PRIVATE MACHINES INC.

ENFORCER R2

FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

This document may be freely reproduced and distributed, but only in its entirety and without modification.

TABLE OF CONTENTS

1 General 6

1.1 Overview 6

1.2 Security Levels 6

2 Cryptographic Module Specification 7

2.1 Description 7

2.2 Tested and Vendor Affirmed Module Version and Identification 8

2.3 Excluded Components 8

2.4 Modes of Operation 8

2.5 Algorithms 8

2.6 Security Function Implementations 11

2.7 Algorithm Specific Information 16

2.8 RBG and Entropy 16

2.9 Key Generation 17

2.10 Key Establishment 17

2.11 Industry Protocols 17

3 Cryptographic Module Interfaces 17

3.1 Ports and Interfaces 17

4 Roles, Services, and Authentication 18

4.1 Authentication Methods 18

4.2 Roles 19

4.3 Approved Services 20

4.4 Non-Approved Services 39

4.5 External Software/Firmware Loaded 39

5 Software/Firmware Security 39

5.1 Integrity Techniques 39

5.2 Initiate on Demand 40

6 Operational Environment 40

6.1 Operational Environment Type and Requirements 40

7 Physical Security 40

7.1 Mechanisms and Actions Required 40

7.2 EFP/EFT Information 41

8 Non-Invasive Security 41

This document may be freely reproduced and distributed, but only in its entirety and without modification.

8.1 Mitigation Techniques 41
9 Sensitive Security Parameters Management 41
9.1 Storage Areas 41
9.2 SSP Input-Output Methods 42
9.3 SSP Zeroization Methods 43
9.4 SSPs 44
10 Self-Tests 52
10.1 Pre-Operational Self-Tests 52
10.2 Conditional Self-Tests 53
10.3 Periodic Self-Test Information 57
10.4 Error States 59
10.5 Operator Initiation of Self-Tests 59
11 Life-Cycle Assurance 60
11.1 Installation, Initialization, and Startup Procedures 60
11.2 Administrator Guidance 60
11.3 Non-Administrator Guidance 60
11.4 Design and Rules 60
11.5 End of Life 61
12 Mitigation of Other Attacks 61
12.1 Attack List 61
12.2 Mitigation Effectiveness 61
13 References 61

This document may be freely reproduced and distributed, but only in its entirety and without modification.

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 11
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Security Function Implementations 16
Table 7: Entropy Certificates 17
Table 8: Entropy Sources 17
Table 9: Ports and Interfaces 18
Table 10: Authentication Methods 19
Table 11: Roles 20
Table 12: Approved Services 39
Table 13: Mechanisms and Actions Required 41
Table 14: EFP/EFT Information 41
Table 15: Storage Areas 42
Table 16: SSP Input-Output Methods 43
Table 17: SSP Zeroization Methods 43
Table 18: SSP Table 1 48
Table 19: SSP Table 2 52
Table 20: Pre-Operational Self-Tests 53
Table 21: Conditional Self-Tests 57
Table 22: Pre-Operational Periodic Information 57
Table 23: Conditional Periodic Information 59
Table 24: Error States 59

This document may be freely reproduced and distributed, but only in its entirety and without modification.

List of Figures

Figure 1 -- ENFORCER R2 7

1 GENERAL

1.1 OVERVIEW

This document forms a cryptographic module Security Policy for Private Machines Inc. ENFORCER R2 under the terms of NIST FIPS 140-3.

The ENFORCER R2 is a single-user, multi-chip stand-alone cryptographic module. This Security Policy specifies the security rules under which this device operates.

1.2 SECURITY LEVELS

The module meets the overall requirements of FIPS 140-3 Security Level 4.

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

Table 1: Security Levels

This document may be freely reproduced and distributed, but only in its entirety and without modification.

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The ENFORCER R2 is illustrated in Figure 1 below. The device's cryptographic boundary is designated at the perimeter of the outer metal enclosure.



Figure 1 -- ENFORCER R2

The key security component within the module is the Security Anchor. All critical module services are provided by the Security Anchor. The module uses the Maxim MAX32550 DeepCover Secure Cortex-M3 Flash Microcontroller as the Security Anchor. The Security Anchor also provides CSP zeroization as a tamper response. This security policy applies to all module components within the cryptographic boundary. A general-purpose computer (GPC) termed the Compute Engine is contained within the cryptographic boundary. After factory initialization, the module operates in an approved mode of operation. All authenticated services are accessible over the module's serial interface using a TLS connection between an external user and the Security Anchor.

Purpose and Use:

The module serves the following purposes:

- Provides a physically secure, Level 4 enclosure protecting CSPs and cryptographic data. A physical tamper event on the enclosure immediately zeroizes module CSPs.
- Provides additional services for module management, module configuration, and for building higher-level application scenarios such as integration into cloud and data center environments.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary is defined as the physical perimeter of the outer enclosure.

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The ENFORCER R2 cryptographic module is designed to meet the requirements of FIPS 140-3 Security Level 4 (refer to Table 2). The module is available in the following configuration.

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ENFORCER R2	ENFORCER.R2.X12	Security Anchor Firmware version: 2.5.3, Security Anchor Bootloader version: 1.1.6, Compute Engine Firmware Version: 1.6.1, Compute Engine Application: “hello, world”	Maxim MAX32550 DeepCover Secure Cortex-M3 and SuperMicro X12SDV-8C-SPT4F	Opaque outer enclosure

Table 2: Tested Module Identification – Hardware

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

2.3 EXCLUDED COMPONENTS

The module does not exclude any components from the requirements of FIPS 140-3.

2.4 MODES OF OPERATION

Modes List and Description:

The module supports a single approved mode of operation. There are no degraded modes, non-approved modes or non-approved services available to the module. Upon successful completion of the pre-operational and conditional self-tests on power-up, the module provides an indicator of the approved mode via the "Get Status" service.

Mode Name	Description	Types of Services	Status Indicator
Approved Mode	The module supports a single approved mode of operation.	Approved	The module's mode of operation can be verified using the "Get Status" service. The "Get Status" service indicates that the module is in the Approved mode.

Table 3: Modes List and Description

2.5 ALGORITHMS

The ENFORCER R2 cryptographic module supports the approved cryptographic algorithms shown in the table below.

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Approved Algorithms:

The module supports the following approved cryptographic algorithms.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-CTR, AES-ECB	A6061	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	C1028	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-GCM	A6061	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
DSA KeyGen (FIPS186-4)	A6061	L - 2048, 3072 N - 224, 256	FIPS 186-4
ECDSA KeyGen (FIPS186-5)	A6061	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6061	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6061	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6063	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC DRBG	A6062	Prediction Resistance - No, Yes Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	A6061	Key Length - Key Length: 8-2048 Increment 8	FIPS 198-1

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A6061	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6061	Domain Parameter Generation Methods - ffdhe2048 Scheme - dhEphem - KAS Role - responder	SP 800-56A Rev. 3
KDF TLS (CVL)	A6061	TLS Version - v1.2 Hash Algorithm - SHA2-384	SP 800-135 Rev. 1
KTS-IFC	A6061	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg1-prime-factor Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 256	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A6061	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2pow100 Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5), RSA SigVer (FIPS186-5)	A6061, A6063	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	A6061	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256, SHA2-384, SHA2-512	A6063	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm	CAVP Cert	Properties	Reference
TLS v1.3 KDF (CVL)	A6061	HMAC Algorithm - SHA2-384 KDF Running Modes - PSK	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module supports the following vendor affirmed algorithms.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	NIST SP 800-133r2 Sections 4 example 1, 5.1, 5.2, and 6.1.

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 SECURITY FUNCTION IMPLEMENTATIONS

Name	Type	Description	Properties	Algorithms
AKG	AsymKeyPair-KeyGen CKG	Asymmetric Key Generation	Standards:NIST FIPS 186-5, SP 800-133r2	CKG: () DSA KeyGen (FIPS186-4): (A6061) Strengths: 112, 128 bits Private Key Lengths: 224, 256 bits RSA KeyGen (FIPS186-5): (A6061) Moduli: 2048, 3072, 4096 ECDSA KeyGen (FIPS186-5): (A6061)

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Type	Description	Properties	Algorithms
				Curves: P-224, P-256, P-384, P-521 HMAC DRBG: (A6062) Prediction Resistance: Yes, No Supports: Reseed
DEC	BC-UnAuth	Symmetric Decryption	Standards:NIST FIPS 197, SP 800-38A	AES-CBC: (A6061) Strength: 128, 192, 256 bits AES-ECB: (A6061) Strength: 128, 192, 256 bits AES-ECB: (C1028) Strength: 256 bits AES-CTR: (A6061) Strength: 128, 192, 256 bits
DEC_Auth	BC-Auth	Authenticated Decryption	Standards:NIST FIPS 197, SP 800-38D	AES-GCM: (A6061) Strength: 128, 192, 256 bits
DRBG	DRBG	Random bit generation	Standard:SP800-90Ar1	HMAC DRBG: (A6062) Prediction Resistance: Yes, No Supports: Reseed Mode: SHA2-256 Entropy Input: 512 Nonce: 256 Personalization String Length: 0 Additional Input: 0 Returned Bits: 1024
ENC	BC-UnAuth	Symmetric Encryption	Standards:NIST FIPS 197, SP 800-38A	AES-CBC: (A6061) Strength: 128, 192, 256 bits AES-ECB: (A6061) Strength: 128, 192, 256 bits AES-ECB: (C1028)

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Type	Description	Properties	Algorithms
				Strength: 256 bits AES-CTR: (A6061) Strength: 128, 192, 256 bits
ENC_Auth	BC-Auth	Authenticated encryption	Standards:NIST FIPS 197, SP 800-38D	AES-GCM: (A6061) Strength: 128, 192, 256 bits
ESV	ENT-ESV	SP800-90B Physical Entropy Source	Standard:SP800-90B Physical Entropy Source	
KAS	KAS-Full	Key agreement schemes and key derivation functions TLS CVL	Standards:NIST SP 800-56Ar3, SP 800-135r1 IG:IG D.F Scenario 2 path (2), split Key confirmation:No Key derivation:IG 2.4.B SP 800-135r1 CVL, SP 800-56Cr2 Caveat:Key establishment methodology provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A6061) Scheme: Ephemeral Unified Model, C(2e, 0s, ECC CDH) KAS-FFC-SSC Sp800-56Ar3: (A6061) Scheme: FFC DH dhEphem, C (2e, 0s, FFC DH) KDF TLS: (A6061) TLS version: v1.2 Hash Algorithm: SHA2-384 TLS v1.3 KDF: (A6061) HMAC Algorithm: HMAC-SHA2-384 KDF Running Modes: PSK
KTS-GCM	KTS-Wrap	Key transport scheme	Standard:NIST SP 800-38D IG:Approved method from IG D.G Caveat:Key establishment methodology provides between 112 and 256 bits of security strength	AES-GCM: (A6061) Strength: 256-bit Direction: Decrypt, Encrypt IV Generation: Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Type	Description	Properties	Algorithms
				Tag Length: 64, 96, 104, 112, 120, 128 IV Length: 96-1024 Increment 8 Payload Length: 8-32768 Increment 8 AAD Length: 0-32768 Increment 8
KTS-RSA	KTS-Encap	RSA key encapsulation and un-encapsulation	Standard:NIST SP 800-56Br2 IG:Approved method from IG D.G Key Confirmation:No Caveat:Key establishment methodology provides between 112 and 140 bits of security strength	KTS-IFC: (A6061) Moduli: 2048, 3072, 4096 Key Generation Method: rsakpg1-prime-factor KAS Roles: initiator, responder
MAC	MAC	Message authentication codes	Standard:NIST FIPS 198-1	HMAC-SHA-1: (A6061) MAC: 160 Key Length: 8-2048 Increment 8 HMAC-SHA2-224: (A6061) MAC: 224 Key Length: 8-2048 Increment 8 HMAC-SHA2-256: (A6061) MAC: 256 Key Length: 8-2048 Increment 8 HMAC-SHA2-384: (A6061) MAC: 384 Key Length: 8-2048 Increment 8 HMAC-SHA2-512: (A6061) MAC: 512 Key Length: 8-2048 Increment 8

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Type	Description	Properties	Algorithms
SHS	SHA	Message Digest	Standard:NIST FIPS 180-4	SHA-1: (A6061) Message Length: 8-65536 Increment 8 SHA2-224: (A6061) Message Length: 8-65536 Increment 8 SHA2-256: (A6061) Message Length: 8-65536 Increment 8 SHA2-384: (A6061) Message Length: 8-65536 Increment 8 SHA2-512: (A6061) Message Length: 8-65536 Increment 8 SHA2-256: (A6063) Message Length: 0-65536 Increment 8 SHA2-384: (A6063) Message Length: 0-65536 Increment 8 SHA2-512: (A6063) Message Length: 0-65536 Increment 8
SigGen	DigSig-SigGen	Digital Signature Generation	Standard:NIST FIPS 186-5	ECDSA SigGen (FIPS186-5): (A6061) Curves: P-224, P-256, P-384, P-521 RSA SigGen (FIPS186-5): (A6061) Moduli: 2048, 3072, 4096
SigVer	DigSig-SigVer	Digital Signature Verification	Standards:NIST FIPS 186-5	ECDSA SigVer (FIPS186-5): (A6061) Curves: P-224, P-256, P-384, P-521 RSA SigVer (FIPS186-5): (A6061, A6063) Moduli: 2048, 3072, 4096

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Type	Description	Properties	Algorithms
				ECDSA SigVer (FIPS186-5): (A6063) Curves: P-256, P-384, P-521
SKG	CKG	Symmetric Key Generation	Standard:NIST SP 800-133r2	HMAC DRBG: (A6062) Prediction Resistance: Yes, No Supports: Reseed CKG: ()

Table 6: Security Function Implementations

2.7 ALGORITHM SPECIFIC INFORMATION

The module utilizes only approved algorithms that are tested and validated under the Cryptographic Algorithm Validation Program (CAVP).

The module's AES-GCM implementation conforms to IG C.H scenario 2. The module uses the approved DRBG (Cert. #A6062) to generate the IV with a length of at least 96 bits. The entropy source producing the DRBG seed is located inside the module’s cryptographic boundary.

The module's use of DSA KeyGen complies with IG C.K. DSA KeyGen (Cert. #A6061) is used exclusively for KAS-FFC-SSC SP 800-56Ar3 (Cert. #A6061). This usage is allowed per IG C.K Resolution 3. The strength of the DSA key pairs thus generated is 112 per NIST SP 800-57 Part 1 Rev. 5, Section 5.6.1.1, Table 2. These DSA keys are ephemeral keys. No DSA static keys are generated.

The module's TLS 1.2 and 1.3 KDF (i.e., KDF TLS CVL (Cert. #A6061) and TLS v1.3 KDF (CVL) (Cert. #A6061)) can only be performed in the context of the TLS protocol.

The module does not truncate HMAC outputs or SHA digests.

For KAS ECC, the module conforms to IG D.F Scenario 2 path (2). The key derivation functions comply with NIST SP 800-135r1 (i.e., KDF TLS CVL Cert. #A6061 and TLS v1.3 KDF (CVL) Cert. #A6061). Furthermore, the module obtains the appropriate assurances as required in Section 5.6.2 of NIST SP 800-56Ar3. For KAS-FFC and KAS-ECC, the module uses C(2e,0s), thus no static key pairs are used as a part of the KAS schemes per NIST SP 800-56Ar3. Full public key validations are implemented (NIST SP 800-56Ar3 Section 5.6.2.3.3). No key confirmation is implemented.

The module only supports the use of SHA-1 in the Approved mode of operation for non-digital signature applications as permitted by NIST SP 800-131Ar2. Per CMVP Programmatic Transitions and NIST SP 800-131Ar2, usage of SHA-1 for non-digital-signature applications is deprecated through Dec 31, 2030.

2.8 RBG AND ENTROPY

The module incorporates a NIST SP 800-90A HMAC-DRBG (Cert. #A6062) that is seeded with a 512-bit Entropy Input of strength 448 bits from its entropy source (Entropy Cert. #E63) and a 256-bit DRBG Nonce of strength 224 bits. No entropy is claimed from the DRBG Nonce. The unmodified output of the DRBG is used for generating cryptographic key material or random bit strings.

Cert Number	Vendor Name
E63	ID QUANTIQUE SA

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
IDQ250C3	Physical	IDQ250C3 with MAX32550	2 bits	1.75 bits	None

Table 8: Entropy Sources

2.9 KEY GENERATION

The module generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90A conforming DRBG (Cert. #A6062) for the encryption and protection of data and cryptographic keys. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-4 and FIPS 186-5 for the facilitation of key agreement in conformance with NIST SP 800-56Ar3 and for the generation or verification of digital signatures. RSA KeyGen (FIPS186-5) (Cert. #A6061) complies with IG C.E. Specifically, RSA KeyGen (FIPS186-5) (Cert. #A6061) is conformant to FIPS 186-5.

2.10 KEY ESTABLISHMENT

The module supports the establishment of cryptographic keys using finite field cryptography (FFC) and elliptic curve cryptography (ECC) in conformance with NIST SP 800-56Ar3 and IG D.F - Scenario #2 path 2. The module implements KAS-ECC-SSC per NIST SP 800-56Ar3 (Cert. #A6061), used in conjunction with KDF per NIST SP 800-135r1 (Cert. #A6061). Key establishment methodology provides at least 112 bits of strength. This is used to establish secure communication sessions.

The module incorporates KTS-IFC in conformance with NIST SP 800-56Br2.

2.11 INDUSTRY PROTOCOLS

The module relies upon TLS and serial protocols for communication with general purpose computer (GPC) systems.

3 CRYPTOGRAPHIC MODULE INTERFACES

3.1 PORTS AND INTERFACES

This document may be freely reproduced and distributed, but only in its entirety and without modification.

The module incorporates physical ports and logical interfaces. The physical ports are defined within the table below and comprise two ribbon cables that pass directly into the module.

Physical Port	Logical Interface(s)	Data That Passes
Serial Ribbon Cable (Security Anchor)	Data Input Data Output Control Input Status Output Power	Service inputs, Service outputs
Serial Ribbon Cable (Compute Engine)	Data Input Data Output Status Output	Firmware as inputs during updates, Compute Engine boot status output

Table 9: Ports and Interfaces

4 ROLES, SERVICES, AND AUTHENTICATION

4.1 AUTHENTICATION METHODS

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Token	Authentication for the Crypto Officer role. The Crypto Officer Token is chosen externally by the operator. The Token is set using the service "Set Crypto Officer Token".	SHS	A token is a bitstring of length 256. The probability that a random attempt will succeed or a false acceptance will occur is at most 1/2^256, which is less than 1/1,000,000.	The module requires the operator to wait after each failed attempt, increasing the time exponentially between attempts up to 1 hour. The operator may make up to 6 attempts in the first minute. The probability of success per minute is at most 6/2^256, which is less than 1/100,000.
Password	Authentication for the KMIP Admin User and the KMIP User roles.	SHS	A password is at least 64 bits long. The probability that a random attempt will succeed or a false acceptance will occur is at most 1/2^64, which	The module requires the user to wait after each failed attempt, increasing the time exponentially between attempts up to 1 hour. A user may make up to 6 attempts in the first minute. The probability of success per

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			is less than 1/1,000,000.	minute is at most 6/2^64, which is less than 1/100,000.
ECDSA Signature	Authentication for the Crypto Officer, KMIP Admin User, and KMIP User roles via an ECDSA Signature-based challenge-response protocol.	SigVer	An ECDSA signature used is at least based on P-256 curve. The probability that an attempt will succeed or a false acceptance will occur is at most 1/2^128, which is less than 1/1,000,000.	The module requires the user to wait after each failed attempt, increasing the time exponentially between attempts up to 1 hour. A user may make up to 6 attempts in the first minute. The probability of success per minute is at most 6/2^128, which is less than 1/100,000

Table 10: Authentication Methods

To use authenticated module services, an operator needs to establish an authenticated session using the module service "Start Authenticated Session". Successfully establishing an authenticated session requires identity-based, multi-factor authentication (ID-based MFA). A session can be terminated by a user using the module service End Authenticated Session". Sessions are automatically terminated in case of inactivity of 15 minutes. Maximum session lifetime is 12 hours. Authentication within sessions is done using encrypted Session Tokens. A Crypto Officer or user can have multiple active sessions. The total number of active sessions is limited to 16. The module supports concurrent operators.

Additional Information

- The module only accepts tokens and passwords as input through a TLS-based secure channel.
- The module does not allow any storage of plaintext token or password hints.
- Tokens and passwords are stored as salted SHA2-256 hashes. A salt is 64 bits and is generated via DRBG Cert. #A6062.
- The module automatically zeroizes all sensitive security parameters on tamper.
- A session token becomes invalid in the following cases: after 15 minutes of inactivity, after 12 hours from token creation time, on power-cycle, and on tamper event.

4.2 ROLES

The module implements the following authenticated roles: Crypto Officer (CO), KMIP Admin User, KMIP User. These are the fixed set of roles. Roles cannot be modified.

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO)	MultiFactorIdentity	CO	Token ECDSA Signature
KMIP Admin User	MultiFactorIdentity	User	Password ECDSA Signature
KMIP User	MultiFactorIdentity	User	Password ECDSA Signature
Unauthenticated	Role	N/A	None

Table 11: Roles

Role selection is explicitly based on the service requested. Some module services are available for a single role, for example, "Set Crypto Officer Token". The use of these services assumes the Crypto Officer role. Some module services are available to multiple roles, for example, "Manage MFA". The role is assigned implicitly based on the identity of the operator. To take on a User role, an operator provides a username. To take on the Crypto Officer role, an operator authenticate with the "CO Token."

The module does not permit an operator to change roles. Results of previous authentication attempts are not used for subsequent authentication.

4.3 APPROVED SERVICES

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
End Authenticated Session	Terminate a previously established authenticated session.	Service Completion	Authentication data	N/A	DEC DEC_Auth	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z KMIP Admin User - SA HW AES Key: E - Session Token Encryption Key: E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Session Tokens: W,E,Z KMIP User - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z
Factory Reset	Zeroize all CSPs.	Service Completion	Authentication data	N/A	DEC DEC_Auth	Crypto Officer (CO) - SA HW AES Key: E,Z - Flash Encryption Keys: Z - Session Token Encryption Key: E,Z - CO Token Hash: Z - Device Private Keys: Z - TLS Server Signing Keys: Z - IE Private Key: Z - KMIP IE DEK: Z - DRBG State: Z - KMIP User Password Hashes: Z - KMIP Symmetric Keys: Z - KMIP Private Keys: Z - KMIP Public Keys: Z - TLS Secret

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: Z - TLS Key Material: Z - Device Public Keys: Z - TLS Server Public Keys: Z - IE Public Key: Z - Root CA Public Key: Z - Session Tokens: W,E,Z - DHE Public Key: Z - Witness Register: Z - User Authentication Public Keys: Z
Generate CSR	Generate a Certificate Signing Request (CSR) for one of the following public keys: Device Public Keys and TLS Server Public Keys.	Service Completion	Authentication data, X509 CSR Subject, X509 CSR Extensions	DER encoded X509 CSR	SigGen DRBG ESV ENC DEC DEC_Auth SHS	Crypto Officer (CO) - SA HW AES Key: E - Flash Encryption Keys: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - Device Private Keys: E - Device Public Keys: E,R - TLS Server Signing Keys: E - TLS Server Public Keys: E,R - DRBG State: G,E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed: G,E,Z - Entropy Input: G,E,Z
Generate or Clear Key Pair	Generate a new key pair. The key pair could be any of the following: Device Private and Public Keys, IE Private and Public Keys, TLS Server Signing and Public Keys	Service Completion	Authentication data	Device Public Keys, IE Public Key, TLS Server Public Keys	AKG DEC DEC_Auth DRBG ESV ENC SHS SigGen	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - Flash Encryption Keys: E - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - Device Private Keys: G,E,Z - Device Public Keys: G,R,Z - IE Private Key: G,Z - IE Public Key: G,R,E,Z - TLS Server Signing Keys: G,Z - TLS Server Public Keys: G,R,Z
Get Compute Engine	Get the Compute Engine	Service Completion	N/A	Compute Engine	DEC SHS	Unauthenticated - SA HW AES Key: E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Applications Certificates	Applications Certificates			Applications Certificates		- Flash Encryption Keys: E
Get Module Configuration	Get Module Configuration	Service Completion	N/A	Module configuration	DEC	Unauthenticated - SA HW AES Key: E
Get Public Key or Certificate	Get a Public Key or Certificate. The Public Key and Certificate could be any of the following public keys or certificates: Root of Trust CA, Device Public Keys, TLS Server Public Keys, and IE Public Key.	Service Completion	N/A	Public Key, Certificate	DEC SHS	Unauthenticated - SA HW AES Key: E - Flash Encryption Keys: E - Root CA Public Key: R - TLS Server Public Keys: R - Device Public Keys: R - IE Public Key: R
Get Random	Return the requested number of random bits generated within the Security Anchor.	Service Completion	Number of bits requested	Random bits	DRBG ESV ENC DEC SHS	Unauthenticated - SA HW AES Key: E - DRBG State: G,Z,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z,R
Get Status	Get module status, version information, error information, or	Service Completion	Nonce length, Nonce	Module status, version information, signed	SigGen SHS DEC DRBG ESV	Unauthenticated - SA HW AES Key: E - Device Private

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	signed witness register value			witness register value, CE Applications Certificates		Keys: E - Flash Encryption Keys: E - Witness Register: R,E - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z
Initiate SA Bootloader or Firmware Update	Set module configuration parameters related to Security Anchor bootloader or firmware. Zeroize user keys.	Service Completion	Authentication data, new module configuration	Updated module configuration	ENC DEC DEC_Auth DRBG ESV SHS	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key: E,Z - Flash Encryption Keys: E,Z - IE Private Key: Z - IE Public Key: Z - KMIP IE DEK: Z - KMIP User Password Hashes: Z - KMIP Symmetric Keys: Z - KMIP Private Keys: Z - KMIP Public Keys: Z - TLS Secret Keys: Z - Witness Register: Z - Session

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z
KMIP Set User Password	For a KMIP user to reset their own password	Service Completion	Authentication data, new user password (for password change operations)	N/A	SHS ENC DEC DEC_Auth DRBG ESV	KMIP User - SA HW AES Key: E - Flash Encryption Keys: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - KMIP User Passwords: W,Z,E - KMIP User Password Hashes: G
KMIP State Management	Configure, reset, import, or export KMIP state	Service Completion	Authentication data, KMIP storage configuration options, encrypted KMIP state, system time	KMIP storage configuration options, KMIP storage usage information, encrypted KMIP state, system time	DEC DEC_Auth DRBG ENC ESV KTS-GCM KTS-RSA SigGen SigVer	KMIP Admin User - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - Root CA Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHS SKG	Key: E - Device Private Keys: E - Device Public Keys: E - Flash Encryption Keys: G,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - KMIP IE DEK: G,R,W,Z - KMIP Symmetric Keys: W,R,Z - KMIP Private Keys: W,R,Z - KMIP Public Keys: W,R,Z - KMIP User Password Hashes: W,R,Z - User Authentication Public Keys: W,R,Z - IE Private Key: E - IE Public Key: E - TLS Server Public Keys: E
KMIP User Management	Create KMIP User, Set KMIP User Password Hash, Delete KMIP User	Service Completion	Authentication data, new user password (for password	N/A	SHS ENC KTS-GCM DEC DEC_Auth	KMIP Admin User - SA HW AES Key: E - Flash Encryption Keys:

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			change operations)		DRBG ESV	E - Session Token Encryption Key: E - Session Tokens: W,E,Z - KMIP Symmetric Keys: Z - KMIP Private Keys: Z - KMIP Public Keys: Z - KMIP User Passwords: E,Z,W - KMIP User Password Hashes: E,G,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z
KMIP v1.4 operations	KMIP protocol compatible operations	Service Completion	Authentication data, KMIP Cryptographic objects	KMIP Cryptographic objects	AKG DEC DEC_Auth DRBG ESV ENC ENC_Auth KTS-GCM MAC SHS SigGen SigVer SKG	KMIP User - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - Flash Encryption Keys: E - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input:

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - KMIP Symmetric Keys: R,W,E,G - KMIP Private Keys: R,W,E,G - KMIP Public Keys: R,W,E,G
Manage MFA	Register, List, Delete MFA credentials.	Service Completion	Authentication data, MFA data	MFA data	ENC DEC DEC_Auth DRBG ESV SHS SigVer	Crypto Officer (CO) - SA HW AES Key: E - Flash Encryption Keys: E - CO Token: W,Z,E - CO Token Hash: G,E - Session Token Encryption Key: E - Session Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - User Authentication Public Keys: W,E,Z KMIP Admin User - SA HW AES Key: E - Flash Encryption Keys: E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KMIP User Passwords: W,Z,E - KMIP User Password Hashes: G,E - Session Token Encryption Key: E - Session Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - User Authentication Public Keys: W,E,Z KMIP User - SA HW AES Key: E - Flash Encryption Keys: E - KMIP User Passwords: W,Z,E - KMIP User Password Hashes: G,E - Session Token Encryption Key: E - Session Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Entropy Input: G,E,Z - User Authentication Public Keys: W,E,Z
Power	Power on, power off, or power cycle the module	Service Completion	N/A	N/A	ENC DEC DRBG ESV SKG	Unauthenticated - SA HW AES Key: E - Session Token Encryption Key: G,Z - Session Tokens: Z - DHE Public Key: Z - Witness Register: Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - DRBG Nonce: G,E,Z
Self-Tests	Perform Self-Tests	Service Completion	N/A	N/A	ENC DEC ESV SHS	Unauthenticated - SA HW AES Key: E - Entropy Input: G,E,Z
Set Crypto Officer Token	Set a new CO Token Hash.	Service Completion	Authentication data, New Crypto Officer Token	N/A	SHS ENC KTS-GCM DEC DEC_Auth	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key:

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DRBG ESV	E - Session Tokens: W,E,Z - CO Token: W,Z,E - CO Token Hash: G - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z
Set Module Configuration	Set module configuration parameters. Zeroize user keys.	Service Completion	Authentication data, new module configuration	Updated module configuration	ENC DEC DEC_Auth DRBG ESV SHS	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key: E,Z - Flash Encryption Keys: E,Z - IE Private Key: Z - IE Public Key: Z - KMIP IE DEK: Z - KMIP User Password Hashes: Z - KMIP Symmetric Keys: Z - KMIP Private Keys: Z - KMIP Public Keys: Z - TLS Secret Keys: Z - Witness Register: Z

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Session Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z
Set or Clear Public Key Certificate	Set or clear a Public Key Certificate. The Public Key Certificate could be for any of the following: Device Public Keys, IE Public Key, and TLS Server Public Keys.	Service Completion	Authentication data, Public Key Certificate	N/A	DEC DEC_Auth DRBG ENC ESV SigGen SHS	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - Flash Encryption Keys: E - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - TLS Server Signing Keys: E,Z - TLS Server Public Keys: E,Z - IE Private Key: Z - IE Public Key: E,Z - Root CA Public Key: W - Device Private Keys: E,Z - Device Public Keys: E,Z - KMIP User

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Password Hashes: Z - KMIP Symmetric Keys: Z - KMIP Private Keys: Z - KMIP Public Keys: Z - KMIP IE DEK: Z - TLS Secret Keys: Z
Start Authenticated Session	Start an authenticated session with the Security Anchor. Authenticated services can only be accessed after a session has been established. Session establishment requires identity-based authentication and MFA.	Service Completion	Authentication data, MFA data	Session Token	DRBG ESV ENC DEC ENC_Auth KTS-GCM DEC_Auth SHS SigVer	Crypto Officer (CO) - SA HW AES Key: E - Flash Encryption Keys: E - CO Token: W,Z,E - CO Token Hash: G,E - Session Token Encryption Key: E - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: W,G,E,Z - Session Tokens: G,R,Z - User Authentication Public Keys: E KMIP Admin User - SA HW AES Key: E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Flash Encryption Keys: E - KMIP User Passwords: W,Z,E - KMIP User Password Hashes: G,E - Session Token Encryption Key: E - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - Session Tokens: W,G,R,Z - User Authentication Public Keys: E KMIP User - SA HW AES Key: E - Flash Encryption Keys: E - KMIP User Passwords: W,Z,E - KMIP User Password Hashes: G,E - Session Token Encryption Key: E - DRBG State: G,E - DRBG Seed: G,E,Z

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Entropy Input: G,E,Z - Session Tokens: W,G,R,Z - User Authentication Public Keys: E
TLS	TLS communication. All authenticated services use this service for TLS communication. Use of this service is implicit in said module services.	TLS handshake Completion	N/A	N/A	AKG DEC DEC_Auth DRBG ENC ENC_Auth KTS-GCM ESV KAS SHS SigGen	Unauthenticated - SA HW AES Key: E - Flash Encryption Keys: E - TLS Secret Keys: G,E,Z - TLS Key Material: G,E,Z - DHE Public Key: G,R,E,Z - Client DHE Public Key: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z - TLS Server Signing Keys: G,E - TLS Server Public Keys: G,R,E - Device Public Keys: R - Device Private Keys: E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Transfer Trusted Application	Transfer Trusted Application on the Compute Engine. An application is trusted if it can be verified using the Compute Engine Applications Certificates.	Service Completion	Application, Application Signatures	N/A	SigVer SHS DEC	Unauthenticated - SA HW AES Key: E - Flash Encryption Keys: E
Transfer Trusted SA Bootloader or Firmware	Transfer and verify Security Anchor bootloader or firmware	Service Completion	Authentication data, signed bootloader, or signed firmware	Transfer status	SHS SigVer ENC DEC DEC_Auth	Unauthenticated - SA HW AES Key: E
Update CE Applications Certificates	Set the Compute Engine Applications Certificates	Service Completion	Authentication data, Certificates	N/A	ENC DEC DEC_Auth SHS DRBG ESV	Crypto Officer (CO) - SA HW AES Key: E - Session Token Encryption Key: E - Session Tokens: W,E,Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z
Update CE Firmware	Update Compute	Service Completion	Authentication data	Update status	SHS SigVer ENC DEC	Crypto Officer (CO) - SA HW AES Key: E

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Engine firmware				DEC_Auth	- Session Token Encryption Key: E - Session Tokens: W,E,Z
Witness	Return Witness Data and extend the Witness Register	Service Completion	Data to witness	N/A	SHS	Unauthenticated - Witness Register: G,E,R
Zeroize User Data	Zeroize SSPs related to user data.	Service Completion	Authentication data	N/A	ENC DEC DEC_Auth DRBG ESV	Crypto Officer (CO) - SA HW AES Key: E - Flash Encryption Keys: Z - Session Token Encryption Key: E - Session Tokens: W,E,Z - KMIP IE DEK: Z - KMIP User Password Hashes: Z - KMIP Symmetric Keys: Z - KMIP Private Keys: Z - KMIP Public Keys: Z - DRBG State: G,E - DRBG Seed: G,E,Z - Entropy Input: G,E,Z

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Table 12: Approved Services

4.4 NON-APPROVED SERVICES

N/A for this module.

4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

There is no complete image replacement process. New firmware for the Security Anchor and the Compute Engine may be separately downloaded and loaded. Any firmware/software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

- Security Anchor firmware is signed by Private Machines, with a digital signature based on ECDSA P-256 and SHA2-256, or ECDSA P-384 and SHA2-384, or ECDSA P-521 and SHA2-512 (Cert. #A6061).
- Compute Engine firmware is signed by Private Machines, with a digital signature based on ECDSA P-256 and SHA2-256, or ECDSA P-384 and SHA2-384, or ECDSA P-521 and SHA2-512 (Cert. #A6063).
- Bootloader firmware is signed by Private Machines, with a digital signature based on ECDSA P-256 and SHA2-256, or ECDSA P-384 and SHA2-384, or ECDSA P-521 and SHA2-512 (Cert. #A6061).
- Compute Engine Application is signed by Private Machines, with any of the following (Cert. #A6063):
    - SHA2-256 or SHA2-384 or SHA2-512
    - ECDSA P-256 digital signature with SHA2-256
    - ECDSA P-384 digital signature with SHA2-384
    - ECDSA P-521 digital signature with SHA2-512
    - RSA PKCS 1.5 or PSS digital signature with 2048 or 3072 or 4096-bit modulus and SHA2-256
    - RSA PKCS 1.5 or PSS digital signature with 2048 or 3072 or 4096-bit modulus and SHA2-384
    - RSA PKCS 1.5 or PSS digital signature with 2048 or 3072 or 4096-bit modulus and SHA2-512

On downloading, the device verifies the firmware including the type, version, and hash or signature of the new firmware package. When the firmware is loaded for execution, its hash or signature is verified again.

5 SOFTWARE/FIRMWARE SECURITY

5.1 INTEGRITY TECHNIQUES

The module includes the following four firmware components subjected to separate firmware integrity tests:

- Security Anchor firmware is signed by Private Machines, with a digital signature based on ECDSA P-256 and SHA2-256, or ECDSA P-384 and SHA2-384, or ECDSA P-521 and SHA2-512 (Cert. #A6061).
- Compute Engine firmware is signed by Private Machines, with a digital signature based on ECDSA P-256 and SHA2-256, or ECDSA P-384 and SHA2-384, or ECDSA P-521 and SHA2-512 (Cert. #A6063).
- Bootloader firmware is signed by Private Machines, with a digital signature based on ECDSA P-256 and SHA2-256, or ECDSA P-384 and SHA2-384, or ECDSA P-521 and SHA2-512 (Cert. #A6061).
- Compute Engine Application is signed by Private Machines, with any of the following (Cert. #A6063):
    - SHA2-256 or SHA2-384 or SHA2-512
    - ECDSA P-256 digital signature with SHA2-256

- ECDSA P-384 digital signature with SHA2-384
- ECDSA P-521 digital signature with SHA2-512
- RSA PKCS 1.5 or PSS digital signature with 2048 or 3072 or 4096-bit modulus and SHA2-256
- RSA PKCS 1.5 or PSS digital signature with 2048 or 3072 or 4096-bit modulus and SHA2-384
- RSA PKCS 1.5 or PSS digital signature with 2048 or 3072 or 4096-bit modulus and SHA2-512

The respective firmware integrity private keys are not stored by the module. The respective public keys are not considered SSPs. The pre-calculated hash and digital signature values are included in the loaded firmware.

5.2 INITIATE ON DEMAND

The module's pre-operational firmware integrity tests can be initiated on demand via the "Self-Tests" service or by power-cycling the module.

6 OPERATIONAL ENVIRONMENT

6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module is defined as a multi-chip embedded cryptographic module whose operational environment is classified as limited. The FIPS 140-3 Area 6 Operational Environment requirements are not applicable because the cryptographic module does not contain a modifiable operational environment. The module has the ability to load its firmware and only accepts firmware that successfully passes the firmware load test. Only the firmware versions identified on the module's validation certificate are included in the scope of this validation. Any other firmware loaded onto the module is not validated and would require a separate FIPS 140-3 validation.

7 PHYSICAL SECURITY

All the components within the cryptographic boundary of the device are protected with a strong, non-removable enclosure. The enclosure is opaque within the visible spectrum and provides tamper evidence. The module is inspected for tamper evidence on delivery, installation, servicing, when the module reports an error state, and on a periodic inspection schedule. The module incorporates an active tamper detection and response mechanism.

7.1 MECHANISMS AND ACTIONS REQUIRED

The device includes a tamper detection and response mechanism. CSPs are zeroized automatically on a tamper event being detected.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence	During installation, re-installation, decommissioning, and servicing. Also inspect when the module reports an error state due to tamper and on a periodic inspection schedule.	Inspect device for obvious damage or other evidence of tamper. Use the "Get Status" service.

Table 13: Mechanisms and Actions Required

7.2 EFP/EFT INFORMATION

As part of the module's general alarm mechanism, measures are taken to protect against environmental failures. Alarm triggering temperature and voltage ranges and protection capabilities are described in the table below.

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-37 +/- 7 deg C	EFP	Zeroization
HighTemperature	120 +/- 10 deg C	EFP	Zeroization
LowVoltage	2.2V	EFP	Zeroization
HighVoltage	3.7V	EFP	Zeroization

Table 14: EFP/EFT Information

8 NON-INVASIVE SECURITY

8.1 MITIGATION TECHNIQUES

The module does not provide protection against non-invasive security methods.

9 SENSITIVE SECURITY PARAMETERS MANAGEMENT

9.1 STORAGE AREAS

SSPs are stored in areas defined in the table below.

Storage Area Name	Description	Persistence Type
Key Register	Security Anchor Zeroizable Battery-Backed Key Register. The SA HW AES Key is stored in the Security Anchor battery-backed key register and is zeroized on tamper or Factory Reset service. Zeroizing the SA HW AES Key prevents access to	Static

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Storage Area Name	Description	Persistence Type
	all other CSPs (stored in NVSRAM and Flash). This is because all persistently-stored CSPs are either encrypted directly with the SA HW AES Key or the Flash Encryption Keys, which in turn are encrypted by the SA HW AES Key.	
NVSRAM	Security Anchor Zeroizable Battery-Backed memory. Entire contents of the NVSRAM are encrypted with the SA HW AES Key.	Dynamic
Flash	Security Anchor Flash.	Dynamic
RAM	Security Anchor RAM. Stores data in plaintext.	Dynamic
External	Storage areas external to the module.	Static

Table 15: Storage Areas

9.2 SSP INPUT-OUTPUT METHODS

All SSPs are stored within the Security Anchor. SSPs are stored in the Security Anchor NVSRAM and in the Security Anchor Flash storage.

The root encryption key is the SA HW AES Key. Zeroizing the SA HW AES Key prevents access to all other CSPs (stored in NVSRAM and Flash). This is because all CSPs are encrypted in one of the following ways:

- Directly with the SA HW AES Key.
- With the Flash Encryption Keys which in turn are encrypted by the SA HW AES Key.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
PE-KAS	External	RAM	Plaintext	Automated	Electronic	KAS
PO-KAS	RAM or Flash	External	Plaintext	Automated	Electronic	KAS
PO	RAM or Flash	External	Plaintext	Automated	Electronic	
TLSE	External	Key Register, NVSRAM, Flash, or RAM	Encrypted	Automated	Electronic	KTS-GCM

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TLSO	Key Register, NVSRAM, Flash, or RAM	External	Encrypted	Automated	Electronic	KTS-GCM

Table 16: SSP Input-Output Methods

9.3 SSP ZEROIZATION METHODS

Zeroization Method	Description	Rationale	Operator Initiation
Tamper Response	Physical tamper detection and response. In the case of a tamper event, the SA HW AES Key (which encrypts the NVSRAM) is zeroized, rendering all other persistently-stored CSPs inaccessible. Additionally, the Security Anchor RAM is also zeroized. After zeroization, the module is power cycled, all services are disabled, and the module enters an error state. Zeroization of the Security Anchor Hardware AES Key occurs within nanoseconds. Zeroization of additional memory such as the Security Anchor RAM occurs within 300 µs. This small timeframe prevents compromise of CSPs since CSPs retrieval would involve drilling through the module's two enclosing aluminum enclosures as well as the Security Anchor chip, and finally accessing the Security Anchor memory: all within 300 µs.	Auto-tamper detection and response against physical attacks on the module.	N/A
Factory Reset	Triggered by an operator to zeroize the SA HW AES Key, which renders all other persistently-stored CSPs inaccessible. 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 the factory. Zeroization time is approximately 300 µs.	Provision for an operator to trigger zeroization.	Triggered by an operator using the "Factory Reset" service.
Auto	Temporary CSPs are automatically zeroized when they are no longer needed, e.g., ephemeral keys generated during key agreement.	Temporary CSPs are zeroized when no longer needed.	N/A

Table 17: SSP Zeroization Methods

This document may be freely reproduced and distributed, but only in its entirety and without modification.

9.4 SSPS

The following two tables list Sensitive Security Parameters (SSPs) for the module. Public keys used for firmware integrity tests are not considered SSPs.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CO Token	The token used to authenticate the Crypto Officer role.	256 - 112	Authentication - CSP	External		SHS
CO Token Hash	The hash of the token used to authenticate the Crypto Officer role.	256 - 256	Authentication - CSP	SHS		
Client DHE Public Key	FFDH or ECDH Public Key, i.e., ephemeral public key received during a TLS handshake.	512, 768, 1042, 2048 - 112-256	Public - PSP	External		KAS
DHE Public Key	FFDH or ECDH Public Key, i.e., ephemeral public key generated during a TLS handshake.	512, 768, 1042, 2048 - 112-256	Public - PSP	AKG		KAS
DRBG Nonce	Input string provided to the HMAC DRBG during its initialization.	256 - 224	ENT - CSP	Internally by ESV E63		DRBG
DRBG Seed	The seed provided to the HMAC DRBG during its initialization and reseeding. Composed of the Entropy Input and DRBG Nonce (initialization only).	768 - 672	ENT - CSP	Internally by ESV E63		DRBG

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG State	HMAC DRBG internal working state V and Key.	256 - 256	ENT - CSP	DRBG		DRBG
Device Private Keys	Used by the Security Anchor to sign data. Part of the TLS trust chain.	224, 256, 384, 521, 2048, 3072, 4096 - 112-256	Private - CSP	AKG		SigGen
Device Public Keys	Used by external clients to verify signatures generated by the Device Private Keys.	512, 768, 1042, 2048, 3072, 4096 - 112	Public - PSP	External AKG		SigVer
Entropy Input	Input string provided to the HMAC DRBG during its initialization and reseeding.	512 - 448	ENT - CSP	Internally by ESV E63		DRBG
Flash Encryption Keys	Used to encrypt all SSPs stored in the Security Anchor Flash.	256 - 256	Symmetric - CSP	SKG		ENC DEC
IE Private Key	Used for unwrapping imported KMIP IE DEK.	2048, 3072, 4096 - 112, 128, 140	Private - CSP	AKG		KTS-RSA
IE Public Key	Used by others for wrapping KMIP IE DEK for the module to import.	2048, 3072, 4096 - 112	Public - PSP	AKG		KTS-RSA

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KMIP IE DEK	Used to encrypt and decrypt KMIP Cryptographic Objects during the KMIP Import and Export operations.	256 - 112	Symmetric - CSP	SKG		ENC_Auth DEC_Auth
KMIP Private Keys	KMIP RSA and ECDSA Private Keys.	2048, 3072, 4096, 224, 256, 384, 521 - 112	Private - CSP	AKG External		SigGen
KMIP Public Keys	KMIP RSA and ECDSA Public Keys.	2048, 3072, 4096, 448, 521, 768, 1042 - 112	Public - PSP	AKG External		SigVer
KMIP Symmetric Keys	KMIP Symmetric Keys for encryption and MAC.	128, 192, 256, 112-1024 - 112	Symmetric - CSP	SKG External		ENC DEC MAC ENC_Auth DEC_Auth
KMIP User Passwords	The passwords used to authenticate KMIP Admin User and KMIP User.	64 - NA	Authentication - CSP	External		SHS
KMIP User Password Hashes	The hashes of KMIP User Passwords. Used as one factor for authenticating KMIP Admin User and KMIP User.	256 - 112	Authentication - CSP	SHS		
Root CA Public Key	The public key of the Root of Trust CA,	256, 384, 521, 2048,	Public - PSP	External		SigVer

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	which endorses the Device Public Keys.	3072, 4096 - 112				
SA HW AES Key	Used to encrypt and decrypt the Security Anchor's zeroizable, battery-backed memory (NVSRAM), which stores some CSPs.	256 - 256	Symmetric - CSP	External		ENC DEC
Session Token Encryption Key	Used to encrypt session IDs to generate session tokens.	256 - 256	Symmetric - CSP	SKG		ENC_Auth DEC_Auth
Session Tokens	Used for session-based authentication.	256 - 112	Authentication - CSP	ENC_Auth		DEC_Auth
TLS Key Material	TLS Shared Secret Z.	256, 384, 521, 2048 - 112	Shared Secret - CSP		KAS	KAS
TLS Secret Keys	TLS session keys for the record protocol.	256 - 112	Symmetric - CSP	KAS		ENC_Auth DEC_Auth
TLS Server Public Keys	Used by clients in the TLS trust chain to verify signatures generated by the module.	512, 768, 1042, 2048, 3072, 4096 - 112	Public - PSP	AKG		SigVer
TLS Server Signing Keys	Used by the Security Anchor to sign its public DHE parameters before sending them to a TLS client.	224, 256, 384, 521, 2048, 3072, 4096 - 112-256	Private - CSP	AKG		SigGen

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
User Authentication Public Keys	Used by the module to authenticate users with a challenge signature request.	256, 384, 521 - 112	Public - PSP	External		SigVer
Witness Register	Usage is user-specific.	256, 384, 512 - 128, 192, 256	Authentication - PSP	SHS		SHS

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CO Token	TLSE	RAM:Plaintext	Until no longer needed	Tamper Response Auto	CO Token Hash:Derives
CO Token Hash		NVSRAM:Encrypted RAM:Plaintext	Until no longer needed	Tamper Response Factory Reset	CO Token:Derived From
Client DHE Public Key	PE-KAS	RAM:Plaintext	Until no longer needed	Tamper Response Auto	DHE Public Key:Used With
DHE Public Key	PO-KAS	RAM:Plaintext	Until no longer needed	Tamper Response Factory Reset Auto	Client DHE Public Key:Used With TLS Server Public Keys:Used With TLS Server Signing Keys:Used With
DRBG Nonce		RAM:Plaintext	Until no longer needed	Tamper Response Auto	Entropy Input:Used With DRBG Seed:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Seed		RAM:Plaintext	Until no longer needed	Tamper Response Auto	Entropy Input:Derived From DRBG Nonce:Derived From DRBG State:Derives
DRBG State		NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	DRBG Seed:Derived From
Device Private Keys		NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	Device Public Keys:Paired With
Device Public Keys	PO PO-KAS TLSO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	Device Private Keys:Paired With Root CA Public Key:Used With
Entropy Input	PO	RAM:Plaintext	Until no longer needed	Auto	DRBG Nonce:Used With DRBG Seed:Derives
Flash Encryption Keys		NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	KMIP User Password Hashes:Encrypts KMIP Symmetric Keys:Encrypts KMIP Private Keys:Encrypts KMIP Public Keys:Encrypts Root CA Public Key:Encrypts Device Public Keys:Encrypts TLS Server Public Keys:Encrypts IE Public Key:Encrypts

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					User Authentication Public Keys:Encrypts
IE Private Key		NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	KMIP IE DEK:Decrypts IE Public Key:Paired With
IE Public Key	TLSO PO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	IE Private Key:Paired With KMIP IE DEK:Encrypts
KMIP IE DEK	TLSE TLSO	NVSRAM:Encrypted External:Encrypted	Until no longer needed	Tamper Response Factory Reset	KMIP Symmetric Keys:Encrypts KMIP Private Keys:Encrypts KMIP Public Keys:Encrypts
KMIP Private Keys	TLSE TLSO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	KMIP IE DEK:Encrypted By KMIP Public Keys:Paired With
KMIP Public Keys	TLSE TLSO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	KMIP Private Keys:Paired With KMIP IE DEK:Encrypted By
KMIP Symmetric Keys	TLSE TLSO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	KMIP IE DEK:Encrypted By
KMIP User Passwords	TLSE	RAM:Plaintext	Until no longer needed	Tamper Response Auto	KMIP User Password Hashes:Derives

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KMIP User Password Hashes	TLSE TLSO	Flash:Encrypted RAM:Plaintext	Until no longer needed	Tamper Response Factory Reset	KMIP User Passwords:Derived From
Root CA Public Key	TLSE PO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	Device Public Keys:Used With
SA HW AES Key		Key Register:Plaintext	N/A	Tamper Response Factory Reset	Flash Encryption Keys:Encrypts CO Token Hash:Encrypts Device Private Keys:Encrypts TLS Server Signing Keys:Encrypts IE Private Key:Encrypts KMIP IE DEK:Encrypts Session Token Encryption Key:Encrypts DRBG State:Encrypts TLS Secret Keys:Encrypts TLS Key Material:Encrypts
Session Token Encryption Key		RAM:Plaintext NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	Session Tokens:Derives
Session Tokens	TLSE TLSO	External:Encrypted RAM:Plaintext	Until no longer needed	Tamper Response Factory Reset Auto	Session Token Encryption Key:Derived From
TLS Key Material		NVSRAM:Encrypted	Until no longer needed	Tamper Response	TLS Secret Keys:Derives

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Factory Reset	
TLS Secret Keys		NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	TLS Key Material:Derived From
TLS Server Public Keys	PO PO-KAS TLSO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	TLS Server Signing Keys:Paired With DHE Public Key:Used With
TLS Server Signing Keys		NVSRAM:Encrypted	Until no longer needed	Tamper Response Factory Reset	DHE Public Key:Used With TLS Server Public Keys:Paired With
User Authentication Public Keys	TLSE TLSO	Flash:Encrypted	Until no longer needed	Tamper Response Factory Reset	
Witness Register	PO	RAM:Plaintext	Until no longer needed	Tamper Response Factory Reset	

Table 19: SSP Table 2

10 SELF-TESTS

10.1 PRE-OPERATIONAL SELF-TESTS

The following pre-operational tests are performed upon power-up.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Security Anchor	ECDSA Digital Signature Verification based on P-256 and SHA2-256, P-384	KAT	SW/FW Integrity	Implicit	Performed during module

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity	and SHA2-384, or P-521 and SHA2-512 (#A6061)				power-on and on-demand via "Self-Tests" service
Bootloader Firmware Integrity	ECDSA Digital Signature Verification based on P-256 and SHA2-256, P-384 and SHA2-384, or P-521 and SHA2-512 (#A6061)	KAT	SW/FW Integrity	Implicit	Performed during module power-on and on-demand via "Self-Tests" service
Compute Engine Firmware Integrity	ECDSA Digital Signature Verification based on P-256 and SHA2-256, P-384 and SHA2-384, or P-521 and SHA2-512 (#A6063)	KAT	SW/FW Integrity	Implicit	Performed during module power-on and on-demand via "Self-Tests" service
Compute Engine Application Integrity	SHA2-256, SHA2-384, or SHA2-512 hash function, or ECDSA Digital Signature Verification based on P-256 and SHA2-256, P-384 and SHA2-384, or P-521 and SHA2-512, or RSA PKCS#1 v1.5 or PSS Digital Signature Verification based on 2048, 3072, or 4096-bit modulus and SHA2-256, SHA2-384, or SHA2-512 hash function (#A6063)	KAT	SW/FW Integrity	Implicit	Performed during module power-on and on-demand via "Self-Tests" service

Table 20: Pre-Operational Self-Tests

10.2 CONDITIONAL SELF-TESTS

The following conditional tests are performed upon power-up, on-demand and periodically.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (C1028)	256-bit	KAT	CAST	Implicit	Encrypt and Decrypt KAT	Power-Up, Periodically,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						and On-Demand
AES-GCM (A6061)	128-bit	KAT	CAST	Implicit	Encrypt and Decrypt KAT	Power-Up, Periodically, and On-Demand
DSA PWCT	ffdhe2048	NIST SP 800-56Ar3 Owner Assurance of Pair-wise Consistency	PCT	Implicit	Pair-wise consistency test per NIST SP 800-56Ar3 Section 5.6.2.1.4 option b	Upon Key Generation
ECDSA PWCT	ECDSA P-256, P-384, P-521	Sign/Verify	PCT	Implicit	ECDSA Sign/Verify	Power-Up and Upon Key Generation
ECDSA SigGen (FIPS186-5) (A6061)	P-256 with SHA2-256	KAT	CAST	Implicit	Digital signature generation KAT	Power-Up, Periodically, and On-Demand
ECDSA SigVer (FIPS186-5) (A6061)	P-256 with SHA2-256	KAT	CAST	Implicit	Digital signature verification KAT	Power-Up, Periodically, and On-Demand
ECDSA SigVer (FIPS186-5) (A6063)	P-256 with SHA2-256	KAT	CAST	Implicit	Digital signature verification KAT	Power-Up, Upon Use, and On-Demand
Entropy Source	N/A	APT and RCT	CAST	Implicit	Adaptive Proportion Test and Repetition Count Test	Power-Up, On-Demand, Upon Use

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A6062)	Instantiate, Generate, and Reseed	KAT	CAST	Implicit	Instantiate, Generate, and Reseed KAT	Power-Up, Periodically, and On-Demand
HMAC-SHA2-384 (A6061)	SHA2-384 with 256-bit key and 736-bit input	KAT	CAST	Implicit	HMAC KAT	Power-Up, Periodically, and On-Demand
KAS-ECC-SSC SP800-56Ar3 (A6061)	P-256	KAT	CAST	Implicit	KAS-ECC Shared Secret Computation KAT	Power-Up, Periodically, and On-Demand
KAS-FFC-SSC SP800-56Ar3 (A6061)	ffdhe2048	KAT	CAST	Implicit	KAS-FFC Shared Secret Computation KAT	Power-Up, Periodically, and On-Demand
KDF TLS (A6061)	HMAC-SHA2-384 with 2048-bit key and 560-bit input	KAT	CAST	Implicit	Key Derivation	Power-Up, Periodically, and On-Demand
Public Key Validation	ffdhe2048, P-256	N/A	Critical Function	Implicit	Occurs during KAS upon receipt of the peer's public keys	During Key Agreement
RSA OAEP PWCT	2048, 3072, 4096 with SHA2-256 in MGF	NIST SP 800-56Br2 Owner Assurance of Key-Pair Validity	PCT	Implicit	Pair-wise consistency test per VE10.35.03	Power-Up and Upon Key Generation
RSA SigGen (FIPS186-5) (A6061)	2048 PKCSv1.5 with SHA2-256	KAT	CAST	Implicit	Digital signature generation KAT. Satisfies KTS-IFC unencapsulation self-test	Power-Up, Periodically, and On-Demand

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					requirements per IG D.G.	
RSA SigVer (FIPS186-5) (A6061)	2048 PKCSv1.5 with SHA2-256	KAT	CAST	Implicit	Digital signature verification KAT. Satisfies KTS-IFC encapsulation self-test requirements per IG D.G.	Power-Up, Periodically, and On-Demand
RSA SigVer (FIPS186-5) (A6063)	2048 PKCSv1.5 with SHA2-256	KAT	CAST	Implicit	Digital signature verification KAT.	Power-Up, Upon Use, and On-Demand
SHS (A6061)	N/A	KAT	CAST	Implicit	Hash KAT	Power-Up, Periodically, and On-Demand
SHS (A6063)	N/A	KAT	CAST	Implicit	Hash KAT	Power-Up, Upon Use, and On-Demand
SW/FW Load Test	SHA2-256, SHA2-384, or SHA2-512, or ECDSA P-256 with SHA2-256, P-384 with SHA2-384, or P-521 with SHA2-512, or RSA PKCS#1 v1.5 or PSS 2048, 3072, or 4096 with SHA2-256, SHA2-384, or SHA2-512	KAT	SW/FW Load	Implicit	SW/FW load test occurs during updates of SA Bootloader or firmware, CE firmware, or CE Application	During SW/FW Updates
TLS v1.3 KDF (A6061)	HMAC-SHA2-384 with 256-bit input for extraction and	KAT	CAST	Implicit	Key Derivation	Power-Up, Periodically,

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	284-bit secret along with 80-bit input for expansion					and On-Demand

Table 21: Conditional Self-Tests

10.3 PERIODIC SELF-TEST INFORMATION

The pre-operational and conditional algorithm self-tests are also automatically run on a periodic basis.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Security Anchor Firmware Integrity	KAT	SW/FW Integrity	N/A	N/A
Bootloader Firmware Integrity	KAT	SW/FW Integrity	N/A	N/A
Compute Engine Firmware Integrity	KAT	SW/FW Integrity	N/A	N/A
Compute Engine Application Integrity	KAT	SW/FW Integrity	N/A	N/A

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (C1028)	KAT	CAST	Daily, Power-Up	Automatic
AES-GCM (A6061)	KAT	CAST	Daily, Power-Up	Automatic
DSA PWCT	NIST SP 800-56Ar3 Owner Assurance of Pair-wise Consistency	PCT	Upon Key Generation	Automatic
ECDSA PWCT	Sign/Verify	PCT	Power-Up and Upon Key Generation	Automatic
ECDSA SigGen (FIPS186-5) (A6061)	KAT	CAST	Daily, Power-Up	Automatic

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A6061)	KAT	CAST	Daily, Power-Up	Automatic
ECDSA SigVer (FIPS186-5) (A6063)	KAT	CAST	Power-Up, Upon Use	Automatic
Entropy Source	APT and RCT	CAST	Daily, Power-Up, Upon Use	Automatic
HMAC DRBG (A6062)	KAT	CAST	Daily, Power-Up	Automatic
HMAC-SHA2-384 (A6061)	KAT	CAST	Daily, Power-Up	Automatic
KAS-ECC-SSC SP800-56Ar3 (A6061)	KAT	CAST	Daily, Power-Up	Automatic
KAS-FFC-SSC SP800-56Ar3 (A6061)	KAT	CAST	Daily, Power-Up	Automatic
KDF TLS (A6061)	KAT	CAST	Daily, Power-Up	Automatic
Public Key Validation	N/A	Critical Function	N/A	N/A
RSA OAEP PWCT	NIST SP 800-56Br2 Owner Assurance of Key-Pair Validity	PCT	Power-Up and Upon Key Generation	Automatic
RSA SigGen (FIPS186-5) (A6061)	KAT	CAST	Daily, Power-Up	Automatic
RSA SigVer (FIPS186-5) (A6061)	KAT	CAST	Daily, Power-Up	Automatic
RSA SigVer (FIPS186-5) (A6063)	KAT	CAST	Power-Up, Upon Use	Automatic
SHS (A6061)	KAT	CAST	Daily, Power-Up	Automatic

This document may be freely reproduced and distributed, but only in its entirety and without modification.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHS (A6063)	KAT	CAST	Power-Up, Upon Use	Automatic
SW/FW Load Test	KAT	SW/FW Load	Upon Use	Automatic
TLS v1.3 KDF (A6061)	KAT	CAST	Daily, Power-Up	Automatic

Table 23: Conditional Periodic Information

10.4 ERROR STATES

Upon entering an error state, the module stores an error indication that can be retrieved when "Get Status" service is invoked. The error indication includes the error states to which the module has entered.

In an error state, all services except for the following are disabled: "Power", "Get Status", and "Factory Reset". Additionally, in an error state, all data outputs are inhibited.

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	Either the Security Anchor or the Compute Engine or both are unable to perform any action or services.	Security Anchor firmware integrity test failure Compute Engine firmware integrity test failure Self-test failure	Power-cycle the module and all self-tests must pass	"Get Status" service indicates that the module has encountered a failure.
Hard Error	Tamper event		No recovery. The module must be returned to Private Machines Inc.	The module no longer responds to commands.

Table 24: Error States

10.5 OPERATOR INITIATION OF SELF-TESTS

Self-tests may be triggered by the user using the "Self-Tests" service or by power-cycling the module, which allows all tests to be run.

This document may be freely reproduced and distributed, but only in its entirety and without modification.

11 LIFE-CYCLE ASSURANCE

11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

As each module is shipped to the customer, a "CO Token" that is unique to each module along with a Device Public Key are communicated to the Crypto Officer via a separate secure channel which may include any of the following: secure phone call, secure email, or in-person delivery.

Upon receiving the module, the Crypto Officer is to perform a physical inspection to ensure that the module has not been tampered with.

Before using the module,

1. Connect the physical ports.
2. Power on the module using the "Power" service.
3. Use the "Get Status" service to ensure that the module is not in an error state.
4. Use the "Get Public Key or Certificate" service to retrieve and verify the correctness of the Device Public Key Certificate.

If the module is not in an error state and if the certificate is valid, proceed with use. It is recommended that the initial "CO Token" is changed on first use.

11.2 ADMINISTRATOR GUIDANCE

To use the module's KMIP services,

1. Initialize the KMIP storage within the Security Anchor using the "KMIP State Management" Service.
2. Set a password and MFA credentials for the KMIP Admin User using the "KMIP Set User Password" and the "Manage MFA" services.
3. Create additional KMIP users using the services of "KMIP User Management" service.

11.3 NON-ADMINISTRATOR GUIDANCE

To use the module's KMIP services as a KMIP user other than the KMIP Admin User, set a user password and MFA credentials for the user via the "KMIP User Management" and the "Manage MFA" services.

11.4 DESIGN AND RULES

The following security rules are enforced by the cryptographic module to ensure that the FIPS 140-3 security requirements are met.

1. The module supports only the approved mode of operation.
2. The module uses multi-factor, identity-based authentication for roles that access approved algorithms and CSPs.
3. The module does not retain the authentication of an operator following power-off or reboot.
4. The module supports the following roles: Cryptographic Officer (CO), KMIP Admin User, and KMIP User.
5. The module does not permit the output of plaintext CSPs.
6. The module does not support a bypass mode or maintenance mode.

This document may be freely reproduced and distributed, but only in its entirety and without modification.

7. The module supports the following logically distinct interfaces:
   a. Data input interface
   b. Data output interface
   c. Control input interface
   d. Status output interface
   e. Power interface.
8. The module protects CSPs from unauthorized disclosure, modification and substitution.
9. The module protects PSPs from unauthorized modification and substitution.
10. The zeroization excludes the overwriting of an unprotected SSP with another unprotected SSP.
11. The module performs power-on, on-demand and periodic self-testing.
12. The module stores an error indication whenever an error state is entered. The error indication can be retrieved using the "Get Status" service.
13. The module does not perform any cryptographic functions while in an error state.
14. Data output is inhibited during Zeroization, SSP Generation, and Firmware Loading.

11.5 END OF LIFE

To prepare the module for disposal, first, zeroize the module using the "Factory Reset" service. Then, remove the external battery and take the module to an electronic recycling facility or return it to the manufacturer.

12 MITIGATION OF OTHER ATTACKS

12.1 ATTACK LIST

N/A for the module.

12.2 MITIGATION EFFECTIVENESS

N/A for the module.

13 REFERENCES

1. ENFORCER Online Product Documentation: https://content.privatemachines.com/.