RigSec Technology Limited

RIGFORT Pro Blockchain HSM

FIPS 140-3 Non-Proprietary Security Policy



Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Table of Contents

1 General 6
1.1 Overview 6
1.2 Security Levels 6
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 11
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 14
2.8 RBG and Entropy 14
2.9 Key Generation 14
2.10 Key Establishment 15
2.11 Industry Protocols 15
3 Cryptographic Module Interfaces 16
3.1 Ports and Interfaces 16
3.2 Trusted Channel Specification 16
4 Roles, Services, and Authentication 17
4.1 Authentication Methods 17
4.2 Roles 18
4.3 Approved Services 18
4.4 Non-Approved Services 31
4.5 External Software/Firmware Loaded 32
5 Software/Firmware Security 32
5.1 Integrity Techniques 32
5.2 Initiate on Demand 33
6 Operational Environment 34
6.1 Operational Environment Type and Requirements 34
7 Physical Security 35
7.1 Mechanisms and Actions Required 35

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

7.2 User Placed Tamper Seals 35
7.5 EFP/EFT Information 38
8 Non-Invasive Security 39
8.1 Mitigation Techniques 39
9 Sensitive Security Parameters Management 40
9.1 Storage Areas 40
9.2 SSP Input-Output Methods 40
9.3 SSP Zeroization Methods 40
9.4 SSPs 41
10 Self-Tests 45
10.1 Pre-Operational Self-Tests 45
10.2 Conditional Self-Tests 45
10.3 Periodic Self-Test Information 47
10.4 Error States 49
10.5 Operator Initiation of Self-Tests 49
11 Life-Cycle Assurance 50
11.1 Installation, Initialization, and Startup Procedures 50
11.2 Administrator Guidance 50
11.3 Non-Administrator Guidance 53
11.4 Rules of Operation 53
11.5 End of Life 54
12 Mitigation of Other Attacks 55
12.1 Attack List 55

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 9
Table 3: Modes List and Description 9
Table 4: Split Knowledge Procedures 11
Table 5: Approved Algorithms 12
Table 6: Vendor-Affirmed Algorithms 12
Table 7: Non-Approved, Not Allowed Algorithms 12
Table 8: Security Function Implementations 14
Table 9: Entropy Certificates 14
Table 10: Entropy Sources 14
Table 11: Ports and Interfaces 16
Table 12: Authentication Methods 18
Table 13: Roles 18
Table 14: Approved Services 31
Table 15: Non-Approved Services 32
Table 16: Mechanisms and Actions Required 35
Table 17: Tamper Seal Placement 35
Table 18: EFP/EFT Information 38
Table 19: Storage Areas 40
Table 20: SSP Input-Output Methods 40
Table 21: SSP Zeroization Methods 41
Table 22: SSP Table 1 42
Table 23: SSP Table 2 44
Table 24: Pre-Operational Self-Tests 45
Table 25: Conditional Self-Tests 47
Table 26: Pre-Operational Periodic Information 48
Table 27: Conditional Periodic Information 48
Table 28: Error States 49

List of Figures

Figure 1 – Front of RIGFORT Pro Blockchain HSM 7
Figure 2 – Back of RIGFORT Pro Blockchain HSM 7
Figure 3 - Right Side of RIGFORT Pro Blockchain HSM 7
Figure 4 - Left Side of RIGFORT Pro Blockchain HSM 7
Figure 5 - Manufacturer Label Sticker of the Module 7
Figure 6 - Cryptographic Boundary Block Diagram 8
Figure 7 – Management Console - Unknown Mode during Initialization 10
Figure 8 - Management Console - Approved Mode 10
Figure 9 - Management Console - Non-Approved 11
Figure 10 - Module Seal Location (Top) 36
Figure 11 - Module Seal Location (Bottom) 37
Figure 12 - Module Seal Location (Left Side) 37
Figure 13 - Module Seal Location (Right Side) 38
Figure 14 - Choose COM Port 51
Figure 15 - Add MNG 51
Figure 16 - Create DMK 52

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Figure 17 - Set Mode of Operation 52
Figure 18 - Restore DMK 53

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

1 General

1.1 Overview

This document defines the Security Policy for the RIGFORT Pro Blockchain HSM, hereafter denoted the Module. The Module is a multiple-chip standalone cryptographic module. It is a security module that supports the encryption algorithm approved by FIPS 140-3 and with physical security protection measures, key management mechanisms, and security features to provide secured and applicable cryptographic services for customer systems. Specifically, the security features include key wrapping, message authentication code (MAC), message digest, data encryption and decryption, digital signature generation and verification, etc.

1.2 Security Levels

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	3

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module is a hardware cryptographic module. The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated Data Encryption Cryptographic implementation. The Module is intended to be used in customer systems requiring security features include key wrapping, message authentication code (MAC), message digest, data encryption and decryption, digital signature generation and verification, etc.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

The physical form of the Module is depicted in Figure 2. The Module is a multiple-chip standalone embodiment. The cryptographic boundary is defined as an entire hardware module, and its physical boundary is defined by the hard metal chassis that surrounds all hardware and firmware of the module. The physical dimensions of the module are 482mm*45.5mm*360mm (W*H*L).



Figure 1 – Front of RIGFORT Pro Blockchain HSM



Figure 2 – Back of RIGFORT Pro Blockchain HSM



Figure 3 - Right Side of RIGFORT Pro Blockchain HSM

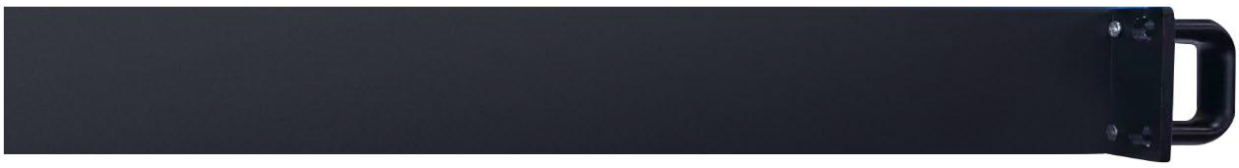


Figure 4 - Left Side of RIGFORT Pro Blockchain HSM



Figure 5 - Manufacturer Label Sticker of the Module

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

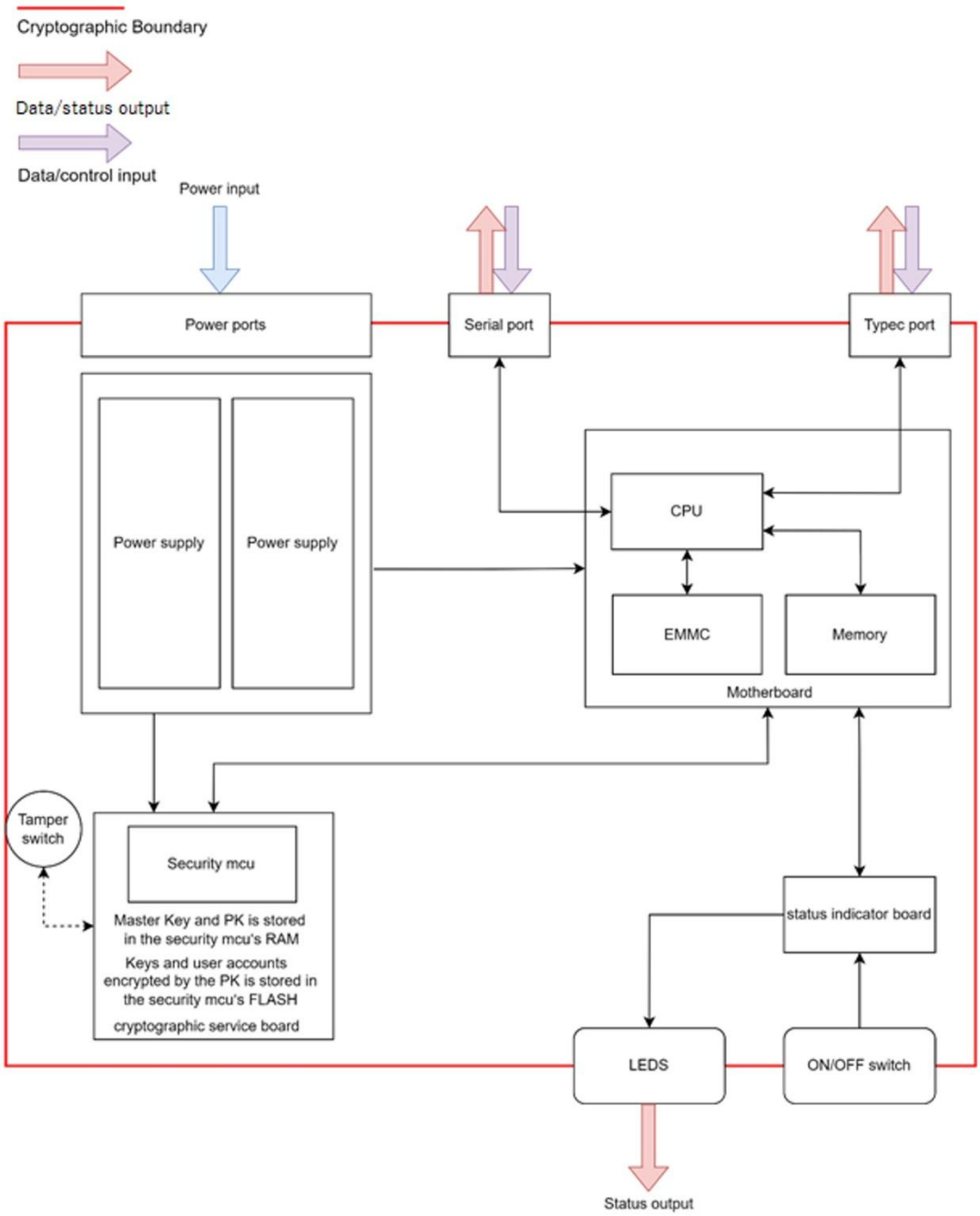


Figure 6 - Cryptographic Boundary Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

RigSec Data Encryption cryptographic module is tested on the following operational environment.

Tested Module Identification – Hardware:

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
RIGFORT Pro Blockchain HSM	3.4.0	1.4.0	ARM Cortex-A9 / ARM Cortex-M	hard metal 1U chassis

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

No components were excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved Mode	Normal Operation with only approved services and security functions available	Approved	See HSM mode in Figure 8
Non-Approved Mode	Non-approved security functions are available. In the Non-Approved Mode, both Non-Approved and Approved algorithms can be configured.	Non-Approved	See HSM mode in Figure 9

Table 3: Modes List and Description

The Module supports both an Approved and non-Approved mode of operation. To verify that the Module is in the Approved mode of operation, the operation mode indicator can be seen on the left side of the management software or check the operation mode status via the menu: Tools → Display Module Status.

The Approved mode of operation is configured at reception of the Module by the CO role who implements the instructions in Section 11.2 Cryptographic Officer Guidance. The operation mode can be selected at initialization through the management software and cannot be changed once selected unless restored to factory settings

The non-Approved mode of operation is configured at reception of the Module by the CO role who implements the instructions in Section 11.2 Cryptographic Officer Guidance. The operation mode can be selected at initialization through the management software and cannot be changed once selected unless restored to factory settings.

Mode Change Instructions and Status:

In order to switch modes, the CO must perform a reset of the module by selecting from Management Console menu: Tools → Reset HSM, which zeroizes all the SSPs.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

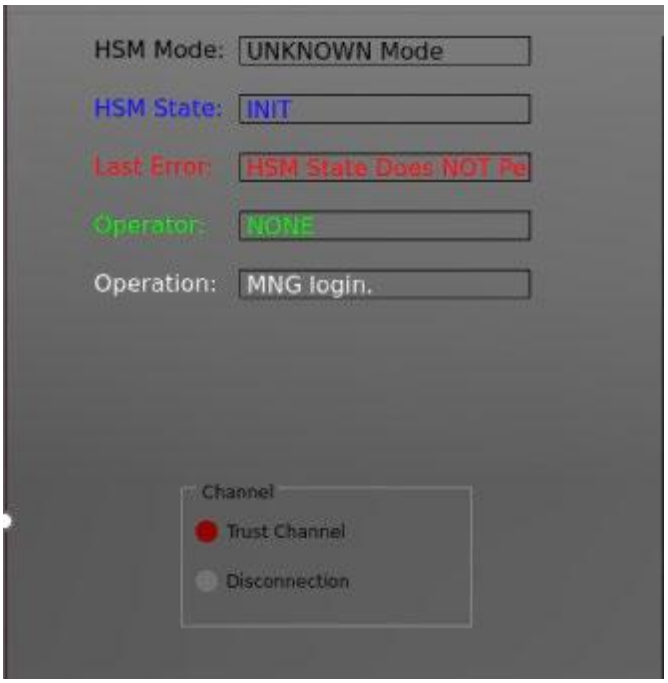


Figure 7 – Management Console - Unknown Mode during Initialization

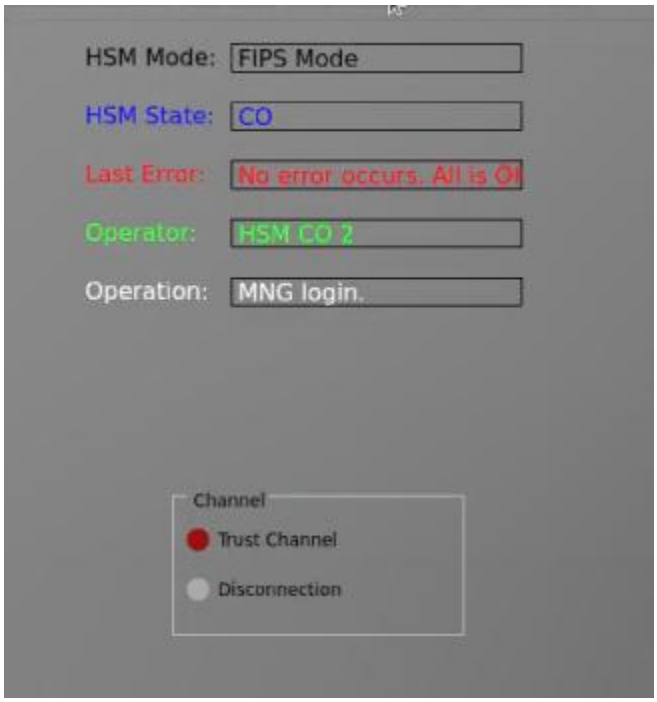


Figure 8 - Management Console - Approved Mode

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

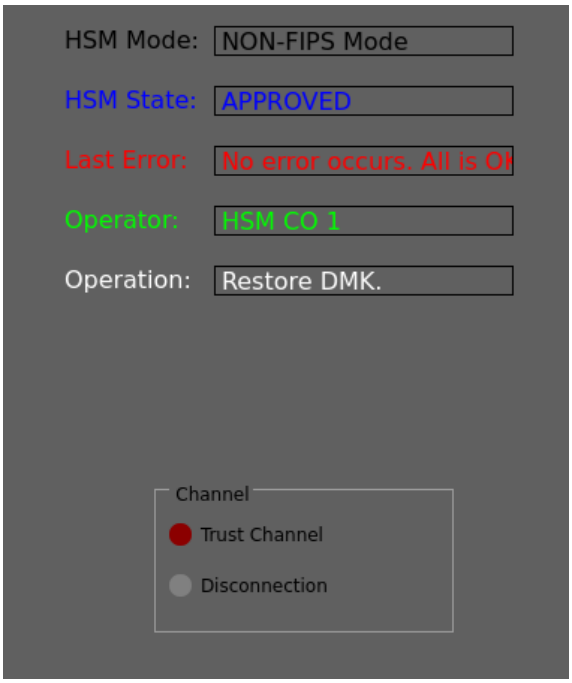


Figure 9 - Management Console - Non-Approved

Split Knowledge Procedures

Algorithm	Caveat	Description
Shamir Secrets Share	Split Knowledge Procedures: Polynomial method used only for secret-sharing. Note: As per NISTIR 8214, Section 6.2, implementation of Shamir Secret Sharing is used to satisfy section 7.9.5 of the FIPS 140-3 standard which defines security requirements for split-knowledge procedures.	The secret sharing algorithm divides the secret and shares the secret among "n" participants more than specific t participants can calculate or recover the secret, and less than t participants cannot get it.

Table 4: Split Knowledge Procedures

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2750	-	SP 800-38A
AES-ECB	A2750	-	SP 800-38A
ECDSA KeyGen (FIPS186-4)	A2750	-	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A2750	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A2750	-	FIPS 186-4
Hash DRBG	A2750	-	SP 800-90A Rev. 1
HMAC-SHA2-256	A2750	-	FIPS 198-1

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Algorithm	CAVP Cert	Properties	Reference
KDF SP800-108	A2750	-	SP 800-108 Rev. 1
KTS-IFC	A2750	-	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-4)	A2750	-	FIPS 186-4
RSA SigGen (FIPS186-4)	A2750	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A2750	-	FIPS 186-4
SHA2-256	A2749	-	FIPS 180-4
SHA2-256	A2750	-	FIPS 180-4

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG1	Key Type:Asymmetric and Symmetric	N/A	SP800-133rev2 Section 4 Example 1 and IG D.H

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
ECDSA_secp256k1	Signature Algorithms of Blockchain
ed25519	Signature Algorithms of Blockchain
ripmd160	Message Digest algorithm of Blockchain
sha3-256 (FIPS 202)	Message Digest algorithm of Blockchain
SM2	Chinese Elliptic Curve Digital Signature Algorithm (asymmetric encryption/decryption, key agreement, signature generation/verification)
SM3	Chinese Message Digest Algorithm (message digest)
SM4	Chinese Block Cipher Symmetric Algorithm (symmetric encryption/decryption)
sr25519	Signature Algorithms of Blockchain

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below.

Name	Type	Description	Properties	Algorithms
Symmetric Encryption / Decryption	BC-UnAuthDecrypt BC-UnAuthEncrypt	Symmetric Encryption / Decryption		AES-CBC: (A2750) AES-ECB: (A2750)
DRBG	DRBG	DRBG		Hash DRBG: (A2750)
Asymmetric Key Generation	AsymKeyPair-KeyGen	Asymmetric Key Generation		ECDSA KeyGen (FIPS186-4): (A2750) RSA KeyGen (FIPS186-4): (A2750)
Signature Generation	DigSig-SigGen	Signature Generation		ECDSA SigGen (FIPS186-4): (A2750) RSA SigGen (FIPS186-4): (A2750) SHA2-256: (A2750) Hash DRBG: (A2750)
Signature Verification	DigSig-SigVer	Signature Verification		ECDSA SigVer (FIPS186-4): (A2750) RSA SigVer (FIPS186-4): (A2750) SHA2-256: (A2750)
Message Digest	SHA	Message Digest		SHA2-256: (A2749, A2750)
KTS1	KTS-Decap KTS-Encap	Key Transport	IG D.G:Approved Key confirmation:yes Caveat: Key establishment methodology provides 112 bits of security strength	KTS-IFC: (A2750)
KTS2	KTS-Unwrap KTS-Wrap	Key Transport	IG D.G:Approved Caveat: Key establishment methodology provides	AES-CBC: (A2750) HMAC-SHA2-256: (A2750)

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Type	Description	Properties	Algorithms
			256 bits of security strength	SHA2-256: (A2750)
Key Derivation from DMK	KBKDF	Key Derivation	Publication:NIST SP 800-108 Rev. 1	HMAC-SHA2-256: (A2750) KDF SP800-108: (A2750)
Symmetric Key Generation	CKG	Symmetric Key Generation		CKG1: ()
Entropy	ENT-ESV ENT-Cond	Physical Entropy Source		SHA2-256: (A2750)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

2.8 RBG and Entropy

Cert Number	Vendor Name
E17	RigSec Technology Limited

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
RigSec HSM AS578 Cryptographic Library	Physical	ARM Cortex-M	256	Full entropy	SHA2-256 (Cert. #A2750)

Table 10: Entropy Sources

The module implements Hash DRBG with SHA2-256, according to SP 800-90A Rev. 1, with prediction resistance using SHA2-256 (A2750) as a conditioning component. The module uses an SP 800-90B-compliant entropy source as specified above. This entropy source is located within the cryptographic boundary of the module.

The module obtains 256 bits from the entropy source to seed the DRBG, and this is sufficient to provide a DRBG with 256 bits of security strength. The largest key strength generated by the module is 256 bits.

2.9 Key Generation

The module generates Keys and SSPs in accordance with FIPS 140-3 IG D.H. The cryptographic module performs Cryptographic Key Generation (CKG) for symmetric and asymmetric keys as per [SP 800-133r2] Section 4, Example 1 (vendor affirmed), compliant with [FIPS186-4], and using DRBG compliant with [SP

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

800-90Ar1]. A seed (the random value) used in asymmetric key generation is obtained from [SP 800-90Ar1] DRBG. The key generation service for RSA and EC key pairs as well as the [SP 800-90Ar1] DRBG have been ACVT tested with algorithm certificates.

The module also implements the following key derivation functions:

- KBKDF Key Derivation according to [SP 800-108r1] to derive symmetric keys. The module supports Counter mode with HMAC-SHA2-256 as the pseudorandom function (PRF).

2.10 Key Establishment

Key Agreement Information

N/A - The module does not implement a Key Agreement method

Key Transport Information

The module implements the following Approved/allowed key transport methods specified in FIPS 140-3 IG D.G:

- RSA key encapsulation/decapsulation

2.11 Industry Protocols

N/A - No parts of the supported Industry protocols have been tested by the CAVP and CMVP.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Power Ports (2)	Power	Connect the module to the power outlet via the redundant power supply
Power button	Control Input	Electrical signal passes through
LEDs	Status Output	Display the working status of the module through different combinations
Serial Port (RS-232)	Data Input Data Output Control Input Status Output	Connected to the management computer to provide management services
Type-c Port	Data Input Data Output Control Input Status Output	Connected to the communication computer to provide cryptographic services for user applications

Table 11: Ports and Interfaces

* Control Output is not available in this module

3.2 Trusted Channel Specification

Trusted Channel

Directly connected cable through a Serial Port (RS-232) from the Management Console to the module.

Description

The Trusted Channel must be setup per section 11.1 Secure Installation, Initialization, Startup and Operation of the Module.

The Management Console connects directly to module via a serial port (RS-232). To protect the plaintext CSPs, the physical ports used for the trusted channel are physically separated from all other ports and will be under the direct supervision of the CO.

A status indicator through the management console is provided when the trusted channel is in use or not. See the Channel section of Figure 8

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
2048-bit RSA key pair.	The CO is authenticated by UKEY_ID and verified using 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.	RSA SigVer (FIPS186-4) (A2750)	112 bits strength of the authentication method, the probability of a successful random attempt is 1 in 2^112	Each RSA Signature Verification authentication attempt takes at least 60ms. So, the number of attempts for one minute cannot exceed 1000. The USB token corresponding to CO allows six (6) consecutive failed attempts before locking. After a successful attempt, the number of failures will be reset to zero. After six (6) consecutive failed attempts, the USB token cannot be used.
Password	The User role sends assigned user name to HSM, and HSM utilizes a challenge-response mechanism for user role authentication. The user's password is protected with a cryptographic hash (SHA256 message digest).	(8) ASCII printable characters and there are 95 ASCII printable characters	Since the password length is eight (8) ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in {(10)*(26^2)*(95^5)} (at least one number, one uppercase, one lowercase).	Within the consecutive PIN code error cycle (24 hours), if the user enters the wrong PIN code 6 times, the HSM will be locked for 60 minutes. After 60 minutes, HSM will clear the number of consecutive PIN code errors, and the consecutive PIN code error cycle will end and be cleared.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Table 12: Authentication Methods

The module uses identity-based authentication to identify and verify users of the module. For roles as the manager are identified by UKEY_ID and verified using a challenge-response mechanism based on a 2048-bit RSA key pair, and user are identified by username and verified using a challenge-response mechanism based on sha2-256. The public key is stored in the module in plaintext, and the private key is stored in the user's USB token.

The module ensures that there is no visible display of the authentication data.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Identity	Crypto-Officer	2048-bit RSA key pair.
User	Identity	User	Password

Table 13: Roles

The Module supports two distinct operator roles, User (User Application external entity) and Cryptographic Officer (CO) (Manager). The cryptographic module enforces the separation of roles using identity-based authentication. Re-authentication is enforced when changing roles. If the CO logs in while the user is logged in, the user will be automatically logged out.
Table – Roles lists all operator roles supported by the Module and their related services. In addition, the Module supports services which does not require to be authenticated, listed UA in Table - Roles.

The Module does not support a maintenance role and bypass capability. The Module does not support concurrent operators. Previous authentications will be cleared on power cycle. The physical security mechanisms employed by the module protect the SSPs from unauthorized disclosure, modification, and substitution via physical intrusions.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Create DMK	Create a DMK, use the Shamir Secrets Share algorithm to divide the DMK into 3 compone	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Generated DMK.	DRBG Key Derivation from DMK	CO - Device Master Key (DMK): G,R,E - Protection

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	nt keys, and back up these three keys to three external USB tokens respectively. Then derive PK through DMK					Key (PK): G
Restore DMK	Import 2 component keys stored in the USB token into the cryptographic module, synthesize the DMK through the Shamir Secrets Share algorithm, and then derive the PK through the DMK.	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	DMK restored	Key Derivation from DMK Symmetric Encryption / Decryption	CO - Device Master Key (DMK): W,E - Protection Key (PK): G
Add MNG	Write ID and RSA public key from management console to	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	The MNG account is created. Success/failure status	Symmetric Encryption / Decryption Signature	CO - CO RSA-pub Key: W

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the module.				Verification	
MNG Login	The cryptographic module authenticates the manager's identity	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Password	Login CO role	DRBG Signature Verification	CO - CO RSA-pub Key: E
MNG Logout	Manager logout	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Logout CO role	Signature Verification	CO
Add User Application	Create a user, write the user name and default password to module, and store it with PK protection.	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	The User Application user account is created. Success/failure status	Symmetric Encryption / Decryption Signature Verification Message Digest	CO - Protection Key (PK): E - User Password: W
Delete User Application	Delete user's information	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	The User Application user account is deleted. Success/failure status	Symmetric Encryption / Decryption Signature Verification	CO - User Password: Z
Reset User Application password	Modify user password, write the new default password to the	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	The User Application default password. Success/failure status	Symmetric Encryption / Decryption Signature	CO - Protection Key (PK): E - User

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	module, and store it with PK protection.				Verification Message Digest	Password: W,Z
List User Application	List all currently existing User Application users	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	User list	None	CO
Create User Key	Create user key, and store it with PK protection.	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Creates AES/HMAC/HASH/RSA 2048/ECDSA-P256 keys for the user	Asymmetric Key Generation Symmetric Key Generation	CO - User AES Key: G - User ECDSA Public Key: G - User ECDSA Private Key: G - User RSA Private Key: G - Protection Key (PK): E
Remove User Key	Remove user key	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Deletes User Keys	Symmetric Encryption / Decryption Asymmetric Key Generation	CO - User AES Key: Z - User ECDSA Public Key: Z - User ECDS

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						A Private Key: Z - User RSA Private Key: Z - User RSA Public Key: Z - Protection Key (PK): E
List User Key	List user key types	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	User key list	Symmetric Encryption / Decryption Signature Verification Message Digest	CO
Key Derivation Function	Perform Key Derivation using NIST SP800-108 KDF in CTR mode	Approved mode; ERROR_OK; ERROR_HSM_STATE;	DMK	PK	Symmetric Encryption / Decryption Key Derivation from DMK	CO - Device Master Key (DMK): R,E - Protection Key (PK): G
View Log	View HSM log	Approved mode; ERROR_OK;	Command In	Log	None	CO

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		ERROR_HSM_STATE;				
User Application Login	Verify Username and PASSWORD	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Login User role	Symmetric Encryption / Decryption DRBG Asymmetric Key Generation Message Digest KTS1	User - User Password: R,E - RSA Key Decryption Key (KDK): G,E,Z - RSA Key Encryption Key (KEK): G,E,Z - Session AES Key: W,E - Session HMAC Key: W,E - Protection Key (PK): E
User Application Logout	User Application Logout	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Logout User role		User - Session HMAC Key: Z - Protec

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						tion Key (PK): E - Session AES Key: Z
Modify User Application password	Modify user password, write the new password to module, and store it with PK protection.	Approved mode; ERROR_OK; ERROR_HSM_STATE;	User Application password	Updated the User Application password. Success/failure status	Symmetric Encryption / Decryption Message Digest KTS2	User - User Password: W - Session AES Key: E - Session HMAC Key: E - Protection Key (PK): E
AES CBC Encryption	AES CBC encryption service	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Plaintext	Ciphertext. Success/failure status	Symmetric Encryption / Decryption KTS2	User - User AES Key: E - Session AES Key: E - Session HMAC Key: E - Protection Key (PK): E

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES CBC Decryption	AES ECB encryption service	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Ciphertext	Plaintext. Success/failure status	Symmetric Encryption / Decryption KTS2	User - User AES Key: E - Session AES Key: E - Session HMAC Key: E - Protection Key (PK): E
AES ECB Encryption	AES ECB encryption service	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Plaintext	Ciphertext. Success/failure status	Symmetric Encryption / Decryption KTS2	User - User AES Key: E - Session AES Key: E - Session HMAC Key: E - Protection Key (PK): E
AES ECB Decryption	User uses AES ECB decryption service	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Ciphertext	Plaintext. Success/failure status	Symmetric Encryption / Decryption KTS2	User - User AES Key: E - Session AES Key: E

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Session HMAC Key: E - Protection Key (PK): E
RSA2048 Signature generation	RSA 2048 signature generation service	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Generated signature. Success/failure status	Signature Generation KTS2	User - User RSA Private Key: E - Protection Key (PK): E - Session AES Key: E - Session HMAC Key: E
RSA2048 Signature verification	RSA 2048 Signature verification service	Approved mode; ERROR_OK; ERROR_HSM_STATE	Signature data	Success/failure status	Signature Verification KTS2	User - User RSA Public Key: E - Protection Key (PK): E - Session AES Key: E

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Session HMAC Key: E
ECDSA Signature generation	ECDSA signature generation service	Approved mode; ERROR_OK; ERROR_HSM_STATE	Command In	Generated signature. Success/failure status	Signature Generation KTS2	User - User ECDSA Private Key: E - Protection Key (PK): E - Session AES Key: E - Session HMAC Key: E
ECDSA Signature verification	ECDSA Signature verification service	Approved mode; ERROR_OK; ERROR_HSM_STATE	Signature data	Success/failure status	Signature Verification KTS2	User - User ECDSA Public Key: E - Protection Key (PK): E - Session AES Key: E - Session

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						HMAC Key: E
Random Bit Generation	Random Bit Generation	Approved mode; ERROR_OK; ERROR_HSM_STATE	Signature data	DRBG Seed	Entropy DRBG Asymmetric Key Generation Symmetric Key Generation	User - DRBG Entropy Input (Seed): G,E - DRBG State V: G,E - DRBG State C: G,E - DRBG Output: G,E CO - DRBG Entropy Input (Seed): G,E - DRBG State V: G,E - DRBG State C: G,E - DRBG Output: G,E
Show Module Version	Display version number of modules in HSM/hard	Approved mode; ERROR_OK; ERROR_HSM_STATE	Command In	Module HW version, FW version information	None	User CO

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	ware/ firmware					
Show Module Status	View Module status	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	FIPS status	None	User CO
Zeroize	Zeroization through Factory reset of the module, tamper switch or EFP failure.	Approved mode; ERROR_OK;	Factory reset Command In / Tamper switch triggered, EFP failed	All keys zeroized / All unprotected SSPs zeroized	None	User - Device Master Key (DMK): Z - Protection Key (PK): Z - RSA Key Decryption Key (KDK): Z - Session AES Key: Z - Session HMAC Key: Z - DRBG Entropy Input (Seed): Z - DRBG State V: Z

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG State C: Z - DRBG Output: Z - User AES Key: Z - User ECDSA Private Key: Z - User RSA Private Key: Z - User Password: Z - CO RSA-pub Key: Z - RSA Key Encryption Key (KEK): Z - User ECDSA Public Key: Z - User RSA Public Key: Z CO

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-Tests	Perform the self-tests automatically when the module is powered on or restarted	Approved mode; ERROR_OK;	Command In (Reset, automatic periodic self-tests)	Success/Reset	None	User CO
Set Mode of operation	Set the mode of operation	Approved mode; ERROR_OK; ERROR_HSM_STATE;	Command In	Success/failure status	DRBG Signature Verification	CO - CO RSA-pub Key: W,E

Table 14: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Create User Key	Create User Key	ECDSA_secp256k1 ed25519 SM2 SM4 sr25519	User
Remove user key	Remove user key	ECDSA_secp256k1 ed25519 SM2 SM4 sr25519	User
List User Key	List User Key types	ECDSA_secp256k1 ed25519 SM2 SM4 sr25519	User
SM4 Decryption	User uses sm4 decryption service	SM4	User
SM4 Encryption	User uses sm4 encryption service	SM4	User
SM2 Signature generation	User uses sm2 signature generation service	SM2	User
SM2 Signature verification	User uses sm2 Signature verification service	SM2	User

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Algorithms	Role
ECDSA_secp256k1 Signature generation	User uses ECDSA_secp256k1 signature generation service	ECDSA_secp256k1	User
ECDSA_secp256k1 Signature verification	User uses ECDSA_secp256k1 Signature verification service	ECDSA_secp256k1	User
sr25519 Signature generation	sr25519 Signature generation	ed25519	User
sr25519 Signature verification	User uses sr25519 Signature verification service	sr25519	User
ed25519 Signature generation	User uses ed25519 signature generation service	ed25519	User
ed25519 Signature verification	User uses ed25519 Signature verification service	ed25519	User
ripmd160 digest	User uses ripmd160 message digest service	ripmd160	User
SHA3-256 digest	User uses sha3-256 message digest service	sha3-256 (FIPS 202)	User
SM3 digest	User uses SM3 message digest service	SM3	User
Zeroize	Zeroization through Factory reset of the module, tamper switch or EFP failure.	ECDSA_secp256k1 ed25519 ripmd160 sha3-256 (FIPS 202) SM2 SM3 SM4 sr25519	CO

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

N/A - The Module does not include a firmware load service.

5 Software/Firmware Security

The Module is a Level 3 multi-chip standalone hardware module.
Firmware integrity verification uses an approved digital signature cryptographic mechanism, if the calculated result is not successfully verified, the test fails, and the module enters the error state.

5.1 Integrity Techniques

In the production process, the public key of the firmware integrity key pair is written into the flash of the AS578 in plaintext. Use the sha256 algorithm to calculate the message digest of the bootloader, kernel, and application of the IMX6 and the message digest of the executable code of the AS578, sign these

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

message digests with the private key of the firmware integrity key pair, and write these signatures into the flash of the AS578. The firmware integrity check of IMX6 and AS578 is performed as follows:

AS578:
• Read the digital signature of executable code message digest stored in the flash of AS578, verify the signature with the public key of the firmware integrity key pair, and get the message digest.
• Read executable code and use sha256 algorithm to calculate message digest.
• Compare the two message digests, if the digests are consistent, the firmware integrity check will pass, otherwise module enters the error state.

imx6:
• Read the images of bootloader, kernel and application on EMMC respectively, use sha256 algorithm to calculate the message digest, and transfer the message digest to AS578.
• Read the digital signature of bootloader, kernel, and application stored in the flash of AS578, verify the signature with the public key of the firmware integrity key pair, and obtain the message digest.
• Compare the two message digests, if the digests are consistent, the firmware integrity check will pass, otherwise module enters the error state.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by rebooting the module.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

The Module has a non-modifiable operational environment at Level 3 under the FIPS 140-3 definitions therefore per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section is not applicable.

The Module does not include a firmware load service to support necessary updates. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

7 Physical Security

The module is a multiple-chip standalone cryptographic module. Physical security is designed according to Level 3 standards.

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-Evident Seals	Inspect tamper-evident seals monthly.	Look for signs of tampering. If tampering is suspected, then the module must be removed from service.

Table 16: Mechanisms and Actions Required

Tamper Detection

The cryptographic module includes a tamper detection feature that will immediately zeroize all SSPs when the module's cover is removed. This forces a factory reset and will put the module into the Invasive Error State. This will also close all external interfaces and stop providing all services.

The tamper detection always remains active including when the module is powered off, which at that point, will operate with an internal battery.

As the tamper-evident seals will need to be broken to remove the cover, there is no recovery from the error state as the module will no longer be in service.

7.2 User Placed Tamper Seals

The cryptographic module is contained within a strong enclosure with four (4) tamper-evident seals on the top, left side and bottom and right side and bottom. Each tamper-evident seal is individually identifiable.

Placement:

Seal ID	Placement
1	Top side
2	Top side
3	Left side and bottom
4	Right side and bottom

Table 17: Tamper Seal Placement

Operator Responsible for Securing Unused Seals: CO

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

If the CO determines that the seals were tampered with, the module is to be removed from service and no longer allowed to be used and is not to be returned to the vendor. The CO will perform the factory reset to zeroize all SSPs.

Part Numbers:

IB6127370XXX



Figure 10 - Module Seal Location (Top)

Amber Group Public Material – May be reproduced only in its original entirety (without revision).



Figure 11 - Module Seal Location (Bottom)



Figure 12 - Module Seal Location (Left Side)

Amber Group Public Material – May be reproduced only in its original entirety (without revision).



Figure 13 - Module Seal Location (Right Side)

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-2.6	EFP	Zeroization
HighTemperature	46	EFP	Zeroization
LowVoltage	68V	EFP	Shutdown
HighVoltage	280V	EFP	Shutdown

Table 18: EFP/EFT Information

The cryptographic module will perform EFP. If the voltage falls outside the normal operating range of the module, the module will shut down immediately.

If the temperature falls outside the normal operating range of the module, the module will immediately zeroizes all unprotected SSPS.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

8 Non-Invasive Security

8.1 Mitigation Techniques

The Module does not implement any mitigation method against non-invasive attack.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Volatile Memory	Dynamic
Flash	Internal flash memory storage drive	Static

Table 19: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input SK	External	RAM	Plaintext	Automated	Electronic	
Output SK	RAM	External	Plaintext	Automated	Electronic	
Input PK	External	Flash	Plaintext	Automated	Electronic	
Output PK	Flash	External	Plaintext	Automated	Electronic	
Input with KAS-IFC	External	RAM	Encrypted	Automated	Electronic	KTS1
Input by User application	External	Flash	Encrypted	Automated	Electronic	KTS2

Table 20: SSP Input-Output Methods

Input SK: Input in plaintext from 2 of the 3 components stored in the token during module initialization using trusted channel and split knowledge

Output SK: Split into 3 components and Output to 3 tokens in plaintext using trusted channel and split knowledge.

Input with KAS-IFC: Generated by SDK using AES algorithm and transmitted into the module through KTS-IFC

Input by User application: Encrypted by session key and Input by User application

Input PK: Generated by USB_TOKEN and imported as identify Key

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Power cycle	Zeroized by Module power cycle	Power off / Reboot
Z2	Zeroize service	Zeroized by the "zeroize" service by overwriting with a fixed pattern of 0s	Invocation of the zeroize CLI command

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Zeroization Method	Description	Rationale	Operator Initiation
Z3	Dereferenced by session termination	Dereferenced by session termination and zeroized by OS memory cleanup.	API call
Z4	Tamper switch is triggered	Zeroized when the tamper switch is triggered or EFP failed.	Tamper detection triggered
Z5	Factory reset	Zeroized by Factory reset	Factory Reset

Table 21: SSP Zeroization Methods

9.4 SSPs

All CSPs and PSPs used by the Module are described in this section. All usage of these SSPs by the Module is described in the services detailed in Approved Services table in Section 4.3.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Device Master Key (DMK)	Device Master Key (DMK)	256 - 256	Master Key - CSP	DRBG		Key Derivation from DMK
Protection Key (PK)	Protection Key (PK)	256 - 256	Protection Key - CSP	Key Derivation from DMK		Symmetric Encryption / Decryption
RSA Key Decryption Key (KDK)	RSA Key Decryption Key (KDK)	112 - 112	Key Decryption Key (KEK) - CSP	Asymmetric Key Generation		KTS1
Session AES Key	AES Key	256 - 256	AES Key - CSP			KTS2
Session HMAC Key	HMAC Key	256 - 256	HMAC Key - CSP			KTS2
DRBG Entropy Input (Seed)	Entropy Input	256 - 256	Entropy Input - CSP	Entropy		DRBG
DRBG State V	HASH DRBG V	256 - 256	DRBG State Value - CSP	DRBG		DRBG
DRBG State C	HASH DRBG C key	256 - 256	DRBG State Value - CSP	DRBG		DRBG

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Output	DRBG Output	256 - 256	DRBG Output - CSP	DRBG		Asymmetric Key Generation Symmetric Key Generation
User AES Key	User AES Key	128/192/256 - 128/192/256	AES Key - CSP	Symmetric Key Generation		Symmetric Encryption / Decryption
User ECDSA Private Key	ECDSA Private Key	128 - 128	Private Key - CSP	Asymmetric Key Generation		Signature Generation
User RSA Private Key	RSA Private Key	112 - 112	Private Key - CSP	Asymmetric Key Generation		Signature Generation
User Password	User Password	8 Characters - Please see Authentication Methods table for details.	Authentication Password - CSP			
CO RSA-pub Key	CO RSA Public Key	112 - 112	CO Public Key - PSP			Signature Verification
RSA Key Encryption Key (KEK)	RSA Key Encryption Key (KEK)	112 - 112	RSA Key Encryption Key (KEK) - PSP	Asymmetric Key Generation		KTS1
User ECDSA Public Key	User ECDSA Public Key	128 - 128	User ECDSA Public Key - PSP	Asymmetric Key Generation		Signature Verification
User RSA Public Key	User RSA Public Key	112 - 112	User Public Key - PSP	Asymmetric Key Generation		Signature Verification

Table 22: SSP Table 1

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Device Master Key (DMK)	Input SK Output SK	RAM:Plaintext	Until Zeroized	Z1 Z2 Z4 Z5	Protection Key (PK):Derives
Protection Key (PK)		RAM:Plaintext	Until Zeroized	Z1 Z2 Z4 Z5	User AES Key:Encrypts User ECDSA Private Key:Encrypts User RSA Private Key:Encrypts User Password:Encrypts CO RSA-pub Key:Encrypts User ECDSA Public Key:Encrypts User RSA Public Key:Encrypts Device Master Key (DMK):Derived From
RSA Key Decryption Key (KDK)		RAM:Plaintext	Until Zeroized	Z1 Z2 Z4 Z5	RSA Key Encryption Key (KEK):Paired with
Session AES Key	Input with KAS-IFC	RAM:Plaintext	Until Zeroized	Z1 Z3 Z4 Z5	Session HMAC Key:Paired With
Session HMAC Key	Input with KAS-IFC	RAM:Plaintext	Until Zeroized	Z1 Z3 Z4 Z5	Session AES Key:Paired With
DRBG Entropy Input (Seed)		RAM:Plaintext	Until Zeroized	Z1 Z2 Z4 Z5	DRBG State V:Used With DRBG Output:Used With
DRBG State V		RAM:Plaintext	Until Zeroized	Z1 Z2 Z4 Z5	DRBG Entropy Input (Seed):Used With DRBG State C:Used With DRBG Output:Used With
DRBG State C		RAM:Plaintext	Until Zeroized	Z1 Z2	DRBG Entropy Input (Seed):Used

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Z4 Z5	With DRBG State V:Used With DRBG Output:Used With
DRBG Output		RAM:Plaintext	Until Zeroized	Z1 Z2 Z4 Z5	DRBG State V:Used With DRBG State C:Used With
User AES Key		Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	Protection Key (PK):Encrypted by
User ECDSA Private Key		Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	User ECDSA Public Key:Paired with Protection Key (PK):Encrypted by
User RSA Private Key		Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	User RSA Public Key:Paired with Protection Key (PK):Encrypted by
User Password	Input by User application	Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	Protection Key (PK):Encrypted by
CO RSA-pub Key	Input PK	Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	
RSA Key Encryption Key (KEK)	Output PK	RAM:Plaintext	Until Zeroized	Z1 Z3 Z4 Z5	RSA Key Decryption Key (KDK):Paired With
User ECDSA Public Key		Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	User ECDSA Private Key:Paired With Protection Key (PK):Encrypted by
User RSA Public Key		Flash:Encrypted	Until Zeroized	Z2 Z4 Z5	User RSA Private Key:Paired With Protection Key (PK):Encrypted by

Table 23: SSP Table 2

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

10 Self-Tests

10.1 Pre-Operational Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self–tests are periodically performed by the Module every 720 hours automatically after the module is powered on, without external input or control. The Module will not accept any commands when a periodic self-test is required; the commands still in the I/O buffer will be processed by The Module and the periodic self-test executed when the I/O buffer is emptied. The Module logs self-test errors in the system log, the CO can consult the error log by View system logs on management software. When HSM powers on, the operator can perform the on-demand self-test through power cycling.

The self-tests error states and status indicator are described in table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A2750)	MOD 2048, SHA2-256	Approved Integrity Technique	SW/FW Integrity	PASS / FAIL console output	Firmware Integrity Test

Table 24: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

NOTE: Conditional KAT tests are run during the startup of the module as part of the Pre-Operational Self-Test phase

NOTE: KAT RSA PKCS#1v1.5 with 2048-bit key and SHA-256, signature verification is performed prior to the Firmware Integrity.

The Module performs the following conditional self-tests:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB Encrypt	256 bits	KAT	CAST	PASS / FAIL console output	Symmetric Encrypt	Module Startup - On Demand
AES-ECB Decrypt	256 bits	KAT	CAST	PASS / FAIL console output	Symmetric Decrypt	Module Startup - On Demand

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt	256 bits	KAT	CAST	PASS / FAIL console output	Symmetric Encrypt	Module Startup - On Demand
AES-CBC Decrypt	256 bits	KAT	CAST	PASS / FAIL console output	Symmetric Decrypt	Module Startup - On Demand
Hash DRBG (A2750)	Hash_DRBG using SHA-256, with PR	KAT	CAST	PASS / FAIL console output	Instantiation, generate, and reseed KATs performed before the first random data generation.	Module Startup - On Demand
ECDSA KeyGen (FIPS186-4) (A2750)	ECDSA P-256 Key Generation Pairwise Consistency Test	PCT	PCT	PASS / FAIL console output	ECDSA Key Generation	Module Startup - On Demand
ECDSA SigGen	ECDSA with P-256 and SHA-256	KAT	CAST	PASS / FAIL console output	Signature Generation	Module Startup - On Demand
ECDSA SigVer	ECDSA with P-256 and SHA-256	KAT	CAST	PASS / FAIL console output	Signature Verification	Module Startup - On Demand
HMAC-SHA2-256 (A2750)	key size 256 bits	KAT	CAST	PASS / FAIL console output	Message Authentication	Module Startup - On Demand
KDF SP800-108 (A2750)	key derivation	KAT	CAST	PASS / FAIL console output	Key Derivation	Module Startup - On Demand
RSA KeyGen	2048-bit RSA Encryption and Decryption / 2048-bit RSA Sign and Verify	PCT	PCT	PASS / FAIL console output	RSA Key Generation PCT	Module Startup - On Demand
RSA KeyGen Encapsulation	2048-bit RSA Encryption	KAT	PCT	PASS / FAIL	RSA Key Generation	Module Startup - On Demand

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	and Decryption			console output	PCT for KTS-IFC	
RSA SigGen	RSA-2048-bit key	KAT	CAST	PASS / FAIL console output	Signature Generation	Module Startup - On Demand
RSA SigVer	RSA-2048-bit key	KAT	CAST	PASS / FAIL console output	Signature Verification	Module Startup - On Demand
SHA2-256 (A2749)	Message Digest	KAT	CAST	PASS / FAIL console output	Message Digest	Module Startup - On Demand
SHA2-256 (A2750)	Message Digest	KAT	CAST	PASS / FAIL console output	Message Digest	Module Startup - On Demand
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	PASS / FAIL console output	As specified in [90B] RCT startup health tests	At boot up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	PASS / FAIL console output	As specified in [90B] APT startup health tests	At boot up
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	PASS / FAIL console output	As specified in [90B] RCT continuous health tests	Continuous when entropy is requested
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	PASS / FAIL console output	As specified in [90B] APT continuous health tests	Continuous when entropy is requested

Table 25: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A2750)	Approved Integrity Technique	SW/FW Integrity	every 720 hour	Programmatically

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Table 26: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB Encrypt	KAT	CAST	On Demand	by power cycling the Module
AES-ECB Decrypt	KAT	CAST	On Demand	by power cycling the Module
AES-CBC Encrypt	KAT	CAST	On Demand	by power cycling the Module
AES-CBC Decrypt	KAT	CAST	On Demand	by power cycling the Module
Hash DRBG (A2750)	KAT	CAST	On Demand	by power cycling the Module
ECDSA KeyGen (FIPS186-4) (A2750)	PCT	PCT	On Demand	by power cycling the Module
ECDSA SigGen	KAT	CAST	On Demand	by power cycling the Module
ECDSA SigVer	KAT	CAST	On Demand	by power cycling the Module
HMAC-SHA2-256 (A2750)	KAT	CAST	On Demand	by power cycling the Module
KDF SP800-108 (A2750)	KAT	CAST	On Demand	by power cycling the Module
RSA KeyGen	PCT	PCT	On Demand	by power cycling the Module
RSA KeyGen Encapsulation	KAT	PCT	On Demand	by power cycling the Module
RSA SigGen	KAT	CAST	On Demand	by power cycling the Module
RSA SigVer	KAT	CAST	On Demand	by power cycling the Module
SHA2-256 (A2749)	KAT	CAST	On Demand	by power cycling the Module
SHA2-256 (A2750)	KAT	CAST	On Demand	by power cycling the Module
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	On Demand	by power cycling the Module or by invoking the SK_RunAllSelfTests() API.
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	On Demand	by power cycling the Module or by invoking the SK_RunAllSelfTests() API.
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A

Table 27: Conditional Periodic Information

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Pre-operational self–tests are periodically performed by the Module every 720 hours automatically after the module is powered on, without external input or control. The Module will not accept any commands when a periodic self-test is required; the commands still in the I/O buffer will be processed by The Module and the periodic self-test executed when the I/O buffer is emptied. The Module logs self-test errors in the system log, the CO can consult the error log by View system logs on management software.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	Upon detection of any failures in a preoperational or conditional self-test	The Module enters Critical error state.	Reset Module	Status of the red LED stays on, the blue LED flashes quickly, otherwise it indicates successful completion by Red LED flashes quickly, blue LED flashes quickly.
Invasive Error	When the module's cover is removed, it triggers the tamper detection, performs a factory reset and immediately zeroizes all SSPs. All external interfaces are closed.	The Module entersInvasive error state.	Although the module can be rebooted into an initialization state, in order to remove the cover, the tamper-evident seals must be broken. The module is now considered non operational and is not to be used.	The LEDs indicate the error state as follows: Red LED stays on, the blue LED flashes normally.

Table 28: Error States

10.5 Operator Initiation of Self-Tests

When HSM powers on, the operator can perform the on-demand self-test through power cycling.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module will be securely delivered to the operators via UPS with tracking codes to ensure there is no tampering during delivery. Upon receipt of the module, the CO must check that the module's outer packaging is intact or that the packaging has been opened during transport.
Upon delivery, the operator must initialize the module as follows:

1. The operator must ensure that the initial security configuration of the module is completed in a restricted environment using a direct cabled serial connection from the management console (standalone PC).
2. From the management program on the console, the operator must select the COM port by selecting “Connect” from the menu bar.
3. Next, the operator must create the Manager role (CO) by selecting from the Management program menu: Device → Add MNG. The operator then must insert the first of 3 USB tokens. A new PASSWORD (8 characters) will be required and stored on the USB token.
4. Repeat this process twice more with different USB Tokens. When the three Manager roles have been created, HSM can be initialized.
5. Next, the operator will create DMK for the HSM, and export DMK components to USB tokens. Select from the Management program menu: Device → Create DMK. With 3 different USB token, CO must sign in the HSM three (3) times, and store DMK component to each USB token. One DMK component, one USB token.
6. With one of 3 USB tokens, the operator selects from menu, choose: Device → Set Mode of Operation, and choose “FIPS Mode”. Once “OK” is selected, the module will reboot and perform the Pre-Operational and Conditional KAT Self-Tests.
7. Select from menu Tools → Reset HSM, which zeroizes all the SSPs, will remove the module from the Approved Mode of Operation

11.2 Administrator Guidance

The serial port is used to connect the cryptographic module and the management computer.
The CO implements management functions such as Add MNG, Restore DMK, user application management, and key management through the management computer. The following is the specific function description.

Connect HSM

Before using the HSM, you have to connect to it first. Choose “Connect” from menu, then the dialog below will appear:

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

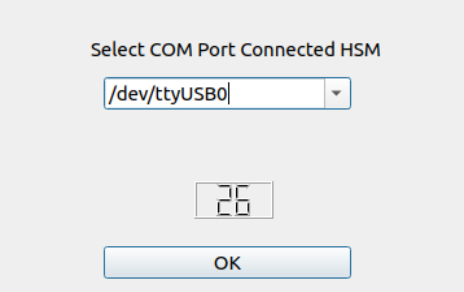


Figure 14 - Choose COM Port

From pull-down control, select COM port which connects to HSM. If the port used are not listed, please input the device full path in the edit control. After selection, please click “OK” button。

Add MNG

The first step to use the HSM is to create HSM manager.

From menu: Device → Add MNG, Follow the instructions shown in the figure below to complete the process.

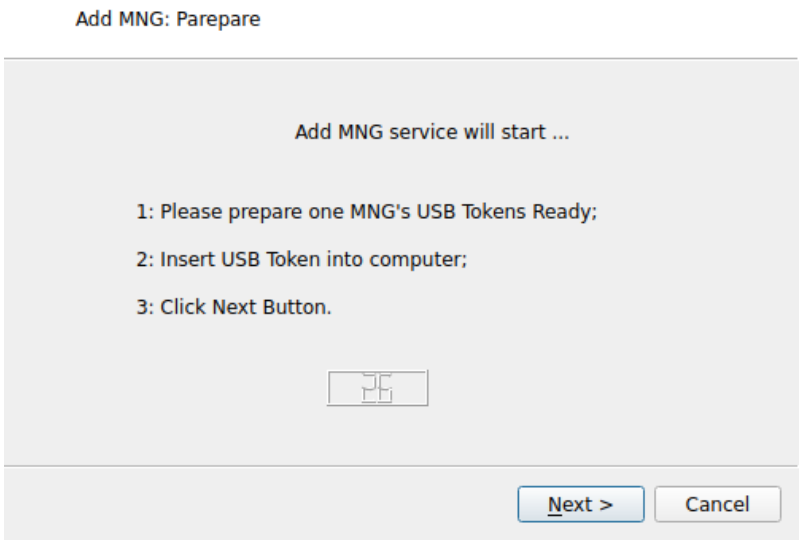


Figure 15 - Add MNG

Create DMK

From menu: Device → Create DMK, Follow the instructions shown in the figure below, the manager can store DMK components to 3 USB Tokens.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

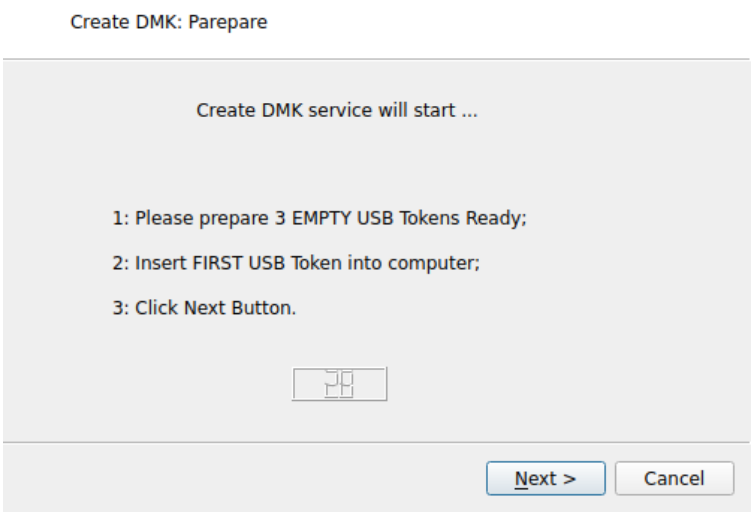


Figure 16 - Create DMK

Set Mode of Operation

The next step sets the HSM operation mode. From menu, choose: Device→ Set Mode of Operation. The CO will have two choices, to select “FIPS Mode” or “Non-FIPS Mode” Once selected, the CO will follow the instructions shown in the figure below to complete the process.

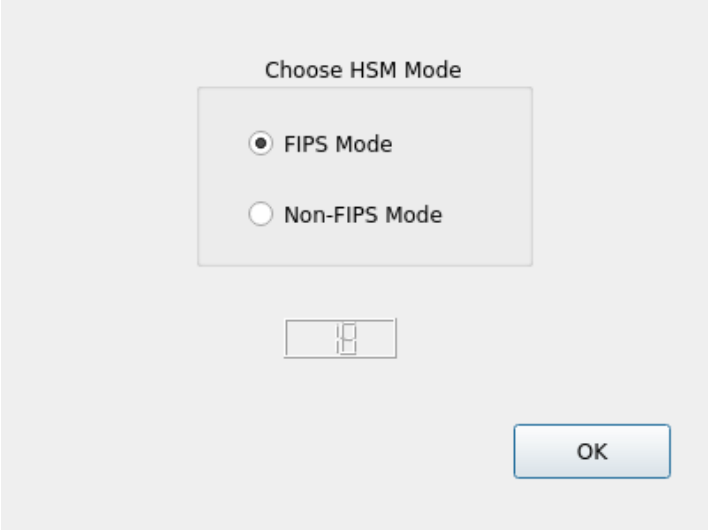


Figure 17 - Set Mode of Operation

Restore DMK

After initialization is complete, when the HSM restarts, the first step is to restore DMK. From menu, choose: Device→ Restore DMK, Follow the instructions below to complete the process.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

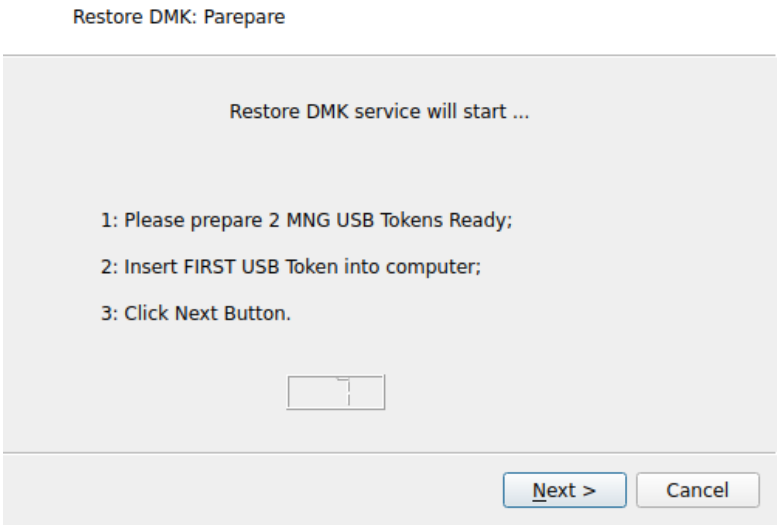


Figure 18 - Restore DMK

Other functions can be selected on the menu of the management software and operated according to the instructions.

COs are responsible for protecting USB tokens and passwords from theft.

COs must periodically check that the tamper evidence seals are intact and located in the correct position on the chassis. If evidence of tampering is detected, the module shall be considered non-compliant and shall be scrapped.

11.3 Non-Administrator Guidance

The Type-C Port is used to connect the cryptographic module and the communication computer. The communication computer is connected to the application server via Ethernet.

When CO creates a user account, a default password is generated. The default password is emailed to the appropriate user. The user must change the password when logging in for the first time. Users can access the services of the cryptographic module only after their identity authentication is passed. The cryptographic module provides user applications with services such as user login/logout, data encryption and decryption, data signature and verification.

Users are responsible for protecting their passwords from theft.

11.4 Rules of Operation

The Module shall be installed as described in Section 11 secure installation, initialization, startup and operation of the Module, and Section 7 Physical Security.

The Module shall be operated such that only the approved mode is enabled.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

Overall Security Design

1. The Module provides two distinct operator roles: User (User Application external entity) and Cryptographic Officer (Manager).
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. Pre-Operational self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are restrictions on which SSPs are zeroized by the zeroization service. Factory reset will zeroize all SSPs of the module, tamper detection or EFP failure will zeroize all unprotected SSPs of the module.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module enters or outputs plaintext CSPs using trusted channel and split knowledge.
15. The Module does not store any plaintext CSPs.
16. The Module does not output intermediate key values.
17. The Module does not provide bypass services or ports/interfaces.

11.5 End of Life

To prepare the module for disposal, zeroize the module using the "Zeroize" service and dispose of it at an electronic recycling facility.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).

12 Mitigation of Other Attacks

12.1 Attack List

The Module does not implement any mitigation method against other attacks.

Amber Group Public Material – May be reproduced only in its original entirety (without revision).