SEALSQ

VaultIC408 1.2.4 - Level 2

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0
Date: August 05, 2026

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 1.2.4.1 of the VaultIC408 1.2.4. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows in Table 1:

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

Table 1: Security Levels

2 Cryptographic Module Specification

The WISeKey VaultIC408 1.2.4 – Level 2, hereafter denoted as “the module” or “VaultIC™”, 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.

The VaultIC™ supports both an Approved and a non-Approved mode of operation, automatically selected according to device state and authenticated operator. The selected mode of operation remains activated while the operator is authenticated. The mode of operation is discarded when the operator logs out or the secure channel is terminated.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated Security Modules.

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.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics:

Cryptographic Boundary:

The block diagram of the Module is depicted in Figure 1. The Module is a Hardware single-chip embodiment. The cryptographic boundary is denoted with the dashed blue line in Figure 1.

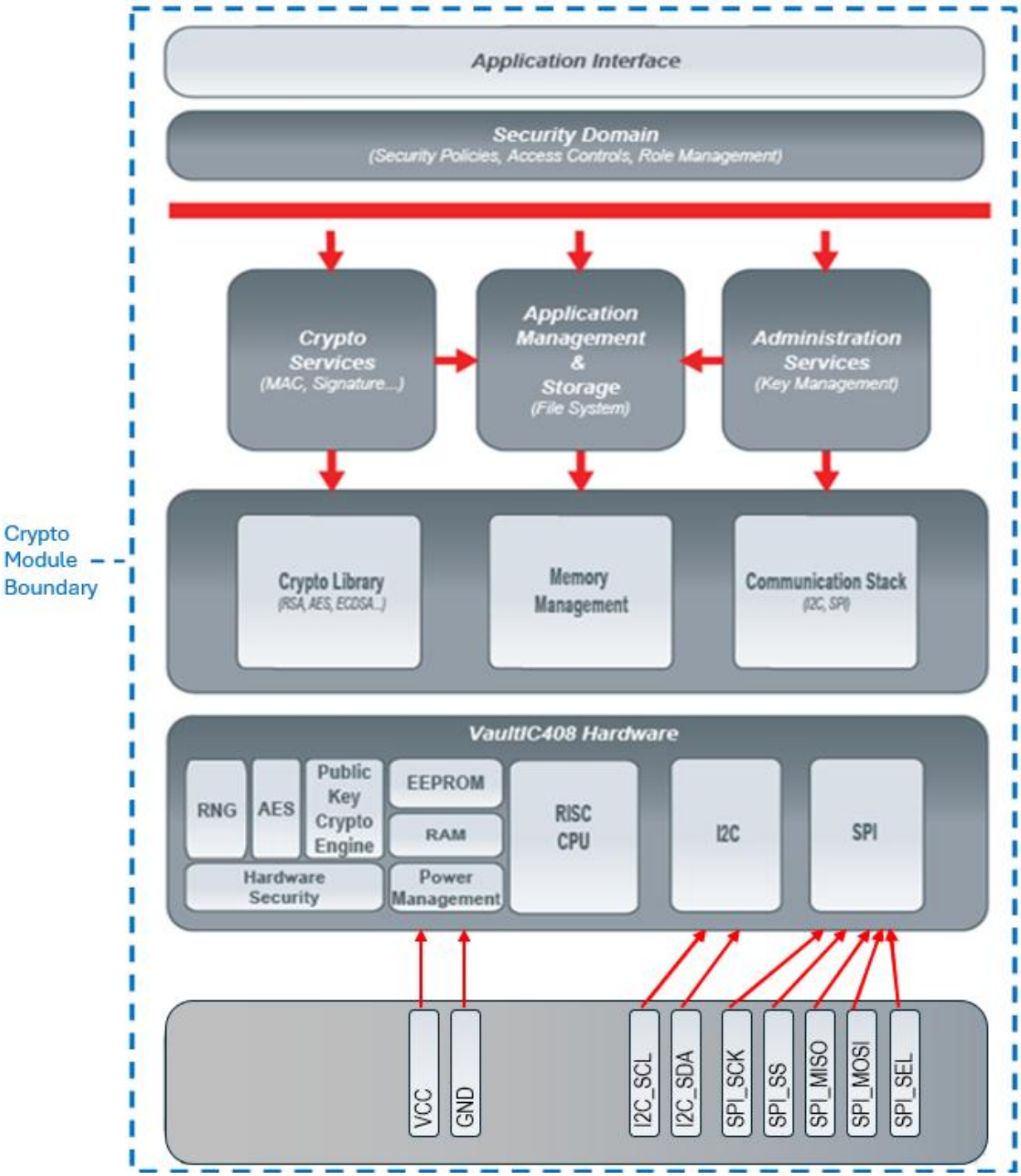
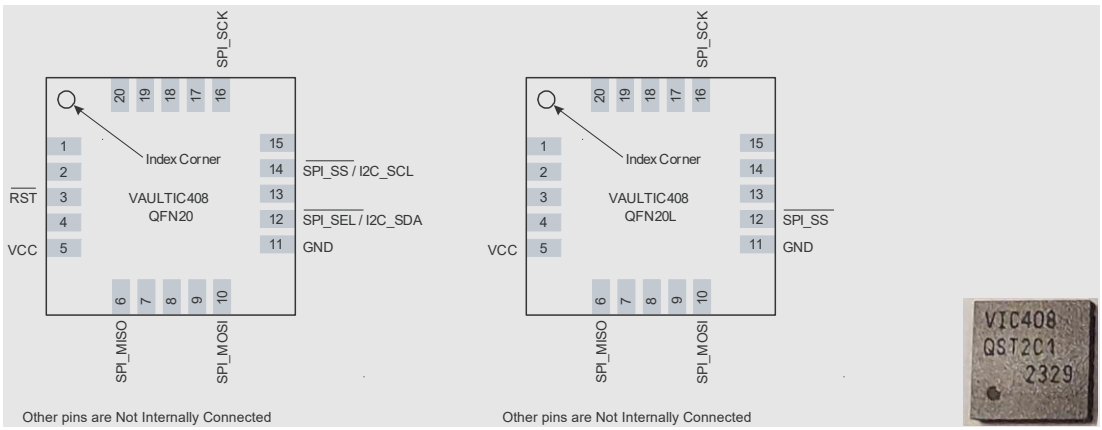


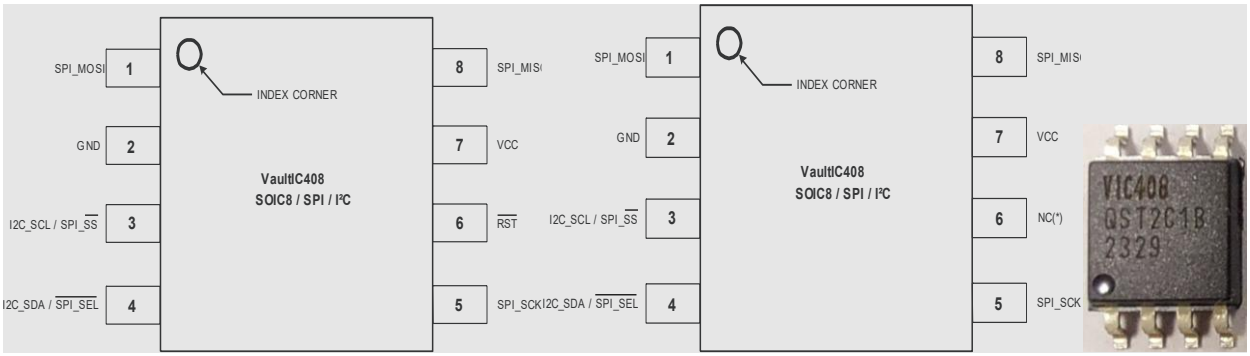
Figure 1 – Module Block Diagram

The module is delivered in two packages:

- QFN20 with and without reset pin



- SOIC8 with and without reset pin



2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware**:**

VaultIC408 1.2.4 – Level 2 cryptographic module is tested on the following operational environment.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
VaultIC408 1.2.4 - Level 2: SOIC8 with Reset	AT90SO28RS rev A	1.2.4.1	AVR Secure Processor	Communication interface SPI or I2C Package SOIC8 with reset pin
VaultIC408 1.2.4 - Level 2: SOIC8 without Reset	AT90SO28RS rev A	1.2.4.1	AVR Secure Processor	Communication interface SPI or I2C Package SOIC8 without reset pin
VaultIC408 1.2.4 - Level 2: QFN20 with Reset	AT90SO28RS rev A	1.2.4.1	AVR Secure Processor	Communication interface SPI or I2C Package QFN20 with reset pin
VaultIC408 1.2.4 - Level 2: QFN20 without Reset	AT90SO28RS rev A	1.2.4.1	AVR Secure Processor	Communication interface SPI or I2C Package QFN20 without reset pin

Table 2: Tested Module Identification – Hardware

Tested Operational Environments - Software, Firmware, Hybrid:
N/A for this module.
Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:
N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	when the device is in ACTIVATED state and an approved user or an approved administrator is successfully authenticated	Approved	Show Version (Get Info) command returns bMode = Approved_Mode
Non-Approved mode	when the device is in ACTIVATED state and a non-approved user or a non-approved administrator is authenticated	Non-Approved	Show Version (Get Info) command returns bMode = Non_Approved_Mode

Table 3: Modes List and Description

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 mode of operation is completely separated from the point of authentication. There are Approved operators and non-Approved operators. The Approved operator cannot access any non-Approved services and vice-versa. In order to transition between modes, the operator must log out and re-authenticate with the mode-specific operator's credentials for the mode desired. 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.

Configuration of the 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 supported. Additional security restrictions may apply.

The module will indicate that it is running in the Approved mode of operation by indicating Mode of Operation: Approved in the response of a Show Version (Get Info) command, as described below:

-> 80 01 01 00 37
<- 56 61 75 6C 74 49 43 34 30 38 20 31 2E 32 2E 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 01 01 00 00 3D 80 03 00 10 00 00 08 03 90 00

In this response:

- The 41st byte (0x07) indicates that the device is in ACTIVATED state.
- The 43rd byte (0x01) indicates that the current authenticated user is an approved user.
- The 44th byte (0x01) indicates that the current mode of operation is approved.

Configuration of the non-Approved Modes 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 Approved, Allowed, and Non-Approved Algorithms are supported.

The module will indicate that it is running in the non-Approved mode of operation by indicating Mode of Operation: non-approved mode in the response of a Show Version (Get Info) command, as described below:

-> 80 01 01 00 37
56 61 75 6C 74 49 43 34 30 38 20 31 2E 32 2E 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 02 02 00 00 3D 80 03 00 10 00 00 08 03 90 00

In this response:

- The 41st byte (0x07) indicates that the device is in ACTIVATED state.
- The 43rd byte (0x02) indicates that the current authenticated user is a non-approved user.
- The 44th byte (0x02) indicates that the current mode of operation is non-approved.

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.

Mode Change Instructions and Status:

When the module is in ACTIVATED state, the mode is selected automatically when a user or admin is authenticated. Session SSPs are zeroised upon session initialization and termination.

2.5 Algorithms

Approved Algorithms:

The Module implements the Approved cryptographic algorithms listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4856	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A4856	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A5349	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A4856	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4856	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5349	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5349	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5349	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A5349	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A4856	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
Counter DRBG	A5349	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A5349	Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Secret Generation Mode - Extra Bits	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A5349	Curve - B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A5349	Component - No Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5349	Component - No Curve - B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A5349	Key Length - Key Length: 80-512 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5349	Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5349	Key Length - Key Length: 128-512 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5349	Key Length - Key Length: 192-1024 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A5349	Key Length - Key Length: 256-1024 Increment 8	FIPS 198-1
KAS-ECC Sp800-56Ar3	A5349	Domain Parameter Generation Methods - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Function - Full Validation, Key Pair Generation, Partial Validation Scheme - onePassDh - KAS Role - Responder KDF Methods - oneStepKdf - Key Length - 512 staticUnified - KAS Role - Responder KDF Methods - oneStepKdf - Key Length - 512	SP 800-56A Rev. 3
KDF SP800-108	A5349	KDF Mode - Counter Supported Lengths - Supported Lengths: 256	SP 800-108 Rev. 1
RSA KeyGen (FIPS186-4)	A5349	Key Generation Mode - B.3.3 Modulo - 2048 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A5349	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048	FIPS 186-4
RSA SigVer (FIPS186-4)	A5349	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048	FIPS 186-4
SHA-1	A5349	Message Length - Message Length: 160, 0-65528 Increment 8	FIPS 180-4
SHA2-224	A5349	Message Length - Message Length: 224, 0-65528 Increment 8	FIPS 180-4
SHA2-256	A5349	Message Length - Message Length: 256, 0-65528 Increment 8	FIPS 180-4
SHA2-384	A5349	Message Length - Message Length: 384, 0-65528 Increment 8	FIPS 180-4
SHA2-512	A5349	Message Length - Message Length: 512, 0-65528 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The Module implements the Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	NIST SP 800-133rev2, Section 4 Example 1, Sections 5.1, 5.2, and 6.1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not implement any Non-Approved, but Allowed Algorithms in the Approved Mode of Operation.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The Module implements the Non-Approved, Allowed cryptographic Algorithms with No Security Claimed.

Name	Caveat	Use and Function
RAM Scrambling	No security claimed - IG 2.4.A, Example Scenario #1.	Volatile memory is scrambled/obfuscated using a proprietary algorithm; all contents of RAM are treated as unprotected plaintext.

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

The Module implements the Non-Approved, Not Allowed cryptographic algorithms listed.

Name	Use and Function
CIP_RSAES (non-compliant)	PKCS#1 v2.1 RSAES-OAEP, RSAES-PKCS1-v1_5, or x509 raw cipher
KAS (non-compliant)	Key Agreement Scheme, compound of: - Static Unified Model, One-Pass Diffie-Hellman Model, defined by ANS X9.63 and NIST SP 800-56A (GFp, GF2m)
KPG_RSAES (non-compliant)	RSA key pair generation for cipher engines
KTS_RSA_OAEP_BASIC (non-compliant)	NIST SP 800-56B Key Transport Scheme based on RSAES OAEP algorithm without key confirmation
RSA (non-compliant)	1024-bit RSA Signature Generation used to sign the logs output from the Module. RSA X.509 signature generation/verification algorithm only applies the RSA primitive without any message encoding or padding
None	None

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

The table below shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
AKP-DP	AsymKeyPair-DomPar	Asymmetric Key-Pair Generation Domain Parameters	Publications:NIST FIPS 186-5, SP 800-90Ar1	KAS-ECC Sp800-56Ar3: (A5349)
AKP-KG	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation	Publications:NIST FIPS 186-5, SP 800-90Ar1, SP 800-133r2, IG D.H	CKG: () Key Type: Symmetric and Asymmetric ECDSA KeyGen (FIPS186-4): (A5349) RSA KeyGen (FIPS186-4): (A5349)
AKP-KV	AsymKeyPair-KeyVer	Asymmetric Key-Pair Verification	Publications:NIST FIPS 186-5	ECDSA KeyVer (FIPS186-4): (A5349)
BC-A-DEC	BC-Auth	Block Cipher - Authenticated Decrypt	Publications:NIST SP 800-38F, SP 800-38D	AES-GCM: (A5349)
BC-A-ENC	BC-Auth	Block Cipher - Authenticated Encrypt	Publications:NIST SP 800-38F, SP 800-38D	AES-GCM: (A5349)
BC-U-DEC	BC-UnAuth	Block Cipher - Unauthenticated Decrypt	Publications:NIST FIPS 197, SP 800-38A	AES-CBC: (A4856) AES-CFB128: (A4856) AES-CTR: (A4856) AES-ECB: (A4856) AES-OFB: (A4856)
BC-U-ENC	BC-UnAuth	Block Cipher - Unauthenticated Encrypt	Publications:NIST FIPS 197, SP 800-38A	AES-CBC: (A4856) AES-CFB128: (A4856) AES-CTR: (A4856) AES-ECB: (A4856)

Name	Type	Description	Properties	Algorithms
				AES-OFB: (A4856)
EC-SigGen	DigSig-SigGen	Digital Signature Generation	Publications:NIST FIPS 186-5, SP 800-90Ar1, FIPS 180-4	ECDSA SigGen (FIPS186-4): (A5349) SHA2-224: (A5349) SHA2-256: (A5349) SHA2-384: (A5349) SHA2-512: (A5349)
EC-SigVer	DigSig-SigVer	Digital Signature Verification	Publications:NIST FIPS 186-5, SP 800-90Ar1, FIPS 180-4	ECDSA SigVer (FIPS186-4): (A5349) SHA-1: (A5349) SHA2-224: (A5349) SHA2-256: (A5349) SHA2-384: (A5349) SHA2-512: (A5349)
Entropy	ENT-ESV	Entropy Source	Publications:NIST SP 800-90B, IG 9.3.A, D.J	Counter DRBG: (A5349)
Hash	SHA	Secure Hash	Publications:NIST FIPS 180-4	SHA-1: (A5349) SHA2-224: (A5349) SHA2-384: (A5349) SHA2-512: (A5349)
KAS-ECC	KAS-Full	Key Agreement	Publications:NIST SP 800-56Ar3, SP 800-90Ar1, FIPS 180-4 IG:IG D.F Scenario 2, path (2), end-to-end Key Confirmation:yes Key Derivation:KDA (tested as part of KAS certificate)	KAS-ECC Sp800-56Ar3: (A5349)

Name	Type	Description	Properties	Algorithms
			Caveat:Key establishment methodology provides between 112 and 256 bits of security strength	
KAS-KG	KAS-KeyGen	Key Agreement Key-Pair Generation	Publications:NIST SP 800-56Ar3, SP 800-90Ar1, FIPS 186-5	CKG: () Key Type: Symmetric and Asymmetric KAS-ECC Sp800-56Ar3: (A5349)
KBKDF	KBKDF	Key-Based Key Derivation	Publications:NIST SP 800-108-r1-upd1	AES-CMAC: (A5349) HMAC-SHA2-224: (A5349) HMAC-SHA2-256: (A5349) HMAC-SHA2-384: (A5349) HMAC-SHA2-512: (A5349) KDF SP800-108: (A5349)
KDA	KAS-56CKDF	Key Derivation Function	Publications:NIST SP 800-56Ar3, SP 800-56Cr2	SHA2-256: (A5349) KAS-ECC Sp800-56Ar3: (A5349)
KTS	KTS-Wrap KTS-Unwrap	Key Transport - Wrapping	Publications:NIST FIPS 197, SP 800-38F IG D.G:Approved method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-KW: (A5349) AES-KWP: (A5349)
KTS-SCP03	KTS-Wrap KTS-Unwrap	Key Transport - Wrapping using Secure Channel Protocol 03	Publications:NIST FIPS 197, SP 800-38F IG D.G:Approved	AES-CBC: (A4856) AES-CMAC: (A5349)

Name	Type	Description	Properties	Algorithms
			method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	
MAC-CMAC	MAC	Message Authentication Code Generation - CMAC	Publications:NIST FIPS 197, SP 800-38B	AES-CMAC: (A5349)
MAC-GMAC	MAC	Message Authentication Code Generation - GMAC	Publications:NIST FIPS 197, SP 800-38D	AES-GMAC: (A5349)
MAC-HMAC	MAC	Message Authentication Code Generation - HMAC	Publications:NIST FIPS 198-1, FIPS 180-4	HMAC-SHA-1: (A5349) HMAC-SHA2-224: (A5349) HMAC-SHA2-256: (A5349) HMAC-SHA2-384: (A5349) HMAC-SHA2-512: (A5349)
RBG	DRBG	Random Number Generation	Publications:NIST SP 800-90Ar1	Counter DRBG: (A5349)
RSA-SigGen	DigSig-SigGen	Digital Signature Generation	Publications:NIST FIPS 186-5, SP 800-90Ar1, FIPS 180-4	RSA SigGen (FIPS186-4): (A5349) SHA2-224: (A5349) SHA2-256: (A5349) SHA2-384: (A5349) SHA2-512: (A5349)
RSA-SigVer	DigSig-SigVer	Digital Signature Verification	Publications:NIST FIPS 186-5, SP 800-90Ar1, FIPS 180-4	RSA SigVer (FIPS186-4): (A5349) SHA-1: (A5349) SHA2-224:

Name	Type	Description	Properties	Algorithms
				(A5349) SHA2-256: (A5349) SHA2-384: (A5349) SHA2-512: (A5349)
SymGen	CKG	Symmetric Key Generation	Publications:NIST SP 800-90Ar1, SP 800-133r2, IG D.H	CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A5349)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM IV Uniqueness

FIPS 140-3 IG C.H, Option 2

The IV is uniform-randomly generated internally in its entirety.

The generation uses an Approved DRBG (Cert. #A5349) that is internal to the module's boundary.

The IV length shall be at least 96 bits (per SP 800-38D).

KAS Implementation

FIPS 140-3 IG D.F, Scenario 2, Path 2

The module's implementation of KAS-ECC has been tested end-to-end under CAVP Cert. #A5349, which is inclusive of shared secret calculation, key derivation, and key confirmation.

SHA-1 Transition

The module supports the limited use of SHA-1 for non-digital signature applications, as well as digital signature verifications for legacy purposes. The module does not support digital signature generation with the use of SHA-1. Per CMVP Programmatic Transitions and NIST SP 800-131Ar2, usage of SHA-1 for non-digital-signature applications is deprecated through Dec 31, 2030.

2.8 RBG and Entropy

Cert Number	Vendor Name
E2	WISeKey

Table 9: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
VaultIC408 Entropy Source	Physical	AVR Secure Processor	1 bit	0.52427	NA

Table 10: Entropy Sources

2.9 Key Generation

The module implements the Key Generation Functions described in Section 9.4. The module supports a CTR_DRBG (CAVP Cert. A5349) and an internal entropy source (ESV Cert. E2) for the purposes of key generation.

The length of the DRBG-EI and Seed used to instantiate the CTR_DRBG is 736 bits. At a min_entropy rate of 0.52427 bits per bit sampled, the 736 bits of output can be construed as containing at least 384 bits of entropy (i.e., 736 * 0.52427 = 385.86272), which is sufficient to claim the full security strength of 256 bits for the CTR_DRBG.

2.10 Key Establishment

Key Agreement Information

The module implements the Key Agreement Functions described in Section 9.4. The module supports KAS-ECC for the purposes of key agreement.

Key Transport Information

The module implements the Key Transport Functions described in Section 9.4. The module supports key transport using NIST SP 800-38F compliant methods, which include:

- AES-KW, AES-KWP
- AES-CBC with AES-CMAC

2.11 Industry Protocols

The module does not implement any Industry Protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below. The module does not support a Control Output interface.

Physical Port	Logical Interface(s)	Data That Passes
SPI_SCK	Control Input	SPI Clock
SPI_MISO	Data Output Status Output	SPI Master In, Slave Out
SPI_MOSI	Data Input Control Input	SPI Master Out, Slave In
SPI_SS	Control Input	SPI Slave Select
I2C_SCL	Control Input	I2C Clock

Physical Port	Logical Interface(s)	Data That Passes
SPI_SEL	Control Input	SPI or I2C Selection
I2C_SDA	Data Input Data Output Control Input Status Output	I2C Data Line
VCC	Power	Power Supply
GND	Power	Ground

Table 11: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Module's authentication methods are listed in Table 12.

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 most 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 at most 127 in 2^{128} which is less than 1 in 100,000.

Secure Password Key

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 at most 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 at most 127 in 2^{128} which is less than 1 in 100,000.

Remark: When operator is deleted (through the Manage Authentication Data service), authentication data, files and keys owned by the operator are zeroized.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
SCP03	The CO/User is authenticated to the module through a Secure Channel Protocol 03 Authentication method	BC-U-ENC	Minimum 2^128	The probability of a random attempt succeeding within a one-minute period is at most 127 in 2^128, which is less than 1 in 100,000.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Secure Password Key	The CO/User is authenticated to the module through a Secure Password Key Authentication method	BC-U-ENC	Minimum 2^128	The probability of a random attempt succeeding within a one-minute period is at most 127 in 2^128, which is less than 1 in 100,000.

Table 12: Authentication Methods

4.2 Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). The module also supports an Unauthenticated role, which does not require any authentication. The cryptographic module enforces the separation of roles using operator IDs and authentication methods. The module does not support changing roles. Re-authentication is enforced when logging in under a new roles/user. The module does not support concurrent operators.

The Roles Table below lists all operator roles supported by the Module.

The Module does not support an operator changing roles.

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer	Identity	CO	SCP03 Secure Password Key
User	Identity	User	SCP03 Secure Password Key
Everyone	Role	Unauthenticated	None

Table 13: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Cancel Authentication	Returns module to un-authenticated state	Status Word	None	Status Word	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: Z - SCP03 R-MAC: Z - SCP03

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						C-ENC: Z User - SCP03 C-MAC: Z - SCP03 R-MAC: Z - SCP03 C-ENC: Z
Compute Message Digest	Computes a digest of provided message	Status Word	Message	Message digest + Status word	BC-U-ENC BC-U-DEC MAC-CMAC Hash	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E
Delete Key	Zeroizes keys	Status Word	Key ID	None	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Transport Key: Z - AES Keys: Z - MAC Keys: Z - RSA Signing Key: Z - ECC Signing Key: Z - RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Verifying Key: Z - ECC Verifying Key: Z - KAS Private Key: Z - KAS Public Key: Z User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Transport Key: Z - AES Keys: Z - MAC Keys: Z - RSA Signing Key: Z - ECC Signing Key: Z - RSA Verifying Key: Z - ECC Verifying Key: Z - KAS Private Key: Z - KAS Public Key: Z
Derive Secret Key	Derives a secret key suitable for	Status Word	Key ID + KDF ID +	Key derivation	BC-U-ENC	Cryptographic Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	later cryptographic use from a shared secret value		Digest ID + Key confirmation policy + Key ID storage + Access control	response + Status word	BC-U-DEC RBG Entropy KDA KAS-KG MAC-CMAC	- SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - KAS Private Key: G - KAS Public Key: G - KAS Shared Secret: E - DRBG-State: G,E - DRBG-EI and Seed: G,E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - KAS Private Key: G - KAS Public Key: G - KAS Shared Secret: E - DRBG-State: G,E - DRBG-EI and Seed: G,E
Encrypt/Decrypt Message	Performs data encryption/decryption of provided message	Status Word	Message	Response message + Status word	BC-A-ENC BC-A-DEC	Cryptographic Officer - SCP03 C-MAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					BC-U-ENC BC-U-DEC MAC-CMAC	- SCP03 R-MAC: E - SCP03 C-ENC: E - AES Keys: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Keys: E
Establish Key Material	Computes a shared secret value utilizing internal approved DRBG	Status Word	ECC private key ID + KAS ID + Shared secret ID + Access control + Status word	Status Word	BC-U-ENC BC-U-DEC RBG Entropy KAS-ECC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - KAS Private Key: E - KAS Public Key: E - KAS Shared Secret: G - DRBG-State: G,E - DRBG-EI and Seed: G,E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - KAS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: E - KAS Public Key: E - KAS Shared Secret: G - DRBG-State: G,E - DRBG-EI and Seed: G,E
External Authenticate	Allows transmission of authentication data	Status Word	SCP03 security level + External Authenticate SCP03 data	Status word	BC-U-ENC BC-U-DEC MAC-CMAC MAC-GMAC MAC-HMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E
File System Command set	Read/Delete/Modify files, folder, and access permissions of internal filesystem (no CSP access)	Status Word	Command	Command response	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E
Generate Key Pair	Generates and stores an	Status Word	Key pair identifier +	Status Word	AKP-DP AKP-KG	Cryptographic Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	asymmetric key pair utilizing internal approved DRBG		Key ID + Access condition + Algorithm parameters		AKP-KV BC-U-ENC BC-U-DEC RBG Entropy KAS-KG MAC-CMAC	- SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - RSA Signing Key: G - ECC Signing Key: G - RSA Verifying Key: G - ECC Verifying Key: G - KAS Private Key: G - KAS Public Key: G - DRBG-State: E,G - DRBG-EI and Seed: G,E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - RSA Signing Key: G - ECC Signing Key: G - RSA Verifying Key: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- ECC Verifying Key: G - KAS Private Key: G - KAS Public Key: G - DRBG-State: G,E - DRBG-EI and Seed: G,E
Generate Random	Generates random data utilizing internal DRBG	Status Word	Length of random	Random value + Status word	BC-U-ENC BC-U-DEC RBG Entropy MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - DRBG-State: G,E - DRBG-EI and Seed: G,E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - DRBG-State: G,E - DRBG-EI and Seed: G,E
Generate Symmetric Key	Generates and stores a symmetric key utilizing internal approved DRBG	Status Word	Key ID + access condition + AES Key Identifier	Status Word	BC-U-ENC BC-U-DEC SymGen	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					RBG Entropy MAC-CMAC	- SCP03 C-ENC: E - AES Keys: G - DRBG-State: G,E - DRBG-EI and Seed: G,E - AES Transport Key: G - MAC Keys: G User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Keys: G - DRBG-State: G,E - DRBG-EI and Seed: G,E - AES Transport Key: G - MAC Keys: G
Generate/Verify Signature	Generates signature on incoming messages or verifies incoming message and signature	Status Word	Message	Signature or None + Status word	BC-U-ENC BC-U-DEC EC-SigGen RSA-SigGen EC-SigVer RSA-SigVer	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - MAC Keys: E - RSA Signing

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					MAC-CMAC MAC-GMAC MAC-HMAC	Key: E - ECC Signing Key: E - RSA Verifying Key: E - ECC Verifying Key: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - MAC Keys: E - RSA Signing Key: E - ECC Signing Key: E - RSA Verifying Key: E - ECC Verifying Key: E
Get Authentication Info	Returns information pertinent to operator	Status Word	User ID	Authentication methods, roles access, security level, number of authentication attempts remaining, sequence counter +	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				Status word		- SCP03 C-ENC: E
Get Config	Provides configuration data that is not available in the Show Version (Get Info) command	Status Word	Length of config to read	Value requested + Status word	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E
Get Data (Show Status)	Provides periodic self-tests information	Status Word	ID of the value to read	Value requested + Status word	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E
Get Error Log	Provides error log information	Status Word	None	Log data + Status word	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SCP03 C-ENC: E
Initialize Algorithm	Initializes cryptographic algorithm with key and algorithm specific parameters	Status Word	Key ID + Algorithm mode + Algorithm ID + Algorithm parameter	None or IV for GCM/GMAC + Status word	BC-U-ENC BC-U-DEC EC-SigGen RSA-SigGen EC-SigVer RSA-SigVer Entropy MAC-CMAC MAC-HMAC MAC-GMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - DRBG-EI and Seed: G,E - AES Keys: E - MAC Keys: E - RSA Signing Key: E - ECC Signing Key: E - RSA Verifying Key: E - ECC Verifying Key: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - DRBG-EI and Seed: G,E - AES Keys: E - MAC Keys: E - RSA Signing

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: E - ECC Signing Key: E - RSA Verifying Key: E - ECC Verifying Key: E
Initialize Update	Used for generation of session keys to setup secure channel and authenticate its message contents	Status Word	User ID =+ Role ID + Host challenge	SCP03 response data + Status word	BC-U-ENC BC-U-DEC RBG Entropy KBKDF MAC-CMAC MAC-GMAC MAC-HMAC	Cryptographic Officer - SCP03 S-MAC: E - SCP03 S-ENC: E - SCP03 C-MAC: G,Z - SCP03 R-MAC: G,Z - SCP03 C-ENC: G - DRBG-State: G,E - DRBG-Eland Seed: G,E User - SCP03 S-MAC: E - SCP03 S-ENC: E - SCP03 C-MAC: G,Z - SCP03 R-MAC: G,Z - SCP03 C-ENC: G - DRBG-State: G,E - DRBG-El

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						and Seed: G,E
Key Confirmation	Verifies the MacTagU given by the host and on success, unlocks the access to the Derived Secret key computed during Derive Secret Key	Status Word	Key ID + MacTag value	Status Word	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - MAC Keys: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - MAC Keys: E
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)	Status Word	User ID + Operation identifier + Authentication data update operations	Status word	KTS-SCP03	Cryptographic Officer - SCP03 S-ENC: W,Z - SCP03 S-MAC: W,Z - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - Secure Password: W,Z - Secure Password AES Key: W,Z User - SCP03 S-ENC:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,Z - SCP03 S-MAC: W,Z - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - Secure Password: W,Z - Secure Password AES Key: W,Z
Put Key	Electronically enters keys in plaintext or encrypted in Approved mode with AES-KWP / AES-KW as per NIST SP 800-38F and/or SCP03	Status Word	Key ID + Access condition + Key object data	Status Word	BC-U-ENC BC-U-DEC KTS KTS-SCP03	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Transport Key: W,E - AES Keys: W - MAC Keys: W - RSA Signing Key: W - ECC Signing Key: W - RSA Verifying Key: W - ECC Verifying Key: W - KAS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: W - KAS Public Key: W User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Transport Key: W,E - AES Keys: W - MAC Keys: W - RSA Signing Key: W - ECC Signing Key: W - RSA Verifying Key: W - ECC Verifying Key: W - KAS Private Key: W - KAS Public Key: W
Read Key	Electronically output keys in plaintext or encrypted in Approved mode with AES-KWP / AES-KW as per NIST SP 800-	Status Word	Key ID	Key object + status word	BC-U-ENC BC-U-DEC KTS KTS-SCP03	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	38F and/or SCP03					- AES Transport Key: R,E - AES Keys: R - MAC Keys: R - RSA Signing Key: R - ECC Signing Key: R - RSA Verifying Key: R - ECC Verifying Key: R - KAS Private Key: R - KAS Public Key: R User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E - AES Transport Key: R,E - AES Keys: R - MAC Keys: R - RSA Signing Key: R - ECC Signing Key: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- RSA Verifying Key: R - ECC Verifying Key: R - KAS Private Key: R - KAS Public Key: R
Self-Tests	Executes the suite of self-test	Status Word	None	Status Word		Cryptographic Officer User
Self-Tests (Power Cycle)	Executes the suite of self-tests as a result of a power cycle.	Status Word	None	Status Word	Entropy	Cryptographic Officer - DRBG-EI and Seed: G,E User - DRBG-EI and Seed: G,E Everyone - DRBG-EI and Seed: G,E
Show Version (Get Info)	Provides current status of the module, and returns Approved mode indicator	Status Word	None	Approved mode indicator and module versioning information.	BC-U-ENC BC-U-DEC MAC-CMAC	Cryptographic Officer - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E User - SCP03 C-MAC: E - SCP03 R-MAC: E - SCP03 C-ENC: E Everyone

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Submit Secure Password	Used to generate the challenge and transmission of authentication data	Status Word	User ID + Role ID + None or challenge response	Challenge or none + Status word	BC-U-DEC RBG Entropy	Cryptographic Officer - Secure Password: E - Secure Password AES Key: E - DRBG-State: G,E - DRBG-EI and Seed: G,E,Z User - Secure Password: E - Secure Password AES Key: E - DRBG-State: G,E - DRBG-EI and Seed: G,E,Z

Table 14: Approved Services

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP.

Note: The Indicator of the services is the Status Word (SW) return by the command. 9000h means that the service completed successfully, else the service returns an error code.

4.4 Non-Approved Services

All non-approved services implemented by the Module are listed in the table below, CO and User in this table are non-approved one:

Name	Description	Algorithms	Role
Initialize Update	Used for generation of session keys to setup secure channel and authenticate its message contents	None	CO, User, Everyone
External Authenticate	Allows transmission of authentication data	None	CO, User, Everyone
Submit Secure Password	Used to generate the challenge and transmission of authentication data	None	CO, User, Everyone
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)	None	CO, User
Get Authentication Info	Returns authentication method, roles access, security level, number of authentication attempts remaining, sequence counter	None	CO, User, Everyone
Cancel Authentication	Returns module to un-authenticated state	None	CO, User, Everyone
Put Key	Electronically enters keys in plaintext or encrypted by AES-KWP, NIST SP 800-56B Key Transport, and/or SCP03	KTS_RSA_OAEP_BASIC (non-compliant)	CO, User
Read Key	Electronically outputs keys in plaintext or encrypted by AES-KWP, NIST SP 800-56B Key Transport, and/or SCP03	KTS_RSA_OAEP_BASIC (non-compliant)	CO, User
Delete Key	Zeroizes keys	None	CO, User
Initialize Algorithm	Initializes cryptographic algorithm with key and algorithm specific parameters	None	CO, User
Encrypt/Decrypt Message	Performs data encryption/decryption of provided message	RSA (non-compliant) CIP_RSAES (non-compliant)	CO, User
Generate/Verify Signature	Generates signature on incoming messages or verifies	RSA (non-compliant)	CO, User

Name	Description	Algorithms	Role
	incoming message and signature		
Generate Symmetric Key	Generates and stores a symmetric key utilizing internal approved DRBG	None	CO, User
Generate Key Pair	Generates and stores an asymmetric key pair utilizing internal approved DRBG	RSA (non-compliant) KPG_RSAES (non-compliant)	CO, User
Establish Key Material	Computes a shared secret value utilizing internal approved DRBG	KAS (non-compliant)	CO, User
Derive Secret Key	Derives a secret key suitable for later cryptographic use from a secret value or a static master key	None	CO, User
Key Confirmation	Verifies the MacTagU given by the host and on success, unlocks the access to the Derived Secret key computed during Derive Secret Key	None	CO, User
Compute Message Digest	Computes a digest of provided message	None	CO, User
Generate Random	Generates random data utilizing internal DRBG	None	CO, User, Everyone
File System Command set	Read/ Delete/ Modify files, folder, and access permissions of internal filesystem (no CSP access)	None	CO, User
Show Version (Get Info)	Provides current status of the module, and returns non-Approved mode indicator	None	CO, User, Everyone
Get Data (Show Status)	Provides periodic self-tests information	None	CO, User, Everyone
Get Error Log	Provides Error log information (after password authentication)	None	Everyone
Get Config	Provides configuration data that is not available in the Show Version (Get Info) command	None	CO, User, Everyone
Self-Tests	Executes the suite of self-tests	None	CO, User, Everyone

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

There is no External Software/Firmware Loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following firmware component(s):

- Component 1: VaultIC408 1.2.4 binary – source code

The firmware component is protected with

- the pre-operational self-test performed before authentication
- the authentication technique Secure Channel Protocol 03 or secure password
- verification of the firmware using an error detection code (HW CRC16)

The operator can initiate the integrity test on demand by sending the Self-Tests command or power cycling.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by sending the Self-Tests command or power cycling.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The module supports a non-modifiable operational environment, which does not support firmware updates.

Type of Operational Environment: Non-Modifiable

6.2 Configuration Settings and Restrictions

The CO role shall configure the Operating System with the following policy:

- Authentication
- User access configuration and credential

Configuration of the Approved Mode of Operation

The Approved mode of operation is configured per the instructions in Section 2.4.

Configuration of the non-Approved modes of operation

The non-Approved mode of operation is configured per the instructions in Section 2.4.

7 Physical Security

7.1 Mechanisms and Actions Required

The following physical security mechanism are implemented by hardware in the Module:

- Hard, opaque, non-removable enclosure (IC packaging)

Mechanism	Inspection Frequency	Inspection Guidance
Tamper resistant packaging	Monthly	The CO is to evaluate the single-chip for evidence of tamper. GetErrorLog command gives the log of the violation after authentication. In case tamper evidence is found, contact the Site Security personnel.

Table 16: Mechanisms and Actions Required

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-60C	EFT	Shutdown
HighTemperature	160C	EFT	Shutdown
LowVoltage	1.4V	EFT	Shutdown
HighVoltage	8V	EFT	Shutdown

Table 17: EFP/EFT Information

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40C
HighTemperature	105C

Table 18: Hardness Testing Temperatures

Note: The module is hardness tested at the lowest and highest temperatures within the module's intended temperature range of operation.

8 Non-Invasive Security

At this time, no requirements have been specified for non-invasive attacks in NIST SP 800-140F. As such, this section is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM (S1)	Only stored in volatile memory (RAM) scrambled.	Dynamic
EEPROM (S2)	Stored in EEPROM in scrambled NVM.	Static
EEPROM (S3)	Stored in EEPROM as a SHA2-256 hash.	Static

Table 19: Storage Areas

All the memory (RAM and EEPROM) of the Module are scrambled.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input AES wrapped	Application Software (Outside)	RAM (S1)	Encrypted	Automated	Electronic	KTS
Output AES wrapped	RAM (S1)	Application Software (Outside)	Encrypted	Automated	Electronic	KTS
Input SCP03 wrapped	Application Software (Outside)	RAM (S1)	Encrypted	Automated	Electronic	KTS-SCP03
Output SCP03 wrapped	RAM (S1)	Application Software (Outside)	Encrypted	Automated	Electronic	KTS-SCP03
Input in plaintext	Application Software (Outside)	RAM (S1)	Plaintext	Manual	Electronic	
Output in plaintext	RAM (S1)	Application Software (Outside)	Plaintext	Manual	Electronic	

Table 20: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroized after use	The SSP is zeroized after it is used.	Automatic
Z2	Zeroized by the zeroization service by	The SSP is zeroized upon deletion of the operator account.	Manage Authentication Data command.

Zeroization Method	Description	Rationale	Operator Initiation
	overwriting with a fixed pattern of zeros.		
Z3	Zeroized the module when it enters the Terminated state.	All SSPs stored in the module are zeroized.	Automatic upon failure of the DRBG KAT or EEPROM CSP integrity self-tests.

Table 21: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Keys	Encryption/decryption operations	128-256 - 128-256	Symmetric - CSP	SymGen		BC-A-ENC BC-A-DEC BC-U-ENC BC-U-DEC
AES Transport Key	Wraps other SSPs for secure transport	128-256 - 128-256	Symmetric - CSP	SymGen		KTS
DRBG-EI and Seed	CTR_DRBG entropy input	736 - 384	ENT - CSP	Entropy		RBG
DRBG-State	AES-based Counter DRBG internal state (V and Key)	256 - 256	RBG - CSP	RBG		AKP-KG SymGen RBG KAS-KG
ECC Signing Key	Signature generation	P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 - 112-256	Asymmetric - CSP	AKP-KG		EC-SigGen
ECC Verifying Key	Signature Verification	P-192 (Legacy), P-224, P-256, P-384, P-521, K-163 (Legacy), K-233, K-283, K-409, K-571, B-163 (Legacy), B-233, B-283, B-409, B-571 - 80 (Legacy), 112-256	Asymmetric - PSP	AKP-KG		EC-SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KAS Private Key	Establishes KAS Shared Secret	P-224, P-256, P384, P-521 K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 - 112-256	Asymmetric - CSP	KAS-KG		KAS-ECC
KAS Public Key	Establishes KAS Shared Secret	P-224, P-256, P384, P-521 K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 - 112-256	Asymmetric - PSP	KAS-KG		KAS-ECC
KAS Shared Secret	Derives key material	112-256 - 112-256	Symmetric - CSP		KAS-ECC	KAS-ECC
MAC Keys	Data integrity key	128-256 - 128-256	MAC - CSP	SymGen		MAC-CMAC MAC-GMAC MAC-HMAC
RSA Signing Key	Signature generation	2048 - 112	Asymmetric - CSP	AKP-KG		RSA-SigGen
RSA Verifying Key	Signature verification	1024 (legacy), 2048 - 80 (legacy), 112	Asymmetric - PSP	AKP-KG		RSA-SigVer
SCP03 C-ENC	SCP03 session encryption key	128-256 - 128-256	Symmetric - CSP	KBKDF		BC-U-ENC BC-U-DEC KTS-SCP03
SCP03 C-MAC	SCP03 session integrity key	256 - 256	MAC - CSP	KBKDF		KTS-SCP03 MAC-CMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SCP03 R-MAC	SCP03 session integrity key	256 - 256	MAC - CSP	KBKDF		KTS-SCP03 MAC-CMAC
SCP03 S-ENC	Used to derive SCP03 session encryption keys	128-256 - 128-256	Symmetric - CSP			KBKDF
SCP03 S-MAC	Used to derive SCP03 session integrity keys	256 - 256	MAC - CSP			KBKDF
Secure Password	Used in addition to the Secure Password AES Key to authenticate the operator	64-256 - 64-256	Authentication - CSP			
Secure Password AES Key	AES key used to encrypt Secure Password during entry	128-256 - 128-256	Symmetric - CSP	SymGen		BC-U-ENC BC-U-DEC

Table 22: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Keys	Input AES wrapped Output AES wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	DRBG-State:Generates AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
AES Transport Key	Input AES wrapped Output AES	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	AES Keys:Protected by MAC Keys:Protected by RSA Signing Key:Protected by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext				ECC Signing Key:Protected by RSA Verifying Key:Protected by ECC Verifying Key:Protected by KAS Private Key:Protected by KAS Public Key:Protected by AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
DRBG-EI and Seed		RAM (S1):Obfuscated	Until use completes	Z1 Z2 Z3	DRBG-State:Establishes
DRBG-State		RAM (S1):Obfuscated	Until use completes	Z1 Z2 Z3	DRBG-EI and Seed:Derived From Secure Password AES Key:Generated By AES Keys:Generated By MAC Keys:Generated By AES Transport Key:Generated By RSA Signing Key:Generated By ECC Signing Key:Generated By RSA Verifying Key:Generated By ECC Verifying Key:Generated By KAS Private Key:Generated By KAS Public Key:Generated By
ECC Signing Key	Input AES wrapped Output AES	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	ECC Verifying Key:Paired With AES Transport Key:Encrypts SCP03 C-ENC:Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext				SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
ECC Verifying Key	Input AES wrapped Output AES wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	ECC Signing Key:Paired With AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
KAS Private Key	Input AES wrapped Output AES wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	KAS Public Key:Paired With KAS Shared Secret:Derived From AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
KAS Public Key	Input AES wrapped Output AES	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	KAS Private Key:Paired With AES Transport Key:Encrypts KAS Shared Secret:Derived

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext				From SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
KAS Shared Secret		RAM (S1):Obfuscated	Until use completes	Z1 Z2 Z3	KAS Private Key:Derives KAS Public Key:Derives
MAC Keys	Input AES wrapped Output AES wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	DRBG-State:Generates AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
RSA Signing Key	Input AES wrapped Output AES wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	RSA Verifying Key:Paired With AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RSA Verifying Key	Input AES wrapped Output AES wrapped Input SCP03 wrapped Output SCP03 wrapped Input in plaintext Output in plaintext	RAM (S1):Obfuscated EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	RSA Signing Key:Paired With AES Transport Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
SCP03 C-ENC		RAM (S1):Obfuscated	Until use completes	Z1 Z2 Z3	SCP03 S-Enc:Derives
SCP03 C-MAC		RAM (S1):Obfuscated	Until use completes	Z1 Z2 Z3	SCP03 S-MAC:Derives
SCP03 R-MAC		RAM (S1):Obfuscated	Until use completes	Z1 Z2 Z3	SCP03 S-MAC:Derives
SCP03 S-ENC	Input SCP03 wrapped	EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	SCP03 C-ENC:Derived From SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
SCP03 S-MAC	Input SCP03 wrapped	EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	SCP03 C-MAC:Derived From SCP03 R-MAC:Derived From SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Secure Password	Input AES wrapped Input SCP03 wrapped	EEPROM (S3):Plaintext	Until use completes	Z2 Z3	Secure Password AES Key:Encrypts SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For
Secure Password AES Key	Input SCP03 wrapped	EEPROM (S2):Obfuscated	Until use completes	Z2 Z3	Secure Password:Encrypted By SCP03 C-ENC:Encrypts SCP03 C-MAC:Provides Integrity For SCP03 R-MAC:Provides Integrity For

Table 23: SSP Table 2

9.5 Transitions

The module implements multiple keys with a security strength of 112 bits. In accordance with IG D.B, applying cryptographic protection (e.g., encryption) with a minimum security strength of 112 bits is acceptable through 2030; thereafter, 128 bits of security strength shall be provided. For 2031 and beyond, the legacy use of cryptographic keys with a minimum of 112 bits of security strength is permitted for the purposes of processing cryptographically protected data (e.g., decryption).

SSPTable2 From Web Cryptik SSPTable2

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 after 65535 (max) command received. The Module will not accept any commands when a periodic self-test is required; the pending commands in the I/O buffer will be processed by the Module after the periodic self-tests complete. The Module logs the latest self-test errors, the approved CO and User can consult the error log after successful authentication.

The Module performs the following pre-operational self-tests in table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity	16-bit CRC Error Detection Code	EDC	SW/FW Integrity	Success or Failure code	Executed on the whole firmware stored in EEPROM before the Module transition to the idle state.
EEPROM CSP area integrity	16-bit CRC Error Detection Code	EDC	Critical Function	Success or Failure code	Executed on the whole CSP stored in EEPROM before the Module transition to the idle state.

Table 24: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CMAC (A5349)	AES-128 CMAC	KAT	CAST	No Error Status Word	Generation and Verification	Power-On
AES-ECB (A4856) Decrypt	AES-128, 192 and 256-bit – ECB	KAT	CAST	No Error Status Word	Decryption	Power-On
AES-ECB (A4856) Encrypt	AES-128, 192 and 256-bit – ECB	KAT	CAST	No Error Status Word	Encryption	Power-On
AES-GCM (A5349) Decrypt	AES-128 and AES-256 - GCM	KAT	CAST	No Error Status Word	Decryption	Power-On
AES-GCM (A5349) Encrypt	AES-128 and AES-256 - GCM	KAT	CAST	No Error Status Word	Encryption	Power-On
Counter DRBG (A5349)	CTR_DRBG	KAT	CAST	No Error Status Word	AES-256 CTR_DRBG instantiate, generate, and reseed KATs performed before the first random data generation. Includes Health Tests.	Power-On
ECDSA KeyGen (FIPS186-4) (A5349)	EC key pair generation.	PCT	PCT	No Error Status Word	EC Key Pair Generation. Signature generation and verification.	Upon Key Generation
ECDSA SigGen (FIPS186-4) (A5349) w/ K-233	Using ECDSA K-233 with SHA2-256	KAT	CAST	No Error Status Word	ECDSA using K-233 with SHA2-256. Signature generation.	Power-On
ECDSA SigGen (FIPS186-4) (A5349) w/ P-224	Using ECDSA P-224 with SHA2-224	KAT	CAST	No Error Status Word	ECDSA using P-224 with SHA2-224. Signature generation.	Power-On
ECDSA SigVer (FIPS186-4) (A5349) w/ K-233	Using ECDSA K-233 with SHA2-256	KAT	CAST	No Error Status Word	ECDSA using K-233 with SHA2-256. Signature verification.	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) (A5349) w/ P-224	Using ECDSA P-224 with SHA2-224	KAT	CAST	No Error Status Word	ECDSA using P-224 with SHA2-224. Signature verification.	Power-On
EEPROM CSP Area Integrity	CRC-16 EDC	KAT	Critical Function	No Error Status Word	16-bit Error Detection Code. Executed on the whole CSP stored in EEPROM before the Module transitions to the idle state.	Power-On
ENT	NIST SP 800-90B Health Tests	APT and RCT	CAST	No Error Status Word	An RCT and APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input	Power-On
HMAC-SHA-1 (A5349)	HMAC SHA-1	KAT	CAST	No Error Status Word	HMAC-SHA-1 KAT	Power-On
HMAC-SHA2-256 (A5349)	HMAC SHA2-256	KAT	CAST	No Error Status Word	HMAC SHA2-256	Power-On
HMAC-SHA2-512 (A5349)	HMAC SHA2-512	KAT	CAST	No Error Status Word	HMAC SHA2-512	Power-On
KAS-ECC Sp800-56Ar3 (A5349)	P-256 and B-233 KAS-ECC	KAT	CAST	No Error Status Word	P-256 and B-233 KAS-ECC with oneStep KDF per IG D.F.	Power-On
KDF SP800-108 (A5349)	AES-CMAC 128 and HMAC SHA2-256	KAT	CAST	No Error Status Word	KDF concatenation using AES-128 and HMAC SHA2-256.	Power-On
RSA KeyGen (FIPS186-4) (A5349)	RSA Key Pair Generation.	PCT	PCT	No Error Status Word	Signature generation and verification.	Upon Key Generation
RSA SigGen (FIPS186-4) (A5349)	2048-bit key using PKCS1.5 and PSS.	KAT	CAST	No Error Status Word	2048-bit Signature Generation using PKCS1.5 and PSS and SHA2-256	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A5349)	2048-bit key using PKCS1.5 and PSS.	KAT	CAST	No Error Status Word	2048-bit Signature Verification using PKCS1.5 and PSS and SHA2-256	Power-On
SHA-1 (A5349)	SHA-1	KAT	CAST	No Error Status Word	SHA-1 Hash	Power-On
SHA2-224 (A5349)	SHA2-224	KAT	CAST	No Error Status Word	SHA2-224 Hash	Power-On
SHA2-256 (A5349)	SHA2-256	KAT	CAST	No Error Status Word	SHA2-256 Hash	Power-On
SHA2-384 (A5349)	SHA2-384	KAT	CAST	No Error Status Word	SHA2-384 Hash	Power-On
SHA2-512 (A5349)	SHA2-512	KAT	CAST	No Error Status Word	SHA2-512 Hash	Power-On

Table 25: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity	EDC	SW/FW Integrity	After 65535 command received (Max)	Automatic
EEPROM CSP area integrity	EDC	Critical Function	Before any CSP access and After 65535 command received (Max)	Automatic

Table 26: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CMAC (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
AES-ECB (A4856) Decrypt	KAT	CAST	After 65535 command received (Max)	Automatic
AES-ECB (A4856) Encrypt	KAT	CAST	After 65535 command received (Max)	Automatic
AES-GCM (A5349) Decrypt	KAT	CAST	After 65535 command received (Max)	Automatic
AES-GCM (A5349) Encrypt	KAT	CAST	After 65535 command received (Max)	Automatic
Counter DRBG (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
ECDSA KeyGen (FIPS186-4) (A5349)	PCT	PCT	Upon Key Generation	Automatic
ECDSA SigGen (FIPS186-4) (A5349) w/ K-233	KAT	CAST	After 65535 command received (Max)	Automatic
ECDSA SigGen (FIPS186-4) (A5349) w/ P-224	KAT	CAST	After 65535 command received (Max)	Automatic
ECDSA SigVer (FIPS186-4) (A5349) w/ K-233	KAT	CAST	After 65535 command received (Max)	Automatic
ECDSA SigVer (FIPS186-4) (A5349) w/ P-224	KAT	CAST	After 65535 command received (Max)	Automatic
EEPROM CSP Area Integrity	KAT	Critical Function	All CSP access	Automatic
ENT	APT and RCT	CAST	After 65535 command received (Max)	Automatic
HMAC-SHA-1 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
HMAC-SHA2-512 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
KAS-ECC Sp800-56Ar3 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
KDF SP800-108 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
RSA KeyGen (FIPS186-4) (A5349)	PCT	PCT	Upon Key Generation	Automatic
RSA SigGen (FIPS186-4) (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
RSA SigVer (FIPS186-4) (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
SHA-1 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
SHA2-224 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
SHA2-256 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
SHA2-384 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic
SHA2-512 (A5349)	KAT	CAST	After 65535 command received (Max)	Automatic

Table 27: Conditional Periodic Information

10.4 Error States

For a complete listing of all possible error messages, please request the VaultIC408 1.2.X Technical Datasheet (TPR0693X) from Sales Representative.

Name	Description	Conditions	Recovery Method	Indicator
ES1	The Module fails a firmware integrity pre-operational self-test or a conditional self-test.	The Module enters the Mute error state	Reboot/Power cycle the module	Outputs No status in error , otherwise it indicates successful completion by a Status word at 9000h
ES2	The Module fails DRBG KAT or EEPROM CSP integrity self-tests.	The Module enters the Terminated state	None	The Module enters the terminated error state, otherwise it indicates successful completion by a Status word at 9000h

Table 28: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Module is delivered securely, with tracking and protection against theft, by contracted logistic partners to the authorized operator. Upon receipt, the Module must be examined for evidence of tamper.

The VaultIC408 is delivered in the CREATION state, which is an uninitialized state that supports status commands, self-tests, and personalization. In order to initialize the module for Approved use, the operator must perform the following:

1. Authenticate using the default password provided by their Sales Representative.
2. Configure an Approved Administrator, along with their authentication credentials.
3. (Optionally) Configure additional Administrators and Users, as desired, for Approved or non-Approved modes.
4. Set FIPS Level 2.

Set Status to transition the module into the ACTIVATED state. This will zeroize the default role and password used to initially authenticate; there is no ability to return to the CREATION state after transitioning to the ACTIVATED state.

Failure to, at minimum, create an Approved Administrator will result in the module only operating in non-Approved mode. Once in the ACTIVATED state, the operator may invoke the Approved or non-Approved services by authenticating to the role associated with the desired mode of operation (i.e., Approved Administrator to invoke the Approved mode, non-Approved Administrator to invoke the non-Approved mode).

11.2 Administrator Guidance

VaultIC408 1.2.X technical datasheet (TPR0693X) describes all the mechanisms for administrator guidance.

Once successfully authenticated, the Administrator user shall perform the personalization data and initialize other operators. Typical personalization process may be:

1. Create operators with administrator and approved-user roles using Manage Authentication Data command.
2. Download initial keyset using Put Key command.

11.3 Non-Administrator Guidance

VaultIC408 1.2.X technical datasheet (TPR0693X) scribes all the mechanisms for non-administrator guidance.

Once successfully authenticated, the non-administrator user can use all the approved commands.

11.4 Design and Rules

Design and Rules – Overall security design and the rules of operation.

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
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 or resetting the Module.
6. All 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 no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does not support manual SSP establishment method.
11. The Module does not have any proprietary external input/output devices used for entry/output of data.
12. The Module does not store any plaintext CSPs.
13. The Module does not output intermediate key values.
14. The Module does not provide bypass services or ports/interfaces.

15. The Module does not support a maintenance role or interface.

11.5 Maintenance Requirements

The Module does not support a maintenance interface or role.

11.6 End of Life

The Module terminated state is an end of life state; however, that cannot be invoked by the operator.

The Module must be zeroized by deleting all operator accounts through the Manage Authentication Data service. The Module may then be physically decommissioned by returning to corporate IT administrator.

12 Mitigation of Other Attacks

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

References and Definitions

The following standards are referred to in this Security Policy.

Table 29 References

Abbreviation*	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, 18 April 2025*
[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, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*

Abbreviation*	Full Specification Name
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, 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*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Cr2]	*NIST Special Publication 800-56C Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, August 2020*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, 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 30 Acronyms and Definitions

Acronym*	Definition
APT	Adaptative Proportion Test
KAT	Know Answer Test
RCT	Repetition Count Test
SSP	Sensitive Security Parameter