Securemetric Technology Sdn. Bhd.

ST3 Ace Cryptographic Module

# FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0.0
Date: August 28, 2026

# Table of Contents

1 – General ..... 5
1.1 Overview ..... 5
1.2 Security Levels ..... 5
2 – Cryptographic Module Specification ..... 6
2.1 Description ..... 6
2.2 Tested and Vendor Affirmed Module Version and Identification ..... 8
2.3 Excluded Components ..... 8
2.4 Modes of Operation ..... 8
2.5 Algorithms ..... 8
2.6 Security Function Implementations ..... 11
2.7 Algorithm Specific Information ..... 15
2.8 RBG and Entropy ..... 15
2.9 Key Generation ..... 16
2.10 Key Establishment ..... 16
2.11 Industry Protocols ..... 16
3 Cryptographic Module Interfaces ..... 17
3.1 Ports and Interfaces ..... 17
4 Roles, Services, and Authentication ..... 18
4.1 Authentication Methods ..... 18
4.2 Roles ..... 20
4.3 Approved Services ..... 21
4.4 Non-Approved Services ..... 44
4.5 External Software/Firmware Loaded ..... 44
5 Software/Firmware Security ..... 45
5.1 Integrity Techniques ..... 45
5.2 Initiate on Demand ..... 45
6 Operational Environment ..... 46
6.1 Operational Environment Type and Requirements ..... 46
7 Physical Security ..... 47
7.1 Mechanisms and Actions Required ..... 47
7.2 EFP/EFT Information ..... 47
7.3 Hardness Testing Temperature Ranges ..... 48
8 Non-Invasive Security ..... 49
8.1 Mitigation Techniques ..... 49

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0 
Securemetric Public Material – May be reproduced only in its original entirety (without revision).

9 Sensitive Security Parameters Management....50
9.1 Storage Areas....50
9.2 SSP Input-Output Methods....50
9.3 SSP Zeroization Methods....51
9.4 SSPs....52
9.5 Transitions....71
10 Self-Tests....72
10.1 Pre-Operational Self-Tests....72
10.2 Conditional Self-Tests....72
10.3 Periodic Self-Test Information....75
10.4 Error States....78
10.5 Operator Initiation of Self-Tests....78
11 Life-Cycle Assurance....79
11.1 Installation, Initialization, and Startup Procedures....79
11.2 Administrator Guidance....79
11.3 Non-Administrator Guidance....79
11.4 Design and Rules....79
11.5 Maintenance Requirements....80
11.6 End of Life....80
12 Mitigation of Other Attacks....81
References and Definitions....82


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

## List of Tables

Table 1 References....82
Table 2 Acronyms and Definitions....83

## List of Figures

Figure 1 – Module Boundary .... 6
Figure 2 – Block diagram .... 7
Figure 3 – Module Appearance .... 7


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

# 1 – General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the ST3 Ace Cryptographic Module. 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 3 module. In this document, the ST3 Ace Cryptographic Module is also referred to, with or without the "Securemetric" prefix, as the "ST3 Ace token", the "ST3 Ace token module", the "ST3 Ace Token cryptographic module", the "ST3 Ace USB Token" or the "Module"; all of these names refer to the same cryptographic module. "ST3 Ace" used alone denotes the model/part number of the Module (see Table 2).

## 1.2 Security Levels

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

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

Table 1: Security Levels

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

# 2 – Cryptographic Module Specification

This Securemetric ST3 Ace token module, hereafter denoted as the Module. The Module supports multiple identity authentication system frameworks such as PKI/OTP/FIDO, among which PKI includes three applications: ePass2003/ePassPIV/ePassOpenPGP. The OTP functional unit complies with OATH standards. The PIV functional unit meets the specifications NIST.SP.800-73-4. The OpenPGP functional unit is an ISO Smart Card Operating Systems.

## 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 identity authentication product, the Module is intended to be used in E-mail encryption, system login, transaction protection, etc.

**Module Type**: Hardware

**Module Embodiment**: MultiChipEmbed

**Cryptographic Boundary:**

The physical form of the Module is depicted in Figure 1. The Module is a multi-chip embedded embodiment. The Module is a USB token containing FEITIAN owned FTCOS, which is embedded in a HSC32K2 with PAA Integrated Circuit (IC) chip and has been developed to support Securemetric ST3 Ace. The Module is designed to provide strong authentication and identification and to support network login, secure online transactions, digital signatures, and sensitive data protection.

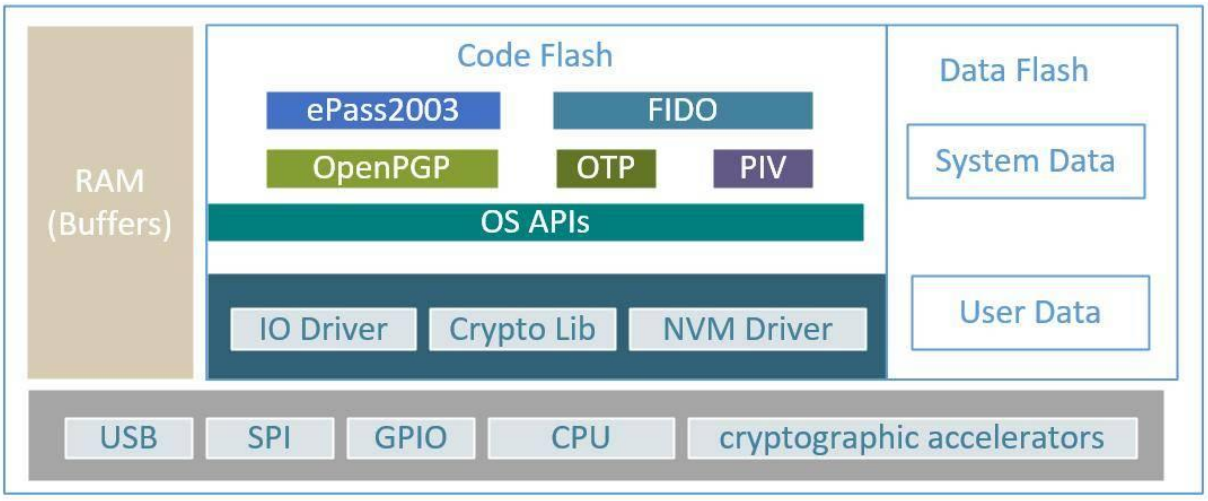



Figure 1 – Module Boundary


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

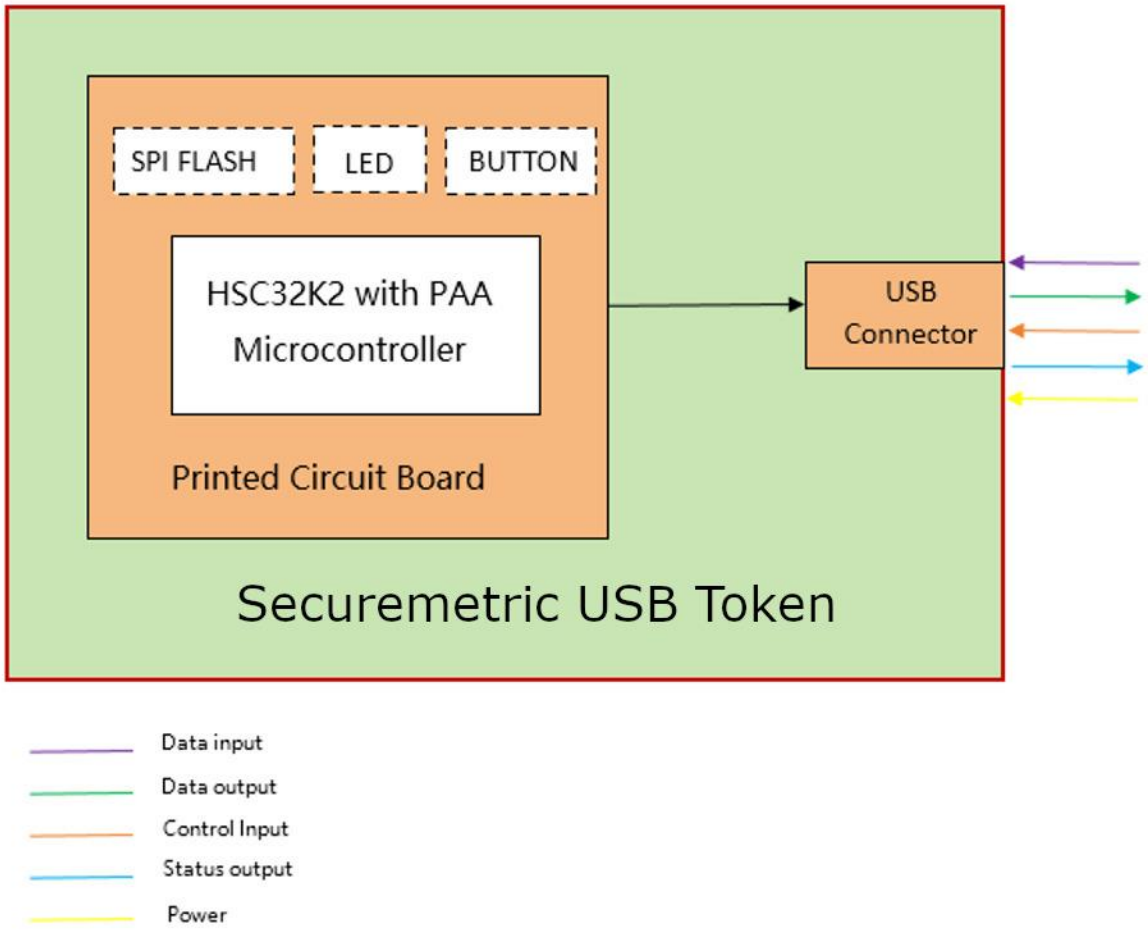



Figure 2 – Block diagram




Figure 3 – Module Appearance

**Model Description**: In the above Figure 3, is ST3 Ace USB Token


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

## 2.2 Tested and Vendor Affirmed Module Version and Identification

The operator can correlate the module's name and versioning information with the CMVP validation record by following the instructions in the Securemetric ST3 Ace Token Cryptographic Module Administrator Guidance, page 31, Section 5.8 Get Device Info, #7 get version info.

**Tested Module Identification – Hardware:**

Securemetric ST3 Ace Token cryptographic module is tested on the following operational environment.

| Model and/or Part Number | Hardware Version | Firmware Version | Processors | Features |
|---|---|---|---|---|
| ST3 Ace | V1.2 | V1.3.02 | HSC32K2 with PAA | |

Table 2: Tested Module Identification – Hardware

## 2.3 Excluded Components

The module does not exclude any components.

## 2.4 Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved Mode | The module has only one mode of operation - the Approved mode, which is entered after power up. | Approved | LED on and blink |

Table 3: Modes List and Description

The module only supports Approved mode. IG 2.4.C scenario 2) is applied to the module, i.e. A static code(9000 or 00) indicating the completion of service. The successful completion of a service is an implicit indicator for the use of an approved service.

## 2.5 Algorithms

**Approved Algorithms:**

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

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A4980 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CMAC | A4980 | Direction - Generation, Verification<br>Key Length - 128, 192, 256 | SP 800-38B |
| AES-ECB | A4980 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-GCM | A4980 | Direction - Decrypt, Encrypt<br>IV Generation Mode - 8.2.2<br>Key Length - 128, 192, 256 | SP 800-38D |
| Counter DRBG | A4980 | Prediction Resistance - Yes<br>Mode - AES-128<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| ECDSA KeyGen (FIPS186-5) | A4980 | Curve - P-256, P-384, P-521<br>Secret Generation Mode - testing candidates | FIPS 186-5 |
| ECDSA KeyVer (FIPS186-5) | A4980 | Curve - P-256, P-384, P-521 | FIPS 186-5 |
| ECDSA SigGen (FIPS186-5) | A4980 | Curve - P-256, P-384, P-521<br>Hash Algorithm - SHA2-256, SHA2-384, SHA2-512<br>Component - Yes | FIPS 186-5 |
| ECDSA SigVer (FIPS186-5) | A4980 | Curve - P-256, P-384, P-521<br>Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 | FIPS 186-5 |
| HMAC-SHA-1 | A4980 | Key Length - Key Length: 8-2048 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A4980 | Key Length - Key Length: 8-2048 Increment 8 | FIPS 198-1 |
| KAS-ECC Sp800-56Ar3 | A4980 | Domain Parameter Generation Methods - P-256<br>Function - Key Pair Generation<br>Scheme - ephemeralUnified -<br>KAS Role - Responder<br>KDF Methods - twoStepKdf -<br>Key Length - 256 | SP 800-56A Rev. 3 |
| KDF SP800-108 | A4980 | KDF Mode - Counter<br>Supported Lengths - Supported Lengths: 8-256 Increment 8 | SP 800-108 Rev. 1 |
| RSA KeyGen (FIPS186-5) | A4980 | Key Generation Mode - probable<br>Modulo - 2048, 3072, 4096<br>Primality Tests - 2powSecStr<br>Private Key Format - crt | FIPS 186-5 |
| RSA SigGen (FIPS186-5) | A4980 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| RSA SigVer (FIPS186-5) | A4980 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |
| SHA-1 | A4980 | Message Length - Message Length: 160, 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A4980 | Message Length - Message Length: 256, 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-384 | A4980 | Message Length - Message Length: 384, 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-512 | A4980 | Message Length - Message Length: 512, 0-65536 Increment 8 | FIPS 180-4 |

Table 4: Approved Algorithms

**Vendor-Affirmed Algorithms:**

The Module implements the FIPS Vendor Affirmed cryptographic algorithms listed below.

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG1 | Key Type::Asymmetric and Symmetric | N/A | [133r2] section 4, example 1 and IG D.H |

Table 5: Vendor-Affirmed Algorithms

**Non-Approved, Allowed Algorithms:**

N/A for this module.

**Non-Approved, Allowed Algorithms with No Security Claimed:**

N/A for this module.

**Non-Approved, Not Allowed Algorithms:**

N/A for this module.

## 2.6 Security Function Implementations

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

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| RSA_GEN_KEY_PAIR | AsymKeyPair-KeyGen | Asymmetric Key-Pair Generation | Publications:Publications: [FIPS 186-5], [SP800-90A], [SP800-133r1], [IG C.E] | RSA KeyGen (FIPS186-5): (A4980) Counter DRBG: (A4980) CKG1: () Key Type:: Symmetric |
| ECC_GEN_KEY_PAIR | AsymKeyPair-KeyGen | Asymmetric Key-Pair Generation | Publications:[FIPS 186-5], [SP800-90A], [SP800-133r1], [IG C.A] | ECDSA KeyGen (FIPS186-5): (A4980) Counter DRBG: (A4980) CKG1: () Key Type:: Symmetric |
| AES_KEY_GEN | CKG | Symmetric Key Generation Sections 4 and 6.1 Direct symmetric key generation using unmodified DRBG output | Publications:[SP800-90A], [IG D.H], [FIPS 197] | AES-CBC: (A4980) Size: 128 AES-GCM: (A4980) Size: 128 AES-ECB: (A4980) Size: 128 Counter DRBG: (A4980) CKG1: () Key |


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

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | Type:: Symmetric |
| SESSIONKEY_GEN | KBKDF | Symmetric Key Generation using KBKDF | Publications:[SP800-108r1], [SP800-38B], [FIPS 197] | AES-CMAC: (A4980) Size: 128 KDF SP800-108: (A4980) Size: 128 |
| RSA_SIG_GEN | DigSig-SigGen | Digital Signature Generation | Publications:[FIPS 186-5], [SP800-133r1], [IG C.E] | RSA SigGen (FIPS186-5): (A4980) SHA2-256: (A4980) SHA2-384: (A4980) SHA2-512: (A4980) |
| RSA_SIG_VER | DigSig-SigVer | Signature Verification | Publications:[FIPS 186-5], [IG C.E] | RSA SigVer (FIPS186-5): (A4980) SHA2-256: (A4980) SHA2-384: (A4980) SHA2-512: (A4980) |
| ECC_SIG_GEN | DigSig-SigGen | Digital Signature Generation | Publications:[FIPS 186-5], [SP800-133r1], [IG C.A] | ECDSA SigGen (FIPS186-5): (A4980) SHA2-256: (A4980) |


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

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | SHA2-384: (A4980) SHA2-512: (A4980) |
| ECC_SIG_VER | DigSig-SigVer | Signature Verification | Publications:[FIPS 186-5], [IG C.A] | ECDSA SigVer (FIPS186-5): (A4980) SHA2-256: (A4980) SHA2-384: (A4980) SHA2-512: (A4980) |
| ECC_KEY_VER | AsymKeyPair-KeyVer | Check the validity of the public key | Publications:[FIPS 186-5], [IG C.A] | ECDSA KeyVer (FIPS186-5): (A4980) |
| DRBG_GEN | DRBG | Random Number Generation | Publications:[SP800-90A], [IG D.L] | Counter DRBG: (A4980) |
| ENT_GEN | ENT-ESV | Entropy Source | Publications:[SP800-90B], [IG 9.3.A], [IG D.J] [IG D.O] | |
| SHAREDSECRETKEY_GEN_KAS | KAS-Full | Key Agreement Shared Secret Calculation [56Ar3] Key Derivation KDA [56Cr2] | IG:D.F Scenario 2, path 2, end-to-end Caveat:Key establishment methodology provides 128 bits of security strength Key confirmation:No Key derivation:KDA (tested as part KAS certificate) | KAS-ECC Sp800-56Ar3: (A4980) |
| AES_ENC_AUTH | BC-AuthEncrypt | Block Cipher | Publications:[FIPS 197] | AES-CMAC: (A4980) Sizes: 128 AES- |


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

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | GCM: (A4980) Size: 128 |
| AES_ENC | BC-UnAuthEncrypt | Block Cipher | Publications:[FIPS 197] | AES-CBC: (A4980) AES-ECB: (A4980) |
| AES_DEC_AUTH | BC-AuthDecrypt | Block Cipher | Publications:[FIPS 197] | AES-CMAC: (A4980) Size: 128 AES-GCM: (A4980) Size: 128 |
| AES_DEC | BC-UnAuthDecrypt | Block Cipher | Publications:[FIPS 197] | AES-CBC: (A4980) AES-ECB: (A4980) |
| HMAC_GEN | MAC | Message Authentication Generation | Publications:[FIPS198-1] [IG C.B] | HMAC-SHA-1: (A4980) HMAC-SHA2-256: (A4980) SHA-1: (A4980) SHA2-256: (A4980) |
| KTS_SCP03_WRAP | KTS-Unwrap | used as SCP03 | Standard:SP 800-38F IG D.G:Approved Caveat:Key establishment methodology provides 128 bits of security strength | AES-CBC: (A4980) Sizes: 128 AES-CMAC: (A4980) Sizes: 128 |
| KTS_AESGCM_WRAP | KTS-Unwrap KTS-Wrap | SP800-38D Based on IG D.G | Standard:SP 800-38F IG D.G:Approved | AES-GCM: (A4980) |


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

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | Caveat:Key establishment methodology provides 128 bits of security strength | Sizes: 128 |
| KTS_CTAP_WRAP | KTS-Unwrap KTS-Wrap | Key Wrapping Based on IG D.G | Standard:SP 800-38F IG D.G:Approved Caveat:Key establishment methodology provides 128 bits of security strength | AES-CBC: (A4980) Sizes: 128 HMAC-SHA2-256: (A4980) |
| SHA_CAL | SHA | Secure Hash Standard | Publications: [FIPS 180-4], [IG C.B] | SHA2-256: (A4980) SHA2-384: (A4980) SHA2-512: (A4980) |

Table 6: Security Function Implementations

## 2.7 Algorithm Specific Information

**AES GCM IV Uniqueness**

**FIPS140-3 IG C.H, Option 2**

The IV is generated internally at its entirety randomly.

The generation uses an Approved DRBG (Cert. #A4980) that is internal to the module's boundary.

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

**KAS [56Ar3]** - Per [IG] D.F Scenario 2 path (2), compliant key agreement scheme where testing is performed end-to-end for the shared secret computation and a KDF compliant with HKDF (2step KDF).

The Module obtains the [FIPS140-3_IG] D.F required key agreement assurances [SP800-56Ar3] in accordance with Section 5.6.2.

## 2.8 RBG and Entropy

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

The scenario 1(a) in IG 9.3.A is applied to the module, the security strength of the DRBG seeded by the entropy source is 128-bit.

According to table 4 of the ESV Public Use Document, to reach 128 bits of strength, at least 581 bits of random nonce are needed to seed the DRBG. A 640-bit nonce is used in the module, so the DRBG entropy strength is 128 bits.

| Cert Number | Vendor Name |
|---|---|
| E134 | Feitian Technologies Co., Ltd. |

Table 7: Entropy Certificates

The Module uses the following entropy sources:

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| HSEC_ES | Physical | HSEC HSC | 1 bit | 0.3308 | N/A |

Table 8: Entropy Sources

## 2.9 Key Generation

For Key Generation, see Section 2.5 and Section 2.6 above.

## 2.10 Key Establishment

**Key Agreement Information**

For Key Agreement, see Section 2.5 and Section 2.6 above.

**Key Transport Information**

For Key Transport, see Section 2.5 and Section 2.6 above.

## 2.11 Industry Protocols

The module does not support any industry protocols that would be of interest to this standard.

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| Power Supply 2 Pins | Power | Vcc Vdd 1.62-5.5V |
| Touch Button 1 Pin | Control Input | Physical input |
| LED 1 Pin | Status Output | Physical output |
| USB(D+/D-) 2 Pins | Data Input<br>Data Output<br>Control Input<br>Status Output | Primary physical interface (USB) for all service data |

Table 9: Ports and Interfaces

Note: The module does not support Control Output.


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

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| Authentication_PIN | A role is authenticated to the Module console with a PIN mechanism The PIN must be to changed by the CO after first authentication with default data. The Module enforced a minimum size of 8 ASCII characters. The number of incorrect attempts for PIN is 3-15, which can be set to a maximum of 15 times and a minimum of 3 times. | Memorized Secrets | PIN8-63 characters PIN, including numbers, letters, and special characters.Therefore, the probability of successful attempt is 1/95^8 | Each authentication attempt takes approximately 60 ms which allows a maximum of 15 attempts per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 15/95^8 |
| Authentication_ AuthKey | The identity is authenticated to the module with a challenge-response mechanism (Cert. #A4980). The entity gets challenge from the module then encrypts it resulting in cryptogram | AES-ECB (A4980) | 128-bit AES-ECB Key Challenge-Response A minimum 16 byte (128 bit) binary string has a probability that a random attempt will succeed or a false acceptance will occur of 1/2^128. | Each authentication attempt takes approximately 60 ms which allows a maximum of 15 attempts per minute. Therefore, the probability of successfully authenticating to the module |


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

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| | using Auth key. The cryptogram is sent back and decrypted in the module using same key, then the module check if the result is matched with original challenge. The Auth key MUST be changed to specific value for each module by the CO after first authentication with default data. The Auth key is generally a random number automatically generated by HSM. The number of incorrect attempts for Auth key is 3-15, which can be set to a maximum of 15 times and a minimum of 3 times. | | | within one minute through random attempts is 15/2^128 . |

Table 10: Authentication Methods

All authentication states are all stored in RAM, so they are cleared automatically once the module is powered down.

**Note:**
Authentication-PIN is an abstract noun that includes the PIN of ST3 Ace unit, PIN/PUK of PIV unit, PIN of FIDO unit, AccessiCode of OTP unit, PGP User PIN(PW1)/ PGP Admin PIN(PW3) of OpenPGP unit.


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

Authentication-AuthKey is an abstract noun that includes the Device authenticate key of a universal service unit, the External Auth Key of an ST3 Ace unit, and the PIV Authentication Key of a PIV unit.

## 4.2 Roles

The Module supports four distinct operator roles, User, Admin, Cryptographic Officer (CO) and Unauth. The CO is responsible for device authentication and resetting user PINs, etc. The Admin is responsible for configuring SSPS and performing cryptographic operations. The User utilizes the module as an authenticator. The unauthenticated role can only access some non-operational SSP services, Such as Select functional unit, get a challenge, read non-security relevant information, self-tests, etc.

The Module does not support a maintenance role.

The Module does not support concurrent operators.

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

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| CO | Identity | Crypto Officer | Authentication_ AuthKey |
| Admin | Identity | User | Authentication_ AuthKey<br>Authentication_PIN |
| User | Identity | User | Authentication_PIN |
| UnAuth | Role | Unauthenticated | None |

Table 11: Roles


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

## 4.3 Approved Services

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

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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| SELECT | Select functional unit | 9000 or error status | Command with AID | FCI(File Control Information) | None | Unauthenticated<br>- KSenc: Z<br>- KSmac: Z |
| Get Device Info | Get device information content including versioning information and show status | 9000 or error status | Command without input parameter | Device Info | None | Unauthenticated |
| Get Challenge | Request random data that will be used as a challenge within the Device Authenticate service | 9000 or error status | Command with expected data length | random value | DRBG_GEN<br>ENT_GEN | Unauthenticated<br>- DRBG V: G,Z<br>- DRBG Seed: G<br>- DRBG Key: G,Z |
| Device Authenticate | Request administrator privileges | 9000 or error status | Kid and cipher text | N/A | AES_DEC_AUTH | CO<br>- Device authenticate key: E |
| Update key | Change Device authenticate key, INIT_KEYenc and | 9000 or error status | cipher text | N/A | AES_DEC | CO<br>- KSenc: E<br>- KSmac: E<br>- Device authentic |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | INIT_KEY mac | | | | | ate key: W,E,Z<br>-<br>INIT_KEY enc: W,Z<br>-<br>INIT_KEY mac: W,Z |
| GP Initialize Update | Create Secure Channel Session | 9000 or error status | Host random Card random | cipher text | SESSIONKEY_GEN | CO<br>-<br>INIT_KEY enc: E<br>-<br>INIT_KEY mac: E<br>- KSenc: G<br>- KSmac: G<br>User<br>-<br>INIT_KEY enc: E<br>-<br>INIT_KEY mac: E<br>- KSenc: G<br>- KSmac: G |
| GP External Authenticate | This service may also be used to both authenticate and initiate a secure session with an external entity. | 9000 or error status | cipher text | N/A | SESSIONKEY_GEN | CO<br>- KSenc: E<br>- KSmac: E<br>User<br>- KSenc: E<br>- KSmac: E |
| Terminate token | The token into terminate state. | 9000 or error status | Command without input parameter | N/A | None | CO<br>- DRBG-EI: Z<br>- DRBG V: Z |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - DRBG Key: Z<br>- Managing Key: Z<br>- Device authenticate key: Z<br>- INIT_KEY enc: Z<br>- INIT_KEY mac: Z<br>- KSenc: Z<br>- KSmac: Z<br>- AES-GCM Key: Z<br>- FIDO Device ECDSA Private Key: Z<br>- FIDO Device ECDSA Public Key: Z<br>- FIDO User ECDSA Private Key: Z<br>- FIDO User ECDSA Public Key: Z<br>- FIDO Agreement ECC Private Key: Z<br>- FIDO Agreeme |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | nt ECC Public Key: Z<br>- FIDO Agreement sharedSecret: Z<br>- FIDO SharedSecret AES Key: Z<br>- FIDO SharedSecret HMAC Key: Z<br>- FIDO PinUvAuthToken: Z<br>- FIDO PIN: Z<br>- PIV Authentication Key: Z<br>- PIV ECC Signature Private Key: Z<br>- PIV ECC verification Public Key: Z<br>- PIV RSA Signature Private Key: Z<br>- PIV RSA verification Public Key: Z<br>- PIV User PIN: Z<br>- PIV PUK PIN: Z<br>- 2003 Internal |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Auth Key: Z - 2003 External Auth Key: Z - 2003 PIN: Z - 2003 PSO calculation key: Z - 2003 Unblock PIN: Z - 2003 RSA Private Key: Z - 2003 RSA Public Key: Z - 2003 ECDSA Private Key: Z - 2003 ECDSA Public Key: Z - OTP HMAC Seed Key: Z - OTP AccessCode: Z - PGP Admin PIN(PW3): Z - PGP User PIN(PW1): Z - PGP Resetting |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Code: Z - PGP Signature Private Key: Z - PGP Verification Public Key: Z - External Agreement ECC Public Key: Z - DRBG Seed: Z - AES-GCM IV: Z |
| Manage Security Environment (MSE) | Prepares the Module for the subsequent commands, Perform Security Operation. | 9000 or error status | Command without input parameter | N/A | None | User Admin |
| Hash | Performs a hash using SHA-256, SHA-384, or SHA-512. | 9000 or error status | message | Hash value | SHA_CAL | Unauthenticated |
| Read Binary | Allows read access to a binary file. A binary file is a file whose content is a sequential string of bits. | 9000 or error status | Command with file info | Binary database | None | Admin User |
| Update Binary | Allows write access to a binary file. | 9000 or error status | Binary data | N/A | None | Admin User |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Read Record | Allows read access to a record. A record is a type of data storage structure as defined within ISO 7816. Records are stored in files. | 9000 or error status | Command With file info | Record data | None | CO<br>User |
| Update Record | Allows write access to a record | 9000 or error status | Record data | N/A | None | CO<br>User |
| Append Record | Allows a record to be append | 9000 or error status | Record data | N/A | None | CO<br>User |
| Internal Authenticate | Authenticate the cryptographic module by an external entity<br>NOTE: In order for this service to be utilized, the external entity must have privileged access to the referenced key. | 9000 or error status | Random data | cipher text | AES_ENC | Admin - 2003 Internal Auth Key: E<br>User - 2003 Internal Auth Key: E |
| External Authenticate | Authenticates an external entity by the | 9000 or error status | cipher text | N/A | AES_DEC | Admin - 2003 External Auth Key: E |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | cryptographic module. NOTE: Prerequisite to this service is the use of Get Challenge service. The key as referenced within the service call exists under the current file | | | | | User - 2003 External Auth Key: E |
| Verify PIN | Provides PIN verification. | 9000 or error status | PIN data | N/A | KTS_SCP03_WRAP | Admin - 2003 PIN: E - KSenc: E - KSmac: E User - KSenc: E - KSmac: E - 2003 PIN: E |
| Change Reference Data | Modify the PIN | 9000 or error status | PIN and new PIN data | N/A | KTS_SCP03_WRAP | Admin - 2003 PIN: W,E - KSenc: E - KSmac: E User - 2003 PIN: W,E - KSenc: E - KSmac: E |
| Reset Retry Counter | Resets the retry counter | 9000 or error | Command without input | N/A | KTS_SCP03_WRAP | User - KSenc: E |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | status | parameter | | | - KSmac: E Admin<br>- KSenc: E<br>- KSmac: E |
| Generate Asymmetric Key Pair | Generates an Asymmetric key pair. | 9000 or error status | Command without input parameter | N/A | RSA_GEN_KEY_PAIR<br>ECC_GEN_KEY_PAIR | Admin<br>- DRBG-EI: G,E<br>- 2003 RSA Private Key: G<br>- 2003 RSA Public Key: G<br>- 2003 ECDSA Private Key: G<br>- 2003 ECDSA Public Key: G<br>- DRBG Seed: G,E User<br>- DRBG-EI: G,E<br>- 2003 RSA Private Key: G<br>- 2003 RSA Public Key: G<br>- 2003 ECDSA Private Key: G<br>- 2003 ECDSA Public Key: G |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - DRBG Seed: G,E |
| Encrypt | Performs an encrypt operation using an Approved security function. | 9000 or error status | Kid and plain text | cipher text | AES_ENC | Admin - 2003 PSO calculation key: E - Managing Key: E User - 2003 PSO calculation key: E - Managing Key: E |
| Decrypt | Performs a decrypt operation. | 9000 or error status | Kid and cipher text | plain text | AES_DEC | Admin - 2003 PSO calculation key: E - Managing Key: E User - 2003 PSO calculation key: E - Managing Key: E |
| Verify Digital Signature | Verifies a digital signature using RSA PKCS#1 or ECDSA | 9000 or error status | Signature and kid | N/A | RSA_SIG_VER ECC_SIG_VER ECC_KEY_VER | Admin - 2003 RSA Public Key: E - 2003 ECDSA Public Key: E User - 2003 RSA Public |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Key: E - 2003 ECDSA Public Key: E |
| Generate Digital Signature | Generates a digital signature using RSA PKCS#1 or ECDSA. | 9000 or error status | message and kid | Signature | RSA_SIG_GEN ECC_SIG_GEN | Admin - 2003 RSA Private Key: E - 2003 ECDSA Private Key: E User - 2003 RSA Private Key: E - 2003 ECDSA Private Key: E |
| Verify Cryptographic Checksum | Performs AES CMAC verification. | 9000 or error status | cipher text | N/A | AES_ENC_AUTH | Admin - 2003 PSO calculation key: E User - 2003 PSO calculation key: E |
| Compute Cryptographic Checksum | Compute AES CMAC. | 9000 or error status | plain text | cipher text | AES_ENC_AUTH | Admin - 2003 PSO calculation key: E User - 2003 PSO calculation key: E |
| Create File | Create a file. | 9000 or error status | Command with file info | N/A | None | Admin |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Delete File | Delete a File. | 9000 or error status | Command with file info | N/A | None | Admin - 2003 Internal Auth Key: Z - 2003 External Auth Key: Z - 2003 PIN: Z - 2003 Unblock PIN: Z - 2003 RSA Private Key: Z - 2003 RSA Public Key: Z - 2003 ECDSA Private Key: Z - 2003 ECDSA Public Key: Z |
| Install Secret | This service is used to enter AES keys, and PINs. SSPs which may be entered are as follows: * Internal Auth Key * External Auth Key * Symmetric Key * PIN | 9000 or error status | Encrypted Symmetric Key or pin | N/A | KTS_SCP03_WRAP | Admin - 2003 Internal Auth Key: W - 2003 External Auth Key: W - 2003 PSO calculation key: W - KSenc: E - KSmac: E - 2003 |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | PIN: W<br>- 2003 Unblock PIN: W |
| Get File List | Allows the reading of the FID list of child files of the current file | 9000 or error status | Command with file | File info | None | Admin User |
| Read Public Key | Allows the output of a public key. | 9000 or error status | Command with key info | RSA/ECC Public Key | None | Admin<br>- 2003 RSA Public Key: R<br>- 2003 ECDSA Public Key: R User<br>- 2003 RSA Public Key: R<br>- 2003 ECDSA Public Key: R |
| Make Credential | This service is used to generate a new credential in the module | 00 or error status | Encrypted Device ECDSA Private Key and message | CredentialID and X.509 certificate | ECC_GEN_KEY_PAIR<br>ECC_SIG_GEN<br>AES_ENC_AUTH<br>KTS_AESGCM_WRAP | User<br>- DRBG-EI: G,E<br>- DRBG V: G,E<br>- AES-GCM Key: E<br>- FIDO Device ECDSA Private Key: E<br>- FIDO User ECDSA Private Key: G,R,W<br>- FIDO |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Device ECDSA Public Key: R<br>- AES-GCM IV: E<br>- DRBG Seed: G,E<br>- DRBG Key: G,E<br>- FIDO User ECDSA Public Key: G,R |
| Get Attestation | This service is using Registration's credential to signature | 00 or error status | Encrypted User ECDSA Private Key and message | Signature | ECC_SIG_GEN<br>ECC_SIG_VER<br>AES_DEC_AUTH<br>KTS_AESGCM_WRAP | User<br>- DRBG-EI: G,E<br>- DRBG V: G,E<br>- AES-GCM Key: E<br>- AES-GCM IV: E<br>- DRBG Seed: G,E<br>- DRBG Key: G,E<br>- FIDO User ECDSA Private Key: E<br>- FIDO User ECDSA Public Key: E |
| Get Next Attestation | The client calls this service when the Attestationr | OK or error status00 | Command without input parameter | Signature | ECC_SIG_GEN | User<br>- DRBG-EI: G,E<br>- DRBG V: G,E |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | esponse contains the number of credentials member and the number of credentials exceeds 1. | or error status | | | | - AES-GCM Key: E<br>- DRBG Seed: G,E<br>- DRBG Key: G,E |
| Get Information | Device Information | 00 or error status | Command without input parameter | Version | None | Unauthenticated |
| PIN Service | This service is used by the platform to establish the shared Secret key, setting a new user PIN, changing existing user PIN, and getting User PinUvAuth Token from the module | 00 or error status | PIN | PinUvAuthToken | ECC_GEN_KEY_PAIR<br>AES_KEY_GEN<br>ECC_KEY_VER<br>SHAREDSECRETKEY_GEN_KAS<br>AES_ENC_AUTH<br>HMAC_GEN<br>KTS_CTAP_WRAP | User<br>- FIDO PIN: W,E<br>- FIDO PinUvAuthToken: G,R,E<br>- FIDO SharedSecret AES Key: G,E<br>- FIDO SharedSecret HMAC Key: G,E<br>- FIDO Agreement sharedSecret: G,E<br>- FIDO Agreement ECC Public Key: G,R<br>- External Agreement ECC Public Key: W,E<br>- |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Managing Key: G |
| FIDO Reset | Zeroization | 00 or error status | Command without input parameter | N/A | AES_KEY_GEN DRBG_GEN | CO - FIDO User ECDSA Private Key: Z - FIDO User ECDSA Public Key: Z - FIDO Agreement ECC Private Key: Z - FIDO Agreement ECC Public Key: Z - FIDO Agreement sharedSecret: Z - FIDO SharedSecret AES Key: Z - FIDO SharedSecret HMAC Key: Z - FIDO PinUvAuthToken: Z - FIDO PIN: Z - AES-GCM Key: G |
| Credential Management | Listing credentials and | 00 or error | pinUvAuthParam | N/A | AES_ENC HMAC_GEN KTS_CTAP_WRAP | User - FIDO |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | deleting credentials | status | | | | PinUvAuthToken: E |
| authenticatorConfig | used to configure various authenticator features through the use of its subcommands. | 00 or error status | pinUvAuthParam | N/A | AES_ENC HMAC_GEN | User - FIDO PinUvAuthToken: E |
| PIV GET DATA | This service is used to read data object | 9000 or error status | Command without input parameter | data object | None | User - PIV ECC verification Public Key: R - PIV RSA verification Public Key: R |
| PIV Verify PIN | This service is used to verify the PIN. | 9000 or error status | PIN | N/A | KTS_SCP03_WRAP | User - KSenc: E - KSmac: E - PIV User PIN: W,E |
| PIV Verify PUK | This service is used to verify the PUK. | 9000 or error status | PUK | N/A | KTS_SCP03_WRAP | Admin - KSenc: E - KSmac: E - PIV PUK PIN: W,E |
| GeneralAuth (Symmetric Key) | This service is used to external and mutual authenticate with PIV Symmetric Key | 9000 or error status | Random data and cipher text | N/A | AES_ENC_AUTH AES_ENC | User - DRBG-EI: E - PIV Authentication Key: E |
| PIV Reset | Reset PIV card state and delete all stored | 9000 or error status | Command without input parameter | N/A | SHA_CAL | CO - PIV User PIN: Z - PIV PUK PIN: Z |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | information Zeroization | | | | | - PIV Authentication Key: Z<br>- PIV ECC Signature Private Key: Z<br>- PIV ECC verification Public Key: Z<br>- PIV RSA Signature Private Key: Z<br>- PIV RSA verification Public Key: Z |
| Set Authentication Key | This service is used to change Authentication key (PIV Symmetric Key) | 9000 or error status | Encrypted Authentication Key | N/A | AES_ENC<br>AES_DEC<br>KTS_SCP03_WRAP | Admin<br>- PIV Authentication Key: W,E<br>- Managing Key: E |
| Change PUK | This service is used to change PUK | 9000 or error status | PUK | N/A | KTS_SCP03_WRAP | Admin<br>- PIV PUK PIN: W,E<br>- KSenc: E<br>- KSmac: E |
| Change PIN | This service is used to change PIN | 9000 or error status | PIN and new PIN | N/A | KTS_SCP03_WRAP | User<br>- PIV User PIN: W,E<br>- KSenc: E<br>- KSmac: E |
| Unblock PIN (Reset retry counter) | This service is used to reset retry counter and set | 9000 or error status | New PIN and PUK | N/A | KTS_SCP03_WRAP | Admin<br>- PIV User PIN: W,E<br>- PIV PUK PIN: W,E<br>- KSenc: |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | new user PIN with known PUK | | | | | E<br>- KSmac: E |
| Generate Asymmetric Key | This service is used to generate an asymmetric key | 9000 or error status | Command with Key length | Asymmetric Public key | RSA_GEN_KEY_PAIR<br>ECC_GEN_KEY_PAIR | Admin<br>- DRBG V: G,Z<br>- PIV ECC Signature Private Key: G<br>- PIV ECC verification Public Key: G<br>- PIV RSA Signature Private Key: G<br>- PIV RSA verification Public Key: G<br>- DRBG Key: G,Z<br>- DRBG Seed: G,E<br>- DRBG-EI: G,E |
| GeneralAuth (RSA/ECDSA) | This service is used to generate signature with asymmetric key | 9000 or error status | message | Signature | RSA_SIG_GEN<br>ECC_SIG_GEN | User<br>- PIV ECC Signature Private Key: E<br>- PIV RSA Signature Private Key: E |
| PIV Put Data | This service is used to write data (certicate, ID and etc) | 9000 or error status | Data object | N/A | None | Admin |
| Personalization OTP | Add a new entry and initialize its seed key | 9000 or error | Seed key | N/A | KTS_SCP03_WRAP | User<br>- OTP HMAC Seed |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | status | | | | Key: W<br>- KSenc: E<br>- KSmac: E<br>- DRBG V: E<br>- OTP AccessCode: E<br>- DRBG Key: E<br>- DRBG Seed: G,E<br>- DRBG-EI: G,E |
| Delete OTP | Remove an entry and its seed key. | 9000 or error status | Command without input parameter | N/A | None | User<br>- OTP AccessCode: E<br>- OTP HMAC Seed Key: Z |
| List | List all the names of the entries. | 9000 or error status | Command without input parameter | Slot info | None | User |
| Calculate OTP | Calculate the OTP value for an entry. | 9000 or error status | Command without input parameter | 6-digit OTP value or 8-digit OTP value | HMAC_GEN | User<br>- OTP HMAC Seed Key: E<br>- OTP AccessCode: E |
| OTP Reset | Reset the applet to manufactory default settings. | 9000 or error status | Command without input parameter | N/A | None | CO<br>- OTP HMAC Seed Key: Z |
| Verify AccessCode | Verify user AccessCode | 9000 or error status | AccessCode | N/A | KTS_SCP03_WRAP | User<br>- OTP AccessCode: E |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Change AccessCode | Change user AccessCode | 9000 or error status | AccessCode | N/A | KTS_SCP03_WRAP | User - OTP AccessCode: W,E |
| Emit OTP from slot | When the device is powered on and the user presses the button, the device outputs a 6-byte or 8-byte password | 9000 or error status | press-button | 6-digit OTP value or 8-digit OTP value | HMAC_GEN | User - OTP HMAC Seed Key: E |
| SELECT DATA | Select a current DO ,a following GET DATA or PUT DATA will access this current DO | 9000 or error status | DO Data | N/A | None | Unauthenticated |
| VERIFY | Verify using user PGP User PIN(PW1) or administrator PGP Admin PIN(PW3) | 9000 or error status | PGP User PIN(PW1) or PGP Admin PIN(PW3) | N/A | KTS_SCP03_WRAP | Admin - PGP Admin PIN(PW3): E User - PGP User PIN(PW1): E |
| OpenPGP CHANGE REFERENCE DATA | Change user PGP User PIN(PW1) or administrator PGP Admin PIN(PW3) | 9000 or error status | Command with data info | N/A | KTS_SCP03_WRAP | Admin - PGP Admin PIN(PW3): W,E User - PGP User PIN(PW1): W,E |
| OpenPGP RESET | Reset PGP User PIN(PW1) | 9000 or error | PW1 or PW3/ | N/A | KTS_SCP03_WRAP | Admin - PGP Admin |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| RETRY COUNTER | counter and set new PGP User PIN(PW1) using PGP Admin PIN(PW3) or Resetting Code. | status | Resetting Code | | | PIN(PW3): W,E<br>- PGP User PIN(PW1): W<br>User<br>- PGP User PIN(PW1): W<br>- PGP Resetting Code: W,E |
| GET DATA | Read protected or unprotected Data Object | 9000 or error status | Command without input parameter | Data Object | None | User<br>- PGP User PIN(PW1): E<br>Unauthenticated |
| PUT DATA | Write data objects except user writable data objects. | 9000 or error status | Data to be written | None | KTS_SCP03_WRAP | Admin<br>- PGP Resetting Code: W<br>- PGP Admin PIN(PW3): E |
| COMPUTE DIGITAL SIGNATURE | Perform signature primitive with signature Private Key | 9000 or error status | message and kid | Signature | RSA_SIG_GEN | User<br>- PGP Signature Private Key: E |
| OpenPGP GENERATE ASYMMETRIC KEY | Generate asymmetric key pair | 9000 or error status | Command without input parameter | RSA public key | RSA_GEN_KEY_PAIR | Admin<br>- DRBG V: G,E<br>- PGP Admin PIN(PW3): E<br>- PGP Signature Private Key: G<br>- PGP |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Verification Public Key: G,R<br>- DRBG Key: G,E<br>- DRBG Seed: G,E<br>- DRBG-EI: G,E |
| TERMINATE DF | This command is designed to renew a card in case of blocked passwords or other problems. | 9000 or error status | Command without input parameter | N/A | None | Admin<br>- PGP Admin PIN(PW3): E |
| ACTIVATE FILE | Initialize to the manufactory default settings. Zeroization | 9000 or error status | Command without input parameter | N/A | None | Admin<br>- PGP Admin PIN(PW3): Z<br>- PGP User PIN(PW1): Z<br>- PGP Resetting Code: Z<br>- PGP Signature Private Key: Z<br>- PGP Verification Public Key: Z |
| Get Error log | Get self-test result | 9000 or error status | Command without input parameter | Self-test result | None | Admin<br>- Device authenticate key: E |
| On-Demand Self-test | Initiate on-demand self-tests | None | None | Pass or Fail | | Admin<br>Unauthenticated |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | by reboot or power cycle | | | | | |

Table 12: Approved Services

## 4.4 Non-Approved Services

N/A for this module.

## 4.5 External Software/Firmware Loaded

NOTE: There is no External Software/Firmware Loaded.


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

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

The Module is composed of the following firmware component(s):
Component 1: cryptographic binary
Component 2: non-modifiable operating system - binary

The firmware components are protected with the error detection code CRC-16. Calculate CRC-16 on code and constant data in flash, then compare the result with expected value, which is also part of pre-operational self-test.

## 5.2 Initiate on Demand

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


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

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

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

**Type of Operational Environment**: Non-Modifiable


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

# 7 Physical Security

The Module is made of a completely hardened, production-grade polycarbonate or metal. The colored polycarbonate or metal enclosure obscures a clear view of the hardware components within. A hard, non-malleable metal casing surrounds the USB connector. The casing is made of hard, production-grade, black, opaque plastic.

The coloring of the Module obscures any visible writing on the PCB. The visible critical components within the Module are further covered to meet FIPS 140-3 level 3 physical security requirements. The HSC32K2 with PAA microcontroller is covered with a black, opaque, tamper-resistant, epoxy encapsulated, thus completely covering all critical cryptographic components from plain view. The USB connector located outside of the casing (in the case of the USB Token-A3) of the USB token is made of a hard, black, opaque, production grade plastic and prevents access to the rest of the USB token. Any attempt at removal or penetration of the enclosure has a high probability of causing serious damage to the Module and the hardware components within the enclosure, which will reveal clear tamper evidence. Removal of the metal surrounding the USB connector will result in physical damage of the USB connector and its associated pins, rendering the entire cryptographic module useless. If the USB connector is exposed, there is no power going to the USB token. Once power is removed from the cryptographic module, all plaintext keys and unprotected SSPs in RAM are zeroized.

## 7.1 Mechanisms and Actions Required

The enclosure of the module is designed with anti-dismantle. After assembly, any attempt at tampering will leave visible damage on the enclosure. So, each time a user uses the module, you should first check the outer appearance of the module to make sure the module has not been tampered since last time use. In case user detects any tamper during inspection, user must stop using the module immediately and contact manufacturer.

| Mechanism | Inspection Frequency | Inspection Guidance |
|---|---|---|
| anti-dismantle enclosure | Each time using the module | check the outer appearance of the module |

Table 13: Mechanisms and Actions Required

## 7.2 EFP/EFT Information

| Temp/Voltage Type | Temperature or Voltage | EFP or EFT | Result |
|---|---|---|---|
| LowTemperature | -29.6 | EFP | shutdown |
| HighTemperature | +86.6 | EFP | shutdown |
| LowVoltage | 2.8V | EFP | shutdown |
| HighVoltage | 5.5V | EFP | shutdown |

Table 14: EFP/EFT Information

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

## 7.3 Hardness Testing Temperature Ranges

| Temperature Type | Temperature |
|---|---|
| LowTemperature | -20C° |
| HighTemperature | +40C° |

Table 15: Hardness Testing Temperatures

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


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

# 8 Non-Invasive Security

## 8.1 Mitigation Techniques

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


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

# 9 Sensitive Security Parameters Management

## 9.1 Storage Areas

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| CHIPRAM(S1) | Session Key stored in volatile memory in plaintext. | Dynamic |
| CHIPRAM(S2) | Session Key stored in volatile memory in encrypted. | Dynamic |
| CHIPNVM(S3) | CSP is encrypted with AES-128 and stored in FLASH | Static |
| CHIPNVM(S4) | CSP stored in flash in SHA2-256 | Static |
| CHIPNVM(S5) | CSP stored in flash in plaintext | Static |
| CHIPNVM(S6) | PSP stored in flash in plaintext | Static |

Table 16: Storage Areas

## 9.2 SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| Input encapsulated by KTS-Wrap SCP03(IO1) | Application Software (outside) | CHIPNVM(S3) | Encrypted | Automated | Electronic | KTS_SCP03_WRAP |
| Input encapsulated by KTS-Wrap AES-GCM (IO2) | Application Software (outside) | CHIPRAM(S2) | Encrypted | Automated | Electronic | KTS_AESGCM_WRAP |
| Output encapsulated by KTS-Wrap AES-GCM (IO3) | CHIPRAM(S2) | Application Software (outside) | Encrypted | Automated | Electronic | KTS_AESGCM_WRAP |
| Input encapsulated by KTS-Wrap AES-CBC with HMAC (IO4) | Application Software (outside) | CHIPNVM(S4) | Encrypted | Automated | Electronic | KTS_CTAP_WRAP |
| Output encapsulated by | CHIPRAM(S2) | Application Software (outside) | Encrypted | Automated | Electronic | KTS_CTAP_WRAP |


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

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| KTS-Wrap AES-CBC with HMAC (IO5) | | | | | | |
| Input in plaintext (IO6) | Application Software (outside) | CHIPRAM(S1) | Plaintext | Automated | Electronic | |
| Output in plaintext (IO7) | CHIPRAM(S1) | Application Software (outside) | Plaintext | Automated | Electronic | |
| Output in plaintext (IO8) | CHIPNVM(S6) | Application Software (outside) | Plaintext | Automated | Electronic | |

Table 17: SSP Input-Output Methods

## 9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Z1 | Zeroized by Terminate token command | All SSP are cleared, completed by explicit indication of 9000 Status | CO |
| Z2 | Overwritten with all 0 after power cycle | Power on and implicit clear, completed by implicit indication of LED on. | Unauth |
| Z3 | Zeroized by 2003 delete MF | Received command to actively clear SSPs, completed by explicit indication of 9000 Status | CO |
| Z4 | "TERMINATE DF" followed by "ACTIVATE FILE" | Received command to actively clear SSPs, completed by explicit indication of 9000 Status | CO |
| Z5 | Zeroized by FIDO Reset | Received command to actively clear SSPs, completed by explicit indication of 00 Status | CO |
| Z6 | Zeroized by PIV Reset | Received command to actively clear SSPs, completed by explicit indication of 9000 Status | CO |
| Z7 | Select functional unit | Received command to actively clear SSPs, completed by explicit indication of 9000 Status | Unauth |
| Z8 | Zeroized by OTP Reset | Received command to actively clear SSPs, completed by explicit indication of 9000 Status | CO |

Table 18: SSP Zeroization Methods

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

## 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 |
|---|---|---|---|---|---|---|
| DRBG-EI | 384-bit entropy and 256-bit nonce input collected from the ESV,used to derive the DRBG seed | 640 - 128 | entropy source and nonce - CSP | ENT_GEN | | DRBG_GEN |
| DRBG Seed | 640-bit DRBG Seed from DRBG-EI | 640 - 128 | entropy source and nonce - CSP | ENT_GEN | | DRBG_GEN |
| DRBG V | Internal CTR_DRBG state value is used for SP800-90A CTR_DRBG (Consists of 128 bits) | 128 - 128 | state value - CSP | DRBG_GEN | | DRBG_GEN |
| DRBG Key | Internal CTR_DRBG state value is used for | 128 - 128 | key value - CSP | DRBG_GEN | | DRBG_GEN |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | SP800-90A CTR_DRBG (Consists of 128 bits) | | | | | |
| Managing Key | 128-bit AES key, used to encrypt SSPs and keys | 128 - 128 | Symmetric Key - CSP | AES_KEY_GEN | | AES_ENC AES_DEC |
| Device authenticate key | 128-bit AES key used for CO role to reach a safe state | 128 - 128 | Authentication - CSP | input during manufacturing | | AES_DEC |
| INIT_KEYenc | AES 128-bit key, used to derive KSenc and KSmac which is then used to encrypt/decrypt data over a secure session between an authorized external | 128 - 128 | Symmetric Key - CSP | input during manufacturing | | SESSIONKEY_GEN |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | entity and the Module. | | | | | |
| INIT_KEY mac | AES CMAC 128-bit key, used to derive a KSenc,KS mac which is then used to authenticate an operator or data over a secure session between an authorized external entity and the Module. | 128 - 128 | Symmetric Key - CSP | input during manufacturing | | SESSIONKEY_GEN |
| KSenc | AES 128-bit key used to encrypt/decrypt data over a secure session | 128 - 128 | session Key - CSP | SESSIONKEY_GEN | | KTS_SCP03_WRAP |
| KSmac | AES CMAC 128-bit key used to authenticat | 128 - 128 | session Key - CSP | SESSIONKEY_GEN | | KTS_SCP03_WRAP |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | e data over a secure session | | | | | |
| AES-GCM Key | 128-bit AES-GCM key used to encrypt the key handle or credentiall D | 128 - 128 | Symmetric Key - CSP | AES_KEY_GEN | | AES_ENC_AUTH AES_DEC_AUTH |
| AES-GCM IV | 96-bit AES-GCM IV used to encrypt the key handle or credentiall D | 96 - N/A | Random IV - CSP | DRBG_GEN | | AES_ENC_AUTH AES_DEC_AUTH |
| FIDO Device ECDSA Private Key | 256-bit ECC private key used to generate signature for registration. | 256 - 128 | Asymmetric Private Key - CSP | input during manufacturing | | ECC_SIG_GEN |
| FIDO Device ECDSA Public Key | 256-bit ECC FIDO public key, it is returned to the server | 256 - 128 | Asymmetric Public Key - PSP | input during manufacturing | | ECC_SIG_VER |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | via the certificate to verify the signature generated after registration | | | | | |
| FIDO User ECDSA Private Key | 256-bit ECC private key used to Attestation signature | 256 - 128 | Asymmetric Private Key - CSP | ECC_GEN_KEY_PAIR | | ECC_SIG_GEN |
| FIDO User ECDSA Public Key | 256-bit ECC FIDO public key, it is transmitted to the server for verifying signature generated after authentication | 256 - 128 | Asymmetric public Key - PSP | ECC_GEN_KEY_PAIR | | ECC_SIG_VER |
| FIDO Agreement ECC Private Key | 256-bit ECC private key used to perform key agreement | 256 - 128 | Asymmetric Private Key - CSP | ECC_GEN_KEY_PAIR | | SHAREDSECRETKEY_GEN_KAS |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | with external public ECC key to get shared Secret | | | | | |
| FIDO Agreement ECC Public Key | 256-bit ECC public key used to perform key agreement, the Module returns it to external to get sharedSecret | 256 - 128 | Asymmetric public Key - PSP | ECC_GEN_KEY_PAIR | | SHAREDSECRETKEY_GEN_KAS |
| FIDO Agreement sharedSecret | 256-bit key Used to derived FIDO SharedSecret AES Key and FIDO SharedSecret HMAC Key by HKDF | 256 - 128 | Shared Secret - CSP | SHAREDSECRETKEY_GEN_KAS | | KAS-ECC Sp800-56Ar3 (A4980) |
| FIDO SharedSec | 256-bit AES CBC key used | 256 - 128 | Symmetric Key - CSP | | SHAREDSECRETKEY_GEN_KAS | SHAREDSECRETKEY_GEN_KAS |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| ret AES Key | for encryption calculation of pin related operations | | | | | |
| FIDO SharedSecret HMAC Key | 256-bit AES CBC key used for HMAC SHA-256 calculation of pin related operations | 256 - 128 | Symmetric Key - CSP | | SHAREDSECRETKEY_GEN_KAS | SHAREDSECRETKEY_GEN_KAS |
| FIDO PinUvAuth Token | 256-bit HMAC SHA-256 Key used to authorize operator after PIN authentication | 256 - 128 | Authentication - CSP | DRBG_GEN | | HMAC_GEN |
| FIDO PIN | Authenticate the User,4 to 63-byte PIN value | 32-248 - N/A | Authentication - CSP | | | KTS_CTAP_WRAP |
| PIV Authentication Key | 128-bit AES ECB key, used for | 128 - 128 | Authentication - CSP | | | AES_ENC_AUTH |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | authentication of PIV CO | | | | | |
| PIV ECC Signature Private Key | 256 bit ECC private key, used for signature operations | 256 - 128 | Asymmetric Private Key - CSP | ECC_GEN_KEY_PAIR | | ECC_SIG_GEN |
| PIV ECC verification Public Key | 256-bit ECC public key, used for client verification operations | 256 - 128 | Asymmetric public Key - PSP | ECC_GEN_KEY_PAIR | | |
| PIV RSA Signature Private Key | 2048 -bit RSA private key, used for signature operations | 2048 - 112 | Asymmetric Private Key - CSP | RSA_GEN_KEY_PAIR | | RSA_SIG_GEN |
| PIV RSA verification Public Key | 2048 -bit RSA public key, used for client verification operations | 2048 - 112 | Asymmetric public Key - PSP | RSA_GEN_KEY_PAIR | | |
| PIV User PIN | 8-byte pin, used for authenticating the PIV user for | 64 - N/A | Authentication - CSP | | | KTS_SCP03_WRAP |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | Asymmetric services | | | | | |
| PIV PUK PIN | 8-byte pin, used for unblocking the PIV admin pin | 64 - N/A | Authentication - CSP | | | KTS_SCP03_WRAP |
| 2003 Internal Auth Key | AES 128,192,256-bit ,used to authenticate the Module to an external entity | 128-256 - 128-256 | Authentication - CSP | | | AES_ENC |
| 2003 External Auth Key | AES 128,192,256-bit, used to modify the security state of the currently selected DF. | 128-256 - 128-256 | Authentication - CSP | | | AES_DEC |
| 2003 PIN | 8-16 byte secret used to modify the security state of the currently selected DF. | 64-128 - N/A | Authentication - CSP | | | |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| 2003 PSO calculation key | AES 128,192,256-bit, Used to encryption, decryption, checksum calculation, and checksum verification in Unit 2003 | 128-256 - 128-256 | Symmetric Key - CSP | | | AES_ENC AES_DEC |
| 2003 Unblock PIN | 8-16 byte secret used to unblocking the 2003 pin the currently selected DF. | 64-128 - N/A | Authentication - CSP | | | AES_ENC |
| 2003 RSA Private Key | 2048,3072, 4096 bit RSA private key is used to sign data | 2048,3072,4096 - 112-152 | Asymmetric Private Key - CSP | RSA_GEN_KEY_PAIR | | RSA_SIG_GEN |
| 2003 RSA Public Key | 2048,3072, 4096-bit RSA public key used to verify data | 2048,3072,4096 - 112-152 | Asymmetric public Key - PSP | RSA_GEN_KEY_PAIR | | RSA_SIG_VER |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| 2003 ECDSA Private Key | 256,384,521bit ECDSA private key used to sign data. | 256,384,521 - 128-256 | Asymmetric Private Key - CSP | ECC_GEN_KEY_PAIR | | ECC_SIG_GEN |
| 2003 ECDSA Public Key | 256,384,521bit ECDSA public key used to verify data. | 256,384,521 - 128-256 | Asymmetric public Key - PSP | ECC_GEN_KEY_PAIR | | ECC_SIG_VER |
| OTP HMAC Seed Key | 16 to 64-byte HMAC SHA-1,HMAC SHA-256 key ,used to calculate OTP values for the User | 128-512 - 128 | Authentication - CSP | | | HMAC_GEN |
| OTP AccessCode | 8-byte pin, used for authenticating the OTP user | 64 - N/A | Authentication - CSP | | | HMAC_GEN<br>KTS_SCP03_WRAP |
| PGP Admin PIN(PW3) | 8 to 127-byte, used for authentication of the OpenPGP CO. | 64-1024 - N/A | Authentication - CSP | | | KTS_SCP03_WRAP |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| PGP User PIN(PW1) | 8 to 127-byte, used for authenticating the OpenPGP user for Asymmetric services. | 64-1024 - N/A | Authentication - CSP | | | KTS_SCP03_WRAP |
| PGP Resetting Code | 8 to 127-byte.Used for resetting the User PIN | 64-1024 - N/A | Authentication - CSP | | | KTS_SCP03_WRAP |
| PGP Signature Private Key | 2048,3072, 4096 bit RSA private key, used for PKCS#1 v1.5 signing operation | 2048,3072 ,4096 - 112-152 | Asymmetric Private Key - CSP | RSA_GEN_KEY_PAIR | | RSA_SIG_GEN |
| PGP Verification Public Key | 2048,3072, 4096 bit RSA public key, used for verification specified in PKCS#1 v1.5 | 2048,3072 ,4096 - 112-152 | Asymmetric public Key - PSP | RSA_GEN_KEY_PAIR | | |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| External Agreement ECC Public Key | 256-bit ECC Public key used to perform key agreement with FIDO Agreement ECC Private Key to get sharedSecret | 256 - 128 | Asymmetric public Key - PSP | | | SHAREDSECRETKEY_GEN_KAS |

Table 19: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| DRBG-EI | | CHIPRAM(S1):Plaintext | after usage is complete | Z2 | |
| DRBG Seed | | CHIPRAM(S1):Plaintext | after usage is complete | Z2 | |
| DRBG V | | CHIPRAM(S1):Plaintext | after usage is complete | Z2 | DRBG-EI:Derived From |
| DRBG Key | | CHIPRAM(S1):Plaintext | after usage is complete | Z2 | DRBG-EI:Derived From |
| Managing Key | | CHIPNVM(S5):Plaintext | | Z1 | Device authenticate key:Encrypts INIT_KEYenc:Encrypts INIT_KEYmac:Encrypts FIDO Device ECDSA Private Key:Encrypts FIDO User ECDSA Private Key:Encrypts |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | | | | | PIV Authentication Key:Encrypts<br>PIV ECC Signature Private Key:Encrypts<br>PIV RSA Signature Private Key:Encrypts<br>2003 Internal Auth Key:Encrypts<br>2003 External Auth Key:Encrypts<br>2003 PSO calculation key:Encrypts<br>2003 RSA Private Key:Encrypts<br>2003 ECDSA Private Key:Encrypts<br>OTP HMAC Seed Key:Encrypts<br>PGP Resetting Code:Encrypts<br>PGP Signature Private Key:Encrypts |
| Device authenticate key | | CHIPNVM(S3):Encrypted | | Z1 | Managing Key:Encrypted by KSenc:Derives |
| INIT_KEYenc | | CHIPNVM(S3):Encrypted | | Z1 | Managing Key:Encrypted by KSenc:Derives |
| INIT_KEYmac | | CHIPNVM(S3):Encrypted | | Z1 | Managing Key:Encrypted by KSmac:Derives |
| KSenc | | CHIPRAM(S1):Plaintext | after usage is completed | Z7 | INIT_KEYenc:Derived From |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| KSmac | | CHIPRAM(S1):Plaintext | after usage is completed | Z7 | INIT_KEYmac:Derived From |
| AES-GCM Key | | CHIPNVM(S5):Plaintext | | Z5 | FIDO User ECDSA Private Key:Wraps |
| AES-GCM IV | | CHIPNVM(S5):Plaintext | | Z5 | FIDO User ECDSA Private Key:Wraps |
| FIDO Device ECDSA Private Key | | CHIPNVM(S3):Encrypted | | Z1 | FIDO Device ECDSA Public Key:Paired With Managing Key:Encrypted by AES-GCM Key:Wrapped by |
| FIDO Device ECDSA Public Key | Output in plaintext (IO8) | CHIPNVM(S6):Plaintext | | Z1 | FIDO Device ECDSA Private Key:Paired With |
| FIDO User ECDSA Private Key | Input encapsulated by KTS-Wrap AES-GCM (IO2) Output encapsulated by KTS-Wrap AES-GCM (IO3) | CHIPNVM(S3):Encrypted | | Z5 | FIDO User ECDSA Public Key:Paired With Managing Key:Encrypted by AES-GCM Key:Wrapped by AES-GCM IV:Wrapped by |
| FIDO User ECDSA Public Key | Output in plaintext (IO7) | CHIPNVM(S6):Plaintext | | Z5 | FIDO User ECDSA Private Key:Paired With |
| FIDO Agreement ECC Private Key | | CHIPRAM(S1):Plaintext | | Z2 | FIDO Agreement ECC Public Key:Paired With FIDO Agreement sharedSecret:Derives |
| FIDO Agreement ECC Public Key | Output in plaintext (IO7) | CHIPRAM(S1):Plaintext | | Z2 | FIDO Agreement ECC Private Key:Paired With |
| FIDO Agreement sharedSecret | | CHIPRAM(S1):Plaintext | after their usage is completed | Z2 | FIDO Agreement ECC Private Key:Derived From External Agreement ECC Public Key:Derived From |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | | | | | FIDO SharedSecret AES Key:Derives<br>FIDO SharedSecret HMAC Key:Derives |
| FIDO SharedSecret AES Key | | CHIPRAM(S1):Plaintext | | Z5 | FIDO Agreement sharedSecret:Derived From |
| FIDO SharedSecret HMAC Key | | CHIPRAM(S1):Plaintext | | Z5 | FIDO Agreement sharedSecret:Derived From |
| FIDO PinUvAuthToken | Output encapsulated by KTS-Wrap AES-CBC with HMAC (IO5) | CHIPRAM(S1):Plaintext | after their usage is completed | Z5 | FIDO SharedSecret AES Key:Wrapped by<br>FIDO SharedSecret HMAC Key:Wrapped by |
| FIDO PIN | Input encapsulated by KTS-Wrap AES-CBC with HMAC (IO4) | CHIPNVM(S4):Encrypted | | Z5 | |
| PIV Authentication Key | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S3):Encrypted | | Z6 | Managing Key:Encrypted by<br>KSenc:Unwrapped by<br>KSmac:Unwrapped by |
| PIV ECC Signature Private Key | | CHIPNVM(S3):Encrypted | | Z6 | PIV ECC verification Public Key:Paired With<br>Managing Key:Encrypted by |
| PIV ECC verification Public Key | Output in plaintext (IO8) | CHIPNVM(S6):Plaintext | | Z6 | PIV ECC Signature Private Key:Paired With |
| PIV RSA Signature Private Key | | CHIPNVM(S3):Encrypted | | Z6 | PIV RSA verification Public Key:Paired With<br>Managing Key:Encrypted by |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| PIV RSA verification Public Key | Output in plaintext (IO8) | CHIPNVM(S6):Plaintext | | Z6 | PIV RSA Signature Private Key:Paired With |
| PIV User PIN | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z6 | KSenc:Unwrapped by KSmac:Unwrapped by |
| PIV PUK PIN | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z6 | KSenc:Unwrapped by KSmac:Unwrapped by |
| 2003 Internal Auth Key | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S3):Encrypted | | Z3 | Managing Key:Encrypted by KSenc:Unwrapped by KSmac:Unwrapped by |
| 2003 External Auth Key | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S3):Encrypted | | Z3 | Managing Key:Encrypted by KSenc:Unwrapped by KSmac:Unwrapped by |
| 2003 PIN | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z3 | |
| 2003 PSO calculation key | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S3):Encrypted | | Z3 | Managing Key:Encrypted by KSenc:Unwrapped by KSmac:Unwrapped by |
| 2003 Unblock PIN | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z3 | Managing Key:Encrypted by KSenc:Unwrapped by KSmac:Unwrapped by |
| 2003 RSA Private Key | | CHIPNVM(S3):Encrypted | | Z3 | 2003 RSA Public Key:Paired With Managing Key:Encrypted by |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| 2003 RSA Public Key | Output in plaintext (IO8) | CHIPNVM(S6):Plaintext | | Z3 | 2003 RSA Private Key:Paired With |
| 2003 ECDSA Private Key | | CHIPNVM(S3):Encrypted | | Z3 | Managing Key:Encrypted by<br>2003 ECDSA Public Key:Paired With |
| 2003 ECDSA Public Key | Output in plaintext (IO8) | CHIPNVM(S6):Plaintext | | Z3 | 2003 ECDSA Private Key:Paired With |
| OTP HMAC Seed Key | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S3):Encrypted | | Z1 | Managing Key:Encrypted by<br>KSenc:Unwrapped by<br>KSmac:Unwrapped by |
| OTP AccessCode | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z8 | KSenc:Unwrapped by<br>KSmac:Unwrapped by |
| PGP Admin PIN(PW3) | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z4 | KSenc:Unwrapped by<br>KSmac:Unwrapped by |
| PGP User PIN(PW1) | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S4):Encrypted | | Z4 | KSenc:Unwrapped by<br>KSmac:Unwrapped by |
| PGP Resetting Code | Input encapsulated by KTS-Wrap SCP03(IO1) | CHIPNVM(S3):Encrypted | | Z4 | KSenc:Unwrapped by<br>KSmac:Unwrapped by |
| PGP Signature Private Key | | CHIPNVM(S3):Encrypted | | Z4 | Managing Key:Encrypted by<br>PGP Verification Public Key:Paired With |
| PGP Verification Public Key | Output in plaintext (IO8) | CHIPNVM(S6):Plaintext | | Z4 | PGP Signature Private Key:Paired With |
| External Agreement ECC Public Key | Input in plaintext (IO6) | CHIPRAM(S1):Plaintext | | Z2 | FIDO Agreement ECC Private Key:Used With |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | | | | | FIDO Agreement sharedSecret:Derives |

Table 20: SSP Table 2


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

## 9.5 Transitions

The SHA-1 algorithm as implemented by the module will be non-approved for all purposes, starting January 1, 2031.


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

# 10 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.

## 10.1 Pre-Operational Self-Tests

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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| FIPS_CRC16_FIT | CRC-16 | KAT | SW/FW Integrity | 9000 or 6F90 | Executed on the whole firmware stored in EEPROM before the Module transition to the idle state. |

Table 21: 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 Encrypt | AES-128-bit - ECB | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | AES Encryption | Bootup |
| AES Decrypt | AES-128-bit - ECB | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | AES decryption | Bootup |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CMAC | AES-128-bit CMAC | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | Message Authentication | Bootup |
| AES-GCM Encrypt | AES-128-bit GCM | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | Authenticated encryption | Bootup |
| AES-GCM Decrypt | AES-128-bit GCM | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | Authenticated decryption | Bootup |
| Counter DRBG | AES-128-bit- ECB | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | AES-128 CTR_DRBG instantiation, generate, and reseed KATs performed before the first random data generation | Bootup |
| KAS-ECC Sp800-56Ar3 | ECDH: P-256 HKDF: Using HMAC-Two step | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | KAS-SSC Shared Secret generation with P-256 per IG D.F. | Bootup |
| ECDSA KeyGen (FIPS186-5) | ECDSA Key Generation | PCT | PCT | 9000(meaning Successful) or 6F90(meaning fail) | Signature and Verification Per IG C.A | Generate ECDSA key pairs |
| ECDSA SigGen (FIPS186-5) | ECDSA Signature Generation | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | ECDSA P-256 with SHA-256 Signature Generation | Bootup |
| ECDSA SigVer (FIPS186-5) | ECDSA Signature Verification | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | ECDSA P-256 with SHA-256 Signature Verification | Bootup |
| HMAC-SHA2-256 | using HMAC-SHA256 | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | HMAC-SHA-256 KAT | Bootup |
| RSA KeyGen (FIPS186-5) | 2048-bit 3072-bit 4096-bit RSA Key Generation Pairwise Consistency Test | PCT | PCT | 9000(meaning Successful) or 6F90(meaning fail) | Signature and Verification per IG C.E. | Generate RSA key pairs |


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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| RSA SigVer (FIPS186-5) | 2048-bit RSA Signature Verification | KAT | CAST | 9000 or 6F90 | 2048-bit RSA PKCSv1.5 with SHA-256 Signature Verification | Bootup |
| RSA SigGen (FIPS186-5) | 2048-bit RSA Signature Generation | KAT | CAST | 9000 or 6F90 | 2048-bit RSA PKCSv1.5 with SHA-256 Signature Generation | Bootup |
| SHA-1 | SHA-1 | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | SHA-1 | Bootup |
| SHA2-256 | SHA2-256 | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | SHA2-256 | Bootup |
| SHA2-384 | SHA2-384 | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | SHA2-384 | Bootup |
| SHA2-512 | SHA2-512 | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | SHA2-512 | Bootup |
| KDF SP800-108 | Using AES128 CMAC | KAT | CAST | 9000(meaning Successful) or 6F90(meaning fail) | AES128 CMAC KAT | Bootup |
| Entropy 90B Start-up Repetition Count Test (RCT) | Repetition Count Test | RCT | CAST | Success or Failure Code | As specified in [90B] RCT startup health tests | At boot up |
| Entropy 90B Start-up Adaptive Proportion Test (APT) | Adaptive Proportion Test | APT | CAST | Success or Failure Code | As specified in [90B] APT startup health tests | At boot up |
| Entropy 90B Continuous Repetition Count Test (RCT) | Repetition Count Test | RCT | CAST | Success or Failure Code | As specified in [90B] RCT continuous health tests | Continuous when entropy is requested |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| Entropy 90B Continuous Adaptive Proportion Test (APT) | Adaptive Proportion Test | APT | CAST | Success or Failure Code | As specified in [90B] APT continuous health tests | Continuous when entropy is requested |

Table 22: Conditional Self-Tests

## 10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| FIPS_CRC16_FIT | KAT | SW/FW Integrity | every 1000 services are processed or power on | performed by the Module programmatically |

Table 23: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES Encrypt | KAT | CAST | every 1000 services are processed or power on | Automatic |
| AES Decrypt | KAT | CAST | every 1000 services are processed and power on | Automatic |
| AES-CMAC | KAT | CAST | every 1000 services are processed or power on | Automatic |
| AES-GCM Encrypt | KAT | CAST | every 1000 services are processed or power on | Automatic |
| AES-GCM Decrypt | KAT | CAST | every 1000 services are processed or power on | Automatic |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Counter DRBG | KAT | CAST | every 1000 services are processed or power on | Automatic |
| KAS-ECC Sp800-56Ar3 | KAT | CAST | every 1000 services are processed or power on | Automatic |
| ECDSA KeyGen (FIPS186-5) | PCT | PCT | Everytime a key pair is generated | Automatic |
| ECDSA SigGen (FIPS186-5) | KAT | CAST | every 1000 services are processed or power on | Automatic |
| ECDSA SigVer (FIPS186-5) | KAT | CAST | every 1000 services are processed or power on | Automatic |
| HMAC-SHA2-256 | KAT | CAST | every 1000 services are processed or power on | Automatic |
| RSA KeyGen (FIPS186-5) | PCT | PCT | Everytime a key pair is generated | Automatic |
| RSA SigVer (FIPS186-5) | KAT | CAST | every 1000 services are processed or power on | Automatic |
| RSA SigGen (FIPS186-5) | KAT | CAST | every 1000 services are processed or power on | Automatic |
| SHA-1 | KAT | CAST | every 1000 services are processed or power on | Automatic |
| SHA2-256 | KAT | CAST | every 1000 services are processed or power on | Automatic |
| SHA2-384 | KAT | CAST | every 1000 services are processed or power on | Automatic |
| SHA2-512 | KAT | CAST | every 1000 services are processed or power on | Automatic |
| KDF SP800-108 | KAT | CAST | every 1000 services are processed and power on | Automatic |
| Entropy 90B Start-up Repetition Count Test (RCT) | RCT | CAST | On Demand | Device Reset |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Entropy 90B Start-up Adaptive Proportion Test (APT) | APT | CAST | On Demand | Device Reset |
| Entropy 90B Continuous Repetition Count Test (RCT) | RCT | CAST | N/A | N/A |
| Entropy 90B Continuous Adaptive Proportion Test (APT) | APT | CAST | N/A | N/A |

Table 24: Conditional Periodic Information

The condition of initiating Periodic Self-Test is to execute every 1000 services. Once every 1000 services being executed, the periodic self-test function will call Pre-Operational Self-Tests and Conditional Self-Tests.

Self-test failures are indicated to the user through LED status and service return status.

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

## 10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| ES1 | The Module fails at CRC16 FIT, ENT RCT and APT, CTR DRBG KAT, ECDSA KAT, RSA KAT, AES ECB KAT, AES CMAC KAT, AES GCM KAT, HMAC KAT, KBKDF KAT, KAS-ECC KAT, SHS KAT, RSA Generate key pair PCT, ECC Generate key pair PCT | The Module enters Critical error state. | Reboot/Power cycle the module | 6F90 and blinking LED |

Table 25: Error States

## 10.5 Operator Initiation of Self-Tests

All self-tests, except for the continuous health tests, can be invoked on demand by restarting the module.


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

# 11 Life-Cycle Assurance

## 11.1 Installation, Initialization, and Startup Procedures

**Installation and Initialization:**

The following steps must be performed in order to securely install, initialize, and start up the ST3 Ace Token cryptographic module in the FIPS 140-3 Approved mode of operation.

The steps for the CO to enter the module and change the default password gain authorized access to the module.

The module is setup at manufacturing and delivered to the CO in approved mode.

**Delivery:**
The following steps must be performed in order to securely deliver the ST3 Ace Token cryptographic module to the authorized operator:

1. Set the required keys in a secure factory environment
2. Complete packaging and user manual
3. Shipping the modules to the final customer. For each shipment, our factory will use the courier agreed with customer, such as FedEx or DHL. Our factory will inform customer in advance with the shipment info by email. When the goods arriving in customer site, the customer will first check the goods according to the shipment info they received, and sign for acceptance.
4. The final customer check the module information according to administrator manual.

## 11.2 Administrator Guidance

Refer to Securemetric ST3 Ace Token Cryptographic Module Administrator Guidance.docx, which will be provided to the issuer through secure communications.

## 11.3 Non-Administrator Guidance

Refer to Securemetric ST3 Ace Token Cryptographic Module Non-Administrator Guidance.docx, which will be provided to the issuer through secure communications.

## 11.4 Design and Rules

### 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 power or resetting the Module.


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

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 concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not have any proprietary external input/output devices used for entry/output of data.
13. The Module does not enter or output plaintext CSPs.
14. The Module does not store any plaintext CSPs.
15. The Module does not output intermediate key values.
16. The Module does not provide bypass services or ports/interfaces.

## 11.5 Maintenance Requirements

The module does not require any maintenance requirements

## 11.6 End of Life

Administrator SHALL invoke Terminate token service after authentication to switch device into the terminated state as a result, all CSPs are cleared, and all services are not available anymore. The device shall be destroyed.

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

# 12 Mitigation of Other Attacks

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


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

# References and Definitions

The following standards are referred to in this Security Policy.

Table 26 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, October 23, 2024 |
| [108r1] | NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), August 2022 INCLUDES UPDATES AS OF 02-02-2024 |
| [133] | NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020 |
| [135] | National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011. |
| [186] | National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 3, 2023. |
| [197] | National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, May 9, 2023 |
| [198-1] | 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 |
| [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 |
| [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 |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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

| Abbreviation | Full Specification Name |
|---|---|
| [56Ar3] | NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018 |
| [56Br2] | NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019 |
| [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 27 Acronyms and Definitions

| Acronym | Definition |
|---|---|
| APT | Adaptative Proportion Test |
| KAT | Know Answer Test |
| RCT | Repetition Count Test |
| SSP | Sensitive Security Parameter |
| PCT | Pairwise Consistency Test |
| KDF | Key Derivation Function |
| KTS | Key Transport Scheme |
| KAS | Key Agreement Scheme |
| VCC | Voltage(at the) Common Collector |
| PIN | Personal Identification Number |
| PGP User PIN (PW1) | user-password |
| PGP Admin PIN (PW3) | admin-password |
| CO | Crypto Officer |
| PUK | PIN Unblocking Key |

Copyright Securemetric Technology Sdn. Bhd., 2026 Version 1.0.0

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