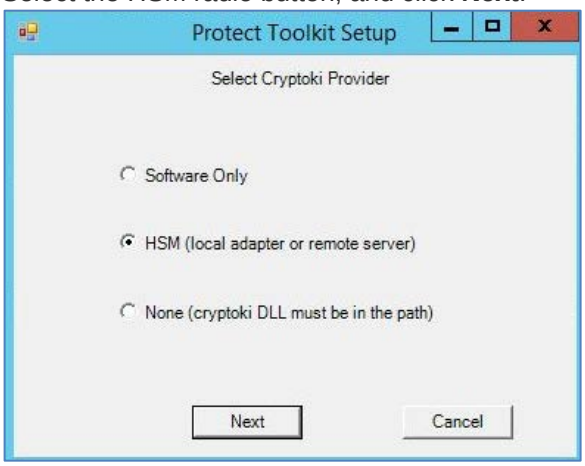
2. Install PTKC (`PTKcpsdk.msi`) package version 5.2.0. To install, follow the steps:
   a. Visit Service Portal (**https://serviceportal.safenet-inc.com**).
   b. Login using your **User ID** and **Password**.
      Note: If you are not registered, register as a **New User** at the portal, using your Customer Identifier Number (CIN).
   c. Search Document ID **DOW4210** in the Knowledge Base, and download.
   d. Install the required package (`PTKcpsdk.msi` package version 5.2.0) only.

   The toolkit provides the pkcs#11 interface and talks to the access provider, which in turn routes the request to the HSM. The SAS server uses the pkcs#11 interface.

   Follow the steps for installation:

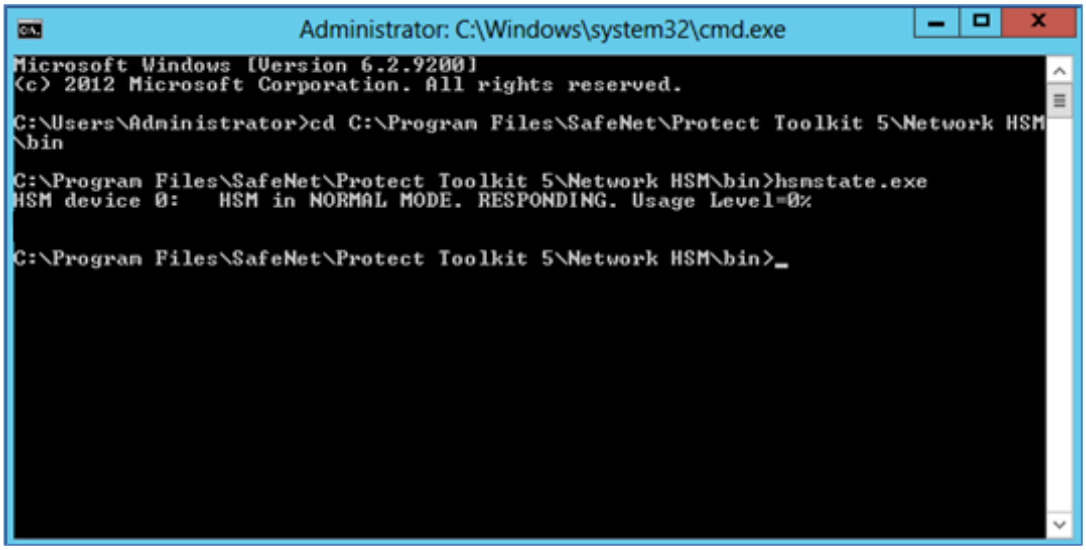
   a. Run `PTKcpsdk.msi` file, with default settings, and continue clicking next until **Select Cryptoki Provider** popup window is displayed.

b. Select the HSM radio button, and click **Next**.



c. Continue clicking next, till the installation process completes.

3. Check if **device 0** is responding or not, by executing `HSMstate.exe` file, available at the following path: `C:\Program Files\SafeNet\Protect Toolkit 5\Network HSM\bin`



4. Restart the server to reflect changes.

Before the HSM can be configured in the SAS solution, **Slot Creation and Initialization** must be completed.
Note: If you require creating a key manually, or edit its attributes, refer **Manual Key Generation** section on page 25.

Creating and Initializing Slot

Install the Java Runtime Environment (**https://www.java.com/en/download/manual.jsp**; x64).
If you do not install the Java environment, the following two batch files will not execute:

- `gCTAdmin HSM.bat`
- `KMU HSM.bat`

In such a case, the Administrator is required to use the Command Line Interface (CLI) to configure the HSM.

Navigate to the following path:
`C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

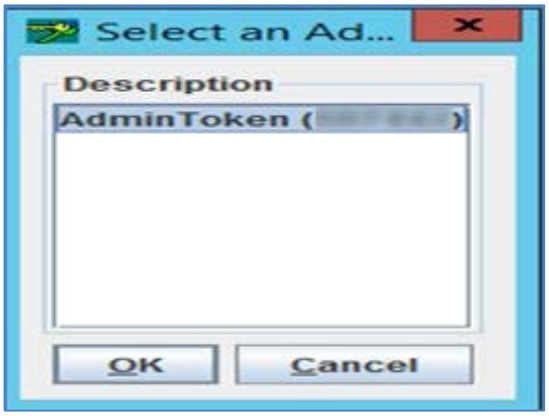
Follow the steps based on whether you are using the **Graphical User Interface (GUI)** or **Command-Line Interface (CLI)**.

Note: The HA setup will work only if the keys are replicated on Slot 0 of **device 0** HSM.

Graphical User Interface Method

i. To open, double-click the `gCTAdmin HSM.bat` batch file.

ii. In **Select an Adapter** dialog box, select **AdminToken** option, and click **OK**.

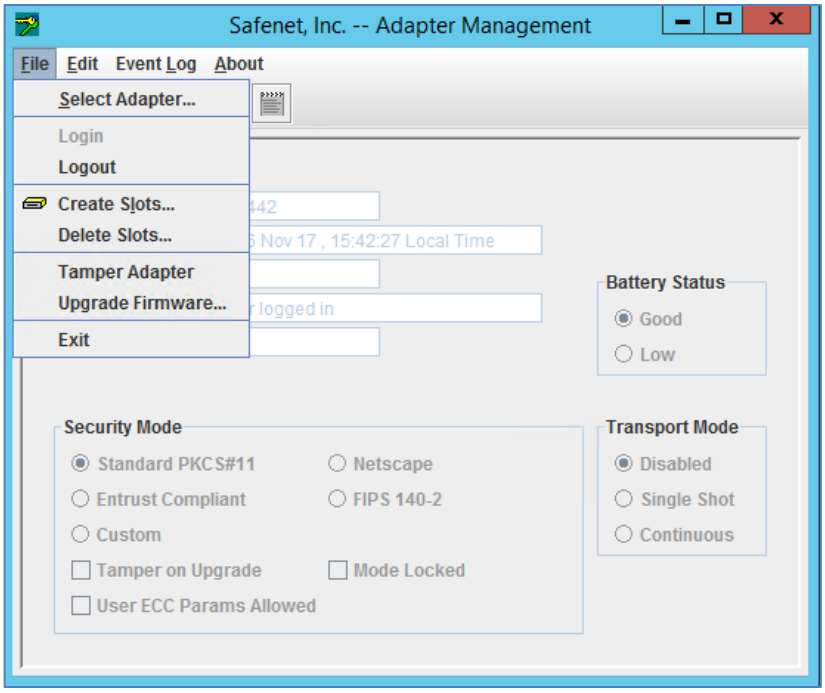


Note: If you are unable to select an Adapter, **set environment variables** first.

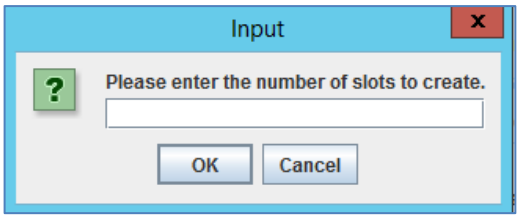
iii. Enter **PIN** in the **Enter PIN** popup window, and click **OK**.

Note: This is the same PIN as generated while **setting up PSE 2 device**.

iv. For slot creation, navigate to **File** > **Create Slots**.



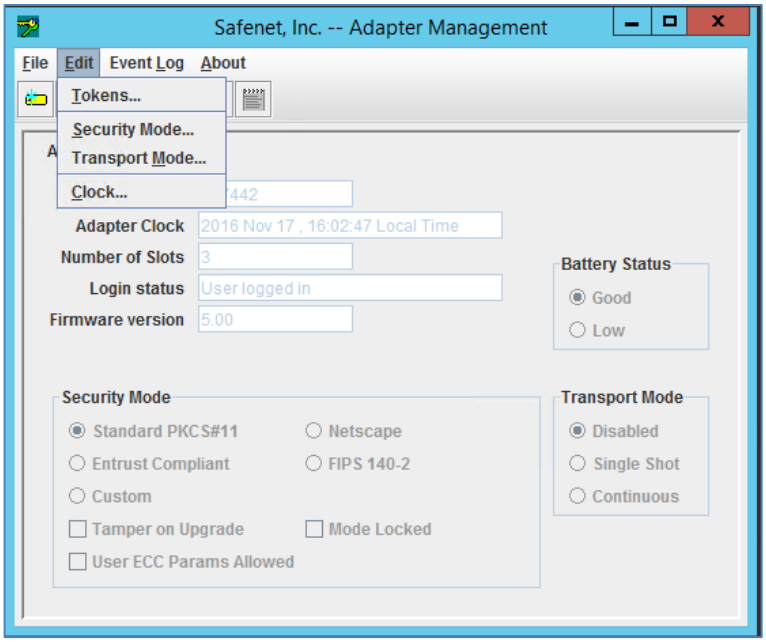
v. Enter the number of slots to be created in the **Input** popup window, and click **OK**. The tokens will be created with uninitialized slots.



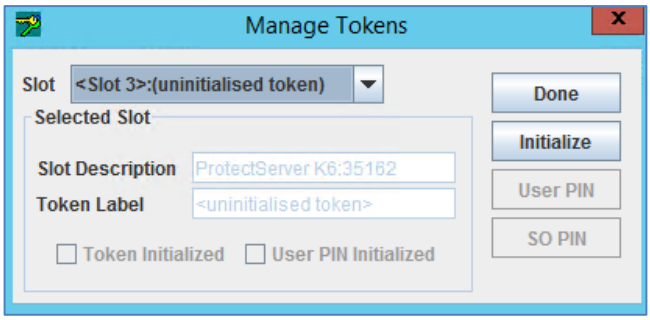
Example: If an Administrator enters **1** in the field, and click **OK**, one token will be created with an uninitialized slot.

vi. The **Adapter Management** window will restart. The Administrator needs to enter the Admin PIN.

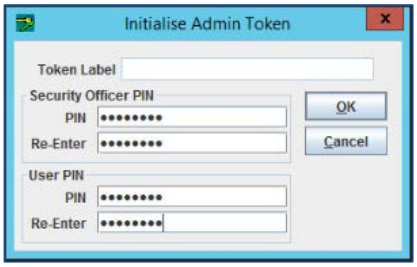
vii. To view the uninitialized slot, navigate to **Edit** > **Tokens**.



viii. Select the uninitialized slot in the **Manage Tokens** popup window, using **Slot** dropdown menu, and click **Initialize** to initialize a slot.



ix. In **Initialise Admin Token** window, provide the **Security Officer PIN** and **User PIN**, and click **OK**.



Note: If an Administrator wants to change PIN for a slot and is using the HA mode, the Administrator should manually change the User PIN for that slot in both HSMs or change the User PIN for one HSM and replicate the slot into another HSM using Command-Line Interface.

Command-Line Interface Method

i. To create an uninitialized slot, execute the following command:

```
Ctconf –a<0,1,2> –c1
```

Where; the first connected HSM device is numbered 0, the second as 1, and so on.
Example: If there are two HSM devices to be configured, the following command sequence should be followed:

```
Ctconf –a0 –c1

Ctconf –a1 –c1
```

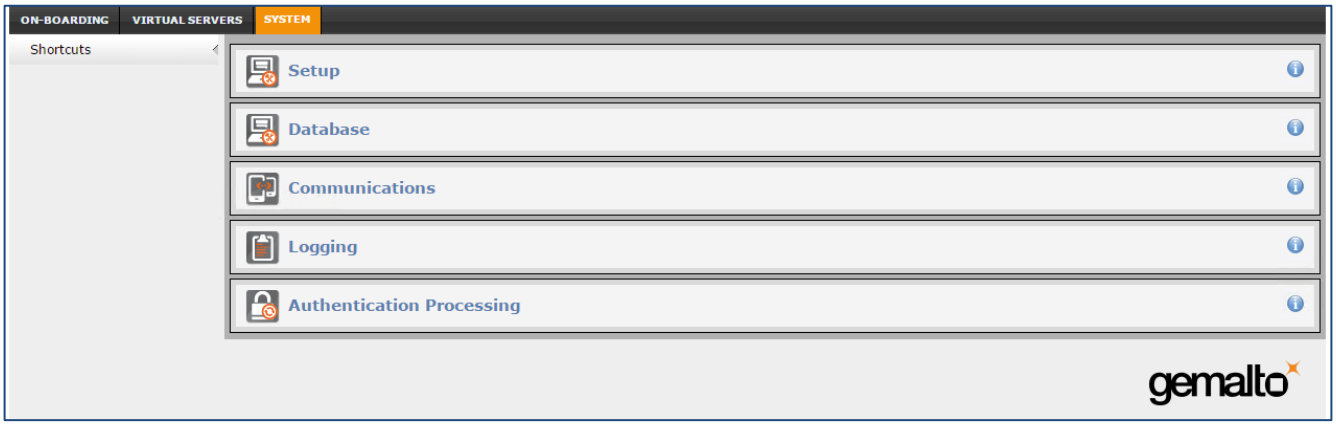
ii. Execute the following command to configure the slot or re-initialize it, if it is already configured:
`ctkmu t –s<slot number>`
Example: `ctkmu t –s0`

Configuring Hardware Security Module in SafeNet Authentication Service

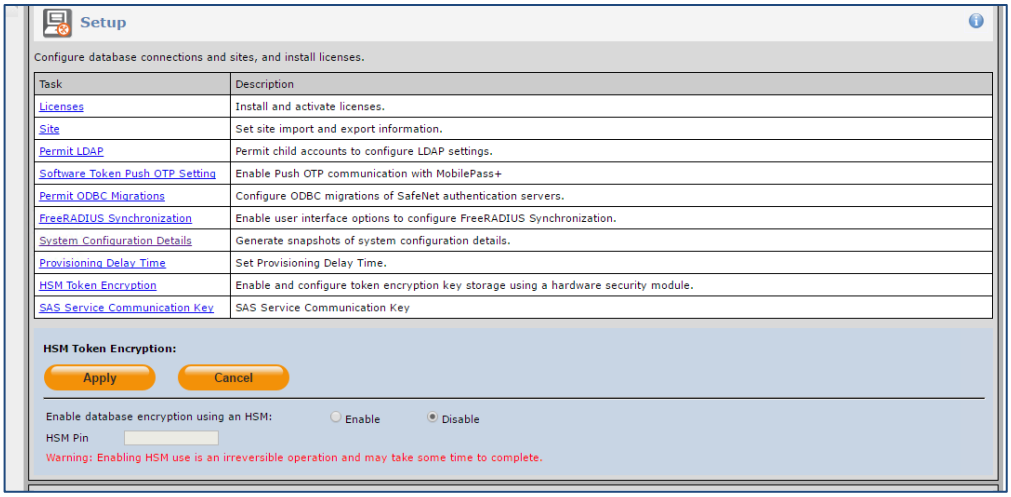
NOTE: For fresh SAS installs (installed and enabled), the HSM encryption is applied. For existing SAS setups, the untouched data is not encrypted till a modification call is made. Once the data is modified, the HSM encryption is applied to it. Existing data may never be encrypted if it doesn't change.

To start encrypting the data, perform the following steps:

1. Login to the SAS console as an Administrator.

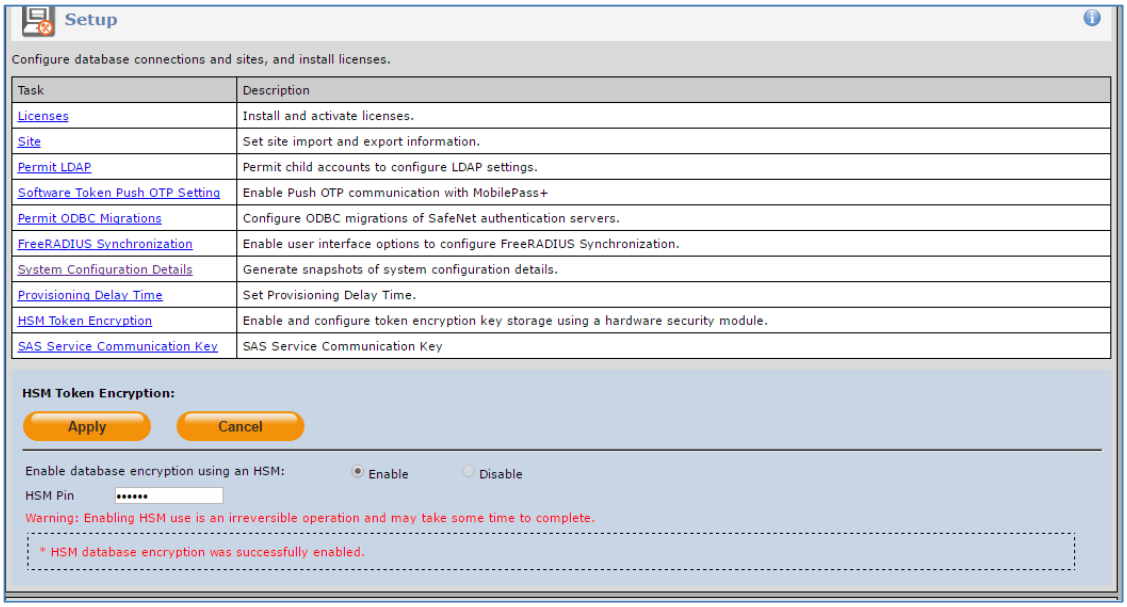


2. Click **SYSTEM** tab and select **Setup**.

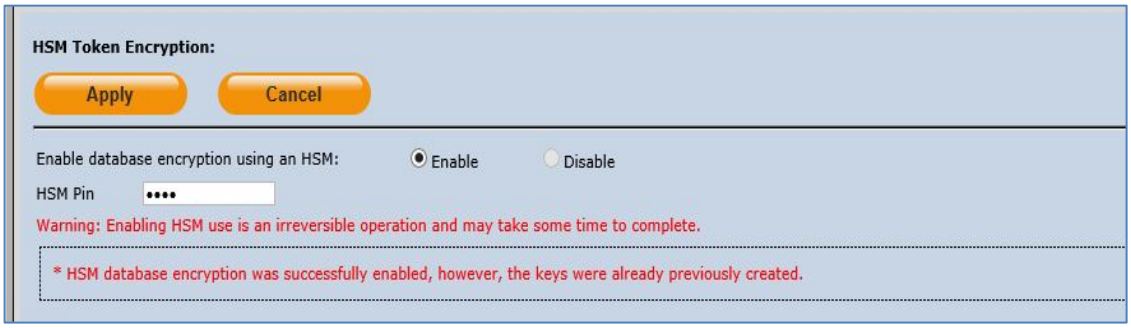


In **Setup** module, click **HSM Token Encryption** link (under the **Task** column).

3. Select **Enable database encryption using an HSM** radio button, provide **HSM PIN** and then click **Apply**.



4. On clicking **Apply**, a key will be generated automatically. If a key is already present in the HSM (or in the case of a PIN update), an appropriate message(s) will be displayed.



Notes:

- If you want to create a key manually or edit its attributes, refer **Manual Key Generation** section on page 25.

- If you are reinstalling the SAS solution, the HSM registry setting `ET_PTKC_GENERAL_LIBRARY_MODE` will default to **Normal** even if it was set as **HA**, before the reinstallation.
  Before continuing, change the setting `ET_PTKC_GENERAL_LIBRARY_MODE` to **HA**.
  Also, `ET_PTKC_WLD_SLOT_0` will default to **SASHSMSlot 0,0,Description**, and needs to be changed to slot label of the HA slot (as described in point 7 of **Configuring Virtual High Availability Slots**).

WARNING: Enabling HSM (with the SAS solution) is a one-way, irreversible operation that cannot be undone.

SAS Site Import

If the HSM is enabled on the primary SAS server, and the administrator wants to import an SAS site on the secondary SAS server, the administrator must perform the following steps to setup the secondary SAS site with HSM integration:

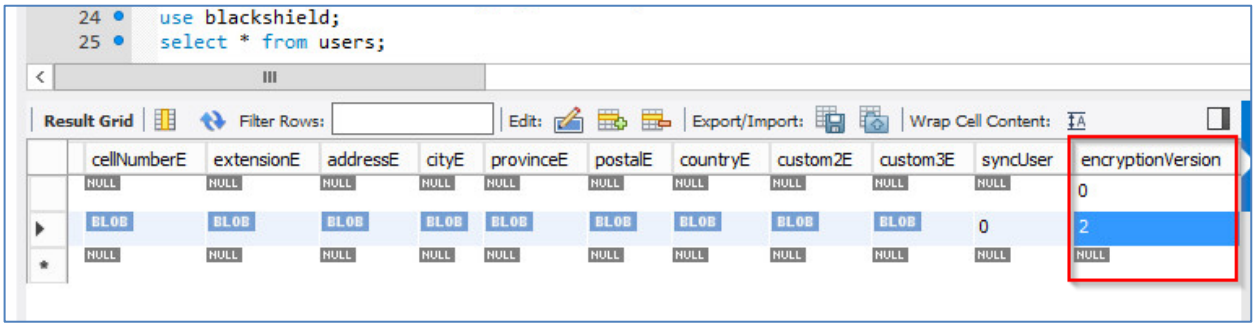
1. Install the secondary SAS server.
2. Install Network HSM Access Provider and PTKC packages.
3. Export site information from the primary SAS server (already running the HSM integration).
4. Import the site information into the secondary SAS server.
5. Enter the HSM PIN.
6. Perform **IISRESET** operation.

Verifying Encryption

To verify if the encryption is completed successfully, check as following:

1. Create a new user (or update an existing user).
2. Check the value of the **encryptionVersion** column.
   If the value of the **encryptionVersion** column is set to **2**, it means that the encryption is achieved

successfully using the HSM.



3

Setting up Hardware Security Module in High Availability Mode

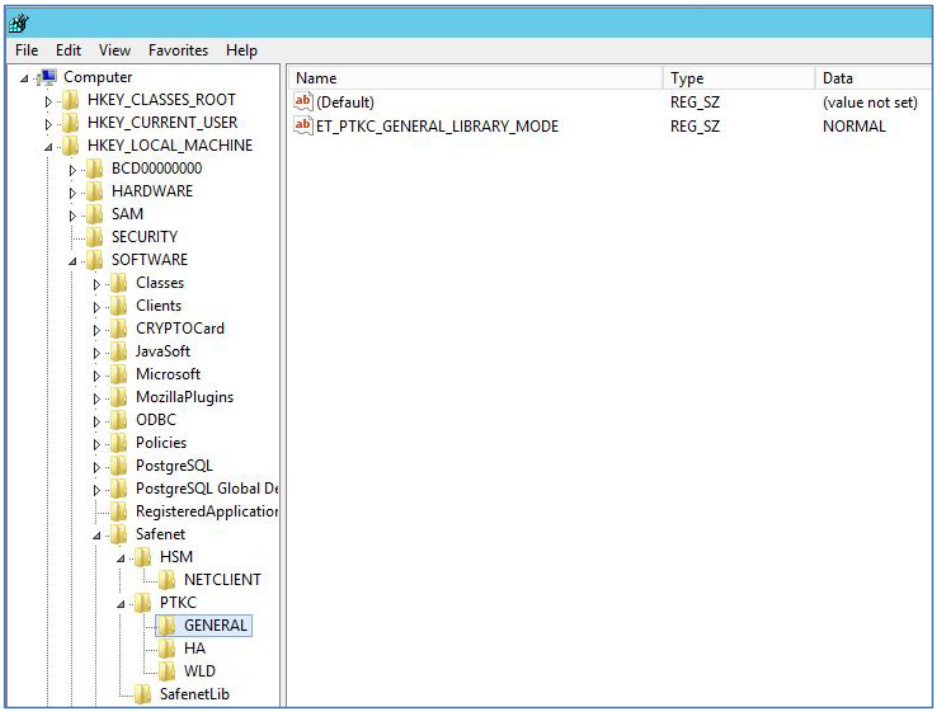
Recommendation for Hardware Security Module in High Availability: We recommend using a minimum of two HSM devices with appropriate backups, due to the irreversibility of operations.

Configuring Virtual High Availability Slots

The following are the steps to configure the virtual HA slots:

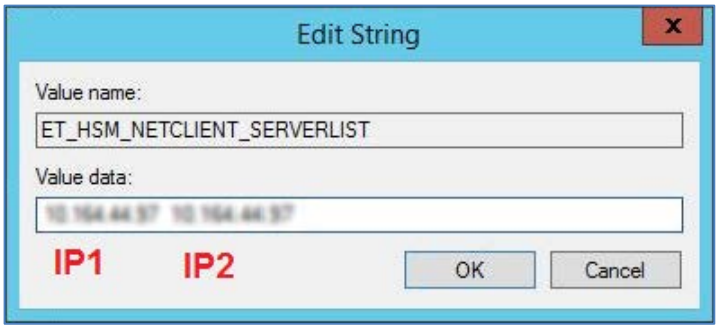
1. In the registry, navigate to the following path:
   `HEY_LOCAL_MACHINE>SOFTWARE>Safenet>PTKC>GENERAL`

   Change the value of `ET_PTKC_GENERAL_LIBRARY_MODE` to **NORMAL**, if not set already.



2. Navigate to the following path:
   `HEY_LOCAL_MACHINE>SOFTWARE>Safenet>HSM>NETCLIENT`

Double-click `ET_HSM_NETCLIENT_SERVERLIST` and assign IP addresses (of both HSMs) separated by a space.

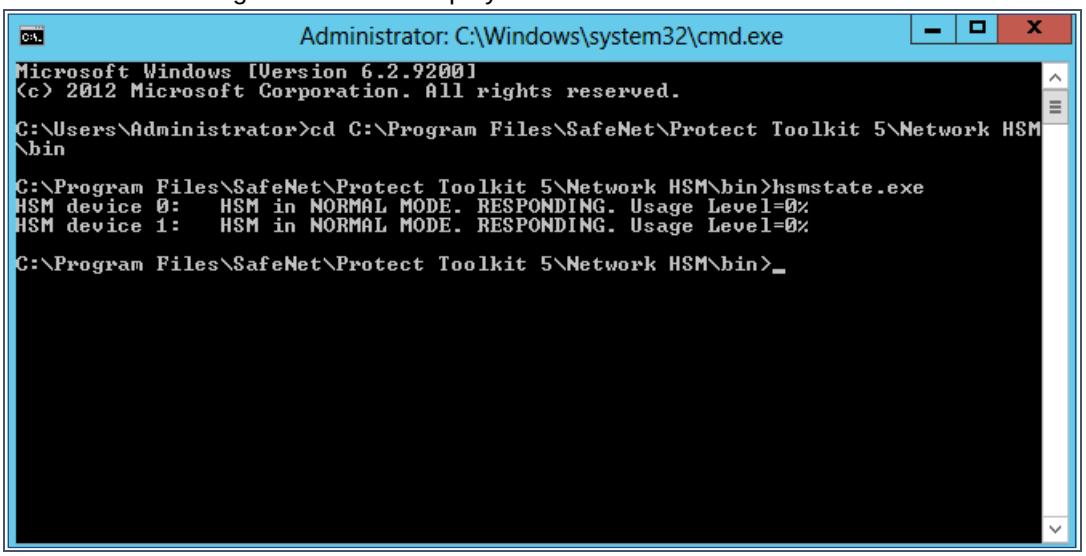


You also need to create an **environment variable**:
`ET_HSM_NETCLIENT_SERVERLIST = <IP1>SPACE< IP2>`
where;
IP1 is the IP address of the HSM **device 0** (first HSM machine Administrator is configuring, as defined earlier).
IP2 is the IP address of the HSM **device 1** (second HSM machine Administrator is configuring as a failover server).

Perform **IISRESET** operation.

3. Reopen the Command Prompt, and run the `HSMstate.exe` file, available at the following path: `C:\Program Files\SafeNet\Protect Toolkit 5\Network HSM\bin`.

   A list of all the configured HSMs is displayed.



As shown in the above screenshot, another HSM device, HSM **device 1** is now added.
Note: If **device 1** is not available, **edit environment variable** with its IP address.

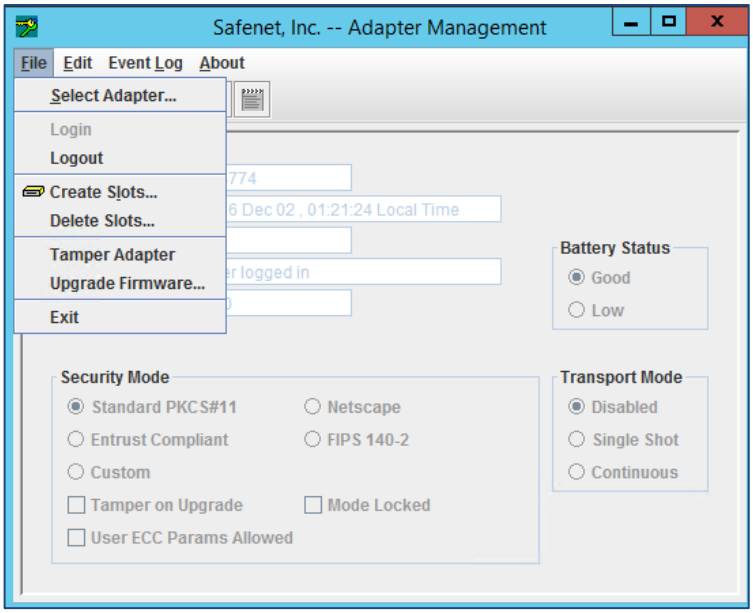
After adding **device 1**, we need to create an uninitialized slot which will be used for replication. Follow the steps to create an uninitialized slot in HSM **device 1**.

   i. To open, double-click `gCTAdmin HSM.bat` batch file, available at the following path: `C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

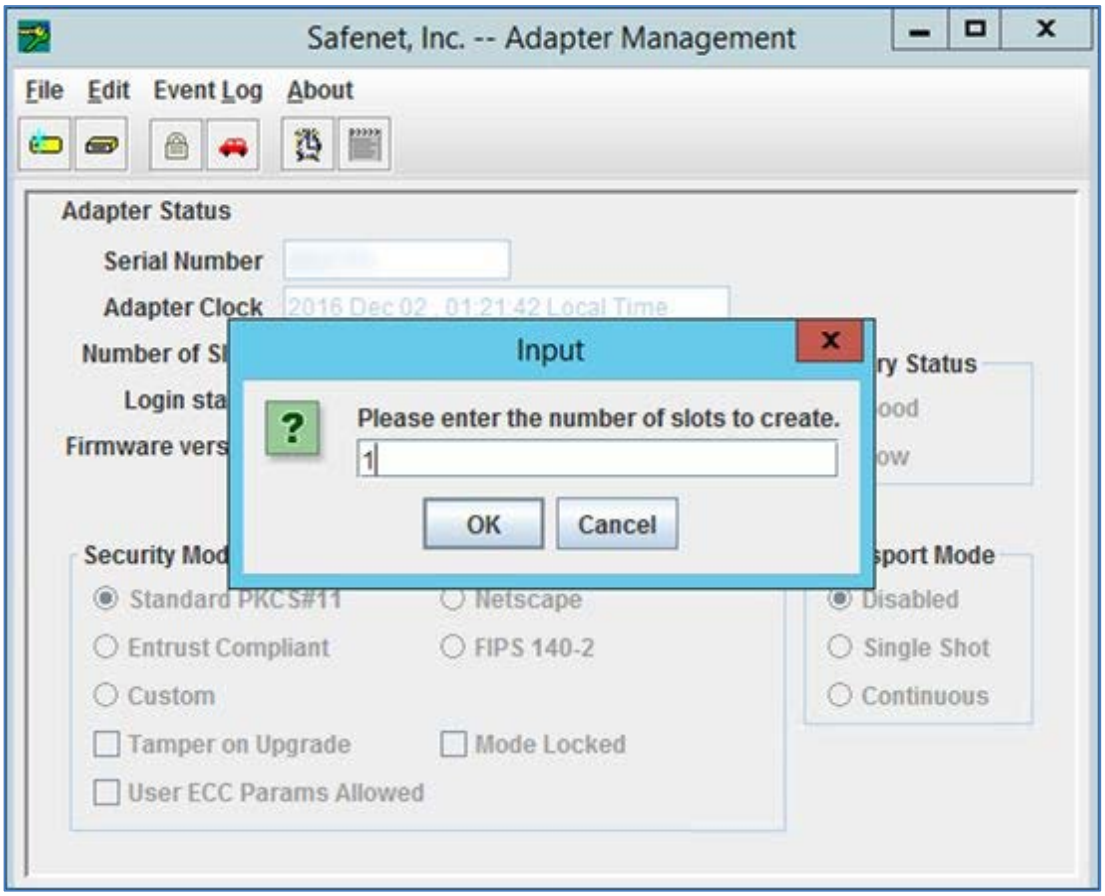
ii. In **Select an Adapter** dialog box, select appropriate **AdminToken** option (the one that belongs to **device 1**), and click **OK**.

iii. Enter **User PIN** in the **Enter PIN** popup window, and click **OK**.

iv. For slot creation, navigate to **File** > **Create Slots**.



v. Enter the number of slots to be created in the **Input** popup window, and click **OK**. The tokens will be created with uninitialized slots.



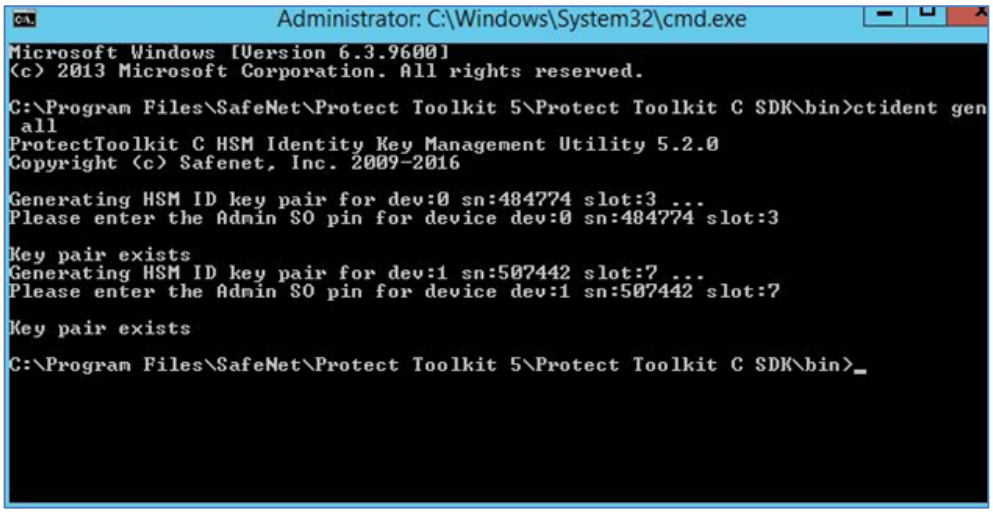
Example: If an Administrator enters **1** in the field, and click **OK**, one token will be created with an uninitialized slot.

vi. The **Adapter Management** window will restart. The Administrator needs to enter the Admin PIN.

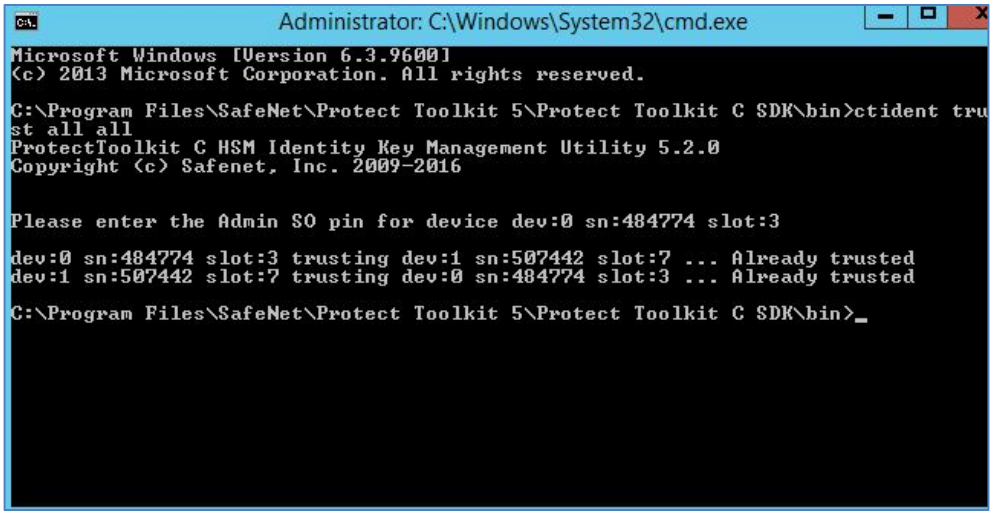
4. Establish Trust: For token replication to be performed from one HSM (holding the token labels) to another, both HSMs must have a trust relationship with each other.

   Run the following commands after navigating to the path:
   `C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

   i. *`ctident gen all`*: This command generates the identity Key Pair on all the HSMs connected to the client (or available to the client machine).



   ii. *`ctident trust all all`*: This command creates the trust between all the HSMs (both ways, from HSM 0 --> HSM 1 and vice versa).



5. Replicate Tokens: Once the trust is established, the tokens can be replicated. The HSM **device 0** can now be replicated to any of the uninitialized/initialized slots of the HSM **device 1**.

   i. For Uninitialized Slot: The following command can be used to replicate the tokens:
   `ctkmu rt` `-s<SLOT_NUMBER> -d<SLOT_NUMBER>`

where,
s is the slot number of the Source HSM.
d is the slot number of the Destination HSM, which is in the uninitialized state.

```
C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin>ctkmu rt -s
0 -d2
ProtectToolkit C Key Management Utility 5.0.0
Copyright (c) Safenet, Inc. 2009-2014

Enter user PIN for slot 0:

Please enter Security Officer PIN for the new token in Slot 2:
Replicate slot 0 to slot 2: SUCCESS
```

As shown below, Slot 0 of HSM **device 0** is now replicated with Slot 2 of HSM **device 1**, and the label of the uninitialized token is also changed.

```
C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin>ctkmu l
ProtectToolkit C Key Management Utility 5.0.0
Copyright (c) Safenet, Inc. 2009-2014


Cryptoki Version   = 2.20
Manufacturer       = Safenet, Inc.
Test                              (Slot 0)
AdminToken (484774)               (Slot 1)
Test                              (Slot 2)
AdminToken (507442)               (Slot 3)

C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin>_
```

ii. For Initialized Slot: Please ensure that PINs (**User PIN** and **Security Officer PIN**) of HSM **device 1** is same as that of HSM **device 0**. You can either modify **device 1** PIN or reinitialize the slot and go through the point (i) again.

6. Verify that the Key Checksum Value (KCV) of the key in both slots is the same.
   For details on how to verify, refer the **section** (Verifying Key Checksum Value in Replicated Slots) on page 38.

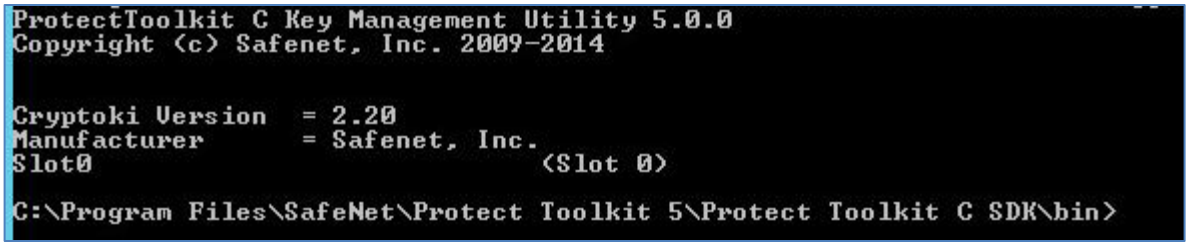
7. Create a new registry under PTKC and name it as HA, if not set already.
   Navigate to the following path:
   `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\PTKC\WLD`
   Create string values as: `ET_PTKC_WLD_SLOT_<HA SLOT_NUMBER>=<HA SLOTS LABEL>`.

   Example:

Variable (String Values)	Assignment
`ET_PTKC_WLD_SLOT_0`	Slot 0

8. Set Library Mode to HA.
   In the registry, navigate to `HEY_LOCAL_MACHINE>SOFTWARE>Safenet>PTKC>GENERAL` and change the value of `ET_PTKC_GENERAL_LIBRARY_MODE` to HA.

9. Check HA Slot Configuration:
   Run the *`ctkmu l`* (HA mode) utility to view the slots.
   Example:



Note: Only the HA virtual slots should be visible.
Any HSM physical slot on the system which has not been associated with an HA virtual slot will no longer be accessible.

10. Advanced HA Configurations:
    Set the following environment variables.
    a. `ET_PTKC_HA_RECOVER_DELAY = <number of minutes>`
    Example: `ET_PTKC_HA_RECOVER_DELAY = 2`
    b. `ET_PTKC_HA_RECOVER_WAIT= <YES / NO>`
    Example: `ET_PTKC_HA_RECOVER_WAIT= YES`

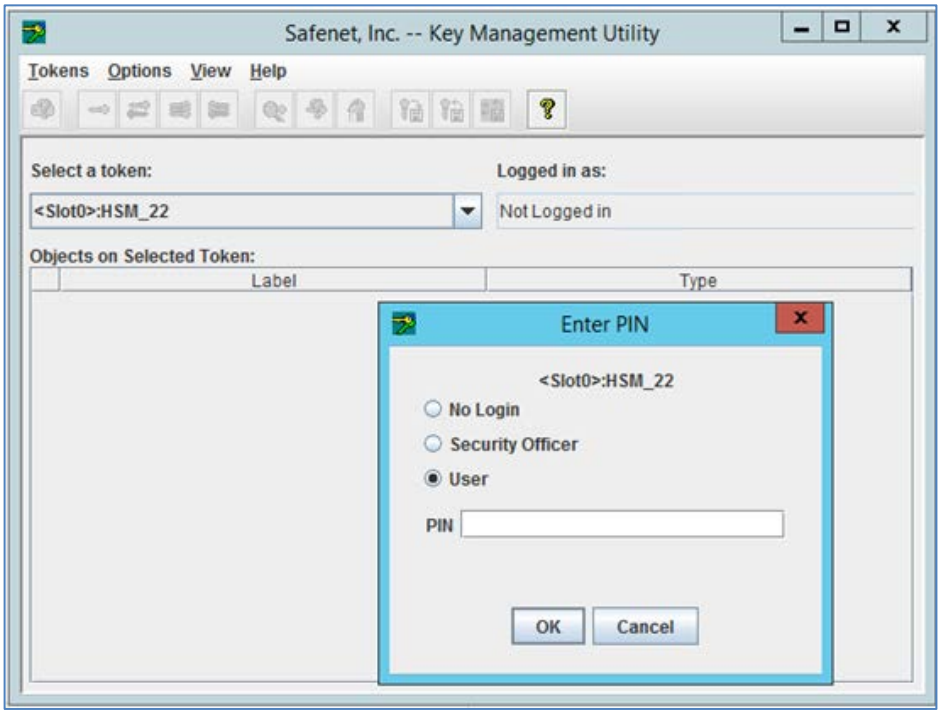
4
Manual Key Generation

The following steps can be used to generate a key (and edit its attributes) manually. Follow the steps based on whether you are using the **Graphical User Interface (GUI)** or **Command-Line Interface (CLI)**.

Graphical User Interface Method

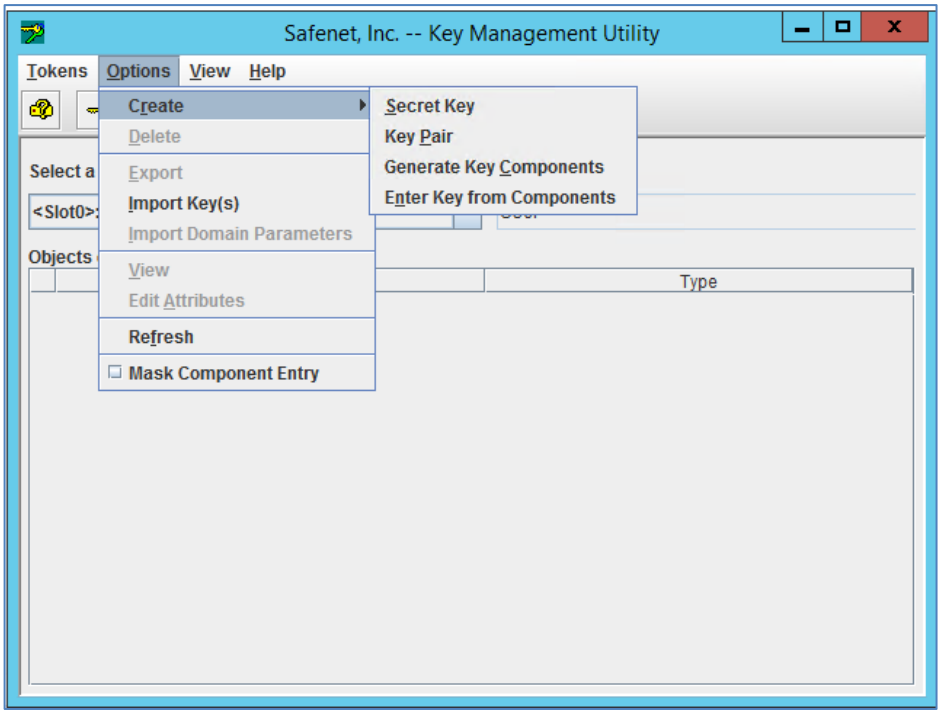
I. Double-click `KMU HSM.Bat` batch file available at the following path:
`C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

II. The **Key Management Utility** (KMU) window is displayed. Select the previously created token [**Slot<SLOT_NUMBER>** for the first token] and use **User PIN** option to login.

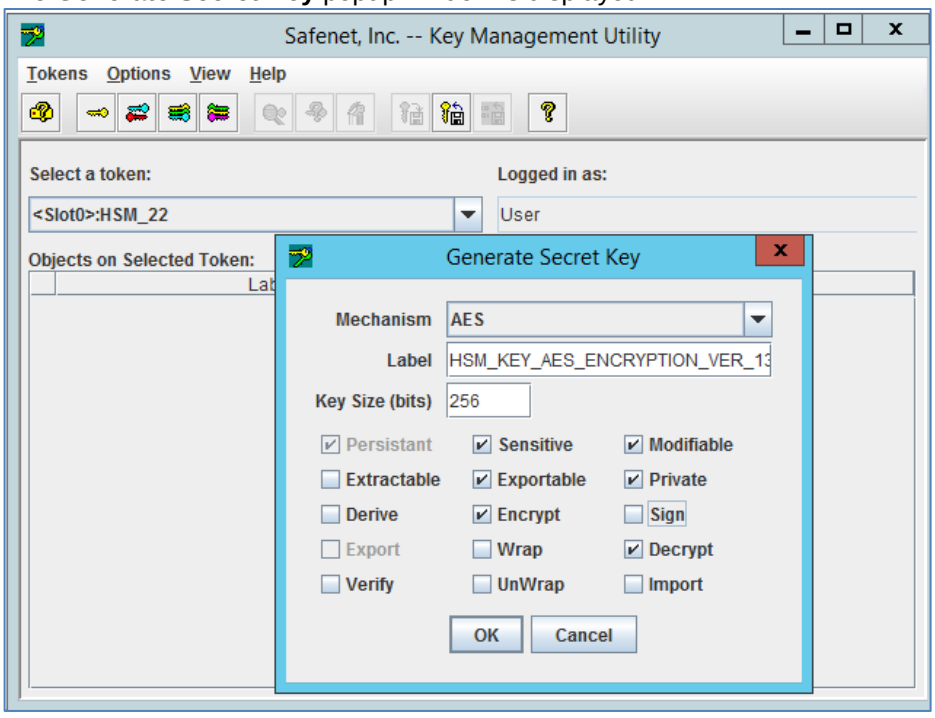


Note: Ensure to select **<Slot 0>** option in **Select a token** dropdown menu.

III. To create a secret key, navigate to **Options** > **Create** > **Secret Key**.



IV. The **Generate Secret Key** popup window is displayed.



Enter/edit the following fields, and click **OK**.

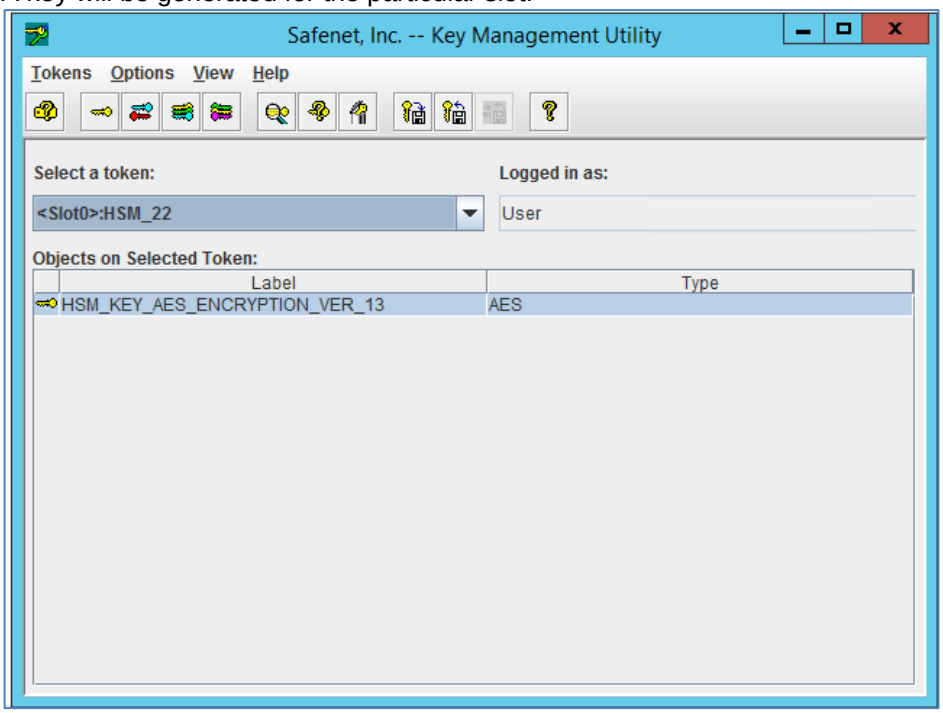
i. **Label**: Provide the label of the key as: **HSM_KEY_AES_ENCRYPTION_VER_13**.

ii. **Key Size (bits)**: Change to **256**, from the default value of **128**.

Ensure that only the following checkboxes are selected:

- ✓ Persistant
- ✓ Sensitive
- ✓ Modifiable
- ✓ Exportable
- ✓ Private
- ✓ Encrypt
- ✓ Decrypt

V. A key will be generated for the particular slot.



Note: Key generation can also be done using SAS itself. When you enable the HSM in SAS System Settings, provide the User PIN for the slot and apply changes, a key is created automatically for the slot.

Command-Line Interface Method

I. Execute the `KMU HSM.Bat` batch file available at the following path:
`C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

II. To create key(s) in the slot, execute the following command:
`ctkmu c –t<type of key> -s <slot number> -n <label of the Key> -a<attributes of the keys>`
Example: `ctkmu c -taes -s0 -nHSM_KEY_AES_ENCRYPTION_VER_13 -aEDMX –z256`

In the above example, the execution of the command will generate an AES (256 bit) key named HSM_KEY_AES_ENCRYPTION_VER_13 in Slot 0 with following attributes: Encrypt, Decrypt,

Exportable and Modifiable

Note: The following lists the attributes, which are allowed:

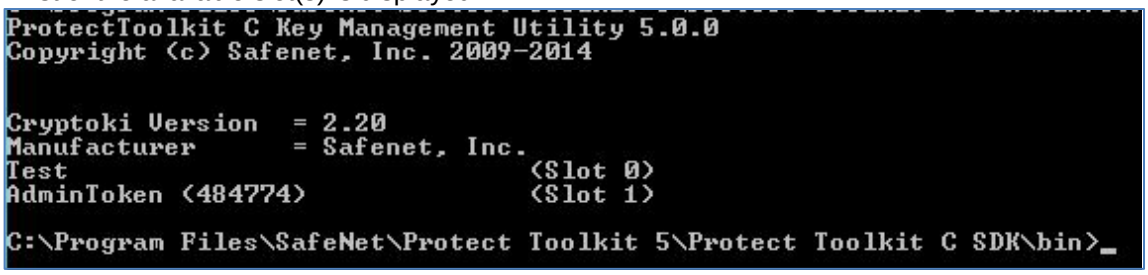
P: CKA_PRIVATE
M: CKA_MODIFIABLE
T: CKA_SENSITIVE
W: CKA_WRAP
w: CKA_EXPORT
I: CKA_IMPORT
U: CKA_UNWRAP
X: CKA_EXTRACTABLE
x: CKA_EXPORTABLE
R: CKA_DERIVE
E: CKA_ENCRYPT
D: CKA_DECRYPT
S: CKA_SIGN
V: CKA_VERIFY
L: CKA_SIGN_LOCAL_CERT

The following table provide descriptions of the listed keys:

Flag	Description
Decrypt	Security Object supports decryption
Derive	Key can be used to derive operations
Encrypt	Security Object supports encryption
Exportable	Key can be exported in cleartext through the pkcs#11 API (Not backup/restore related). Note: HSM prevents the export operation.
Extractable	Key can be wrapped with transport key of the HSM (Not backup/restore related)
Import	NA
Modifiable	Allow attributes to be changed after key generation
Private	Authentication required prior to security object being visible
Sensitive	Security sensitive attributes non-readable
Sign	Security Object supports signing
UnWrap	Security Object supports unwrapping (can be used to unwrap another key)
Verify	Security Object supports verification (public key)
Wrap	Security Object supports wrapping (can be used to wrap another key)

III. Close and reopen the Command Prompt, and run the `Ctkmu l` command.

A list of the available slot(s) is displayed.



Note: If you need to export the Private Key created at one SAS machine to another SAS machine, refer **Chapter 5: Exporting and Importing Private Keys** on page 30.

5
Exporting and Importing Private Keys

To export SAS generated key (on **Slot 0** of one HSM device) to another server (with SAS PCE installed on some other machine), follow the steps:

1. **Exporting Private Key (from one HSM device)**
2. **Importing Private Key (to another HSM device)**
3. **Verifying Private Key Operations Success**

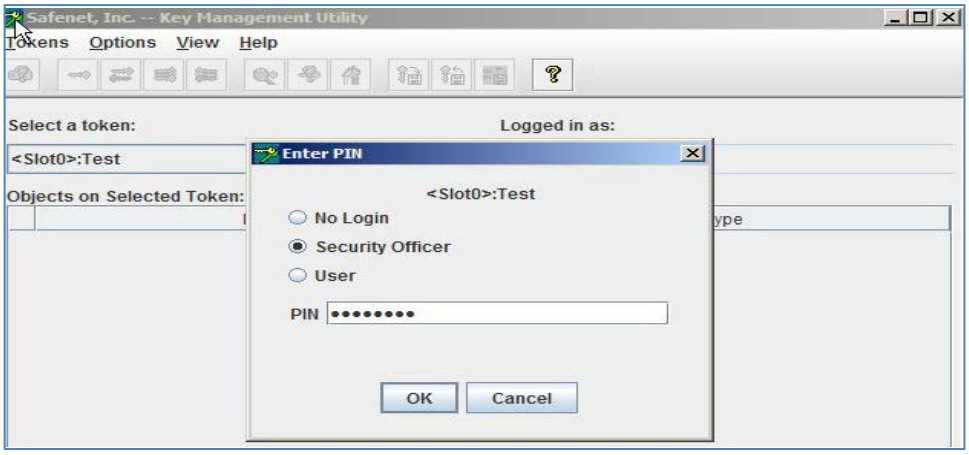
Exporting Private Keys

1. Navigate to the following path:
   `C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

2. To launch the KMU tool, double-click the `KMU HSM.bat` batch file.

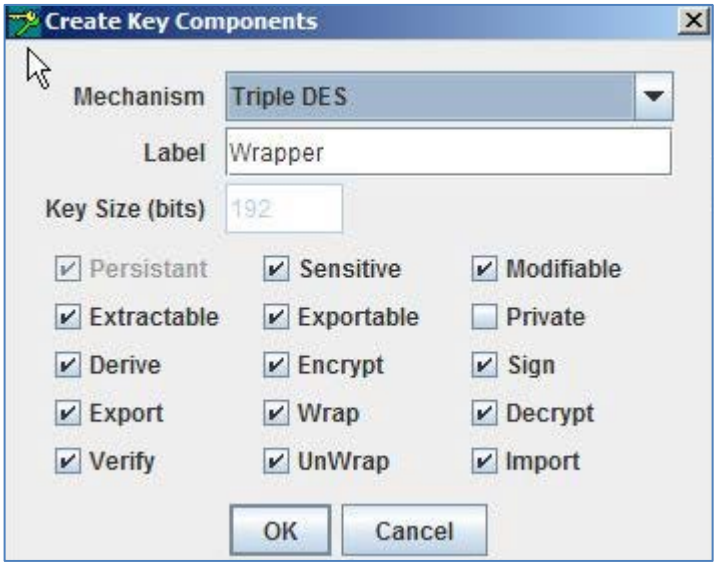
3. Login to KMU using User PIN credentials to verify that a key was generated (for **Slot 0**), by the SAS solution.

4. Login to KMU (for Slot 0) using Security Officer credentials.



5. Navigate to **Options** > **Create** > **Generate Key Components**.

6. The **Create Key Components** popup window is displayed. Edit the following attributes, and click **OK**:
   a. **Mechanism**: Select **Triple DES** from the dropdown list.
   b. Check **Export** and **Import** checkboxes.
   c. Clear **Private** checkbox.

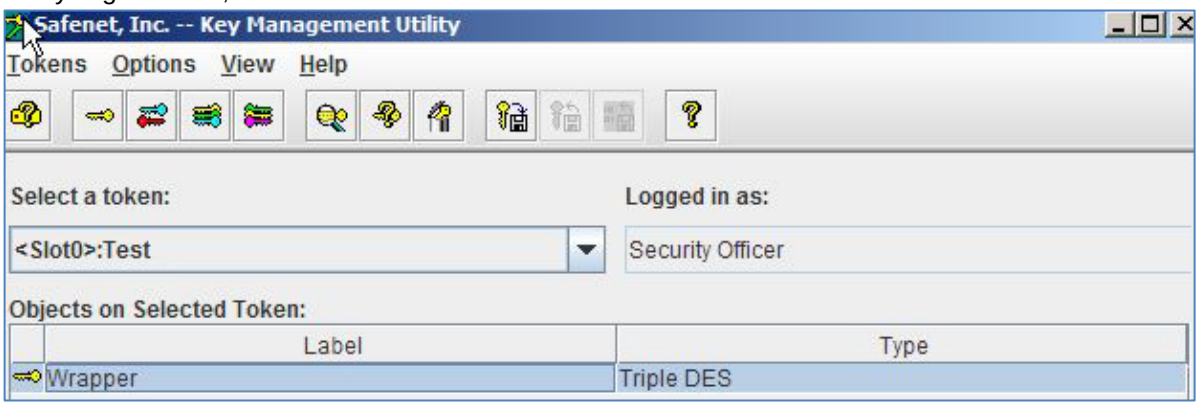


7. The **Number of Components?** window is displayed. The field, **Number of components to create** is default populated as **2**. Click **OK**, and click **OK** again.

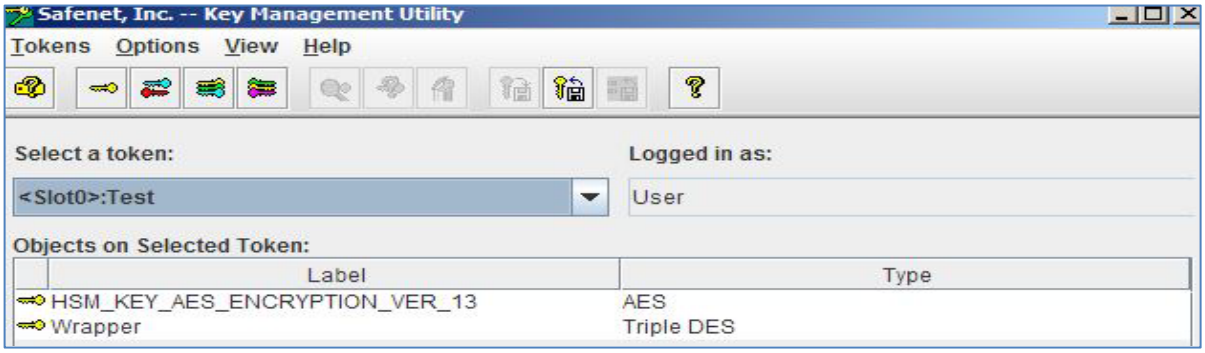
8. Copy the hexadecimal component and KCV to a text file (say, *info.txt* file)

9. Repeat steps 6 and 7, as above, for the second component.

10. A key is generated, and is now visible.

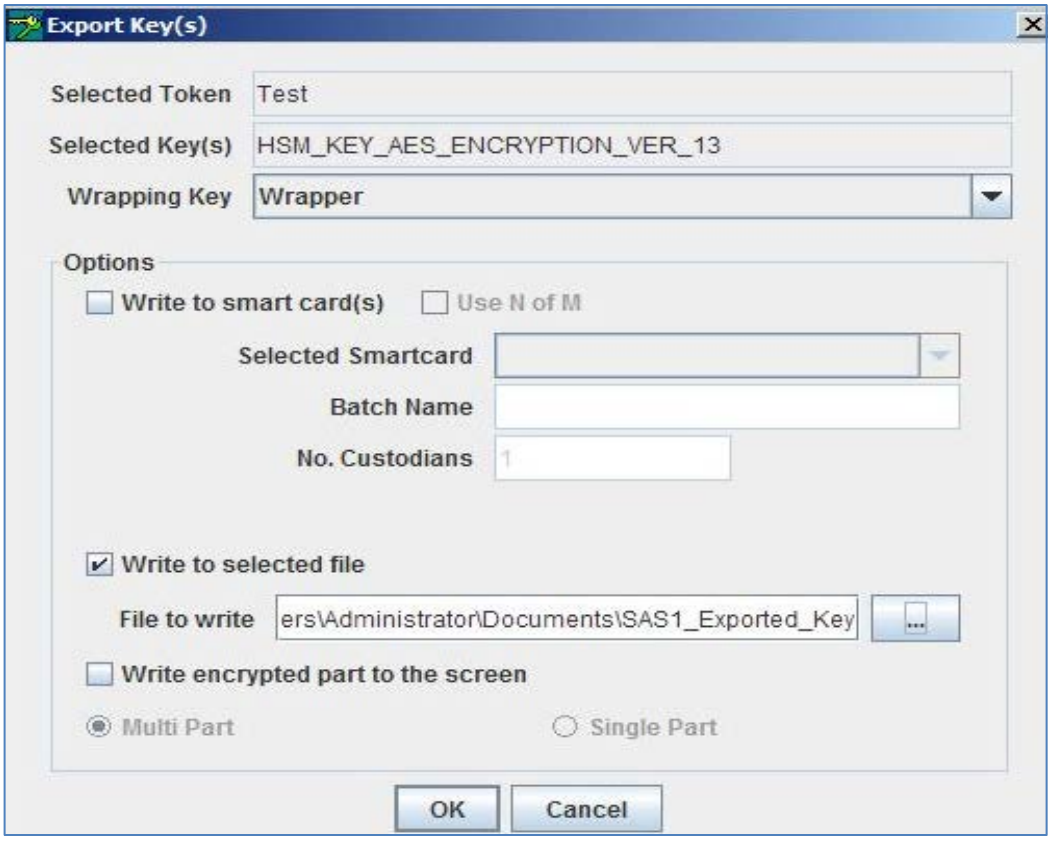


11. Login to KMU using User PIN credentials (for **Slot 0**). The SAS generated key and the wrapper key will be available.

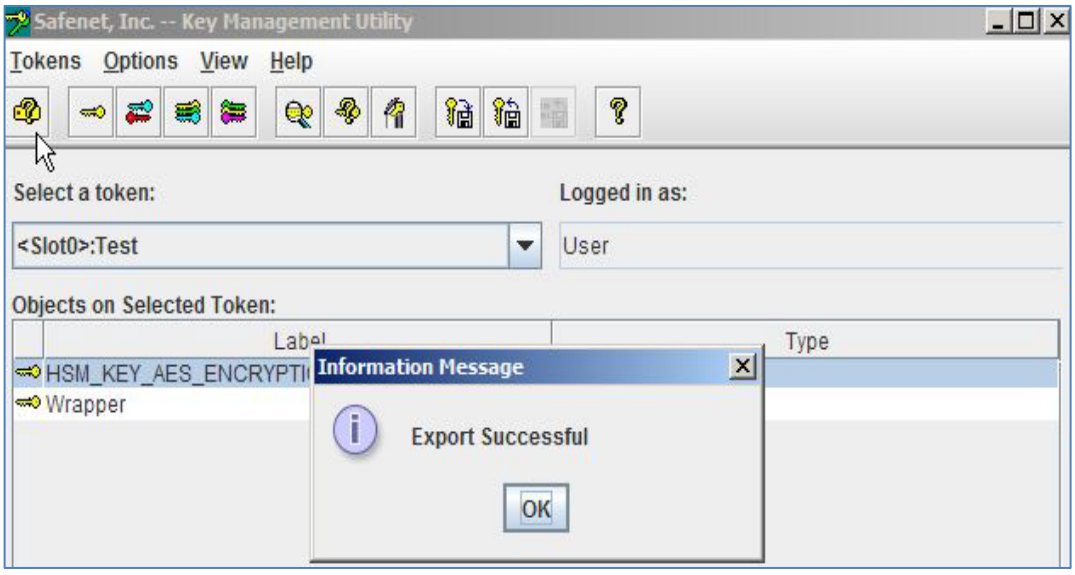


12. Right-click the SAS generated key and select **Export**.

13. The **Export Key(s)** window is displayed. Select the wrapper key (generated, as above, in step 10) from the **Wrapping Key** dropdown field and provide a path for the file to export, and click **OK**.



14. The key is exported, and a success message, **Export Successful** is displayed.



Importing Private Keys

As a prerequisite to importing, SAS and PTKC 5.2.0 should already be installed on this (second) machine with a different HSM device.

1. Copy the exported file (as above) and the text (*info.txt*) file to the machine where the key needs to be imported.

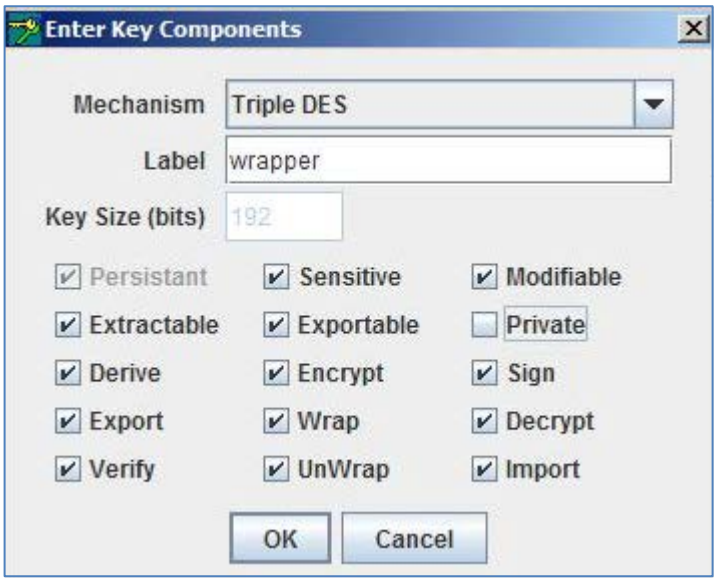
2. Navigate to the following path:
   `C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

3. To launch the KMU tool, double-click the `KMU HSM.bat` batch file.

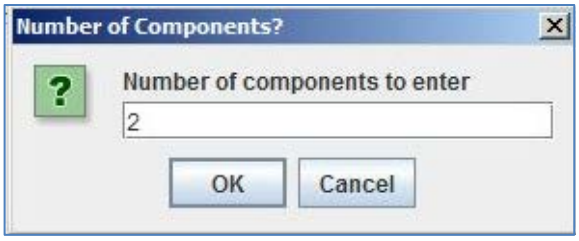
4. Login to KMU using Security Officer credentials.

5. Navigate to **Options** > **Create** > **Enter Key from Components**.

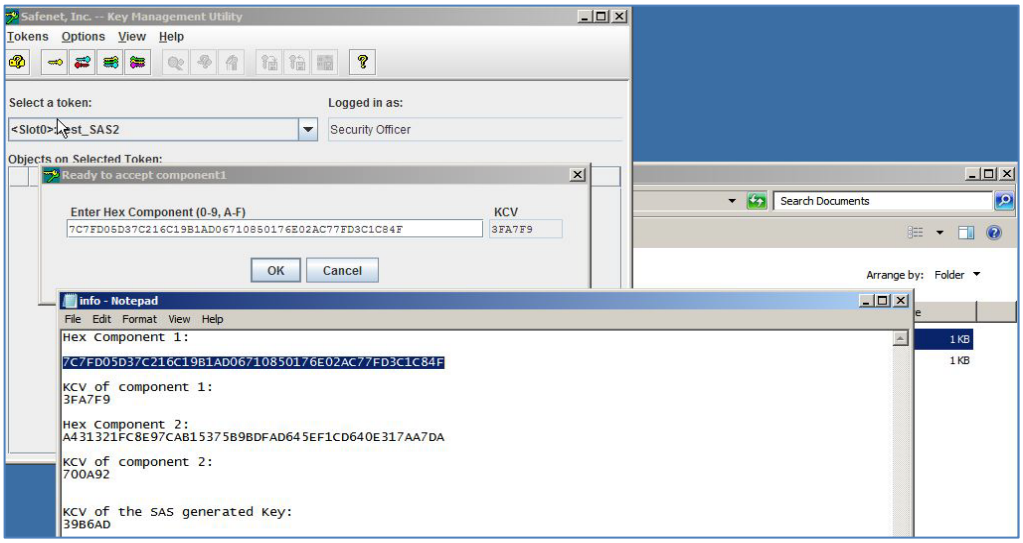
6. The **Enter Key Components** popup window is displayed. Edit the following attributes, and click **OK**:
   a. **Mechanism**: Select **Triple DES** from the dropdown list.
   b. Check **Export** and **Import** checkboxes.
   c. Clear **Private** checkbox.



7. The **Number of Components?** window is displayed. Enter **2** in the **Number of components to enter** field, and click **OK**.



8. Enter the hexadecimal component values from the text file (*info.txt* file).



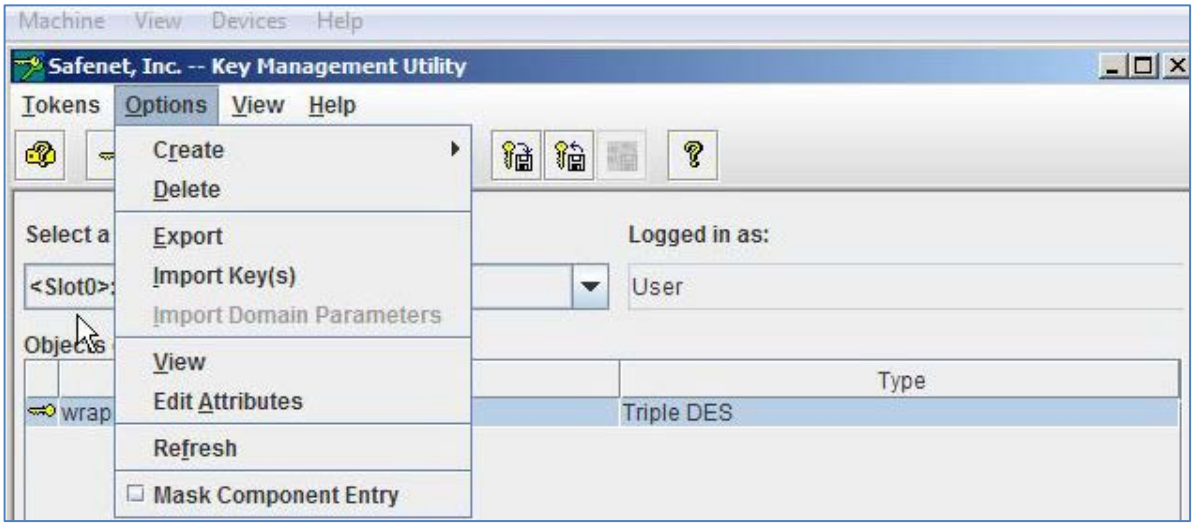
Note: The **KCV** value is populated, by default.

9. Repeat the above step (step 8) for the second component.

10. The wrapper key is created. It is the same key that got created in **Exporting Keys** (step 11). Right-click to compare and verify that KCVs of these wrapper keys on different machines is the same.

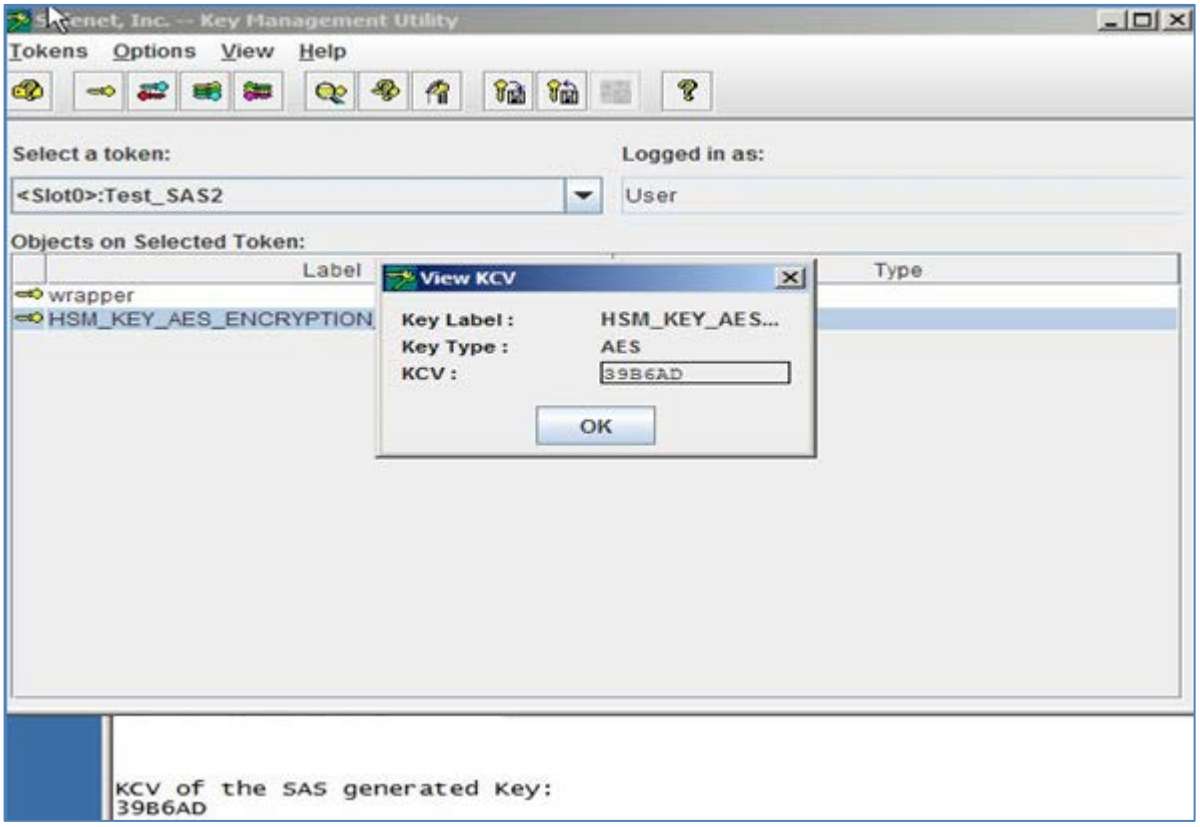
11. Login to KMU using User PIN credentials (for **Slot 0**).

12. Navigate to **Options** > **Import Key(s)**.



13. The **Import Key(s)** window is displayed. Select the wrapper key (generated, as above, in step 10) from the Wrapping Key dropdown field and provide the path for the file to import. This path should be the same as the one provided for export in step 13 of **Exporting Keys**.

14. The key is imported, and a success message, **Import Successful** is displayed.
    To verify if the same key (which was exported) has been imported, compare KCV of the two keys on different machines.



Verifying Key Operations

To verify that the Private Key export and import operations were successful, follow the steps:

Verifying Private Key Export and Import Success

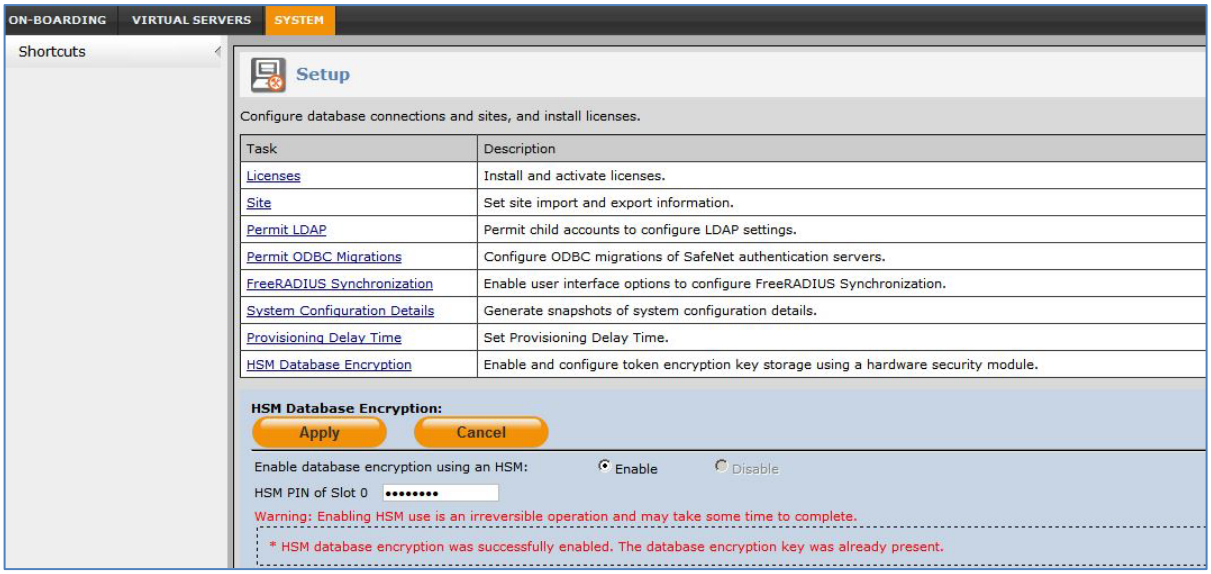
1. Launch SAS Manager and login as administrator.

2. Navigate to **System** > **Setup** > **HSM Database Encryption**.

3. Provide User PIN (for Slot 0) of the HSM device configured on the second machine.

4. The message, **HSM database encryption was successfully enabled. The database encryption key ...** is displayed. The success message confirms that both the Private Key export and import operations

were successful.



6
Recommendations and Troubleshooting

IISRESET Use Cases

Following are a few cases, where **IISRESET** operation is highly recommended.

1. When an HSM (with which the SAS solution is communicating), is turned off, and then subsequently turned on, an **IISRESET** is recommended to re-enable the SAS to start communicating with the HSM.

2. Whenever there is a change in Registry Settings, or an Environment Variable, an **IISRESET** operation is recommended.

Setting Environment Variables

If you are unable to select an Adapter, during **Slot Creation and Initialization**, follow the steps to configure environment variables:

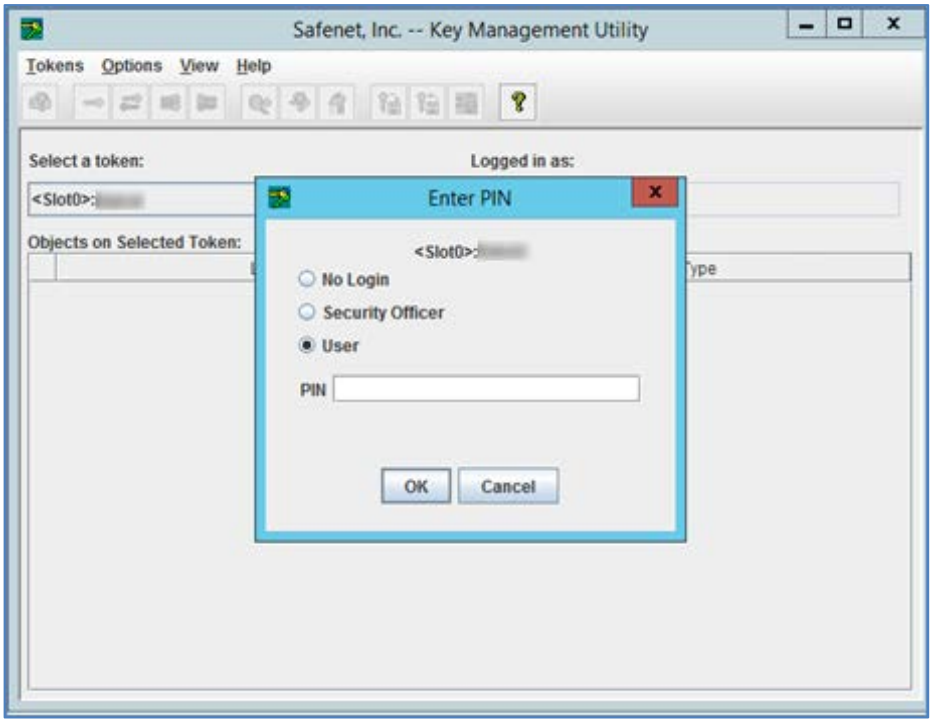
1. Click **Control Panel** > **System**.
2. From the left pane, click **Advanced System Settings**.
3. The **System Properties** dialog box with **Advanced** tab selected, is displayed.
4. To configure, click **Environment Variables**.

Verifying Key Checksum Value in Replicated Slots

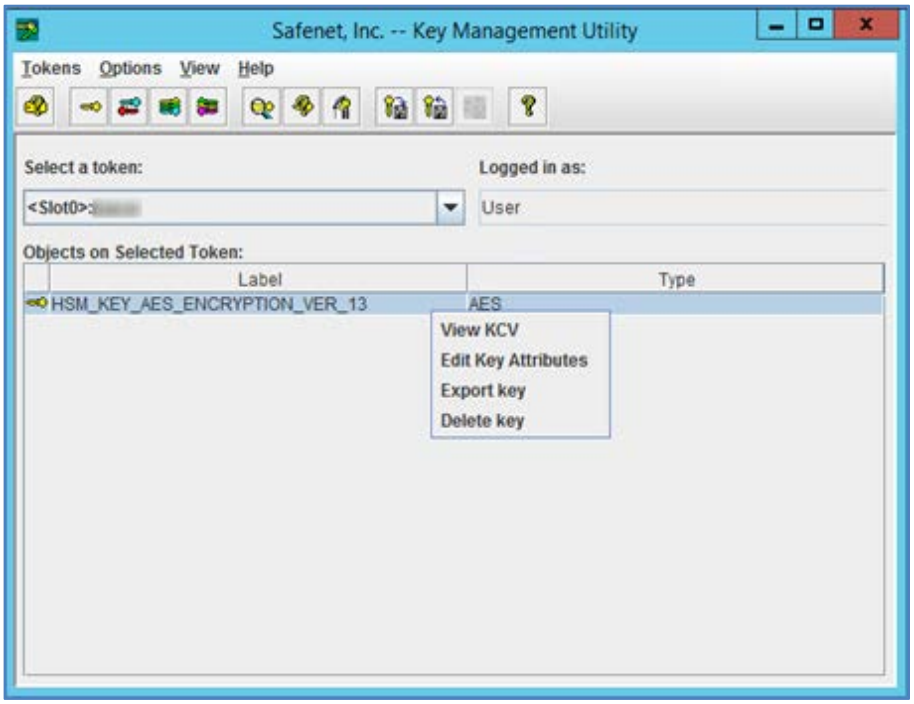
To verify if KCV of the key in both slots is the same, follow the steps:

1. Execute the `KMU HSM.bat` batch file available at the following path:
   `C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin`

2. Select Slot 0 of **device 0** and provide **User PIN** to login.

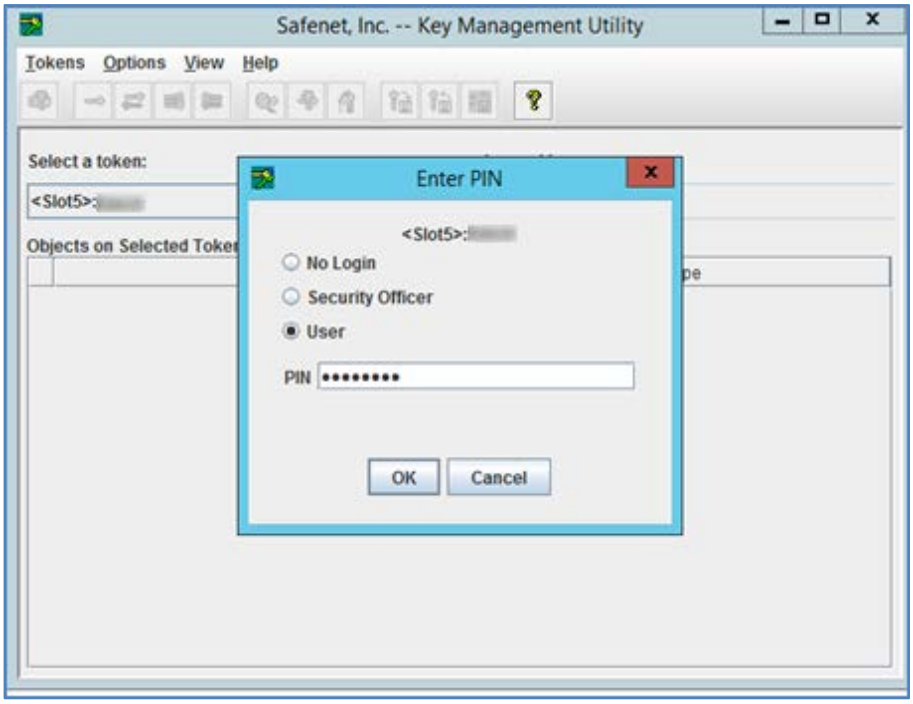


3. Right-click the key and select **View KCV**.

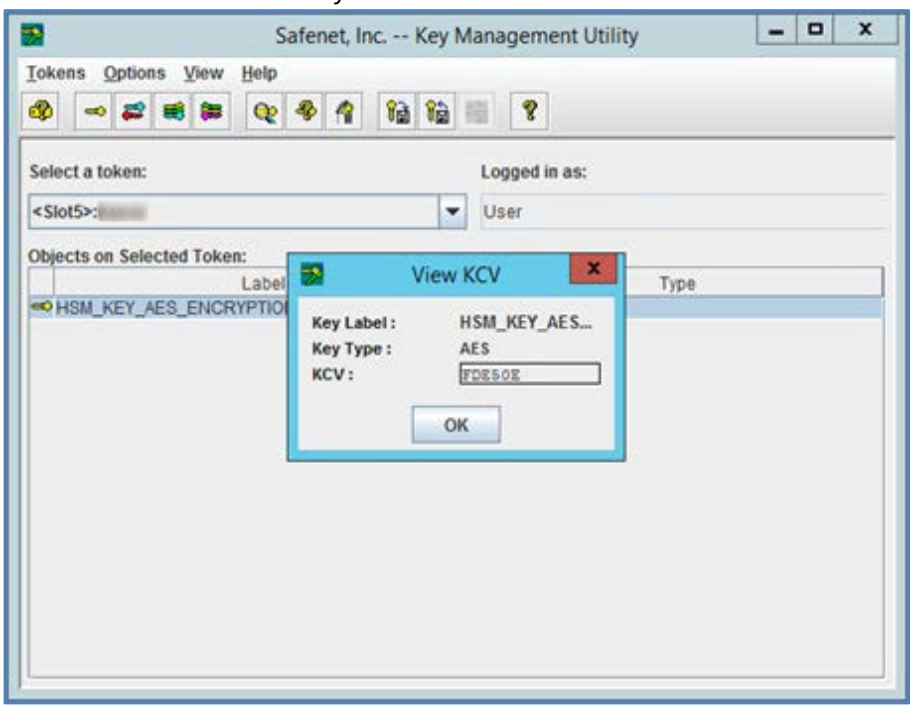


Note down the KCV value for Slot 0 of **device 0**.

4. Select replicated slot from **device 1** and login as **User PIN** of Slot 0 of **device 0**.



5. Right-click the key and select **View KCV**.
   The value of KCV for this key should be the same as noted from Slot 0 of **device 0**.

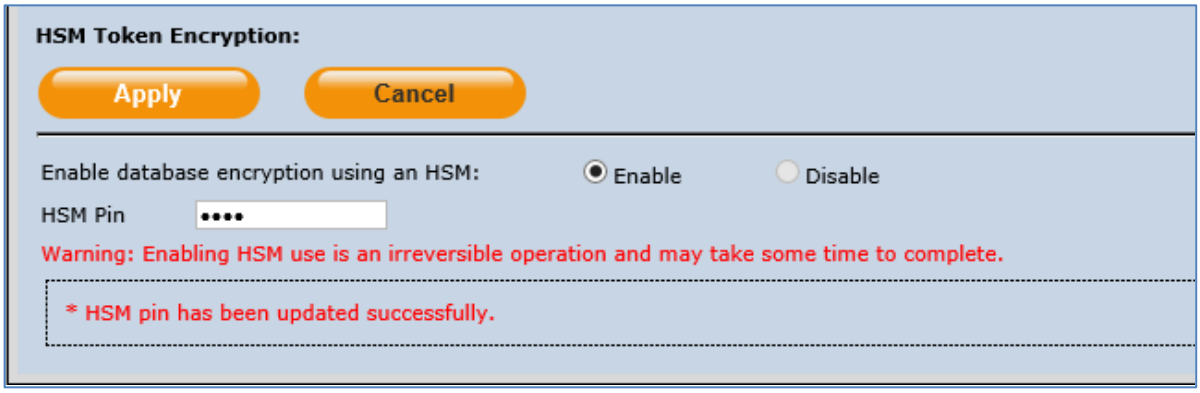


Updating User PIN in SAS

An Administrator may require changing the User PIN of HSM. After changing User PIN of an HSM slot, the

same User PIN must also be updated in the SAS solution, otherwise, the SAS solution will not allow the Administrator to create users, and perform related activities. Following are the steps, to achieve the same:

1. Login to SAS Administrator console using username and password.
2. Navigate to **System** > **HSM Token Encryption**.
3. Update the new User PIN in the **HSM PIN** field, and click **Apply**. The appropriate messages, as shown in the screenshot, will be displayed.



4. The server on which the SAS solution is installed will now need to be **restarted**, to ensure that a new session is created between the SAS and HSM.

Unresponsive Failover Server

If the failover server is not responding, ensure that the below steps were followed. If they were not, perform the steps that were missed:

1. Install SAS.
2. Install PTKC 5.2.0 (`PTKnethsm.msi` and `PTKcpsdk.msi`) packages.
3. Provide only one IP for HSM **device 0** while installing `PTKnethsm.msi`.
4. Create a slot in HSM (if not already available).
5. Enable HSM in SAS (in Normal mode).
6. Create users in SAS.
7. Stop HSM device.
8. Try to open the created user. If the Created User page is accessible, perform an **IISRESET** operation. If the Created User page is inaccessible, continue following the steps.
9. Start HSM and open created user. The user detail page is displayed.
10. Update `ET_HSM_NETCLIENT_SERVERLIST` in registry and environment variable. Add IP of the second HSM (**device 1**).
11. Perform **IISRESET** operation.
12. Open command line and execute `hsmstate` and `ctkmu l` commands. State of both HSMs, and slot details of both HSMs should be displayed.
13. Create a new slot in HSM **device 1** (second HSM device). Replicate the newly created slot with Slot 0 of

HSM **device 0**.

Note: After successful replication, please verify KCV of keys in both slots, they should be the same.

14. Change `ET_PTKC_GENERAL_LIBRARY_MODE` to HA and `ET_PTKC_WLD_SLOT_0 to <Slot label>` in the registry.
15. Add key `ET_PTKC_HA_LOG_FILE` in the registry, available at the following path: `HKEY_LOCAL_MACHINE/SOFTWARE/Safenet/PTKC/HA`, and set its value to NULL.
16. Perform **IISRESET** operation.
17. Execute `ctkmu l` command. Only Slot 0 should be visible.
18. Open SAS, and open the created user.
19. Test the failover server without performing an **IISRESET** operation.

7
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult the support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	**https://serviceportal.safenet-inc.com** Existing customers with a Technical Support Customer Portal account can login to manage incidents, get latest software upgrades, and access the Gemalto Knowledge Base.	
Documentation	All SAS documentation (Cloud, PCE, SPE, Token and Integration) can be found on the **SafeNet Knowledge Base** page. All SAS Agents documentation can be found on the **SafeNet Authentication Service Downloads** page.	