Sansec HSM

User Manual v2.2

Beijing Sansec Technology Development Co., Ltd.

July 2016

Welcome to use SANSEC HSM

The contents of this document are subject to change with or without notice. Any changes to content will not be included within this publication but will be in a newer release. Our company makes no express or implied warranties, including the content of the manual on merchantability or implied warranties for the specific purpose.

In accordance with the copyright laws of China, our organization has exclusive rights and authorities to these resources. No additions, deletion, adaptation, reproduction, modification or imitation permitted without our organization's written consent.

Beijing Sansec Technology Development Co., Ltd.

May 2016

Table of contents

1. Product Overview

1.1. Product Introduction

Sansec HSM is a special device developed and designed by Beijing Sansec Technology Development Co., Ltd. combined with the characteristics of domestic and foreign financial business applications. It's mainly used for the host application layer to encrypt and decrypt data, verify message source correctness and do key management etc. It can also provide secure data communication services for the networking information systems to prevent fake cards and other frauds effectively.

The HSM is a high-end information security device. It connects with the business host through the TCP / IP protocol , with high processing power, stable performance and other characteristics, applicable to all types of financial information systems, especially for cross-regional and cross-agency financial transaction systems to provide data encryption and security protection. It can be widely used in banking, securities, public transport, petrochemical, urban card and other computer network systems.

1.2. Product Functions

1.2.1.Standard Functions

Sansec HSM is a host peripheral, using its own complex DES, RSA, SM2 and other encryption algorithms to provide information encryption to ensure that the network and point to point data security, including the data security on the host and network communication are working properly.

In general, the standard functions are as below:

- Support ATM, POS and other services provided by banks.
- Support ANSI and ISO security standard.
- Support PIN forwarding and verification.
- Support verification of Message authentication Code (MAC).
- Support transaction integrity verification.

- Support the conversion between DES / 3DES / AES algorithms and Chinese financial encryption algorithms (SM1 / SM4).
- Support IC card key management and card issuing system.
- Support key management .
- Support complete hardware based true random key generation.
- Large-capacity key secure storage space.
- Support key generation, distribution, backup, and update.
- Support cipher-text data conversion function when the HSM replaces the local master key.

1.2.2.Extended Function

- Support the generation and storage of RSA key pair, with 2048/3072/4096Bits.
- Support the generation and storage of SM2 key pair, with 256Bits.
- Support the generation and storage of ECDSA key pair, with the curve P-256/P-384/P-521.
- Support a variety of Public-Key Cryptography Standards, such as PKCS1, ANSIX9.31, EMV2000, etc.
- Support RSA, ECDSA, SM2 signature and verification of data.
- Support RSA, SM2 data encryption and decryption operations.
- Support the importing of RSA public and private key pairs into the HSM in a indexing way.
- Use physical hardware to generate true random numbers.
- Support cryptography letter, cryptography application letter and key letter printing function, serial port communication parameters and communication format configuration (support communication speed of 300 ~ 115200bps, 7N1, 7O1, 7E1, 8N1, 8O1 and 8E1 and other communication formats).

1.2.3.Physical Interface

- Support TCP/IP protocol，and 10/100/1000M adaptive。
- Support gateway setting configuration function when used in cross-network segment.

- Support white list function, and client access HSM IP address filtering function.
- Support configuration of the number of TCP socket connections , up to a maximum of 4096 .
- equipped with Independent key management port, host port, printing port; support a variety of communication protocols that work in parallel.

1.2.4.Stability and Security

- System is very stable because its research and development are based on a high stability, optimized, dedicated operating platform.
- Hardware design stratifies FIPS140-2LEVEL3 standard, so it has high security.
- Support hierarchical authority management function , so the security of the devices improved. .
- Management commands such as critical operations and key import / export / conversion need to be executed under administrative privileges.
- Support the master key's backup to secure media and recovery from secure media to HSM.
- Support physical double protection mechanism to ensure that the cryptography system has anti-spying functionality and radiation protection.

2. Key Concepts

- **Device ID**：The device serial number on the label. It consists of the production date, production batch and a serial number. Combined with the product model, it can uniquely identify with each product.
- **Device model**： Encryption product model approved by the national cryptography management agencies.
- **Digital envelope**：A method of enveloping which uses data encryption keys to protect data and the recipient public key to encrypt and protect the data encryption key
- **Digital signature**：Signature data attached to the data. It is used to protect and verify the data source and its integrity as well as to prevent counterfeiting and denial of issuing.
- **Key components**：At least two random or pseudo random parameters with key features of the encryption key. The cryptographic key is made through a combination of one or more of such parameters.
- **Key segmentation**：The key segments are distributed among several key managers; the key can only be fully recovered when a minimum number of key managers are present to restore the key.
- **Key encrypts key（KEK）**：The key used to encrypt the session key or file key. Also known as secondary key or key for transporting key. Each node in the communication network is assigned one such key.
- **Key index**：The value that represents the numerical key location within the device or system。
- **Private signature key**：Private key used for signature calculation.
- **Private encryption key**：Used for implementing the private key for data confidentiality.
- **Private key access control code**：The password used for obtaining the private key.

- **Symmetric/private keys**：The keys used by a group of specific entities when using symmetric cryptography.
- **Session key**：Key of the lowest layer within the key management system. The key is only used for a session within a limited time and will be deleted once the session ends.

3. Quick start guide

a) Device installation

For more details on installation, refer to chapter 4.1

b) HSM connection

For more details refer to chapter 4.2: Login to HSM

c) Run management tools

For more details refer to chapter 4.3: Start up management program

d) Installation wizard

For more details refer to chapter 4.4: Installation wizard

e) Administrator and operator

For more information, refer to section 6's administrator guide (chapter 6.5) and operator guide(chapter 6.6).

f) Modify PIN password

For more information, refer to section 6's "modify user password (chapter 6.4)"

g) RSA key management

For more information, refer to section 7's "RSA key management (chapter 7.3)"

h) ECDSA key management

For more information, refer to section 7's " ECDSA key management (chapter 7.5) "

i) SM2 key management

For more information, refer to section 7's " SM2 key management (chapter 7.4) "

j) Symmetric key management

For more information, refer to section 7's "Symmetric key management (chapter

7.5) "

k) Network configuration

For more information, refer to section5's "viewing/modifying network configuration(chapter 5.4) ".

l) Service management and configuration

For more information, refer to section8's "Service management "

m) Backup and recovery

For more information, refer to section 7's " Backup and recovery(chapter 7.6) "

n) Key destruction

For more information see chapter 7's key initialization part(chapter 7.1)

4. Installation

4.1. Installation

a) Open the HSM installation package and check the contents list to make sure that your set is complete with all of the equipment and accessories.

b) Remove the machine from the package and set it up in an appropriate installation location.

c) Connect the device to a power supply.

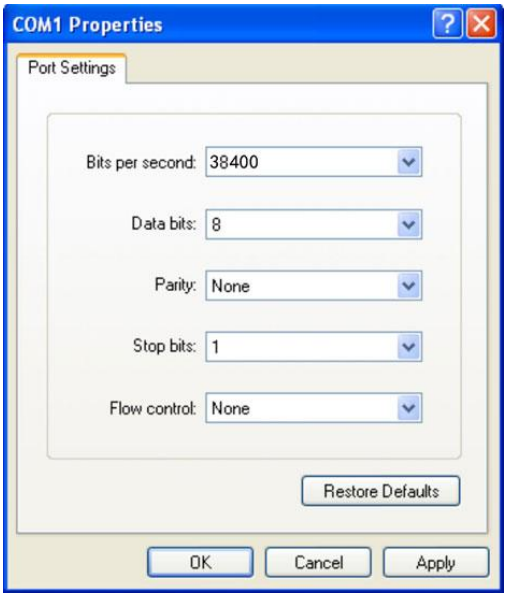
d) Turn on the device by pressing the power button and startup the machine.

4.2. Device management

a) Use the serial port control cable to connect the HSM to a personal computer with Windows operating system installed.

b) Run the "HyperTerminal" tool that comes with the Windows operating system, which can be found from the "Start menu" -> "All Programs: -> "Accessories" -> "Communication" -> "HyperTerminal". You can also use other terminal software with a serial port connectivity function, such as SecureCRT, PuTTY, NetTerm and so on.

c) Select "New Connection", then select the corresponding COM port. On the "Port Settings" part of the " per second number", select the baud rate value of "38400" as the following picture shows:



d) After connecting to the terminal, press any key, the shell interface will appear.

4.3. Start up Management Program

a) Connect to the HSM

b) Run management program: execute the "hsmm" command to start the Sansec HSM management program.

Management program main interface is shown as below:

```
<---------- SANSEC HSM Management Application[v2.5]---------->

Welcome:

Welcome to use SANSEC HSM. More information about SANSEC product:
http://www.sansec.com.cn

 ->1| User Login
     |  The appropriate administrative functions can be performed after administrators or operators log in.
   2|System Management
     | View device information and system running status.  Configure network parameters;
   3| Authority Management
     |  Management functions for administrators and operators.
   4 | Key Management
     |  View key information and generate or delete key pair.
   5 | Sevice Management
     |  Configure service parameters;
          View service status;
          Start or stop service;
   6 | Backup and Recovery
     | Back up the key information to file or restore key information from file to  cryptography module.
   7 | Installation Guide
     | Complete the basic configuration of HSM according to the guide when the first time using it.
```

4.4. Installation Wizard

If this is the first time you have used this device, you can run the step by step installation wizard to complete the basic configuration. If you need to use other configurations, refer to other parts of this chapter for more management operation instructions.

The wizard contains the following configuration functions:

a) **Device initialization**：Clear up all keys and the corresponding management **information**

b) **Add administrator**：To ensure the safety, reliability, and proper use of all the system features, it is recommended to set up three administrators

c) **Add operator**：For starting cryptographic service.

d) **Local master key management**：Set the new master key to ensure the storage security of other keys.

e) **Symmetric key management**：Used to generate the symmetric key required in the business system.

f) **RSA key managemen**t：Generate RSA key pairs and save them into the device.

g) **ECDSA key managemen**t：Generate ECDSA key pairs and save them into the device

h) **SM2 key management**：Generate SM2 key pairs and save them into the device.

i) **Network configuration**：View or modify networking configuration parameters of the devices.

j) **Device maintenance information**：Set up application system name, device maintenance personnel and other information.

k) **Service information configuration** ：Modify service startup parameters

l) **Client authorization**：modify the service authorization whitelist, access control.

m)**Backup key information**：Encrypt important key information and backup to file for safe storage.

5. System Management

5.1. Checking on Device Basic Information

Product information, such as producer, device serial number, system version, supported algorithms, etc., are shown below.

```
Device basic information:
-----------------

    Successfully read device information.

     |     Item      |   Return value
   _|_______________|_____________________________________________________
   1|   Manufacture | SANSEC
   2| Product Model | secHSM V2
   3|  Product No.  | SJ6A21-SC9EDLR
   4|  Serial No.   | 2015040714501174
   5|   Version     | v2.00.0001
```

5.2. Viewing /Modifying Device Maintenance Information

Users can view or modify device maintenance information.

```
Modifying device maintenance information:
-----------------
     |        Item         |              Value
   _|_____________________|_____________________________________________
   1|  *Application name  |  ** application
   2|    Company name     |  Sansec
   3|      Department     |  Product department
   4|  *Principal of maintenancing device   |  GAO
   5|    *Tel.number      |  010-84109583
   6| Mobile phone number|  13333333333
   7|      E-Mail         |
```

5.3. Viewing Device Operating Information

```
Viewing device operating information：
-----------------
  _|_____________________|_____________________________________________________
  1|      Encryption service                |   Running
  2|    Memory utilization                  |   0.93%
  3|    Current number of occurrences       |   0
```

5.4. Viewing /Modifying Network Configurations

View or modify network configuration parameters such as IP address, gateway, etc.

```
Modifying network configurations：
------------------
     |          Item              |                    Value
   _| _________________________|_____________________________________________
   1|         * IP address       |   192.168.1.209
   2|       *Subnet mask         |   255.255.255.0
   3|       Default gateway      |   192.168.1.1

   4|    Enable the above configuration immediately.

Select the function to be performed or [Quit(Q)] [Next Step(N)]>
```

5.5. Viewing /Modifying Financial Application Parameters

View or modify financial application-related parameters such as header length, PIN length and so on.

```
Modifying financial application parameters:：
------------------

     |          Item                          |                    Value
   _| _____________________________________|_____________________________________
   1| Default length of PIN[4~12]            | 6
   2| The length of encrypted PIN[5~13]      | 6
   3|The length of zone master key           | 16
   4| The length of message head [0~255]     | 0
   5|The baud rate of printer                | 9600
    |                            |
   9|Set test key for LMK        |
```

5.6 View management audit log

View audit log needs that log in the auditor.

```
Management log:

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

 ->1|View recent management logs
    |
    |    Ctrl+f for next screen, Ctrl+b for last screen.

   2|View history logs
    |
    |    Ctrl+f for next screen, Ctrl+b for last screen.

Select the function to be performed or [Quit(Q)] [Next Step(N)]>1
```

```
Management logs:

-------------
[2017-09-04 14:07:14][swhsm:start hsmm success.]
[2017-09-04 14:07:18][swhsm:start hsmm success.]
[2017-09-04 14:11:19][swhsm:start hsmm success.]
[2017-09-04 14:12:06][swhsm:Operator log in success。]
[2017-09-04 14:12:13][swhsm:start hsmm success.]
[2017-09-04 14:12:20][swhsm:start hsmm success.]
[2017-09-04 14:12:55][swhsm:Administrator 3 log in success.]
[2017-09-04 14:13:35][swhsm:Administrator 2 log in success.]
[2017-09-04 14:13:53][swhsm:Administrator 1 log in success.]
[2017-09-04 14:14:37][swhsm:start hsmm success.]
[2017-09-04 14:15:31][swhsm:start hsmm success.]
[2017-09-04 14:16:58][swhsm:start hsmm success.]
[2017-09-04 15:25:22][swhsm:start hsmm success.]
[2017-09-04 15:26:19][swhsm:Administrator 1 log in success.]
[2017-09-04 15:27:14][swhsm:Administrator 2 log in success.]
[2017-09-04 15:27:50][swhsm:All user log out success]
[2017-09-04 15:28:07][swhsm:start hsmm success.]
```

6. Authority Management

6.1. Viewing Login Status

View the current administrator or login status of an operation.

```
Viewing login status：
-----------------
     |            Item                    |      Value
    _|____________________________________|_____________________________________
    1|      Current authority status      |      Super administrator
    2|       Administrator number         |      3
    3|      Logged on administrators      |      1 2 3
    4|    Login status of operators       |      Operator has not logged.
```

6.2. User Login

Administrator or operator login.

When logging in to the system, plug in the administrator (or operator) token in the direction indicated and enter the PIN to gain access to the token.

```
User login：
---------
      Insert the user's token into the USB port in the correct direction and input password.

Input PIN password or [Quit(Q)] [Next Step(N)]>
```

<!> Safety reminder： The default passwords of all the user tokens are initialized to "12345678". In order to ensure the security of the system, please modify the passwords through the "modify user password" function right after your first login.

6.3. User Logoff

There are menu options for user logoff in Administrator Management and Operator Management. You can release administrator authority or operator authority by performing this function.

```
User logoff：
-------------
      Please select the user’s type which to be logged off:

    _|_____________________________________
    1|   Operator
    2|   All administrators
    3|   All users(administrator or operator)

    4|   Viewing login status

Please select [Quit(Q)] [Next Step(N)]>
```

```
Logoff user：
_____________

          Insert the user's token into the USB port in the correct direction and input password.

Input PIN password or [Quit(Q)] [Return(R)]>
```

<!> Safety reminder：Upon completion of the management operation, it is recommended to logoff the administrator in time, while only retaining the operator login status, which is enough for running the financial data HSM cryptographic services and status monitoring function.

6. 4. Modify User Password

a) Insert the administrator token in the USB port indicated and enter the PIN.

```
Modifying the password of the token:
___________________
      Please insert the USB token.

Input the old password of    [Quit(Q)] [Return(R)]> ********
```

b) Input the new password.

```
Input the new password of    [Quit(Q)] [Return(R)]> ********
```

c) Input the new password again to compete password modification.

```
Input the new password again to complete password modification [Quit(Q)] [Return(R)]>

The password of USB token has been modified.
```

<!>Safety reminder：The default passwords of all the user tokens are initialized to "12345678". In order to ensure the security of the system, please modify the passwords

through the "modify user password" function right after your first login.

6. 5. Administrator management

6.5.1.Add administrator

a) Select "add management" from "administrator management" menu.

b) Insert the administrator token in the direction indicated

c) Enter the PIN to get the access authority of the USB token.

```
Add administrator:
----------
    Insert the user's USB token  into the USB port  in the correct direction and input password.

Input a password    [Quit(Q)] [Return(R)]>
```

d) After correctly inputting the PIN, the "add new administrator" function can be executed.

```
Successfully add NO.2 administrator.
```

<!>Safety reminder：The device supports up to 5 administrators. To ensure security, it is recommended to have at least 3 administrators.

<!>Safety reminder：The default passwords of all the user tokens are initialized to "12345678". In order to ensure the security of the system, please modify the passwords through the "modify user password" function right after your first login.

6.5.2.Delete administrator

Insert the administrator's token and input the PIN, the administrator will be deleted.

```
Delete administrator:
--------------------

    Please insert the administrator's token, and input the PIN.

Please input PIN or [Quit(Q)] [Return(R)]>********
Successfully delete NO.2 administrator.
```

6.6. Operator management

6.6.1.Add operator

a) Select the "add operator" function from the "operator management" menu

b) Insert the operator USB token in the direction indicated

c) Enter the PIN

```
Add operator:
-----------
    Insert the user's USB token into the USB port in the correct direction and input password.

Please input password or [Quit(Q)] [Return(R)]> ********
```

d) After inputting the correct password, you can complete the new operator addition function.

```
Successfully add operator.
```

<!>Safety reminder： The default passwords of all the user tokens are initialized to "12345678". In order to ensure the security of the system, please modify the passwords through the "modify user password" function right after your first login.

6.6.2.Update operator password

This operation resets the state of the operators and the login passwords saved in the device. After this operation is completed, all existing operators will be deleted; so the "Add operator" function will be needed to run in order to add new operators to the system.。

```
Update the password of operator:
---------------
    Executing the operation will update the operator password in HSM, and the operator which have registered will become invalid. You must re-added the new operator.

Please input “YES” to decide [Quit(Q)] [Return(R)]>


    Insert the user's USB token into the USB port in the correct direction and input password.

Please input password or [Quit(Q)] [Return(R)]> ********

Successfully add operator.
```

6. 7. Auditor management

6.7.1.Add auditor

a) Select the "add auditor" function from the "auditor management" menu

b) Insert the auditor USB token in the direction indicated

c) Enter the PIN

```
Add auditor:
-----------
    Insert the user's USB token into the USB port in the correct direction and input password.

Please input password or [Quit(Q)] [Return(R)]> ********
```

d) After inputting the correct password, you can complete the new auditor addition function.

```
Successfully add auditor.
```

<!>Safety reminder： The default passwords of all the user tokens are initialized to "12345678". In order to ensure the security of the system, please modify the passwords through the "modify user password" function right after your first login.

6.7.2.Update auditor password

This operation resets the state of the auditors and the login passwords saved in the device. After this operation is completed, all existing auditors will be deleted; so the "Add auditor" function will be needed to run in order to add new auditor to the system.。

```
Update the password of auditor:
---------------
    Executing the operation will update the auditor password in HSM, and the operator which have registered will become invalid. You must re-added the new auditor.

Please input “YES” to decide [Quit(Q)] [Return(R)]>


    Insert the user's USB token into the USB port in the correct direction and input password.

Please input password or [Quit(Q)] [Return(R)]> ********


Successfully add auditor.
```

6.8. Checking Privilege Setting Table

For ease of use, you can check on the privilege setting tables for each management operation. For details of the tables, please refer to the "Appendix: Management - Access Privilege Table " section.

Viewing management privilege tables

->1|Viewing system management privilege
| The privilege for viewing the system management, service management and other functions.

2 Viewing permission for management privilege
| The privilege for viewing administrators and operators and other functions.

3|Viewing key management privilege
| The privilege for viewing RSA key, ECDSA key and SM2 key information and other functions.

7. Key Management

7.1. Key Initialization

This operation destroys all keys and user information in the cryptographic device.

```
Key initialization:
-----------
Please be careful, because this operation destroys all keys and user information in the device.

Please input “YES” to decide [Quit(Q)] [Return(R)]>
```

<!>Safety reminder：This function is used not only to reset the initial state of the cryptographic device, but also to destroy all keys and user files in the device.

7.2. Setting Local Master Key

This operation is used to generate a new master key to ensure the security of other keys. Three key fragments need to be entered to set up the master key; and the HSM will automatically synthesize the master key internally.

```
Setting local master key:
-----------
    Please select the type to setting.
        _|_____________________________________
        1|  Randomly setting local master key.
        2|  Synthesizing local master key by key fragments.
        3|  Viewing the check value of local master key.
```

<!>Safety reminder：Please keep the key fragments separate and secure.

7.3. RSA Key Management

7.3.1.Generate Key Pair

The device supports one RSA key pairs for each index location. The steps are as follows:

a) Specify the key location according to the prompted key index range.

```
Generate RSA key pair:
-----------------
Generate new RSA key pair according to key index.

Please input the key index(1-100)(Default index[1]), or [Return(R)] [Next Step(N)]>11
```

b) Select the bit size of the key.

```
Generate RSA key pair:
-----------------
Select the bit size of the key, from 2048 bits to 3072 bits.
  _|_____________________________________________
  1|  2048
  2|  3072

Select bit size of the key(Default[2048]), or [Quit(Q)] [Return(R)] [Previous Step(P)] [Next
Step(N)]>1
```

c) The generated key pair will be encrypted by the system protection key and saved to the key storage area.

```
Generate RSA key pair:------------------
Generating RSA key pair...

  _|_____________________|_____________________________________________
  1|        Key index     |      1
  2|      Bit size of key  |      2048

Generating RSA key pair with index 1 and 2048 bits...successful

 Select [Quit(Q)] [Return(R)] [Previous Step(P)] >
```

7.3.2.Key Pair Deletion

Follow the prompts to enter the key index and delete the RSA key pair for the specified key index location.

```
Delete RSA key pair
-------------
_____|_____________________________________________________________________________
     1| [3072] [3072] [2048] [2048] [- -] [ - - ]   [ - - ] [--]   [- -] [- -]
    11| [3072] [3072] [2048] [2048] [- -] [ - - ]   [ - - ] [--]   [- -] [- -]

Input the key index or range of index for RSA key pairs which will be deleted or [Return(R)]>1
The key pair with index 1 has been deleted.
```

7.3.3.View Key State

Obtains the RSA key pair storage state in the current device.

```
Viewing RSA key pair state-----------------
_____|_____________________________________________________________________________
     1| [3072] [3072] [2048] [2048] [- -] [ - - ]   [ - - ] [--]   [- -] [- -]
    11| [3072] [3072] [2048] [2048] [- -] [ - - ]   [ - - ] [--]   [- -] [- -]
```

7.4. SM2 Key Management

7.4.1. Key Pair Generation

Each index location of the device corresponds to one SM2 key pair. The detailed steps are as follows:

a) Specifies the key location based on the indicated key index range.

```
Generate SM2 key pair
-----------------
Generate new SM2 key pair according to key index.



Please input the key index or key index range(1-100, for example:1,3,5-12), or [Return(R)] >11
```

b) The generated key pair will be stored in the key storage area after it has been encrypted by the system protection key.

```

Generating SM2 key pair with index 11 and 256 bits...successful
```

7.4.2.Key Pair Deletion

Based on the prompt, input the key index, and delete SM2 key pair in the specified location. This will completely destroy the SM2 key pair in this location.

```
Delete SM2 key pair----------
_____|_____________________________________________________________________________
     1| [256] [256] [ - ] [ - ] [256] [ - ] [ - ] [ - ] [ - ][ - ]
    11| [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ]

Input the key index for SM2 key pairs which will be deleted or [Return(R)]>1



The key pair with index 1 has been deleted.
```

7.4.3. View Key State

View the SM2 key pair storage state in the current cryptographic device.

```
Viewing SM2 key pair state-----------------
_____|_____________________________________________________________________________
     1| [256] [256] [ - ] [ - ] [256] [ - ] [ - ] [ - ] [ - ][ - ]
    11| [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ]
```

7.5. ECDSA Key Management

7.5.1.Key Pair Generation

Each index location of the device corresponds to one ECDSA key pair. The detailed steps are as follows:：

a) Specifies the key location based on the indicated key index range.

```
Generate ECDSA key pair
------------------
Generate new ECDSA key pair according to key index.




Please input the key index or key index range(1-100, for example:1,3,5-12), or [Return(R)] >11
```

b Select the bit size of the key.

```
Generate ECDSA key pair
------------------
Select the bit size of the key, from 256 bits to 521 bits.
   _|_____________________________________
   1|   256
   2|   384
   3|   521
Select bit size of the key(Default[256]), or [Quit(Q)] [Return(R)] [Previous Step(P)] [Next
Step(N)]>1
```

c) The generated key pair will be encrypted by the system protection key and saved to the key storage area.

```
Generate ECDSA key pair:------------------
Generating ECDSA key pair...

   _|_____________________|_____________________________________________
   1|          Key index          |       1
   2|        Bit size of key      |       256
Generating ECDSA key pair with index 11 and 256 bits...successful
  Select [Quit(Q)] [Return(R)] [Previous Step(P)] >
```

7.5.2.Key Pair Deletion

Follow the prompts to enter the key index and delete the RSA key pair for the specified key index location.

```
Delete ECDSA key pair
_____________
_____|_____________________________________________________________________________
    1| [256] [256] [ - ] [ - ] [256] [ - ] [ - ] [ - ] [ - ][ - ]
   11| [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ] [ - ]
Input the key index or range of index for RSA key pairs which will be deleted or [Return(R)]>1

The key pair with index 1 has been deleted.
```

7.5.3.View Key State

Obtains the ECDSA key pair storage state in the current device.

```
Viewing ECDSA key pair state
-----------------
_____|_____________________________________________________________________________
     1| [521] [521] [384] [384] [- -] [ - - ]   [ - - ] [--]   [- -] [- -]
    11| [256] [256] [256] [256] [- -] [ - - ]   [ - - ] [--]   [- -] [- -]
```

7.6. Symmetric Key Management

This is to manage various symmetric keys saved in the HSM.

```
Symmetric keys managements----------
 ->1|Generate randomly symmetric key
        |      Generate randomly or update key.
    2| Synthesizing key by fragments
        |      Enter the key fragments manually and synthesize the key.
    3|Delete key
        |      Delete expired or discarded key.
    4|Viewing key status
        |      Query the existing key information.
    5| Viewing the check value of key
        |      Query the existing key check value.
```

7.6.1. Random Key Generation

a) Select algorithm type

```
Generate or update symmetric key:
------------------
Generate new symmetric key according to key index.
Select algorithm type
    _|_____________________________________
    1|   3DES
    2|   SM4
    3|   SM1
    4|   AES
    5|   3DES(variant)
Select, or [Return(R)] [Next Step(N)] >
```

b) If you choose the 3DES or 3DES variant in the above step, please select the key strength.

```
Select the bit size of the key, from 64 bits to 192 bits.
    _|_____________________________________
    1|    64
    2|   128
    3|   192

Select bit size of the key, or [Return(R)] [Previous Step(P)] [Next Step(N)]>1
```

c)Enter the index

```
Enter key index(1-2048) or [Return(R)]>1
```

d)Key Generated successfully

```
Generate key with index 1 successfully.
```

7.6.2. Key Generation Via Synthesizing Key Segments

a）Select algorithm

```
Synthesize key by key segments----------
      Enter the key segments manually and synthesize the key.

     Please select algorithm type.      _|_____________________________________
         1|   3DES
         2|   SM4
         3|   SM1
         4|   AES
         5|   3DES(Variant LMK protect it)
Select, or [Return(R)] [Next Step(N)]>
```

b）Enter the number of segments, then enter the key segments

```
 Enter the number of segments(Default 2) or [Return(R)]>2Please input key segment 1 or
[Return(R)]>
*(1)*(2)*(3)*(4)*(5)*(6)*(7)*(8)*(9)*(10)*(11)*(12)*(13)*(14)*(15)*(16)*(17)*(18)*(19)*(20)
*(21)*(22)*(23)*(24)*(25)*(26)*(27)*(28)*(29)*(30)*(31)*(32)
 Please input key segment 2 or [Return(R)]>
*(1)*(2)*(3)*(4)*(5)*(6)*(7)*(8)*(9)*(10)*(11)*(12)*(13)*(14)*(15)*(16)*(17)*(18)*(19)*(20)
*(21)*(22)*(23)*(24)*(25)*(26)*(27)*(28)*(29)*(30)*(31)*(32)

Check value is [8ca64de9c1b123a7].
```

c）Verify whether the key ciphertext is needed to be exported or not, and if it does , then enter the key type.

```
Verify whether the key cipher text is needed to be exported or not.
   _|_____________________________________
   1|   YES
   2|   NO

Select, or [Return(R)] [Next Step(N)]>1 Please enter algorithm type or [Return(R)]>001
Key cipher text07 74 9e 49 c9 e3 12 8f 07 74 9e 49 c9 e3 12 8f
```

d）Verify whether the import key needs to be imported or not, and if it does, then enter the index.

```
Verify whether the key needs to be imported or not.
   _|_____________________________________
   1|   YES
   2|   NO

 Select, or [Return(R)] [Next Step(N)]>1Enter key index(1-2048) or [Return(R)] >200
Export successfully.
```

```
Select [Quit(Q)] [Return(R)]>
```

7.6.3. Key Deletion

Delete the expired or obsolete keys

a)Input key index numbers

```
Delete symmetric key----------
 Enter key index(1-2048) or [Return(R)] >200
 Please enter the key index number(1-2048) again to confirm the deletion or [Return(R)] >200Successfully delete the symmetric key with index 200.
```

7.6.4. View Key State

View the existing key information.

```
  1 |[128][X]   [ - ][-]   [ - ][-]   [ - ][-]   [128][S]   [ - ][-]   [128][U]   [ - ][-]
  9 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 17 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 25 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 33 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 41 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 49 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 57 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 65 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 73 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 81 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 89 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
 97 |[ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]   [ - ][-]
```

7.6.5.View Key Verification Value

Input key index, view key verification value

```
View key verification value----------
 Please enter key index(1-2048) or [Return(R)] >5
 The verification value of key with index 5 is 5acbf918d30573b0.
Select [Quit(Q)] [Return(R)]>
```

7. 7. Backup and Recovery

7.7.1.Key Backup

Run the key backup wizard to create the backup key and export it. Then encrypt the

sensitive information, such as the RSA private key, ECDSA private key and SM2 private key, and the symmetric key using this backup key and save it into a file. Export the backup files through FTP and keep them in good order. The detailed steps are as follows:

a) Log in at least half of all administrators to obtain super administrator rights. Prepare 3 administrator tokens which will be used to store the backup key segments.

```
Key backup wizard:
-------------
    1. Start backup key
    Log in at least half of all administrators to obtain super administrator rights and prepare three administrator tokens.
```

b) Output the 3 backup keys segments. This procedure requires the insertion of the token and inputting the PINs.

```
2. Output the first backup keys segment.
        Please select an administrator USB token to insert the USB port in the correct direction and enter the protection password.

Please enter USB token password or [Quit(Q)]>
```

```
3. Output the second backup keys segment.

      Please select another administrator USB token to insert the USB port in the correct direction and enter the protection password.
```

```
4. Output the third backup keys segment.

      Please select the third administrator USB token to insert the USB port in the correct direction and enter the protection password.
```

c) Encrypt keys and other data using the backup key and back it up into a file.

```
Key backup wizard:
-------------

    5. Generating the backup file.

The backup process is being performed, in the process the key data is encrypted and saved to the backup file.
The key information and other information have been encrypted and saved to the backup file. Please continue or [Quit(Q)] [Return(R)]>
```

d) Start the FTP service, then download the backup file "swhsmbak.dat" to the local

file and save it properly through the FTP tool. The FTP login name and password are the same as the ones you use to login into the HSM terminal.

```
Key backup wizard:
-------------

        6. Download the backup file.

  Starting FTP service…
FTP service is running. Please use a FTP tool to download key backup file.
Continue after downloading the file or [Quit(Q)] [Return(R)]>
```

e) Logoff from the FTP service after the backup is complete.

```
Key backup wizard
-------------

          7. Complete the key backup
        The FTP service will be stopped and the backup file will be deleted from HSM. Please seriously manage backup file and USB tokens.

Please select [Quit(Q)] [Return(R)]>
```

7.7.2.Key Recovery

Run the recovery wizard to synthesize the key segments stored inside the 3 administrator USB tokens, then decrypt key information in the backup file using the key. The detailed steps are as follows:

a) Start the key recovery wizard and prepare to perform the recovery function.

```
Key recovery wizard:
--------------------
       1.Start recovery key
        Please prepare two of the three administrator USB tokens that are used to store the backup key segment when backing up.
```

b) Start up FTP service，import back up file to the HSM via FTP tool and make sure the file name is"swhsmbak.dat".

```
Key recovery wizard:

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

2. Import backup file.



 Starting FTP service…

FTP service is running. Please use a FTP tool to import key backup file. The name of backup file must be swhsmbak.dat。
```

c) Import any 2 backup key segments, one by one. You need to insert a user USB token and enter the PIN during the process.

```
Key recovery wizard:

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

    3. Import the first backup key segment

Please select an administrator USB token to insert the USB port in the correct direction and enter the protection password.

 Please enter USB token password or [Quit(Q)]>
```

```
4. Import the second backup key segment
Please select another administrator USB token to insert the USB port in the correct direction and enter the protection password.
```

d) Key recovery Wizard will then restore the backup files.

```
Key recovery wizard:

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

5. The key information is being restored



Restoring management information… successfully.

Restoring system protection key… successfully.

Restoring key and user files… successfully.

 All processes for restoring key have been finished.
```

8. Service Management

8.1. Check Service State

Users can check the current service operating state, including number of concurrent requests and Loading state.

```
Check service state----------
_|_____________________|_____________________________________________________

1|      Current running state      |  Running

2|      Current loading state      |

3|       Concurrent requests       |  0
```

8.2. Check Service Configuration

View or modify the service start-up parameters.

	Items	**Default value**	**Notes**
1.	Service port	8008	
2.	Whether service automatically start up or not at boot	1	The 1 indicates that the service automatically start up at boot. The 0 indicates that the service does not automatically start up at boot.
3.	Session timeout （minutes）	100	In order to prevent the idle service caused by the abnormal situation, when a session in the timeout time is not active, the session will be automatically terminated.
4.	Maximum concurrent requests	2048	Maximum concurrent requests number that HSM supports
5.	Service connection password	11111111	The authentication password when the client and HSM create a session
6.	Service start-up password	12345678	If the service start-up state is automatically starting up at boot, the service firstly make operator login HSM automatically, and the start-up password is the operator's PIN password

a) Select the item to modify, then input the required value

```
Modify service configuration:

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

 _|_____________________________________________|_____________________________

 1|         * Service port                       |      8008

 2|    Service automatically start up at boot    |      1

 3|         Session timeout (minutes)            |      100

 4|         Maximum concurrent requests          |      2048

 5|          Service connection password         |      ********

 6|             Service start-up password        |      ********


Select the item to be modified or [Quit(Q)] [Return(R)]>2

Please select Whether service automatically start up or not at boot [Yes(Y)/No(N)]
or [Quit(Q)] [Return(R)]>
```

b) After completing the parameter modification, press the "Enter" key to save the modified configuration.

```
Select the item to be modified or [Quit(Q)] [Return(R)] [Save(S)]>s



Successfully modify service configuration.
```

8.3. White List Management

To ensure the security of the cryptographic device, the device supports the white list function to further control the client's access authority.

a) Press the Enter key to add a new IP address.

```
Add a new IP address or select the item to be deleted or [Quit(Q)] [Return(R)]>

 Please enter a new IP address >192.168.1.12
```

b) Select the specified IP number to be removed from the whitelist.

```
Service White List Management:--------------------

     |  The IP address or IP address range which can access HSM

   _|_____________________________________________________________________________

     1|  192.168.1.10

     2|  192.168.1.15

     3|  192.168.1.12



     4|    Add a new IP address

Select the item to be deleted or    [Quit(Q)] [Return(R)]>1

The IP address has been deleted successfully from white list.
```

<!>Safety reminder：If the white list is empty, it means this function is disabled. However for safety reasons, it is recommended not to disable this function.

<!>Reminder：If the service has been started, the new settings will only become effective after you restart the service.

8. 4. Start or stop service

If the service is stopped, you can select "start services".

If the service has begun, you can run the following functions：

1. **Stop service immediately** ： Stop all the service immediately.
2. **Restart service immediately** ： Stop all the service immediately and restart new service processes.

Appendix A： Management - Access Privilege Table

Management category	**Operations**	**Required Access Privilege**
Device management Service management	Check basic device information	None
	Check working information	Operator
	Check maintenance information	None
	Modify maintenance information	Administrator
	Check management audit logs	Auditor
Network management	Start service	Operator
	Stop service	Operator
	Modify service configuration	Operator
Authority management	Restart network	Operator
	Modify network configuration	Operator
Key management	Check login state	None
	Check authority setting table	None
	Add first administrator	None
	Add administrator	Super administrator
	Delete administrator	Super administrator
	Add operator	Super administrator
	Delete operator	Super administrator
	Set system protection key	Super administrator
	Check state of RSA key pair	Operator
	Generate RSA key pair	Administrator
	Delete RSA key pair	Administrator
	Import RSA key pair	Administrator
	Check SM2 key pair state	Operator
	Generate SM2 key pair	Administrator
	Delete SM2 key pair	Administrator
	Import SM2 key pair	Administrator
	Check ECDSA key pair state	Operator
	Generate ECDSA key pair	Administrator
	Delete ECDSA key pair	Administrator
	Import ECDSA key pair	Administrator
	Check symmetric key state	Operator
	Generate Symmetric key	Administrator
	Delete symmetric key	Administrator
	Import symmetric key	Administrator
Backup and recovery	Key backup	Super administrator
	Key recovery	None

Appendix B： Safety Instructions

1. Please read the safety instructions carefully before using this product.
2. Please follow the warning signs and instructions of the product.
3. When cleaning the device, unplug the machine from the power socket first. Do not use chemical cleaning agents.
4. Do not put the product close to a water source or a fire source.
5. Do not put the product on an unstable trolley, chair or table to avoid damage to the product.
6. When using this product, please pay attention to the voltage label. If you are not uncertain about anything, please inquire the dealer or local hydro company.
7. Please do not put anything on the power cord; do not put the power cord near entrances or exits to avoid being trampled.
8. When using extension cord, please pay attention to its power load. The total electricity consumption of devices attached to the same extension line should not exceed the load of the extension cord. At the same time, the power consumption of same socket cannot exceed the load of the fuse.
9. Do not insert anything in the product’s groove to avoid accidental electric shocks that may cause a short circuit or a fire. Please do not pour any liquid onto the product.
10. Please do not repair products yourself. Improper disassembly may cause electric shocks or other adverse consequences. Therefore, please contact the qualified technical service personnel for any maintenance issues.
11. When the following conditions are encountered, Please unplug the power and seek assistance from qualified service personnel:
    a. When the power cord or plug is damaged;

b. When liquid intrudes into the device;

c. When the product still does not function properly after you operate it following the instructions given;

d. When the product is accidentally dropped on the ground or the shell has any damage.

e. When product features change significantly; which indicates a need for maintenance.

Appendix C: Technical Support

If you have any problems with installing or using our products, please call the technical support center.

Technical support center：010-84109583

E-mail：support@sansec.com.cn

Website：www.sansec.com.cn

FCC STATEMENT

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.