Non-Proprietary Security Policy

Primus HSM

FIPS 140-2 Cryptographic Module Security Policy

Version: 1.3

Date: 2019-12-18

Securosys SA

Förrlibuckstrasse 70

8005 Zürich

Switzerland

Table of Contents

List of Tables

List of Figures

Introduction

This document defines the Security Policy for the Securosys Primus HSM, hereafter denoted the Module. The Module is a physically secure banking HSM with cryptographic toolkit functionality provided over multiple APIs (PKCS11, JCE, CNG). The Module meets FIPS 140-2 overall Level 3 requirements.

The variants of the Module are shown in the table below. Note that the Module consists of two families, denoted the E-Module and the X-Module.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N	FW Versions
1	E20	60-1004 Rev0	2.5.3, 2.5.13
2	E60	60-1004 Rev0	2.5.3, 2.5.13
3	E150	60-1004 Rev0	2.5.3, 2.5.13
4	EP700	60-1008 Rev0	2.5.3, 2.5.13
5	X200	60-1002 Rev1	2.5.3, 2.5.13
6	X400	60-1002 Rev1	2.5.3, 2.5.13
7	X700	60-1002 Rev1	2.5.3, 2.5.13
8	X1000	60-1010 Rev1	2.5.3, 2.5.13

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated HSM. The Module is a multi-chip standalone embodiment; the cryptographic boundary includes the entire HSM device with exception of power supplies. The variants of the Module are firmware compatible and differ only in the amount of FPGA resources and clocking speed.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

	FIPS 140-2 Area	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
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	**3**

1.1 Hardware and Physical Cryptographic Boundary

The physical forms of the Module are depicted in the following Figures. The boundary of the module includes the chassis and everything within. However, this does not include the removable power supplies on the X-Module – they are outside the boundary and may be removed, replaced, etc. The X-Module also relies on Smart Cards as external input/output devices, for the purposes of operator authentication.

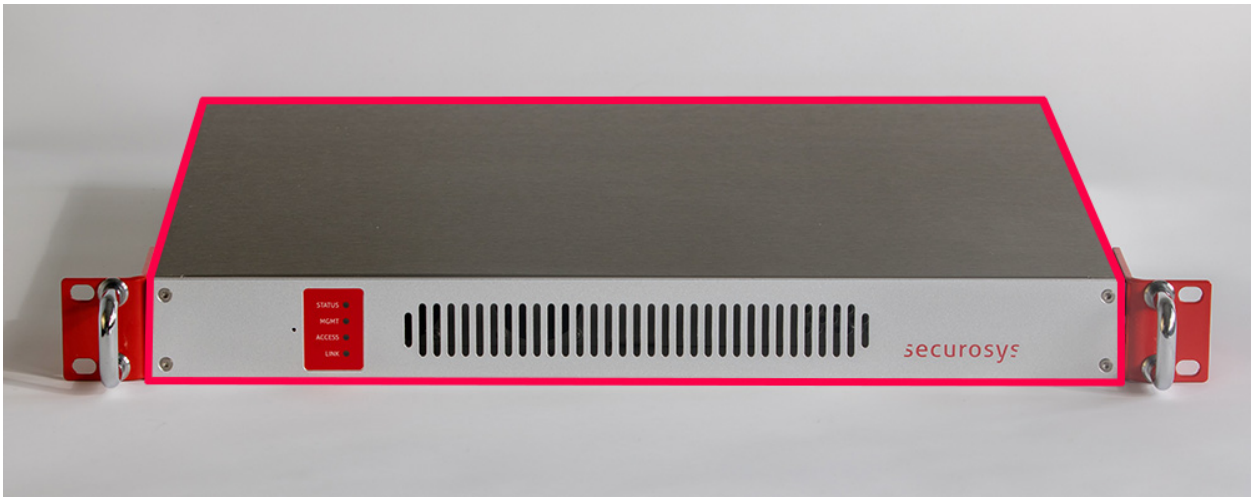


Figure 1: E-Module Front with cryptographic boundary in red

Figure 2: E-Module back with cryptographic boundary in red

Table 3 – Ports and Interfaces (E-Module)

Port	Description	Logical Interface Type
Ethernet	4x Ethernet for network connections	Control in | Data in | Data out | Status out
USB	USB port for backup/restore functionality	Control in | Data in | Data out | Status out
Console	RS-232 port for local console access	Control in | Data in | Status out
Power	AC power input	Power
LEDs	Status LEDs (STATUS, MGMT, ACCESS, LINK)	Status out

Figure 3: X-Module Front with cryptographic boundary in red

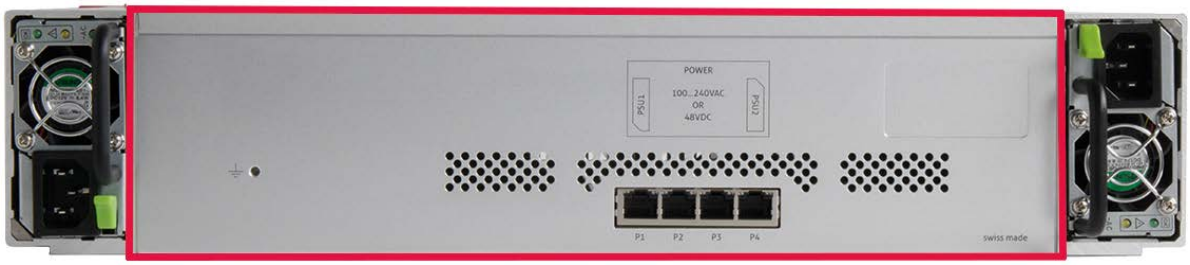


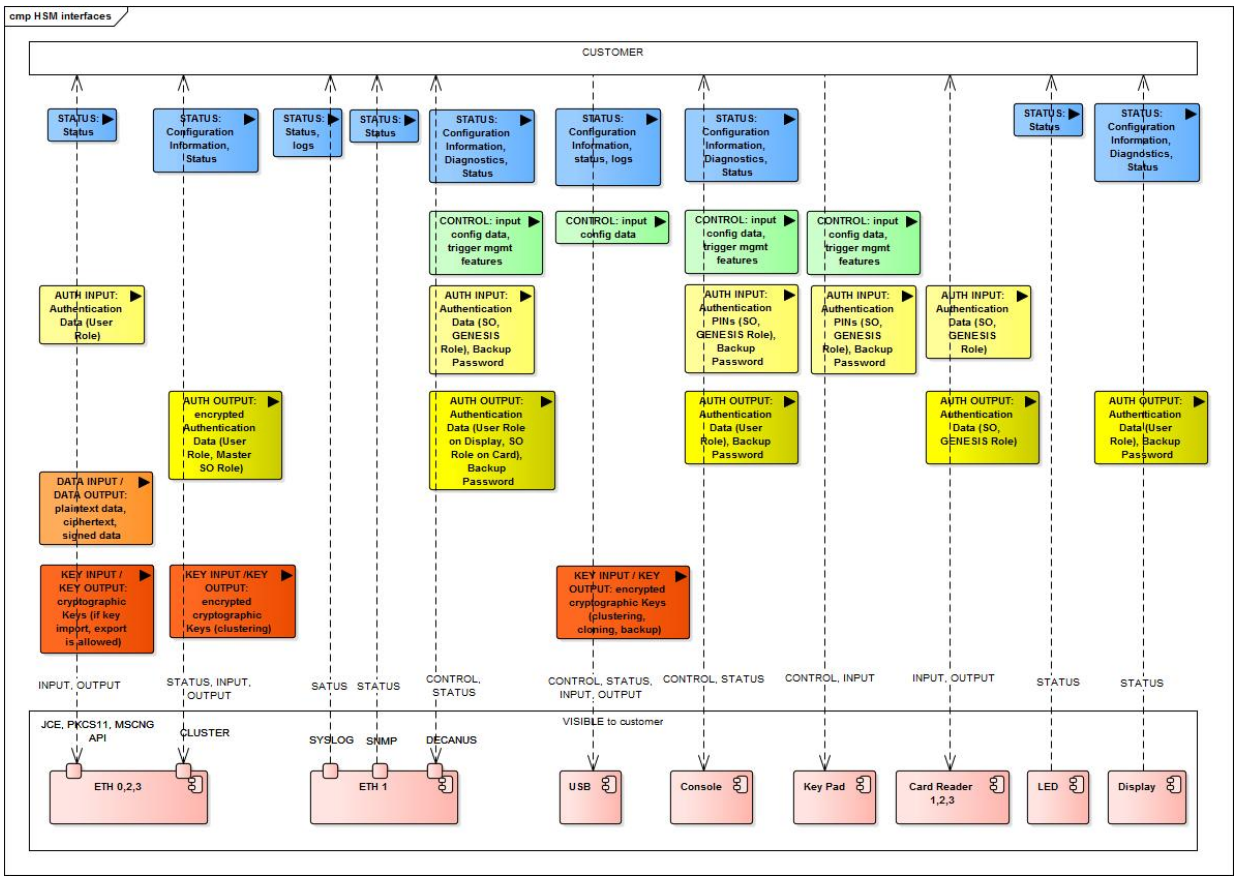
Figure 4: X-Module back with cryptographic boundary in red

Table 4 – Ports and Interfaces (X-Module)

Port	Description	Logical Interface Type
Ethernet	4x Ethernet for network connections	Control in | Data in | Data out | Status out
USB	USB port for backup/restore functionality	Control in | Data in | Data out | Status out
Console	RS-232 port for local console access	Control in | Status out | Data in
Card readers	3x Card readers for operator authentication	Data in | Data out
Power	2x DC power inputs (redundant)	Power
Front panel	Front panel LCD and front panel keypad	Control in | Status out
Status LEDs	Status LEDs (STATUS, MGMT, ACCESS, LINK)	Status out

1.1.1 Logical Interfaces Diagram

The following graphic displays all physical and logical interfaces in detail:



The distinction of control input and key input as well as status output and key output is essential within the USB interface. Not only do the clone, cluster, and backup files (key & data files) have different names than the config and log files (control & status files); the former category is also specifically encrypted and only recognized as Key input if decrypted correctly.

1.1.2 Excluded Hardware and Software Components

The following HW and SW components are excluded:

- Power supply (X-Module): The power supply is not considered security relevant. While the device depends on the supply of power, a faulty or rigged power supply cannot reveal any information from the device. The power supply for storing and processing CSPs is not taken directly from the PSU but is created with cascaded DC/DC converters with enough buffering capacity to avoid the risk of revealing information by side-channel monitoring, when performing key operations. In addition to this HW based attenuation of power spikes, the cryptographic cores are designed to consume constant power dependent only of the key length, but not the key content. Overvoltage, could potentially destroy some of the power input circuitry and render the device unusable. The tamper circuitry, however, will remain active, due to an independent, battery based, power feed.

2 Modes of Operation

The module implements both a FIPS-Approved mode and a non-FIPS-Approved mode. The mode can only be switched during device initial configuration, or after a Factory Reset has occurred. Please see Section 9 for more detailed instructions.

2.1 Indication of Mode & Status

The front panel status LEDs indicate the mode of operation: In FIPS mode, the Status LED is white.

The bar LED shows blue light alternating during the boot process. Once the device is operational, the status bar is all blue if the device is in factory state, all red if the device is tampered or a status indication as per PRIMUS HSM User Guide

When operational, the Status LED can be any of the following colors:

- WHITE: FIPS mode, nominal operation
- GREEN: Non-FIPS mode, nominal operation
- ORANGE or RED: Warning or error condition

Additionally, the mode is visible in the Configuration and Diagnostics menu tree and the console

>>>hsm_net_list_config fips_mode = true

See Primus HSM User Guide for how to access configuration and diagnostics through the front panel.

In FIPS mode, only FIPS-140-2 compliant algorithms and key sizes are available.

3 Cryptographic Functionality

The mode of operation (see previous section) determines the available cryptographic functionality.

3.1 FIPS-Approved Mode Algorithms

The Module implements the Approved and allowed cryptographic functions listed in the tables below.

Table 5 – Approved Cryptographic Functions Tested by CAVP

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CTR Key sizes: 128, 192, 256 bits	5485

Algorithm	Description	Cert #
AES-CMAC	[SP 800-38B] Functions: MAC Generation, MAC Verification Key sizes: 128, 192, 256 bits	5485
AES-GCM	[FIPS 197, SP 800-38D] Functions: Authenticated Encryption, Authenticated Decryption, GMAC Generation, GMAC Verification Key sizes: 128, 192, 256 bits IV-Construction: RBG-based Construction with 96-bit random field and 0-bit free field. A unique IV is constructed for each usage. For line encryption an IV is calculated for each direction (send/receive) and increased after each packet. Note: The IV is generated internally at its entirety randomly as per technique 2 of IG A.5.	5485
AES-KW	[SP 800-38F] Functions: Key Wrap, Key Unwrap Modes: KW, KWP Key sizes: 128, 192, 256	5485
DRBG	[SP 800-90A] HMAC DRBG with internal function SHA-512 CTR DRBG with internal function AES-256	2160
DSA	[FIPS 186-4] Functions: PQG Generation, Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	1412
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification, Public Key Validation Curves/Key sizes: P-224, P-256, P-384, P-521 (Strength: 112, 128, 192, 260)	1471
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	3643
KAS (FFC, ECC)	[SP 800-56Ar1] Parameter sets/Key sizes: FC, EB, EC, ED, EE Modes: dhStatic responder, Static Unified responder Scheme: SHA2 Note: Key establishment methodology provides between 112 and 256 bits of encryption strength	184
KDF	[SP 800-108] Modes: Counter, Feedback, Double Pipeline Iteration Mode PRFs: CMAC(AES-128/192/256), HMAC (SHA-1, 224, 256, 384, 512)	226

Algorithm	Description	Cert #
KTS (Symmetric)	[SP800-38F] Functions: Key Wrap, Key Unwrap Variants: 38D: AES-GCM (256 bits) 38F: AES-KW, AES-KWP Key Transport – Provides between 128 and 256 bits of encryption strength.	5485 (AES)
RSA	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PSS and PKCS1.5)] Functions: Key Pair Generation, Signature Generation, Signature Verification, Component Test Key sizes: 2048, 3072, 4096 bits Some RSA-4096 functions are listed here but not displayed on RSA Cert. #2946. These are vendor-affirmed, as CAVP does not provide testing for these functions.	2946
SHA	[FIPS 180-4, FIPS 202] Functions: Digital Signature Generation, Digital Signature Verification, component of HMAC and HMAC_DRBG, general hashing SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	4402 48 (SHA-3)
Triple-DES (TDES)	[SP 800-67] Functions: Decryption Modes: TECB, TCBC Key sizes: 3-key	2762

Table 6 – Approved Cryptographic Components Tested by CAVP (CVL)

Algorithm	Description	CVL Cert #
ECDSA SigGen Component	[FIPS 186-4] Curves/Key sizes: P-224, P-256, P-384, P-521	1941
KAS Component	[SP 800-56A Section 5.7.1.2 ECC CDH Primitive] Parameter sets/Key sizes: EB, EC, ED, EE	1938
RSA DP	[SP 800-56B] Key sizes: 2048 bits	1940
RSA SP	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PSS and PKCS1.5)] Key sizes: 2048 bits	1939

Table 7 – Approved Cryptographic Functions Tested with Vendor Affirmation

Algorithm	Description	IG Ref.
CKG	[SP800-133] Asymmetric Key Generation (SP800-133 §6) Symmetric Key Generation (SP800-133 §7: Direct output from DRBG)	IG D.12; Annex D

Algorithm	Description	IG Ref.
KTS (RSA)	[SP 800-56B] Functions: Key Wrap, Key Unwrap Key sizes: 2048, 3072, 4096 bits Key {Agreement | Transport} – Provides 112 to 150 bits of encryption strength. Wrap Methods: RSASVE, RSA-OAEP	IG D.4; Annex D

Table 8 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	[FIPS IG G.13] The NDRNG sole purpose is an entropy source for the DRBG built according to SP800-90A. The source's min-entropy is conservatively claimed at 0.66 bits per bit, although it assessed at 0.83 bits per bit
ECC operations with non-NIST curves.	[FIPS IG A.2] Elliptic Curve operations with non-NIST curves, as follows: Curve: • Brainpool 224r1, 256r1, 320r1, 384r1, 512r1 • Frp 256v1 • X9.62p239v1, v2, v3 • secp224k1, 256k1 Security Strength: • 112, 128, 160, 192, 256 • 128 • 119 • 112, 128

3.2 Non-FIPS Mode Algorithms

The module performs all algorithms from the FIPS-Approved mode, however no claim of compliance to the appropriate standard is made in the non-Approved mode.

In addition, the module performs the following non-Approved Cryptographic Functions in non-FIPS mode only:

- MD5
- Camelia
- SHA-1 (non-compliant) (for other operations than verification)
- DH with safe prime parameters
- CBC-MAC
- Securosys TRNG (NDRNG)
- Securosys RNG (AES-128 (non-compliant))
- Triple-DES encryption (non-compliant)

3.3 Keys, Passwords, and other CSPs

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 9 – Critical Security Parameters (CSPs)

CSP	Type	Description / Usage
Internal System CSPs		
KEK	AES-256-GCM AES-128-KW(P) AES-192-KW(P) AES-256-KW(P)	Protects the Keystore Key and the Card Keys
Keystore Key	AES-256-CBC	Protects all User Keys in Keystore
DRBG Seed	Misc.	Seed for DRBG
DRBG State	Misc.	Internal DRBG state (size varies based on DRBG)
Other System CSPs		
SO Card Keys	AES-ECB-128	Keys for encrypting/decrypting data on Security Officer smart cards.
SO PINs	Misc.	PINs for logging in as a Security Officer (8-12 characters, numerical)
Genesis PIN	8-Digit PIN	Randomly created by the HSM in production and is 8 digits and cannot be changed. It is used only for genesis authentication, backup operations, and factory reset operations.
Cluster Auth Keys	RSA-4096	Private keys used to establish a mutually-authenticated cluster session. (One for signing, one for key establishment.)
Cluster Session Keys	AES-256-GCM	Transports keys (KTS) and data within the HSM cluster.
Cloning RSA Key	RSA-4096	RSA private key for unwrapping the cloning AES key (KTS).
Cloning AES Key	AES-256-GCM	Encrypts or decrypts the cloning package.
Backup Key	AES-256-GCM	Encrypts or decrypts a backup of the module configuration.
User CSPs		
API DH Key	DH-2048	Ephemeral DH-2048 private key for establishing an API session (for User role).
API Initial Secret	Misc.	129-bit password for initial trust establishment to connect an API session, generated by the module using RBG
API Secret	Misc.	256-bit shared secret for establishing an API session, generated by the module using RBG
API Session Key	AES-256-GCM	Encrypts/decrypts between the module and the API. Unique IV per direction.
User Keys	Misc.	Keys of various types (AES, Triple-DES, HMAC, RSA, DSA, ECDSA, DH, ECDH), used by the User for various operations (encrypt data with AES key, verify data with HMAC key, etc.). Refer to Tables 5-8 for the detailed list of possible algorithm variants.

3.3.1 Input and output of Keys, Passwords and other CSPs

- User keys are only in- and outputted through the authenticated and encrypted user session (KTS). No plaintext import or export of User Keys is possible.
- Authentication data is plaintext inputted, if a console is used to enter PINs instead of entering the PINs directly on the device front panel UI.
- User keys are in- and outputted in AES256-GCM encrypted if a restore / backup is performed.
- The Backup key is split into three parts. The password part is outputted on the display or the console and needs to be inputted on the UI or console in the restore process. The second part is stored on the GN-card. The last is stored internal in the module.

No other Keys, Passwords or CSPs are input or output.[1]

The output of API Setup Password and Backup Password are part of services, which is authenticated by SO (2 operators). Therefore, the SO needs to be activated and the Service needs to be triggered.

Backup Password is split into 2 parts, of which part one is output, and entered in case of restore, on the UI display or console and a second part which is written onto the GN Card (virtual GN memory E-Series) and protected by the GN PIN. The input and output is on the UI, which is part of the cryptographic boundary or on the console, which is connected with the serial port with a directly attached cable and thus requires physical access to the device.

3.4 Public Keys

Table 10 – Public Keys

Key	Type	Description / Usage
API DH Public Keys	DH-2048	Ephemeral DH-2048 public key for establishing an API session (for User role).
FW Update Pub Key	RSA-4096	Validates signature of firmware update packages.
Cluster Auth Pub Keys	RSA-4096	Establishes a mutually-authenticated cluster session (KTS-RSA).
Clone Auth Pub Key	RSA-4096	Wraps the Cloning AES Key when creating a clone package (KTS-RSA).
Cloning RSA Key	RSA-4096	RSA public key for wrapping the cloning AES key (KTS).
Digital Seal	Misc.	128b value, system chosen random value at factory reset
User Public Keys	Misc.	Public keys of various types (RSA, DSA, ECDSA, DH, ECDH), used by the User for various operations (Verify signature with ECDSA, encrypt key with RSA, etc.).

[1] Each device has its own keystore key, even during clustering, cloning and backup/restore.

4 Roles, Authentication, and Services

4.1 Module Roles

The module supports four different roles: Genesis, Security Officer (SO), User, and Clustering. These are described below. All roles use identity-based authentication, and multiple operators can use the module concurrently. Authenticated sessions are cleared upon power cycle.

Items to note:

1. Authentication to the Security Officer role requires 2 operators as per the 4-eye-principle. When device is in operational state SO activation is required before Genesis activation for backup and restore operations. (see section 4.3).
2. The User role may access its services independently of SO and Genesis activation. For this role, here are no restrictions on concurrent operators.
3. Authentication methods are described in detail in the “Authentication Methods” section.
4. It is not possible for an operator to change roles.

Table 11 – Roles Overview

Role ID	Role Description	Authentication Type	Authentication Data
Genesis	Sets up the module. Performs factory reset.	Identity-based	PIN and Card
			PIN Only
Security Officer (SO)	Administrative role which manages the module.	Identity-based	PIN and Card
			PIN Only
User	Technical User. This role is access through the API and provides general cryptographic functionality.	Identity-based	Username and Setup Password
			Username and User Secret
Clustering	In a cluster, a clone HSM connects to the Master HSM to sync U and Data	Identity-based (machine-to-machine)	UID and RSA Signature

4.1.1 Genesis Role (G)

The Genesis role is used only for setting up the module. It can be accessed with a PIN* and Card (X variant), or with a PIN by itself (E variant). The Genesis role performs initialization functions such as Security Officer creation, KEK generation, and Keystore Key generation. If the module has already been initialized, the Genesis role can only be accessed by performing a factory reset.

4.1.2 Security Officer Role (SO)

The SO manages administrative tasks for the module, such as security configurations, firmware upgrading, identity creation for the SO and User roles, and cloning. It can be authenticated with a PIN and Card (X variant) or with a PIN by itself (E variant, or X variant if set up that way).

4.1.3 User Role (U)

The User role is accessed over the API (e.g., by business applications or clients) and serves to manage and use the User Keys. The User role may generate, load, and perform cryptographic operations with these keys.

User Keys, private, secret and public can only be accessed if the user is authenticated. This includes listing of available keys or any other operation with keys.

APIs are libraries with standardized interfaces such as PKCS#11, Java JCA/JCE, MS Crypto API.

4.1.4 Clustering Role (C)

Multiple instances of the module can establish a secure channel to perform clustering. When this occurs, modules authenticate to one another in the Clustering role.

4.2 Authentication Methods

4.2.1 Genesis Role Access

The Genesis role is identified by a unique Genesis card tied to the module. Therefore, the role is identity-based access controlled IBAC.

4.2.1.1 PIN and Card

This method is only supported for the X variants of the module. The operator inserts a Card and provides a PIN. The module retrieves and decrypts the correct PIN from the Card and compares it with the PIN entered by the operator. The PIN is 8-digits in length.

This method of authentication is impossible without possession of a valid Card. As such, false authentication would require a Card to be spoofed. Card integrity is provided by a 32-bit CRC across the internal data; both are stored encrypted with one of the Smart Card Keys. Successfully spoofing a Card would require the creation of "forged" ciphertext which, when decrypted, has a correct 32-bit CRC by random chance. The probability of this occurring for any given attempt is 2^{-32}, which is less than 1 in 1,000,000.

It would take at least one second for the module to reject an invalid Card. This limits Card spoofing to 60 attempts per minute. As such, the probability of spoofing a Card in one minute is $60*2^{-32}$, which is less than 1 in 100,000.

Note that the above estimates are a lower bound on difficulty, and do not include additional requirements for false authentication which are hard to quantify, such as spoofing a card with the correct UID, correct username, valid PIN, and other miscellaneous values; as well as actually guessing the correct PIN for a spoofed Card afterwards.

4.2.1.2 Pin Only

This method is similar to the PIN and Card method but only uses a PIN. It is available on the E variant by default and can also be configured on the X variant. False authentication requires guessing the PIN.

The PIN is an 8-digit number; as such, the chance of a random authentication for a minimum-length PIN is 10^{-8} or 1 in 100,000,000.

An operator can make four PIN entry attempts before being permanently locked out. As such, the probability of false authentication over any time interval is $4*10^{-8}$, which is less than 1 in 100,000.

4.2.2 Security Officer Role Authentication

The Security Officer is identified by Security Officer Name. Therefore, this Role is identity-based access controlled IBAC.

The Security Officer role uses the same authentication methods as the Genesis role, but with the following differences:

- The Security Officer PINs are CSPs, and can range from 8 to 12 digits in length.
- Two identities are required to authenticate to the Security Officer role, as per the Four Eye Principle.

4.2.3 User Role Authentication

The User role is identity-based access controlled (IBAC).

At creation, an identity belonging to this role is given a one-time password, the User Setup Password. It consists of 25 alphanumeric characters, each of which can be any of 36 values (A-Z, 0-9). As such, the probability of false authentication is 36^{-25}, which is less than 1 in 1,000,000. This password expires after its lifespan time which is three days by default, but can be configured by a security officer to be up to one year.

After the first-time use with the User Setup Password, a User Secret is established between the module and the operator. This is a random 256-bit value for machine-to-machine authentication. The probability of false authentication is 2^{-256}, which is less than 1 in 1,000,000.

For either case, it takes more than one millisecond to reject an incorrect value. As such, the probability of false authentication in a one-minute timespan is $60,000*36^{-25}$ or $60,000*2^{-256}$; both are less than 1 in 100,000.

In addition to power cycle events, this role also requires reauthentication 4 hours have passed or after 1GB of data.

4.2.4 Clustering Role Authentication

The clustering role is identity-based access controlled, IBAC.

Clustering peers are identified by UID and authenticated with an RSA-4096 signature. False authentication requires forging this signature, which would require at least 2^{128} computational operations. As such, false authentication is impossible over any time frame. After the initial authentication which takes one-minute, further authentications take approximately 2 seconds to complete, allowing for 30 attempts in the minute. As such the probability of false authentication in a one-minute timespan is 30 * 2^-128 chance (less than 1 in 100,000).

4.3 Services

All services implemented by the Module are listed in the table below. Each service description also describes all usage of CSPs by the service. The module's non-Approved services are identical to those defined in Table 12 and 13 below. However, non-Approved algorithms from Section 3.2 above can be used in lieu of Approved algorithms.

Table 12 – Authorized* Services

Service	Description	G	SO	U	C
Initialize HSM	Initialize the HSM from factory settings. Creates a new KEK, a new Keystore Key, a new "first identity" for the SO role, and a new Security Seal. Note that this can only be performed on first module access, or directly after performing the Factory Reset service.	X			
SO Login	Log in as the Security Officer (SO)		X		
SO Management	Create additional Security Officer identities, and designate a PIN.		X		
User Login	Log in as the User			X	
User Management	Create User, Delete User, Change Username, new User setup Password, new User Secret CSP: uses Card Keys for SO activation,		X		
Change Security Configurations	Configuration changes such as security policy, logging policy, user security policies. CSP: uses Card Keys for SO activation		X		

Service	Description	G	SO	U	C
Firmware Management	Firmware Update, Rollback CSP: uses Card Keys for SO activation, uses Firmware Update Key to verify integrity and decrypt Firmware		X		
Data Management	Create Keys, Delete Keys, import/export Keys, Use Keys for encryption, signing etc. via Ethernet Port, and access through Client Application, Business Application, or API CSP: uses KEK and keystore Key			X	
Cloning	Create a Clone, second HSM Device with same U and same Data as Master CSP: uses Card Keys for SO activation, creates Clone Key for Clone Data Transport protection, creates Cluster Authentication Key for clustering		X		
Clustering	Multiple HSM build a cluster. Clones log into Master to sync Data and U CSP: uses Cluster Authentication Key				X
Backup	Create an offline Backup File CSP: uses Card Keys for Genesis Activation (SO and Genesis cards are required)		X		
Restore	Restore Data, SO, U, C onto a new HSM device in initial State CSP: uses Card Keys for Genesis Activation		X		
Digital Seal	Display Seal; set new Seal without performing Factory Reset		X		
Factory Reset	Zeroizes all key data and CSP. Restores factory default configuration. Deletes all data, logs, user accounts (identities for the other roles), deletes KEK, sets new Digital Seal	X			
Export Logs to USB	Export all current logfiles to USB		X		
Show Security Status	User, SO, Cluster diagnostics		X		

*This table includes Genesis-role services, which require a PIN but are not considered authenticated in the usual sense.

Table 13 – Unauthenticated Services

Service	Description
Show Status	LED; some diagnostics, SNMP
Network configuration	Change Network Configuration
Reboot (Self-Test)	Self-Tests is automatically executing after every Reboot. Rebooting is triggered with no role authentication.
Emergency Erase	Deletes KEK, by concurrent long press on ERASE and ENTER button (X-Module), long press with paper clip (E-Module). The Status LED turns on red when process is complete. Works in power-off state.

Service	Description
Tamper Response	Attempts to access the internals of the module will trigger a tamper response that will zeroized all CSP's.

Tables 14-16 define the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- O = Output: The module outputs the CSP.
- E = Execute: The module performs an operation using the CSP.
- W = Write: The module writes the CSP using provided data. (Includes key exchange, but not random generation.)
- Z = Zeroize: The module zeroizes the CSP.

Table 14 – CSP Access Rights within Services (System CSPs)

Service	CSPs											
	SO Card Keys	SO PINs	Cluster Auth Keys	Cluster Session Keys	Cloning RSA Key	Cloning AES Key	Backup Key	KEK	Keystore Key	DRBG Seed	DRBG State	GN PIN
Initialize HSM	G		G		G		G	G	G	G	ZGE	
SO Login		E						E				
SO Management		OWZ						E			E	
User Login								E	E		E	
User Management								E	E			
Change Security Configurations											E	
Firmware Management											E	
Data Management								E	E		E	
Cloning					E	GEZ		E	OW[2]		E	
Clustering			E	GEZ				E	OW		E	
Backup							EO	E	O		E	E
Restore							EZ	E	W		E	
Digital Seal											E	
Factory Reset	Z	Z	Z	Z	Z	Z	Z	Z	Z	ZG	ZG	E
Export Logs to USB												
Show Security Status												
Show Status												
Network Configuration												
Reboot (Self-Test)				Z		Z				ZG	ZG	
Emergency Erase	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	
Tamper Response	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	

[2] Each device has its own keys, even when cloned or clustered.

Table 15 – CSP Access Rights within Services (User CSPs)

Service		CSPs			
	API DH Key	API Initial secret	API Secret	API Session Key	User Keys
Initialize HSM					
SO Login					
SO Management					
User Login	GEZ	GEOWZ	E	GEZ	
User Management		Z	WZ		
Change Security Configurations					
Firmware Management					
Data Management					GWOEZ
Cloning			OW		OW
Clustering			OW		OW
Backup			O		O
Restore			W		W
Digital Seal					
Factory Reset	Z		Z	Z	Z
Export Logs to USB					
Show Security Status					
Show Status					
Network Configuration					
Reboot (Self-Test)	Z			Z	
Emergency Erase	Z		Z	Z	Z

Table 16 – Public Key Access Rights within Services

Service			CSPs				
	FW Update Pub Key	Cluster Auth Pub Keys	Clone Auth Pub Key	Cloning RSA Key	API DH Public Keys	Digital seal	User Public Keys
Initialize HSM							
SO Login							
SO Management							
User Login					GEZ		
User Management							
Change Security Configurations							
Firmware Management	WE						
Data Management							GWOEZ
Cloning			GE	GE			OW
Clustering		GE					OW
Backup		O	O	O		O	O
Restore		W	W	W		W	W
Digital Seal						GO	
Factory Reset		Z	Z	Z	z	GZ	Z
Export Logs to USB							
Show Security Status							
Show Status							
Network Configuration							
Reboot (Self-Test)					Z		
Emergency Erase		Z	Z	Z	Z	Z	Z
Tamper Response		Z	Z	Z	Z	Z	Z

5 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up, the Module performs the self-tests described in Table 17 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the error state.

The system uses simple memory compare to test the value of a test against its expected value. In cases where the comparison operation could be used for side channel attacks, the memory compare function is expanded in a way to compare all bytes instead of just until the first mismatch.

Only after successful self-test and power up, the Ethernet goes up and the HSM is available to the User.

There are no user callable self-test. The user may trigger a reboot to perform the start-up self-tests.

Table 17 – Power Up Self-tests

Test Target	Description
AES	KATs: Encryption, Decryption Modes: ECB, CTR, GCM/GMAC Key sizes: 256 bits
DRBG	KATs: HMAC DRBG KATs: CTR DRBG
DSA	PCT: Signature Generation, Signature Verification Key sizes: 2048 bits w/SHA-224
ECDSA	PCT: Signature Generation, Signature Verification Curves/Key sizes: P-521 w/SHA-384
HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
KBKDF	KAT: SP800-108 KDF KAT PRFs: HMAC, CMAC Modes: Counter, Feedback, Double-Pipeline Iteration
RSA-SP	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
RSA-PKCS	KAT: Signature Generation, Signature Verification Key size: 2048 bits, PKCS#1 v1.5 with SHA-256
SHA	KATs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
TDES	KATs: Decryption Modes: EBC Key sizes: 3-key
RSA-DP	KATs: Encryption, Decryption Key sizes: 2048 bits
Key Transport Using RSA	PCT Encryption, Decryption Key sizes: 3072 bits, OAEP with SHA256
Firmware integrity	Calculate a Hash Value over the entire firmware and compare it to the value that was calculated during the last firmware update, SHA512

Table 18 – Conditional Self-tests

(performed if certain conditions happen. e.g. create new pki key pair)

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG. DRBG tests that previous value is not same as next value (stuck fault test) DRBG 11.3 Health checks per SP 800-90A
DSA	DSA Pairwise Consistency Test performed on every DSA key pair generation. DSA Pairwise Consistency Test performed on every DSA signature calculation.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation. ECDSA Pairwise Consistency Test performed on every ECDSA signature calculation.
ECDH	ECDH tests if public point is on curve on every ECDH key pair generation.
DH	DH tests if public key is calculated correctly within parameters on every DH key pair generation.
NDRNG	Performed continuously per SP 800-90B Section 4.4.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation. RSA Pairwise Consistency Test performed on every RSA signature calculation.
Firmware update integrity	RSA 4096 digital signature is validated during firmware load.
Manual Key Entry Test	Confirms the key components entered to decrypt the backup file are correct

Table 19 – Critical Function Tests

Test Target	Description
FPGA self-tests	Check if Software and Hardware Implementation result in the same output. Executed during startup
Memory Test	Test if Memory size Is correct and memory has no errors
Flash-Test	Test if size, access, formatting and type of the inserted flash disc is correct.
RSA signature	PCT: Verify each RSA signature after signature generation.

6 Physical Security Policy

6.1 Tamper Seal Overview

Figure 5: E Variant Tamper-Evident Seal Locations (Top, Back) (Red Arrows)

Figure 6: Tamper-evident label (1) E-Module front

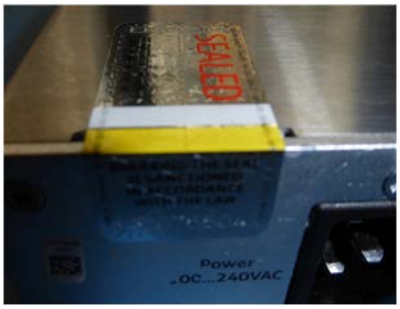


Figure 7: Tamper-evident label (2) E-Module back

Figure 8: X Variant Tamper-Evident Seal Location (Top, Back) (Red Arrow)

Figure 9: Tamper-evident label X-Module back

The modules are equipped with two (2) tamper-evident seals on E-Series or one tamper-evident seal on X-Series and a tamper-response mechanism which will zeroize all keys in the event of a physical breach.

The tamper-evident seals are factory mounted as shown on the pictures above.

The operator must check the seals and LED alerts regularly (see below).

Thorough inspection of the device is required if any of the following conditions of the seals applies

- white and yellow stripes are missing
- white and yellow stripes have changed color

In these cases carefully check the device according to the “Physical Security Inspection Guidelines” as this may indicate an attempted intrusion.

Figure 10: Tamper-evident label showing signs of tamper (“void” imprint, blue color strip from heat)

6.2 Inspection Guidelines

Table 20 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Housing	1 month to 1 year	Check that there are no signs of attempted intrusion, such as holes, dents and scratches.
Tamper LEDs	1 month to 1 year	Apply power and examine the front panel LEDs. In the event of a tamper, all four LEDs will be red.
Digital Seal	Initial setup after factory reset	Check against provided seal on shipping documents. In case of resealing write down new seal and check against this seal.
Physical Tamper seal	1 month to 1 year	Inspect the seal and ensure it is not ruptured or missing, it does not display “void” on any part of the label surface.

If tamper is detected do not continue to use device until you have asserted the device to be free of any unwanted circuits and is running genuine firmware.

In case tamper was indicated by tamper LEDs, you may want to export logs before the factory reset to find out about time and possible reason of the tamper response. All key information has been zeroized when the tamper response was triggered. You will have to do a factory reset, before device can be re-setup again. If in doubt about integrity of device return it to the factory for inspection.

In case of physical tamper evidence, carefully inspect the integrity of the device. If in doubt return the device to the factory for inspection. Do a factory reset to completely wipe all information including configuration from the device, before shipping.

The table below lists the physical security alerts the module provides for tilt, digital seal tamper, environmental conditions (non-critical), and movement.

Table 21 – Additional Physical Security Alerts

Physical Security Mechanism	Inspection/Test Guidance Details
Tilt alert	Check who has moved the device or what has caused the movement, such as work on the rack. Check for signs of attempted intrusion.
Digital Seal	The 25-character digital seal randomizes whenever a factory reset has occurred. The operator should check the digital seal if an unauthorized factory reset is suspected.
Non-critical alert	Apply power and examine the “STATUS” LED. If this LED is red, but the other LEDs are not red, a non-critical alert has been logged. The alert can be cleared by the SO.
Movement Sensor	A “tilt” warnings is logged in operation if lots of movement is detected. The security of the physical environment should be checked.

7 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

8 Mitigation of Other Attacks

The module has environmental monitors for temperature, temperature rate-of-chance (ROC), movement, and fan blockage. Alerts created by these monitors are logged, and some trigger a tamper response.

The module also mitigates against side-channel attacks, power analysis, and timing analysis.

Attack	Mitigation	Logging	Tamper
Rapid change of temperature, such as cold spray on the PCB, or freezing with N or CO2	Monitoring (also when powered off)	After event	yes
Temperature grossly outside specified range.	Monitoring (also when powered off)	Yes, After event (if power off)	yes
Fan blocked by probe (the probe will end on solid wall covering the PCB)	Monitoring	yes	no
Timing attack on crypto	Constant time dependent on key size.	no	no
Power analysis	Power design, constant power algorithm	no	no
Fault injection	Reverse operation	yes, operation fails	no

9 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The module provides 4 distinct operator roles: Genesis, Security Officer (SO), User, and Clustering
2. The module provides identity-based authentication for all roles.
3. The module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The operator can command the module to perform the power up self-tests by cycling power the module.
6. Power up self-tests do not require any operator action.
7. Data output is inhibited during self-tests and error states. Data output is logically disconnected from all processes performing key generation and zeroization.
8. Status information does not contain CSPs or any other sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module supports concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module uses smart cards for entry/output of data.
13. The module uses split knowledge to enter or output plaintext keys (backup key).
14. The module does not support the update of the logical serial number or vendor ID.
15. The module can be cloned only from a master device. Cloning from existing clones is not possible. Elevating a clone to a master role, requires SO role of original master.
16. The initial secret for logging in is valid for a limited period time period. This is defaulted to 3 days. After this time logging is not possible and a new initial secret has to be generated.
17. Logged-in sessions are valid for maximum of 4 hours or 2GB of data, if a session still exists after these limits it is terminated regardless of the state currently of open transactions. The module informs the connected clients after 2 hours, 1GB to renew its session. This implies, that no single transaction should be planned taking more than 2 hours or 1GB of data to complete. The renewed session can exist in parallel to the old session.
18. SO role times out after 1 hour at the latest, regardless of the presence of the credential (smartcard). A reactivation will be required.
19. The following steps shall be taken during initial configuration of the device in order to place it in FIPS approved mode (from Quick Start Guide):
    a. Power-up device in factory state: 4 steady blue LEDs
    b. Start setup wizard
        b.i. On front panel UI select: LOGIN/SETUP/WIZARD
        b.ii. Or type on console: >hsm_initial_wizard
    c. When prompted to select “NORMAL MODE” answer NO, when prompted for “FIPS MODE” answer YES
    d. Finish the wizard which guides through generation of KEK, security officers and initial user partition.
    e. When done, check WHITE status LED for indication of active FIPS mode

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 22 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

Table 23 – Acronyms and Definitions

Acronym	Definition
KEK	Key encryption Key
SO	Security Officer
UID	Unique Identifier
E-Series	Devices with model designators E followed by a performance number, such as E20, E60, E150
X-Series	Devices with model designators X followed by a performance number, such as X200, X400, X700, X1000
G	Genesis role, the role to initially setup the device and generate the SO role