WISeKey Semiconductors

VaultIC™ 405 1.2.6

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.2

Date: 16 August 2022

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Wisekey VaultIC™ 405 1.2.6 module, hereafter denoted "the Module" or "VaultIC". The Module is a security module designed to secure various applications such as anticloning, physical access control, personal access control for multimedia and web applications, hardware authentication, user strong authentication, SSL support, PKCS#11 or Microsoft® CSP based applications, PKI applications, DRM, trusted computing, and IP protection. It is a turnkey solution that combines powerful cryptographic capabilities and secure data storage.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	VaultIC™ 405 1.2.6	AT90SO72 rev C	1.02.6F

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

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The Module is a single chip embodiment. The cryptographic boundary is denoted with the dashed blue line in Figure 1.

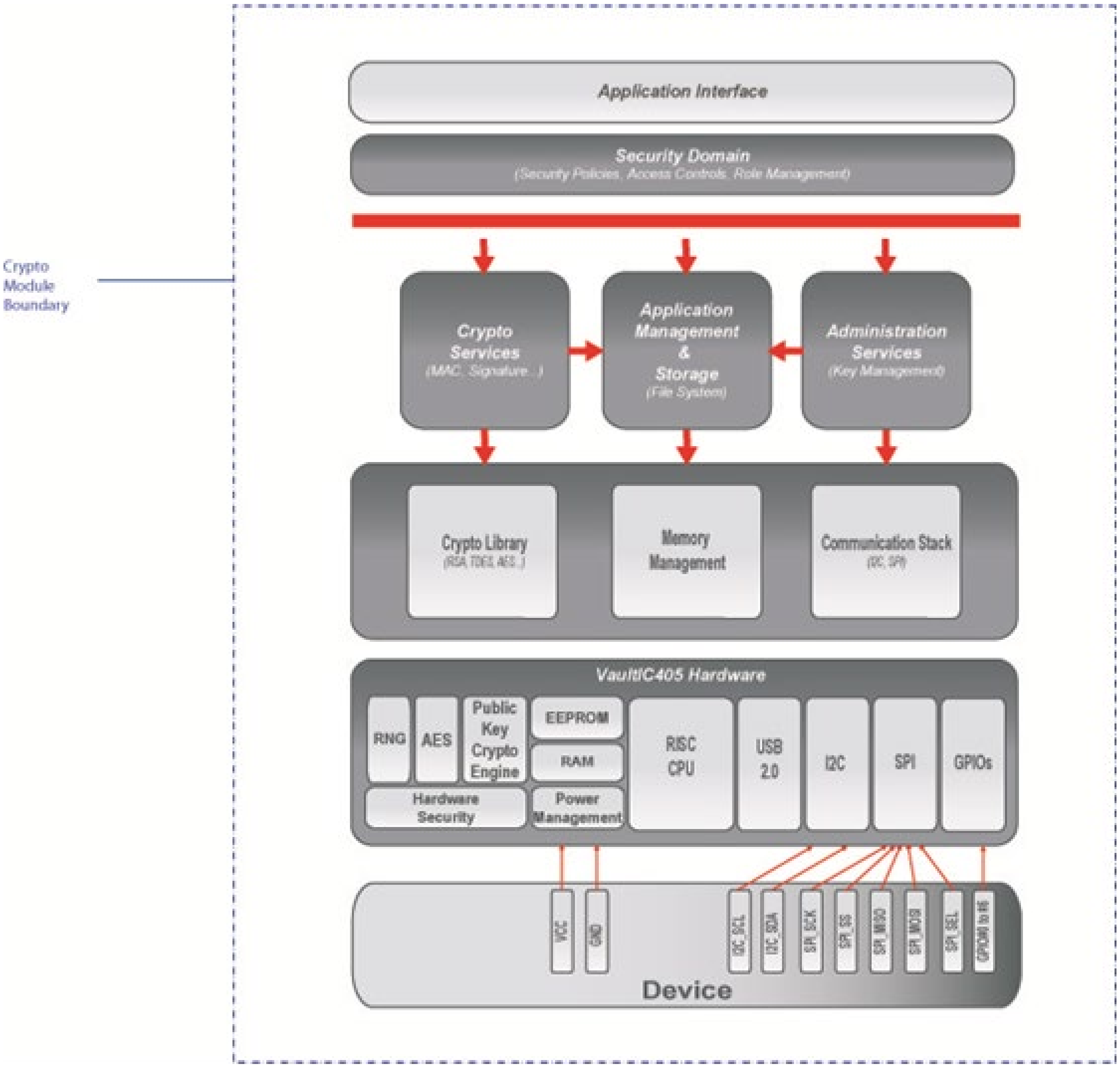

Figure 1 – Module

The proven technology used in the security module is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers and authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented.

The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised. Strong Authentication capability, secure storage, and flexibility thanks to its various interfaces (SPI, I2C), low pin count and low power consumption are main features of the VaultIC. Its embedded firmware provided advanced functions such as Identity-based authentication, large Cryptographic command set, Cryptographic protocols, Secure Channel Protocols, Robust communication protocol.

The module's ports and associated FIPS defined logical interface categories are listed in Table 3.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
SPI_SCK	SPI Clock	Control Input
VCC	Power Supply	Power
GND	Ground	Power
SPI_MISO	SPI Master In Slave Out	Status Output, Data Output
SPI_MOSI	SPI Master Out Slave In	Control Input, Data Input
SPI_SS	SPI Slave Select	Control Input
I2C_SCL	I2C Clock	Control Input
SPI_SEL	SPI or I2C selection	Control Input
I2C_SDA	I2C Data line	Control Input, Data Input, Data Output, Status Output
GPIO#0 to #6	GPIO / I2C Address	Control Input, Data Input, Data Output

1.2 Modes of Operation

The VaultIC operates in different modes of operation, given different conditions of use of keys and cryptographic services. The mode of operation is automatically selected according to the device state and the authenticated operator. The selected mode of operation remains activated while the operator is authenticated. The mode of operation is discarded when the authentication is cancelled, or the secure channel is terminated.

FIPS Approved Mode of Operation

This mode is automatically selected when the device is in ACTIVATED state and an approved user or an approved administrator is successfully authenticated. While in an approved mode of operation, only Approved and Allowed Algorithms are allowed. Additional security restrictions may apply.

The module will indicate that it is running in the FIPS Approved mode of operation by indicating *Mode of Operation: Approved* in the response of a *Get Info command*.

Non-Approved Mode of Operation

This mode is automatically selected when the device is in ACTIVATED state and a non-approved user or a non-approved administrator is authenticated. While in a non-approved mode of operation, the VaultIC usage is not restricted and both Approved and Allowed Algorithms and Non-Approved, Non-Allowed Algorithms are allowed.

The module will indicate that it is running in the non-FIPS Approved mode of operation by indicating *Mode of Operation: non-approved mode* in the response of a *Get Info command*.

CSPs are not shared between the non-Approved and Approved modes of operation and the internal state of the DRBG is zeroized each time the DRBG is instantiated.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
A2383	AES [197]	ECB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
A2383	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
A2383	AES [197]	CTR [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
A2383	AES [197]	OFB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
A2383	AES [197]	CFB128 [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
A2384	AES [197]	GCM[1] [38C]	Key Sizes: 128, 192, 256 Tag Len: 96, 112, 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
A2384	AES [197]	KW, KWP [38F]	Forward Key Sizes: 128, 192, 256	Authenticated Encrypt, Authenticated Decrypt
A2384	AES [197]	CMAC [38B]	Key Sizes: 128, 192, 256 Tag Len: 128	Message Authentication
VA	CKG	-	Section 4 Using the Output of a Random Bit Generator Section 6.1 The "Direct Generation" of Symmetric Keys Section 6.2.2 Symmetric Keys Derived from a Pre-existing Key	Cryptographic Key Generation
A2384	DRBG [90A]	CTR	Use_df AES-256	Deterministic Random Bit Generation Security Strength = 256
-	ENT (P) [90B]	-	-	Entropy source, provides sufficient entropy to seed the DRBG to a security strength of 256-bits.
A2384	KBKDF [108]	Counter	CMAC (AES-128, AES-192, AES-256)	Key Based Key Derivation
A2383, A2384	KTS	AES-CBC, AES-CMAC	AES-128, AES-192, AES-256	Key establishment methodology provides between 128 and 256 bits of encryption strength). Key Transport with SCP03.

[1] 96-bit IV is randomly generated in its entirety using the internal DRBG in accordance with IG A.5, Scenario 2.

Cert	Algorithm	Mode	Description	Functions/Caveats
A2384	KTS	AES-KW, AES-KWP	AES-128, AES-192, AES-256	Key establishment methodology provides between 128 and 256 bits of encryption strength).
A2384	SHS [180]	SHA-224 SHA-256 SHA-384 SHA-512	-	Message Digest Generation, Password Obfuscation

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
XOR	IG 1.23. Obfuscation of data values in memory; no security claimed

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- 3-DES
- DES
- GMAC
- HMAC
- SHA-1

2.1 Critical Security Parameters

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 6 – Critical Security Parameters (CSPs) description

Key Name	Type	Description	Strength (bits)
CTR_DRBG Key	AES-CTR 256 bits	Used for AES CTR DRBG encryption	256
CTR_DRBG V	Initialisation Vector	Used for AES CTR DRBG encryption	128
Entropy	Entropy input	Used for the FIPS Approved DRBG (CTR_DRBG_AES256)	256
SCP03 S-ENC Static Key	AES CBC (128, 192, 256 bits)	SCP03 static AES encryption key; used to derive session keys	128,192 or 256
SCP03 S-MAC Static Key	AES C-MAC (128, 192, or 256 bits)	SCP03 static AES MAC key; used to derive session keys	128,192 or 256
SCP03 C-MAC Session Key	AES C-MAC (128, 192, or 256 bits)	SCP03 AES session key for authentication of incoming data	128,192 or 256
SCP03 R-MAC Session Key	AES C-MAC (128, 192, or 256 bits)	SCP03 AES session key for authentication of outgoing data	128,192 or 256

Key Name	Type	Description	Strength (bits)
SCP03 C-ENC Session Key	AES CBC (128, 192, or 256 bits)	SCP03 AES session key for data encryption	128,192 or 256
AES Keys	AES ECB, CBC, OFB, CFB, CTR, CMAC, GCM or KW/KWP (128, 192, or 256 bits)	Used to encrypt/decrypt messages or generate C-MACs	128,192 or 256
Secure Password password	8-32 byte string	Secure Password data to be provided to authenticate a user. 8-32 bytes.	N/A
Secure password AES key	AES-CBC (128, 192, 256)	Secure Password AES key used to encipher the authentication data	128, 192 or 256

Table 7 - Critical Security Parameters (CSPs) usage

Key Name	Generation	Storage	Entry	Output	Destruction
CTR_DRBG Key	Internally via FIPS Approved DRBG	Stored in RAM	N/A	N/A	Power-off or DRBG health-test failed
CTR_DRBG V	Internally via FIPS Approved DRBG	Stored in RAM	N/A	N/A	Power-off or DRBG health-test failed
Entropy	Internally via the SP800-90B ENT (P)	Stored in RAM	N/A	N/A	Deleted after use, power-off or DRBG health-test failed
SCP03 S-ENC Static Key	Externally generated. Initial value pre-installed.	Stored & optionally masked (1) in EEPROM	Wrapped by SCP03 session	N/A	Zeroized when user is deleted. Also zeroized when the user is locked with bSecurityOption set to 1
SCP03 S-MAC Static Key	Externally generated. Initial value pre-installed.	Stored & optionally masked (1) in EEPROM	Wrapped by SCP03 session	N/A	Zeroized when user is deleted. Also zeroized when the user is locked with bSecurityOption set to 1
SCP03 C-MAC Session Key	Derived from SCP03 S-MAC Static Key using KBKDF	Stored & optionally masked in RAM	N/A	N/A	Zeroized when secure channel is closed
SCP03 R-MAC Session Key	Derived from SCP03 S-MAC Static Key using KBKDF	Stored & optionally masked in RAM	N/A	N/A	Zeroized when secure channel is closed
SCP03 C-ENC Session Key	Derived from SCP03 S-ENC Static Key using KBKDF	Stored & optionally masked in RAM	N/A	N/A	Zeroized when secure channel is closed
AES Keys	Internally via FIPS Approved DRBG with the “Generate Symmetric Key” service	Stored & optionally masked in EEPROM	Wrapped by AES-KW, AES-KWP, SCP03 session, or	Wrapped by AES-KW, AES-KWP, SCP03	Delete key Service or zeroized when user is deleted

Key Name	Generation	Storage	Entry	Output	Destruction
			directly entered in plaintext	session, or directly output in plaintext	
Secure Password password	Externally generated	SHA-256 Hash stored in EEPROM	Wrapped by SCP03 session or by Secure Password AES key	N/A	Zeroized when user is deleted. Also zeroized when the user is locked with bSecurityOption set to 1
Secure Password AES key	Externally generated	Stored & optionally masked (1) in EEPROM	Wrapped by SCP03 session	N/A	Zeroized when user is deleted. Also zeroized when the user is locked with bSecurityOption set to 1

(1) The Key is Xor-ed with random data in order to avoid having them in plaintext in memory; this obfuscation operation provides no FIPS approved or allowed security.

2.2 Public Keys

Table 8 - Public Keys

Key	Description / Usage
N/A	N/A

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, the *User* and the *Administrator* (Cryptographic Office). The cryptographic module enforces the separation of roles using identity-based authentication mechanisms. It is identity based because keys and passwords used for the authentication are unique to each other.

Table 9 lists all operator roles supported by the module. The Module does not support a maintenance role. The Module does not support concurrent operators.

Table 9 - Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Approved-Administrator (CO)	The administrator authenticates to manage the approved roles authentication data and perform approved-only cryptographic operations and key sizes.	Knowledge of a Shared Secret	AES S-ENC Key and AES S-MAC Key OR Secure Password password and Secure Password AES key
Approved-user (User)	A user is authenticated to perform general security services and approved-only cryptographic operations and key sizes.	Knowledge of a Shared Secret	AES S-ENC Key and AES S-MAC Key OR Secure Password password and Secure Password AES key

3.2 Authentication Methods

3.2.1 Secure Channel Protocol 03

Knowledge of 128, 192 or 256-bit AES Keys (S-ENC and S-MAC) provides at least 128 bits of security. The probability of a random attempt or a false acceptance occurring is then at least 1 in 2^{128} which is less than 1 in 1,000,000. For multiple attempts in a one-minute period, the device will lock out after a maximum of 127 failed authentication attempts. Therefore, the probability of a random attempt succeeding within a one-minute period is 127 in 2^{128} which is less than 1 in 100,000.

3.2.2 Secure Password

Knowledge of a 128, 192 or 256-bit AES-CBC Key (Secure Password AES Key) provides 128 bits of security. The probability of a random attempt or a false acceptance occurring is then 1 in 2^{128} which is less than 1 in 1,000,000. For multiple attempts in a one-minute period, the device will lock out after a maximum of 127 failed authentication attempts. Therefore, the probability of a random attempt succeeding within a one-minute period is 127 in 2^{128} which is less than 1 in 100,000.

Remark: When operator is locked (Lock Mechanism), authentication data, files and keys owned by this operator are deleted. Folders owned by the operator are not deleted.

Table 10 - Authentication Description

Authentication Method	Probability	Justification
Knowledge of Shared Secret	2^{128}	See chapter Authentication Methods

3.3 Services

3.3.1 Approved Services

All services implemented by the Module are listed in the table(s) below.

Table 11 - Authenticated Services

Service	Description	CO	U
Initialize Update	Used for generation of session keys to setup secure channel and authenticate its message contents	X	X
External Authenticate	Allows transmission of authentication data	X	X
Submit Secure Password	Used to generate the challenge and transmission of authentication data	X	X
Manage Authentication Data	Authenticated administrator can add, delete or modify authentication data of any approved operators. Authenticated operator can update their own authentication data (change password or static keyset)	X	X
Get Authentication Info	Returns authentication method, roles access, security level, number of authentication attempts remaining, sequence counter	X	X
Cancel Authentication	Returns module to un-authenticated state	X	X
Put Key	Electronically enters key. Key may be encrypted by the “AES Key” (with AES-KW or AES-KWP as per SP800-38F), SCP03, or directly entered in plaintext	X	X
Read Key	Electronically outputs key. Key may be encrypted by the “AES Key” (with AES-KW or AES-KWP as per SP800-38F), SCP03, or directly output in plaintext	X	X
Delete Key	Zeroizes keys	X	X
Initialize Algorithm	Initializes cryptographic algorithm with key and algorithm specific parameters	X	X
Encrypt/Decrypt Message	Performs data encryption/decryption of provided message	X	X
Generate/Verify Signature	Generates AES CMAC signature on incoming messages or verifies incoming message and signature	X	X
Generate Symmetric Key	Generates and stores a symmetric key utilizing internal approved DRBG	X	X
Compute Message Digest	Computes a digest of provided message	X	X

Service	Description	CO	U
Generate Random	Generates random data utilizing internal DRBG	X	X
GPIO command set	Provides access to General Purpose I/O pin data (no CSP access)	X	X
File System Command set	Read/ Delete/ Modify files, folder, and access permissions of internal filesystem (no CSP access)	X	X
Get Info (Get Status)	Provides current status of the module, and returns FIPS mode indicator	X	X
Self-Tests	Executes the suite of self-test	X	X
Test Command set	Dummy commands for integration testing purposes (no CSP access)	X	X

Table 12 – Unauthenticated Services

Service	Description
Self-Tests	Executes the suite of self-tests as a result of a power cycle.

Table 13 defines the relationship between access to Security Parameters and the different Approved services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

Table 13 - Security Parameters Access by Service

Service	CSPs										
	SCP03 S-ENC	SCP03 S-MAC	SCP03 C-MAC	SCP03 R-MAC	SCP03 C-ENC	Secure Password password	Secure Password AES key	AES keys	CTR_DRBG Key	CTR_DRBG V	Entropy
Initialize Update	E	E	G, Z	G, Z	G, Z	-	-	-	E, G	E, G	E, G, Z
External Authenticate	-	-	E	E	E	-	-	-	-	-	-
Submit Secure Password	-	-	Z	Z	Z	E	E	-	E, G	E, G	E, G, Z
Manage Authentication Data	G, I, Z	G, I, Z	E, G, I, Z	E, G, I, Z	E, G, I, Z	G, I, Z	G, I, Z	-	-	-	-
Get Authentication Info	-	-	E	E	E	-	-	-	-	-	-
Cancel Authentication	-	-	Z	Z	Z	-	-	-	-	-	-
Put Key	-	-	E	E	E	-	-	E, I	-	-	-
Read Key	-	-	E	E	E	-	-	E, O	-	-	-

Service	CSPs										
	SCP03 S-ENC	SCP03 S-MAC	SCP03 C-MAC	SCP03 R-MAC	SCP03 C-ENC	Secure Password password	Secure Password AES key	AES keys	CTR_DRBG Key	CTR_DRBG V	Entropy
Delete Key	-	-	E	E	E	-	-	Z	-	-	-
Initialize Algorithm	-	-	E	E	E	-	-	E	-	-	E, G
Encrypt/Decrypt Message	-	-	E	E	E	-	-	E	-	-	-
Generate/Verify Signature	-	-	E	E	E	-	-	E	-	-	-
Generate Symmetric Key	-	-	E	E	E	-	-	G	G, E	G, E	E, G
Compute Message Digest	-	-	E	E	E	-	-	-	-	-	-
Generate Random	-	-	E	E	E	-	-	-	G, E	G, E	E, G
GPIO command set	-	-	E	E	E	-	-	-	-	-	-
File System Command set	-	-	E	E	E	-	-	-	-	-	-
Get Info (Get Status)	-	-	E	E	E	-	-	-	-	-	-
Self-Tests	-	-	E	E	E	-	-	E	G, E	G, E	E, G
Test Command set	-	-	E	E	E	-	-	-	-	-	E, G
Self-Tests (power cycle)	-	-	-	-	-	-	-	-	-	-	E, G

3.3.2 Non-Approved Services

All services available in the Approved mode are available in the non-Approved mode with the following additional service listed in Table 14 being exclusive to the non-Approved mode.

Table 14 – Additional Non-Approved Services

Service	Description
Submit Password	Submits plaintext password

4 Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power up self-tests are available on demand by power cycling the module.

All algorithm Known Answer Tests (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 infinite loop error state.

The module performs the following algorithm KATs on power-up.

- Firmware Integrity: 16-bits CRC
- AES-GCM-128 encrypt and decrypt KATs (CAVP Cert. #A2384)
- AES CMAC-128 generate and verify KATs (CAVP Cert. #A2384)
- AES ECB, CBC, OFB, CFB and CTR KATs (CAVP Cert. #A2383)
- SP 800-90A CTR_DRBG KAT for instantiate, generate and reseed functions
- SHA-224, SHA-256, SHA-384 and SHA-512 KAT
- SP 800-108 KBKDF-CTR 128 bits KAT

The module performs the following conditional self-tests as indicated.

- ENT (P): SP800-90B Health Tests (i.e., APT and RCT); performed at power-on and continuously.
- DRBG: SP800-90A Health Tests (i.e., Instantiate, Generate, Reseed); performed at each use.

5 Physical Security Policy

The module is a single-chip embodiment per FIPS 140-2 definitions and provides a production-grade, hard, opaque, removal-resistant packaging that satisfies the requirements of Level 3 physical security.

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Module does not contain a modifiable operational environment.

7 Mitigation of Other Attacks Policy

The module does not claim to mitigate any attacks beyond the scope of FIPS 140-2 requirements.

8 Security Rules and Guidance

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

1. The cryptographic module shall provide two distinct operator roles. These are the Approved User role and the Cryptographic Officer role.
2. The module provides identity-based authentication.
3. The module shall clear previous authentications on power cycle.

4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

5. The cryptographic module shall perform the following tests:

   a. Power up Self-Tests
   – Firmware Integrity Test – 16-bit CRC
   – AES-GCM 128-bit Encrypt and Decrypt Known Answer Tests
   – AES-CMAC 128-bit Generate and Verify Known Answer Tests
   – DRBG Known Answer Test (Instantiate, Generate, Reseed)
   – SHA-224, SHA-256, SHA-384 and SHA-512 KAT
   – SP800-108 KDF-CTR 128 bits KAT

   b. Critical Functions Tests
   – N/A

   c. Conditional Self-Tests
   – SP800-90A DRBG Health Tests
   – SP800-90B ENT (P) Health Tests (RCT and APT)

6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module
7. Power up self-tests do not require any operator action.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module does not support concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support manual key entry.
14. The module does not have any proprietary external input/output devices used for entry/output of data.
15. The module does not output intermediate key values.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 - References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 2, *March 2019*
[133]	*NIST Special Publication 800-133, Revision 2, Recommendation for Cryptographic Key Generation, June 2020*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*

Table 16 - Accronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard algorithm as defined in FIPS PUB 197
ASSP	Application Specific Standard Product
CBC	Cipher Block Chaining method applied to block ciphers
CFB	Cipher Feedback Register chaining method applied to block ciphers
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
DRBG	Deterministic Random Bit Generator as defined in SP 800-90
ECB	Electronic Code Book chaining method applied to block ciphers
FIPS	Federal Information Processing Standards
MAC	Message Authentication Code - A bit string of fixed length, computed by a MAC generation algorithm, that is used to establish the authenticity and, hence, the integrity of a message.
Master	The device that initiates and terminates a transmission. The Master also generates the clock for synchronous interface.
NIST	National Institute of Standards and Technology
OFB	Output Feedback Register chaining method applied to block ciphers
OS	Operating Systems
Receiver	The device reading data from the bus
SCP	Secure Channel Protocol as defined by GlobalPlatform v2.2
SHA	Secure Hash Algorithm as defined in FIPS PUB 180-4
Slave	The device addressed by a master