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

**Feature Documentation** 



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.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013558-001, Rev. C Release Date: February 2017

## **Table of Contents**

1 Hardware Security Module and SafeNet Authentication Service	
Introduction	4
Hardware Security Module with SafeNet Authentication Service	4
Compatibility Information	5
Supported Hardware Versions	5
Supported Software Versions	5
Supported Databases	5
Supported Operating Systems	5
Setting up ProtectServer External 2 Device	5
2 Setting up Hardware Security Module in Normal Mode	7
Installing and Configuring Protect Toolkit C Package	8
Creating and Initializing Slot	10
Graphical User Interface Method	11
Command-Line Interface Method	13
Configuring Hardware Security Module in SafeNet Authentication Service	
SAS Site Import	
veniying Encryption	
3 Setting up Hardware Security Module in High Availability Mode	
Configuring Virtual High Availability Slots	18
4 Manual Koy Concration	25
4 Marida Rey Generation	
Graphical User Interface Method	25
5 Exporting and Importing Private Keys	
Exporting Private Keys	
Importing Private Keys	33
Verifying Key Operations	
6 Recommendations and Troubleshooting	
IISRESET Use Cases	
Setting Environment Variables	
Verifying Key Checksum Value in Replicated Slots	
Updating User PIN in SAS	40
Unresponsive Failover Server	41
7 Support Contacts	43

# 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:

- 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. <u>Adjust Network Configurations</u>: Assign an IP address to ETH0 interface in /etc/sysconfig/network-scripts/ifcfg-eth0 file.
- 3. <u>Add Hostname</u>: Add a hostname of the system to /etc/sysconfig/network file. Example: HOSTNAME=examplename
- 4. <u>Add Default Gateway</u>: Add the default gateway to /etc/sysconfig/network file. Example: GATEWAY=192.168.1.1

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

<u>Note</u>: 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

<u>Prerequisite</u>: 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.

B

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.

<u>Optional Step</u>: 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  ${\tt hosts}$  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).
  - Login using your User ID and Password. <u>Note</u>: 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.

6	Protect Server Setup	- • ×
	Enter server configuration string: cname_or_IP1> cname_or_IP2>	
	IP1OKCancel	

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).
  - Login using your User ID and Password. <u>Note</u>: 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.

Select Cryptoki Provider
C Software Only
<ul> <li>HSM (local adapter or remote server)</li> </ul>
C None (cryptoki DLL must be in the path)

- 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.

<u>Note</u>: 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.

Descri	ption		
Admin	Toker	1 (	)

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**.

-	Enter PIN X			
	<slot3>:AdminToken ( )</slot3>			
	Security Officer			
	User			
	PIN			
	OK Cancel			

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

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

Safenet, Inc Adapter Managemer	nt 🗕 🗖 🗙
<u>File</u> <u>E</u> dit Event Log <u>A</u> bout	
Select Adapter	
Login	
Logout	
Create Slots 142	
Delete Slots 6 Nov 17 , 15:42:27 Local Time	
Tamper Adapter	Battery Status
Upgrade Firmware rlogged in	Good
Exit	⊖ Low
Security Mode	Transport Mode
Standard PKC S#11     O Netscape	Disabled
O Entrust Compliant O FIPS 140-2	O Single Shot
○ Custom	⊖ Continuous
Tamper on Upgrade Mode Locked	
User ECC Params Allowed	
]	

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.

	Input ×
?	Please enter the number of slots to create.

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**.

≫		Safenet, Inc Adapter Managemer	nt 🗕 🗖 🗙
<u>F</u> ile	Edit Event Log	About	
<del>ک</del> ه	<u>T</u> okens		
	Security Mode		
A	Transport Mode		
	Clock	442	
	Adapter Clock	2016 Nov 17 , 16:02:47 Local Time	
	Number of Slots		Battery Status
	Login status	User logged in	Good
F	irmware version		O Low
	Security Mode		Transport Mode
	Standard PK	S#11 O Netscape	Disabled
	O Entrust Comp	liant O FIPS 140-2	O Single Shot
	O Custom		O Continuous
	Tamper on U	ograde 🗌 Mode Locked	
	User ECC Par	ams Allowed	
1			

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

1	Manage Tokens	X
Slot <slot 3="">:(un</slot>	initialised token)	Done
Selected Slot		Initialize
Slot Description Token Label	ProtectServer K6:35162	User PIN
Token Initialized User PIN Initialized		SO PIN

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

	Initialise Admin	Token
Token La	ibel	
Security C	fficer PIN	OK
PIN	•••••	QK
Re-Enter	•••••	Cancel
Jser PIN		
PIN	*******	
Re-Enter		

<u>Note</u>: 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:

B

1. Login to the SAS console as an Administrator.

Shortcuts	Setup	0
	Database	Û
	Communications	Û
	Logging	0
	Authentication Processing	0
		gemalto <sup>×</sup>

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.

Setup	(				
Configure database connections and	sites, and install licenses.				
Task	Task Description				
<u>Licenses</u>	Install and activate licenses.				
Site Set site import and export information.					
Permit LDAP	Permit child accounts to configure LDAP settings.				
Software Token Push OTP Setting	Enable Push OTP communication with MobilePass+				
Permit ODBC Migrations	Configure ODBC migrations of SafeNet authentication servers.				
FreeRADIUS Synchronization	Enable user interface options to configure FreeRADIUS Synchronization.				
System Configuration Details	Generate snapshots of system configuration details.				
Provisioning Delay Time	Set Provisioning Delay Time.				
HSM Token Encryption	Enable and configure token encryption key storage using a hardware security module.				
SAS Service Communication Key	SAS Service Communication Key				
HSM Token Encryption:	ncel				
Enable database encryption using HSM Pin •••••• Warning: Enabling HSM use is an in * HSM database encryption was	an HSM:   Enable  Disable  reversible operation and may take some time to complete.  successfully enabled.				

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.

SM Token Encryption:		
able database encryption using an HSM: SM Pin ••••	• Enable	C Disable
arning: Enabling HSM use is an irreversible o	peration and may tak	ke some time to complete.

SafeNet Authentication Service PCE/SPE with Support for HSM PSE 2 Integration: Feature Documentation Document PN: 007-013558-001, Rev. C, © Gemalto 2017. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and are registered in certain countries.

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 <u>SASHSMSIot 0,0,Description</u>, and needs to be changed to slot label of the HA slot (as described in point 7 of Configuring Virtual High Availability Slots).

g

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).
- 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.

	24 • use 25 • sel	<pre>blackshie ect * from</pre>	ld; users;		22502 22 <sup>4</sup> 04						
<		Ш									
Res	sult Grid 📗	🚷 Filter Row	/5:		Edit: 💋	j 🖦 🛱	Export/In	mport: 📳	🐻   Wrap (	Cell Content:	IA D
	cellNumberE	extensionE	addressE	cityE	provinceE	postalE	countryE	custom2E	custom3E	syncUser	encryptionVersion
	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	0
•	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	0	2
	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

## **3** Setting up Hardware Security Module in High Availability Mode

<u>Recommendation for Hardware Security Module in High Availability</u>: 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:

B

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.

1 Alexandre and a second secon			
File Edit View Favorites Help			
⊿ 📲 Computer	Name	Туре	Data
HKEY_CLASSES_ROOT	ab (Default)	REG_SZ	(value not set)
HKEY_CURRENT_USER	<pre>et_PTKC_GENERAL_LIBRARY_MODE</pre>	REG_SZ	NORMAL
▲ HKEY_LOCAL_MACHINE			
▷ - BCD0000000			
D HARDWARE			
SAM			
SOETWARE			
Clients			
CRYPTOCard			
JavaSoft			
Microsoft			
MozillaPlugins			
⊳ - 🐌 ODBC			
Policies			
PostgreSQL			
PostgreSQL Global De			
RegisteredApplication			
A Safenet			
A PTKC			
GENERAL			
HA			
WLD			
J SafenetLib			

#### 2. Navigate to the following path:

HEY\_LOCAL\_MACHINE>SOFTWARE>Safenet>HSM>NETCLIENT

SafeNet Authentication Service PCE/SPE with Support for HSM PSE 2 Integration: Feature Documentation Document PN: 007-013558-001, Rev. C, © Gemalto 2017. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and are registered in certain countries.

Double-click ET\_HSM\_NETCLIENT\_SERVERLIST and assign IP addresses (of both HSMs) separated by a space.

	E	dit String		×
Value name:				
ET_HSM_N	ETCLIENT_SERVE	RLIST		
Value data:				
10.164.44.3	7 10.164.44.37			
IP1	IP2		ОК	Cancel

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. <u>Note</u>: 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**.

*	Select an Adapter	x
Des	scription	_
Adn	ninToken ( )	
Adn	ninToken ( )	
	OK Cancel	

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

-	Enter PIN
	<slot2>:AdminToken ( ) Security Officer User</slot2>
	PIN •••••
	OK Cancel

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

Safenet, Inc Adapter Manager	ment 🗕 🗖 🗙
<u>File</u> <u>E</u> dit Event Log <u>A</u> bout	
Select Adapter	
Login	
Logout	
Create Slots	
Delete Slots	
Tamper Adapter	Battery Status
Upgrade Firmware	Good
Exit	O Low
Security Mode	Transport Mode
Standard PKCS#11     O Netscape	Disabled
O Entrust Compliant O FIPS 140-2	O Single Shot
○ Custom	○ Continuous
Tamper on Upgrade Mode Locked	
User ECC Params Allowed	
J	

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.

Survive, Inc. Adapter Manag	ement -
e Edit Event Log About	
Adapter Status Serial Number	
Adapter Clock     Input       Number of SI     Input       Login sta     Please enter the number of slot       Firmware vers     1	ry Status ood ow
Security Mod	sport Mode
Standard PKCS#11      Netscape	Disabled
O Entrust Compliant O FIPS 140-2	O Single Shot
O Custom	O Continuous
Tamper on Upgrade  Mode Locked  User ECC Params Allowed	

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. <u>For Uninitialized Slot</u>: 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.



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 ProtectToolkit C Key Management U Copyright (c) Safenet, Inc. 2009-	Toolkit 5\Protect Toolkit C SDK\bin>ctkmu 1  tility 5.0.0 ∙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. <u>For Initialized Slot</u>: 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.
- 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.

 Check HA Slot Configuration: Run the *ctkmu 1* (HA mode) utility to view the slots. Example: ProtectToolkit C Key Management Utility 5.0.0 Copyright (c) Safenet, Inc. 2009-2014 Cryptoki Version = 2.20 Manufacturer = Safenet, Inc. Slot0 (Slot 0) C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin>

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.

Safenet, Inc	Key Management Utility 📃 🗖 🗙
Iokens Options View Help	9 9 9 m P
Select a token:	Logged in as:
<slot0>:HSM_22</slot0>	Not Logged in
Objects on Selected Token:	
Label	Туре
	Enter PIN
	O No Login
	Security Officer
	User
	PIN
	OK Cancel

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

<b>%</b> -	C <u>r</u> eate ►	<u>S</u> ecret Key Key <u>P</u> air	
Select a <slot0>:</slot0>	<u>E</u> xport <b>Import Key(s)</b> Import Domain Parameters	Generate Key Components Enter Key from Components	
Objects	<u>V</u> iew Edit <u>A</u> ttributes		Туре
	Re <u>f</u> resh	_	

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

IV. The Generate Secret Key popup window is displayed.

<b>2</b>	Safenet, Inc K	ey Management	Utility	_		x
<u>T</u> okens <u>O</u> ptions <u>V</u> iew <u>H</u> el	p					
Select a token: Logged in as:						
<slot0>:HSM_22</slot0>		▼ User				
Objects on Selected Token:	2	Generate Secret	Кеу	x		
Lat						
	Mechanism	AES				
	Label	HSM_KEY_AES_EN	ICRYPTION_VER_1			
	Key Size (bits)	256				
	Persistant	Sensitive	Modifiable			
	Extractable	✓ Exportable	✓ Private			
	Derive	Encrypt	Sign			
	Export	Wrap	✓ Decrypt			
	Verify	UnWrap	Import			
		OK Cance	el			

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.

Iokens Options View Help   Image: Im	Safenet, Inc	Key Management Utility 📃 🗖 🗙			
Select a token: SlotD>:HSM_22   User     Objects on Selected Token:     Label   Type   Type     HSM_KEY_AES_ENCRYPTION_VER_13	Iokens Options View Help				
<slot0>:HSM_22 User Objects on Selected Token:  Label Type  → HSM_KEY_AES_ENCRYPTION_VER_13 AES</slot0>	Select a token:	Logged in as:			
Objects on Selected Token: Label Type  HSM_KEY_AES_ENCRYPTION_VER_13 AES	<slot0>:HSM_22</slot0>	User			
HSM_KEY_AES_ENCRYPTION_VER_13 AES	Objects on Selected Token:				
HSM_KEY_AES_ENCRYPTION_VER_13 AES	Label	Туре			

<u>Note</u>: 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**

- 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\_EXTRACTABLE R: CKA\_EXPORTABLE R: 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
	Key can be exported in cleartext through the
Exportable	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
Madifiable	Allow attributes to be changed after key
	generation
Priveto	Authentication required prior to security object
	being visible
Sensitive	Security sensitive attributes non-readable
Sign	Security Object supports signing
	Security Object supports unwrapping (can be
Unwrap	used to unwrap another key)
Verify	Security Object supports verification (public key)
	Security Object supports wrapping (can be used
vvrap	to wrap another key)

III. Close and reopen the Command Prompt, and run the Ctkmu 1 command.

A list of the available slot(s) is displayed. 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) C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin>\_

<u>Note</u>: 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**

- 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.

📌 Safenet, Inc Key Management Utility		
<u>Tokvins Options View Help</u>		
Select a token:	Logged in as:	
<slot0>:Test</slot0>	User	
Objects on Selected Token:		
Label	Туре	
HSM KEY AES ENCRYPTION VER 13	AES	

<mark>%</mark> Safenet, Inc Key Manage		<u> </u>
Tokens Options View He	lp	
	* * 4 12 12 12 12	
Select a token:	Logged in as	3:
<slot0>:Test</slot0>	🎽 Enter PIN	×
Objects on Selected Token:	<slot0>:Test No Login Security Officer User PIN ••••••</slot0>	уре
	OK Cancel	

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

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

🤧 Safene	et, Inc Key Management Utilit	ny la	
Tokens	Options View Help		
	Create Delete	<u>S</u> ecret Key     Key <u>P</u> air	
Select a	Export Import Key(s) Import Domain Parameters	Generate Key <u>C</u> omponents E <u>n</u> ter Key from Components	
Objects	<u>V</u> iew Edit <u>A</u> ttributes	Туре	
	Refresh		
	Mask Component Entry		

6. The Create Key Components popup window is displayed. Edit the following attributes, and click OK:

X

- a. Mechanism: Select Triple DES from the dropdown list.
- b. Check Export and Import checkboxes. Clear Private checkbox. ~

c. Clear <b>Friv</b>	
🤧 Create Key Con	nponents
2	
Mechanism	Triple DES

Mechanism	Triple DES Wrapper	
Label		
Key Size (bits)	192	
Persistant	✓ Sensitive	Modifiable
Extractable	🖌 Exportable	Private
Derive	Encrypt	🖌 Sign
Export	🖌 Wrap	🖌 Decrypt
Verify	🗹 UnWrap	🗹 Import

SafeNet Authentication Service PCE/SPE with Support for HSM PSE 2 Integration: Feature Documentation Document PN: 007-013558-001, Rev. C, © Gemalto 2017. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and are registered in certain countries. 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.

Number of Components?		
?	Number of components to cross       2       OK     Cancel	eate

- 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.

Safenet, Inc Key Management Utility	
<u>Tokens Options View Help</u>	
Select a token:	Logged in as:
<slot0>:Test</slot0>	Security Officer
Objects on Selected Token:	
Label	Туре
	Triple DES

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

Safenet, Inc Key Management Utility		
Tokens Options View Help		
Select a token:	Logged in as:	
<slot0>:Test</slot0>	User	
Objects on Selected Token:		
Label	Туре	
HSM_KEY_AES_ENCRYPTION_VER_13     Wrapper	AES Triple DES	

- 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**.

Selected Token	Test	
Selected Key(s)	HSM_KEY_AES_ENCRYPTION_VER_13	
Wrapping Key	Wrapper	-
Options		
Write to sr	mart card(s) 🗌 Use N of M	
1	Selected Smartcard	-
	Batch Name	
	No. Custodians	
✓ Write to set	elected file	
	are\AdministratorDocuments\SAS1 Exported Key	
File to write	erswammistratoribocuments/sAST_Exported_Key	
File to write	rypted part to the screen	<u> </u>

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

🤧 Safenet, Inc Key Management Utility	
<u>Tokens</u> <u>Options</u> <u>View</u> <u>H</u> elp	
Select a token:	Logged in as:
<slot0>:Test</slot0>	▼ User
Objects on Selected Token:	
Label	Туре
HSM_KEY_AES_ENCRYPTI Information Messa	ge 🛛 🗶
Wrapper Export Su	Iccessful
	OK

#### **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**.

Machine Safen	View Devices Help et, Inc Key Management Utilit:	y	
Tokens	Options View Help		
	Create Delete	<u>S</u> ecret Key Key <u>P</u> air	
Select a	Export Import Key(s) Import Domain Parameters	Generate Key <u>C</u> omponents E <u>n</u> ter Key from Components	
Objects	<u>V</u> iew Edit <u>A</u> ttributes		Туре
	Re <u>f</u> resh		
	Mask Component Entry		

- 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.

Mechanism	Triple DES	
Label	wrapper	
(ey Size (bits)	192	
Persistant	Sensitive	Modifiable
Extractable	🖌 Exportable	Private
Derive	🖌 Encrypt	🖌 Sign
Export	🖌 Wrap	🖌 Decrypt
Verify	UnWrap	✓ Import

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).

🔁 Safenet, Inc Key Management Utility	<u>_0×</u>	
Tokens Options View Help		
Select a token: Logged in as:		
<slot0>12est_SAS2</slot0>		
Objects on Selected Token:		
Ready to accept component1	×	×
Enter Hex Component (0-9, A-F)	KCV	👻 🔯 Search Documents 😥
7C7FD05D37C216C19B1AD06710850176E02AC77FD3C1C84F	3FA7F9	8= - 🗊 🕢
OK Cancel		Arrange by: Folder 🔻
📕 📗 info - Notepad		
File Edit Format View Help		
Hex Component 1:		1KB
7C7FD05D37C216C19B1AD06710850176E02AC77FD3C1C84	F	1 KB
KCV of component 1: 3FA7F9		
Hex Component 2: A431321FC8E97CAB15375B9BDFAD645EF1CD640E317AA7E	DA	
KCV of component 2: 700A92		
KCV of the SAS generated Key: 3986AD		

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)**.

🥍 Safene	et, Inc Key Management Utility	
Tokens	Options View Help	
<b>@</b> =	C <u>r</u> eate	
Select a	<u>Export</u> Import Key(s) Import Domain Parameters	Logged in as: User
Objects	View Edit <u>A</u> ttributes	Type Type
	Refresh	
	Mask Component Entry	

SafeNet Authentication Service PCE/SPE with Support for HSM PSE 2 Integration: Feature Documentation Document PN: 007-013558-001, Rev. C, © Gemalto 2017. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and are registered in certain countries.

- 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.

🔊 났enet, Inc Key Hanagement Tokens Options View Help	Utility	<u>_   ×</u>
@ <b>~ ~ * * *</b> Q 4	» 🕆 Va Va 💷 🕈	
Select a token:	Logged in as:	
<slot0>:Test_SAS2</slot0>	▼ User	
Objects on Selected Token:		
₩rapper HSM_KEY_AES_ENCRYPTION KCV of the SAS ger 3986AD	Key Label: HSM_KEY_AES Key Type: AES KCV: 39B6AD OK	

### **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.		
ON-BOARDING VIRTUAL SERV		
Shortcuts	Setup Configure database connections ar	nd sites, and install licenses.
	Task	Description
	Licenses	Install and activate licenses.
	Site	Set site import and export information.
	Permit LDAP	Permit child accounts to configure LDAP settings.
	Permit ODBC Migrations	Configure ODBC migrations of SafeNet authentication servers.
	FreeRADIUS Synchronization	Enable user interface options to configure FreeRADIUS Synchronization.
	System Configuration Details	Generate snapshots of system configuration details.
	Provisioning Delay Time	Set Provisioning Delay Time.
	HSM Database Encryption	Enable and configure token encryption key storage using a hardware security module.
	HSM Database Encryption: Apply C Enable database encryption usin HSM PIN of Slot 0 Warning: Enabling HSM use is an	Cancel Ig an HSM: © Enable © Disable In irreversible operation and may take some time to complete.
	* HSM database encryption wa	as successfully enabled. The database encryption key was already present.

## SafeNet Authentication Service PCE/SPE with Support for HSM PSE 2 Integration: Feature Documentation Document PN: 007-013558-001, Rev. C, © Gemalto 2017. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and are registered in certain countries.

## 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:

 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	Safenet, Inc Key Management Util	ity	 x
Iokens Options ⊻iew I	telp (한 주 참 1월 1월 1월 1월		
Select a token:	Logged in as:		
<slot0>:</slot0>	Enter PIN	×	
Objects on Selected Token:	<slotd>:</slotd>	<u>ype</u>	

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

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

Safenet, Inc.	Key M	Management Utility -	x
Iokens Options View Help	12 12		
Select a token:		Logged in as:	
<slot0>:</slot0>	-	User	
Objects on Selected Token:			
Label		Туре	_
	Edit Exp Del	sit Key Attributes xport key elete key	
			_

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

2	Safenet, Inc Key Management Ut	ility 💶 🗆 🗙
Iokens Options View I	eep (영 우 슈 1월 1월 1월 1월	
Select a token: <slot5>: Objects on Selected Token</slot5>	Slot5>: No Login Security Officer User PIN	pe
	Cancer	

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.

Tokens Options View Help	
4 + + + + + + + + + + + + + + +	
Select a token: Logged in as:	
<slot5>: User</slot5>	
Objects on Selected Token:	
Key Type: AES KCV: FDESOE OK	

#### **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.

HSM Token Encryption: Apply Cancel				
Enable database encryption using an HSM: <ul> <li>Enable</li> <li>Disable</li> </ul>				
HSM Pin	••••			
Warning: Enabling HSM use is an irreversible operation and may take some time to complete.				
* HSM pin has been updated successfully.				

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 1 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 1 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 International	1-800-545-6608 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 <b>SafeNet Knowledge Base</b> page. All SAS Agents documentation can be found on the <b>SafeNet Authentication Service Downloads</b> page.		