



TASS Crypto Engine

Firmware Version H1.00.00

Hardware P/N CE2-A2H004

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.5

Last update: 2021-04-19

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1 Introduction	6
1.1 Purpose of the Security Policy.....	6
1.2 Target Audience.....	6
1.3 How this Security Policy was Prepared	6
2 Cryptographic Module Specification.....	7
2.1 Module Overview	7
2.2 FIPS 140-2 Validation Scope	7
2.3 Definition of the Cryptographic Module	8
2.4 Definition of the Cryptographic Boundary	8
2.5 Modes of Operation.....	11
3 Module Ports and Interfaces	12
4 Roles, Services and Authentication.....	16
4.1 Roles.....	16
4.2 Identification, Authentication, Authorization.....	17
4.2.1 Manager, Operator, Auditor.....	17
4.2.2 User Application	18
4.2.3 Authentication Strength	19
4.3 Services	19
4.3.1 Services in the FIPS-Approved Mode of Operation	20
4.3.2 Services in the Chinese Non-FIPS Mode of Operation.....	24
4.3.3 Services in the Compatibility Non-FIPS-Approved Mode of Operation	29
4.4 Cryptographic Algorithms	33
4.4.1 FIPS-Approved Cryptographic Algorithms.....	33
4.4.2 Non-Approved-but-Allowed Cryptographic Algorithms	37
4.4.3 Non-Approved Cryptographic Algorithms	38
5 Physical Security	39
5.1 Static Protection.....	39
5.2 Dynamic Protection.....	40
6 Operational Environment	41
6.1 Applicability	41
7 Cryptographic Key Management.....	42
7.1 Random Number Generation	45
7.2 Key Generation	46
7.3 Key/CSP Storage	46

7.4 Key/CSP Zeroization.....	46
7.5 Key Establishment	47
7.6 Split Knowledge	47
7.7 Key Entry/Output	48
8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	49
9 Self-Tests.....	50
9.1 Power-Up Self-Tests	50
9.1.1 Integrity Tests	50
9.1.2 Cryptographic Algorithm Tests	50
9.2 Conditional Self-Tests	51
9.3 On-Demand Self-tests.....	52
10 Guidance.....	53
10.1 Crypto-Officer Guidance	53
10.1.1 Module Initialization.....	53
1.1. USB Tokens.....	58
1.2. Verification of Tamper Evidence Seals	58
1.3. Secure Distribution Process	59
10.1.2 Packing	59
10.1.3 Delivery	59
10.1.4 Receiving acceptance.....	59
10.2 Algorithm Considerations.....	60
10.2.1 AES-GCM IV	60
10.2.2 AES-XTS	60
10.2.3 Key Usage and Management.....	60
10.3 Handling Self-Test Errors	61
11 Mitigation of Other Attacks	62
12 Terms and Abbreviations	63
13 References	64

List of Tables

Table 1: FIPS 140-2 Security Requirements.	7
Table 2: Physical ports of the module.	13
Table 3: Logical interfaces and their mapping to physical ports.	14
Table 4: Roles and their authentication methods.	16
Table 5: Services in the FIPS-approved mode of operation.	20
Table 6: Services in the non-FIPS approved mode of operation.	25
Table 7: Services in the Compatibility non-FIPS mode of operation.	29
Table 8: FIPS-approved cryptographic algorithms.	34
Table 9: Non-Approved but allowed cryptographic algorithms.	38
Table 10: Non-FIPS approved cryptographic algorithms.	38
Table 11: Lifecycle of keys and other Critical Security Parameters (CSPs).	42
Table 12: Self-tests.	51
Table 13: Conditional self-tests.	52

List of Figures

Figure 1: Application scenario of the module, wherein application servers request cryptographic services.	7
Figure 2: Front panel of the module.	8
Figure 3: Back panel of the module (note: the tamper evident seals are not reflected here).....	8
Figure 4: Side panels and top cover of the module (note: the tamper evident seals are not reflected here).....	9
Figure 5: Hardware block diagram of the module.	10
Figure 6: Physical ports (front panel).	12
Figure 7: Physical ports (back panel).	13
Figure 8: Tamper evidence labels.	39

Copyrights and Trademarks

Copyright ©2021, Beijing JN TASS Technology Co., Ltd. TASS reserves the right to revise of the document, and can, at any time, perform necessary modifications to possible mistakes and discrepancies in the document against up-to-date information without notice.

TASS enjoys and retains the ownership and the power of interpretation of the document. Without permission, any company and individual shall not use and modify the content of the document. This document may be reproduced or distributed whole and intact including this copyright notice.

1 Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for version H1.00.00 of the TASS Crypto Engine module. It contains the security rules under which the module must be operated and describes how this module meets the requirements as specified in FIPS 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 3 module.

1.1 Purpose of the Security Policy

There are three major reasons that a security policy is needed:

- It is required for FIPS 140 2 validation.
- It allows individuals and organizations to determine whether a cryptographic module, as implemented, satisfies the stated security policy.
- It describes the capabilities, protection and access rights provided by the cryptographic module, allowing individuals and organizations to determine whether it will meet their security requirements.

1.2 Target Audience

This document is part of the package of documents that are submitted for FIPS 140-2 conformance validation of the module. It is intended for the following audience:

- FIPS 140-2 testing lab.
- The Cryptographic Module Validation Program (CMVP).
- Customers using or considering integration of TASS Crypto Engine.

1.3 How this Security Policy was Prepared

The vendor has provided the non-proprietary Security Policy of the cryptographic module, which was further consolidated into this document by atsec information security together with other vendor-supplied documentation as guided by FIPS 140-2 IG G.9. In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

2 Cryptographic Module Specification

2.1 Module Overview

The TASS Crypto Engine (hereafter referred to as the “module”) is a security module supporting FIPS 140-2 Approved cryptographic algorithms. The module is a hardware security module (HSM) with physical security protection measures, key management mechanisms and security functions to provide secure application-level cryptographic services for customer systems. The security functionalities include key wrapping, message authentication code (MAC), message digest, data encryption and decryption, digital signature generation and verification, among others.

A computer host connects to the module through the network using the TCP/IP protocol. The host authenticates itself to the module with a User Application UserName and a PIN. Once authentication succeeds, the host requests cryptographic services to the module, which processes the requests and sends back the result. In addition, users of the module can access the management functions by connecting to the module through the management console. The management console is connected to the module via the serial port or use the web browser. A typical application scenario is shown in Figure 1.

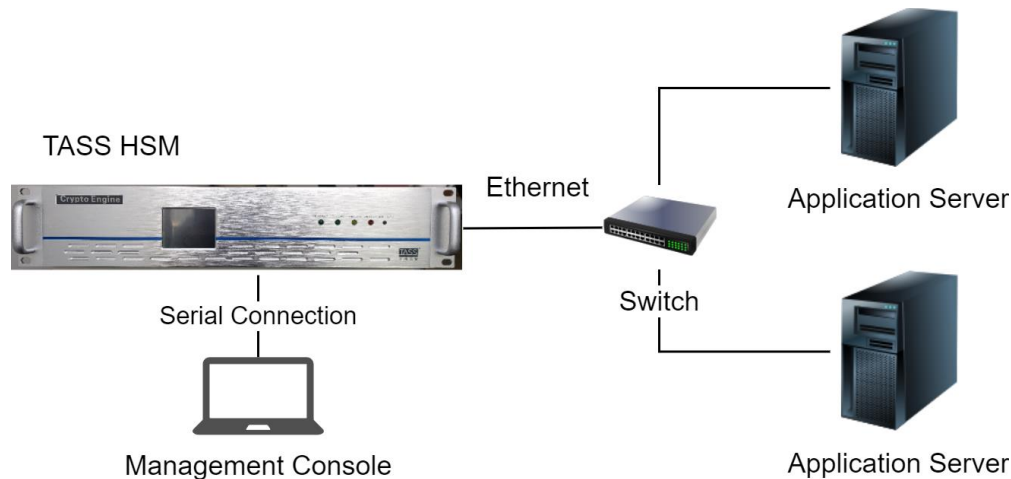


Figure 1: Application scenario of the module, wherein application servers request cryptographic services.

2.2 FIPS 140-2 Validation Scope

Table 1 shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard.

Table 1: FIPS 140-2 Security Requirements.

Security Requirements Section		Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles and Services and Authentication	3
4	Finite State Machine Model	3
5	Physical Security	3

Security Requirements Section		Level
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3
Overall Level		3

2.3 Definition of the Cryptographic Module

The TASS Crypto Engine is defined as a multi-chip standalone module per the requirements within FIPS 140-2.

The firmware version is H1.00.00 and the part number is CE2-A2H004.

The module internally uses an Intel Xeon E3 processor and a SSX1702 processor used by the Protection Card.

2.4 Definition of the Cryptographic Boundary

The cryptographic boundary of the module is defined as the entire hardware security module (HSM). The physical boundary of the physical module is defined by the hard metal chassis that surrounds all the hardware and firmware components of the module.

The physical dimensions of the module are 465 mm x 88.8 mm x 557.5 mm (width x height x length).

Figure 2 shows the front panel of the module. Figure 3 shows the back panel of the module. Figure 4 depicts the two side panels and the top cover. The front panel and its indicators and controls is detailed in Section 3.



Figure 2: Front panel of the module.



Figure 3: Back panel of the module (note: the tamper evident seals are not reflected here)



Figure 4: Side panels and top cover of the module (note: the tamper evident seals are not reflected here)

The module as an HSM provides a hardened, tamper-resistant environment. The HSM is enclosed entirely within an opaque secure steel chassis which deters physical tampering. The HSM also includes a tamper detection and response circuitry in the event the enclosure is opened.

Figure 5 shows a hardware block diagram of the module.

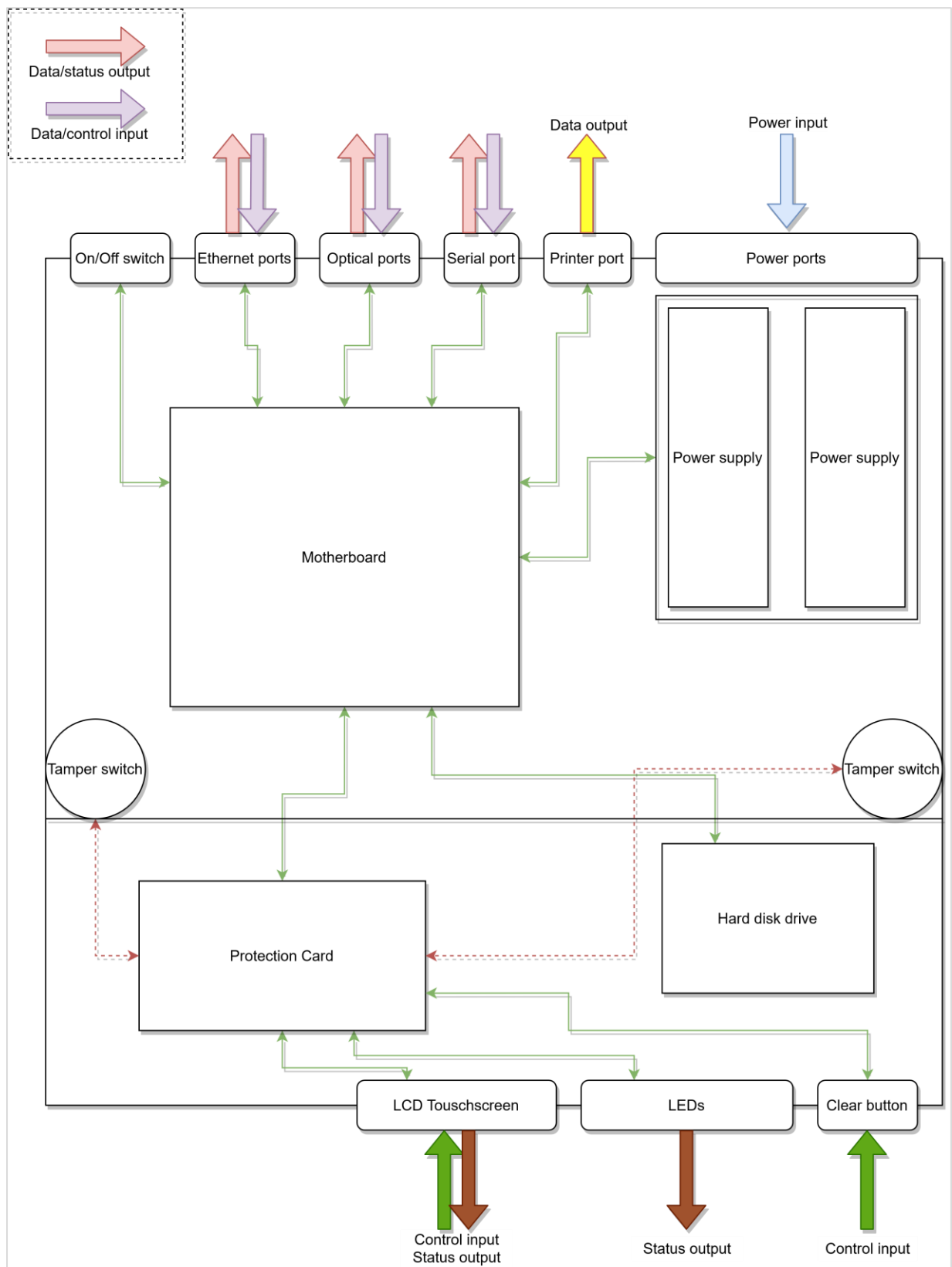


Figure 5: Hardware block diagram of the module.

The module includes a Protection Card, a hardware component with a built-in battery and volatile RAM. The Protection Card stores the Device Master Key in plaintext in its own RAM.

No components are excluded from the requirements of FIPS 140-2.

2.5 Modes of Operation

The module supports three modes of operation: one FIPS mode, and two non-FIPS modes.

- **FIPS mode:** This is the Approved mode of operation. Only approved or allowed security functions with sufficient security strength are offered by the module in this mode.
- **Chinese non-FIPS mode.** A non-Approved mode of operation. In this mode, cryptographic algorithms from the Chinese National Standard are offered by the module (and no FIPS-approved or allowed security functions are available).
- **Compatibility non-FIPS mode.** A non-Approved mode of operation. Both services and algorithms from the FIPS mode and the Chinese mode are available (note that, in this mode, the algorithms from the FIPS mode operate as non-approved).

The mode of operation is indicated by the module in the following manners:

- Indicated on the LCD touch screen located on the front panel.
- By invoking the “Display Operation Mode” service through the web management console or serial console.
- By invoking the “View Device Base Info” service using the NC command by a User Application.

The mode of operation is defined upon the module configuration, and the module retains that mode of operation at subsequent power-ons. To change the mode of operation, the module must be restored to factory settings, which erases information and keys stored in the module. The factory reset initiates a new configuration routine. At that moment, the new mode of operation can be defined, and it will be maintained until a new configuration routine is invoked. These operations are accessible to specific roles as indicated in Section 4.

Keys and Critical Security Parameters (CSPs) used or stored in FIPS mode are not shared with the non-FIPS mode of operation, and vice-versa, as a switch between the modes of operation forces the factory reset and erasure of all information and keys stored in the module. While the module is operating in the FIPS mode, the module enforces that only service requests for approved cryptographic services, approved algorithms and key sizes are allowed. Similarly, the module enforces that only the cryptographic services configured for the other respective non-FIPS modes of operation are available while the module is operating in those modes.

3 Module Ports and Interfaces

Figure 6 shows the front panel of the module and identifies the ports and indicators.

The front panel includes an LCD touch screen through which the module presents its mode of operation and other information. An operator of the module may also use the touch screen to navigate among different pages of information.

Indicators include a power light, a work light (if the HSM is performing some cryptographic operations from a command), an alarm light (if no DMK – Device Master Key- is present and no Manager is registered), and a fault light. The Clear button, if pressed for 10 seconds, zeroes the DMK.

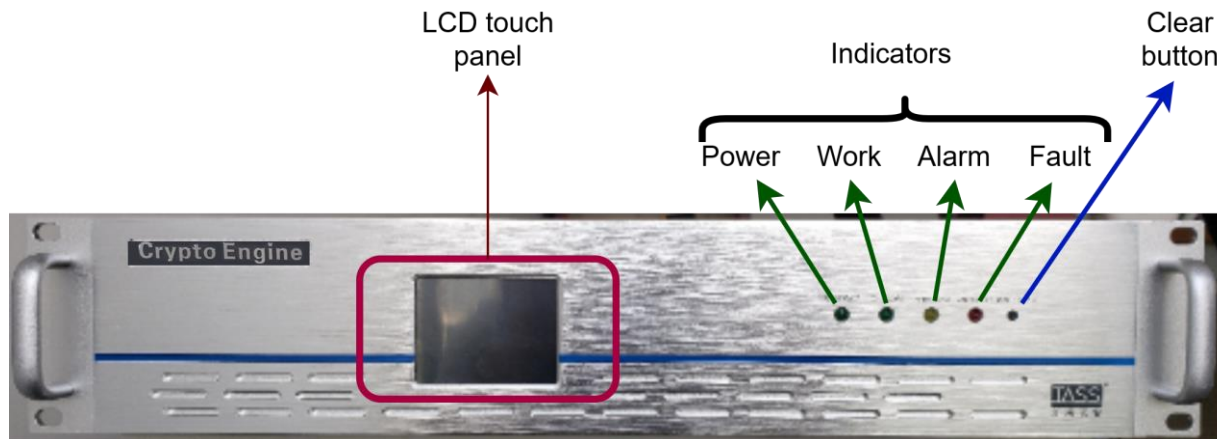


Figure 6: Physical ports (front panel).

Figure 7 depicts the ports and interfaces on the back panel of the module.

The module contains a redundant power supply. If one of the units fails or is not connected, the module emits an alarm, also indicated with the alarm light.

User Applications connect to the module via the two service optical network ports to send and receive data pertinent to the cryptographic services. These two optical ports operate in IEEE 802.3ad Link Aggregation mode.

A printer can be connected to the printer serial port for the service of printing non-security relevant business PINs and non-security relevant key components¹ to a security envelope. A management console can be connected to the management serial port for command-line input and output of management services (e.g., network configuration, factory reset). Two RJ-45 Ethernet ports and two optical ports provide connection to management and User Application services through for users and Crypto Officers.

¹ These non-security relevant business PIN and key components are considered non-security relevant (i.e., not CSPs) because they are not used as keys in any of the cryptographic services of the module, and are not managed or stored in the module. They are considered random strings.

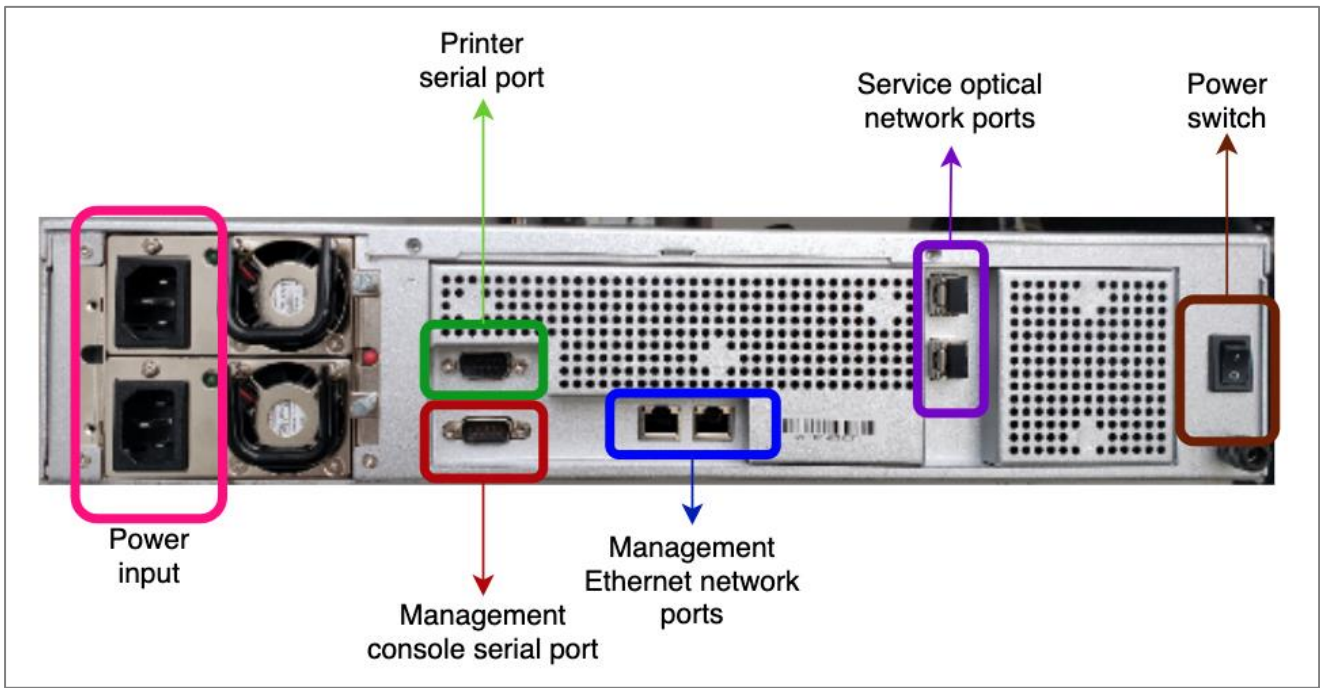


Figure 7: Physical ports (back panel).

Table 2 summarizes the physical ports contained in the module. A number in parenthesis, if present, indicates the quantity of physical ports.

Table 2: Physical ports of the module.

Physical Port	Description
Power switch	Powers the module on and off.
Power inputs (2)	Connect the module to the power outlet via the redundant power supply.
LCD touch screen	Displays module information in multiple pages, including mode of operation. Pages can be navigated by touch.
Power LED indicator	Shows whether the module is powered on.
Work LED indicator	Module is performing a cryptographic service.
Alarm LED indicator	Indicates that no DMK is present on the system, and that no user information is present
Fault LED indicator	Shows that the module is in the error state
Clear button	When pressed for 10 seconds, clears the DMK, user information, and encrypted keys and CSPs are removed from the database stored in the module.

Physical Port	Description
	Configuration information remains on the system.
Printer serial port	Connects to a printer for printing non-security relevant business PIN or non-security relevant key components to a security envelope.
Management console serial port	Permits connecting a serial console for command-line management services.
Management RJ-45 Ethernet network ports (2)	Access to a web interface for management services or for connection to other computers hosting User Applications that will request services from the module. The ports are configured to operate in IEEE 802.3ad Link Aggregation mode.
Service optical network ports (2)	

Table 3 lists the logical interfaces and power input and their mapping to the physical ports of the module.

Table 3: Logical interfaces and their mapping to physical ports.

Logical Interface	Physical Port	Description
Data Input	Management Ethernet ports	Backup archive for key restore. Authentication information. Configuration information. Other data input through management web interface.
	Optical network ports	Data input fields in service request messages.
	Management console serial port	Data input through management console.
Data Output	Optical network ports	Data output fields in service response messages.
	Management console serial port	Data output shown by management console.
	Management Ethernet ports	Data output shown by management web interface. Backup archive for key backup.
	Printer serial port	Print non-security relevant business PIN/key component to a security envelope.
Control Input	Power switch	Power on/off the module.
	LCD touch screen	Page selection in LCD touch screen.
	Management console serial port	Commands invoked in command-line management console.

Logical Interface	Physical Port	Description
	Optical network ports	Control input fields in service request messages.
	Management Ethernet ports	Control input fields in service request messages.
	Clear button	Clear keys stored in the module (if pressed for 10 seconds).
Status Output	LCD touch screen	Display module information and mode of operation.
	LED indicators (power, work, alarm, fault)	Indicate power on/off, work activity, alarm, fault states.
	Management console serial port	Status output shown by management console.
	Management Ethernet ports	Status output shown by management web interface.
	Optical network ports	Status fields in service response messages.
	Buzzer/audible alarm	Indicates that only one power cable is plugged in.
Power Input	Power connectors	The module supports two power cables used for power redundancy.

4 Roles, Services and Authentication

4.1 Roles

The module implements four roles: Manager, Operator, Auditor, and User Application. The module uses identity-based authentication to authenticate the operator of the module and verify that the operator is authorized to assume its role. Manager, Operator and Auditor are Crypto Officer roles, assigned to users of the module who perform management operations. The User Application role is a User role assigned to user applications (external entities) that connect to the module request cryptographic services.²

When the module is initialized for the first time, as there are no registered users provided by default, the Manager role is assigned to the user who accesses the module via the management interface to initialize it.

The User Application role is always assigned to external entities. These entities are the user applications that connect to the module.

The module allows concurrent Crypto Officers (Manager, Operator, Auditor) to log in. However, it is not advised to do so since as Managers might overwrite each other's data (i.e., if two Managers log in and create a key with the same Index).

Table 4 depicts the roles defined in the module and the method used to authenticate the roles. Section 4.2 details the authentication mechanism. The module also implements services that require no authentication.

Table 4: Roles and their authentication methods.

Role	Max Number of User	Authentication Method	Description
Manager	5	Username and 2048-bit RSA key	This role is assigned upon successful authentication of a user identified with this role. The first Manager registers to the module upon the first configuration of the module. The Manager can perform authentication and authorization management (add and delete all other users and roles), key management, backup/restore operations, factory reset, and view their own logs. The Manager can also modify their own USB token PIN. The Manager can perform User Application role management (add, delete User Applications) functions.
Operator	1	Username and 2048-bit RSA key	This role is assigned upon successful authentication of a user identified with this role. The Operator can perform User Application role management (configure their authentication PIN), configure communication protocol options, including TLS client/server certificate

² Throughout this document, when referring to the "Operator" or "User Application roles", these names will have their first letter in uppercase. Otherwise, "operator" and "user" (in all lowercase) will refer to a generic operator or user of the module, applicable to any role.

Role	Max Number of User	Authentication Method	Description
			management; perform device configuration (network ports, serial ports, IP address whitelist), and modify their own USB token PIN. The Operator can perform diagnosis such as self-tests, view auditing logs from Operator and User Application, view system logs and configure the level of logging.
Auditor	1	Username and 2048-bit RSA key	The Auditor role is assigned to users after successful authentication of their identity and role. The Auditor can view audit logs of Managers and Operator and configure their own USB token PIN.
User Application	∞	Username and authentication PIN	This role is assigned when an external entity, the User Application, successfully authenticates to the module via a TCP/IP network connection and via the service optical network ports. The User Application can request cryptographic services to the module. The module supports an undefined number of User Application users but limited to the size of the IP address whitelist if this whitelist is enabled.

4.2 Identification, Authentication, Authorization

The module employs identity-based authentication to identify and authenticate users of the module. For the Manager, Operator and Auditor roles, the users are identified by a username and authenticated using a challenge-response mechanism based on a 2048-bit RSA key pair. The public key is stored in the module in plaintext, and the private key is stored in the user's USB token.

For the User Application role (external entities), users with this role are identified by their assigned username and authenticate using a challenge-response protocol based on their PIN. The module also uses an IP address whitelist to filter user applications. The IP address list and usernames are stored in the module in plaintext. User Application PINs are stored in the module encrypted with the local master keys (LMKs) using AES-256-GCM.

4.2.1 Manager, Operator, Auditor

COs with the Manager, Operator and Auditor roles authenticate in the following manner:

1. The CO connects to the module via the management web interface (through the configured management ports) using a management computer and browser and establishing a TLS (via HTTPS) connection between the browser and the module's web interface. The TLS connection uses server authentication only (using the module's certificate).
2. The TLS connection is established via the management web interface between the CO and the module.

3. The user inserts the USB token into the USB port of the management computer. The CO must enter the USB token PIN to unlock the private key stored in the USB token.
4. The CO sends their username to the module.
5. The module verifies the username against the user database. The module generates a challenge consisting of a random value R of 256 bits, and sends the challenge to the CO.
6. Upon receiving the challenge, the CO generates a signature of R using their private key stored in the USB token. The CO sends the signature to the module.
7. The module verifies the received signature. If the signature verifies successfully, the CO user is now authenticated.

The module allows a maximum of 6 consecutive incorrect attempts to authenticate. After 6 consecutive failed authentication attempts, the username of the respective user will be locked from further authentication requests for a one-minute period.

When a new CO with the Manager role is added (obeying the limits of COs per role per Table 4), the module commands the CO's USB token to generate a 2048-bit RSA key pair and the module requests an 8-digit PIN for access control to the key stored in the USB token (the 8-digit PIN is controlled by the USB token, not by the module). The RSA public key is sent to the module, and the RSA private key is stored in the USB token.³

4.2.2 User Application

Users with the User Application role identify and authenticate to the module, before being granted access to any cryptographic service, according to the following protocol:

1. The User Application connects to the module via the service optical or ethernet network ports using Clear, One-Way, or Two-Way TLS.
2. The module verifies the user against the whitelist of IP addresses (if enabled) to determine whether the peer is authorized to connect to the module, and then whether the authentication mechanism should continue. If the user IP address is not contained in the IP address whitelist, the module refuses the connection.
3. The module generates a random value R of 256 bits and sends to the User Application.
4. The User Application generates an HMAC-SHA-256 value with its Authentication PIN as key and R as input. The User Application sends the HMAC value to the module.
5. The module obtains the User Application PINs from the database (the User Application may have up to two PINs). The module then verifies the received HMAC value using the first PIN from the database. If this value is valid, the user is now authenticated. Otherwise, the module will verify the HMAC value using the second PIN found in the database. If the value is valid, the user is authenticated. If there is no second PIN, or if this second verification fails, the authentication fails.

The module allows a maximum of 10 consecutive failed attempts to login as a User Application. After these 10 consecutive failed attempts, the respective User Application ID will be blocked from new attempts for 3 minutes.

³ It is recommended for every user to change their PIN code upon receiving a USB token.

The User Application PIN is a 128-bit long PIN. A User Application may have one or two PINs for authentication, as described before.

User Application credentials are managed (added or deleted) by a user with the Operator or Manager role. The PINs are stored in the module's hard disk encrypted with AES-256-GCM.

The User Application entity remains authenticated to the module only during the life span of the session, or until the module is powered off. No authentication data remains in the module for the User Application.

4.2.3 Authentication Strength

For the Manager, Operator and Auditor roles, the user authentication mechanism uses a 2048-bit RSA key pair for signature generation. According to [SP800-57], such a key length in the aforementioned mechanism provides a security strength of 112 bits. Therefore, the probability of a successful authentication by guessing the private key, using a USB token with a non-registered user's credential, is $2^{-112} \approx 10^{-33}$. This probability is less than the maximum probability of 10^{-6} that a random attempt to authenticate will succeed, or a false acceptance will occur, as required by the FIPS 140-2 standard.

Considering that the authentication process requires entering the 8-digit USB token PIN manually through the module's web interface, and considering that the module enforces the limit that the user can perform a maximum of 6 attempts to authenticate, and then wait for one minute, the total probability of guessing the credentials is approximately $6 * 10^{-33}$ in one minute. This number is less than the maximum probability of 10^{-5} that, for multiple attempts to use the authentication mechanism during a one-minute period, a random attempt to authenticate will succeed, or a false acceptance will occur, as required by the FIPS 140-2 standard.

For the User Application, the user authentication mechanism employs a 128-bit key (the PIN) that is used in the HMAC-SHA-256 algorithm during the challenge-response protocol, and a 256-bit value R as the input. Per [SP800-57], the security strength provided by the HMAC-SHA-256 in this mechanism is 128 bits. Thus, the probability of a successful authentication by guessing the User Application secret key or the output of the HMAC-SHA-256 response itself is $2^{-128} \approx 10^{-38}$. This probability is less than the maximum probability of 10^{-6} that a random attempt to authenticate will succeed, or a false acceptance will occur, as required by the FIPS 140-2 standard.

The User Application authentication mechanism is implemented such that a maximum of 10 failed attempts to authenticate are allowed, and then the respective User Application ID is blocked from new attempts for 3 minutes. As such, for multiple authentication attempts, the probability of a successful authentication in a one-minute period for the User Application is less than 10^{-38} . This value is less than the maximum probability of 10^{-5} that, for multiple attempts to use the authentication mechanism during a one-minute period, a random attempt to authenticate will succeed, or a false acceptance will occur, as required by the FIPS 140-2 standard.

4.3 Services

The module provides services to users connected through the management interfaces and to external User Applications (User Application role) connected through the service optical network interfaces. Some of the services do not require authentication. Services are basically divided into those accessible to human users connected through the management interfaces, and services available to external entities assuming the User Application role, connected through the service optical network interfaces.

Table 5 and Table 6 depict all services provided by the module.

The tables use the following convention:

When specifying the role which is authorized to request the service (Role column). A checkmark indicates which role has access to that service. The Manager, Operator and Auditor are Crypto Officer (CO) roles. The User Application is a User role per FIPS 140-2 standard.

- **MNG**: Manager role.
- **OP**: Operator role.
- **AUD**: Auditor role.
- **UA**: User Application role.

When specifying the access permissions that the module has for each CSP or key (Access Types column).

- **Create (C)**: the calling application can create a new CSP.
- **Read (R)**: the calling application can read the CSP.
- **Update (U)**: the calling application can write a new value to the CSP.
- **Zeroize (Z)**: the calling application can zeroize the CSP.
- **N/A**: the calling application does not access any CSP or key during its operation.

4.3.1 Services in the FIPS-Approved Mode of Operation

Table 5 provides a full description of FIPS Approved services and the non-Approved but Allowed services provided by the module in the FIPS-approved mode of operation and lists the roles allowed to invoke each service.

Table 5: Services in the FIPS-approved mode of operation.

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		MNG	OP	AUD	UA		
Management							
Backup DMK	Divide DMK into external media	✓				DMK CO RSA public/private keys	R
Update DMK	Regenerate or import DMK Re-encrypt user keys Regenerate configuration information validation value	✓				DMK CO RSA public/private keys	C, R, U
List COs	List information from all COs	✓				CO RSA private/public keys	R

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P	A U D	U A		
Add CO	Write ID and RSA public key from CO to module Regenerate configuration information integrity check value	✓				CO RSA private/public keys LMKs	C
Delete CO	Delete CO record Regenerate configuration information integrity check value	✓				CO RSA private/public keys LMKs	R, U
List User Application users	List all currently existing User Application users	✓	✓			CO RSA private/public keys	R
Add User Application user	Create a new user Calculate user information integrity check value	✓				CO RSA private/public keys LMK	C, R
Delete User Application	Delete user's information, and recalculate user information integrity check value	✓				CO RSA private/public keys LMK	R, U
Check User Application PIN	Check if User Application PIN is set	✓	✓			CO RSA private/public keys	R
Create User Application PIN	Generate a new User Application PIN		✓			CO RSA private/public keys User Application PIN	C, R, U
Delete User Application PIN	Delete a User Application PIN		✓			CO RSA private/public keys User Application PIN	C, R, U
Create User Applications key	Generate a new key or key pair and calculate the integrity check value.	✓				CO RSA private/public keys User Applications AES/HMAC/RSA/ECDSA keys	U
Delete User Application key	Delete a key or key pair	✓				CO RSA private/public keys User Applications AES/HMAC/RSA/ECDSA keys	U
Backup keystore database	Generate and backup key-backup key (KBK)	✓				CO RSA private/public keys KBK	C, R, U

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P	A U D	U A		
	Download encrypted keystore database						
Restore keystore database	Restore keystore database	✓				CO RSA private/public keys KBK	C, R, U
Configure IP addresses white-listing	Enable/disable IP whitelisting List, add, delete addresses in the IP whitelist		✓			CO RSA private/public keys	R
Configure HTTPS/TLS protocol	Configure certificate for the HTTPS protocol for management services Configure TLS protocol for User Applications		✓			CO RSA private/public keys	C, R, U
Configure network parameters	Configure the network interface parameters, IP address, network mask, gateway of network ports		✓			CO RSA private/public keys	N/A
Configure printer serial port parameters	Configure communication properties of printer serial port		✓			CO RSA private/public keys	N/A
Configure management services serial port parameters	Configure communication properties of the management services serial port		✓			CO RSA private/public keys	N/A
Configure logging level	Configure run logging level (error, information, debug).		✓			CO RSA private/public keys	N/A
View device status	View the running status and the occupancy rate of internal resources	✓	✓			CO RSA private/public keys	N/A
Run self-tests	Self-test of approved cryptographic algorithms		✓			CO RSA private/public keys	N/A
View device base info	View version, serial, mode of operation, DMK check value	✓	✓			CO RSA private/public keys	N/A
View CO audit logs	View all COs' logs and system logs			✓		CO RSA private/public keys	N/A

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
View User Applications audit logs	View all User Application's logs		✓			CO RSA private/public keys	N/A
Export audit logs	Export the specified event logs.			✓		CO RSA private/public keys	N/A
Clear all audit logs	Clear all logs			✓		CO RSA private/public keys	N/A
View own operation logs	View CO's own logs	✓	✓	✓		CO RSA private/public keys	N/A
View own information	View your own information (UserName, role, USB token serial number)	✓	✓	✓		CO RSA private/public keys	N/A
Modify USB token PIN	Modify CO's own USB token PIN	✓	✓	✓		CO RSA private/public keys	N/A
User Application							
Cryptographic operations using internal keys (using algorithms from Table 8)	Cryptographic functions using keys stored in the keystore database				✓	AES, HMAC, RSA, ECDSA keys LMKs	R, U
Cryptographic operations using external keys (using algorithms from Table 8)	Cryptographic functions using keys stored in the User Application's own keystore database				✓	AES, HMAC, RSA, ECDSA keys LMKs	R, U
Generate, store and export keys	Generate, store and export a new key				✓	AES, HMAC, RSA, ECDSA keys LMKs	C, R, U
Generate and export keys	Generate and export a new key				✓	AES, HMAC, RSA, ECDSA keys LMKs	C, R, U
Transfer keys from old to new DMK	Use old and new LMKs to re-wrap the keys and calculate the integrity check value				✓	LMKs	R, U
Generate non-security related business PIN and	Generate non-security relevant business PIN and print it with the printer Output encrypted PIN				✓	N/A User Application's AES key	C, R, U

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
print it to serial printer							
Random Number Generation	SP800-90A CTR_DRBG with AES-256				✓	Entropy input string Internal state	R, U
Other FIPS-related, non-Authenticated Services							
TLS network protocol v1.2	Provide HTTPS connection for the management web interface and TLS connection for User Applications with AES and RSA. The service provides a connection before user authentication starts. Ciphersuites: <ul style="list-style-type: none"> • AES-256-GCM-SHA384 • AES-128-GCM-SHA256 	N/A		AES keys RSA public/private keys		C, R, U	
Display mode of operation	Display mode of operation on the LCD touch screen and through the serial port terminal commands.	N/A		N/A		N/A	
Display module version	Display module version on the LCD touch screen and through the serial port terminal commands.	N/A		N/A		N/A	
Display network address	Display network address on the LCD touch screen and through the management serial console port.	N/A		N/A		N/A	
Factory reset (zeroization)	Factory reset the module	N/A		DMK LMKs		Z	
Device initialization	Execute when module is uninitialized. Select the operation mode. Generate/compose DMK. Register the first Manager.	N/A		DMK		C, R, U	

4.3.2 Services in the Chinese Non-FIPS Mode of Operation

Table 6 presents the services available in the Chinese non-FIPS mode of operation.

© 2021 Beijing JN TASS Technology Co., Ltd./ atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table 6: Services in the non-FIPS approved mode of operation.

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
Management							
Backup DMK	Divide DMK into external media	✓				DMK CO SM2 public/private keys	R
Update DMK	Regenerate or import DMK Re-encrypt user keys Regenerate configuration information validation value	✓				DMK CO SM2 public/private keys	C, R, U
List COs	List information from all COs	✓				CO SM2 private/public keys	R
Add CO	Write ID and RSA public key from CO to module Regenerate configuration information integrity check value	✓				CO SM2 private/public keys LMKs	C
Delete CO	Delete CO record Regenerate configuration information integrity check value	✓				CO SM2 private/public keys LMKs	R, U
List User Application users	List all currently existing User Application users	✓	✓			CO SM2 private/public keys	R
Add User Application users	Create a new user Calculate user information integrity check value	✓				CO SM2 private/public keys LMK	C, R
Delete user application	Delete user's information, and recalculate user information integrity check value	✓				CO SM2 private/public keys LMK	R, U
Check User Application PIN	Check if User Application PIN is set	✓	✓			CO SM2 private/public keys	R
Create User Application PIN	Generate a new User Application PIN		✓			CO SM2 private/public keys User Application PIN	C, R, U
Delete User Application PIN	Delete a User Application PIN		✓			CO SM2 private/public keys User Application PIN	C, R, U

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P	A U D	U A		
Create User Applications keys	Generate a new key or key pair and calculate the integrity check value.	✓				CO SM2 private/public keys User Applications SM4/HMAC/RSA/SM2 keys	U
Delete User Application keys	Delete a key or key pair	✓				CO SM2 private/public keys User Applications SM2/HMAC/RSA/SM2 keys	U
Backup keystore database	Generate and backup key-backup key (KBK) Download encrypted keystore database	✓				CO SM2 private/public keys KBK	C, R, U
Restore keystore database	Restore keystore database	✓				CO SM2 private/public keys KBK	C, R, U
Configure IP addresses whitelisting	Enable/disable IP whitelisting List, add, delete addresses in the IP whitelist		✓			CO SM2 private/public keys	R
Configure HTTPS/TLS protocol	Configure certificate for the HTTPS protocol for management services Configure TLS protocol for User Applications		✓			CO SM2 private/public keys	C, R, U
Configure network parameters	Configure the network interface parameters, IP address, network mask, gateway of network ports		✓			CO SM2 private/public keys	N/A
Configure printer serial port parameters	Configure communication properties of printer serial port		✓			CO SM2 private/public keys	N/A
Configure management services serial port parameters	Configure communication properties of the management services serial port		✓			CO SM2 private/public keys	N/A
Configure logging level	Configure run logging level (error, information, debug).		✓			CO SM2 private/public keys	N/A

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
View device status	View the running status and the occupancy rate of internal resources	✓	✓			CO SM2 private/public keys	N/A
Run self-tests	Self-test of approved cryptographic algorithms		✓			CO SM2 private/public keys	N/A
View device base info	View version, serial, mode of operation, DMK check value	✓	✓			CO SM2 private/public keys	N/A
View CO audit logs	View all COs' logs and system logs			✓		CO SM2 private/public keys	N/A
View User Applications audit logs	View all User Application's logs		✓			CO SM2 private/public keys	N/A
Export audit logs	Export the specified event logs.			✓		CO SM2 private/public keys	N/A
Clear all audit logs	Clear all logs			✓		CO SM2 private/public keys	N/A
View own operation log	View CO's own logs	✓	✓	✓		CO SM2 private/public keys	N/A
View own information	View your own information (UserName, role, USB token serial number)	✓	✓	✓		CO SM2 private/public keys	N/A
Modify USB token PIN	Modify CO's own USB token PIN	✓	✓	✓		CO SM2 private/public keys	N/A
User Application							
Cryptographic operations using internal keys (using algorithms from Table 8)	Cryptographic functions using keys stored in the keystore database				✓	SM2, HMAC, SM4 keys LMKs	R, U
Cryptographic operations using external keys (using algorithms from Table 8)	Cryptographic functions using keys stored in the User Application's own keystore database				✓	SM2, HMAC, SM4 keys LMKs	R, U
Generate, store and export key	Generate, store and export a new key				✓	SM2, HMAC, SM4 keys LMKs	C, R, U

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P	A U D	U A		
Generate and export key	Generate and export a new key				✓	SM2, HMAC, SM4 keys LMKs	C, R, U
Transfer keys from old to new DMK	Use old and new LMKs to re-wrap the keys and calculate the integrity check value				✓	LMKs	R, U
Generate non-security related business PIN and print it to serial printer	Generate non-security relevant business PIN and print it with the printer Output encrypted PIN				✓	N/A User Application's SM4 key	C, R, U
Random Number Generation	SP800-90A CTR_DRBG with AES-256				✓	Entropy input string Internal state	R, U
Other non-Authenticated Services							
TLS network protocol v1.2	Provide HTTPS connection for the management web interface and TLS connection for User Applications with AES and RSA. The service provides a connection before user authentication starts. Ciphersuites: <ul style="list-style-type: none"> • AES-256-GCM-SHA384 • AES-128-GCM-SHA256 	N/A		AES keys RSA public/private keys		C, R, U	
Display mode of operation	Display mode of operation on the LCD touch screen and through the serial port terminal commands	N/A		N/A		N/A	
Display module version	Display module version on the LCD touch screen and through the serial port terminal commands	N/A		N/A		N/A	
Display network address	Display network address on the LCD touch screen and through the management serial console port.	N/A		N/A		N/A	
Factory reset (zeroization)	Factory resets the module	N/A		DMK LMKs		Z	

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
Device initialization	Execute when module is uninitialized. Select the operation mode. Generate/compose DMK. Register the first Manager.	N/A				DMK	C, R, U

4.3.3 Services in the Compatibility Non-FIPS-Approved Mode of Operation

Table 6 presents the services only available in the Compatibility non-FIPS mode of operation.

Table 7: Services in the Compatibility non-FIPS mode of operation.

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
Management							
Backup DMK	Divide DMK into external media	✓				DMK CO RSA public/private keys	R
Update DMK	Regenerate or import DMK Re-encrypt user keys Regenerate configuration information validation value	✓				DMK CO RSA public/private keys	C, R, U
List COs	List information from all COs	✓				CO RSA private/public keys	R
Add CO	Write ID and RSA public key from CO to module Regenerate configuration information integrity check value	✓				CO RSA private/public keys LMKs	C
Delete CO	Delete CO record Regenerate configuration information integrity check value	✓				CO RSA private/public keys LMKs	R, U
List User Application users	List all currently existing User Application users	✓	✓			CO RSA private/public keys	R

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
Add User Application user	Create a new user Calculate user information integrity check value	✓				CO RSA private/public keys LMK	C, R
Delete user application	Delete user's information, and recalculate user information integrity check value	✓				CO RSA private/public keys LMK	R, U
Check User Application PIN	Check if User Application PIN is set	✓	✓			CO RSA private/public keys	R
Create User Application PIN	Generate a new User Application PIN		✓			CO RSA private/public keys User Application PIN	C, R, U
Delete User Application PIN	Delete a User Application PIN		✓			CO RSA private/public keys User Application PIN	C, R, U
Create User Applications keys	Generate a new key or key pair and calculate the integrity check value.	✓				CO RSA private/public keys User Applications AES/HMAC/RSA/ECDSA/SM2/SM4 keys	U
Delete User Application key	Delete a key or key pair	✓				CO RSA private/public keys User Applications AES/HMAC/RSA/ECDSA/SM2/SM4 keys	U
Backup keystore database	Generate and backup key-backup key (KBK) Download encrypted keystore database	✓				CO RSA private/public keys KBK	C, R, U
Restore keystore database	Restore keystore database	✓				CO RSA private/public keys KBK	C, R, U
Configure IP addresses whitelisting	Enable/disable IP whitelisting List, add, delete addresses in the IP whitelist		✓			CO RSA private/public keys	R
Configure HTTPS/TLS protocol	Configure certificate for the HTTPS protocol for management services		✓			CO RSA private/public keys	C, R, U

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
	Configure TLS protocol for User Applications						
Configure network parameters	Configure the network interface parameters, IP address, network mask, gateway of network ports		✓			CO RSA private/public keys	N/A
Configure printer serial port parameters	Configure communication properties of printer serial port		✓			CO RSA private/public keys	N/A
Configure management services serial port parameters	Configure communication properties of the management services serial port		✓			CO RSA private/public keys	N/A
Configure logging level	Configure run logging level (error, information, debug).		✓			CO RSA private/public keys	N/A
View device status	View the running status and the occupancy rate of internal resources	✓	✓			CO RSA private/public keys	N/A
Run self-tests	Self-test of approved cryptographic algorithms		✓			CO RSA private/public keys	N/A
View device base info	View version, serial, mode of operation, DMK check value	✓	✓			CO RSA private/public keys	N/A
View CO audit logs	View all COs' logs and system logs			✓		CO RSA private/public keys	N/A
View User Applications audit logs	View all User Application's logs		✓			CO RSA private/public keys	N/A
Export audit logs	Export the specified event logs.			✓		CO RSA private/public keys	N/A
Clear all audit logs	Clear all logs			✓		CO RSA private/public keys	N/A
View own operation log	View CO's own logs	✓	✓	✓		CO RSA private/public keys	N/A
View own information	View your own information (UserName, role, USB token serial number)	✓	✓	✓		CO RSA private/public keys	N/A

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P	A U D	U A		
Modify USB token PIN	Modify CO's own USB token PIN	✓	✓	✓		CO RSA private/public keys	N/A
User Application							
Cryptographic operations using internal keys (using algorithms from Table 8)	Cryptographic functions using keys stored in the keystore database				✓	AES, HMAC, RSA, ECDSA, SM2, SM4 keys LMKs	R, U
Cryptographic operations using external keys (using algorithms from Table 8)	Cryptographic functions using keys stored in the User Application's own keystore database				✓	AES, HMAC, RSA, ECDSA, SM2, SM4 keys LMKs	R, U
Generate, store and export key	Generate, store and export a new key				✓	AES, HMAC, RSA, ECDSA, SM2, SM4 keys LMKs	C, R, U
Generate and export key	Generate and export a new key				✓	AES, HMAC, RSA, ECDSA, SM2, SM4 keys LMKs	C, R, U
Transfer keys from old to new DMK	Use old and new LMKs to re-wrap the keys and calculate the integrity check value				✓	LMKs	R, U
Generate non-security related business PIN and print it to serial printer	Generate non-security relevant business PIN and print it with the printer Output encrypted PIN				✓	N/A User Application's AES/SM4 key	C, R, U
Random Number Generation	SP800-90A CTR_DRBG with AES-256				✓	Entropy input string Internal state	R, U
Other FIPS-related, non-Authenticated Services							
TLS network protocol v1.2	Provide HTTPS connection for the management web interface and TLS connection for User Applications with AES and RSA. The service provides a connection before user authentication starts.	N/A				AES keys RSA public/private keys	C, R, U

Service	Service Description and Algorithms	Role				Keys and CSPs	Access Types
		M N G	O P D	A U D	U A		
	Ciphersuites: <ul style="list-style-type: none"> • AES-256-GCM-SHA384 • AES-128-GCM-SHA256 						
Display mode of operation	Display mode of operation on the LCD touch screen and through the serial port terminal commands	N/A			N/A	N/A	
Display module version	Display module version on the LCD touch screen and through the serial port terminal commands	N/A			N/A	N/A	
Display network address	Display network address on the LCD touch screen and through the management serial console port.	N/A			N/A	N/A	
Factory reset (zeroization)	Factory resets the module	N/A			DMK LMKs	Z	
Device initialization	Execute when module is uninitialized Select the operation mode Generate/compose DMK Register the first Manager	N/A			DMK	C, R, U	

4.4 Cryptographic Algorithms

The module implements cryptographic algorithms that are used by the services provided by the module. The cryptographic algorithms that are approved to be used in the FIPS mode of operation are tested and validated by the CAVP. No parts of the Transport Layer Security (TLS) protocol have been tested by the CAVP, but for the key derivation function (KDF).

Table 8, Table 9 and Table 10 present the cryptographic algorithms in specific modes of operation. These tables include the CAVP certificate number, the algorithm name, respective standards, the available modes and key sizes wherein applicable, and usage. Information from certain columns may be applicable to more than one row.

4.4.1 FIPS-Approved Cryptographic Algorithms

Table 8 lists the cryptographic algorithms that are approved to be used in the FIPS mode of operation. Note that not all algorithms listed in the certificates are used in the approved mode of operation.

Table 8: FIPS-approved cryptographic algorithms.

Algorithm	Standard	Mode/Method	Key size	Use	CAVP Cert. #
AES	[FIPS197] [SP800-38A]	ECB, CBC, CFB128, CTR, OFB	128, 192 and 256 bits	Data Encryption and Decryption	#C1323
	[FIPS197] [SP800-38B]	CMAC		MAC Generation and Verification	
	[FIPS197] [SP800-38D]	GMAC			
	[FIPS197] [SP800-38C]	CCM	128 and 256 bits	Data Encryption and Decryption	
	[FIPS197] [SP800-38D]	GCM			
	[FIPS197] [SP800-38E]	XTS			
	[FIPS197] [SP800-38F]	KW, KWP	128, 192 and 256 bits	Key Wrapping and Unwrapping	
DRBG	[SP800-90A]	CTR_DRBG AES256 without DF, with PR	N/A	Random Number Generation	#C1323
ECDSA	[FIPS186-4]	Testing Candidates		Key Pair Generation	#C1323

Algorithm	Standard	Mode/Method	Key size	Use	CAVP Cert. #
		SHA2-224, SHA2-256, SHA2-384, SHA2-512	<ul style="list-style-type: none"> • P-224, P-256, P-384, P-521 • K-233, K-283, K-409, K-571 • B-233, B-283, B-409, B-571 	Signature Generation and Signature Generation Component	
		N/A	<ul style="list-style-type: none"> • P-192, P-224, P-256, P-384, P-521 • K-163, K-233, K-283, K-409, K-571 	Public Key Verification	
		SHA-1 ⁴ , SHA2-224, SHA2-256, SHA2-384, SHA2-512	<ul style="list-style-type: none"> • B-163, B-233, B-283, B-409, B-571 	Signature Verification	
HMAC	[FIPS198-1]	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	128, 192 and 256 bits	Message Authentication Code	#C1323
KDF TLS (TLS v1.2) Component	[SP800-135]	SHA2-256, SHA2-384		Key Derivation	#C1323
RSA	[FIPS186-4]	B.3.3 Probably Prime	2048, 3072 bits	Key Pair Generation	#C1323
			4096 bits		#A185
		X9.31, PKCS#1v1.5 and PSS with:	2048 and 3072 bits	Digital Signature Generation	#C1323

⁴ SHA-1 is not allowed for signature generation.

Algorithm	Standard	Mode/Method	Key size	Use	CAVP Cert. #
		SHA2-224, SHA2-256, SHA2-384, SHA2-512	4096 bits		#A51
		X9.31, PKCS#1v1.5 and PSS with: SHA-1 ⁴ , SHA2-224, SHA2-256, SHA2-384, SHA2-512	1024, 2048, 3072 bits	Signature Verification	#C1323
			4096 bits		#A48
	[FIPS186-2]	X9.31, PKCS#1v1.5 with: SHA-224, SHA-256, SHA-384, SHA-512	4096 bits	Signature Generation	#C1323
RSA Primitive Component	[SP800-56B]	Decryption (RSADP)	2048 bits	Key Establishmen t	#C1323
	PKCS#1v2.1	PKCS#1v1.5 and PSS (RSASP)	N/A	Signature Generation	#C1323
SHS	[FIPS180-4]	SHA-1 ⁴ , SHA2-224, SHA2-256, SHA2-384, SHA2-512		Message Digest	#C1323
SHA3	[FIPS202]	SHA3-224, SHA3-256, SHA3-384, SHA3-512		Message Digest	#C1323

Algorithm	Standard	Mode/Method	Key size	Use	CAVP Cert. #
KDF	[SP800-108]	KDF Mode: Counter MAC Mode: HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	64, 256 bits	Key Derivation	#C1323
ENT	[SP800-90B]	N/A	N/A	N/A	N/A
KTS	[SP800-38F]	AES-CCM, AES-GCM, AES-KW, AES-KWP	128, 192, 256 bits	Key Wrapping	#C1323
	[SP800-38F]	AES-GCM	128, 256 bits	Key Wrapping in TLS	#C1323
	[SP800-38F]	AES-ECB and AES-CMAC	128, 192, 256 bits	Key Wrapping	#C1323
CKG	SP800-133 IG D.12	N/A	128, 192, 256 bits	Symmetric Key Generation	N/A

4.4.2 Non-Approved-but-Allowed Cryptographic Algorithms

Table 9 lists the non-Approved-but-Allowed cryptographic algorithms provided by the module that are allowed to be used in the FIPS mode of operation.

Table 9: Non-Approved but allowed cryptographic algorithms.

Algorithm	Usage
RSA Key Wrapping with key size between 2048 bits and 4096 bits	Key wrapping, key establishment methodology provides between 112 and 149 bits of encryption strength.
EC Diffie-Hellman with P-256 curve ⁵	Key agreement with shared secret computation and with TLS KDF Cert. #C1323; key establishment methodology provides 128 bits of encryption strength). Algorithm is not self-tested. Allowed to be used in the approved mode by IG D.8 Scenario 4.

4.4.3 Non-Approved Cryptographic Algorithms

Table 10 lists the cryptographic algorithms that are not allowed to be used in the FIPS mode of operation. These algorithms (and corresponding services in Table 6) are only available in the non-FIPS mode of operation, as enforced by the module.

Table 10: Non-FIPS approved cryptographic algorithms.

Algorithm	Usage
SM2	Chinese Elliptic Curve Digital Signature Algorithm (asymmetric encrypt/decrypt, key agreement, signature generation/verification)
SM3	Chinese Message Digest algorithm (message digest)
SM4	Chinese Block Cipher Symmetric algorithm (symmetric encryption/decryption)

⁵ The KAS-ECC component was tested under Certs. #C1323 and #C1328. As this algorithm is not being claimed as approved, but allowed, these certificates are not listed in this entry. The TLS KDF algorithm was tested under Cert. #C1323.

5 Physical Security

The module employs several different physical security mechanisms in compliance with FIPS 140-2 physical security requirements for a Security Level 3 module.

5.1 Static Protection

The module is enclosed in a stainless steel and aluminum which is made from production grade material. The module also contains three tamper evident seals produced and factory installed by the vendor. The label positions, as shown in Figure 8, are:

1. A label on the left side of the chassis, covering the joint gap between the upper cover and the chassis, attached at approximately 8 cm from the rear of the chassis.
2. A label on the right side of the chassis, covering the joint gap between the upper cover and the chassis, attached at approximately 8 cm from the rear of the chassis.
3. A label on the rear panel of the chassis, covering the joint with the upper cover, attached above the power switch.



Figure 8: Tamper evidence labels.

Any attempt to remove any of the seals or open the case will leave an evidence. Users of the HSM with physical access to the device are responsible for following the guidance at

Section 1.2 and regularly inspecting the seals and verifying that they remain intact and remain in the original location as shown in Figure 8.

If evidence of tampering is detected, the module shall be considered non-compliant and its use as a FIPS validated module shall cease immediately. A user with a Crypto Officer role must again follow the guidance in Section 1.2.

5.2 Dynamic Protection

The module contains a removable top cover, which is protected by two tamper switches. Removing the top cover causes the module to zeroize the DMK stored in the Protection Card and powers-off the module. Both switches work independently of each other: if either one is triggered, the module will zeroize the DMK and power-off.

6 Operational Environment

6.1 Applicability

The module operates in a non-modifiable operational environment. The firmware components of the module, once loaded, cannot be modified or erased. Therefore, the FIPS 140-2 requirements for the operational environment are not applicable to the module.

7 Cryptographic Key Management

Table 11 summarizes the keys and other CSPs that are used by the cryptographic services implemented in the module. The other subsections describe how keys and CSPs are managed during their lifetime.

Table 11: Lifecycle of keys and other Critical Security Parameters (CSPs).

Name	Use	Generation	Entry and Output	Storage	Zeroization
Device Master Keys (DMK)	Master Key	During HSM initialization, using the SP 800-90A DRBG.	Entry: via USB tokens during initialization or restoration. Output: to USB token via secret sharing.	In the protection card	<ul style="list-style-type: none"> ▪ Zeroized if chassis is opened (tamper switch is triggered). ▪ Via factory reset service. ▪ If Clear button is pressed for 10 seconds. Zeroization overwrites contents with 0xFF.
Local Master Keys (LMK)	Encryption/Decryption of User Application keys/CSPs with AES-GCM or AES-ECB with AES-CMAC.	Derived from the DMK using the SP 800-108 CTR KDF (HMAC).	N/A	RAM	Deleted from RAM whenever the module powers off: <ul style="list-style-type: none"> ▪ if chassis is opened (tamper switch is triggered). ▪ Via factory reset service. ▪ If Clear button is pressed for 10 seconds.
User Application AES keys	Encryption/decryption. CMAC.	SP 800-90A DRBG	(Non-public keys) Entry and output wrapped with LMK using AES-ECB with AES-CMAC.	In the module's keystore database. RAM.	<ul style="list-style-type: none"> ▪ N/A when stored in hard disk (non-public keys are stored encrypted). ▪ Deleted from RAM whenever the module powers off: <ul style="list-style-type: none"> ○ if chassis is opened (tamper switch is triggered). ○ Via factory reset service. ○ If Clear button is pressed for 10 seconds.
User Application HMAC keys	HMAC generation and verification.		Also output in encrypted form as result of backup process.		
User Application RSA public/private keys	Encryption/decryption. Signature generation and verification.	SP 800-133. FIPS 186-4. SP 800-90A DRBG.			
User Application ECDSA public/private keys	Signature generation and verification				
Key Backup Key (KBK)	Used as key encryption key when	SP 800-90A DRBG	Entry via USB tokens during	RAM	Deleted from RAM whenever the module powers off:

Name	Use	Generation	Entry and Output	Storage	Zeroization
	backing up the keystore database.		restoration via secret sharing scheme (split knowledge). Output to USB tokens during the backup process using secret sharing (split knowledge).		<ul style="list-style-type: none"> ▪ if chassis is opened (tamper switch is triggered). ▪ Via factory reset service. ▪ If Clear button is pressed for 10 seconds.
Crypto Officer Authentication private RSA key	CO authentication	N/A (generated by USB token outside of module)	N/A	N/A	N/A
Crypto Officer Authentication public RSA key	CO authentication	N/A (generated by USB token outside of module)	Entry upon generation by USB token in plaintext. Output encrypted as part of the backup process.	In module's keystore database. RAM.	Deleted from RAM whenever the module powers off: <ul style="list-style-type: none"> ▪ if chassis is opened (tamper switch is triggered). ▪ Via factory reset service. ▪ If Clear button is pressed for 10 seconds.
User Application PIN	User Application authentication	SP 800-90A DRBG	N/A	In the module's keystore database on the hard disk. RAM.	<ul style="list-style-type: none"> ▪ N/A when stored in hard disk (keys are stored encrypted). ▪ Deleted from RAM whenever the module powers off: <ul style="list-style-type: none"> ○ if chassis is opened (tamper switch is triggered). ○ Via factory reset service. ○ If Clear button is pressed for 10 seconds.
Entropy input string	Seed the SP 800-90A DRBG	Obtained from the NDRNG	N/A	RAM	Deleted from RAM whenever the module powers off:

Name	Use	Generation	Entry and Output	Storage	Zeroization
					<ul style="list-style-type: none"> ▪ if chassis is opened (tamper switch is triggered). ▪ Via factory reset service. ▪ If Clear button is pressed for 10 seconds.
DRBG internal state (V, C, key)	DRBG internal state	During DRBG initialization	N/A	RAM	Zeroized when DRBG is uninstantiated (overwritten by a pattern).
TLS Specific Keys and CSPs					
AES derived keys	Encryption, decryption	Derived during TLS handshake using the SP 800-135 KDF	N/A	RAM	Zeroized when TLS session is terminated (overwritten by a pattern).
HMAC derived keys	HMAC generation and verification	Derived during TLS handshake using the SP 800-135 KDF	N/A	RAM	
EC Diffie-Hellman public/private key	Key agreement	Generated internally by the module during the establishment of the TLS tunnel. Generation uses FIPS 186-4 key generation method, and the random value used is generated using the SP800-90A DRBG.	N/A	RAM	
Pre-Master Secret	Establishment of TLS tunnel.	Generated internally by the module (from the EC Diffie-Hellman key agreement) during the establishment	Entry: if received by module as TLS server, wrapped with server's public RSA key; otherwise, no entry.	RAM	

Name	Use	Generation	Entry and Output	Storage	Zeroization
		nt of the TLS tunnel. Received by the module via API if module is acting as a TLS server.	Output: if generated by module as TLS client, wrapped with server's public RSA key; otherwise, no output.		
Master secret	Establishment of TLS tunnel.	Generated internally by the module (from the ([SP800-135] TLS KDF) during the establishment of the TLS tunnel.	N/A	RAM	
TLS Server RSA public/private key	Server-side TLS authentication	N/A	Entry: imported in a P12 certificate through TLS. No output.	In the module's keystore database on the hard disk. RAM.	<ul style="list-style-type: none"> ▪ N/A when stored in hard disk (non-public keys are stored encrypted) ▪ Deleted from RAM whenever the module powers off: <ul style="list-style-type: none"> ○ if chassis is opened (tamper switch is triggered). ○ Via factory reset service. ○ If Clear button is pressed for 10 seconds.
TLS KDF internal state	Establishment of TLS tunnel.	SP800-135 TLS KDF	N/A	RAM	Zeroized when TLS session is terminated (overwritten by a pattern).

7.1 Random Number Generation

The module employs a Deterministic Random Bit Generator (DRBG) compliant with [SP800-90A] for the generation of symmetric and asymmetric keys, creation of random number challenges for the identity-based authentication mechanism, and processing of the Random Number Generation service request.

The DRBG supports the AES-256 CTR-DRBG mechanisms. The DRBG is initialized during module initialization, without derivation function and with prediction resistance. The module performs DRBG health tests as defined in Section 11.3 of [SP800-90A].

For seeding the DRBG, the module uses a Non-Deterministic Random Number Generator (NDRNG). The NDRNG is implemented by the cryptographic module compliant with [SP800-90B] and marked as ENT on the certificate. The NDRNG provides a 768-bit seed with at least 356 bits of entropy to the DRBG. The DRBG is thus capable of supporting a minimum of 256 bits of encryption strength in its output.

The NDRNG implements continuous health tests required by [SP800-90B] within its architecture to ensure that the noise source and the entire entropy source continue to operate as expected.

7.2 Key Generation

For generating RSA, ECDSA, and EC Diffie-Hellman keys the module implements asymmetric key generation services compliant with [FIPS186-4] and using a DRBG compliant with [SP800-90A]. The random value used in asymmetric key generation is obtained from the DRBG. The public and private key pairs used in the EC Diffie-Hellman key agreement schemes are generated internally by the module using the same ECDSA key generation mechanism compliant with [FIPS186-4] and [SP800-56A].

For generating symmetric keys, the module uses random data obtained from the DRBG. Symmetric keys may also be derived from the shared secret established by EC Diffie-Hellman in a manner that is compliant to [SP800-135] through the TLS KDF.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) for symmetric and asymmetric keys as per [SP800-133] (vendor affirmed). The generation mechanism uses an unmodified output from the approved DRBG.

7.3 Key/CSP Storage

The module stores all User Applications' private and secret keys and CSPs in encrypted form in non-volatile memory in the file system's database.

The module protects keys and CSPs using key wrapping compliant with [SP800-38F]. The computed integrity value is stored with the encrypted key/CSP. The integrity of the stored key/CSP are verified upon decryption.

The DMKs are stored in plaintext in the RAM of the Protection Card.

The LMKs are stored in plaintext in the RAM of the module.

7.4 Key/CSP Zeroization

The module performs the zeroization upon certain events:

- When the factory reset service is invoked through the management serial console, the module zeroizes the DMK and overwrites it with 0xFF. It also zeroizes the user information, configuration information, and removes all encrypted keys and CSPs entries from the module's keystore database.
- If the tamper detection mechanism detects a tamper event, such as when the chassis is opened, the zeroization is initiated.
- If the Clear button in the front panel is pressed for 10 seconds, the zeroization is initiated.

All keys/CSPs stored in RAM, including the LMKs, are destroyed whenever the module is powered-off, which happens every time the zeroization is triggered.

7.5 Key Establishment

The module provides the EC Diffie-Hellman key agreement scheme as part of the TLS protocol. The module provides AES key wrapping per [SP800-38F] and RSA key wrapping using public key encryption and private key decryption primitives as allowed by [FIPS140-2_IG] D.9. RSA key wrapping may be used as part of the TLS protocol key exchange.

If keys are input to or output from the module, the module protects these keys with diverse approved key transport mechanisms according to IG D.9, and as listed in Table 11. The module thus implements the following key transport mechanisms:

- AES-KW and AES-KWP key wrapping.
- Approved authenticated encryption mode compliant with [SP800-38F] (e.g., AES-GCM, AES-CCM).
- Combination of approved symmetric encryption (AES-ECB) and approved message authentication code (AES-CMAC).
- Key wrapping provided by the TLS protocol with cipher suites AES-256-GCM-SHA384 and AES-128-GCM-SHA256. The module provides, in this context, approved authenticated encryption mode (AES-GCM) key wrapping as a result of the cipher suite encryption.
- RSA key encapsulation with RSA public encryption and private decryption primitives compliant with [SP800-56B].

Table 8 and Table 9 specify the key sizes allowed in the FIPS mode of operation. According to [SP800-57], the key sizes of AES key wrapping, RSA and EC Diffie-Hellman provide the following security strengths:

- AES key wrapping provides between 128 and 256 bits of encryption strength.
- RSA key wrapping provides between 112 and 149 bits of encryption strength.
- EC Diffie-Hellman key establishment methodology provides 128 bits of encryption strength.
- Approved authenticated encryption mode key establishment methodology (AES-GCM, AES-CCM) provides between 128 and 256 bits of encryption strength.
- Combination of approved symmetric encryption (AES-ECB) and approved message authentication code (AES-CMAC) provides between 128 and 256 bits of encryption strength.
- Key wrapping provided by the TLS protocol using approved authenticated encryption mode (AES-GCM). This key establishment methodology provides 128 or 256 bits of encryption strength.

7.6 Split Knowledge

The module uses two different split knowledge procedures for entering and outputting the Device Master Key (DMK), the Key Backup Key (KBK), and generating symmetric keys. These are the Split Knowledge using random numbers and XOR, and the Split Knowledge using the Shamir Shared Secret scheme.

The Operator has the possibility, when generating symmetric keys, to manually enter between two to five (2 to 5) component of the symmetric key. The Operator must enter each component twice and the module verified that the components match. The final is constructed by XORing all components together. The symmetric key obtained through this procedure is then entered into the module. It is not possible to export these symmetric keys using split knowledge procedures, or as plaintext.

The split knowledge procedure used to back-up the KBK is based on Shamir's Secret Sharing algorithm. The module splits the key into three to five components, which are then stored separately in three to five different USB tokens belonging to the Manager role after each Manager has authenticated successfully to the module. Any two out of three, or three out of five components need be entered into the module to reconstruct the original key.

The split knowledge procedure used to back-up the DMK functions as follows. If n is the number of parts, $n-1$ random numbers will be generated and output to the USB tokens belonging to the Manager role. The last Manager USB token will receive the KBK XORed with all random numbers. This ensures that all Managers authenticate to reconstruct the KBK, and that each component is necessary to reconstruct the KBK. Therefore, one USB token receives:

$$\left(\sum_{i=1}^{n-1} r_i \right) \oplus DMK$$

And all others USB tokens receive the $r_i, i \in \llbracket 1, 4 \rrbracket$.

7.7 Key Entry/Output

The module supports electronic distribution of keys in encrypted form. The module does not support intermediate key generation and does not accept entry or output of keys in plaintext format from outside its physical boundary.

The module also supports manual entry of symmetric keys in encrypted form, with the exception of the DMK and KBK, which can be input and output using split knowledge procedures (Section 7.6). Split knowledge input and output of the DMK and the KBK is done through the key management services and using external USB tokens. Note that all keys entered or output to or from the module are however encrypted by a TLS channel for the Crypto Officers, or by key wrapping for the User Application.

Cryptographic services requested by User Applications may involve input of keys in the request message or output of keys in the response message. The module uses key wrapping compliant with [SP800-38F] as the key transport mechanism.

Table 11 lists the methods for input and output of each key and CSP, when applicable.

8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module has been tested and found to conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, FCC PART 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., Home use). These devices are designed to provide reasonable protection against harmful interference when the devices are operated in a commercial environment.

9 Self-Tests

9.1 Power-Up Self-Tests

The module implements a series of power-up self-tests (POSTs) to ensure that cryptographic algorithms work as expected, and that the module has not been corrupted. The power-up self-tests include integrity tests on the firmware and cryptographic algorithm self-tests.

The module performs the self-tests automatically as the module is powered on. No operator intervention is necessary to run the POSTs. While the module is executing the POSTs, services are not available, and input and output are inhibited. The module is not available for use until successful completion of the POSTs. The execution of the POSTs is indicated on the LCD touch screen.

The POST for the NDRNG include the Repetition Count Test and Adaptive Proportional Test on 1,024 samples of raw entropy data (the data is later discarded).

When the module finishes the power-up self-tests successfully, the LCD touch screen becomes responsive.

If any of the POSTs fail, the module enters the error state. The LCD touch screen indicates the error information, and the fault indicator light is illuminated. In the error state, input and output are inhibited, and neither management, nor cryptographic services are available. The module must then be restarted, which will force the execution of the POST again.

9.1.1 Integrity Tests

The system starts in the form of two ISO images. The integrity test routine verifies the firmware of the protection card and the ISO images by comparing a CRC-32 value calculated at runtime with the value, stored in the module, that was computed during the production process. The ISO images include all the programs, libraries, web pages and the core components of the operating system. If the integrity test succeeds, the ISO images are further mounted and loaded, thus continuing with the POST routines on the algorithms. Similarly, the module performs the integrity test on the keystore database and on the configuration data.

If the CRC-32 values do not match, the integrity test fails, and the module enters the error state.

9.1.2 Cryptographic Algorithm Tests

Table 12 details the self-tests that are performed on the FIPS-approved cryptographic algorithms supported in the FIPS-approved mode of operation, using the Known-Answer Tests (KATs) and Pairwise Consistency Tests (PCTs).

During KATs, the module computes the result of a cryptographic operation and compares it with the known value. If the answer does not match the known answer, the KAT has failed, and the module enters the error state. During PCTs, asymmetric key pairs are used for signature generation and verification, or for encryption and decryption. If any of those operations fail (signaling an inconsistency with key pairs), the module enters the error state.

Table 12: Self-tests.

Algorithm	Test
AES	<ul style="list-style-type: none"> • KAT AES(ECB) with 128-bit key, encryption • KAT AES(ECB) with 128-bit key, decryption • KAT AES(CCM) with 192-bit key, encryption • KAT AES(CCM) with 192-bit key, decryption • KAT AES(GCM) with 256-bit key, encryption • KAT AES(GCM) with 256-bit key, decryption • KAT AES(CMAC) with 128-bit, 192-bit and 256-bit key • KAT AES(XTS) with 128-bit and 256-bit keys, encryption • KAT AES(XTS) with 128-bit and 256-bit keys, decryption
DRBG	<ul style="list-style-type: none"> • KAT CTR_DRBG using AES-256 without DF, with PR • Health tests
ECDSA	<ul style="list-style-type: none"> • PCT ECDSA for signature generation/verification with P-224 and SHA-512, and B-233 and SHA-512
HMAC	<ul style="list-style-type: none"> • KAT HMAC-SHA-224 • KAT HMAC-SHA-256 • KAT HMAC-SHA-384 • KAT HMAC-SHA-512
RSA	<ul style="list-style-type: none"> • KAT RSA PSS signature generation and verification with 2048-bit key and SHA-256
SHA3	<ul style="list-style-type: none"> • SHA3-224 • SHA3-256 • SHA3-384 • SHA3-512
SHS	<ul style="list-style-type: none"> • KAT SHA-1 • SHA2 self-tests are performed within the HMAC self-tests.
NDRNG	<ul style="list-style-type: none"> • Adaptive Proportion Test • Repetitive Count Test

9.2 Conditional Self-Tests

Conditional tests are performed during operational state of the module when the respective cryptographic functions are used. If any of the conditional tests fails, the module transitions to error state.

Table 13 lists the conditional self-tests performed by the functions.

Table 13: Conditional self-tests.

Algorithm	Test
ECDSA Key generation	PCT using SHA-256, signature generation and verification.
RSA Key generation	PCT using SHA-256, signature generation and verification, and for encryption and decryption.
NDRNG	Continuous health tests (Repetition Count Test and Adaptive Proportion Test).
Manual key entry	Duplicate key entries

9.3 On-Demand Self-tests

The module provides the Self-Test service to perform self-tests on demand. On demand self-tests can be invoked by powering-off and reloading the module. This service performs the same cryptographic algorithm tests executed during power-up.

10 Guidance

This section provides guidance for the Crypto Officer (Manager, Operator, Auditor) and User Application roles to maintain proper use of the module per FIPS 140-2 requirements. In the FIPS mode of operation, all FIPS 140-2 requirements are enforced by the module. Service requests that do not meet the requirements are rejected by the module.

10.1 Crypto-Officer Guidance

Crypto Officers shall not backup a DMK or a keystore along with a KBK from FIPS mode and restore it to the Compatibility mode. Vice versa, Crypto Officers shall not backup a DMK or a keystore along with a KBK from the Compatibility mode and restore it to the FIPS mode.

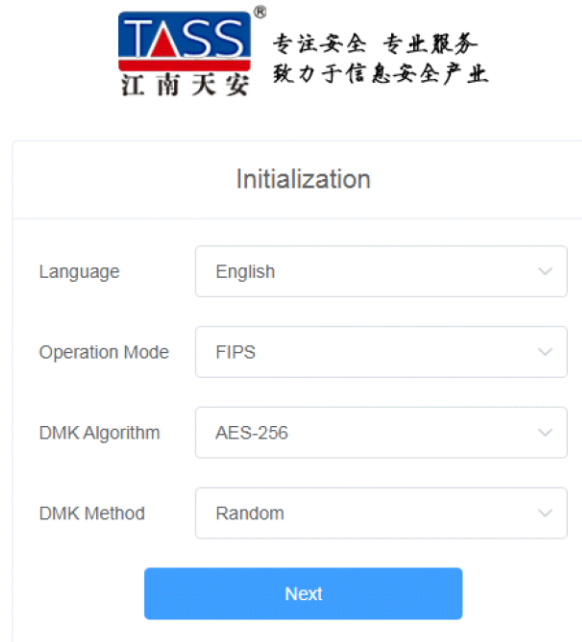
10.1.1 Module Initialization

The module is shipped to the user without any initialization of keys or CSPs, or authentication information. The mode of operation is selected during this initialization routine and can only be changed to another mode by re-initializing the module.

The user must perform the initialization of the module following the instructions included in module's User's Manual.

1. Verify that the external condition of the package to see if there are signs of damage, or if the package has been opened during transit.
2. Open the package and verify with the content list that the HSM and all accessories are included.
3. Verify that the three tamper evidence seals are intact and located at the expected positions (see Section 5.1).
4. Connect the module's power supplies.
5. Connect a computer to the module through the management serial port.
6. Power-up the module.
7. Login into the system and run the management program.
8. Verify that the product model and version provided in the "View Device Basic Information" menu option matches the following information:
 - Operation Mode: FIPS approved.
 - Firmware Version: H1.00.00.
9. Use the Installation Wizard to perform the following activities:
 - Initialize the device, Note: For uninitialized Crypto Engine, the home page will be automatically jumped to the initialization page, which contains two steps:
 - a. Set up the operation mode and choose the DMK algorithm and generation mode.
 - b. Register the first Manager UKEY .

As below:



Initialization

Language English

Operation Mode FIPS

DMK Algorithm AES-256

DMK Method Random

Next

Figure 9: Initialize - 1



Administrator Registration

CO Name 6315

UKey TASS06315

* PIN

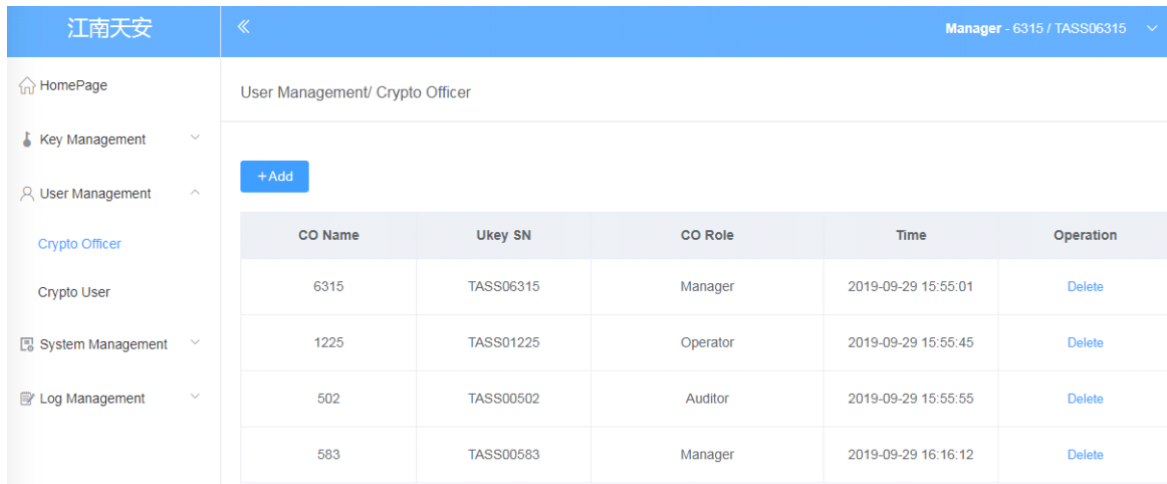
Register

Figure 10: Initialize - 2

After initialization, the device will be restarted automatically, and the management page will jump to the login home page.

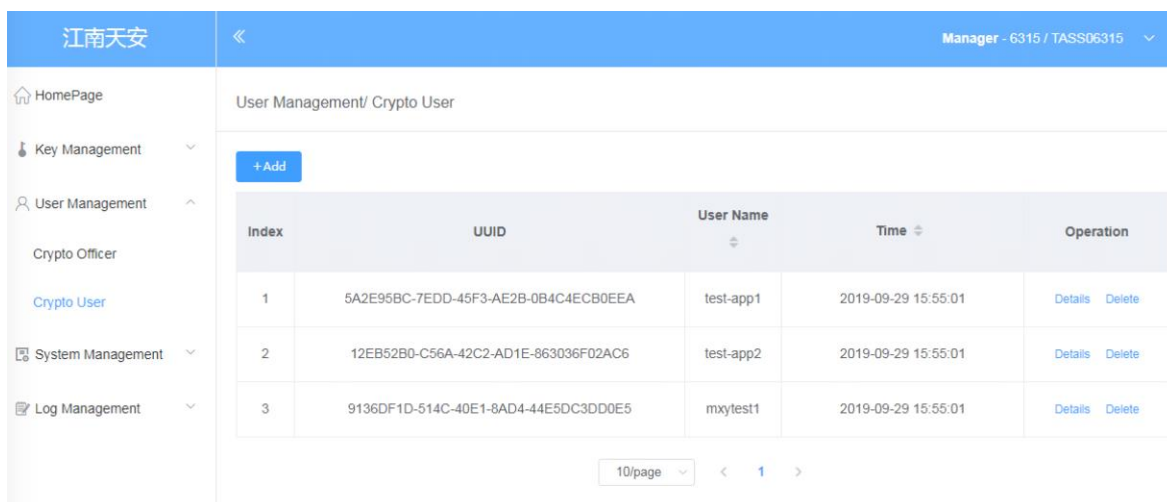
- After manager login, Create the users needed (Managers, Operator, Auditor, User Applications) and generate their credentials in the USB tokens.

As below:



CO Name	Ukey SN	CO Role	Time	Operation
6315	TASS06315	Manager	2019-09-29 15:55:01	Delete
1225	TASS01225	Operator	2019-09-29 15:55:45	Delete
502	TASS00502	Auditor	2019-09-29 15:55:55	Delete
583	TASS00583	Manager	2019-09-29 16:16:12	Delete

Figure 11: User Management – Crypto Officer



Index	UUID	User Name	Time	Operation
1	5A2E95BC-7EDD-45F3-AE2B-0B4C4ECB0EEA	test-app1	2019-09-29 15:55:01	Details Delete
2	12EB52B0-C56A-42C2-AD1E-863036F02AC6	test-app2	2019-09-29 15:55:01	Details Delete
3	9136DF1D-514C-40E1-8AD4-44E5DC3DD0E5	mxytest1	2019-09-29 15:55:01	Details Delete

Figure 12: User Management – Crypto User

- Generate (or import) symmetric keys (optional).

As below:

Key Management/ Symmetric Key

+Generate Key ->Export List Clear All

Index	Alias	Algorithm	Check Value	Creation Time	Operation
1	test1	AES-128	92B469F4E62C8237	2019-09-29 15:55:00	Details Delete
10	test10	AES-192	A416FEDEF9468D7D	2019-09-29 15:55:00	Details Delete
123		AES-256	27194ADA41ECE60E	2019-09-29 15:55:00	Details Delete

Total 3 10/page < 1 >

Figure 13: Key Management – Symmetric Key

- Generate RSA and ECDSA keys (optional).
- After operator login, Configure the network.

As below:

Management Network Port

* Network Port LAN2

* IP 192.168.22.30

* Subnet mask 255.255.255.0

* Gateway 192.168.22.254

Save

Host Network Port

* Network Port LAN1

* IP 192.168.22.30

* Subnet mask 255.255.255.0

* Gateway 192.168.22.254

Save

Figure 14: Network Configuration

- Configure the device configuration, includes Host Service Property and Communication Configuration.

As below:

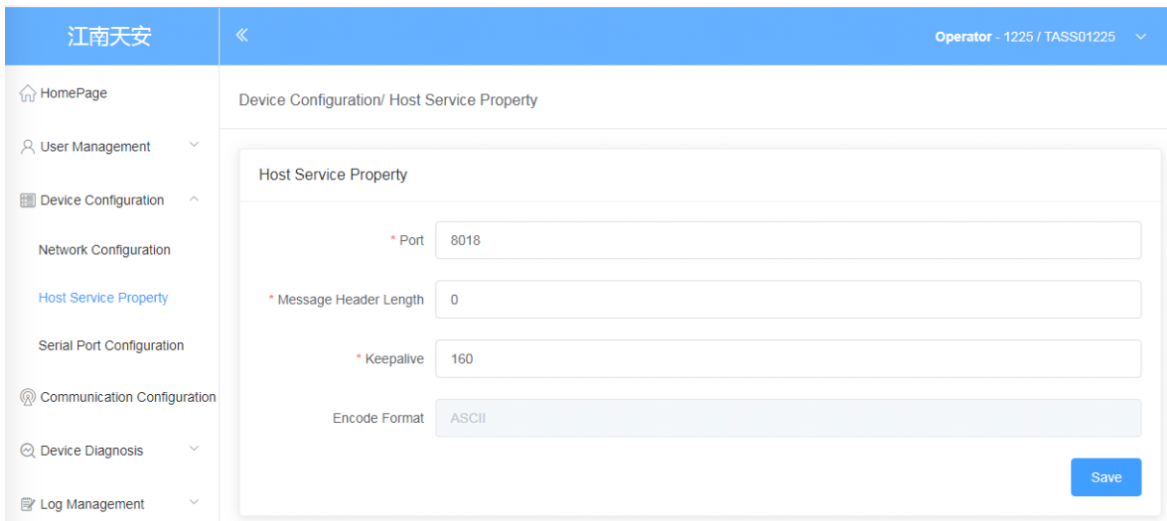


Figure 15: Device Configuration – Host Service Property

- Configure the IP address whitelist and User Applications for the services.
As below:

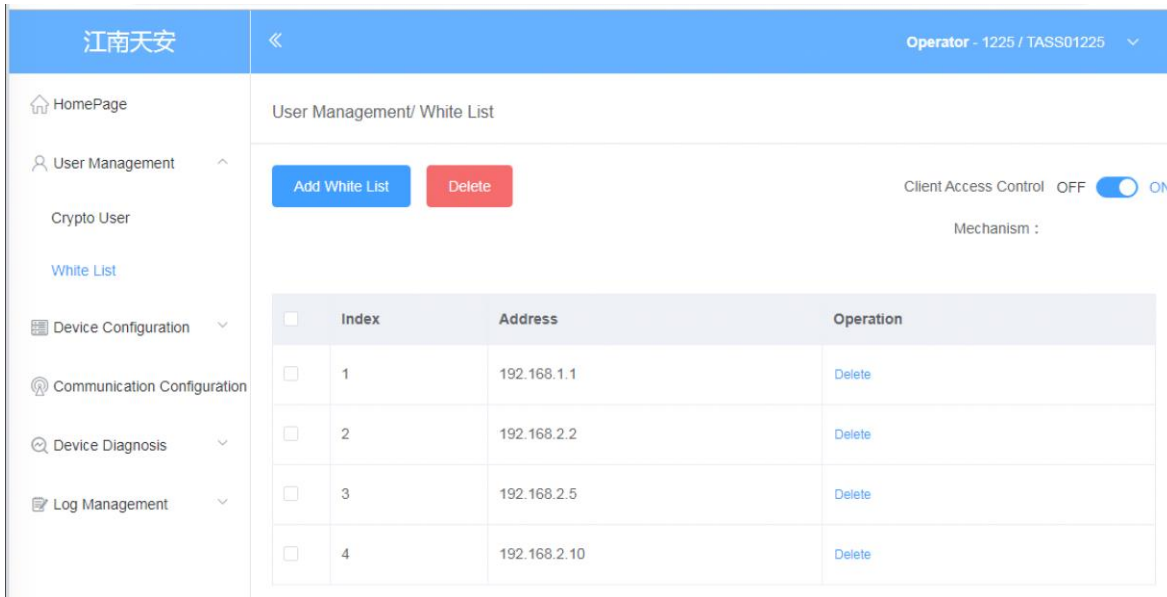


Figure 16: User Management – White List

The screenshot shows a web interface for 'User Management / Crypto User'. The left sidebar contains navigation options: HomePage, User Management (expanded), Crypto User (selected), White List, Device Configuration, Communication Configuration, Device Diagnosis, and Log Management. The main content area displays a table with the following data:

Index	UUID	User Name	Time	Operation
1	5A2E95BC-7EDD-45F3-AE2B-0B4C4ECB0EEA	test-app1	2019-09-29 15:55:01	PIN Management
2	12EB52B0-C56A-42C2-AD1E-863036F02AC6	test-app2	2019-09-29 15:55:01	PIN Management
3	9136DF1D-514C-40E1-8AD4-44E5DC3DD0E5	mxytest1	2019-09-29 15:55:01	PIN Management

At the bottom of the table, there is a pagination control showing '10/page' and navigation arrows.

Figure 17: User Management – Crypto User

1.1. USB Tokens

In order to initialize the module, the USB tokens must be available. These USB tokens are utilized as such:

- One USB token for each Manager, one USB token for the Operator, one USB token for the Auditor.
- Minimum three USB tokens are needed for exporting the KBK components.
- Minimum two USB tokens are needed for exporting the DMK.

The USB tokens must be initialized with an ad-hoc utility shipped with the management firmware: the module's management interface comes with a utility that allows the first user of the module to create the Manager role and start creating USB tokens (RSA keys + PINs) to deploy to other Administrators. This utility is the first thing that a user gets access to when the module is set to factory default. Access to the USB token is protected through an eight-digit PIN.

1.2. Verification of Tamper Evidence Seals

Users of the HSM with physical access to the module, typically users with a Crypto Officer role, must visually verify that the tamper evidence seals are intact and located in the expected positions of the chassis per Section 5.1. The procedure is as follows.

At least once a month, a user with the Crypto Officer role shall verify each of the three tamper-evidence labels at the locations per Section 5.1. In case evidence of tampering is found, the Crypto Officer shall immediately cease operation of the module and shall perform the factory reset service. Next, the Crypto Officer shall contact the manufacturer to return the module for repair and maintenance. At the factory, new tamper-evidence labels shall be applied as specified in Section 5.1. Upon receiving the restored module, the Crypto Officer shall follow the guidance as applicable to a new module.

1.3. Secure Distribution Process

10.1.2 Packing

The whole equipment and accessories are first packed into the inner packing box, and the foam plastic is cushioning in the packing box. The module is firmly wrapped, and then packed into the outer packing box together with the inner packing box, and TASS is used. The transparent tape of logo pastes the joint of the carton; in addition, one side of the outer packing box is pasted with the model and serial number of the equipment in the package; finally, the packing box is bound with the automatic packer, as shown in the following figure:

The whole equipment and accessories are first packed into the inner packing box, and the foam plastic is cushioning in the packing box, and the module is firmly wrapped.

Then, it is packed into the outer packing box, and the adhesive tape with the manufacturer's logo is used to paste the carton joints. In addition, one side of the outer packing box is affixed with the type and serial number of the equipment.

And finally, use the automatic packaging to bundle the packing box, as shown in the following figure:



10.1.3 Delivery

Express delivery (SF) is chosen for delivery. The express sheet is pasted on the transparent tape at the joint of the outer package, and then delivered to the express company.

Each express bill has a unique order number. From the delivery to the courier, you can query and track the logistics situation through the express official website.

In addition, the manufacturer will inform the receiving party of the express bill number, equipment model and serial number by e-mail.

10.1.4 Receiving acceptance

After receiving the package, the receiving party needs to check: the express bill, packing strap and the transparent tape at the joint are complete, and the express bill number,

equipment model and equipment serial number are consistent with the contents of the mail, then the package shall be signed for acceptance; if there is any abnormality, the package shall be rejected.

10.2 Algorithm Considerations

10.2.1 AES-GCM IV

AES-GCM encryption is used in the following contexts in the module:

- TLS protocol version 1.2. The module is compliant with [SP 800-52] and the mechanism for IV generation is compliant with [RFC5288]. The operations of one of the two parties involved in the TLS key establishment scheme are performed entirely within the cryptographic boundary of the module, including the setting of the counter portion of the IV. In case the module's power is lost and then restored, the key and IV used for AES-GCM encryption or decryption shall be re-distributed. In this case, the nonce_explicit part of the IV is 64 bits long. Should the nonce_explicit part of the IV wrap, the TLS connection would terminate and a new key and IV would need to be renegotiated by the module.
- Encryption of the Application Users' PINs in the module's database. The AES-GCM IV is constructed by hashing (with SHA-256 in the approved mode) the UserName of the Application User. The UserName is unique, and therefore the IV will be unique per AES-GCM encryption instance for each 128-bit PIN. The key and IV used for the GCM encryption are derived from the DMK and the UserName. The key and IV are not stored permanently in the module.
- User Application request to encrypt with AES-GCM. In that case, the command will determine whether the IV is:
 - Provided by the command, in which case the IV is externally generated and therefore non-FIPS Approved.
 - Randomly generated using the module's approved DRBG and IV of at least 96 bits. This case of IV generation is compliant with scenario 2 of IG A.5.

In case of loss of power, only the GCM key will remain in the module's database. Any request provided with a specific IV will need to be re-initiated.

10.2.2 AES-XTS

The AES algorithm in XTS mode can be only used for the cryptographic protection of data on storage devices, as specified in [SP800-38E]. In addition, the module enforces that the length of a single data unit encrypted with the XTS-AES does not exceed 2^{20} AES blocks (that is 16 MiB of data) by using a counter of the number of encryptions performed with each key since its generation.

For those keys provided by external entities (User Applications) as part of the cryptographic service requests, the verification of this limit must be enforced by the entities that request the service (e.g. server applications).

In addition, to meet the requirement in [FIPS140-2_IG] A.9, the module implements a check to ensure that the two AES keys used in XTS-AES algorithm are not identical.

10.2.3 Key Usage and Management

In general, a single key shall be used for only one purpose (e.g., encryption, integrity, authentication, key wrapping, random bit generation, or digital signatures) and be disjoint

between the modes of operations of the module. Thus, if the module is switched between its FIPS mode and non-FIPS mode or vice versa, the following procedures shall be observed:

- The DRBG engine shall be reseeded.
- CSPs and keys shall not be shared between security functions of the two different modes.

10.3 Handling Self-Test Errors

When the module is in error state, output is inhibited, and no cryptographic operations are available. Any calls to the cryptographic functions in error state will return error code: '99' in response message.

The only way to recover from the error state is to reload the module and restart the application. If failures persist, the module must be reinstalled.

11 Mitigation of Other Attacks

RSA is vulnerable to timing attacks. In a setup where attackers can measure the time of RSA decryption or signature operations, blinding must be used to protect the RSA operation from that attack.

The API function of `RSA_blinding_on()` turns blinding on for RSA and generates a random blinding factor. The random number generator is seeded prior to calling `RSA_blinding_on()`.

RSA blinding cannot be turned off and is always used.

12 Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DMK	Device Master Key
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
HMAC	(Keyed) Hash Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function
LMK	Local Master Key
NDRNG	Non-Deterministic Random Number generator
NIST	National Institute of Standards and Technology
POST	Power On Self Test
PR	Prediction Resistance
PSS	Probabilistic Signature Scheme
PUB	Publication
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
TLS	Transport Layer Security

13 References

The FIPS 140-2 standard, and information on the CMVP, can be found at <http://csrc.nist.gov/groups/STM/cmvp/index.html>. More information describing the module can be found on the vendor web site at www.tass.com.cn.

This Security Policy contains non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is proprietary and is releasable only under appropriate non-disclosure agreements.

Document	Author	Title
FIPS 140-2	NIST	FIPS 140-2: Security Requirements for Cryptographic Modules
FIPS IG	NIST	Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program
FIPS 140-2 Annex A	NIST	FIPS 140-2 Annex A: Approved Security Functions
FIPS 140-2 Annex B	NIST	FIPS 140-2 Annex B: Approved Protection Profiles
FIPS 140-2 Annex C	NIST	FIPS 140-2 Annex C: Approved Random Number Generators
FIPS 140-2 Annex D	NIST	FIPS 140-2 Annex D: Approved Key Establishment Techniques
DTR for FIPS 140-2	NIST	Derived Test Requirements (DTR) for FIPS 140-2, Security Requirements for Cryptographic Modules
NIST SP 800-67	NIST	Recommendation for the Triple Data Encryption Algorithm TDEA Block Cipher
FIPS PUB 197	NIST	Advanced Encryption Standard
FIPS PUB 198-1	NIST	The Keyed Hash Message Authentication Code (HMAC)
FIPS PUB 186-4	NIST	Digital Signature Standard (DSS)
FIPS PUB 180-4	NIST	Secure Hash Standard (SHS)
NIST SP 800-131A	NIST	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes
PKCS#1	RSA Laboratories	PKCS#1 v2.1: RSA Cryptographic Standard
RFC 5288	https://tools.ietf.org/html/rfc5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS
Shamir's Secret Sharing	Shamir, Adi	"How to Share a Secret", Communications of the ACM, 22 (11), pp. 612-613. 1979, https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf