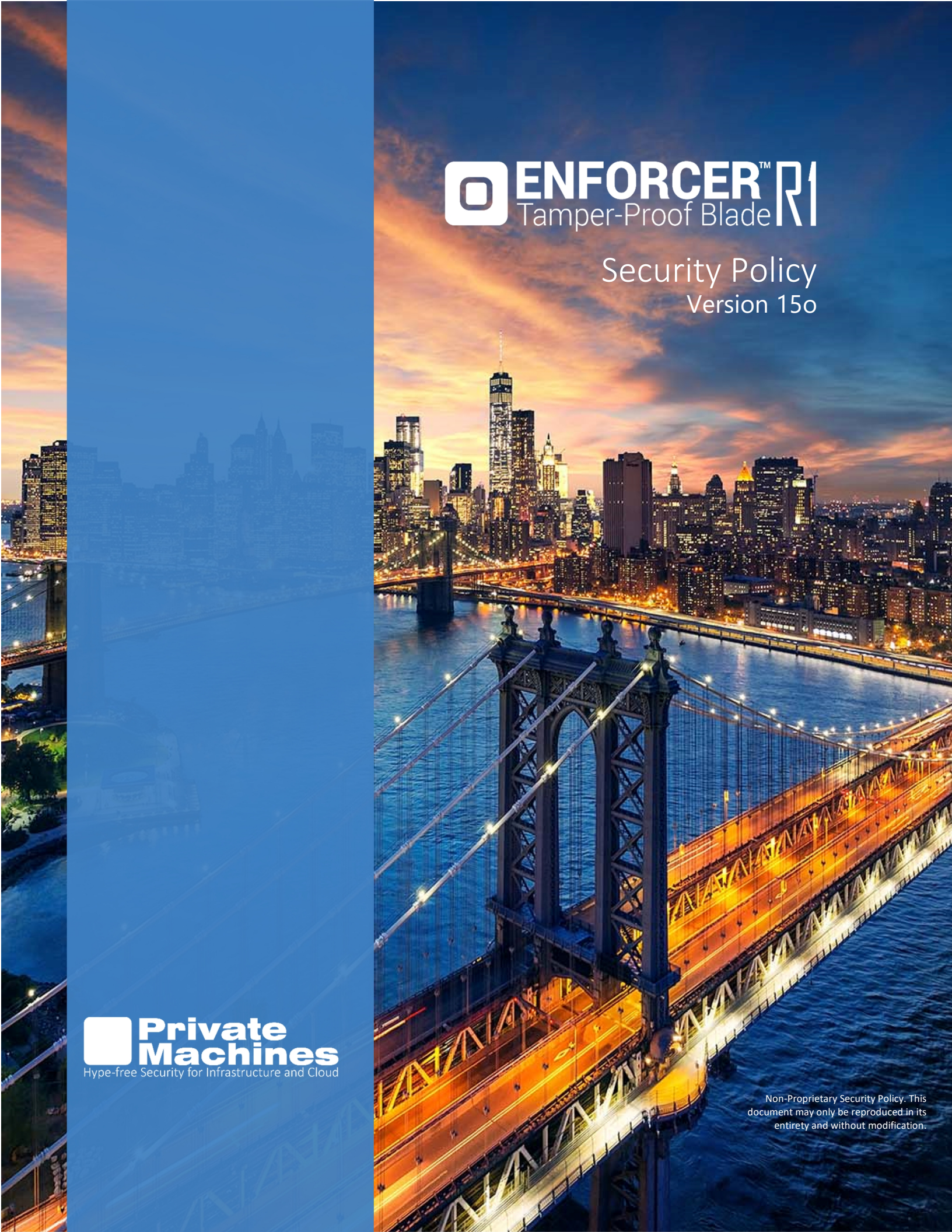

ENFORCER™ R1
Tamper-Proof Blade

Security Policy
Version 15o

Private Machines
Hype-free Security for Infrastructure and Cloud

Table of Contents

TABLE OF TABLES

TABLE OF FIGURES

INTRODUCTION

This document is the Security Policy for the Private Machines Inc. ENFORCER R1. Table 1 lists the hardware and firmware versions covered by this document. Hereafter, the term "Security Anchor Firmware" refers to the combination of firmware specified in Table 1.

Table 1 : Hardware and Firmware Versions

Hardware (The module may have any one of the listed versions)	• ENFORCER.R1.A2SDi.1.0.0 (1) • ENFORCER.R1.X10SDV.1.0.0 (1) • ENFORCER.R1.M11SDV.1.0.0 (1) • ENFORCER.R1.X11SDV.1.0.0 (1) (1) Plus other excluded components described in section 1.4
Firmware (The module includes all the listed components)	• Security Anchor Firmware 1.2.0 • Libdrbg: 1.0.2 • Libucl: 2.5.13

The "ENFORCER R1" is a single-user, multi-chip stand-alone cryptographic module. Hereafter, we refer to the ENFORCER R1 as the "module".

The module serves the following purposes:

1. Provides a physically secure, Level 4 enclosure protecting CSPs and cryptographic data. A physical tamper event on the enclosure immediately zeroizes module CSPs (Section 4.5).
2. Provides a KMIP (Key Management Interoperability Protocol [1]) service (Section 5.3.1) for key management to external users.
3. Provides additional services (Section 5.3) for module management, module configuration, and for building higher-level application scenarios such as integration into cloud and data center environments.

The key security component within the module is the "Security Anchor". All module services are provided by the Security Anchor. The module uses a secure microcontroller as the Security Anchor. The Security Anchor also provides CSP zeroization as a tamper response (Section 4.5.1).

This security policy applies to all module components within the cryptographic boundary (Section 1.3.3). A general-purpose computer (GPC) termed the "Compute Engine" is contained within the cryptographic boundary, but it is excluded from the requirements of FIPS 140-2 [2] per AS.01.09. The Compute Engine remains powered off during the FIPS lifecycle of the module. Turning on the Compute Engine permanently and irreversibly invalidates the FIPS certificate, as indicated by the Lost Cert Ratchet (Section 1.2.2). Compute Engine components are indicated in 1.4.

After factory initialization, the module operates in FIPS approved mode (Section 1.2). All authenticated services are accessible over the module's serial interface using a secure, encrypted TLS connection between an external user (or Crypto Officer) and the Security Anchor (Section 5.1).

1. CRYPTOGRAPHIC MODULE SPECIFICATION

1.1 Security Level

The module meets the overall security requirements of FIPS 140-2 Level 4 (Table 2).

Table 2 : FIPS 140-2 [2] Security Requirements

FIPS Area	Security Requirements Section	Level
1	Cryptographic Module Specification	4
2	Cryptographic Module Ports and Interfaces	4
3	Roles, Services and Authentication	4
4	Finite State Model	4
5	Physical Security (Multi-chip, stand-alone)	4
6	Operational Environment	N/A
7	Cryptographic Key Management	4
8	Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)	4
9	Self-Tests	4
10	Design Assurance	4
11	Mitigation of Other Attacks	4

1.2 Mode of Operation

The module has only one mode of operation – "FIPS approved" mode (approved mode). The module's mode of operation can be verified using the "Get Status" service (Section 5). Additionally, the external FIPS Status LED indicates whether the module is in an error state.

1.2.1 FIPS Approved Mode

After factory initialization, the module operates in FIPS approved mode. The FIPS approved mode is invoked by powering on the module. The module implements the approved algorithms listed in Table 9 and the allowed algorithms listed in Table 10. The module does not support any other mode of operation.

1.2.1.1 Error State

The following requirements must be met for the module to operate without entering an error state.

- The Security Anchor is loaded with the correct, verified firmware.
- All power-up and self-tests pass.
- No tamper event is triggered.

If any of the above conditions are violated, the module transitions to an error state. In an error state, all services except "Get Status" are disabled (Section 5). The "Get Status" service indicates whether the module has met the conditions above or is in an error state. To exit an error state, the module must be power cycled and all conditions must be satisfied (Section 1.2.1).

1.2.2 Lost Cert Ratchet

The module supports an irreversible lost cert ratchet. The lost cert ratchet indicates whether the module's FIPS certificate has been invalidated. The lost cert ratchet is set when the Compute Engine is powered on. The status of the ratchet can be verified using the "Get Status" service.

1.3 Specifications

The module is a multi-chip standalone cryptographic module.

1.3.1 Block Diagram and Images

Figure 1 : Module Block Diagram

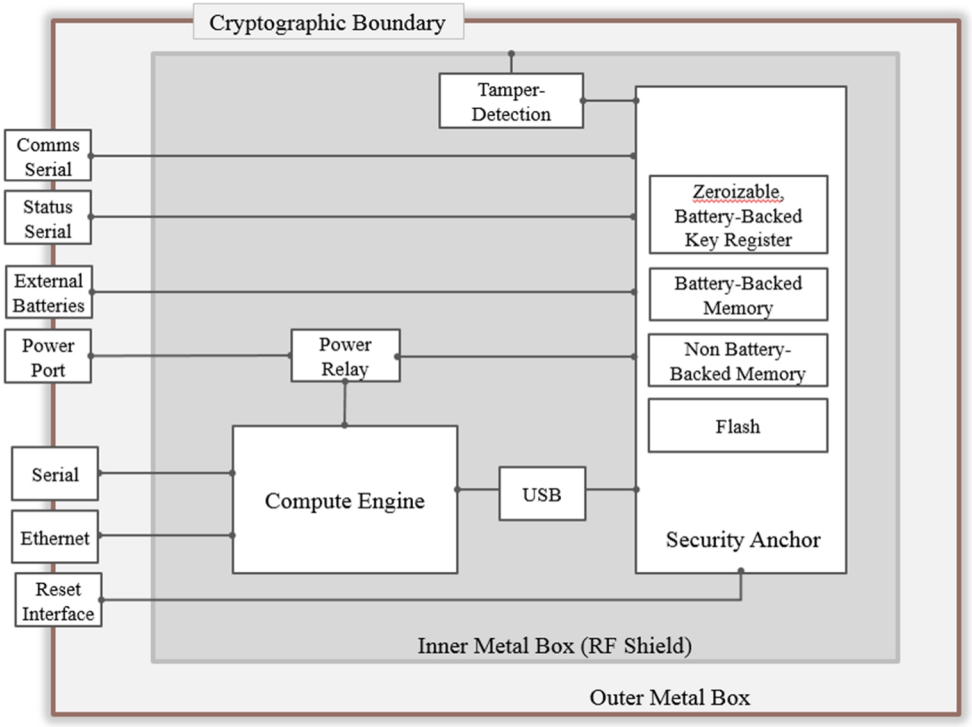

Figure 2 : Module Image

1.3.2 Security Anchor

The key security component within the module is the "Security Anchor". All module services are provided by the Security Anchor, and all CSPs are stored within the Security Anchor. The Security Anchor features embedded voltage, temperature, and membrane sensors that constantly monitor the module for tamper attempts. When a tamper attempt is detected the Security Anchor zeroizes all CSPs as part of its tamper response mechanism. The Security Anchor provides additional anti-tamper and zeroization features as outlined in "Mitigation of Other Attacks" (Section 11).

1.3.3 Cryptographic Boundary

The FIPS 140-2 cryptographic boundary is the outer metal box (Figure 1). The entire module is protected by the physical security policy described in Section 7.

1.4 Module Hardware Versioning: Excluded Components

The module is composed of the hardware components specified in Table 1. The components excluded from FIPS 140-2 comprise the Compute Engine. The Inner Enclosure may be configured to contain exactly one Compute Engine (with components as indicated in Table 3 and Table 4), or it may be left empty. The table below lists which Compute Engine Motherboard Models are compatible with which Inner Enclosures. For each Model, one hardware version exists (version *1.0.0.modelnumber*). Table 3 lists which Compute Engines are compatible with which Inner Enclosures.

Table 3 : Compute Engine Inner Enclosure Compatibility List

Inner Enclosure Version	Compute Engine Motherboard Model Numbers	
1.0.0.A2SDi-A.9	• A2SDi-2C-HLN4F • A2SDi-4C-HLN4F • A2SDi-8C-HLN4F • A2SDi-8C+-HLN4F	• A2SDi-12C-HLN4F • A2SDi-16C-HLN4F • A2SDi-H-TP4F • A2SDi-H-TF
1.0.0.X10SDV-A.7	• X10SDV-2C-TLN2F • X10SDV-4C-TLN2F • X10SDV-4C-TLN4F • X10SDV-4C+-TLN4F • X10SDV-6C-TLN4F • X10SDV-6C+-TLN4F • X10SDV-8C+-LN2F	• X10SDV-8C-TLN4F • X10SDV-12C-TLN4F • X10SDV-12C+-TLN4F • X10SDV-16C-TLN4F • X10SDV-16C+-TLN4F • X10SDV-TLN4F • X10SDV-F
1.0.0.M11SDV-A.6	• M11SDV-4C-LN4F • M11SDV-4CT-LN4F • M11SDV-8C+-LN4F	• M11SDV-8C-LN4F • M11SDV-8CT-LN4F
1.0.0.X11SDV-A.1	• X11SDV-8C-TLN2F • X11SDV-8C+-TLN2F • X11SDV-4C-TLN2F	• X11SDV-16C-TLN2F • X11SDV-16C+-TLN2F • X11SDV-12C-TLN2F

The Compute Engine itself may be configured with various amounts of storage and RAM in addition to the motherboard. The allowed part numbers of each component, along with the number of components that can be present in a valid configuration, are described below.

Table 4 : Compute Engine RAM and Storage Configurations

Component Type	Component Part Number		Number of Components Allowed
RAM	• RAM.00000000.4GB • RAM.00000000.8GB • RAM.00000000.16GB	• RAM.00000000.32GB • RAM.00000000.64GB	1 - 4
SATA SSD	• SSD.SATA.00000000.512GB • SSD.SATA.00000000.1TB • SSD.SATA.00000000.2TB	• SSD.SATA.00000000.4TB • SSD.SATA.00000000.8TB	0 - 4
M.2 SSD	• SSD.M2.00000000.512GB • SSD.M2.00000000.1TB • SSD.M2.00000000.2TB	• SSD.M2.00000000.4TB • SSD.M2.00000000.8TB	0 - 1

An example Compute Engine configuration consists of four 8 GB RAM sticks (RAM.00000000.8GB), two 4 TB SATA SSDs (SSD.SATA.00000000.4TB) and one 512 GB M.2 SSD (SSD.M2.00000000.512GB).

2. MODULE PORTS AND INTERFACES

Module ports and interfaces are described in Table 5. All module interfaces are pins on two ribbon cables that pass directly into the module's internal circuitry, but additional vendor-supplied components outside the module boundary are required for the full functionality specified in the tables below. Status output LEDs are described in Table 6.

Access to authenticated services occurs over a Trusted Path (per IG 2.1), which relies on TLS 1.2 as described in Section 4.2.4.1 Trusted Path: TLS 1.2 Implementation.

Table 5 : Module Ports and Interfaces

Logical Interface	Data	Flow	Hardware
Data input	Service inputs User data	• Encrypted (TLS) communication between an external user and the Security Anchor • Unauthenticated services only: Unencrypted communication between an external user ("General" role) and the Security Anchor	External comms serial port and Security Anchor
Data output	Service outputs User data		
Control input	Service inputs Control inputs	• Encrypted (TLS) communication between an external user and the Security Anchor • Unauthenticated services only: Unencrypted communication between an external user ("General" role) and the Security Anchor	External comms serial port and Security Anchor
		External factory reset (deactivation) to Security Anchor	External loop wire and jumper
		External power button to module interior	Power circuit
Status output	FIPS status	Security Anchor to an external user	External comms serial port and Security Anchor; external status serial port and Security Anchor
		Security Anchor to external status LED	External FIPS Status LED

Logical Interface	Data	Flow	Hardware
	Low battery Indicator		External battery to external Low Battery Indicator LED
	Security Anchor Power Status		Power circuit to external Security Anchor Power Status LED
Power inputs			• External battery to Security Anchor • DC Power port inputs

Table 6 : LED states

LED (outside module boundary)	LED State	Status
External FIPS Status LED	Green	Module is in FIPS approved mode and not in an error state
	Red and blinking	Module is in error state
	Blue	FIPS certificate has been invalidated
Low battery indicator LED	Off	External battery is OK
	On (Red)	External battery is low (<3.0 V)
Security Anchor Power Status LED	Off	Security Anchor firmware is not executing
	On (Green)	Security Anchor firmware is executing

3. ROLES AND AUTHENTICATION

The module implements three authenticated roles: Crypto Officer, KMIP Admin User and KMIP User. The module implements identity-based authentication with explicit role selection (Table 8). Authentication is required for each individual service request.

Table 7 : Roles

Role	Description
Crypto Officer	Privileged services, such as module configuration, are permitted only to the Crypto Officer role.
KMIP Admin User	The KMIP Admin User role is permitted to perform KMIP user management (Table 21), and KMIP state management (Table 22) operations
KMIP User	The KMIP User role is permitted to perform KMIP1.4 operations (Table 23). The KMIP User role is not permitted to perform KMIP user management (Table 21) (with the exception of updating a user's own password), or KMIP state management (Table 22) operations.
General	No authentication is required for non-critical services.

Table 8 : Authentication for Roles

Role	Role Selection	Auth. Type	Auth. Info	Auth. Mechanism	Strength of Mechanism
Crypto Officer	Based on service requested	Identity-based	CO User ID: fixed value provided by CO (cannot consist of only zeroes). Only one Crypto Officer is permitted. 256-bit token	Comparison to token saved in the Security Anchor (time-independent token comparison[1])	• For a random attempt, the probability of success is $1/(2^{256}-1)$, which is less than 1/1,000,000. • Because the Security Anchor enforces an exponentially increasing delay for each failed authentication attempt, a maximum of 350 failed attempts can be made in one minute. The probability of a successful random attempt[2] in one minute is therefore $350/(2^{256})$, which is significantly less than 1/100,000.
KMIP Admin User	Based on service requested	Identity-based	User name: fixed user name for KMIP admin. Only one KMIP Admin User is permitted. Password: Between 64 and 1024 bits.	Comparison to a salted password hash (SHA-256 w/ 256-bit salt) stored encrypted by the Flash Encryption Key in Security Anchor flash storage.	• If the minimum length password (64 bits) is used, the probability that a random attempt to guess the password will succeed is 1/(2^64), which is less than 1/1,000,000. • Because the Security Anchor enforces an exponentially increasing delay for each failed authentication attempt, a maximum of 350 failed attempts can be made in one minute. The probability of a successful random attempt in one minute is therefore 350/(2^64), which is significantly less than 1/100,000.
KMIP User	Based on service requested	Identity-based	User name: Unique to each user Password: Between 64 and 1024 bits		

3.1 Initialization

After factory initialization, the module operates in FIPS approved mode. The Crypto Officer role is initialized in factory using the "Set Crypto Officer Token" service (Section 5.3). The initial Crypto Officer Token is communicated to the customer via a separate, secure channel (outside the module). Upon receipt of the module, customers are recommended to change the Crypto Officer Token using the "Set Crypto Officer Token" service.

KMIP user management operations are part of the module's "KMIP Key Management" service (Section 5.3.1). After module receipt, customers need to first set up an "admin" KMIP user using the following steps:

1. Invoke the KMIP "Create Admin" operation to create a KMIP Admin User with the desired password.
2. Using the KMIP Admin User, create additional users as desired using the "Create KMIP User" operation (Table 21).

[1] For a time-independent comparison function, the time required to compare two fixed-size bit strings is independent of the content of bit strings.

[2] $1/(2^{256}-1)$ is effectively $1/(2^{256})$

4. CRYPTOGRAPHIC KEY MANAGEMENT

4.1 Algorithms

4.1.1 FIPS Approved Algorithms

The Module supports the following FIPS-approved cryptographic algorithms (Table 9).

Table 9 : FIPS Approved Algorithms[3]

Algorithm & Cert.	Standard(s)	Modes / Methods	Key Bit Lengths, Curves or Moduli	Use
AES #5073	FIPS 197 [3] SP800-38A [4] SP800-38D [5]	CBC CTR ECB GCM[4][5]	128, 192, and 256 bits	• KMIP operations: Encrypt, Decrypt • To encrypt and decrypt all KMIP cryptographic objects stored in flash storage (AES CBC 256) • To encrypt and decrypt KMIP data during KMIP Import/Export (AES GCM 256) • TLS (AES GCM 256)
AES #C1028	FIPS 197 [3] SP 800-38A [4]	ECB	256 bits	• To encrypt and decrypt items stored in the NVSRAM (zeroizable, battery-backed RAM) using the Security Anchor Hardware AES Key
CKG (vendor affirmed)	SP 800-133r1 [6]		256 (Security Strength)	• The unmodified output of the DRBG #C558 is used for symmetric key generation and as seeds for asymmetric key generation. See DRBG uses for a full list.

[3] Not all algorithms/modes verified through CAVS certificates are implemented in the module.
[4] IVs are generated according to FIPS 140-2 IG A.5 (refer to the CSP entry for AES GCM Authenticated Encryption IV for more detail).
[5] GMAC is validated by the CAVP but not used in the module

Algorithm & Cert.	Standard(s)	Modes / Methods	Key Bit Lengths, Curves or Moduli	Use
DRBG #C558	SP 800-90Ar1 [7]	HMAC-SHA-256 Prediction resistance enabled	256 (Security Strength)	• KMIP operations: Create, Create Key Pair, Encrypt (IV generation), Sign (PSS salt generation), RNG Retrieve • Ephemeral Key Pair and Ephemeral Public Key Certificate generation, KMIP Key Management Import/Export Key Pair and KMIP Key Management Import/Export Public Key Certificate generation, Get Randoms, Set Crypto Officer Token, KMIP User creation and password update (256-bit password salt), KMIP Import/Export (AES GCM 256) by KMIP storage layer (AES CBC 256 key and IV) • TLS
DSA #1336	FIPS 186-4 [8]	Key pair generation	(2048, 256)[6]	DH key generation for TLS (Section 4.2.4) (DSA sign/verify functionality is not implemented)
ECDSA #1316	FIPS 186-4 [8]	Key pair generation	P-224, P-256, P-384, P-521	KMIP operations: Create Key Pair, Sign, Signature Verify
		Signature generation	P-224, P-256, P-384, P-521 with SHA-224, SHA-256, SHA-384, SHA-512	
		Signature verification [7]	P-224, P-256, P-384, P-521 with SHA-224, SHA-256, SHA-384, SHA-512	
HMAC #3385	FIPS 198-1 [9]	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	KS < BS KS > BS KS = BS KS and BS are the sizes of keys/blocks. The module supports all key lengths between 112 and 1024 bits, inclusive (multiples of 8).	• KMIP operations: MAC, MAC Verify • DRBG implementation (Cert #C558, 256-bit key) • TLS (as part of KDF CVL #1633, 384-bit key)

[6] Validated sizes (2048, 224) and (3072, 256) are not used in the module.
[7] P-192 signature verification is validated by the CAVP but not used in the module.

Algorithm & Cert.	Standard(s)	Modes / Methods	Key Bit Lengths, Curves or Moduli	Use
KAS-SSC (vendor affirmed)	SP 800-56Ar3 [10]	FFC DH dhEphem, C (2e, 0s, FFC DH) Scheme using 186-type primes	(2048, 256)	• Key agreement using FFC DH for shared secret computation in accordance with IG D.1-rev3 (with DSA #1336 prerequisite for key pair generation) and TLSv1.2 KDF (CVL #1633) for key derivation. Derives TLS Ks for Trusted Path. • Key establishment methodology provides 112 bits of encryption strength
KDF TLS CVL #1633	SP 800-135r1 [11]	TLSv1.2 with SHA-384		• Application-specific Key Derivation Function (KDF) used by TLS. • The module's TLS implementation conforms to IG D.11, option 2. The module implements a validated KDF from SP 800-135rev1. No parts of this protocol other than the KDF have been tested by the CAVP and CMVP.
KTS (AES #5073)	SP 800-38F [12]	AES GCM	256	• TLS Ks (TLS Session Keys) are used for encryption and decryption for TLS, as described in section 4.2.4. • The KMIP Import/Export Data Encryption Key (established using Allowed RSA key wrapping) is used to protect transported KMIP CSPs (ref. Table 15) and KMIP data during KMIP Import/Export (ref. Table 22).
RSA #2751	FIPS 186-4 [8]	Key generation	2048, 3072, 4096[8]	• KMIP operations: Create Key Pair, Sign, Signature Verify • Signature generation and verification for KMIP
		Signature generation PKCS 1.5	2048, 3072, 4096[9] with SHA-256, SHA-512	
		Signature generation PKCSPSS	2048, 3072, 4096[10] with SHA-256, SHA-512	

[8] Per IG A.14, CAVP certification is not required for RSA 4096 key generation because CAVP testing is unavailable
[9] 4096 is tested to FIPS 186-2 [22] because CAVP testing is unavailable for 4096 testing to FIPS 186-4 [8]. See IG G.18.
[10] 4096 is tested to FIPS 186-2 [22] because CAVP testing is unavailable for 4096 testing to FIPS 186-4 [8]. See IG G.18.

Algorithm & Cert.	Standard(s)	Modes / Methods	Key Bit Lengths, Curves or Moduli	Use
		Signature verification PKCS 1.5[11]	2048, 3072, 4096[12] with SHA-256, SHA-512	import and export RSA key wrapping (Section 5.3.1) • Generate Ephemeral Keypair, Generate Ephemeral Public Key Certificate, Generate KMIP Key Management Import/Export Public Key Certificate, Get Signed Witness, Get Status, Set Module Configuration • TLS (Section 4.2.4)
		Signature verification PKCSPSS[13]	2048, 3072, 4096[14] with SHA-256, SHA-512	
RSASP1 component CVL #1634	PKCS#1 v2.1: RSA Cryptography Standard	RSASP1 Signature Primitive	2048[15] 3072 4096	KMIP Operations: Sign KMIP Users may call the signature primitive directly and perform padding/hashing separately.
RSADP Component CVL #1635	SP 800-56B [13]	RSA Decryption Primitive	2048	As part of the RSA key wrapping used in the KMIP Key Management Import/Export operations (Section 5.3.1)
SHS #4131	FIPS 180-4 [14]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512		• To generate the Ephemeral Public Key Certificate and KMIP Key Management Import/Export Public Key Certificate (Generation of X509 Subject/Key ID) (SHA-1). • KMIP operations: Sign, Signature Verify, Hash (Sign and Signature Verify do not support SHA-1) • Integrity checks on Security Anchor KMIP storage layer (SHA-256) • To hash the provided KMIP Admin User/KMIP User password for all such authenticated services (SHA-256) • TLS (SHA-384)

[11] The following RSA PKCS signature verification is CAVP validated, but not used in the module: 186-2 PKCS 1.5 (1024, 1536, 2048, 3072), 186-4 PKCS 1.5 (1024)
[12] 4096 is tested to FIPS 186-2 because CAVP testing is unavailable for 4096 testing to FIPS 186-4. See IG G.18.
[13] The following RSA PKCSPSS signature verification is CAVP validated, but not used in the module: 186-2 PKCSPSS (1024, 1536, 2048, 3072), 186-4 PKCSPSS (1024)
[14] 4096 is tested to FIPS 186-2 because CAVP testing is unavailable for 4096 testing to FIPS 186-4. See IG G.18.
[15] Only 2048 is CAVP testable, but 3072 and 4096 are Approved as per IG A.14

4.1.2 FIPS Non-Approved but Allowed Algorithms

Table 10 : FIPS Non-Approved but Allowed Algorithms

Algorithm	Strength/Caveats	Use
NDRNG	The NDRNG entropy rate and the DRBG implementation ensure that the DRBG has a full entropy output (256 bits)	Entropy source for seeding DRBG #C558
RSA (CVL Cert. #1635, key wrapping)	RSA: 2048, 3072, 4096 Key establishment methodology provides between 112 and 149 bits of encryption strength	Allowed RSA-OAEP key wrapping used in the KMIP Key Management Import/Export operations (Section 5.3.1) to establish KMIP Import/Export Data Encryption Key (AES GCM 256) The RSA decryption primitive has been tested for conformance to SP 800-56B [13], as indicated by the CVL. This key wrapping is considered Allowed per IG D.9.

4.1.3 FIPS Non-Approved, not Allowed Algorithms

The module does not support any non-approved, not allowed algorithms.

4.2 Critical Security Parameters

4.2.1 Critical Security Parameter Management

All CSPs are stored within the Security Anchor. CSPs are stored in the Security Anchor NVSRAM (zeroizable, battery-backed memory) and in the Security Anchor flash storage. The entire NVSRAM (including stored CSPs and keys) is encrypted with the Security Anchor Hardware AES Key (AES ECB 256, AES #C1028). The entire flash storage is encrypted using the Flash Encryption Key (AES CBC 256, AES #5073). The Flash Encryption Key in turn is stored in NVSRAM, encrypted using the Security Anchor Hardware AES Key.

The Security Anchor Hardware AES Key is stored in a separate battery-backed key register and destroyed upon zeroization. Zeroizing the Security Anchor Hardware AES Key prevents access to all other CSPs (NVSRAM and flash). This is because all CSPs are either encrypted directly with the Security Anchor Hardware AES Key or the Flash Encryption Key (AES CBC 256), which in turn is encrypted by the Security Anchor Hardware AES Key.

All CSPs that are input or output are encrypted by at least one of the following methods:

1. Communication over the module's Trusted Path relying on TLS 1.2. The Trusted Path is encrypted by TLS Ks (AES GCM 256, key establishment methodology provides 112 bits of encryption strength). Details are provided in Section 4.2.4.1 Trusted Path: TLS 1.2 Implementation.
2. Imported or exported key management states are encrypted by the KMIP Import/Export Data Encryption Key (AES GCM 256, key establishment methodology provides between 112 and 149 bits of encryption strength).
3. The KMIP Import/Export Data Encryption Key is wrapped by the KMIP Key Management Import/Export Public Key or KMIP Key Management Client Import/Export Public Key (RSA 2048, 3072, or 4096 allowed key wrapping, key establishment methodology provides between 112 and 149 bits of encryption strength).

4. The TLS session ticket is wrapped by the TLS Session Ticket Encryption Key (TLS STEK) (AES GCM 256, full 256-bit encryption strength). Note that this is not a KTS because keys are not transported.

Module CSPs are divided into the following categories (specified in the tables below): General CSPs, DRBG CSPs, TLS CSPs, and KMIP Cryptographic Objects (CSPs and Public Keys).

4.2.2 General Critical Security Parameters (CSPs)

Table 11 : General Critical Security Parameters (CSPs)

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
Security Anchor Hardware AES Key	The AES key used to encrypt and decrypt the Security Anchor's zeroizable, battery-backed memory which stores other CSPs. The AES key cannot be read by the module's firmware, Crypto Officer, or users.	Format: 256-bit AES key in ECB mode Storage: Security Anchor's 256-bit, battery-backed key register. Protection: Stored in plaintext, not accessible to firmware.	Use: Used by all module services when accessing Security Anchor battery-backed memory
			Generation: • In-factory activation (DRBG #C558)
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization
Flash Encryption Key	The Flash Encryption Key is used to encrypt and decrypt objects that comprise the KMIP Key Management state (Section 4.2.5).	Format: 256-bit AES key in CBC mode. Storage: Zeroizable, battery-backed memory (NVSRAM). Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Used to encrypt and decrypt all KMIP Cryptographic Objects (Section 4.2.5) stored within the Security Anchor flash storage.
			Generation: • In-factory activation (DRBG #C558) • Key Management State Operations Configure KMIP Storage and Import Init (Section 5.3.1) (DRBG #C558)
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • KMIP Key Management State Operation: Reset • KMIP Key Management State Operation: Import Init • KMIP Key Management State Operation: Import Cancel • Power on Compute Engine

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
Crypto Officer Token	The token used to authenticate the Crypto Officer role. Only the Crypto Officer (after successful authentication) can request a new token to be generated.	Format: The Crypto Officer token is a 256-bit value. A valid token contains at least one non-zero bit. Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Used by module services for Crypto Officer authentication
			Generation: • First, during in-factory activation (DRBG #C558) • Via the set Crypto Officer Token service (DRBG #C558)
			Input: Input for all Crypto Officer authenticated services. Input over TLS, encrypted by TLS Ks (AES GCM 256)
			Output: When a new token is set using the Set Crypto Officer Token service, the new token is communicated over TLS, encrypted by TLS Ks (AES GCM 256)
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service
Device Private Key (CARsaPriv)	The Device Private Key is used by the Security Anchor to sign data. The Device Private Key is generated once during factory initialization and cannot be changed after the module has shipped. The Device Key Pair also serves as a unique module identifier.	Format: RSA private exponent. Can be 2048, 3072, or 4096 bits. Size is configurable using the "Set Module Configuration" service (Section 5.3). Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Used by the following services: • Get Signed Witness • Get Status • Generate Ephemeral Key Pair • Generate KMIP Key Management Import/Export Key Pair • Get Device Public Key • KMIP Key Management State Operation: Export Init (Section 5.3.1) • Part of the TLS trust chain
			Generation: In factory (RSA #2751)
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service
Ephemeral Private Key (KRsaPriv)	The Ephemeral Key Pair is used during TLS session negotiation. It is	Format: RSA private exponent. Can be 2048, 3072, or 4096 bits. Size is configurable using	Use: By the Security Anchor to sign its public DHE parameters before sending them to a TLS client (PKCS 1v1.5 SHA-512, RSA #2751)

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
	periodically regenerated by the Security Anchor, the frequency of which can be modified via the module's configuration.	the Set Module Configuration service. Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Generation: • Generate Ephemeral Key Pair service (RSA #2751) • Set Module Configuration (RSA #2751) • Auto-generated periodically by the Security Anchor (RSA #2751)
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine
KMIP Key Management Import/Export Private Key	The RSA key used in the KMIP Import/Export Allowed RSA key wrapping. It is periodically regenerated by the Security Anchor, the frequency of which can be modified via the module's configuration.	Format: RSA private exponent. Can be 2048, 3072, or 4096 bits. Size is configurable using the Set Module Configuration service. Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: In the KMIP Import/Export RSA key wrapping to decrypt the KMIP Import/Export Data Encryption Key (CVL #1635)
			Generation: • Generate KMIP Import/Export Key Pair service (RSA #2751) • Auto-generated periodically by the Security Anchor (RSA #2751)
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Set Module Configuration Service • Power on Compute Engine
KMIP Import/Export Data Encryption Key	The AES GCM 256 (AES #5073) key used to encrypt and decrypt data during the KMIP Export/Import procedure.	Format: 256-bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: To encrypt and decrypt KMIP Cryptographic Objects during the KMIP Import and Export operations
			Generation: Generated by the module's DRBG (#C558) during KMIP Export Init
			Input: Via the KMIP Import Init operation as part of the KMIP Import/Export RSA allowed key wrapping. Encapsulated by KMIP Key Management Import/Export Public Key (RSA 2048, 3072, or 4096).

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
			Output: Via the KMIP Export Init operation as part of the KMIP Import/Export RSA allowed key wrapping. Encapsulated by KMIP Key Management Client Import/Export Public Key (RSA 2048, 3072, or 4096).
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • KMIP Key Management State Operations: Reset, Configure KMIP Storage • On completion or termination of Key Management Import/Export operation • Power on Compute Engine
AES GCM Authenticated Encryption IV	The IV to be used in the GCM authenticated	Format: 96, 104, 112, 120, 128 bits	Use: KMIP Encrypt and Decrypt operations, KMIP Import/Export, and TLS

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
	encryption function. As per SP 800-38D [5], section 9.1, the IV is no longer considered a CSP after it is used in an invocation of the authenticated encryption function.	Storage: NVSRAM and RAM Protection: Encrypted using the Security Anchor Hardware AES Key unless stored in RAM, where it is stored in plaintext.	Generation: Either generated entirely randomly using the DRBG (#C558) as per IG A.5 Scenario 2: • KMIP Import/Export Data Encryption Key • TLS STEK • KMIP Cryptographic Objects: AES GCM Keys Or, for TLS Ks: IV is generated in conformance to IG A.5 Scenario 1a whereby: 1. IV generation is performed according to the TLS 1.2 protocol and the GCM cipher suite as described in RFC 5288 [15] and included in SP 800-52 Rev 2 [16]. 2. IV is used only in the context of the AES GCM mode encryption within the TLS protocol 3. The operations of one of the parties included in the TLS scheme is performed entirely within the module 4. The counter portion of the IV is set by the module within its cryptographic boundary and the requirements of IG A.5 Scenario 3 for the counter field are met, including IV Restoration Condition 3 When nonce_explicit exhausts the maximum values for a given key (64 bits) the module aborts the session and a new TLS session with a new encryption key must be established.[16] Both portions of this IV are stored in RAM.
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Start TLS Session, End TLS Session, Clear TLS State • 64-bit GCM IV counter used with TLS Ks reaches maximum value • KMIP v1.4 Operation: Encrypt • Key Management State Operation: Export • Generate Ephemeral Key Pair, Set Module Configuration, Reset, Power on Compute Engine

[16] If the security anchor's power is lost a new TLS session must be established with the security anchor as per scenario 3 of IG A.5, restoration condition 3.

4.2.3 DRBG CSPs

All DRBG CSPs are used whenever the DRBG is accessed. Many services access the DRBG, view Services 5 for a complete list.

Table 12 : DRBG CSPs

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
Entropy Input	Input string provided to the HMAC DRBG during its initialization and reseeding	Format: 464 bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: As part of the seed of DRBG #C558 (initialization and re-seeding)
			Generation: By the Security Anchor's NDRNG
			Input: N/A
			Output: N/A
			Zeroization: • Immediately after DRBG initialization/reseeding • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine • Perform Self-Tests • Power-up Self-Tests
Nonce	Input string provided to the HMAC DRBG during its initialization	Format: 216 bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: As part of the seed of DRBG #C558 (initialization only)
			Generation: By the Security Anchor's NDRNG
			Input: N/A
			Output: N/A
			Zeroization: • Immediately after DRBG initialization • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine • Perform Self-Tests • Power-up Self-Tests
Seed	The seed provided to the HMAC DRBG during its initialization	Format: 744 bits (initialization only) or 464 – 720 bits Storage: NVSRAM	Use: As the seed material of DRBG #C558
			Generation: By the Security Anchor's NDRNG

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
	and reseeding. Comprised of the Entropy Input CSP, Nonce CSP (initialization only), a Personalization String (initialization only), and additional input (reseed only)	Protection: Encrypted using the Security Anchor Hardware AES Key	Input: N/A Output: N/A Zeroization: • Immediately after initialization/reseeding • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine • Perform Self-Tests • Power-up Self-Tests
HMAC V	The DRBG's internal HMAC V value	Format: 256 bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: As part of the internal HMAC state Generation: As part of the DRBG generation function (see NIST SP 800-90Ar1 [7], section 10.1.2.5) Input: N/A Output: N/A Zeroization: • Immediately after initialization/reseeding • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine • Perform Self-Tests • Power-up Self-Tests
HMAC K	The DRBG's internal HMAC Key	Format: 256-bit HMAC key Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: As part of the internal HMAC state Generation: As part of the DRBG generation function (see NIST SP 800-90Ar1 [7], section 10.1.2.5) Input: N/A Output: N/A Zeroization: • Immediately after initialization/reseeding • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine • Perform Self-Tests • Power-up Self-Tests

4.2.4 TLS 1.2

4.2.4.1 Trusted Path: TLS 1.2 Implementation

The module is compatible with TLSv1.2 [17], which it uses to establish a Trusted Path (per IG 2.1) for the protection of plaintext CSPs. The Trusted Path is used for all authenticated services; the operator may choose to use the trusted path for unauthenticated services as well (refer to Section 5.2 Service Access). To set up the Trusted Path, the operator establishes and operates the TLS session as specified below.

Table 13 describes the Cipher Suite Supported by this implementation of TLS, which is specified in SP 800-52 Rev 2 [16], Section 3.3.1.1.2.

TLS key establishment is per the vendor affirmed SP 800-56Ar3 [10] KAS-SSC (dhEphem, C(2e, 0s, FFC DH) Scheme with 186-type primes) specified in Table 9. The module implements a validated KDF (CVL #1633) from SP 800-135rev1. No parts of this protocol other than the KDF have been tested by the CAVP and CMVP. TLS generates AES GCM 256 keys (key establishment methodology provides 112 bits of encryption strength) that are used to encrypt the session. These AES 256 GCM keys provide authenticated encryption in conformance with SP 800-38F [12]. TLS does not implement RSA key encapsulation.

The Ephemeral private (KRsaPriv) and public (KRsaPub) keys are used as the TLS key pair for session negotiation. The Ephemeral Public Key (KRsaPub) is signed by the Device Private Key (CARsaPriv). The Device Public Key (CARsaPub) is in turn signed by the Manufacturer Private Key. The resulting trust chain is:

Manufacturer Public Key → Device Public Key (CARsaPub) → Ephemeral Public Key (KRsaPub) → public DHE parameters → TLS Pre-MS (Z) → TLS MS → TLS Session Keys.

During TLS connection establishment, clients (Crypto Officer or users) validate the entire trust chain to identify the module as the source of the Trusted Path and prevent MiTM and other attacks.

Table 13 : Cipher Suite Supported by the Module's TLS Implementation in FIPS Mode

TLS Implementation	
Suite Name	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
Authentication	RSA (RSA #2751; 2048, 3072 and 4096 bits)
Key Establishment	DHE (DSA #1336; L: 2048, N: 256)
Symmetric Cryptography	AES GCM 256(AES #5073)
Hash	SHA-384 (SHA #4131)

4.2.4.2 TLS CSPs

Table 14 : TLS CSPs

CSP	**Description**	**Format, Storage, and Protection**	**Lifecycle and Use**
DHE private (r_U)	2048-bit Diffie-Hellman ephemeral private key	Format: 2048-bit Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Establish TLS Pre-MS (Z)
			Generation: Generated using DRBG (#C558) during TLS session initialization in accordance with FIPS 186-4 and NIST SP 800-56Ar3 [10] (DSA #1336)
			Input: N/A

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • 64-bit GCM IV counter used with TLS Ks reaches maximum value • Start TLS Session, End TLS Session, Clear TLS State • Generate Ephemeral Key Pair, Set Module Configuration, Reset, Power on Compute Engine
Pre-MS (Z)	TLS pre-master secret	Format: 2048-bit Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Derive TLS MS
			Generation: Derived from the client DH public parameters in accordance with NIST SP 800-56Ar3 [10], 5.7.1.1
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • 64-bit GCM IV counter used with TLS Ks reaches maximum value • Start TLS Session, End TLS Session, Clear TLS State • Generate Ephemeral Key Pair, Set Module Configuration, Reset, Power on Compute Engine
MS	TLS master secret	Format: 384 bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Derive TLS Ks
			Generation: Derived from Pre-MS (Z) using a KDF in accordance with SP 800-135r1 (CVL #1633)
			Input: Input as part of a session ticket, encrypted by the TLS STEK (AES GCM 256)
			Output: Output as part of a session ticket, encrypted by the TLS STEK (AES GCM 256)

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • 64-bit GCM IV counter used with TLS Ks reaches maximum value • Start TLS Session, End TLS Session, Clear TLS State • Generate Ephemeral Key Pair, Set Module Configuration, Reset, Power on Compute Engine
TLS Ks	TLS Session Keys (AES GCM 256-bit)	Format: 256 bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Encrypt and decrypt data over TLS (AES GCM 256-bit, AES #5073)
			Generation: Derived from MS using a KDF in accordance with SP 800-135r1 (CVL #1633)
			Input: N/A
			Output: N/A
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • 64-bit GCM IV counter used with TLS Ks reaches maximum value • Start TLS Session, End TLS Session, Clear TLS State • Generate Ephemeral Key Pair, Set Module Configuration, Reset, Power on Compute Engine
TLS STEK	TLS Session Ticket Encryption Key (AES GCM 256-bit)	Format: 256 bits Storage: NVSRAM Protection: Encrypted using the Security Anchor Hardware AES Key	Use: Encrypt and decrypt TLS Sessions containing the MS (RFC5077 [18]) (AES GCM 256-bit, AES #5073).
			Generation: Generated internally using DRBG (#C558). Session tickets are regenerated using the DRBG when a new TLS connection is initiated and the current session key expires. The lifetime of a session key is configurable via the Set Module Configuration service.
			Input: N/A
			Output: N/A

CSP	Description	Format, Storage, and Protection	Lifecycle and Use
			Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Generate Ephemeral Key Pair, Set Module Configuration, Reset, Power on Compute Engine

4.2.5 KMIP Cryptographic Objects (CSPs and Public Keys)

Table 15 describes KMIP cryptographic objects stored within the Security Anchor as part of the "KMIP Key Management" service (Section 5.3.1). KMIP objects are protected by the tamper detection and response mechanisms (Section 4.5.1). Key management state includes all KMIP CSPs and cryptographic objects.

Table 15 : KMIP Cryptographic Objects (CSPs and Public Keys)

Type and Format	Storage and Protection	Lifecycle
User Passwords Format: between 64 and 1024 bits in length	Storage: Security Anchor flash storage Protection: Encrypted using the Flash Encryption Key (AES CBC 256 #5073) User passwords are first salted with a 256-bit random salt retrieved from the DRBG (#C558), then encrypted (AES CBC 256 #5073)	Use: Passwords are used for user role authentication (KMIP Admin User or KMIP User). Use of keys is KMIP User-specific. Generation: As part of KMIP Key Management service (Section 5.3.1) Input: • As part of KMIP Key Management Operations (Section 5.3.1) over Trusted Path with TLS, encrypted by TLS Ks (AES GCM 256) • Key Management State Operations: Import, encrypted by KMIP Import/Export Data Encryption Key (AES GCM 256) Output: • As part of KMIP Key Management Operations (Section 5.3.1), with the exception of User Passwords, over Trusted Path with TLS, encrypted by TLS Ks (AES GCM 256)
Symmetric Keys Format: 128, 192, or 256-bit Encryption/Decryption Modes: CBC, CTR, ECB, GCM[17] (AES #5073)		
HMAC Keys HMAC (#3385) Format: 112 to 1024 bits		
RSA Keys (public and private) Format: 2048, 3072, or 4096-bit Sign/Signature Verify Modes: PKCS 1v1.5/PSS with SHA256/SHA512 (RSA #2751), no padding method with SHA256/SHA512/none (RSA Signature Primitives RSASP1 Component CVL #1634)[18]		

[17] As per [5] keys used in GCM mode must not have been, or ever be, used in any other mode. The same key may however be used in ECB, CBC and CTR modes.
[18] As per [8], section 5.1, an RSA key pair may only be used with a single signature scheme throughout its lifetime.

Type and Format	Storage and Protection	Lifecycle
ECDSA Keys (public and private) Format: P-224, P-256, P-384, P-521 Sign/Signature Verify Modes: ECDSA with SHA224/SHA256/SHA384/SHA512 (ECDSA #1316)		• Key Management State Operations: Export, encrypted by KMIP Import/Export Data Encryption Key (AES GCM 256) Zeroization: • Tamper response • Factory Reset (Physical Zeroization) • Procedural Zeroization • Reset Service • Power on Compute Engine • KMIP Key Management State Operations: Reset, Import Init, Import Cancel • Key Management User Operation: Delete User • KMIP v1.4 Operation: Destroy (except for User Passwords)

4.3 General Public Keys and Parameters (PSPs)

In addition to CSPs, the Security Anchor stores certain public parameters. Public parameters do not require protection from distribution outside of the module. Hence, any role can read public parameters. Modification of public parameters however, is role-dependent. Public parameters are summarized in Table 16 (in addition to the public parameters specified in Table 15).

Table 16 : General Public Keys and Parameters (PSPs)

Public Parameter	Description	Format, Storage, and Protection	Lifecycle
Witness Register	Allows the creation of a public, historical record.	Format: 224, 256, 384, or 512 bits. Storage: Non-Zeroizable, non-battery-backed memory. Protection: Stored in plaintext	Use: User-specific
			Generation: Cleared (set to 0) on module power on. No other modifications are allowed while the Compute Engine is powered off.
			Input: N/A
			Output: Get Signed Witness service
			Deletion: Reset on power cycle
DHE Public Key (t_U)	2048-bit Security Anchor Diffie-Hellman public key.	Format: 2048 bits Storage: Security Anchor volatile RAM Protection: Stored in plaintext	Use: Establish TLS Pre-MS (Z)
			Generation: Generated using DRBG (#C558) during TLS session initialization in accordance with FIPS 186-4 and NIST SP 800-56Ar3 [10] (DSA #1336)
			Input: N/A

Public Parameter	Description	Format, Storage, and Protection	Lifecycle
			Output During the establishment of a TLS session (Start TLS Session service)
			Deletion Whenever the DHE private (r_U) is zeroized
Client DHE Public Key (t_V)	2048-bit client Diffie-Hellman public key.	Format: 2048 bits Storage: Security Anchor volatile RAM Protection: Stored in plaintext	Use: Establish TLS Pre-MS (Z)
			Generation: Generated by an external TLS client during the establishment of a TLS session.
			Input: During the establishment of a TLS session (Start TLS Session service)
			Output: N/A
			Deletion Whenever the DHE private (r_U) is zeroized
Device Public Key (CARsaPub)	The public key corresponding to the CSP "Device Private Key (CAPsaPriv)".	Format: 2048, 3072, or 4096-bit RSA modulus Storage: Security Anchor flash storage. Protection: Stored in plaintext	Use: By external clients to verify signatures by the Device Private Key.
			Generation: In factory (RSA #2751)
			Input: N/A
			Output: • Get Device Public Key service • As part of a plaintext X509 certificate via the Get Device Public Key Certificate service
			Deletion: Rendered unusable on zeroization of the Device Private Key
Device Public Key Certificate	The public key certificate for the Device Key Pair (CARsaPub and CARsaPriv). Proves the module's endorsement by the signer. When the module is shipped, the module comes with a certificate signed by the manufacturer (Private Machines Inc.).	Format: X.509 certificate (1-4092 bytes) Storage: Security Anchor flash storage Protection: Stored in plaintext	Use: • To uniquely identify the Security Anchor • Verification of data signed by the Device Private Key
			Generation: Generated by the manufacturer outside of the module during factory initialization.
			Input: N/A
			Output: Get Device Public Key Certificate service
			Deletion: Rendered unusable on zeroization of the Device Private Key
Client Device Public Key	The client Device Public Key provided to the Security Anchor during a KMIP Import/Export Init operation.	Format: 2048, 3072, or 4096-bit RSA modulus Storage: Security Anchor RAM	Use: To help validate the KMIP Importer/Exporter's root of trust (Section 5.3.1)
			Generation: Obtained by the module from an external client (the importing/exporting module.)

Public Parameter	Description	Format, Storage, and Protection	Lifecycle
		Protection: Stored in plaintext	Input: • Key Management State Operation: Import/Export – Init service
			Output: N/A
			Deletion: On the completion of the KMIP Key Management Import/Export - Init service
Client Device Public Key Certificate	The certificate for the Client Device Public Key. Provided to the Security Anchor during a KMIP Import/Export Init operation.	Format: X.509 certificate (1-4092 bytes) Storage: Security Anchor flash storage Protection: Stored in plaintext	Use: To help validate the KMIP Importer/Exporter's root of trust (Section 5.3.1)
			Generation: Obtained by the module from an external client (the importing/exporting module).
			Input: • Key Management State Operation: Import/Export – Init service
			Output: N/A
			Deletion: On the completion of the KMIP Key Management Import/Export – Init service
Ephemeral Public Key (KRsaPub)	The public key corresponding to the CSP Ephemeral Private Key (KRsaPriv).	Format: 2048, 3072, or 4096-bit RSA modulus Storage: Security Anchor flash storage. Protection: Stored in plaintext	Use: By clients in the TLS trust chain to verify signatures by the Ephemeral Private Key.
			Generation: When a new Ephemeral Private Key is generated
			Input: N/A
			Output: • Get Ephemeral Public Key service • As part of a plaintext X509 certificate via the Get Ephemeral Public Key Certificate service
			Deletion: Rendered unusable on zeroization of the Ephemeral Private Key
Ephemeral Public Key Certificate	The public key certificate for the Ephemeral Public Key (KRsaPub).	Format: X.509 certificate (1-4092 bytes) Storage: Security Anchor flash storage. Protection: Stored in plaintext	Use: TLS trust chain
			Generation When a new Ephemeral Private Key is generated
			Input N/A
			Output Get Ephemeral Public Key Certificate service
			Deletion Rendered unusable on zeroization of the Ephemeral Private Key

Public Parameter	Description	Format, Storage, and Protection	Lifecycle
Manufacturer Public Key (Device Certificate signer's public key)	The manufacturer's public key. This is the public key that endorses the Device Public Key.	Format: 2048, 3072, or 4096-bit RSA modulus and 32-bit public exponent Storage: Security Anchor flash storage Protection: Stored in plaintext	Use: To identify the module's manufacturer. Used by the KMIP Key Management services' Import/Export operations for signature verification in conjunction with the Device Public Key Certificate.
			Generation: Generated by the manufacturer outside of the module. Cannot be changed after the module is shipped.[19]
			Input: N/A
			Output: Get Device Public Key Certificate service
			Deletion: Rendered unusable on zeroization of the Device Private Key
Security Anchor Customer Root Key (SA CRK)	ECDSA P-256 public key.	Format: 512 bits (256-bit x and y offline coordinates) Storage: Security Anchor one-time programmable (OTP) flash Protection: Stored in plaintext	Use: To verify Security Anchor firmware integrity (ECDSA-SHA-256)
			Generation: Generated by manufacturer outside of the module. Cannot be changed after the module ships.
			Input: N/A
			Output: N/A
			Deletion: N/A
Lost Cert Ratchet	Indicates whether the FIPS certificate is invalidated. FIPS	Format: 1 byte	Use: Indicates whether the FIPS certificate is invalidated

[19] The SHA-512 hash of the Manufacturer Public Key that is loaded onto the module during manufacturing is:

```
d3ddcc162c06714affee7f26dd418046e984a3d03243e7be9e2321c1436959ba3e155bcf9663a
            b9491701531bda4eebe3d3fbf0263718abbc255f59db935fcb8
ff9f010b5bdd7591d052fdb8cfc6e7b842f8f973ab37a91ea5e16449c17e9278d9f95f265b050
            8f083348376aeb16d7f02b7b86cde634e8c9f875287049360de
d3ddcc162c06714affee7f26dd418046e984a3d03243e7be9e2321c1436959ba3e155bcf9663a
            b9491701531bda4eebe3d3fbf0263718abbc255f59db935fcb8
ff9f010b5bdd7591d052fdb8cfc6e7b842f8f973ab37a91ea5e16449c17e9278d9f95f265b050
            8f083348376aeb16d7f02b7b86cde634e8c9f875287049360de
```

The corresponding private key is used by the manufacturer to sign the Device Private Key. See also https://privatemachines.com/

Public Parameter	Description	Format, Storage, and Protection	Lifecycle
	certificate is invalidated when the Compute Engine is powered on.	Storage: Security Anchor flash storage Protection: Stored in plaintext	Generation: • Set to zero when the module ships indicating that the FIPS certificate is valid • Set to one when the Compute Engine is powered on indicating that the FIPS certificate is invalid. Cannot be reset back to zero.
			Input: N/A
			Output: • Get Status service • All non KMIP v1.4 services, as well as the KMIP v1.4 Query service
			Deletion: N/A
KMIP Key Management Import/Export Public Key	The public key corresponding to the CSP KMIP Import/Export Private Key.	Format: 2048, 3072, or 4096-bit RSA modulus Storage: Security Anchor flash storage Protection: Stored in plaintext	Use: Used by an external client to encrypt the KMIP Import/Export Data Encryption Key as part of the KMIP Import/Export RSA key wrapping
			Generation: When a new KMIP Key Management Import/Export Private Key is generated
			Input: N/A
			Output: • Get KMIP Import/Export Public Key service • As part of a plaintext X509 certificate via the Get KMIP Import/Export Public Key Certificate service
			Deletion: Rendered unusable on zeroization of the KMIP Key Management Import/Export Private Key
KMIP Key Management Import/Export Public Key Certificate	The public key certificate for the KMIP Key Management Import/Export Public Key.	Format: X.509 certificate (1-4092 bytes) Storage: Security Anchor flash storage Protection: Stored in plaintext	Use: Used by an external client to validate the KMIP Importer/Exporter's root of trust (Section 5.3.1)
			Generation: When a new KMIP Import/Export Private Key is generated
			Input: N/A
			Output: Get KMIP Import/Export Public Key Certificate service
			Deletion: Rendered unusable on zeroization of the KMIP Key Management Import/Export Private Key
KMIP Key Management Client Import/Export Public Key	The client public key for KMIP Import/Export.	Format: 2048, 3072, or 4096-bit RSA modulus Storage: Security Anchor RAM	Use: To encrypt the KMIP Import/Export Data Encryption Key as part of the KMIP Import/Export RSA key wrapping
			Generation: Generated by an external client.

Public Parameter	Description	Format, Storage, and Protection	Lifecycle
		Protection: Stored in plaintext	Input: Key Management State Operation: Export – Init service
			Output: N/A
			Deletion: On completion of the KMIP Key Management Client Export - Init service
KMIP Key Management Client Import/Export Public Key Certificate	The certificate for the KMIP Key Management Client Import/Export Public Key.	Format: X.509 certificate (1-4092 bytes) Storage: Security Anchor RAM Protection: Stored in plaintext	Use: To validate the KMIP Importer/Exporter's root of trust (Section 5.3.1)
			Generation: Generated by an external client.
			Input: Key Management State Operation: Export – Init service
			Output: N/A
			Deletion: On completion of the KMIP Key Management Export - Init service

4.4 User Data Storage

The Security Anchor also provides the "Volatile Access" service to allow users to store and retrieve arbitrary data. Table 17 describes the available storage.

Table 17 : Custom Storage Objects

Type	Description	Format	Lifecycle
Volatile RAM storage	RAM storage organized as slots	Format: 16 slots, 4096 bytes each Storage: Security Anchor RAM Protection: Stored in plaintext	Use: User specific
			Generation: N/A
			Input: Input by external user via the Volatile Access service
			Output: Output to external user via the Volatile Access service
			Zeroization: • On module power cycle • Reset • Power on Compute Engine

4.5 Zeroization

The module implements several mechanisms to protect CSPs. The module's tamper detection, response and zeroization mechanisms are discussed in detail in Section 7. Refer to the paragraphs below and Table 18.

4.5.1 Tamper Response

In the case of a tamper event, the Security Anchor Hardware AES Key (which encrypts the NVSRAM) is zeroized, rendering all other CSPs inaccessible. All memory that may temporarily contain CSPs, such as RAM, is also zeroized. After zeroization the module is also power cycled, after which all services are disabled and the module is in an error state.

4.5.2 Factory Reset (Physical Zeroization)

Factory Reset is triggered by bringing the Deactivate GPIO pin low for two consecutive seconds. The Deactivate pin is exposed outside the cryptographic boundary via one of the pins on the two ribbons described in Section 2. This pin is brought low by removing a jumper or cutting a loop wire located outside the module's cryptographic boundary. Factory Reset zeroizes the Security Anchor Hardware AES Key, which renders all other CSPs inaccessible (see Section 4.5.1). All memory that may temporarily contain CSPs, such as RAM, is also zeroized. The module is then power cycled, after which all services are disabled and the module is deactivated. After deactivation the module can only be reactivated in factory.

4.5.3 Procedural Zeroization

Procedural zeroization is an authenticated service available to the Crypto Officer role. Procedural zeroization achieves the same effect as Factory Reset (Physical Zeroization), the only difference being that procedural zeroization is triggered by explicit communication with the Security Anchor.

4.5.4 Reset Service and Other Zeroization Methods

The authenticated "Reset" service zeroizes all CSPs except the Security Anchor Hardware AES Key. It also zeroizes User Data Storage (volatile RAM storage). CSPs can later be generated within the Security Anchor in a FIPS conformant manner using appropriate services.

The "Reset" service, as well as any other zeroization event (with the exception of the Tamper, Factory Reset and Procedural Zeroization events) zeroizes CSPs by overwriting their memory locations with zeroes.

4.5.5 Summary of CSP Zeroization

Table 18 : Module Zeroization

Event	Zeroization Time	CSPs that are zeroized on event occurrence
Tamper Event	Less than 1 µs if the ARM core is off, 300 µs if it is on.	All CSPs
Factory Reset (Physical Zeroization)	300 µs	All CSPs
Procedural Zeroization	300 µs	All CSPs
Reset	4 ms or less	All CSPs except the Security Anchor Hardware AES Key
Power on Compute Engine	4 ms or less	All CSPs except the following[20]:

[20] These CSPs are not zeroized because:
a) the Security Anchor Hardware AES key encrypts the memory region where the other two are stored
b) the Crypto Officer Token is used to maintain the module's ownership by the operator
c) the Device Private Key is used to confirm the module's provenance (i.e. from the manufacturer)

Event	Zeroization Time	CSPs that are zeroized on event occurrence
		• Security Anchor Hardware AES Key • Crypto Officer Token • Device Private Key (CARsaPriv)

5. SERVICES

5.1 Services Implementation

All services are implemented by the Security Anchor firmware. The firmware is stored on the Security Anchor's flash memory during factory initialization. The firmware cannot be altered after factory initialization.

5.2 Service Access

Physical connectivity for service access spans over the external comms serial port and the Security Anchor.

TLS communication is employed over this physical channel. TLS is used to establish a Trusted Path per IG 2.1, as specified in 4.2.4.1 Trusted Path: TLS 1.2 Implementation. The Trusted Path is encrypted by TLS Ks (AES GCM 256, key establishment methodology provides 112 bits of encryption strength).

The module requires TLS be used for all authenticated services. The operator may choose to use TLS for all other services[21].

5.3 Approved Services

Services available in FIPS approved mode are described in Table 20. Table 20 also lists the CSPs accessed by an operator performing a service under an assumed role along with the access type. The following access types are covered:

- SA-Read: The CSP is read by the Security Anchor Firmware but is not returned to the operator.
- Operator-Read: The CSP is read by the Security Anchor Firmware and returned to the operator. The corresponding SA-Read is omitted.
- Operator-Generate: The CSP is generated at the specific request of the operator. The CSP is generated by the Security Anchor using approved algorithms.
- SA-Write: The CSP is written by the Security Anchor Firmware.
- Operator-Write: The CSP contents are provided by the operator to the Security Anchor and are written by the firmware. The corresponding SA-Write is omitted.
- SA-Zeroize: The CSP is zeroized by the Security Anchor Firmware.
- Operator-Zeroize: The CSP is zeroized by the Security Anchor Firmware at the specific request of the operator. The corresponding SA-Zeroize is omitted.

[21] Authenticated services must be executed via a TLS connection established between the operator and the module via the Start TLS Session service. The module will reject all such services sent in plaintext. This falls under IG 3.1 scenario (d): initialization procedures to set up the operator's authentication credentials.

Table 19 : Generic CSP Accesses (in Addition to Table 20)

Role	Service	Reason for Access	Algorithms	CSP/ Key Access
All	All services that access CSPs	CSPs are stored in NVSRAM and any access to this memory region requires the MAX32550 Memory Encryption Unit (MEU) hardware [19] to read this key to decrypt or encrypt the memory.	#C1028	MEU-Read: Security Anchor Hardware AES Key
All	All services executed over TLS	Encryption of TLS records sent to the operator.	AES #5073	SA-Read/SA-Write: AES GCM Authenticated Encryption IV, TLS Ks
Crypto Officer	All Crypto Officer Services	Crypto Officer Authentication		SA-Read Crypto Officer Token
All	All services except KMIP v1.4 operations, Tamper Response, Factory Reset, and End TLS Session	Internal state check performed by the Security Anchor firmware.		SA-Read: Crypto Officer Token
KMIP Admin User, KMIP User, General	All KMIP services (KMIP v1.4, User and State)	KMIP objects are stored encrypted by this key	AES #5073	SA-Read: Flash Encryption Key
KMIP Admin User, KMIP User	All KMIP services (KMIP v1.4, User and State)	Access to KMIP services via password authentication	AES #5073 SHA #4131	SA-Read: User Passwords

Table 20 : Services Available in FIPS Approved Mode

Role	Service	Service Function	Algorithms	CSP/ Key Access
Crypto Officer	Set Module Configuration	Sets the following module configuration parameters. · Witness Size: 224, 256, 384, or 512 bits · Ephemeral RSA key size: 2048, 3072, or 4096 bits · Ephemeral key pair auto-generation interval · KMIP Import/Export RSA key size: 2048, 3072, or 4096 bits · KMIP Import/Export key pair auto-generation interval · Flash access time and number of Flash accesses allowed per time interval · Manufacturer Set: Read-only parameter. If set, indicates the Manufacturer Public Key is set · TLS DH modulus size: 2048 · TLS session ticket lifetime in seconds · Flush communication buffers: If set, any transport-level communication buffers within the Security Anchor are flushed before each new connection · Compute engine power option. Can be auto or manual. Default is manual (Compute Engine not powered on). Powering on the Compute Engine calls the Power On Compute Engine service.	DRBG #C558 RSA #2751 SHS #4131	SA-Read/SA-Write: Ephemeral Private Key (KRsaPriv) SA-Zeroize: KMIP Import/Export Private Key, AES GCM Authenticated Encryption IV, All TLS CSPs DRBG Reseed CSP Accesses[22]

[22] To simplify the table, "DRBG Reseed CSP accesses" indicates: SA-Read/SA-Write: HMAC V/K, SA-Read/SA-Write/SA-Zeroize: Entropy Input/Seed

Role	Service	Service Function	Algorithms	CSP/ Key Access
Crypto Officer	Generate Ephemeral Key Pair	Generates a new Ephemeral key pair. The Ephemeral key pair is also auto-generated by the Security Anchor at a fixed interval.	DRBG #C558 RSA #2751 SHS #4131	SA-Read: Device Private Key (CARsaPriv) SA-Read/SA-Write/SA-Zeroize: Ephemeral Private Key (KRsaPriv) SA-Zeroize: AES GCM Authenticated Encryption IV, All TLS CSPs Operator-Generate: Ephemeral Private Key (KRsaPriv) DRBG Reseed CSP Accesses
Crypto Officer	Generate KMIP Key Management Import/Export Key Pair	Generates a new Key Management Import/Export key pair. The Key Management Import/Export key pair is also auto-generated by the Security Anchor at a fixed interval.	DRBG #C558 RSA #2751 SHS #4131	SA-Read: Device Private Key (CARsaPriv) SA-Read/SA-Write/SA-Zeroize: KMIP Import/Export Private Key Operator-Generate: KMIP Import Export Private Key DRBG Reseed CSP Accesses
Crypto Officer	Procedural Zeroization	Zeroizes all CSPs.	N/A	Operator-Zeroize: All CSPs

Role	Service	Service Function	Algorithms	CSP/ Key Access
Crypto Officer	Reset	Functional zeroization; zeroizes all CSPs except the Security Anchor Hardware AES Key.	N/A	Operator-Zeroize: All CSPs except the Security Anchor Hardware AES Key
Crypto Officer	Set Crypto Officer Token	Generates and returns to the caller a new Crypto Officer token.	DRBG #C558	Operator-Read: Crypto Officer Token Operator-Generate: Crypto Officer Token DRBG Reseed CSP Accesses
KMIP Admin User	KMIP Key Management Operations: User (Table 21)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Management of KMIP users and clock.	AES #5073 DRBG #C558 SHA #4131	Operator-Write: KMIP User Passwords Operator-Zeroize: All KMIP Cryptographic Objects[23] Operator-Write: KMIP User Passwords DRBG Reseed CSP Accesses

[23] See Key Management User Operation: Delete User

KMIP Admin User	KMIP Key Management Operations: State (Table 22)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Retrieve status information regarding the key management state and perform an Import or Export of the key management state. The key management state is encrypted by the KMIP Import/Export Data Encryption Key (AES GCM 256 #5073), which is generated by the exporting module and shared via an allowed key wrapping using the KMIP Import/Export Key Pair.	AES #5073 DRBG #C558 RSA #2751 SHA #4131 KTS (AES #5073) RSA (CVL Cert. #1635, key wrapping)	SA-Read: KMIP Import Export Private Key SA-Read/SA-Write/SA-Zeroize: KMIP Import/Export Data Encryption Key, AES GCM Authenticated Encryption IV SA-Write/SA-Zeroize: Flash Encryption Key Operator-Read/Operator-Write: KMIP Import/Export Data Encryption Key[24], All KMIP Cryptographic Objects[25] Operator-Generate: KMIP Import/Export Data Encryption Key, AES GCM Authenticated Encryption IV Operator-Zeroize: All KMIP Cryptographic Objects DRBG Reseed CSP Accesses

Role	Service	Service Function	Algorithms	CSP/ Key Access
KMIP Admin User	KMIP Key Management Operations: KMIP v1.4(Table 23)	No KMIP v1.4 operations are available to the KMIP Admin User.	N/A	N/A
KMIP User	KMIP Key Management Operations: User (Table 21)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Update the password of the caller to the specified value. KMIP Users can change their own passwords (DRBG used for password salt).	AES #5073 DRBG #C558 SHS #4131	Operator-Write: KMIP User Passwords DRBG Reseed CSP Accesses
KMIP User	KMIP Key Management Operations: State (Table 22)	No State operations are available to KMIP Users.	N/A	N/A

[24] Wrapped via the KMIP Import/Export Public Key or corresponding Client Public Key; transferred during Export/Import.
[25] Encrypted via the KMIP Import/Export Data Encryption Key; transferred during Export/Import.

Role	Service	Service Function	Algorithms	CSP/ Key Access
KMIP User	KMIP Key Management Operations: KMIP v1.4 (Table 23)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Execute any of authenticated KMIP v1.4 services provided by the module.	AES #5073 DRBG #C558 ECDSA #1316 HMAC #3385 RSA #2751 SHA #4131 RSASP1 component CVL #1634	SA-Read/SA-Write/SA-Zeroize: AES GCM Authenticated Encryption IV Operator-Read/Operator-Write/ Operator-Zeroize: All KMIP Cryptographic Objects[26] except User Passwords Operator-Generate: AES GCM Authenticated Encryption IV, All KMIP Cryptographic Objects[27] except User Passwords DRBG Reseed CSP Accesses
General	KMIP Key Management Operations: User (Table 21)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Create the module's KMIP Admin User and set the provided password (DRBG used for password salt). Only available if a KMIP Admin User does not exist, during the initialization of the KMIP layer.	AES #5073 DRBG #C558 SHS #4131	Operator-Write: User Password (only to set the initial password) DRBG Reseed CSP Accesses

[26] All KMIP Cryptographic Objects belonging to the KMIP User.
[27] All KMIP Cryptographic Objects belonging to the KMIP User.

Role	Service	Service Function	Algorithms	CSP/ Key Access
General	KMIP Key Management Operations: State (Table 22)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Configure the KMIP storage layer if not already configured or reset the KMIP storage layer.	AES #5073 RSA #2751 DRBG #C558	SA-Read: Device Private Key (CARsaPriv) SA-Write: Flash Encryption Key Operator-Zeroize: Flash Encryption Key, KMIP Import Export Data Encryption Key DRBG Reseed CSP Accesses
General	KMIP Key Management Operations: KMIP v1.4 (Table 23)	For details regarding the Security Anchor's KMIP Key Management service refer to Section 5.3.1. Execute the Discover Versions and Query KMIP v1.4 services.	N/A	N/A
General	Power on Compute Engine	Powers on the Compute Engine. When the Compute Engine is powered on, all CSPs are cleared with the exception of the Security Anchor Hardware AES Key[28], Crypto Officer Token and Device Private Key. Additionally, the FIPS certificate for the module is permanently invalidated by setting the Lost Cert ratchet. Certificate invalidation can be checked using the "Get Status" service or via the external status LED.	N/A	Operator-Zeroize: All CSPs except the Security Anchor Hardware AES Key, Crypto Officer Token, and Device Private Key
General	Get Compute Engine Power State	Returns a value indicating whether the Compute Engine is powered on or powered off.	N/A	N/A

[28] The Security Anchor Hardware AES key is not zeroized only because it encrypts the memory region in which the Crypto Officer Token and Device Private Key reside.

Role	Service	Service Function	Algorithms	CSP/ Key Access
General	Start TLS Session	Negotiate a TLS session with the module. TLS sessions are protected by AES GCM 256 #5073, which is conformant to SP 800-38F. TLS STEK are used by the server (module), but not known to the operator.	AES #5073 DSA #1336 DRBG #C558 HMAC #3385 KAS-SSC (vendor affirmed) KDF CVL #1633 RSA #2751 SHS #4131	SA-Read: Ephemeral Private Key (KRsaPriv) SA-Read/SA-Write/SA-Zeroize: AES GCM Authenticated Encryption IV, All TLS CSPs Operator-Read/Operator-Write: TLS MS (encrypted via the STEK) Operator-Generate: AES GCM Authenticated Encryption IV, All TLS CSPs with the exception of the STEK DRBG Reseed CSP Accesses
General	End TLS Session	Terminate a TLS session with the module.	AES #5073	SA-Read/SA-Zeroize: TLS Ks SA-Read/SA-Write/SA-Zeroize: AES GCM Authenticated Encryption IV Operator-Zeroize: All TLS CSPs with the exception of the STEK

Role	Service	Service Function	Algorithms	CSP/ Key Access
General	Clear TLS State	Clears the current TLS state between an external client and the Security Anchor. After this service, a new TLS session must be negotiated.	N/A	Operator-Zeroize: AES GCM Authenticated Encryption IV, All TLS CSPs with the exception of the STEK
General	Factory Reset (Physical Zeroization)	When triggered, all CSPs are zeroized.	N/A	Operator-Zeroize: All CSPs
General	Get Module Configuration	Returns the module configuration that was set using the "Set Module Configuration" service.	N/A	N/A
General	Get Device Public Key	Returns the Device Public Key.	N/A	SA-Read: Device Private Key (CARsaPriv)
General	Get Device Public Key Certificate	Returns the Device Public Key Certificate and the certificate signer's public key. This can be used to verify data signed within the Security Anchor using the Device Private Key.	N/A	N/A
General	Get Ephemeral Public Key	Returns the Ephemeral Public Key.	N/A	SA-Read: Ephemeral Private Key (KRsaPriv)
General	Get Ephemeral Public Key Certificate	Returns the Ephemeral Public Key Certificate. This can be used for TLS trust chain verification	N/A	SA-Read: Ephemeral Private Key (KRsaPriv)
General	Get KMIP Import/Export Public Key	Returns the KMIP Key Management Import/Export public key.	N/A	SA-Read: KMIP Import/Export Private Key
General	Get KMIP Import/Export Public Key Certificate	Returns the KMIP Key Management Import/Export Public Key Certificate.	N/A	N/A
General	Get Randoms	Returns the requested number of random bytes generated within the Security Anchor Random number generation is implemented using an HMAC-based DRBG with a security strength of 256 bits and with entropy input by the Security Anchor's NDRNG.	DRBG #C558	DRBG Reseed CSP Accesses
General	Get Signed Witness	The module signs and returns the Witness Register concatenated with the user-provided nonce.	RSA #2751	SA-Read: Device Private Key (CARsaPriv)

Role	Service	Service Function	Algorithms	CSP/ Key Access
General	Get Status	Returns the module's status, which also indicates whether the FIPS certificate has been invalidated (lost cert ratchet is set).	RSA #2751	SA-Read: Device Private Key (CARsaPriv)
General	Perform Self-Tests	Perform power-up self-tests, excluding the Firmware integrity test. For details, refer to Section 10.	All	SA-Read/SA-Write/SA-Zeroize: All DRBG CSPs
General	Power Cycle	Power cycles the module.	N/A	N/A
General	Power-up Self-Tests	Power-up self-tests (Section 10) are automatically triggered each time the module is powered on.	All	SA-Read/SA-Write/SA-Zeroize: All DRBG CSPs
General	Tamper Response	The Tamper Response service is triggered by physically manipulating the module (penetrating the protecting membrane, bringing the module outside of the valid temperature range etc.). In response to a tamper event all CSPs are zeroized and the module enters an error state. See (Section 7) for more information.	N/A	Operator-Zeroize: All CSPs
General	Volatile Access	Stores or reads data to/from a specified slot in the Security Anchor's User Data Storage.	N/A	N/A
General	Get Error	Returns information about any critical and non-critical errors that occurred during service execution.	N/A	N/A
General	Configure Critical Error Log	The critical error log contains information about fatal system errors. Using this service, the critical error log can be enabled, disabled, or cleared. (This service does not impact reporting or response to critical errors.) If disabled, no new entries are added to the critical error log.	N/A	N/A
General	Get Version	Returns the version of the Security Anchor firmware, API, KMIP Data Import/Export format, libucl and libdrbg versions.	N/A	N/A

5.3.1 KMIP Key Management Service

The Security Anchor provides a KMIP[29] 1.4 compliant key management service to users. Key management enables users to manage cryptographic keys and objects stored securely in the Security Anchor's flash storage. Keys and objects are stored encrypted with the CSP "Flash Encryption Key". Like other CSPs, cryptographic keys and objects managed via the key management service are protected through zeroization as part of the module's tamper detection and response mechanisms (Section 7).

[29] KMIP: Key Management Interoperability Protocol [1].

Table 21 : Key Management User Operations

Accessible to	Operation	Description
General Accessible only when the KMIP Admin User is not already set (e.g. during initialization).	Create Admin	Creates the KMIP Admin User with the password provided by the operator. Only one KMIP Admin User can exist at a time.
KMIP Admin User	Create User	Create a new KMIP User with a given username and password. The KMIP Admin User can only be created using the "Create Admin" operation.
KMIP Admin User	List Users	List all users.
KMIP Admin User	Delete User	Delete the KMIP User with the given username. The KMIP Admin User may not be deleted.
KMIP Admin User	Set User Password	Change the password of any user.
KMIP User	Set User Password	Change the password of a KMIP User. A KMIP User can only change their own password.
KMIP Admin User	Set Time	Set the Security Anchor's system time. The time is used only for KMIP operations, including import and export, and during the generation of the Ephemeral and KMIP Import/Export Public Key certificates.
KMIP Admin User	Get Time	Get the Security Anchor's current system time.
KMIP Admin User	Set Trim	Set the Security Anchor's RTC trim value to improve clock accuracy.
KMIP Admin User	Get Trim	Get the Security Anchor's RTC trim value.

Table 22 : Key Management State Operations

Accessible to	Operation	Description
General Accessible only when the KMIP storage layer is not already configured.	Configure KMIP Storage	The total available storage within the Security Anchor for KMIP objects is approximately 800KB. The "Configure KMIP Storage" operation is used to specify how the total available storage in the storage layer is distributed among different KMIP object types. Storage allocation is specified as the number of 4096-byte pages. KMIP objects are specified in Table 15.
KMIP Admin User	Get KMIP Storage Configuration	Get the KMIP configuration that was previously set using the "Configure KMIP Storage" operation.
KMIP Admin User	Get KMIP Storage Usage	Get details of how the storage layer is being used, including the amount of space available to store the various supported cryptographic objects.
KMIP Admin User	Export	Exports the Security Anchor's key management state. Key management state includes all KMIP CSPs and cryptographic objects (Table 15). The exported state is encrypted by the Security Anchor using the KMIP Import/Export Data Encryption Key (AES GCM 256 #5073), which is encrypted using the importing module's KMIP Import/Export Public Key as part of the allowed RSA key wrapping. Sub-operations: • Export Init: Initialize the KMIP export operation. The Security Anchor verifies the importer's root of trust, generates the KMIP Import/Export Data Encryption Key (AES key using DRBG

Accessible to	Operation	Description
		#C558), encrypts it using the importer's KMIP Import/Export Public Key (KMIP Key Management Client Import/Export Public Key) and returns the result to the caller. The result is also signed by the exporter's Device Private Key and the resulting signature returned as well. • Export: Start export of KMIP state. Security Anchor encrypts the KMIP state using the KMIP Import/Export Data Encryption Key (AES #5073) and exports the encrypted KMIP state. • Export Cancel: Cancel an in-progress KMIP export operation.
KMIP Admin User Accessible only when the KMIP storage layer is configured and a KMIP Admin User is set.	Import	Imports a given key management state (KMIP Cryptographic Objects) into the Security Anchor. Only a key management state exported from a module with the same root of trust[30] and firmware version can be imported. The imported state is encrypted using the KMIP Import/Export Data Encryption Key (AES GCM 256 #5073). The AES key is provided to the Security Anchor via the KMIP Import/Export RSA key wrapping. Sub-operations: • Import Init: Initialize the KMIP import operation. The KMIP Import/Export Data Encryption Key is transferred to the importing Security Anchor via the KMIP Import/Export RSA key wrapping. The importing Security Anchor decrypts the Data Encryption Key using the module's KMIP Import/Export Private Key • Import: Start import of KMIP state (AES #5073) • Import Cancel: Cancel an in-progress KMIP import operation.
General Triggered by three consecutive failed authentication attempts for the KMIP Admin User.	Reset	Resets the key management state. Reset zeroizes the CSP "Flash Encryption Key" which renders all cryptographic objects created via the KMIP-compliant operations irrecoverable. Also, zeroizes other KMIP-relevant CSPs. This does not zeroize other CSPs.

Table 23 : KMIP v1.4 Operations[31]

Accessible to	Operation[32]	Description
KMIP User	Create	Create an AES or HMAC Key and store the resulting KMIP Cryptographic Object (DRBG #C558)
KMIP User	Create Key Pair	Generate an RSA or ECDSA key pair and store the resulting KMIP Cryptographic Object (RSA #2751, ECDSA #1316, DRBG #C558)
KMIP User	Register	Register an AES, HMAC, RSA or ECDSA key/key pair and store the resulting KMIP Cryptographic Object
KMIP User	Locate	Locate all or a subset of the KMIP Cryptographic Objects the caller has access to
KMIP User	Check	Verify a KMIP Cryptographic Object's Cryptographic Usage Mask attribute

[30] Same root of trust implies that the Device Public Key of both the exporting and importing modules is certified by the same authority.
[31] These operations touch all KMIP Cryptographic Object CSPs with the exception of the KMIP User Password CSP, which is not specified in the KMIP 1.4 [1] specification.
[32] See KMIP 1.4 [1] and the module's KMIP user guide for implementation details.

Accessible to	Operation[32]	Description
KMIP User	Get	Return a KMIP Cryptographic Object
KMIP User	Get Attributes	Return the attributes of a KMIP Cryptographic Object
KMIP User	Get Attributes List	Return a list of the attributes set for a KMIP Cryptographic Object
KMIP User	Add Attribute	Add an attribute to a KMIP Cryptographic Object
KMIP User	Destroy	Destroy a KMIP Cryptographic Object
KMIP User	Encrypt	Encrypt data using the AES key stored in a KMIP Cryptographic Object (AES #5073, DRBG #C558)[33]
KMIP User	Decrypt	Decrypt data using the AES key stored in a KMIP Cryptographic Object (AES #5073)
KMIP User	Sign	Generate a signature using the key pair in a KMIP Cryptographic Object (RSA #2751, RSASP1 component CVL #1634[34], ECDSA #1316, DRBG #C558, SHS #4131)
KMIP User	Signature Verify	Verify a signature using the key pair in a KMIP Cryptographic Object (RSA #2751, ECDSA #1316, SHS #4131)
KMIP User	MAC	Perform a MAC using the key in a KMIP Cryptographic Object (HMAC #3385)
KMIP User	MAC Verify	Verify a MAC using the key in a KMIP Cryptographic Object (HMAC #3385)
KMIP User	RNG Retrieve	Generate and return random bytes using the module's DRBG (DRBG #C558)
KMIP User	RNG Seed	A no-operation (NOP) (does nothing)
KMIP User	Hash	Hash the provided data (SHS #4131)
General	Discover Versions	Return the KMIP versions supported by the module
General	Query	Return the capabilities of the KMIP server implemented by the module, including what operations are supported

5.4 Non-Approved Services

The module does not implement any non-approved services or functions.

6 SECURITY RULES

This section documents the security rules enforced by the cryptographic module to implement the security requirements of a FIPS 140-2 Level 4 Module.

- Secret Keys, Private Keys, Cryptographic Key Components, and all other CSPs are protected from unauthorized disclosure, modification, and substitution.
- Public keys are protected from unauthorized modification and substitution.
- In the event of tamper, all CSPs are zeroized.
- On change of certain module configuration parameters, user data and cryptographic objects are zeroized.
- After factory initialization, the module is shipped in FIPS approved mode.
- The module does not support a bypass or maintenance role
- The module does not support concurrent operators.
- If a self-test fails, the module transitions to an error state.
- All services except "Get Status" are disabled in an error state.

[33] For AES-GCM keys registered or created in the KMIP layer, a KMIP user may encrypt arbitrary data using IV lengths of >=96 bits and a valid tag. IVs are always generated internally via the DRBG, and in compliance with FIPS 140-2 IG A.5 case 2.

[34] KMIP Users may call the signature primitive directly and perform padding/hashing separately

- All data output via the data output interface is inhibited during self-tests, key generation and when in an error state.

6.1 Vendor-Imposed Security Rules

Following additional security rules are imposed by the vendor

- Key management state can only be exported between modules with the same root of trust[35].

7 PHYSICAL SECURITY POLICY

The module implements several mechanisms to protect CSPs. The module's physical design implements mechanisms to detect tamper events. CSPs are zeroized as a response to tamper events or by using certain module services. Table 18 summarizes zeroization.

7.1 Tamper Detection

Module's cryptographic boundary is the outer metal box (Figure 1). The inner metal box is completely enveloped by a tamper-sensitive membrane. Any attempt to gain access to components within the cryptographic boundary by physical tamper of the membrane is detected by the Security Anchor. Once physical tampering is detected, all CSPs are immediately zeroized.

7.2 Tamper Inspection

An operator can inspect the module for tamper and status using either (1) the external FIPS status LED (Table 6) or (2) the "Get Status" service (Section 5.3). If the module reports that it has been tampered with, the operator may check the source of the tamper event via the "Get Status" service. The tamper source returned by the service should be used for informational purposes only as a tampered Security Anchor may not be trusted. Once tampered, the module will not be reinitialized by the manufacturer. Any attempted reinitialization, even if successful, will not contain the manufacture-signed certificates and hence clearly indicates to clients (users, Crypto Officers, KMIP users) that the module is not as per its original FIPS certified state.

7.3 Environmental Failure Protection (EFP) and Testing (EFT)

In addition to tamper detection mechanisms, the module also provides Environmental Failure Protection (EFP) features. EFP features are provided by the Security Anchor for temperature and voltage extremes. Environmental Failure Testing (EFT) demonstrated that if the operating temperature or battery voltage varies outside of the module's normal operating range, the module does not compromise CSPs.

8 OPERATIONAL ENVIRONMENT

The FIPS 140-2 operational environment requirements for the module are not applicable because the device does not contain a modifiable operational environment. Security Anchor firmware is loaded in factory and cannot be modified once the module has shipped.

9 EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

[35] Same root of trust implies that the Device Public Key of both the exporting and importing modules is certified by the same authority.

10 SELF-TESTS

Self-tests are performed by the Security Anchor. Self-tests cover all cryptographic functions used by the module's services. A reboot of the module automatically triggers the self-tests irrespective of the mode of operation. Self-tests, excluding the "Firmware tests", can also be performed via the 'Perform Self-Tests' service. Firmware tests are part of the power-up tests. Algorithm self-tests are performed as Known Answer Tests (KATs) or Pairwise Consistency Tests (PWCTs).

If any self-test fails the module enters an error state. In an error state, all Crypto Officer and user services except "Get Status" are disabled. To restore functionality, the module must be power-cycled and all self-tests must pass.

10.1 Power-up Self-Tests

Table 24 - Firmware Power-up Self-test

Tested Function	Self-Test	Error	Error Indicator	Access	Error Resolution
• Security Anchor Firmware • Libdrbg • Libucl	Firmware integrity test: Verification of the ECDSA P-256 Signature using the Security Anchor Customer Root Key (SA CRK) (ECDSA #1316)	Power-on failure	Module does not boot	All services (cryptographic operations and data output) are disabled	Power cycle the module

Table 25 : Algorithm Power-up Self-tests (all modes of operation)

Tested Function	Self-Tests	Error Response
AES Tests (AES #5073)	• AES ECB Encrypt KAT • AES ECB Decrypt KAT • AES CBC Encrypt KAT • AES CBC Decrypt KAT • AES CTR Encrypt KAT • AES CTR Decrypt KAT • AES GCM Encrypt KAT • AES GCM Decrypt KAT	Error: Self-test failure Error Indicator: Get Status service indicates Error State. External FIPS Status LED is red and blinks. Access: All services (cryptographic operations and data output) are disabled Error Resolution: Power cycle the module and all self-tests must pass
AES Tests (#C1028)	• AES ECB Encrypt KAT • AES ECB Decrypt KAT	
DRBG Health Tests[36] for HMAC DRBG (#C558)	• DRBG instantiate KAT • DRBG generate KAT • DRBG reseed KAT	
ECDSA Tests (ECDSA #1316)	• ECDSA sign/verify PWCT	
HMAC Tests (HMAC #3385)	• HMAC-SHA-384 KAT	

[36] In accordance with IG 9.8, the SP 800-90Ar1 [7] compliant DRBG does not perform the continuous random number generator test described in FIPS 140-2 section 4.9.2

Tested Function	Self-Tests	Error Response
KAS (SP 800-56Ar3 with FFC DH and KDF CVL #1633)	• DH primitive Z computation KAT • KDF KAT SHA-384 (covered by SHA KAT)	
RSA Tests (RSA #2751)	• RSA PKCS signature generation KAT • RSA PKCS signature verification KAT	
SHA Tests (SHA #4131)	• SHA-1 KAT • SHA-224 KAT • SHA-256 KAT • SHA-384 KAT • SHA-512 KAT	
Critical Function Test: Check Past Tamper Record	Check if a tamper event occurred previously	
Critical Function Test: Compute Engine Status	Check whether the Compute Engine (CE) has ever been powered on by checking if the LOST_CERT ratchet is set.	Error: Lost cert ratchet is set; module has lost its FIPS 140-2 certificate Error Indicator: Get Status service indicates the certificate has been lost. External FIPS Status LED turns blue. Access: All services remain enabled, All CSPs are zeroized except for the Security Anchor Hardware AES key, Crypto Officer Token and Device Private Key. See Table 18 and the Power on Compute Engine service for more information. Error Resolution: No resolution possible, certificate is lost for the lifetime of the module.
Critical Function Test: Security Monitor External Sensor Check	Check whether the MAX32550 [19] Security Monitor external sensors are properly configured.	Error: The module fails to ensure that the external sensors are configured properly. Error Indicator: The module clears all CSPs (Procedural Zeroization) and power cycles the module. Access: The module is reverted to factory state. Error Resolution: No resolution possible; CSPs are cleared and module is returned to factory state.
Critical Function Test: Ephemeral Key Pair and Ephemeral Public Key Certificate are present	Check whether the Ephemeral Key Pair and Ephemeral Public Key Certificate are present. If not, an attempt is made to generate them.	Error: The module fails to generate an Ephemeral Key Pair and/or the Ephemeral Public Key Certificate. Error Indicator: Get Status service indicates Error State. External FIPS Status LED is red and blinks. Access: All services (cryptographic operations and data output) are disabled Error Resolution: Power cycle the module and all self-tests must pass, including this critical function test.

10.2 Conditional Self-Tests

Table 26 : Conditional Self-tests

Tested Function	Self-Tests	Initiation	Error Response
NDRNG[37]	Continuous Random Number Generator Test (CRNGT)	By a service that uses the DRBG (Table 9)	Error: Conditional-test failure Error Indicator: Get Status service indicates error state. External FIPS Status LED is red and blinks. Access: All services (cryptographic operations and data output) are disabled Error Resolution: Power cycle the module and all self-tests must pass
KAS (SP 800-56Ar3 with FFC DH and KDF CVL #1633)	Pairwise consistency for Diffie Hellman keys (DSA #1336) (per 5.6.2.1.4 a of [10])	TLS (Section 5.1)	
	FFC Full Public Key Validation (per 5.6.2.3.1 of [10])		
	Assurance of Domain Parameter Validity (per 5.5.2 option 3 [10])		
ECDSA (ECDSA #1316)	Pair-wise consistency test for KMIP key generation (ECDSA) using ECDSA-SHA256	Each new key pair for service: KMIP Key Management	
RSA Sign/Verify (RSA #2751)	Pair-wise consistency test for Security Anchor key generation (RSA) of keys used for signature generation and verification. The PKCS1v1.5-SHA256 or SHA512 method is used.	Each new key pair for services: Generate Ephemeral Key Pair, and KMIP Key Management	
RSA Key Wrapping (CVL #1635)	Pair-wise consistency test for Security Anchor key generation (RSA) of keys used in allowed RSA key wrapping using OAEP-SHA256	The Generate KMIP Import/Export Key Pair service	
Critical Function Test: Ephemeral Key Pair and Ephemeral Public Key Certificate Generation	Ensure that the Ephemeral Key Pair and Certificate are successfully regenerated	Execution of the Generate Ephemeral Key Pair or the Set Module Configuration service.	
Critical Function Test: Compute Engine Status	Check whether the CE has ever been powered on by checking if the Lost Cert ratchet is set.	Execution of the Get Status or Power on Compute Engine service	Error State: Lost Cert Ratchet is set or Compute Engine is powered on. Error Indicator: External status LED turns blue indicating the FIPS certificate is invalidated.

[37] The NDRNG performs the continuous random number generator test described in FIPS 140-2 section 4.9.2

Tested Function	Self-Tests	Initiation	Error Response
			Get Status service indicates the same. Access: All services remain enabled. All CSPs are zeroized except for the Security Anchor Hardware AES key, Crypto Officer Token and Device Private Key. See Table 18 and the Power on Compute Engine service for more information. Error Resolution: No resolution possible, FIPS certificate is invalidated for the lifetime of the module.

11 MITIGATION OF OTHER ATTACKS

In addition to the protections provided by FIPS 140-2 Level 4, the module mitigates the following attacks:

Table 27 - Mitigations of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Invasive Attacks: Membrane	A random signal is constantly sent out across the module's membrane by the Security Anchor and checked for correctness. Any break in the membrane will result in a different than expected value being received by the Security Anchor.	N/A
Invasive Attacks: Chip	The System on a Chip (SoC) on which the Security Anchor executes has a protective shield built into the chip that triggers a tamper response when it is penetrated.	N/A
SPA/DPA Attacks	The module employs protections against SPA/DPA attacks by internally regulating and filtering the voltage lines to the Security Anchor. The amplitude of the power signal an attacker observes is significantly reduced from the actual power draw of the Security Anchor. Additionally, the input power to the Compute Engine is low-pass filtered. An attacker's observable signal is 100-350 dB below the true power draw of the Compute Engine.	N/A
SEMA/DEMA Attacks	The module grounds the inner enclosure containing all cryptographically sensitive module circuitry. This creates a Faraday cage that significantly reduces EM radiation entering or leaving the module.	N/A
Timing Attacks	The module employs RSA blinding and constant time comparisons when appropriate.	N/A

12 ABBREVIATIONS AND DEFINITIONS

Compute Engine	General purpose motherboard that remains off during the FIPS lifecycle of the module.
Security Anchor	The security module that generates and stores CSPs, and provides tamper response and CSP zeroization
DRBG	Deterministic Random Bit Generator
NDRNG	Non-Deterministic Random Number Generator
SHA	Secure Hash Algorithm
AES	Advanced Encryption Standard
OAEP	Optimal Asymmetric Encryption Padding
KAT	Known Answer Test
ROM	Read Only Memory
OTP	One-time Programmable Storage
GPIO	General Purpose Input Output
KMIP	Key Management Interoperability Protocol
Root of Trust	For the purpose of this policy, the authority that signs the Security Anchor's Device Public Key
ECDSA	Elliptic Curve Digital Signature Algorithm
SPA/DPA	Simple power analysis/differential power analysis
SEMA/DEMA	Simple electromagnetic analysis/differential electromagnetic analysis

13 REFERENCES

[1] OASIS, "KMIP (Key Management Interoperability Protocol) v1.4," 22 November 2017. [Online]. Available: http://docs.oasis-open.org/kmip/spec/v1.4/kmip-spec-v1.4.html. [Accessed 21 June 2018].

[2] NIST, "FIPS 140-2," 25 May 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf. [Accessed 21 November 2019].

[3] NIST, "FIPS 197 - Advanced Encryption Standard (AES)," 26 November 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. [Accessed 21 November 2019].

[4] NIST, "SP 800-38A - Recommendation for Block Cipher Modes of Operation," December 2001. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf. [Accessed 21 November 2019].

[5] NIST, "SP 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," November 2007. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf. [Accessed 21 November 2019].

[6] NIST, "SP 800-133 r1 - Recommendation for Cryptographic Key Generation," July 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r1.pdf. [Accessed 21 November 2019].

[7] NIST, "SP 800-90A r1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators," June 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf. [Accessed 21 November 2019].

[8] NIST, "FIPS 186-4 - Digital Signature Standard (DSS)," July 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf. [Accessed 21 November 2019].

[9] NIST, "FIPS 198-1 - Keyed-Hash Message Authentication Code (HMAC)," July 2008. [Online]. Available: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf. [Accessed 2019 21 November].

[10] NIST, "SP 800-56A r3 - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf. [Accessed 21 November 2019].

[11] NIST, "SP 800-135 r1 - Recommendation for Existing Application-Specific Key Derivation Functions," December 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf. [Accessed 21 November 2019].

[12] NIST, "SP 800-38F - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping," December 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf. [Accessed 21 November 2019].

[13] NIST, "SP 800-56B - Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography," August 2009. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-56b.pdf. [Accessed 21 November 2019].

[14] NIST, "FIPS 180-4 - Secure Hash Standard," August 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. [Accessed 21 November 2019].

[15] IETF, "RFC5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS," August 2008. [Online]. Available: https://tools.ietf.org/html/rfc5288. [Accessed 21 November 2019].

[16] NIST, "SP 800-52 r2 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," August 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf. [Accessed 21 November 2019].

[17] IETF, "RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2," August 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246. [Accessed 21 November 2019].

[18] IETF, "RFC5077 - Transport Layer Security (TLS) Session Resumption without Server-Side State," January 2008. [Online]. Available: https://tools.ietf.org/html/rfc5077. [Accessed 21 November 2019].

[19] MAXIM, "MAX32550: DeepCover Secure Arm Cortex-M3 Flash Microcontroller," MAXIM, [Online]. Available: https://www.maximintegrated.com/en/products/microcontrollers/MAX32550.html. [Accessed 21 November 2019].

[20] OASIS, "KMIP (Key Management Interoperability Protocol) v1.3," [Online]. Available: http://docs.oasis-open.org/kmip/spec/v1.3/os/kmip-spec-v1.3-os.pdf.

[21] F. 186-4., "NIST FIPS 186-4: Digital Signature Standard, Jul-2013.".

[22] NIST, "FIPS 186-2 - Digital Signature Standard (DSS)," 27 January 2000. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/fips/186/2/archive/2000-01-27/documents/fips186-2.pdf. [Accessed 21 November 2019].

[24] "Max v2," [Online]. Available: http://www.minnowboard.org/meet-minnowboard-max/.

[25] MAX32550, [Online]. Available: https://www.maximintegrated.com/en/products/digital/microcontrollers/MAX32550.html.

[26] "FIPS 197 - ADVANCED ENCRYPTION STANDARD (AES)," [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Private Machines
Hype-free Security for Infrastructure and Cloud

Private Machines Inc.
164 20 Street, 4th floor
Brooklyn, NY 11232

https://privatemachines.com
info@privatemachines.com
+1 - 631 - 731 - 1695
+1 - 8777 - CIPHER