

SANSEC HSM

User Manual

Version 2.1

Beijing Sansec Technology Development Co.,Ltd.

July 2016

1. Product Overview

Sansec HSM is a special device developed and designed by Beijing Sansec Technology Development Co.,Ltd. (hereinafter referred to as Sansec), 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 is an effective physical tool for protecting the safety of financial data and is particularly suitable for the use to a variety of bank financial information systems, such as providing data encryption and security protection for the ATM/POS networking information systems of inter-bank transactions. It can protect the PIN (Personal Identification Number) in financial networks reliably and safely in ways including pin encryption and decryption, authentication and forwarding. It can also support message authentication code(MAC) generation, verification, and forwarding of sources, for preventing fake cards and other frauds effectively.



2. Technical Specifications

2.1. Compatible with all versions of PBOC

Sansec HSM supports the latest version of the pboc3.0, also compatible pboc2.0 and pboc1.0 version, and supports debits and credits applications and electronic cash, qPBOC transaction process. It supports both SM algorithms (such as SM2,

SM3, etc.) and international algorithms (such as RSA, SHA-1, etc.). Sansec HSM can also support the gold card system, IC card application system, online banking system, etc.

2.2. Stability and security

Sansec HSM use clipped Linux kernel by removing unnecessary system modules and services, to reduce security vulnerabilities, enhancing system stability and security.

The customized system platform is installed on the DOM disk, which supports forced start up or shut down, improving the robustness of the system.

Cryptography service supports connection password and white list mechanism that implementing the application server authorization by the HSM, and further enhancing the security for the HSM application.

Sansec HSM supports multi-level authorization management mechanism based on smart card, and ensures the security of device management and use.

2.3. Key management features

Sansec HSM uses a strict three-layer key management system, to implement a special key for the special use, and supports high strength local master key with 192bits length. During the generation of the local master key, the HSM does not save any key component and security parameters, and the master key is not allowed to export in any plaintext way.

The HSM supports sensitive data and key stored in the user storage area or key storage area, and also supports ciphered key stored in the local host. The key in the device is stored in cipher-text way. Sansec HSM supports ANSI X9.17 encryption mode which defined a safety mechanism for key importing and exporting.

At any time, all user keys are not allowed show in plaintext way out the device, and the key backup file is protected by the master key.

Sansec HSM supports key component composition mechanism, and also supports the different length of key segmentation and key component printing. It also supports DUKPT (Derived Unique Key Per Transaction) mechanism.

2.4. Multiple command set and API interfaces

Sansec HSM supports multiple command set, compliant with the China Union Pay related standards, and also compatible with the RACAL command set. We extend the RACAL command set, for supporting the SM cryptographic algorithms.

Sansec HSM also provides a rich API interfaces, such as the API compatible with the 《Cryptographic device application interface specification》's requirements, and also supports PKCS#11, JCE and CSP and other international standard interface. Interface can support a variety of mainstream operating systems, such as Microsoft Windows series, Linux series, Solaris, AIX and HP-UX operating system, etc.

Sansec HSM also supports custom development, designing and developing based on users' needs for specific functions and interfaces.

2.5. Rich Cryptogram Algorithms

Sansec HSM series products support rich cryptogram algorithms, including a variety of international standard algorithms and national SM algorithms. National SM algorithms can be used in domestic banks between the self-service terminal and the host. The international standard algorithms can be used for international card business processing. Algorithms mainly include the state secret algorithm SM1 and SM4, international standard symmetric algorithm DES/3DES/AES, asymmetric algorithm RSA and the domestic cryptographic algorithm SM2. Data digest algorithm supports SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, ISO-10118-2, SM3, etc. HMAC algorithm supports HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-ISO-10118-2, HMAC-SM3, etc.

3. Technical Specifications

3.1. Main functions

Encryption / decryption for all kinds of application layer data
Message integrity protection (MAC calculation and verification)
Protection of transaction validity (TAC calculation and verification)
Protection of personal PIN code (PINBLOCK encryption, conversion, verification)
VISA PIN and Card Verification
Key Encryption, derivation and translation, etc.
Asymmetric digital signature and verification
Data digest(SHA1、SHA256、SHA512、SM3, etc.)
PIN mailer support

3.2. Financial services standards supported

PBOC 1.0/2.0/3.0
ANSI X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52, X9.97

3.3. Interface supported

Host Commands set (China Union Pay command set, RACAL command set and extension)
IBM Enterprise PKCS#11 (EP11)
Compliant with 《Cryptographic device application interface specification》
Supports PKCS#11、CSP、JCE interface
Self-defining interface
Supports Microsoft Windows, Linux, Solaris、AIX、HP-UX, etc.

3.4. Algorithm supported

Symmetric algorithm: DES and Triple DES (key lengths 112 bit, 168 bit), AES (key lengths 128 bit, 192 bit, 256 bit), SM4(key lengths 128 bit)

Asymmetric algorithm: RSA (key lengths up to 2048 bit), SM2(key lengths 256 bit)

Abstract algorithm: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, ISO-10118-2, SM3

3.5. Key management

Compliant with ANSI X9.17, ANSI X9.24

Supports key generation, synthesis and storage

Supports DUKPT

A three-layer key system

Key stored in the form of cipher-text, and can't be read in plaintext

Supports the storage of 2048 symmetric keys

Supports the storage of 100 pairs of RSA key pairs

Supports the storage of 100 pairs of SM2 key pairs

3.6. Device management

Management based on serial port dumb terminals

Multi-level authorization management mode based on smart card

3.7. Security features

A three-layer key system

Multiple local master keys LMK

Log audit

Supports the management of Two- Factor Authentication devices based on

password and smart card

Supports application white list mechanism.

3.8. Communication protocol

TCP/IP

Multiple concurrent operations

3.9. Physical characteristics

Form Factor	2U
Dimension (DWH)	520x440x89mm
Weight	14Kg
Electrical Supply	220V,50Hz, Dual power supply(option)
Power Consumption	100W(maximum)
NIC	RJ-45 ,10/100/1000Mb x2
Work Protocol	TCP/IP
Operating Temperature	10°C-60°C
Non-condensing Operating Humidity	5%-85%
Storage Temperature	0°C-60°C
Non-condensing Storage Humidity	5%-95%

4. Typical application scenarios

Agricultural Bank of China

During the domestic cryptographic algorithm transformation project of China Agricultural Bank, Sansec HSM is applied in the key management system in the card issuing process and the front-system in the ATM transaction. It provides key generation, data encryption and decryption of national SM algorithms and international algorithms for key management system. It provides PIN translation,

MAC Calculation and data transfer encryption of domestic SM algorithms and international algorithms for front-system, implementing the joint with China Union Pay front-system.

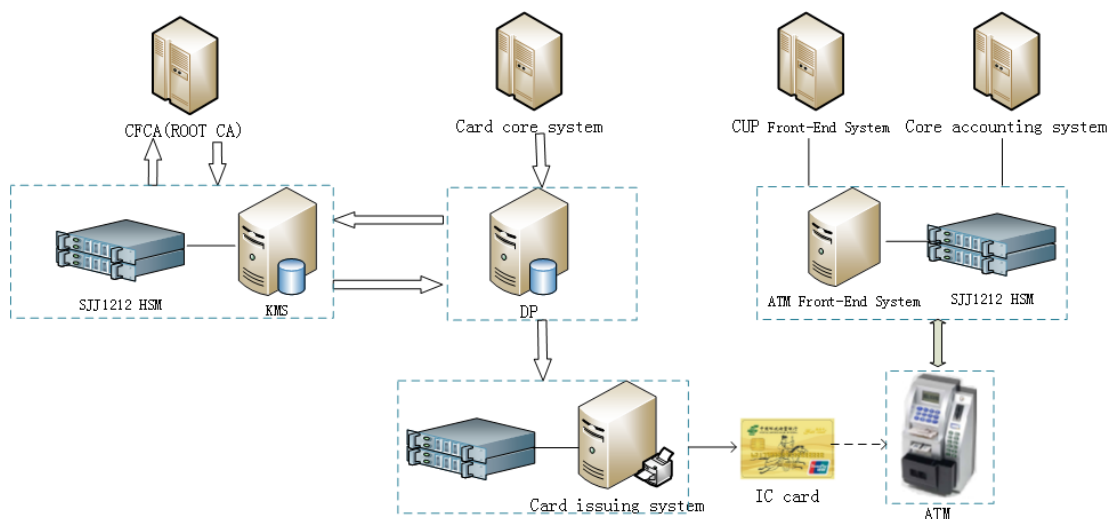


Fig 5.1 topology

Postal Savings Bank of China

During the domestic cryptographic algorithm transformation project of China Postal Savings Bank uses Sansec key management system and Sansec HSM. The key management system mainly used for card issuing banks certificate, the CA root certificate, certificate requirement management, providing IC card key, certificate data, etc. Sansec HSM is mainly used to provide IC card key pair and symmetric key derivation for data preparation system.

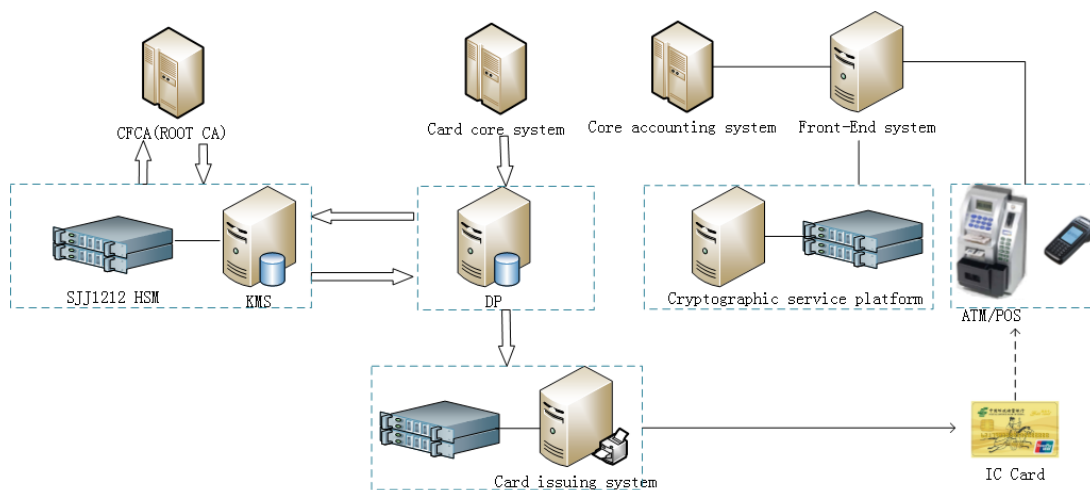


Fig 5.2 topology

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.