CUSTOMER RELEASE NOTES

SafeNet DataSecure and KeySecure

Version: 6.2.0
Build: 16
Issue Date: 16 Nov 2012

Contents

DataSecure and KeySecure Product Descriptions

DataSecure:

The SafeNet DataSecure appliance is fundamental in SafeNet data encryption and control solutions. Using hardware-based encryption, DataSecure appliances cover the broadest variety of data types. The DataSecure appliance provides a unified platform with data encryption and a GUI interface that can be applied to databases, applications, mainframe environments, and individual files. By providing centralized management of keys, policies, and essential functions, DataSecure simplifies administration, helps ensure compliance, and maximizes security.

KeySecure:

The SafeNet KeySecure appliance offers robust capabilities for managing cryptographic keys across their entire lifecycle, including key generation, key import and export, key rotation, and much more. KeySecure is a KMIP 1.0 standards-based enterprise key management server, so it is ready to integrate with all KMIP compliant encryption devices and software. KeySecure can be integrated through open APIs with database encryption, laptop and device encryption, and file and storage level encryption products.

KeySecure centrally manages keys using a hardened appliance, which maximizes overall security.

Below listed are main features of DataSecure and KeySecure.

Key Management

All cryptographic keys are kept in the centralized, hardened appliance to simplify administration while helping ensure tight security for the broadest array of data types. Key versioning streamlines the time-consuming task of key rotation.

Policy Management

Administrators can set authentication and authorization policies that dictate which application, database, or file servers can be accessed by particular users in the clear. When combined with strong authentication, this policy-driven security provides a vital layer of protection. DataSecure also offers granular access controls to support compliance with the separation of duties required in many security mandates. An administrator can create a policy that prevents certain users from accessing sensitive data without interfering with their day-to-day system administration duties.

Logging, Auditing, and Reporting

When encrypting data within an enterprise, data, keys, and logs are often generated, accessed, encrypted, and managed on multiple devices, in multiple locations. To reduce the cost and complexity of security management, DataSecure and KeySecure provide a single, centralized interface for logging, auditing, and reporting access to data and keys. A centralized mechanism increases security and helps ensure compliance with industry mandates and government regulations.

Broad Flexibility

KeySecure offers key management capabilities that can be integrated with virtually any commercial encryption product. SafeNet supports a wide range of open cryptographic standard interfaces. KeySecure supports the Key Management Interoperability Protocol (KMIP). Further, customers and partners can take advantage of SafeNet's XML interface to develop their own custom software utilizing the enterprise key management functionality of KeySecure.

High Availability

SafeNet customers can deploy multiple KeySecure or DataSecure appliances in a clustered configuration with real-time replication of keys, policies, and configuration information across multiple appliances - enabling complete disaster recovery and business continuity.

Release Description

DataSecure version 6.2 is supported on the following server hardware platforms:

- i150
- i450
- i460

At the release time, DataSecure version 6.2 supports the following SafeNet client platforms and versions, and previous releases. Please refer to the release notes of each client for details and latest release information.

- ProtectFile-Linux v5.4.x
- ProtectFile Windows v5.x
- ProtectDB v5.4, v6.1
- ProtectV v1.2
- ProtectApp -.NET v6.1.0
- ProtectApp-JCE v6.1.0
- ProtectApp-ICAPI v6.1.0
- ProtectApp-JCE/KMIP v6.1.0
- ProtectApp ICAPI/KMIP v 6.1.0
- Tokenization Manager v5.5.1

KeySecure version 6.2 is supported on the following server hardware platforms:

- k150
- k460

At the release time, KeySecure version 6.2 supports the following SafeNet client platforms and versions, and previous releases. Please refer to the release notes of each client for details and latest release information.

- ProtectApp-JCE /KMIP v6.1.0
- ProtectApp ICAPI/KMIP v6.1.0
- StorageSecure v1.1
- HSM Management for Luna SA and PCI 4.4 and 5.0

KeySecure version 6.2 also supports the following:

- NetApp Storage Encryption (NSE)
- Brocade Encryption Switch (BES, FS8-18 Blade)
- Quantum Scalar Tape Libraries
- HP ESL G3 Tape Library
- Hitachi VSP Native Array Encryption

Note: As a general rule, the Server version number should be as high as or higher than the client/connector version number, for supported environments.

Upgrade Information and Instructions appear below the Known Issues section.

New Features and Enhancements

Secure Key Caching for i460 and k460

On the i460 and k460, secure key caching improves performance by providing faster access to the key while maintaining data security. In SafeNet test environments, some key management operations ran 2 -3 times faster when key caching was enabled. Secure key caching stores the HSM master keys in the process memory of internal servers. To ensure security, these keys are obfuscated, and they are never swapped to disk. On a KeySecure, only the HSM keys that are specific to the KeySecure VM are cached; the SSKM VM keys are not. FIPS compliance is not compromised by enabling secure key caching.

Administrators can enable and disable secure key caching by using CLI commands on the i460 or k460 as described in the User Guide and the CLI Guide.

Certificate Management

KeySecure and DataSecure now provide a mechanism to manage Certificates imported over KMIP (the Key Management Interoperability Protocol). The new Certificate management feature extends the support of cryptographic objects to cryptographic certificates, significantly enhancing the range of objects managed by enterprise security systems using the well-known published protocol. This capability complements existing support for symmetric and asymmetric keys and certificates imported over the proprietary NAE-XML protocol.

Certificate management options include many of the operations familiar to those working with keys over SafeNet's NAE-XML protocol. When managing certificates using the KMIP protocol, Administrators can import, query, download and delete certificates. They may also assign KMIP-defined or custom attributes to the objects under management and use them in a number of customer-specific key-management applications. All certificate related operations, such as registration and retrieval, are audited and logged.

Certificates used in web and application servers can be imported or exported programmatically by a KMIP client such as SafeNet JCE/KMIP client.

Retry Key Replication across Cluster

The replication of security configuration data such as encryption keys across a cluster may fail due to various network related issues. The Management Console now consolidates all failed key-related operations (create, modify, delete) in a single page, which in itself is a useful resource. Administrators referring to this page will find it even more useful because it enables them to explicitly select and retry the operation. Note that only the most recent instance of a failed operation is shown. In the Management console, see Device » Cluster » Retry Replication.

Improved Device Statistics Page in Management Console

The Statistics page provides real-time system statistics about client connections and network throughput; and about the utilization of cache, CPU, and memory. The modified page displays information about the cryptographic requests made to the NAE-XML server. You can now reset the page to start a new session of statistical data collection without restarting the server.

Improved Replication across Cluster using Asynchronous Replication

Replication stability and performance have been improved.

Advisory Notes

Initialization

After initializing the Data Secure/KeySecure, the command line prompt instructs you to press Return to continue. If you do not press Return and end the console connection before seeing the login prompt, you will not be able to establish a new console connection until you reboot the DataSecure/KeySecure.

FIPS-140-2 approved mode considerations

Warning: Changing the FIPS policy on the k460 HSM is a destructive process. If the HSM contains data, make a comprehensive system backup prior to changing the FIPS mode. Detailed instructions for setting FIPS mode operations are provided below the Upgrade Instructions heading later in this document. If you have already used the HSM when it was not set to FIPS mode, and you now need to change to FIPS approved Mode, follow these instructions. After reviewing the procedures as documented below, contact SafeNet customer support if you have

any doubts about how to proceed.
Ref: DS-4719

Notes:

- SSKM instructions such as backup and restore SSKM configuration, export and import SSKM keys, and zeroize SSKM are all done through the SSKM interface, also known as the SSMC (StorageSecure Management Console), not with KeySecure or the HSM. For guidance, refer to the StorageSecure Key Manager User's Guide.

DataSecure and KeySecure no longer provide the "Disable RSA Encryption and Decryption" option.
This was necessary to allow clients to perform key wrapping and unwrapping (encryption and decryption) using RSA keys. Using RSA keys to encrypt key data does *not* compromise FIPS compliance, whereas applying RSA keys to user data *does*. To maintain FIPS compliance, do not use RSA encryption and decryption on user data (credit cards, social security numbers, medical records, etc.). If you restore an older backup which has this setting enabled, the 6.2 software will ignore the RSA Encryption and Decryption setting from the configuration.

Backup and Restore

- The time required to restore a backup is directly related to the number of keys in the backup file and can take several hours when restoring hundreds of thousands of keys.

- Special characters (including a space) are not allowed in a backup file name. When naming a backup, use only alphanumeric characters in a solid string. Users are not overtly prevented from entering special characters, and the logs do not explicitly warn about the failure of the backup.

Ref: DS-7351, DS-7284

Importing Keys and Certificates using NAE-XML
When importing RSA keys using NAE-XML protocol, the Public key must be imported. Because the Private key holds the Public key, if you import the Private Key, then you will not need to import the public key separately. To import certificates stored in a Netscape database to a KeySecure, you must convert the individual certificates to a format that the KeySecure can use. PKCS#12 format will work, and can be used to import both the certificate and key in PKCS#12 format. You can find more information and tools for this conversion process at http://www.mozilla.org/projects/security/pki/nss/tools/pk12util.html.

Certificate Authorities
Chain revocation is not supported for Certificate Authority Certificates. If a CA certificate is revoked, the certificates signed by the CA certificate are not automatically revoked. Those certificates must be revoked individually. Installing a known CA certificate more than once on a KeySecure can render, under some circumstances, the CRL information unreliable for that CA. In such cases, a certificate that was revoked by that CA actually appears as active. Before installing a known CA, consult the list of CAs on the KeySecure. Do not install duplicates. CAs issue serial numbers to the certificates they sign in order to keep track of them. Local CAs use a seed value to determine the serial number. Each time a certificate is signed, the seed value is incremented. If you back up a local CA, continue to issue certificates with that CA, and then restore the backup, you might disrupt the CRL operations on that local CA, because the seed value before restoring the backup local CA will be x + n, where n is the number of certificates signed by that local CA since the backup was created. When the backup is restored,

the seed value for the local CA will revert to x. As such, it is possible that the local CA will issue identical serial numbers to multiple certificates. To avoid this problem, back up local CAs after using them to issue certificates.

Algorithm Support
HmacSHA512, HmacSHA384, and HmacSHA256 are not supported by KMIP Create Request; use Register Request instead.

Group Permissions and Certificates
Group permissions specified for groups of certificates will not have any effect.

Resolved Issues, Known Issues and Workarounds

Issue Severity and Classification

The following table serves as a key to the severity and classification of the issues listed in the **Resolved Issues** table and the **Known Issues and Workarounds** table, which can be found in the sections below.

Severity	Severity Classification	Definition
C	Critical - C	No reasonable workaround exists
H	High - H	Reasonable workaround exists
M	Medium - M	Medium-level priority problems
L	Low _- L	Lowest-level priority problems

Resolved Issues

Severity	Issue	Synopsis of Resolved Issue
M	DS-4779, DS-4781	**Summary:** Password corruption. Fixed: On the HSM page in the GUI, if you click the set password button and make no change whatsoever to the password value, then click on Save, the result is a corrupted password. The Firefox browser in particular does not display the expected characters when user clicks the Set Password button.

Severity	Issue	Synopsis of Resolved Issue
L	DS-3004 (MKS165946)	**Summary:** Special characters (including the space) are not allowed in a backup file name. Special characters (including the space) are not allowed in a backup file name, but the user is not overtly prevented from entering special characters. The logs do not list all pieces of potentially useful data related to the failure of the backup.
L	DS-3143	**Summary: The "zeroize all keys" function may hang.** The "zeroize all keys" function may hang if executed during any other activity on the server. Rebooting the box will solve this problem. Recommendation: Do not run "zeroize all keys" on the CLI when there is activity on the box.
M	DS-2863 (MKS154301)	**Creating Multiple large-size Remote Key Foundry (RKF) keys** When creating multiple large-size RKF keys, such as keys 4K in size, or especially 8K, you should pause the operation after the UI returns from the creation phase of each key. This pause is crucial if the UI returns a warning message about KS time-out while communicating with HSM. If you do not voluntarily observe this delay, you should expect errors when you attempt to create the next several RKF keys. We recommend that you delay from 45 seconds to 1 minute after initiating each creation operation to allow for processing. Be aware that the creation of these RKF keys is only enabled when HSM Management is enabled.
M	DS-3204, DS-3205, DS-3206	**CLI commands corrections have been added to CLI Guide** Correction have been made to the following CLI command documentation: • show Ethernet port • show gateway • show mac address.

Known Issues and Workarounds

Severity	Issue	Synopsis
M	DS-3173, DS-7051	**With the FIPS settings turned on (that is, when Disable Non-FIPS Algorithms and Key Sizes is ON), DataSecure does not support SHA1withRSA in the CryptoRequest (NAE-XML) signing operation.**

Severity	Issue	Synopsis
M	DS-7284	**Auto-Backup error…** When creating a backup file location, if you make an error in specifying the target directory name for the backup file, then the backup may fail, and an error message will be generated, which is associated with failure to delete the existing backup copy. The real issue appears after this user error has occurred: after subsequent backups that succeed (when correct backup file path/name data is provided), error messages continue to appear even though the backup succeeds and the backup copy is replaced successfully.
L	DS-7361, DS-7326	**CLI commands that enable and disable Secure key cache CLIs don't return an error on i150, k150 and i450 platforms.** **Workaround:** Secure key caching is available only on k460 and i460 platforms. The two related CLI commands, **hsm disable secure-key-cache** and **hsm disable secure-key-cache**, should not be used with the i150, k150 and i450 platforms.
M	DS-4798, DS-7364	**When using Key Query or Certificate Query, searches based on some certificate properties do not work.** When defining a query that filters certificate data, if you select a field that begins with the string “Certificate Subject” or “Certificate Issuer”, the search results will be misleading. A query that is based on one of these fields always returns a null set.
M	DS-7356, DS-7357, DS-7358	**KMIP Locate request by Certificate Identifier, Certificate Issuer and Certificate Subject is not supported.**
M	DS-7302	**Certificate managed object queries are not showing up in create backup page.**
L	DS-7301	**You cannot choose a subset of certificates to back up.** You should be able to create a certificate backup that selects just one, or some subset, of the certificates by using the Choose From Query option to back up. **Workaround:** Perform a backup of all certificates if you cannot backup the subset you want. Better to be safe.

Severity	Issue	Synopsis
H	DS-7378	**Remote Administration Settings do not allow login from a browser with a properly created certificate.** After using SSL to create a web client server certificate, signing the certificate with a CA on the DataSecure, and setting up Remote Access to use that list, you should be able to import the certificate and then log into the device with the signed certificate. The login process seems to proceed normally, and asks you to verify that you are using the certificate, but it does not log you in.
L	DS-7413	**On the Retry Replication page, the time is shown as UTC, not local time** In the Management Console, the Replication failure time on the Retry Replication page is shown as UTC. All log files provide time data that has been adjusted for the local time zone. Unless your local time zone the Greenwich meridian, the Replication failure time on the Retry Replication page is incorrect. **Workaround:** Apply the standard adjustment differentiating your time zone from UTC to the time displayed on this page.
L	DS-7381	**Certificate Properties modification not supported in 6.2.0.** Certificate properties such as certificate name and certificate owner currently are not modifiable.
M	DS-7442	**KMIP Register request for certificate doesn't support Link attribute.** **Workaround:** Use KMIP Add Attribute request to add Link attribute to a certificate managed object.
L	DS-7355	**Online help still shows documentation for Import a Certificate as a Key** The GUI now enables you to import certificate using a newly supported KMIP Certificate section only. Import certificate is available at this location in the Management Console: Security » Certificates » Import Certificate. Documentation for this function under Security » Keys is no longer valid.
H	DS-4723	**Failure to Sign Request** When the HSM is zeroized, the user cannot use local ca to sign certificates. Zeroizing HSM renders all keys, certificates and local CA's unusable. An attempt to use local-ca for signing may show success when the signing did not actually succeed. This misleading error message may incorrectly appear: "Certificate request has been signed." **Workaround:** Create a full backup before HSM zeroization, then delete all keys, certificates and local CAs; and then restore the backup after HSM reinitialization.

Severity	Issue	Synopsis
M	DS-4725	**On KeySecure, the command hsm generate certificate does not correctly update the HSM status** When HSM is reinitialized, using the “hsm generate certificates” command does not result in any failure when SSKM is running, although certificates are not actually generated. **Workaround:** Stop SSKM by using the "sskm halt" command, then run the "hsm generate certificates" command.
M	DS-3074	**Creating a backup using FTP or an automated scheduled backup with FTP is not supported.**
L	DS-2700	**Incorrect password entered during the first run after the HSM initialization, password rejected.** If you enter an incorrect password during the first run after the HSM has been initialized, the first run does not accept the correct password as valid. Note that you can press <n> (the line break or end-of-line marker), to get out of the password re-entry loop. **Workaround**: Set the HSM password and Crypto User login through commands, as follows: 1. Skip setting the password if it fails. 2. Let the first run complete. 3. Reboot 4. Set hsm password through "hsm set password" command. 5. Do hsm crypto-user login through "hsm login crypto user" 6. Configure SSKM and start it through "sskm interface" and "sskm start" commands…...
L	DS-3144	**A local CA: ham_mgmt_ca and an ssl cert: nae_kmip_server are automatically set up on both i450 and k460, when they are needed only on the k460.** After installing the OS on to an i450 server, both the local CA hsm_mgmt_ca and ssl cert nae_kmip_server are set up. In fact, they are only needed on the k460. These should be set up only on the k460 platform, not the i450. **Workaround:** On an i450, the CA and ssl cert can be removed if desired.
M	165944	**Log file base names do not currently support the use of a space in the name.** Backup (immediate or scheduled) silently fails, despite logged confirmation, when there is a space in the log file base name.

Severity	Issue	Synopsis
M	128873	**During an Administrator lockout period, which begins when any Administrator is locked out, attempting to change any Administrator password through the CLI will permanently disallow use of that password** **Summary:** When the Administrator Lockout Period is engaged, attempting to change any administrator password using the CLI will permanently lock that account. For example, if Administrator One failed 5 consecutive login attempts, then a lockout commences. Suppose that, during the resulting lockout period, the CLI is used to change the password of Administrator Two. In this scenario, the password change will fail and Administrator Two will be permanently locked out. **Best Practice:** After failing multiple consecutive login attempts, wait for the Administrator Lockout Period to expire prior to taking any further administrative account action using the CLI. The default lockout time is 5 minutes for the serial console and 30 minutes for the remote access (either the Management Console or the remote CLI using SSH).
L	122526	**System does not currently support the detection o the BIOS version.** **Summary:** After rebooting the device, you may see the following error message in the System Log: localhost System Health: Could not detect current BIOS version. Error 1. This message can be ignored.
M	121747	**Networking: Route Table Creation is Not Working Properly When Multiple IPs are Configured for a Single Ethernet Port** **Summary:** Adding multiple IP addresses to a single Ethernet port and then deleting some of those IP addresses can cause the routing table to become out of sync. Modifying the default gateway when the routing table is in this state can cause the system to lose the default gateway settings.
M	120712	**String-based Key Queries Time Out on Devices Containing 1 Million Keys** **Summary:** When using a key query to search for key names containing a specific value, if the device holds 1 million keys, the key query will time out after ten minutes.
M	100536	**SNMP XML Key statistics Missing Failed Key Import Requests** SMNP statistics do not report KeyImport requests – they are always 0. The statistics reported on the Management Console (Device >> Statistics >> NAE-XML Statistics) and the CLI (show statistics) are correct.

Severity	Issue	Synopsis
M	85494	**Cluster: After Removing Node, Cluster Page Still Shows Node Information** **Summary:** If removing a node from a KeySecure cluster takes longer than 30 seconds, the Management Console reports an error even though the node is removed. After clicking Remove from Cluster the node may remain in the cluster list. **Workaround:** Clicking Remove from Cluster a second time will remove it from the Management Console's list.
L	60022 57596	**Log Signing While the KeySecure is Under a Heavy Load** **Summary:** If the KeySecure is under a heavy load - performing more than 3000 operations per second – enabling the Log Signing feature will slow the log rotation mechanism to the point where the server will not be able to rotate and sign the log files quickly enough. This can potentially disable the logging feature. **Workaround:** Do not enable log signing when the KeySecure is expected to operate under a heavy load.
L	59942	**Advancing the System Date Can Render the Software Check Invalid** **Summary:** Setting the system date beyond 02/18/2017 causes the KeySecure to fail the software integrity test. **Workaround:** Do not set the system date ahead of this date. New software signing certificates will be issued as needed.
M	59245 57588	**Log Signing Feature** **Summary:** When enabled, the Log Signing feature uses a large percentage of system memory. **Workaround:** Disable log signing to decrease memory usage by up to 5%. Workaround info may be incorrect: issue 59245 says, "The total memory usage went up to 80% (i426, i416)." And "the memory use went down to 5% after turning log signing off."

Severity	Issue	Synopsis
M	48080	**Key Generation Requests and Key Permissions** **Summary:** Users cannot see keys that they do not have permission to use. However, when a user tries to create a key using the XML interface, the request will be refused if another key already uses the keyname provided in the key generation request. This is true even if the user does not have permission to view or use the existing key. As such, a user can discover the names of existing keys by making key generation requests with various names until a duplicate name is found. **Workaround:** Do not enable the **Allow Key and Policy Configuration Operations** checkbox for the NAE-XML protocol. This is disabled by default. To check the setting, navigate to Device >> Key Server. Select the NAE-XML protocol and click **Properties.**

Upgrade Information and Instructions

Supported Upgrade Paths

The following upgrade paths are supported:

- For i150, i450, k150: 5.4 → 6.2.0
- For i150, i450, k150: 6.1.1 → 6.2.0
- For i460, k460: 6.1.2 → 6.2.0; note that only 6.2.1 HSM (K6) firmware is supported

Note: To upgrade from a patch to a new release, you must first roll back the patch software and then upgrade.

Always make a complete backup of all systems before upgrading.

Upgrading to Version 6.2.0 using the CLI

To upgrade the software:

1. Log in to the CLI as an administrator with Software Upgrade and System Health Access Control.
2. Enter configuration mode by typing config.
3. Execute the software install command.
4. Select the method you'll use to upload the new software. SafeNet recommends SCP, which works on more platforms, including Windows. Then enter the host, filename, username, and password. If the information is correct, click Confirm to start the upgrade process.
5. Wait while the DataSecure downloads and installs the new software. This will take a few minutes. The CLI will indicate the status of the process. After the software is installed, the DataSecure will reboot. Again, this will take a few minutes. During the reboot you will lose all client connections.

6. Check that the upgrade was successful by logging in to the CLI. Run the show software command to see the current software version.

Safely turning on the FIPS Mode Settings (for k460/i460 devices)

Note: If your device came from the factory set up with the "FIPS mode" setting turned on, then the following information does NOT apply to you.

Pre-requisite - Before you start:

Verify if the HSM is set to use only FIPS-140-2 approved algorithms by running the command as shown below, then follow the instructions for your situation:

```
<DemoBox># hsm fips show
```

One of the following responses will appear:

- `"HSM policy is set to be in FIPS approved mode"`

or

- `"HSM policy is set to be NOT in FIPS approved mode"`

→ If your `hsm fips show` test indicates that HSM policy is already in FIPS approved mode, then this advisory note does not apply to you. Stop.

→ If you are NOT in FIPS approved mode, but you have ***never*** used the HSM: Create a backup as a precaution, and then perform the initialization process from scratch, starting from step 1of the instructions in the Quick Start Guide for your device. There is one addition to these steps: If you are using the k460, you should temporarily halt SSKM while creating certificates.

→ If you are NOT in FIPS approved mode, and there is data on the HSM, and you have used the device: Plan to completely backup and restore all information associated with the current device. When you use the `fips on` command, you will delete partitions and the data in them, SSKM information (if you use SSKM), and also the Crypto User data, from your HSM. Your complete backup of all this information will enable you to recover all crucial data after you reinitialize your HSM. Follow the instructions below. Be aware that your Security Officer key and Domain key will still function after you re-initialize your HSM.

Note: To change HSM FIPS policy, you must be able to login as an HSM security officer.

A. **CRUCIAL: First create a complete system backup!**
Do not proceed until you are certain that you have created a complete backup of all components as described below.

- Create a complete KeySecure or DataSecure Backup. Refer to the KeySecure or DataSecure User Guide for instructions.
- If SSKM is running, create a backup of SSKM using the StorageSecure Management Console (SSMC). Refer to the StorageSecure Key Manager User's Guide for SSMC instructions.
- Export SSKM keys using SSMC.

- Zeroize SSKM using SSMC.

B. Enter Config Mode.

```
<DemoBox># config
```

C. Stop SSKM. Use this command:

```
<DemoBox># sskm halt
```

D. Logout Crypto User

```
<DemoBox># hsm logout crypto user
```

The CLI should display the following messages. Respond Yes (y) when asked if you want to log out.

```
Logging out of HSM could cause failure in applications that use HSM
Are you sure you want to log out? y/[n]: y
Logged out of HSM partition successfully
```

E. Login as Security Officer (requires blue key)

```
<DemoBox># hsm login security officer
```

F. Set the HSM to be in FIPS mode. You must be prepared to delete any existing HSM partitions and data. Execute the commands below.

```
<DemoBox># hsm fips on
```

The CLI should display the following message:

```
------------------------------------------------------------------
WARNING: CHANGING DEVICE's FIPS POLICY DESTROYS ALL HSM PARTITION
         CONTENTS REQUIRING RE-SETUP OF PARTITION IT IS RECOMENDED TO
TAKE SYSTEM BACKUP BEFORE PROCEEDING FURTHER
------------------------------------------------------------------
Are you SURE you want to proceed? [n]/y: y

'hsm changePolicy' successful.

Policy Allow non-FIPS algorithms is now set to value: 0

Please setup HSM partition again
```

G. R e-initialize the HSM, using the following steps:

- Zeroize HSM

```
<DemoBox># hsm zeroize
```

```
Warning: zeroizing the HSM will cause all of your keys, certificates,
and local CAs to be inaccessible.
```

```
CAUTION:  Are you sure you wish to reset this HSM to factory
   default settings? All partitions and data will be erased.
   Partition policies will be reverted to factory settings.
   HSM level policies will not be changed.
   Type 'proceed' to return the HSM to factory default, or
   'quit' to quit now.
   > proceed
'hsm factoryReset' successful.

Please wait while the HSM is reset to complete the process.
```

- Initialize HSM (Requires Blue and Red Key)

  ```
  <DemoBox># hsm initialize
  ```

- Create partition (Needs Black and Red Key)

  ```
  <DemoBox># hsm create partition
  ```

  Save the password displayed. You will need it later.

- Generate certificates for HSM

  ```
  <DemoBox># hsm generate certificates
  ```

- Save password for partition

  ```
  <DemoBox># hsm set password <Password as displayed on PED>
  ```

  Keep the password safe and secure. You will need it later.

- Login crypto user

  ```
  <DemoBox># hsm login crypto user
  ```

- Check fips mode

  ```
  <DemoBox># hsm fips show
  ```

  The following response *must* appear:

  ```
  HSM policy is set to be in FIPS approved mode
  ```

H. Restore the KeySecure or DataSecure backup. Refer to the appropriate User Guide for instructions.

I. Restart SSKM:

```
<DemoBox># sskm start
```

J. Restore SSKM backup

- Restore SSKM backup.
- Import the SSKM keys.

  Refer to the StorageSecure Key Manager User's Guide for instructions.

Product Documentation

The following product documentation is associated with this release:

- DataSecure User Guide for Version 6.2.0
- KeySecure User Guide for Version 6.2.0
- KeySecure Command Line Interface (CLI) Guide 6.2.0
- DataSecure Command Line Interface (CLI) Guide 6.2.0

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Technical Support Information

If you have questions or need additional assistance, contact Technical Support through the listings below:

Customer Connection Center (C3)	
http://c3.safenet-inc.com Existing customers with a Customer Connection Center account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	
Support and Downloads	
http://www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Email-based Support	
support@safenet-inc.com	
Telephone-based Support	
United States	(800) 545-6608, (410) 931-7520
Australia and New Zealand	+1 410-931-7520
China	(86) 10 8851 9191
France	0825 341000
Germany	01803 7246269
India	+1 410-931-7520
United Kingdom	0870 7529200, +1 410 931-7520