Google, LLC.

OpenSK Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
October 15th, 2025

Prepared by:

Lightship Security

www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Google, LLC. OpenSK Cryptographic Module (running firmware version 4.0.2), hereafter referred to as, “the module”. It contains the security rules under which the module must operate and describes how the module meets the requirements as specified in FIPS PUB 140-3 for an overall Security Level 1 cryptographic module.

1.2 Security Levels

The table below describes the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

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

Table 1: Security Levels

The Module has an overall security level of 1.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module is a USB 1.1/2.0 compliant Client To Authenticator Protocol (CTAP) 2.1 token, instantiated as a single chip hardware module, used for first or second factor authentication. It is also backwards compatible with Universal 2nd Factor (U2F, also known as CTAP1). CTAP standardizes how request and response messages are sent over the USB transport to the CTAP key.

After registration, a user can use their Security Key with an origin-specific key pair across all online services that implement WebAuthn. CTAP and WebAuthn are both part of FIDO2, a set of standards for online authentication. The Security Key performs two operations that focus on authentication (with a backwards compatible alternative): MakeCredential (or U2F Register) associates a key pair (or credential) with an origin, google.com here, while GetAssertion (or U2F Authenticate), verifies that signature with the Titan Security Key, Chip Boundary to prove physical possession of the hardware second factor. Then, and only then, is the User able to authenticate to Google services.

In addition, CTAP 2.1 provides functionality related to this process: GetInfo lists information about the Security Key. ClientPin allows setting up a PIN to unlock some of the Security Key commands. Reset performs a factory reset by deleting all stored user data, including credentials. CredentialManagement allows listing and deleting existing credentials. Selection performs a user presence check, so users can indicate what device they want to use. LargeBlobs lets you read and write a binary string to store inside the security key.

There are two custom commands that are not part of the CTAP specification. Both are used for upgrading the firmware: One that provides detailed information about the running firmware version, and the other to send the new, signed firmware binary.

The chip runs a version of OpenSK that manages all access control, cryptographic algorithms and the life cycle of all keys. OpenSK is an app running on top of a version of TockOS, which manages all low-level resources.

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary of the module is the outer perimeter of the chip, as shown in the figures below.

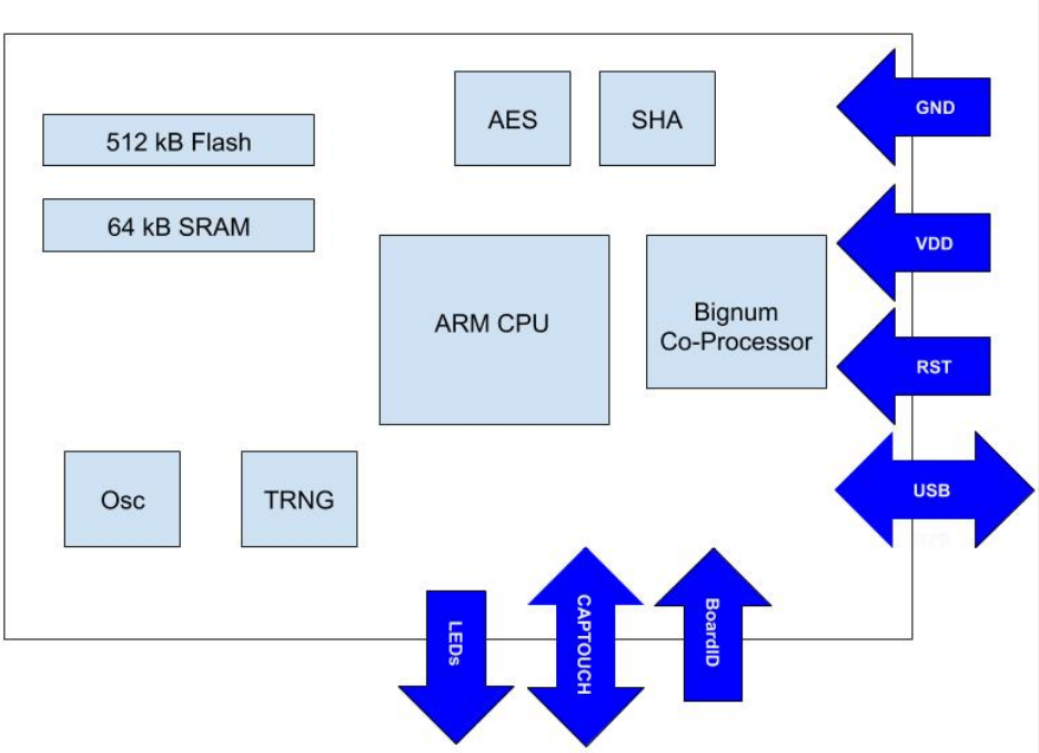

Figure 1: OpenSK Cryptographic Module (Block Diagram)

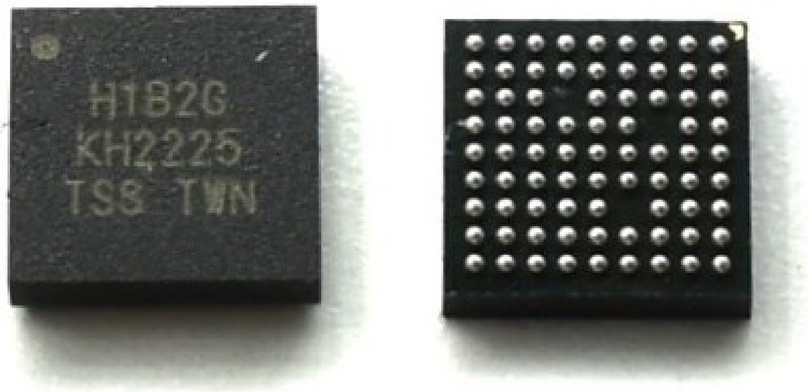

Figure 2: OpenSK Cryptographic Module (Front and Back)

Tested Operational Environment's Physical Perimeter (TOEPP):

The module is a single-chip module as defined by FIPS 140-3. The hardware version of the module is H1B2G.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
OpenSK Cryptographic Module	H1B2G	OpenSK 4.0.2	N/A	

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

There are no components within the cryptographic boundary that are excluded from the FIPS 140-3 security requirements.

2.4 Modes of Operation

Modes List and Description:

The table below details the Modes of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	Operation mode where the module executes approved services	Approved	The module always operates in the approved mode

Table 3: Modes List and Description

Mode Change Instructions and Status:

The module implements only one mode of operation, the approved mode, in which the approved services are available. No configuration is necessary for the module to operate and remain in the approved mode.

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode.

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5101	-	SP 800-38A
AES-ECB	A5101	-	SP 800-38A
ECDSA KeyGen (FIPS186-4)	A5101	-	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A5101	-	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A5101	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5101	-	FIPS 186-4
HMAC DRBG	A5101	-	SP 800-90A Rev. 1
HMAC-SHA2-256	A2352	-	FIPS 198-1
HMAC-SHA2-256	A5101	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5101	-	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A5101	-	SP 800-56C Rev. 2
SHA2-256	A2352	-	FIPS 180-4
SHA2-256	A5101	-	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The table below lists all the Vendor-Affirmed Algorithms supported by the module.

Name	Properties	Implementation	Reference
CKG	CKG:Cryptographic Key Generation Publication:NIST SP 800-133r2 Sections 4, 5, and 6	Titan OpenSK Gnubby cryptographic library	FIPS 140-3 IG D.H

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The table below lists all the Non-Approved, Allowed Algorithms supported by the module.

Name	Properties	Implementation	Reference
KDF	KDF:Asymmetric Key Derivation Method	Titan OpenSK Gnubby cryptographic library	N/A

Table 6: Non-Approved, Allowed Algorithms

Non-Approved, Allowed Algorithms with No Security Claimed:

The table below lists all the Non-Approved, Allowed Algorithms with No Security Claimed.

Name	Caveat	Use and Function
LargeBlobKey FIDO extension	FIPS 140-3 IG 2.4.A	Encoding up to 256 bits

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

The module supports largeBlobKey FIDO extension functionality where an external party can encode an arbitrary string of bits on the device. No security is claimed for this encoded arbitrary data is considered the equivalent to plaintext.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved Algorithms that are not Allowed in the Approved Mode of Operation.

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Data Encryption/Decryption	BC-UnAuth	Symmetric Encryption/Decryption	Publication:NIST SP 800-38A	AES-CBC: (A5101) AES-ECB: (A5101)
Asymmetric Key Generation	AsymKeyPair-KeyGen AsymKeyPair-KeyVer	Asymmetric Key Pair Generation and Verification	Publication:FIPS 186-4 Publication: NIST SP 800-133r2	ECDSA KeyGen (FIPS186-4): (A5101) ECDSA KeyVer (FIPS186-4): (A5101) CKG: () CKG: Cryptographic Key Generation Publication: NIST SP 800-133r2 Sections 4, 5, and 6
Digital Signature	DigSig-SigGen DigSig-SigVer	Digital Signature Generation and Verification	Publication:FIPS 186-4	ECDSA SigGen (FIPS186-4): (A5101) ECDSA SigVer (FIPS186-4): (A5101)
Deterministic Random Bit Generation	DRBG	Deterministic Random Bit Generation	Publication:SP 800-90Ar1	HMAC DRBG: (A5101)
Message Authentication FW	MAC	MAC Generation and Verification	Publication:FIPS 198-1	HMAC-SHA2-256: (A5101)
Key Agreement ECC	KAS-SSC	Key Agreement	Publication:NIST SP 800-56Ar3	KAS-ECC-SSC Sp800-56Ar3: (A5101)
Key Derivation Function	KBKDF	Key Derivation Function	Publication:NIST SP 800-56Cr2	KDA HKDF SP800-56Cr2: (A5101)

Name	Type	Description	Properties	Algorithms
Message Digest FW	SHA	Hashing	Publication:FIPS 180-4	SHA2-256: (A5101)
Message Authentication	MAC	MAC Generation and Verification	Publication:FIPS 198-1	HMAC-SHA2-256: (A2352)
Message Digest	SHA	Hashing	Publication:FIPS 180-4	SHA2-256: (A2352)
Key Transport	KTS-Wrap	Key Transport	Publication:FIPS 140-3 IG D.G	AES-CBC: (A5101) HMAC-SHA2-256: (A5101)
Symmetric Key Generation	CKG	Symmetric Key Generation	Publication:NIST SP 800-133r2	CKG: () CKG: Cryptographic Key Generation Publication: NIST SP 800-133r2 Sections 4, 5, and 6

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

There is no algorithm specific information.

2.8 RBG and Entropy

The tables below detail the modules ESV information.

Cert Number	Vendor Name
E147	Google

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Titan Security Key TRNG Implementation	Physical	Google H1B2	256 bits	256 bits	A2352 (SHA2-256)

Table 10: Entropy Sources

The module generates a minimum of 256 bits of entropy for key generation.

2.9 Key Generation

The module generates Keys and SSPs in accordance with FIPS 140-3 IG D.H. The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per SP 800-133r2 (vendor affirmed), compliant with FIPS 186-4, and using DRBG compliant with SP 800-90A]. A seed (the random value) used in asymmetric key generation is obtained from SP 800-90A DRBG. The key generation service for ECDSA, as well as the SP 800-90A DRBG have been ACVP tested with algorithm certificates found in Approved Algorithms Table.

2.10 Key Establishment

The module provides SP 800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with ECDH shared secret computation. A Hash-Based KDF specified in NIST SP 800-56Crev2 is used as the Key Derivation Algorithm.

The module provides key transport according to FIPS 140-3 IG D.G using an approved key wrapping technique based on AES-CBC and HMAC-SHA2-256.

2.11 Industry Protocols

The module does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The table below details the module Ports and Interfaces.

Physical Port	Logical Interface(s)	Data That Passes
USB pins (D+ and D-)	Data Input Data Output Control Input Status Output	HID command and parameters for data, HID input parameters for control
LED pins	Status Output	Signals (high/low)
VDD pins	Power	Power
GND pins	Control Input	N/A
RST pins	Control Input	N/A
BoardID pins	Status Output	Status values
CAPTOUCH pins	Control Input	Circuit (high/low)
NC (Not Connected)	None	N/A

Table 11: Ports and Interfaces

All communication between the module and a host device is conducted in accordance with the U2F and CTAP protocol. The U2F protocol is based on a request-response mechanism, where a requester sends a request message to a U2F device, which always results in a response message being sent back from the U2F device to the requester. All request-response messages are framed in ISO7816-4:2005 APDU format. This specifies how to transport the raw message and any error codes if the command failed.

The CTAP2 protocol supports longer messages using CTAPHID. The CTAPHID messages are encoded in CBOR.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication for roles.

N/A for this module.

4.2 Roles

The module supports two roles that an operator may assume: Crypto Officer (CO) role and User role. Roles are assumed implicitly based on the service accessed. The table below lists the roles supported by the module.

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None
User	Role	User	None

Table 12: Roles

4.3 Approved Services

The table below lists all approved services supported by the module. The abbreviations of the access rights to keys and SSPs have the following interpretation:

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.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialization	Connect to host over USB	N/A	None	None	None	Crypto Officer
Wink Command	Command issued to device to blink LEDs	N/A	APDU over HID command	Status output to LED pin	None	Crypto Officer
FIDO U2F: U2F_Register	Create a U2F credential	Success or Fail	APDU over HID command and parameters	APDU over HID command and response / Status output to LED pin	Asymmetric Key Generation Digital Signature Deterministic Random Bit Generation Message Digest FW Key Transport	User - DRBG Entropy Input: G,E - DRBG Seed: E - DRBG V: E - DRBG Key: E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Symmetric Key Generation	Individual Attestation Deterministic Seed: G,E - Individual Attestation Signing (Private) Key: G,E - Batch Attestation Deterministic Seed: G,E - Batch Attestation Signing (Private) Key: G,E - Personality Deterministic Seed: G,E - Key Handle Encryption Key: G - Key Handle Authentication Deterministic Seed: G,E - Key Handle Authentication Key: G - U2F/Server-Side Determini

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						stic Seed: W,E - U2F/Server-Side Signing (Private) Keys (Legacy): G - U2F/Server-Side Signing (Public) Keys (Legacy): G,R - Batch Attestation Signing (Public) Key: R - Individual Attestation Signing (Public) Certificate: R
FIDO U2F: U2F_Authenticate	Sign to Authenticate	Success or Fail	APDU over HID command and parameters	APDU over HID command and response / Status output to LED pin	Data Encryption/Decryption Digital Signature Deterministic Random Bit Generation Message Authentication FW Message Digest FW	User - DRBG Entropy Input: G,E - DRBG Seed: E - DRBG V: E - DRBG Key: E - Key Handle Encryption Key: E - Key Handle Authentication Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- U2F/Server-Side Signing (Private) Keys (Legacy): E
FIDO U2F: U2F_Version	Show U2F version string	Success or Fail	APDU over HID command	APDU over HID command and response / Status output to LED pin	None	User
FIDO2_Make_Credential	Create a FIDO2 credential	Success or Fail	CTAP HID command and parameters	CTAP HID command and response / Status output to LED pin	Data Encryption/Decryption Asymmetric Key Generation Deterministic Random Bit Generation Key Transport	User - DRBG Entropy Input: G,E - DRBG Seed: E - DRBG V: E - DRBG Key: E - Resident Signing (Private) Keys: G - PIN UV Auth Token: R,E - FIDO2/Server-Side Deterministic Seed: W,E - FIDO2/Server-Side Signing (Private) Keys : G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- FIDO2/Server-Side Signing (Public) Keys: G,R - Resident Signing (Public) Keys: G,R
FIDO2_Get_Assertion	Sign to Authenticate	Success or Fail	CTAP HID command and parameters	CTAP HID command and response / Status output to LED pin	Data Encryption/Decryption Asymmetric Key Generation Digital Signature Deterministic Random Bit Generation Message Authentication FW Key Derivation Function Message Digest FW Key Transport Symmetric Key Generation	User - DRBG Entropy Input: G,E - DRBG Seed: E - DRBG V: E - DRBG Key: E - Key Handle Encryption Key: E - Key Handle Authentication Key: E - U2F/Server-Side Signing (Private) Keys (Legacy): E - Resident Signing (Private) Keys: E - PIN UV Auth Token: E - CredRandom Deterministic Seed:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E - CredRandom Deriving Keys (with and without UV): G,E - CredRandom: G,E - FIDO2 HMAC Secret Salts: W,E - FIDO2 HMAC Secret Outputs: R - FIDO2/Server-Side Signing (Private) Keys : E
FIDO2_Get_Next_Assertion	Sign to Authenticate a different credential	Success or Fail	CTAP HID command	CTAP HID command and response / Status output to LED pin	Data Encryption/Decryption Asymmetric Key Generation Digital Signature Deterministic Random Bit Generation Message Authentication FW Key Derivation Function Message Digest FW Key Transport Symmetric Key Generation	User - DRBG Entropy Input: G,E - DRBG Seed: G,E - DRBG V: G,E - DRBG Key: G,E - Key Handle Encryption Key: E - Key Handle Authentication Key: E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						U2F/Server-Side Signing (Private) Keys (Legacy): E - Resident Signing (Private) Keys: E - CredRandom Deterministic Seed: G,E - CredRandom Deriving Keys (with and without UV): G,E - CredRandom: G,E - FIDO2 HMAC Secret Salts: W,E - FIDO2 HMAC Secret Outputs: R - FIDO2/Server-Side Signing (Private) Keys : E
FIDO2_Get_Info	Show device information	Success or Fail	CTAP HID command	CTAP HID command and respon	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				se / Status output		
FIDO2_Client_Pin	Setup / Change / Use a PIN	Success or Fail	CTAP HID command and parameters	CTAP HID command and response / Status output to LED pin	Data Encryption/Decryption Asymmetric Key Generation Deterministic Random Bit Generation Message Authentication FW Key Agreement ECC Key Derivation Function Message Digest FW Key Transport	User - DRBG Entropy Input: G,E - DRBG Seed: E - DRBG V: E - DRBG Key: E - PIN Protocol Agreement Key: G,E - PIN Protocol Deriving Z: G,E - PIN Protocol Encryption Key: G,E - PIN Protocol Authentication Key: G,E - PIN UV Auth Token: G,R,E - PIN: W - PIN Hash: E - PIN Hash Attemp: W - Pin Protocol Agreement (Public) Key: G,R - PIN

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Protocol Deriving (Public) Key: W,E
FIDO2_Reset	Factory reset	Module reset to factory	CTAP HID command	CTAP HID command and response / Status output to LED pin	None	User - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG V: Z - DRBG Key: Z - Personality Deterministic Seed: Z - Individual Attestation Deterministic Seed: Z - Batch Attestation Deterministic Seed: Z - Key Handle Authentication Deterministic Seed: Z - Batch Attestation Signing (Private) Key: Z - Individual Attestation Signing

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(Private) Key: Z - Key Handle Encryption Key: Z - Key Handle Authentication Key: Z - U2F/Server-Side Signing (Private) Keys (Legacy): Z - FIDO2/Server-Side Signing (Private) Keys : Z - Resident Signing (Private) Keys: Z - PIN Protocol Agreement Key: Z - PIN Protocol Deriving Z: Z - PIN Protocol Encryption Key: Z - PIN Protocol Authentication Key: Z - PIN UV Auth Token: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIN: Z - PIN Hash: Z - PIN Hash Attemp: Z - CredRandom Deterministic Seed: Z - CredRandom Deriving Keys (with and without UV): Z - CredRandom: Z - FIDO2 HMAC Secret Salts: Z - FIDO2 HMAC Secret Outputs: Z - Pin Protocol Agreement (Public) Key: Z - PIN Protocol Deriving (Public) Key: Z - U2F/Server-Side Signing (Public) Keys (Legacy):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - FIDO2/Server-Side Signing (Public) Keys: Z - Resident Signing (Public) Keys: Z - U2F/Server-Side Deterministic Seed: Z - FIDO2/Server-Side Deterministic Seed: Z
FIDO2_Credential_Management	Enumerate and delete credentials	Success or Fail	Success or Fail	CTAP HID command and response / Status output to LED pin	None	User - PIN UV Auth Token: E,Z - FIDO2/Server-Side Signing (Public) Keys: R
FIDO2_Selection	Touch to choose device	Success or Fail	CTAP HID command	Status output to LED pin	None	User
FIDO2_Large_Blobs	Store binary data	Success or Fail	CTAP HID command and parameters	CTAP HID command and response / Module status	None	User - PIN UV Auth Token: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Vendor_Upgrade	Firmware upgrade	Success or Fail	CTAP HID command and parameters	Status Output	Digital Signature	Crypto Officer
Vendor_Sysinfo	Show vendor specific information	Return module version information	CTAP HID command	CTAP HID command and response / Module status	None	Crypto Officer
Show Status	Return the module status	None	None	Module status	None	User
On-Demand Self-test	Initiate on-demand self-tests by reboot or power cycle	None	None	Pass or Fail	Data Encryption/Decryption Asymmetric Key Generation Digital Signature Deterministic Random Bit Generation Message Authentication FW Key Agreement ECC Key Derivation Function Message Digest FW Message Authentication Message Digest	Crypto Officer

Table 13: Approved Services

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports external firmware loaded for upgrades. An Approved ECDSA Signature Verification (P-256, SHA2-256) firmware load test operation is performed prior to a firmware upgrade.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the executable firmware is verified by comparing a SHA2-256 digest calculated at boot time with the SHA2-256 digest value stored in the module that was computed at build time.

5.2 Initiate on Demand

The integrity test is performed as part of the pre-operational self-tests, which are executed when the module is initialized. The integrity test can be invoked on demand via reboot or power-cycle the module, which will perform (among others) the firmware integrity test.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The limited modifiable operational environment of the module prevents users from accessing secret keys, private keys or SSPs which they are not authorized to access. There was no logical or physical access to the SSPs.

The module is designed to accept only controlled firmware changes that successfully pass the software/firmware load test.

7 Physical Security

7.1 Mechanisms and Actions Required

The table below details the Physical Security Mechanisms supported by the module.

Mechanism	Inspection Frequency	Inspection Guidance
N/A	N/A	N/A

Table 14: Mechanisms and Actions Required

The module has a single-chip embodiment that employs standard passivation techniques and meets commercial grade specs regarding power and voltage ranges, temperature, reliability, and shock/vibration. The module is encased in an opaque, tamper-evident, removal-resistant IC packaging material which cannot be removed or penetrated without causing serious damage to the module (i.e. the module will not function).

7.2 EFP/EFT Information

The table below details the module Environmental Failure Testing information.

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-20° C	EFT	Environmental Failure
HighTemperature	85° C	EFT	Environmental Failure
LowVoltage	2V	EFT	Environmental Failure
HighVoltage	6V	EFT	Environmental Failure

Table 15: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

The table below details the module Hardness Testing Temperature Ranges.

Temperature Type	Temperature
LowTemperature	-5°C
HighTemperature	+70°C

Table 16: Hardness Testing Temperatures

8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The table below lists Sensitive Security Parameters (SSPs) storage areas for the module. Section 9.4 below selects from the storage areas listed and specifies the appropriate parameter in the "Storage" column if applicable to a specific SSP.

Storage Area Name	Description	Persistence Type
RAM	Random Access Memory	Dynamic
Flash	Flash Memory	Static

Table 17: Storage Areas

9.2 SSP Input-Output Methods

The table below lists SSP input and output methods for the module. Section 9.4 below selects from the input and output methods listed and specifies the appropriate parameter in the "Inputs/Outputs" column if applicable to a specific SSP.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
PSP Export	RAM	Outside	Plaintext	N/A	N/A	
PIN Protocol Output	RAM	Outside	Encrypted	Automated	Electronic	Key Transport

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The table below lists SSP zeroisation methods for this module. Section 9.4 below selects from the zeroisation methods listed and specifies the appropriate parameter in the "Zeroization" column if applicable to a specific SSP.

Zeroization Method	Description	Rationale	Operator Initiation
Reboot	Zeroisation when module is rebooted	Keys are procedurally zeroised by rebooting the module, which is acceptable at Security Level 1	Crypto Officer by rebooting the host system
Reset command	Zeroisation when the module is reset	Keys are automatically zeroised by resetting the module, which is acceptable at Security Level 1	Crypto Officer or User by resetting the module
Remove power	Zeroisation when power is removed from the module	Keys are procedurally zeroised by rebooting the module, which is acceptable at Security Level 1	Crypto Officer by removing power

Zeroization Method	Description	Rationale	Operator Initiation
Environmental Failure	Zeroisation when the temperature or voltage falls outside the module's normal operating ranges	Keys are automatically zeroised by a power cycle, which is acceptable at Security Level 1	Automatically when an environmental failure occurs

Table 19: SSP Zeroization Methods

9.4 SSPs

The following table summarizes the keys and Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Input bitstring that provides an assessed minimum amount of unpredictability for the DRBG mechanism	256 - 256	DRBG Parameter - CSP	Factory Loaded and Internal TRNG		Deterministic Random Bit Generation
DRBG Seed	A string of bits that is used as input to a DRBG mechanism	256 - 256	Seed - CSP			Deterministic Random Bit Generation
DRBG V	Secret value of the DRBG internal state	N/A - N/A	Internal Value - CSP			Deterministic Random Bit Generation
DRBG Key	Secret value of the DRBG internal state	N/A - N/A	Symmetric Key - CSP			Deterministic Random Bit Generation
Personality Deterministic Seed	Parameter related to user credentials (key handle, user). Used to derive	256 - 256	Deterministic Seed - CSP	Allowed KDF Method		Deterministic Random Bit Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	the Key Handle Encryption Key					
Individual Attestation Deterministic Seed	Deterministic seed used to derive the Individual Attestation Key	256 - 256	Deterministic Seed - CSP	Allowed KDF Method		Deterministic Random Bit Generation
Batch Attestation Deterministic Seed	Deterministic seed used to derive the Batch Attestation Key	256 - 256	Deterministic Seed - CSP	Allowed KDF Method		Deterministic Random Bit Generation
Key Handle Authentication Deterministic Seed	Deterministic seed used to derive the Key Handle Authentication Key	256 - 256	Deterministic Seed - CSP	Allowed KDF Method		Deterministic Random Bit Generation
Batch Attestation Signing (Private) Key	Used for signature in U2F and FIDO2 registration during batch attestation	256 - 256	Private Key - CSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature
Individual Attestation Signing (Private) Key	Used for signature in U2F and FIDO2 registration during enterprise attestation	256 - 256	Private Key - CSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Key Handle Encryption Key	Encrypt server-side credentials	256 - 256	Symmetric Key - CSP	Deterministic Random Bit Generation Symmetric Key Generation		Data Encryption/Decryption
Key Handle Authentication Key	Authenticate server-side credentials	256 - 256	Authentication Key - CSP	Deterministic Random Bit Generation Symmetric Key Generation		Message Authentication FW
U2F/Server-Side Signing (Private) Keys (Legacy)	Private key for core Legacy FIDO functionality	256 - 256	Private Key - CSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature
FIDO2/Server-Side Signing (Private) Keys	Private key for core FIDO2 functionality	256 - 256	Private Key - CSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature
Resident Signing (Private) Keys	Private key for core FIDO2 functionality	256 - 256	Private Key - CSP	Asymmetric Key Generation Deterministic Random		Digital Signature

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				Bit Generation		
PIN Protocol Agreement Key	Module's pin protocol agreement private key	256 - 256	Private Key - CSP	Asymmetric Key Generation Deterministic Random Bit Generation		Key Agreement ECC
PIN Protocol Deriving Z	Shared Secret for client PIN	256 - 256	Shared Secret - CSP		Key Agreement ECC	Key Derivation Function
PIN Protocol Encryption Key	Derived shared encryption key	256 - 256	Symmetric Key - CSP	Key Derivation Function		Data Encryption/Decryption
PIN Protocol Authentication Key	Derived shared authentication key	256 - 256	Authentication Key - CSP	Key Derivation Function		Message Authentication FW
PIN UV Auth Token	Short lived authentication token	256 - 256	Authentication Token - CSP	Deterministic Random Bit Generation Symmetric Key Generation	Key Transport	Data Encryption/Decryption
PIN	User verification knowledge factor	Minimum 6 characters - 48 bits	PIN - CSP		Key Transport	
PIN Hash	Hash prefix of PIN	128 - 128	Hash Value - CSP			
PIN Hash Attemp	User guessed PIN hash	128 - 128	Hash Value - CSP		Key Transport	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CredRandom Deterministic Seed	Deterministic Seed used to derive the CredRandom Deriving Keys	256 - 256	Deterministic Seed - CSP	Allowed KDF		Deterministic Random Bit Generation
CredRandom Deriving Keys (with and without UV)	Derived keys used to derive the CredRandom	256 - 256	Symmetric Key - CSP	Deterministic Random Bit Generation Symmetric Key Generation		Key Derivation Function
CredRandom	Derived key used for hmac-secret extension	256 - 256	Derived Symmetric Key - CSP	Key Derivation Function		Message Authentication FW
FIDO2 HMAC Secret Salts	Input for hmac-secret extension	256 - 256	Salt - CSP		Key Transport	Message Authentication FW
FIDO2 HMAC Secret Outputs	Outputs for hmac-secret extension, used to do offline encryption with arbitrary user data	256 - 256	MAC Output - CSP		Key Transport	Data Encryption/Decryption
Pin Protocol Agreement (Public) Key	Module's pin protocol agreement public key	256 - 256	Public Key - PSP	Asymmetric Key Generation Deterministic Random Bit Generation		Key Agreement ECC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Batch Attestation Signing (Public) Key	Batch attestation	256 - 256	Public Key - PSP	Factory Loaded		Digital Signature
PIN Protocol Deriving (Public) Key	Client PIN Protocol agreement public key	256 - 256	Public Key - PSP		Key Agreement ECC	
U2F/Server-Side Signing (Public) Keys (Legacy)	Public key for core Legacy FIDO functionality	256 - 256	Public Key - PSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature
FIDO2/Server-Side Signing (Public) Keys	Public key for core FIDO2 functionality	256 - 256	Public Key - PSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature
Resident Signing (Public) Keys	Public key for core FIDO2 functionality	256 - 256	Public Key - PSP	Asymmetric Key Generation Deterministic Random Bit Generation		Digital Signature
Individual Attestation Signing (Public) Certificate	Used for signature in U2F and FIDO2 registration during	256 - 256	Public Certificate - PSP	Factory Loaded		Digital Signature

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	enterprise attestation					
U2F/Server-Side Deterministic Seed	Deterministic seed used to derive the U2F/Server-Side signing (Private) Keys (Legacy)	256 - 256	Deterministic Seed - CSP		Key Transport	Deterministic Random Bit Generation
FIDO2/Server-Side Deterministic Seed	Deterministic seed used to derive the FIDO2/Server-Side Signing (Private) Keys	256 - 256	Deterministic Seed - CSP		Key Transport	Deterministic Random Bit Generation

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	DRBG Seed:Used With DRBG V:Used With DRBG Key:Used With
DRBG Seed		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	DRBG Entropy Input:Used With DRBG V:Used With DRBG Key:Used With
DRBG V		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG V:Used With
Personality Deterministic Seed		Flash:Plaintext	N/A	Reset command	
Individual Attestation Deterministic Seed		Flash:Plaintext	N/A	Reset command	
Batch Attestation Deterministic Seed		Flash:Plaintext	N/A	Reset command	
Key Handle Authentication Deterministic Seed		Flash:Plaintext	N/A	Reset command	
Batch Attestation Signing (Private) Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	Batch Attestation Deterministic Seed:Derived From
Individual Attestation Signing (Private) Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	Individual Attestation Deterministic Seed:Derived From
Key Handle Encryption Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	Personality Deterministic Seed:Derived From
Key Handle Authentication Key		RAM:Plaintext	Until module loses power/reboot or	Reboot Remove power	Key Handle Authentication Deterministic

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			environmental failure occurs	Environmental Failure	Seed:Derived From
U2F/Server-Side Signing (Private) Keys (Legacy)		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	U2F/Server-Side Deterministic Seed:Derived From
FIDO2/Server-Side Signing (Private) Keys		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	FIDO2/Server-Side Deterministic Seed:Derived From
Resident Signing (Private) Keys		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
PIN Protocol Agreement Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
PIN Protocol Deriving Z		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
PIN Protocol Encryption Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	PIN Protocol Deriving (Private) Key:Derived From
PIN Protocol Authentication Key		RAM:Plaintext	Until module loses power/reboot	Reboot Remove power	PIN Protocol Deriving (Private)

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			or environmental failure occurs	Environmental Failure	Key:Derived From
PIN UV Auth Token	PIN Protocol Output	RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
PIN		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
PIN Hash		Flash:Encrypted	N/A	Reset command	
PIN Hash Attemp		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
CredRandom Deterministic Seed		Flash:Plaintext	N/A	Reset command	
CredRandom Deriving Keys (with and without UV)		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	CredRandom Deterministic Seed:Derived From
CredRandom		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	CredRandom Deriving Keys (with and without UV):Derived From
FIDO2 HMAC Secret Salts		RAM:Plaintext	Until module loses power/reboot or	Reboot Remove power	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			environmental failure occurs	Environmental Failure	
FIDO2 HMAC Secret Outputs	PIN Protocol Output	RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
Pin Protocol Agreement (Public) Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	PIN Protocol Agreement Key:Paired With
Batch Attestation Signing (Public) Key	PSP Export	Flash:Plaintext	N/A	N/A	
PIN Protocol Deriving (Public) Key		RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	
U2F/Server-Side Signing (Public) Keys (Legacy)	PSP Export	RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	U2F/Server-Side Signing (Private) Keys (Legacy):Paired With
FIDO2/Server-Side Signing (Public) Keys	PSP Export	RAM:Plaintext	Until module loses power/reboot or environmental failure occurs	Reboot Remove power Environmental Failure	FIDO2/Server-Side Signing (Private) Keys :Paired With
Resident Signing (Public) Keys	PSP Export	RAM:Plaintext	Until module loses power/reboot or environmenta	Reboot Remove power Environmental Failure	Resident Signing (Private) Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			I failure occurs		
Individual Attestation Signing (Public) Certificate	PSP Export	Flash:Plaintext	N/A	N/A	
U2F/Server-Side Deterministic Seed		Flash:Plaintext	N/A	Reset command	
FIDO2/Server-Side Deterministic Seed		Flash:Plaintext	N/A	Reset command	

Table 21: SSP Table 2

9.5 Transitions

Per FIPS 140-3, IG C.K FIPS 186-4 CAVP tests performed are mathematically identical to FIPS 186-5 CAVP tests, therefore the module can claim FIPS 186-5 compliance for these tests.

10 Self-Tests

This section specifies the pre-operational and conditional self-tests performed by the module. The pre-operational and conditional self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

10.1 Pre-Operational Self-Tests

Pre-operational Self-Tests are run upon the power up/initialization of the module. The module transitions to the operational state only after the pre-operational self-tests (and the cryptographic algorithm self-tests (CASTs)) are passed successfully. The design of the module ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational self-test condition. The Pre-Operational Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A2352)	256-bit hash	Firmware Integrity	SW/FW Integrity	Status Output	Approved Hash

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Conditional Self-Tests are run when an applicable security function or process is invoked. The Conditional Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A5101)	256-bit hash	KAT	CAST	Successful initialization of the module	Hash	Module Initialization
HMAC-SHA2-256 (A5101)	256-bit key	KAT	CAST	Successful initialization of the module	MAC	Module Initialization
ECDSA SigGen (FIPS186-4) (A5101)	NIST P-256	KAT	CAST	Successful initialization of the module	Signature Generation	Module Initialization
ECDSA SigVer (FIPS186-4) (A5101)	NIST P-256	KAT	CAST	Successful initialization of the module	Signature Verification	Module Initialization
KAS-ECC-SSC Sp800-	NIST P-256	KAT	CAST	Successful initializatio	Ephemeral Unified	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
56Ar3 (A5101)				n of the module		
HMAC DRBG (A5101)	As specified in NIST SP 800-90Ar1 Section 11.3	KAT	CAST	Successful initialization of the module	Instantiate, Generate and Reseed	Module Initialization
KDA HKDF SP800-56Cr2 (A5101)	HMAC-SHA2-256	KAT	CAST	Successful initialization of the module	Key Derivation	Module Initialization
AES-CBC (A5101)	256-bit key	KAT	CAST	Successful initialization of the module	Encryption/Decryption	Module Initialization
ECDSA KeyGen (FIPS186-4) (A5101)	NIST P-256	PCT	PCT	Success or failure of service	Key Pair Generation	Key Pair Generation and Key Agreement
SHA2-256 (A2352)	256-bit hash	KAT	CAST	Successful initialization of the module	Hash	Module Initialization
HMAC-SHA2-256 (A2352)	256-bit key	KAT	CAST	Successful initialization of the module	Hash	Module Initialization
Firmware Load Test	ECDSA Signature Verification with NIST P-256	Firmware Load Test	SW/FW Load	Successful firmware update	N/A	Firmware Update Request
Entropy Source 90B Start-Up RCT and APT	Repetition Count Test (RCT) and Adaptative	Start-up Health Tests	CAST	Successful initialization of the entropy source	Entropy Generation	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	Proportion Test (APT) as specified in NIST SP 800-90B Sections 4.4.1 and 4.4.2					
Entropy Source 90B Continuous RCT and APT	Repetition Count Test (RCT) and Adaptative Proportion Test (APT) as specified in NIST SP 800-90B Sections 4.4.1 and 4.4.2	Continuous Health Tests	CAST	Successfull output of entropy bits	Entropy Generation	Entropy Bits Request

Table 23: Conditional Self-Tests

The module performs self-tests on all approved cryptographic algorithms supported in the approved mode of operation, using the tests shown in the table above. To ensure all conditional CASTs are performed prior to the first operational use of the associated algorithm, all CASTs are performed during the module's initial power-up sequence. The CASTs for algorithms used in the pre-operational firmware integrity test are performed prior to the integrity test itself; all other CASTs are executed immediately after the successful completion of the firmware integrity test.

Services are not available, and data output (via the data output interface) is inhibited during the self-tests. If any of these tests fails, the module transitions to the error state.

10.3 Periodic Self-Test Information

Pre-operational self-tests can be run on-demand, for periodic testing, by rebooting the module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A2352)	Firmware Integrity	SW/FW Integrity	On Demand	Reboot, reset or power cycle

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
HMAC-SHA2-256 (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
ECDSA SigGen (FIPS186-4) (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
ECDSA SigVer (FIPS186-4) (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
KAS-ECC-SSC Sp800-56Ar3 (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
HMAC DRBG (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
KDA HKDF SP800-56Cr2 (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
AES-CBC (A5101)	KAT	CAST	On Demand	Reboot, reset or power cycle
ECDSA KeyGen (FIPS186-4) (A5101)	PCT	PCT	On Demand	Reboot, reset or power cycle
SHA2-256 (A2352)	KAT	CAST	On Demand	Reboot, reset or power cycle
HMAC-SHA2-256 (A2352)	KAT	CAST	On Demand	Reboot, reset or power cycle
Firmware Load Test	Firmware Load Test	SW/FW Load	On Demand	Firmware Update Request
Entropy Source 90B Start-Up RCT and APT	Start-up Health Tests	CAST	On Demand	Reboot, reset or power cycle
Entropy Source 90B Continuous RCT and APT	Continuous Health Tests	CAST	Entropy Generation	Entropy Bits Request

Table 25: Conditional Periodic Information

10.4 Error States

If any of the Pre-operational Self-Tests or Conditional Self-Tests fail, the module will output an error status and enter an error state, where all data output is inhibited. Upon entering an error state, an operator can attempt to clear the error state by removing the module from the USB port and reinserting it to restart the module. If the error state cannot be cleared, the module must be returned to the manufacturer. The table below shows the different causes that lead to the Error States and the status indicators reported.

Name	Description	Conditions	Recovery Method	Indicator
Error	The module's error state	POST, CAST or PCT Failure	Module reboot and power cycle	Error Code

Table 26: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No configuration of the module or installation steps are required from the operator. When the module is powered on its power-up self-tests are executed without any operator intervention. The module enters in approved mode automatically if the power-up self-test completes successfully. If any of the self-tests fail during power-up, the module transitions to an Error state.

The operator can verify that the module is in the Approved mode of operation and that the FIPS validated version is being used, by checking the version output using the "Vendor_Sysinfo" command and comparing it against the versioning information on the module certificate.

The status of the module can be determined by the availability of the module or by executing the “Show Status” service. If the module is available, it has passed all self-tests. If it is unavailable, it is in the error state.

11.2 Administrator Guidance

None.

11.3 Non-Administrator Guidance

None.

12 Mitigation of Other Attacks

The module is protected against the following non-invasive attacks:

Fault Injection:

- Code signing
- Execution gating
- Storage parity
- Transmission parity
- Power On Self-Test
- Voltage monitoring
- Temperature monitoring
- Internal clock
- Active Security Shield

Side-Channel Attacks:

- Constant-time (data-independent) code execution
- Random insertion of wait states
- Jittery clock
- Power masking
- Data blinding
- TRNG Entropy Churning
- Computation Throttling