**Google, LLC**

# Google HSM

## FIPS 140-3 Non-Proprietary Security Policy

# Table of Contents

# List of Tables



# List of Figures

# 1 General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Google HSM Module. It contains a specification of the rules under which the module must operate and describes how this module meets the requirements as specified in FIPS 140-3 (Federal Information Processing Standards Publication 140-3) for a Security Level 3 Hardware cryptographic module. This security policy is for the validation of the Google HSM Cryptographic Module.

In this document, the terms “Google HSM Cryptographic Module”, “cryptographic module” or “module” are used interchangeably to refer to the Google HSM Cryptographic Module with Firmware version 0.1.0 and Hardware version H1D3P.

## 1.2 Security Levels

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

Table 1: Security Levels

# 2 Cryptographic Module Specification

## 2.1 Description

**Purpose and Use:**

This module is a single chip hardware cryptographic module with 0.1.0 firmware. The module’s operational environment is limited.

An embedded chip designed to securely manage and protect cryptographic keys and perform cryptographic operations.

**Module Type**: Hardware

**Module Embodiment**: Single Chip

**Cryptographic Boundary:**

The cryptographic boundary is defined as the entire single-chip physical boundary.

**Tested Operational Environment's Physical Perimeter (TOEPP):**

The module's Tested Operational Environment's Physical Perimeter (TOEPP) is depicted in Figure 1 & 2 below. The physical Cryptographic boundary is the surface, edges, and pin connections of the chip.


Figure 1: H1D3P Chip (Top)

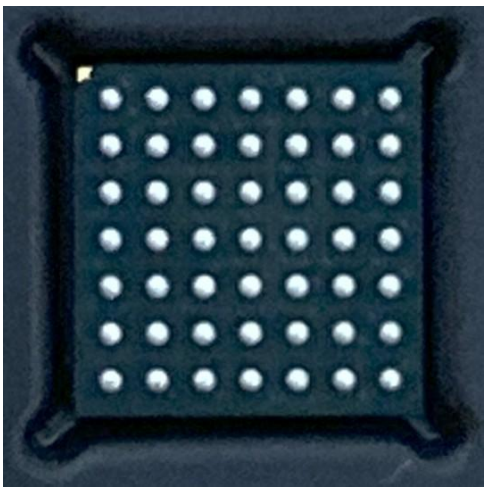

Figure 2: H1D3P Chip (Bottom)

## 2.2 Tested and Vendor Affirmed Module Version and Identification

**Tested Module Identification – Hardware:**

| Model and/or Part Number | Hardware Version | Firmware Version | Processors | Features |
|---|---|---|---|---|
| H1D3P | H1D3P | 0.1.0 | On-chip RISC-V processor | |

Table 2: Tested Module Identification – Hardware

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

N/A for this module.

**Tested Module Identification – Hybrid Disjoint Hardware:**

N/A for this module.

**Tested Operational Environments - Software, Firmware, Hybrid:**

N/A for this module.

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

N/A for this module.

## 2.3 Excluded Components

N/A for this module.

## 2.4 Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved Mode of Operation | The module is always in the approved mode of operation. | Approved | FIPS-compliant mode: true |

Table 3: Modes List and Description

The module has one approved mode of operation and is in the approved mode of operation by default. No configuration is required for the module to operate in the approved mode of operation. The module does not claim implementation of a degraded or non-Approved mode of operation.

## 2.5 Algorithms

**Approved Algorithms:**

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-GCM | A6546 | Direction - Decrypt, Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.1, 8.2.2<br>Key Length - 256 | SP 800-38D |
| ECDSA KeyGen (FIPS186-5) | A6546 | Curve - P-256<br>Secret Generation Mode - testing candidates | FIPS 186-5 |
| ECDSA SigGen (FIPS186-5) | A6546 | Curve - P-256<br>Hash Algorithm - SHA2-256 | FIPS 186-5 |
| ECDSA SigVer (FIPS186-5) | A6546 | Curve - P-256<br>Hash Algorithm - SHA2-256 | FIPS 186-5 |
| HMAC DRBG | A6546 | Prediction Resistance - No<br>Mode - SHA2-256 | SP 800-90A Rev. 1 |
| HMAC-SHA2-256 | A6546 | Key Length - Key Length: 8-512 Increment 8 | FIPS 198-1 |
| KAS-ECC-SSC Sp800-56Ar3 | A6546 | Domain Parameter Generation Methods - P-256<br>Scheme -<br>ephemeralUnified -<br>KAS Role - responder | SP 800-56A Rev. 3 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| KDF SP800-108 | A6546 | KDF Mode - Feedback Supported Lengths - Supported Lengths: 256 | SP 800-108 Rev. 1 |
| SHA2-256 | A6546 | Message Length - Message Length: 0-65528 Increment 8 | FIPS 180-4 |

Table 4: Approved Algorithms

**Vendor-Affirmed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG - Asymmetric | Key Type:Asymmetric | N/A | NIST SP 800-133r2 Section 4 and Section 5.1 - The unmodified output of the DRBG is used for generation of asymmetric keys. |
| CKG - Symmetric | Key Type:Symmetric | N/A | NIST SP 800-133r2 Section 4 and Section 6.1 - The unmodified output of the DRBG is used for generation of symmetric keys. |

Table 5: Vendor-Affirmed Algorithms

The module supports the following vendor affirmed algorithms in accordance with IG D.H (refer to Table 5).

**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 |
|---|---|---|---|---|
| KAS-ECC | CKG KAS-Full | Key Agreement Scheme per SP800-56Arev3 with key derivation function per SP800-108. The module's KAS | Caveat:Key establishment methodology provides 128 bits of security strength IG:IG D.F Scenario 3 | KAS-ECC-SSC Sp800-56Ar3: (A6546) KDF SP800-108: (A6546) HMAC DRBG: (A6546) CKG - |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | (ECC) implementation is FIPS 140-3 IG D.F Scenario 3 compliant. | Key Derivation:SP 800-108 | Asymmetric: () Key Type: Asymmetric |
| KTS (Secure Channel) | KTS-Unwrap KTS-Wrap | KTS via Secure Channel by using AES-GCM | Caveat:Key establishment methodology provides 128 bits of security strength Standard:SP 800-38F IG D.G:method: use of any approved authenticated symmetric encryption mode | AES-GCM: (A6546) Key Length: 256 bits |
| Secure Channel Keying Materials Development | KBKDF | Secure Channel session keying materials, used to derive Secure Channel session keys. | | KDF SP800-108: (A6546) |
| Secure Channel Privacy | BC-Auth | Secure Channel protection. | | AES-GCM: (A6546) Key Length: 256 bits |
| DRBG Function | DRBG | Used for DRBG generation | | HMAC DRBG: (A6546) HMAC-SHA2-256: (A6546) |
| ECDSA KeyGen | AsymKeyPair-KeyGen CKG | ECDSA KeyGen | | ECDSA KeyGen (FIPS186-5): (A6546) HMAC DRBG: (A6546) CKG - Asymmetric: () Key Type: Asymmetric |
| ECDSA SigGen | DigSig-SigGen | ECDSA SigGen | | ECDSA SigGen (FIPS186-5): (A6546) |
| ECDSA SigVer | DigSig-SigVer | ECDSA SigVer | | ECDSA SigVer (FIPS186-5): (A6546) |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| Firmware Load Test | DigSig-SigVer | ECDSA SigVer and SHA2-256 for Firmware Load Test | | ECDSA SigVer (FIPS186-5): (A6546) SHA2-256: (A6546) |
| Block Cipher Encrypt/Decrypt | BC-Auth | Block Cipher Encrypt/Decrypt | | AES-GCM: (A6546) Key Length: 256 bits |

Table 6: Security Function Implementations

## 2.7 Algorithm Specific Information

- AES GCM is used by the secure tunnel, in accordance with Implementation Guidance C.H. scenario #3. The 96-bit IV is comprised of a 64-bit “fixed field” derived from the characteristics of the secure tunnel to be established, concatenated with a 32-bit non-deterministic non-repetitive counter “invocation field”.
- AES GCM is used by the *Symmetric Encrypt* & *Symmetric Decrypt* services, in accordance with the Implementation Guidance C.H scenario #2. The 96-bit IV is generated randomly from an Approved DRBG within the Modules cryptographic boundary.
- In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation as per section 5 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A DRBG.

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|---|---|
| E149 | Google, LLC |

Table 7: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Titan-D TRNG Entropy Source | Physical | H1D3P | 256 | Full Entropy | A1863 (SHA2-256) |

Table 8: Entropy Sources

The module employs a Deterministic Random Bit Generator (DRBG) implementation based on SP800-90Arev1. This DRBG is used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

The DRBG implemented is an SHA2-256 HMAC DRBG, seeded by the entropy source described in the table above. The HMAC DRBG does not employ prediction resistance.

The DRBG is instantiated with a 256-bits long entropy input (corresponding to 256 bits of entropy). Additionally, the DRBG is reseeded with a 256-bits long entropy input (corresponding to 256 bits of entropy).

## 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. #A6546) for the encryption and protection of data and cryptographic keys. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-5 for the verification of digital signatures, or for the facilitation of key agreement in conformance with NIST SP 800-56ar3.

## 2.10 Key Establishment

The module provides the following key/SSP establishment service in the approved mode of operation:

**KAS-ECC:**

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides 128 bits of encryption strength.

## 2.11 Industry Protocols

N/A for this module.

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| VDDIOM, VDDIOA, VDDIOB, VSS | Power | Power input |
| USBN, USBP | Data Input | Data input into the module for all the services defined in Tables 8-11 |
| USBN, USBP | Data Output | Data output from the module for all the services defined in Tables 8-11 |
| USBN, USBP | Control Input | Control data input into the module for all the services defined in Tables 8-11 |
| USBN, USBP | Status Output | Status Information output from the module |

Table 9: Ports and Interfaces

The module provides physical interfaces for power and USB which are mapped to logical interfaces provided by the module (power, data input, data output, control input, and status output) as above.

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| ECDSA-Based Certificate | Identity-based. Allows the Crypto Officer and User to authenticate to the module. | ECDSA SigVer | 128-bits | The modules support ECDSA public-key based authentication mechanism using curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most ~1,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 1,000 * 60 = 60,000/(2^128), which is less than 1/100,000. |

Table 10: Authentication Methods

The module supports identity-based authentication.

## 4.2 Roles

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| Crypto Officer (CO) | Identity | Crypto Officer | ECDSA-Based Certificate |
| User | Identity | User | ECDSA-Based Certificate |

Table 11: Roles

## 4.3 Approved Services

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Show Status | Provide Module's current status | Method: HsmInfo | RPC Call: HsmInfoRequest | RPC Response: HsmInfoResponse | None | Crypto Officer (CO)<br>User |
| Show Version | Provide Module's name and version information | Method: HsmInfo | RPC Call: HsmInfoRequest | RPC Response: HsmInfoResponse | None | Crypto Officer (CO)<br>User |
| Perform Self-Tests | perform Self-Tests (Pre-Operational self-tests and Conditional Self-Tests) | Method: SelfTest | RPC Call: SelfTestRequest | RPC Response: SelfTestRequest | None | Crypto Officer (CO)<br>User |
| Perform Zeroization | Perform Zeroization | Method: Zeroize | RPC Call: ZeroizeRequest | RPC Response: ZeroizeResponse | None | Crypto Officer (CO)<br>- Group Wrapping Key: Z<br>- Group Private Key: Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - Group Public Key: Z<br>- VHSM wrapping key: Z<br>- VHSM Private Key: Z<br>- VHSM Public Key: Z<br>- HSM keypair/ self-signed certificate: Z<br>- Crypto Officer CA certificate: Z<br>- Crypto Officer user certificate: Z<br>- User CA certificate: Z<br>- User certifica |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | te: Z<br>- User crypto key: Z<br>- Secure Channel ECDH Private Key: Z<br>- Secure Channel ECDH Public Key: Z<br>- Peer Secure Channel ECDH Public Key: Z<br>- Secure Channel Shared Secret: Z<br>- Secure Channel HSM to Client |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Encryption Key: Z<br>- Secure Channel Client to HSM Encryption Key: Z<br>- DRBG Entropy Input: Z<br>- DRBG Seed: Z<br>- DRBG Internal State V value: Z<br>- DRBG Key: Z |
| Firmware Load Test | Execute the Firmware Load Test | Method: UpdateChunk | RPC Call: UpdateChunkRequest | RPC Response: UpdateChunkResponse | Firmware Load Test | Crypto Officer (CO)<br>- Firmware Load Test Key: E |
| Assign Owner | Assign owner of HSM | Method: AssignOwner | RPC Call: AssignOwnerStartRequest, AssignOwnerEndRequest | RPC Response: AssignOwnerStartResponse, AssignOwnerEndResponse | None | Crypto Officer (CO) |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Create Group | Create a new group and associate the HSM with this group | Method: CreateGroup | RPC Call: CreateGroupRequest | RPC Response: CreateGroupResponse | DRBG Function ECDSA KeyGen | Crypto Officer (CO)<br>- Group Wrapping Key: G,E<br>- Group Private Key: G,E<br>- Group Public Key: G,E<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E |
| Exit Group | Remove the group data associate | Method: ExitGroup | RPC call ExitGroupRequest | RPC response ExitGroupResponse | None | Crypto Officer (CO)<br>- Group |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | d with the HSM specified group | | | | | Wrapping Key: Z<br>- Group Private Key: Z<br>- Group Public Key: Z |
| Clone Group to Destination | Clone group data associated with HSM to destination | Method: DestinationCloneGroup | RPC call DestinationCloneGroupStartRequest, DestinationCloneGroupEndRequest | RPC response DestinationCloneGroupStartResponse, DestinationCloneGroupEndResponse | DRBG Function<br>Block Cipher Encrypt/Decrypt | Crypto Officer (CO)<br>- Group Wrapping Key: W,E<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E |
| Clone Group | Clone group data | Method: SourceCloneGroup | RPC call SourceCloneGroupStartRequest, | RPC response SourceCloneGroupStartResponse, | Block Cipher | Crypto Officer (CO) |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| from Source | associated with HSM from source | | SourceCloneGroupEndRequest | SourceCloneGroupEndResponse | Encrypt/Decrypt | - Group Wrapping Key: R,E |
| Create VHSM | Create a VHSM to be part of a group associated with the HSM | Method: CreateHsm | RPC call CreateHsmRequest | RPC response CreateHsmResponse | DRBG Function ECDSA KeyGen | Crypto Officer (CO)<br>- VHSM wrapping key: G<br>- VHSM Private Key: G<br>- VHSM Public Key: G<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Park VHSM | Wraps VHSM context and exports it outside of HSM | Method: ParkHsm | RPC call ParkHsmRequest | RPC response ParkHsmResponse | DRBG Function<br>ECDSA SigGen<br>Block Cipher Encrypt/Decrypt | Crypto Officer (CO)<br>- VHSM wrapping key: R,E<br>- VHSM Private Key: R,E<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E |
| Unpark VHSM | Unwraps VHSM and imports into HSMs volatile memory | Method: UnparkHsm | RPC call UnparkHsmRequest | RPC response UnparkHsmResponse | DRBG Function<br>ECDSA SigVer<br>Block Cipher Encrypt/Decrypt | Crypto Officer (CO)<br>- VHSM wrapping key: W,E<br>- VHSM |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Public Key: W,E<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E |
| Generate Symmetric Key | Generate AES256-GCM key for User of VHSM | Method: GenerateKey | RPC call GenerateKeyRequest | RPC response GenerateKeyResponse | DRBG Function | User<br>- User crypto key: G<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - DRBG Key: G,E |
| Symmetric Encrypt | Encrypt data with User generated key on VHSM with AES256-GCM | Method: SymmetricEncrypt | RPC call SymmetricEncryptRequest | RPC response SymmetricEncryptResponse | DRBG Function Block Cipher Encrypt/Decrypt | User - User crypto key: E - DRBG Entropy Input: G,E - DRBG Seed: G,E - DRBG Internal State V value: G,E - DRBG Key: G,E |
| Symmetric Decrypt | Decrypt data with User generated key on VHSM with AES256-GCM | Method: SymmetricDecrypt | RPC call SymmetricDecryptRequest | RPC response SymmetricDecryptResponse | DRBG Function Block Cipher Encrypt/Decrypt | User - User crypto key: E - DRBG Entropy Input: G,E - DRBG Seed: G,E - DRBG |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Internal State V value: G,E<br>- DRBG Key: G,E |
| Run Secure Channel | Execute the Secure Channel Protocol to mutually authenticate Client and HSM to use HSM approved services. | Any time Client make RPC to HSM | RPC request to HSM | RPC response from HSM | KAS-ECC KTS (Secure Channel)<br>Secure Channel Keying Materials Development<br>Secure Channel Privacy<br>DRBG<br>Function<br>ECDSA SigGen<br>ECDSA SigVer | Crypto Officer (CO)<br>- HSM keypair/ self-signed certificate: R<br>- Crypto Officer CA certificate: E<br>- Crypto Officer user certificate: W<br>- Secure Channel ECDH Private Key: G,E<br>- |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Secure Channel ECDH Public Key: G,R<br>- Peer Secure Channel ECDH Public Key: W,E<br>- Secure Channel Shared Secret: G,E<br>- Secure Channel HSM to Client Encryption Key: G,E<br>- Secure Channel Client to HSM Encrypti |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | on Key: G,E<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E<br>User<br>- HSM keypair/ self-signed certificate: R<br>- User CA certificate: E<br>- User certificate: W<br>- Secure Channe |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | l ECDH Private Key: G,E<br>- Secure Channel ECDH Public Key: G,R<br>- Peer Secure Channel ECDH Public Key: W,E<br>- Secure Channel Shared Secret: G,E<br>- Secure Channel HSM to Client Encryption Key: G,E<br>- |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Secure Channel Client to HSM Encryption Key: G,E<br>- DRBG Entropy Input: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State V value: G,E<br>- DRBG Key: G,E |

Table 12: Approved Services

## 4.4 Non-Approved Services

N/A for this module.

## 4.5 External Software/Firmware Loaded

The module also supports the firmware load test by using ECDSA P-256 with SHA2-256 (Cert. #A6546) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module in the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails

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

## 4.6 Additional Information

The module does not support concurrent operators.

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

To ensure firmware security, the module is protected by a proprietary 32-bit Error Detection Code (EDC). The EDC is embedded into the firmware image, and is validated before the module can become operational. If the integrity test fails, the module will enter into an Error state with all crypto functionality inhibited until the integrity test passes.

## 5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the tested platform to initiate the firmware integrity test on-demand.

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

**Type of Operational Environment**: Limited

The module operates within a limited operational environment. The module contains a locked down OS and the module only allows authentic firmware to be loaded. See section 4.5 for firmware loading.

# 7 Physical Security

## 7.1 Mechanisms and Actions Required

The device includes a production-grade tamper-evident coating which encompasses the entire module. The hard opaque tamper-evident coating protects the module from physical tampering and inspection from unauthorized operators within the tested operational ranges listed below.

| Mechanism | Inspection Frequency | Inspection Guidance |
|---|---|---|
| Tamper-evident coating on chip | 12 months | Inspect the module for any dents, scratches or marks. |

Table 13: Mechanisms and Actions Required

## 7.2 EFP/EFT Information

The Google HSM is equipped with temperature, overvoltage, and undervoltage sensors. The firmware enables these sensors at boot to handle out-of-range measurements.

If the measured temperature or voltage is outside that range, the module enters the error state.

When the firmware handles a temperature or voltage out-of-range error, it writes the appropriate error code to the FIPS Error Log and then immediately reboots.

| Temp/Voltage Type | Temperature or Voltage | EFP or EFT | Result |
|---|---|---|---|
| LowTemperature | 0 C | EFP | Shutdown |
| HighTemperature | 80 C | EFP | Shutdown |
| LowVoltage | 2.97 V | EFP | Shutdown |
| HighVoltage | 3.63 V | EFP | Shutdown |

Table 14: EFP/EFT Information

## 7.3 Hardness Testing Temperature Ranges

| Temperature Type | Temperature |
|---|---|
| LowTemperature | 0 C |
| HighTemperature | 80 C |

Table 15: Hardness Testing Temperatures

## 7.4 Additional Information

The module is a single-chip embodiment that meets the commercial-grade specifications for power, temperature, reliability and shock/vibration. The standard design of the module provides protections from probing and direct visual observation of the circuit detail in the visible spectrum, and well as passivation. The module is coated with a hard tamper evident coating.

# 8 Non-Invasive Security

N/A for this module.

# 9 Sensitive Security Parameters Management

## 9.1 Storage Areas

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| RAM | Random Access Memory | Dynamic |
| Flash | Non-Volatile Memory | Static |

Table 16: Storage Areas

## 9.2 SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| Peer Public Key Input | External (Outside of the Module's Boundary) | RAM | Plaintext | Automated | Electronic | |
| Module Public Key Output | RAM | External (Outside of the Module's Boundary) | Plaintext | Automated | Electronic | |
| Secure Channel Input | External (Outside of the Module's Boundary) | Flash | Encrypted | Automated | Electronic | KTS (Secure Channel) |
| Secure Channel Output | Flash | External (Outside of the Module's Boundary) | Encrypted | Automated | Electronic | KTS (Secure Channel) |

Table 17: SSP Input-Output Methods

## 9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Zeroization RPC | Overwrites SSPs with zeros | The zeroization RPC will zeroize all SSPs stored in the RAM or Flash of the module. | RPC call, service: ManagementService, method: Zeroize, req: ZeroizeRequest |

Table 18: SSP Zeroization Methods

Please note that the Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

## 9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| DRBG Entropy Input | Used to seed the DRBG | 256-bits - 256-bits | Entropy Input - CSP | | | DRBG Function |
| DRBG Seed | Used in DRBG Generation | 256-bits - 256-bits | DRBG Seed - CSP | | | DRBG Function |
| DRBG Internal State V value | Used in DRBG Generation | 256-bits - 256-bits | DRBG Internal State V value - CSP | | | DRBG Function |
| DRBG Key | Used in DRBG Generation | 256-bits - 256-bits | DRBG Key - CSP | | | DRBG Function |
| Group Wrapping Key | Wraps all secrets accessible to every HSM in a particular group - most importantly, the exported VHSMs (and VHSM wrapping keys) belonging to the group. | 256-bits - 256-bits | Symmetric Key - CSP | DRBG Function | | Block Cipher Encrypt/Decrypt |
| Group Private Key | Signs VHSMs belonging to a group. | 256-bits - Curve: P-256 | Asymmetric: Private Key - CSP | ECDSA KeyGen | | ECDSA SigGen |
| Group Public Key | Authenticates signed VHSMs belonging to a group. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | ECDSA KeyGen | ECDSA SigVer |
| VHSM wrapping key | Wraps all exported keys belonging to a particular VHSM. | 256-bits - 256-bits | Symmetric key - CSP | DRBG Function | | Block Cipher Encrypt/Decrypt |
| VHSM Private Key | Signs User Crypto Keys belonging to the VHSM. | 256-bits - Curve: P-256 | Asymmetric: Private Key - CSP | ECDSA KeyGen | | ECDSA SigGen |
| VHSM Public Key | Authenticates signed crypto keys belonging to the VHSM. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | ECDSA KeyGen | ECDSA SigVer |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| HSM keypair/ self-signed certificate | Authenticates the HSM side of the secure channel connections. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | ECDSA KeyGen | | ECDSA SigGen |
| Crypto Officer CA certificate | Crypto Officer CA certificate uploaded to the HSM and authenticates Crypto Officer certificates signed by the external private key. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | | ECDSA SigGen |
| Crypto Officer user certificate | Used by Crypto Officer to authenticate to the HSM. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | | ECDSA SigVer |
| User CA certificate | User CA certificate uploaded to the HSM and authenticates User certificates signed by the external private key. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | | ECDSA SigGen |
| User certificate | Used by User to authenticate to the HSM. | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | | ECDSA SigVer |
| User crypto key | AES256-GCM key created and managed by the HSM. | 256-bits - 256-bits | Symmetric Key - CSP | DRBG Function | | Block Cipher Encrypt/Decrypt |
| Firmware Load Test Key | Used for Firmware Load Test | 256-bits - Curve: P-256 | Asymmetric: Public Key - CSP | | | Firmware Load Test |
| Secure Channel ECDH Private Key | Used to derive Secure Channel Shared Secret | 256-bits - Curve: P-256 | Asymmetric: Private Key - CSP | KAS-ECC | | KAS-ECC |
| Secure Channel ECDH Public Key | Used to derive Secure Channel Shared Secret | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | KAS-ECC | |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Peer Secure Channel ECDH Public Key | Used to derive Secure Channel Shared Secret | 256-bits - Curve: P-256 | Asymmetric: Public Key - PSP | | | KAS-ECC |
| Secure Channel Shared Secret | Used to derive Secure channel Encryption Keys | 256-bits - Curve: P-256 | Shared Secret - CSP | | KAS-ECC | Secure Channel Keying Materials Development |
| Secure Channel HSM to Client Encryption Key | Used to protect Secure Channel HSM to Client Session | 256-bits - 256-bits | Symmetric Key - CSP | | Secure Channel Keying Materials Development | Secure Channel Privacy |
| Secure Channel Client to HSM Encryption Key | Used to protect Secure Channel Client to HSM Session | 256-bits - 256-bits | Symmetric Key - CSP | | Secure Channel Privacy | Secure Channel Privacy |

Table 19: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| DRBG Entropy Input | | RAM:Plaintext | Immediately after use | Zeroization RPC | DRBG Seed:Used With<br>DRBG Internal State V value:Used With<br>DRBG Key:Used With |
| DRBG Seed | | RAM:Plaintext | Immediately after use | Zeroization RPC | DRBG Entropy Input:Used With<br>DRBG Internal State V value:Used With<br>DRBG Key:Used With |
| DRBG Internal State V value | | RAM:Plaintext | Zeroization, or on reboot | Zeroization RPC | DRBG Entropy Input:Used With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | | | | | DRBG Seed:Used With<br>DRBG Key:Used With |
| DRBG Key | | RAM:Plaintext | Zeroization, or on reboot | Zeroization RPC | DRBG Entropy Input:Used With<br>DRBG Seed:Used With<br>DRBG Internal State V value:Used With |
| Group Wrapping Key | | Flash:Plaintext | Erased from flash when an HSM leaves a group or is zeroized. | Zeroization RPC | VHSM wrapping key:Encrypts |
| Group Private Key | Secure Channel Output | Flash:Plaintext | Erased from flash when an HSM leaves a group or is zeroized. | Zeroization RPC | Group Public Key:Paired With<br>VHSM Private Key:Signs<br>VHSM Public Key:Signs |
| Group Public Key | Secure Channel Output | Flash:Plaintext | Erased from flash when an HSM leaves a group or is zeroized. | Zeroization RPC | Group Private Key:Paired With |
| VHSM wrapping key | Secure Channel Output | Flash:Plaintext | Erased from flash when all HSMs which own the VHSM leaves the group or have been zeroized. | Zeroization RPC | User crypto key:Encrypts |
| VHSM Private Key | Secure Channel Output | RAM:Plaintext | Erased from flash when all HSMs which own the VHSM leaves the group or have been zeroized. | Zeroization RPC | VHSM Public Key:Paired With<br>User crypto key:Signs |
| VHSM Public Key | Secure Channel Output | Flash:Plaintext | Erased from flash when all HSMs which own the VHSM leaves the group or have been zeroized. | Zeroization RPC | VHSM Private Key:Paired With |
| HSM keypair/ self-signed certificate | Module Public Key Output | RAM:Plaintext | Unique per physical HSM. New random keypair generated on reboot. | Zeroization RPC | |
| Crypto Officer CA certificate | Secure Channel Input | Flash:Plaintext | | Zeroization RPC | |
| Crypto Officer user certificate | Peer Public Key Input | RAM:Plaintext | While Secure Channel is Active | Zeroization RPC | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| User CA certificate | Secure Channel Input | Flash:Plaintext | | Zeroization RPC | |
| User certificate | Peer Public Key Input | RAM:Plaintext | While Secure Channel is Active | Zeroization RPC | |
| User crypto key | | Flash:Plaintext | | Zeroization RPC | |
| Firmware Load Test Key | | Flash:Plaintext | | N/A | |
| Secure Channel ECDH Private Key | | RAM:Plaintext | While Secure Channel is active | Zeroization RPC | Secure Channel ECDH Public Key:Paired With<br>Peer Secure Channel ECDH Public Key:Used With |
| Secure Channel ECDH Public Key | Module Public Key Output | RAM:Plaintext | While Secure Channel is active | Zeroization RPC | Secure Channel ECDH Private Key:Paired With |
| Peer Secure Channel ECDH Public Key | Peer Public Key Input | RAM:Plaintext | While Secure Channel is active | Zeroization RPC | Secure Channel ECDH Private Key:Used With |
| Secure Channel Shared Secret | | RAM:Plaintext | While Secure Channel is active | Zeroization RPC | Secure Channel ECDH Private Key:Derived From<br>Peer Secure Channel ECDH Public Key:Derived From |
| Secure Channel HSM to Client Encryption Key | | RAM:Plaintext | While Secure Channel is active | Zeroization RPC | Secure Channel Shared Secret:Derived From |
| Secure Channel Client to HSM Encryption Key | | RAM:Plaintext | While Secure Channel is active | Zeroization RPC | Secure Channel Shared Secret:Derived From |

Table 20: SSP Table 2

# 10 Self-Tests

## 10.1 Pre-Operational Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| Firmware Integrity Test | 32-bit Error Detection Code (EDC) | KAT | SW/FW Integrity | Module is in normal operation | 32-bit Checksum EDC |

Table 21: Pre-Operational Self-Tests

The module performs the firmware integrity test prior to the module becoming operational. Following the successfully pre-operational self-test, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs) detailed below.

## 10.2 Conditional Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-GCM Authenticated Encrypt KAT (A6546) | 256-bits | KAT | CAST | Success: No Error Code; Failure: "Aes256GcmKatFail" | Authenticated Encrypt | Power Up |
| AES-GCM Authenticated Decrypt KAT (A6546) | 256-bits | KAT | CAST | Success: No Error Code; Failure: "Aes256GcmKatFail" | Authenticated Decrypt | Power Up |
| HMAC DRBG Instantiate KAT (A6546) | HMAC-SHA2-256 | KAT | CAST | Success: No Error Code; Failure: "DrbgHmacSha256KatFail" | Instantiate KAT | Power Up |
| HMAC DRBG Generate KAT (A6546) | HMAC-SHA2-256 | KAT | CAST | Success: No Error Code; Failure: "DrbgHmacSha256KatFail" | Generate KAT | Power Up |
| HMAC DRBG Reseed KAT (A6546) | HMAC-SHA2-256 | KAT | CAST | Success: No Error Code; Failure: "DrbgHmacSha256KatFail" | Reseed KAT | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| ECDSA SigGen (FIPS186-5) KAT (A6546) | Curve: P-256 with SHA2-256 | KAT | CAST | Success: No Error Code; Failure: "EcdsaP256KatFail" | ECDSA SigGen KAT | Power Up |
| ECDSA SigVer (FIPS186-5) KAT (A6546) | Curve: P-256 with SHA2-256 | KAT | CAST | Success: No Error Code; Failure: "EcdsaP256KatFail" | ECDSA SigVer KAT | Power Up |
| Entropy Source RCT Start-up Health Tests | Repetition Count Test (RCT) | RCT | CAST | Module is in normal state | N/A | Power up |
| Entropy Source APT Start-up Health Tests | Adaptive Proportion Test (APT) | APT | CAST | Module is in normal state | N/A | Power up |
| Entropy Source RCT Continuous Health Tests | Repetition Count Test (RCT) | RCT | CAST | Module is in normal state | N/A | Performed continuously as entropy source is active |
| Entropy Source APT Continuous Health Tests | Adaptive Proportion Test (APT) | APT | CAST | Module is in normal state | N/A | Performed continuously as entropy source is active |
| HMAC-SHA2-256 KAT (A6546) | HMAC-SHA2-256 | KAT | CAST | Success: No Error Code; Failure: "HmacSha256KatFail" | HMAC-SHA2-256 | Power Up |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A6546) | Curve: P-256 | KAT | CAST | Success: No Error Code; Failure: "EcdhP256KatFail" | Primitive Z KAT | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| KDF SP800-108 KAT (A6546) | HMAC-SHA2-256 Feedback | KAT | CAST | Success: No Error Code; Failure: "KdfHmacSha256KatFail" | KDF KAT | Power Up |
| ECDSA KeyGen (FIPS186-5) PCT (A6546) | Curve: P-256 with SHA2-256 | PCT | PCT | Success: No Error Code; Failure: "EcdsaP256PairwiseConsistencyCheckFail" | Pairwise consistency test | After key pair generation |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A6546) | Curve: P-256 | PCT | PCT | Success: No Error Code; Failure: "EcdhP256PairwiseConsistencyCheckFail" | Pairwise consistency test | After key pair generation |
| Firmware Load Test | ECDSA P-256 with SHA2-256 | KAT | SW/FW Load | Success: No Error Code; Failure: "InvalidImageChecksum" | ECDSA SigVer and SHA2-256 | When firmware has been uploaded to the module |

Table 22: Conditional Self-Tests

All cryptographic algorithm self-tests (CASTs) must be performed and passed prior to any other use of cryptography by the module.

## 10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Firmware Integrity Test | KAT | SW/FW Integrity | 24 Hours | Automatic Reboot |

Table 23: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-GCM Authenticated Encrypt KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| AES-GCM Authenticated | KAT | CAST | 24 Hours | Automatic Reboot |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Decrypt KAT (A6546) | | | | |
| HMAC DRBG Instantiate KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| HMAC DRBG Generate KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| HMAC DRBG Reseed KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| ECDSA SigGen (FIPS186-5) KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| ECDSA SigVer (FIPS186-5) KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| Entropy Source RCT Start-up Health Tests | RCT | CAST | 24 Hours | Automatic Reboot |
| Entropy Source APT Start-up Health Tests | APT | CAST | 24 Hours | Automatic Reboot |
| Entropy Source RCT Continuous Health Tests | RCT | CAST | 24 Hours | Automatic Reboot |
| Entropy Source APT Continuous Health Tests | APT | CAST | 24 Hours | Automatic Reboot |
| HMAC-SHA2-256 KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| KDF SP800-108 KAT (A6546) | KAT | CAST | 24 Hours | Automatic Reboot |
| ECDSA KeyGen (FIPS186-5) PCT (A6546) | PCT | PCT | 24 Hours | Automatic Reboot |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A6546) | PCT | PCT | 24 Hours | Automatic Reboot |
| Firmware Load Test | KAT | SW/FW Load | N/A | N/A |

Table 24: Conditional Periodic Information

The module maintains a self-test internal timer; each time the timer expires the module automatically performs all the cryptographic algorithm self-tests (CASTs) and resets the timer. The operator can also initiate the pre-operational and conditional self-tests on demand by rebooting the module.

### 10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Error State | A FIPS error can be detected in any state and always results in a reboot. | Self-test failure<br>Firmware EDC check failure<br>Temperature outside operational range<br>Voltage outside operational range | Reboot the module | From HSM: HSM is in error state |

Table 25: Error States

If anyone of the above-mentioned self-tests fails, the pre-operational firmware integrity test fails, or the temperature/ voltage is outside the operational range, the module logs the cause of the error to the FIPS error log and enters the error state. In the error state, all cryptographic services are halted, and the data output from the data output interface is inhibited. The only way to recover the module from the error state is to reboot the module, which will perform the pre-operational, cryptographic algorithm self-tests and check the temperature/ voltage. The module will only enter into the operational state after successfully passing the pre-operational and cryptographic algorithm self-tests and the temperature/ voltage is within the operational range.

## 11 Life-Cycle Assurance

### 11.1 Installation, Initialization, and Startup Procedures

The module is configured in the factory to be in the Approved mode of operation, and can only be operated in the Approved mode of operation. No procedures for the secure installation, initialization, and startup of the module are required.

The operator can verify the module is in the Approved mode of operation by authenticating to the module and performing the `Show Status` service and confirm the module outputs: “FIPS-compliant mode: true.”

### 11.2 Administrator Guidance

No specific Administrator guidance.

### 11.3 Non-Administrator Guidance

No specific Non-Administrator guidance.

# 12 Mitigation of Other Attacks

N/A for this module.