# Google, Inc.

Knuckle Cryptographic Module

# FIPS 140-3 Non-Proprietary Security Policy


Google, LLC 2026

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

# Table of Contents

1 General ..... 4
1.1 Overview ..... 4
1.2 Security Levels ..... 5
2 Cryptographic Module Specification ..... 5
2.1 Description ..... 5
2.2 Tested and Vendor Affirmed Module Version and Identification ..... 7
2.3 Excluded Components ..... 7
2.4 Modes of Operation ..... 7
2.5 Algorithms ..... 7
2.6 Security Function Implementations ..... 9
2.7 Algorithm Specific Information ..... 10
2.8 RBG and Entropy ..... 12
2.9 Key Generation ..... 12
2.10 Key Establishment ..... 12
2.11 Industry Protocols ..... 12
3 Cryptographic Module Interfaces ..... 13
3.1 Ports and Interfaces ..... 13
4 Roles, Services, and Authentication ..... 13
4.1 Authentication Methods ..... 13
4.2 Roles ..... 14
4.3 Approved Services ..... 14
4.5 External Software/Firmware Loaded ..... 20
4.6 Bypass Actions and Status ..... 20
4.7 Cryptographic Output Actions and Status ..... 21
5 Software/Firmware Security ..... 21
5.1 Integrity Techniques ..... 21
5.2 Initiate on Demand ..... 21
6 Operational Environment ..... 21
6.1 Operational Environment Type and Requirements ..... 21
6.2 Configuration Settings and Restrictions ..... 21
7 Physical Security ..... 22
7.1 Mechanisms and Actions Required ..... 22
8 Non-Invasive Security ..... 22
8.1 Mitigation Techniques ..... 22


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

9 Sensitive Security Parameters Management....22
9.1 Storage Areas....22
9.2 SSP Input-Output Methods....22
9.3 SSP Zeroization Methods....23
9.4 SSPs....23
10 Self-Tests....25
10.1 Pre-Operational Self-Tests....25
10.2 Conditional Self-Tests....25
10.3 Periodic Self-Test Information....29
10.4 Error States....31
10.5 Operator Initiation of Self-Tests....32
11 Life-Cycle Assurance....32
11.1 Installation, Initialization, and Startup Procedures....32
11.2 Administrator Guidance....32
11.3 Non-Administrator Guidance....32
11.4 Design and Rules....32
11.5 End of Life....32
12 Mitigation of Other Attacks....33
12.1 Attack List....33


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

## List of Tables

Table 1: Security Levels ..... 5
Table 2: Tested Module Identification – Hardware ..... 7
Table 3: Modes List and Description ..... 7
Table 4: Approved Algorithms ..... 8
Table 5: Vendor-Affirmed Algorithms ..... 8
Table 6: Security Function Implementations ..... 10
Table 7: Entropy Certificates ..... 12
Table 8: Entropy Sources ..... 12
Table 9: Ports and Interfaces ..... 13
Table 10: Roles ..... 14
Table 11: Approved Services ..... 20
Table 12: Mechanisms and Actions Required ..... 22
Table 13: Storage Areas ..... 22
Table 14: SSP Input-Output Methods ..... 22
Table 15: SSP Zeroization Methods ..... 23
Table 16: SSP Table 1 ..... 24
Table 17: SSP Table 2 ..... 25
Table 18: Pre-Operational Self-Tests ..... 25
Table 19: Conditional Self-Tests ..... 29
Table 20: Pre-Operational Periodic Information ..... 29
Table 21: Conditional Periodic Information ..... 30
Table 22: Error States ..... 31

## List of Figures

Figure 1: Block Diagram ..... 6
Figure 2: Knuckle Application Specific Integrated Circuit (ASIC) ..... 6

# 1 General

This document describes the cryptographic module security policy for Google LLC. Knuckle Cryptographic Module (Hardware version: A1) (also referred to as the “module” hereafter) with Google Knuckle ASIC Security Firmware (Firmware version: 1.1.1). It contains specifications of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard.

## 1.1 Overview

The Knuckle Cryptographic Module is defined as a sub-chip cryptographic subsystem module. The module implements a combination of hard and soft cryptographic functions and algorithms in the Knuckle Application Specific Integrated Circuit (ASIC) (P/N: GCNX-3200AB-CB5T). The cryptographic functions are split between:


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

- Firmware algorithms implemented within the ARM Crypto Cell IP block with firmware management functions executing in the ARM M3 CPU;
- ROM and
- NPC IP block which performs crypto offload for AES XTS

## 1.2 Security Levels

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

Table 1: Security Levels

# 2 Cryptographic Module Specification

## 2.1 Description

**Purpose and Use:**

The Knuckle Cryptographic Module is defined as a sub-chip cryptographic subsystem within a single-chip physical embodiment. The module is the primary component of a PCIe-based NVMe controller which provides AES-XTS encryption of data-at-rest and key management functionality per Trusted Computing Group (TCG) Opal specifications. The NVMe controller also includes a Google Titan chip for providing a Root of Trust (RoT) and boot security.

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated storage devices. The Module is intended to be used in a storage system.

**Module Type**: Hardware

**Module Embodiment**: Single Chip

**Module Characteristics**: SubChip

**Cryptographic Boundary:**


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

Figure 1 below depicts the cryptographic boundary of the module (red outline).

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

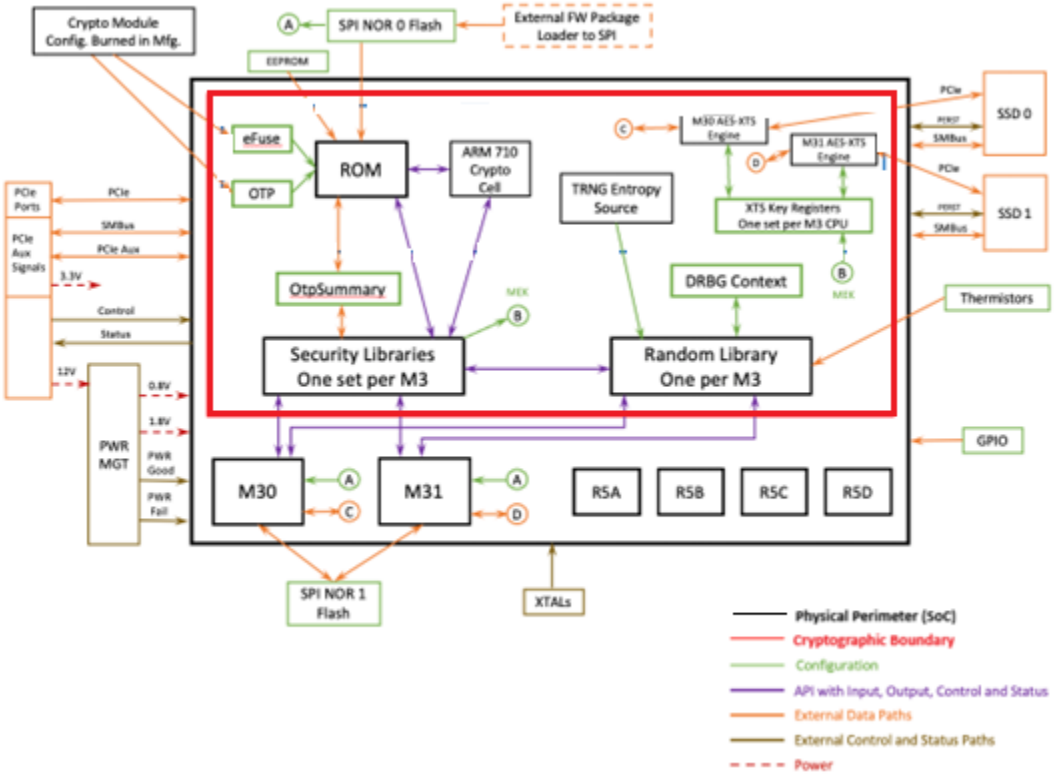


Figure 1: Block Diagram

Figure 2: Knuckle Application Specific Integrated Circuit (ASIC)


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

## 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 |
|---|---|---|---|---|
| GCNX-3200AB-CB5T ASIC | A1 | 1.1.1 | ARM Cortex M3 CPU with Trustzone | N/A |

Table 2: Tested Module Identification – Hardware

## 2.3 Excluded Components

No components have been excluded from the cryptographic boundary of the module.

## 2.4 Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved Mode | The module only supports approved cryptography and thus only supports an Approved Mode of operation by default; The module enters the Approved mode of operation upon successful completion of self-tests | Approved | Successful completion of self-tests |

Table 3: Modes List and Description

## 2.5 Algorithms

**Approved Algorithms:**

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A6544 | Direction - Encrypt<br>Key Length - 256 | SP 800-38A |
| AES-CBC | A6545 | Direction - Decrypt, Encrypt<br>Key Length - 256 | SP 800-38A |
| AES-CMAC | A6545 | Direction - Generation<br>Key Length - 256 | SP 800-38B |
| AES-CTR | A6545 | Direction - Decrypt, Encrypt<br>Key Length - 256 | SP 800-38A |


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

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-ECB | A6545 | Direction - Decrypt, Encrypt<br>Key Length - 256 | SP 800-38A |
| AES-KW | A6544 | Direction - Encrypt<br>Key Length - 256 | SP 800-38F |
| AES-KW | A6545 | Direction - Decrypt<br>Key Length - 256 | SP 800-38F |
| AES-XTS Testing Revision 2.0 | A6543 | Direction - Decrypt, Encrypt<br>Key Length - 256 | SP 800-38E |
| Counter DRBG | A6544 | Prediction Resistance - Yes<br>Mode - AES-256<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| HMAC-SHA2-384 | A6544 | Key Length - Key Length: 256 | FIPS 198-1 |
| HMAC-SHA2-384 | A6545 | Key Length - Key Length: 256 | FIPS 198-1 |
| KDF SP800-108 | A6545 | KDF Mode - Counter<br>Supported Lengths - Supported Lengths: 256-1536 Increment 256 | SP 800-108 Rev. 1 |
| PBKDF | A6544 | Iteration Count - Iteration Count: 128-16384 Increment 128<br>Password Length - Password Length: 8-32 Increment 8 | SP 800-132 |
| RSA SigVer (FIPS186-5) | A6545 | Modulo - 3072<br>Signature Type - pkcs1v1.5, pss | FIPS 186-5 |
| SHA2-384 | A6545 | Message Length - Message Length: 8-2048 Increment 8, 2048-65280 Increment 256 | FIPS 180-4 |

Table 4: Approved Algorithms

There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

**Vendor-Affirmed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG - Section 4 | Key Type:Symmetric | N/A | NIST SP800-133r2 Section 4: symmetric key generation using the output of an approved DRBG |
| CKG - Section 6.3 | Key Type:Symmetric | N/A | NIST SP800-133r2 Section 6.3: Symmetric Keys Produced by Combining (Multiple) Keys and Other Data |

Table 5: Vendor-Affirmed Algorithms

**Non-Approved, Allowed Algorithms:**


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

The module does not support any Non-Approved, Allowed Algorithms.

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

The module does not support any Non-Approved, Allowed Algorithms with No Security Claimed.

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

The module does not support any Non-Approved, Not Allowed Algorithms.

## 2.6 Security Function Implementations

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| Symmetric Encryption/Decryption | BC-Auth BC-UnAuth | Data Encryption and Decryption using AES | AES:[SP 800-38A] | AES-XTS Testing Revision 2.0: (A6543) AES-CBC: (A6544, A6545) AES-CTR: (A6545) AES-ECB: (A6545) AES-CMAC: (A6545) |
| Hash Generation | SHA | Hashing using SHA2-384 | SHS:[FIPS 180-4] | SHA2-384: (A6545) |
| Keyed Hash Generation | MAC | Hash based MAC Generation using HMAC-SHA2-384 | HMAC:FIPS 198-1 | HMAC-SHA2-384: (A6544, A6545) |
| Random Bit Generation | DRBG | Random Bit Generation using Counter DRBG | DRBG:[SP 800- 90Arev1] | Counter DRBG: (A6544) CKG - Section 4 : () Key Type: Symmetric CKG - Section 6.3: () Key Type: Symmetric |
| Key Derivation 1 | KBKDF | Key Based Key Derivation | KBKDF:[SP 800-108] | KDF SP800-108: (A6545) |


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

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| Key Derivation 2 | PBKDF | Password Based Key Derivation | PBKDF2:[SP 800-132] | PBKDF: (A6544) |
| Signature Verification | DigSig-SigVer | Digital Signature Verification using RSA | RSA:[FIPS 186-5] | RSA SigVer (FIPS186-5): (A6545) |
| KTS | KTS-Unwrap KTS-Wrap | Key Wrapping and Key Unwrapping using AES-KW | AES:[SP 800-38F] | AES-KW: (A6544, A6545) |

Table 6: Security Function Implementations

## 2.7 Algorithm Specific Information

IG D.H
CKG is supported for the following sections per NIST SP 800-133r2 as documented in the Security Policy Section 2.5, Vendor Affirmed Algorithms Table: Section 4 (symmetric key generation using the output of an approved DRBG).

IG D.J
The module receives entropy from a source within its cryptographic boundary in accordance with IG 9.3.A 1.a. The entropy source is a hardware True Random Number Generator (TRNG) integrated within the module. It generates raw entropy that is used to seed the NIST SP 800-90Ar1 Counter DRBG (AES-256). Per the ESV Cert #E289 the min-entropy per bit provided by the entropy source is 0.76214 bits and 3219 bits per 4224 bit-block which is sufficient for generation of keys with a security strength of up to 256 bits. Given that 256 bits is the maximum key length supported by the module, the entropy provided is deemed sufficient and a caveat per IG 9.3.A thus does not apply.

IG D.L
Per the IG, the Entropy Input, DRBG Seed and Counter DRBG State values - V and Key have been defined as CSPs. Per Additional Requirement #2. in the IG, the module has been tested with a derivation function.

IG D.M
In accordance with IG D.M, the SP 800-108 KDF is used only for generation of symmetric keys.

IG D.G
The SSP establishment method supported by the module in accordance with IG D.G has been documented in the Security Policy Section 2.6, Security Function Implementations Table (KTS).

IG D.N
The module is compliant with IG D.N and NIST SP 800-132 Section 5.4 Option 1a. The iteration count values used per NIST SP 800-132 Section 5.2 are set whereby the iteration count shall be


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

selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The derived key must possess a minimum-security strength of 112 bits. The module supports NIST SP 800-133r2 Section 6.2.2. In accordance with NIST SP 800-132 requirements, usage of the derived keys is restricted to storage applications alone.

The module supports a minimum 8-character long password and a maximum length of 32-characters. The ASCII system comprises of 94 printable characters (letters, digits, punctuation, and symbols). For a 8-character password/passphrase chosen from 94 printable ASCII characters, the total combinations are: 94^8. Thus, the probability of guessing the correct password/passphrase on a random attempt is: 1/94^8 ~ 1.64e^-16.

In accordance with NIST SP 800-132, passwords shorter than 10 characters are usually considered to be weak. There are many other properties that may render a password weak. For example, it is not advisable to use sequences of numbers or sequences of letters as passwords. Easily accessed personal information, such as the user's name, phone number, and date of birth, should not be used directly as a password.

Passphrases frequently consist solely of letters, but they make up for their lack of entropy by being much longer than passwords, typically 20 to 30 characters. Passphrases shorter than 20 characters are usually considered weak.

IG 2.3.B
The module meets the following applicable requirements per IG 2.3.B:

The physical perimeter of the module is defined as the single chip i.e. the ASIC within which the sub-chip module is contained as explained in Section 2.1.

The ports and interfaces have been defined at the HMI and listed in the Security Policy Section 3.1, Ports and Interfaces Table. The operational testing for the module was performed at the HMI as well (i.e. at the sub-chip boundary).

The Sensitive Security Parameter requirements have been applied at the sub-chip crypto subsystem boundary as well per IG 9.5.A (although the IG does state: Transferring SSPs including the entropy input between a sub-chip cryptographic subsystem HMI and an intervening functional subsystem for Security Levels 1 and 2 on the same single chip does not require meeting the sensitive security parameter establishment requirements, per IG 9.5.A).

Versioning information has been provided for the single-chip in the OE field in the module information section of the validation report (i.e. on the module certificate), as well as in the hardware version column in the Security Policy Section 2.2, Tested Module Identification - Hardware Table.

Additional Comment #2 in the IG also applies to the module and is satisfied per the module's design i.e. the FIPS 140-3 requirements have been applied at the HMI of the sub-chip cryptographic subsystem; not at the boundary of the single-chip in the event that the sub-chip cryptographic subsystem enters an error state.

IG C.I


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

Per IG C.I, usage in accordance with [SP800-38E], the XTS-AES algorithm is only used for confidentiality on storage devices. The Module complies with [FIPS140-3_IG] C.I by explicitly checking that Key_1 ≠ Key_2 before using the keys in the XTS-AES algorithm to process data with them. Key 1 and Key 2 are generated independently.

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|---|---|
| E289 | Google LLC |

Table 7: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| GCNX-3200AB-CB5T Knuckle TRNG | Physical | GCNX-3200AB-CB5T, Version A1 | 1 bit | 0.76214 | N/A |

Table 8: Entropy Sources

The seed value comes from a 4224-bit raw entropy source value. This means 2^4224 possible permutations of the value. That entropy is post-processed by approved algorithms found in the NIST document NIST SP.800-90Ar1, with a nonce, personalization string and additional data. This results in a DRBG seed of 384 bits of entropy or 2^384 possible permutations. The module supports an approved Counter DRBG algorithm per NIST 800-90Ar1. The security strength of the random SSP value is 256 bits or 2^256 possible values. Thus, the number of operations needed to guess the seed value will exceed the number of operations required to determine the resulting DRBG SSP.

## 2.9 Key Generation

Keys are derived in the ROM using KDF. The only keys generated using a DRBG are the AES-XTS keys.

## 2.10 Key Establishment

The module supports KTS (per IG D.G) as specified in the Section 2.6 Security Functions Implementation Table.

## 2.11 Industry Protocols

The module does not implement any industry protocols.


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

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| Thermistors | Data Input | Used for reading of external component temperatures; not connected to any thermal area but provide variable data at the time read |
| SPI NOR Flash (Serial Port Interface) | Data Input | Firmware/System tables; SPI NOR 0 is used to store the module firmware image |
| UART | Control Input<br>Status Output | Used for console IO (Messages with system info, states and operator commands) |
| Power | Power | Provides 0.8V and 1.8V power to the chip which in turn provides power to the module |
| PCIe ports | Data Input<br>Data Output | Host-facing PCIe Interface: endpoint for communication with the host; SSD-facing PCIe Interfaces: for communication with the attached NVMe SSDs; PCIe Registers: Access to configuration registers for the PCIe interfaces |

Table 9: Ports and Interfaces

All data and control inputs, and data and status outputs of the cryptographic module and services are directed through the module's defined ports/interfaces. The module does not support a control output interface.

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

N/A for this module.

The module does not support authentication. The module supports a Crypto Officer (CO) role alone.


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

## 4.2 Roles

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| Crypto Officer (CO) | Role | Crypto Officer | None |

Table 10: Roles

The Crypto Officer (CO) role can be implicitly assumed via service invocation and is authorized to access all services provided by the module. The module does not support a Maintenance or User role.

## 4.3 Approved Services

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Symmetric Encryption/Decryption | AES services provided directly by the ARM 710 crypto cell. They include ECB, CBC, CTR and CMAC | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | Depending on the mode: An encryption/decryption key, IV, a buffer, length to encrypt/decrypt, plaintext/ciphertext | Plaintext/Ciphertext | Symmetric Encryption/Decryption | Crypto Officer (CO) - KEK (KDR): G,E |
| Hash Generation | SHA2-384 hash of passed buffer; Generally used to generate a hash of the ROM metal at boot to compare the hash | Implicit indicator via successful completion of the service combined with the Approved | Data to be hashed | 48 byte hash value | Hash Generation | Crypto Officer (CO) |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | of the ROM with the hash value burned into the OTP as the first internal integrity check | Mode indicator | | | | |
| Keyed Hash Generation | HMAC; This uses the KEK key found in the OtpSummary as its key | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | The KEK PSP from the OtpSmmary and the buffer on which the MAC operation is to be performed | 48-byte HMAC value | Keyed Hash Generation | Crypto Officer (CO) - FAK: G,E |
| Random Bit Generation | Random bit/number generation is performed with DRBG and its corresponding DRBG context | Implicit indicator via successful completion of the service combined with the Approved Mode | DRBG context is instantiated with the 48-byte processed raw 528 byte entropy from the entropy source along with a personalization string and additional data; The only usage input via the API is | Random value of the desired length requested at input | Random Bit Generation | Crypto Officer (CO) - DRBG Entropy Input: G,E - DRBG Seed |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | indicator | the desired length of the random number | | | : G,E - DRBG State - V : G,E - DRBG State - Key: G,E |
| Key Derivation | Used only by the ROM and includes the hidden ARM processed and hidden KDR value as part of the key generation | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | Hidden secure KDR data; Label created from a portion of the sha386 of the ROM; Context created from a portion of the sha386 of the ROM | 1536 key bits that make up the keys described in the SSP column here | Key Derivation 1<br>Key Derivation 2 | Crypto Officer (CO) - KDR : G,E |
| Key Wrapping/Unwrapping | Using the PS KEK in the OtpSummary, wraps the passed key using the cipher block method based on | Implicit indicator via successful completion of the service combined with the Approved | Wrapping: KEK, Key to be wrapped; Unwrapping: same KEK as wrapping used and the wrapped Key | Wrapping: SSP that represents the wrapped Key; Unwrapping: SSP that represents the unwrapped key | KTS | Crypto Officer (CO) - KEK (KDR): G,E - FWK : G,E |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | NIST 800-38F; Key is unwrapped using the same internal KEK | Mode indicator | | | | |
| Signature Verification | Used to authenticate the firmware on load | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | RSA Public Key and certificate data | Status/success or failure of the signature verification operation or Root-of-Trust Authentication (as part of the firmware load process) | Signature Verification | Crypto Officer (CO) |
| On-demand Self-Tests (Perform Self-tests) | From both the UART and via NVMe (over PCIe interfaces), the CO can requisition the on-demand to be run; If the crypto module is already in the error | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | Execution of the on-Demand NVMe command via the UART | UART results; If any test fails, the module enters the error state and all cryptographic operations are prohibited | None | Crypto Officer (CO) |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | state, all tests will fail; If not and the on-demand test fails any of the self-tests, the crypto module will go into the error state and the system will lock | | | | | |
| Show Status | The module denotes status i.e. indication that it is in the Approved mode of operation after successful completion of all self-tests; If any self-tests were to fail, the module returns the error indicator as the status output | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | Execution of the on-Demand NVMe command via the UART | Output/results (i.e. success/failure indicator for self-tests) sent to the UART post command execution | None | Crypto Officer (CO) |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Show module's versioning information (Show Version) | All versioning information (module name, hardware version and firmware version) is returned in the output to the UART as a response to the ver command | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | Execution of the ver command on the UART | module name, hardware version and firmware version | None | Crypto Officer (CO) |
| Zeroise (Perform zeroisation) | Performed via a reboot since all SSPs are stored ephemerally | Implicit indicator via successful completion of the service combined with the Approved Mode indicator | Power cycle/reboot | N/A | None | Crypto Officer (CO) - KDR: Z - FAK: Z - FWK: Z - KEK (KDR): Z - DRBG Entropy |


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

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Input: Z - DRBG Seed: Z - DRBG State - V: Z - DRBG State - Key: Z |

Table 11: Approved Services

The abbreviations of the access rights to the module's SSPs listed in the table above have the following interpretations:

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g., the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

## 4.5 External Software/Firmware Loaded

The module supports loading of firmware at every boot (the same firmware i.e. entire firmware image is loaded on each boot). An RSA mod 3072 SHA2-384 signature verification is performed by the module in support of the same. The RSA public key used for the same is stored within the module and considered a non-SSP. Any firmware 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 Bypass Actions and Status

The module does not support a bypass capability.


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

### 4.7 Cryptographic Output Actions and Status

The module does not support any self-initiated cryptographic output capability.

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

In the firmware release process at Google, the firmware is integrity checked by comparing the three firmware libraries that are within the cryptographic boundary (part of the firmware loaded on each boot as an image/binary) by a SHA2-256 comparison against the ‘golden’ hash values for each library. If the comparison fails, that release will not occur.

The module is integrity protected by the ISO 19790/FIPS 140-3 requirements as follows:

First, the metal that makes up the ROM is hashed (SHA2-384, the hash is considered a non-SSP) and then compared to a hash value burned into the OTP.

The next stage in integrity checking is by the ROM (metal) running (as always) a conditional self-test on RSA prior to use that is then used to verify the M30 boot loader prior to loading. This only verifies that the metal (ROM) has not changed. If this test were to fail, the module is rendered unusable. The integrity of the M30 boot loader is verified by the ROM. The M30 boot loader then does an RSA mod 3072 SHA2-384 signature verification (using the RSA public key, a non-SSP) on the M31 boot loader and the M30 main firmware i.e. the module firmware.

## 5.2 Initiate on Demand

The integrity test can be called on demand by invoking the Perform Self-Tests (On-demand Self-Tests) service and by rebooting the module.

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

**Type of Operational Environment**: Limited

**How Requirements are Satisfied**:

The Module has a limited operational environment. The Module includes a firmware load function to support necessary updates for Google Knuckle ASIC Security Firmware (Firmware version 1.1.1) and Google Knuckle ASIC ROM (version A1).

## 6.2 Configuration Settings and Restrictions


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

Once the module leaves manufacturing, the module cannot be configured or its operating environment changed by any external operation or operator.

# 7 Physical Security

## 7.1 Mechanisms and Actions Required

| Mechanism | Inspection Frequency | Inspection Guidance |
|---|---|---|
| Standard passivation applied to the ASIC | None | None |

Table 12: Mechanisms and Actions Required

The module has a single chip physical embodiment. The single chip has been developed with production grade components.

# 8 Non-Invasive Security

## 8.1 Mitigation Techniques

The module does not support any non-invasive attack mitigations and thus the requirements per this section do not apply.

# 9 Sensitive Security Parameters Management

## 9.1 Storage Areas

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| SRAM | OtpSummary (burned on every boot), DRBG Context | Dynamic |
| ROM | Code in metal | Static |

Table 13: Storage Areas

## 9.2 SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| OtpSummary | External location (within the SoC) | SRAM | Plaintext | Automated | Electronic | |

Table 14: SSP Input-Output Methods


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

## 9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Reboot | Zeroisation can be performed via a reboot of the module | SSPs stored ephemerally within the module can be zeroised upon reboot | Operator Initiated |

Table 15: SSP Zeroization Methods

## 9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| KDR | Device Root Key | 256 bits - 256 bits | Key Derivation Symmetric Key - CSP | Random Bit Generation | | Key Derivation 1<br>Key Derivation 2 |
| FAK | Firmware Authentication Key | 256 bits - 256 bits | Symmetric Key - CSP | Key Derivation 1<br>Key Derivation 2 | | Keyed Hash Generation |
| KEK (KDR) | Key Encryption Key; Used to wrap and unwrap XTS MEKs stored in SPI | 256 bits - 256 bits | Symmetric Key - CSP | Key Derivation 1<br>Key Derivation 2 | | KTS |
| FWK | Firmware Encryption Key Wrapping Key | 256 bits - 256 bits | Symmetric Key - CSP | Key Derivation 1<br>Key Derivation 2 | | KTS |
| MEK | Media Encryption Key (AES-XTS key) | 256 bits - 256 bits | Symmetric Key - CSP | Random Bit Generation | | Symmetric Encryption/Decryption |


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

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| DRBG Entropy Input | Entropy Input to the seed the Counter DRBG from the entropy source; Per Resolution 3. in IG D.L | 4224 bits - 256 bits | Entropy Input - CSP | | | Random Bit Generation |
| DRBG Seed | Seed provided to the Counter DRBG (derived from the Entropy Input); Per Resolution 3. in IG D.L | 384 bits - 256 bits | Seed - CSP | Random Bit Generation | | Random Bit Generation |
| DRBG State - V | DRBG Internal State Value - V; Per Resolution 3. in IG D.L | 128 bits - 128 bits | DRBG Internal State Value - CSP | Random Bit Generation | | Random Bit Generation |
| DRBG State - Key | DRBG Internal State Value - Key; Per Resolution 3. in IG D.L | 256 bits - 256 bits | DRBG Internal State Value - CSP | Random Bit Generation | | Random Bit Generation |

Table 16: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| KDR | | SRAM:Plaintext | Until reboot | Reboot | |
| FAK | OtpSummary | SRAM:Plaintext | Until next Reboot | Reboot | KDR:Derived From |
| KEK (KDR) | OtpSummary | SRAM:Plaintext | Until next reboot | Reboot | KDR:Derived From |
| FWK | OtpSummary | SRAM:Plaintext | Until next reboot | Reboot | KDR:Derived From |


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

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| MEK | | SRAM:Plaintext | Until reboot | Reboot | |
| DRBG Entropy Input | | SRAM:Plaintext | Until reboot | Reboot | DRBG Seed:Used to derive |
| DRBG Seed | | SRAM:Plaintext | Until reboot | Reboot | DRBG Entropy Input:Derived From<br>DRBG State - V :Used to derive<br>DRBG State - Key:Used to derive |
| DRBG State - V | | SRAM:Plaintext | Until reboot | Reboot | DRBG Seed:Derived From<br>DRBG State - Key:Paired With |
| DRBG State - Key | | SRAM:Plaintext | Until reboot | Reboot | DRBG Seed:Derived From<br>DRBG State - V :Paired With |

Table 17: 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 | RSA SigVer PSS mod 3072 | KAT | SW/FW Integrity | - | Verify |

Table 18: Pre-Operational Self-Tests

The module performs pre-operational self-tests automatically at power-on. An operator can execute a specific UART command for invocation of the pre-operational and conditional self-tests on demand. While the module is executing self-tests, services are not available, and input and output are inhibited.

## 10.2 Conditional Self-Tests


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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-XTS Testing Revision 2.0 (A6543) - Encrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_hw_data_path_xts_aes_enc_self_test (Test 16) passed | Encrypt | On boot |
| AES-XTS Testing Revision 2.0 (A6543) - Decrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_hw_data_path_xts_aes_dec_self_test (Test 15) passed | Decrypt | On boot |
| AES-CBC (A6544) | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_cbc_encrypt_kat (Test 4) passed | Encrypt | Prior to first use |
| AES-KW (A6544) | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_kwf_kat (Test 9) passed | Encrypt | Prior to first use |
| Counter DRBG (A6544) | Key Length: 256 bits | Known Answer Test | CAST | crypto_fsl_drbg_kat (Test 12) passed | Generate, Reseed, Instantiate functions | On boot |
| HMAC-SHA2-384 (A6544) | Key Length: 384 bits | Known Answer Test | CAST | crypto_rom_hmac_kat (Test 7) passed | MAC generation/verification | Prior to first use |
| PBKDF (A6544) | Key Length: 256 bits | Known Answer Test | CAST | crypto_fsl_pbkdf_kat (Test 14) passed | Key Derivation | Prior to first use |


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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CBC (A6545) - Encrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_cbc_encrypt_kat (Test 4) passed | Encrypt | Prior to first use |
| AES-CBC (A6545) - Decrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_cbc_decrypt_kat (Test 5) passed | Decrypt | Prior to first use |
| AES-CMAC (A6545) | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_cmac_kat (Test 6) passed | MAC generation/verification | Prior to first use |
| AES-CTR (A6545) - Encrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_ctr_enc_kat (Test 0) passed | Encrypt | Prior to first use |
| AES-CTR (A6545) - Decrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_ctr_dec_kat (Test 1) passed | Decrypt | Prior to first use |
| AES-ECB (A6545) - Encrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_ecb_enc_kat (Test 2) passed | Encrypt | Prior to first use |
| AES-ECB (A6545) - Decrypt | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_aes_ecb_dec_kat (Test 3) passed | Decrypt | Prior to first use |
| AES-KW (A6545) | Key Length: 256 bits | Known Answer Test | CAST | crypto_fsl_kwf_kat (Test 13) passed | Decrypt | Prior to first use |


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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| HMAC-SHA2-384 (A6545) | Key Length: 384 bits | Known Answer Test | CAST | crypto_rom_hmac_kat (Test 7) passed | MAC generation/verification | Prior to first use |
| KDF SP800-108 (A6545) | Key Length: 256 bits | Known Answer Test | CAST | crypto_rom_kdf_kat (Test 8) passed | Key Derivation | Prior to first use |
| RSA SigVer (FIPS186-5) (A6545) | Modulo: 3072 bits SHA2-384 | Known Answer Test | CAST | crypto_rom_rsa_kat (Test 10) passed | Verify | On boot |
| SHA2-384 (A6545) | SHA2-384 | Known Answer Test | CAST | crypto_rom_sha_kat (Test 11) passed | Hash | On boot |
| NIST SP 800-90B Health Test - RCT | False positive rate of 2^-40 | Repetition Count Test (RCT) | CAST | Entropy health tests are provided implicitly through successful execution of the start-up or reseed health test, as the entropy source runs to fulfill a single health test request before being disabled | - | On boot and if the age of the seed has passed its limit |
| NIST SP 800-90B Health Test - APT | False positive rate of 2^-40 | Adaptive Proportion Test (APT) | CAST | Entropy health tests are provided implicitly through successful execution of the start-up or reseed health test, as the entropy source runs to fulfill a single health test request before being disabled | - | On boot and if the age of the seed has passed its limit |
| NIST SP 800-90B Health Test - Develo | False positive rate of 2^-40 | Developer Defined Test | CAST | Entropy health tests are provided implicitly through successful execution of the start-up or reseed health test, as the entropy source runs to fulfill a single health test request before being disabled | - | On boot and if the age of the seed has |


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

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| per Defined | | | | | | passed its limit |

Table 19: Conditional Self-Tests

## 10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Firmware Integrity Test | KAT | SW/FW Integrity | On Demand | Manually via a reboot |

Table 20: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-XTS Testing Revision 2.0 (A6543) - Encrypt | Known Answer Test | CAST | On Demand | Manually, via a reboot |
| AES-XTS Testing Revision 2.0 (A6543) - Decrypt | Known Answer Test | CAST | On Demand | Manually, via a reboot |
| AES-CBC (A6544) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-KW (A6544) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| Counter DRBG (A6544) | Known Answer Test | CAST | On Demand | Manually, via a reboot |
| HMAC-SHA2-384 (A6544) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| PBKDF (A6544) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-CBC (A6545) - Encrypt | Known Answer Test | CAST | On Demand | Manually, via service invocation |


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

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CBC (A6545) - Decrypt | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-CMAC (A6545) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-CTR (A6545) - Encrypt | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-CTR (A6545) - Decrypt | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-ECB (A6545) - Encrypt | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-ECB (A6545) - Decrypt | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| AES-KW (A6545) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| HMAC-SHA2-384 (A6545) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| KDF SP800-108 (A6545) | Known Answer Test | CAST | On Demand | Manually, via service invocation |
| RSA SigVer (FIPS186-5) (A6545) | Known Answer Test | CAST | On Demand | Manually, via a reboot |
| SHA2-384 (A6545) | Known Answer Test | CAST | On Demand | Manually, via a reboot |
| NIST SP 800-90B Health Test - RCT | Repetition Count Test (RCT) | CAST | On Demand | Manually, via a reboot |
| NIST SP 800-90B Health Test - APT | Adaptive Proportion Test (APT) | CAST | On Demand | Manually, via a reboot |
| NIST SP 800-90B Health Test - Developer Defined | Developer Defined Test | CAST | On Demand | Manually, via a reboot |

Table 21: Conditional Periodic Information


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

## 10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Hard Error State | In the event that any self-test in the firmware/ROM/M30/M31 boot loaders fails, the module inhibits all data output and enters the Hard Error State; In the event that the integrity test fails the error handing depends on the boot stage at which the failure has been encountered i.e. a failure in the integrity check performed on the ROM/M30 bootloader will result in the module redirecting to a Boot Failure Menu from where the CO will need to load a new firmware image on next boot (still the equivalent of a Hard Error state); A failure in the M31 bootloader integrity check results in the module also entering the hard error state | Failure of a self-test | Usually unrecoverable; the CO can attempt to reboot the ASIC but if the failure persists, the module will be considered to be unrecoverable | An error message sent by the module on the UART port for a CAST failure (an indicator of the form "msg: <Algorithm name> Pre-Use Cypher Test Failed!" for RSA SigVer, DRBG and AES-XTS and an indicator of the form ""<Algorithm name> Cypher Test Failed!" for all other algorithms) and the module becomes unresponsive and gets stuck in case of a firmware integrity test failure (in case of the integrity failure in the ROM/M30 bootloader the module also re-directs to a Boot Failure Menu) |
| Soft Error State | In the event of a failure in the NIST SP 800-90B Health Tests for the entropy source, the module enters the Soft Error State | Failure of a NIST SP 800-90B Health Test | If at any point the health tests fail, the block is zeroized and an error is signaled via the function's return value and the source (and the module as a whole) continues to be operational | If at any point an error occurs (to include a health test failure) the return value will be non-zero |

Table 22: Error States


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

### 10.5 Operator Initiation of Self-Tests

Operator initiated self-tests i.e., on-demand self-tests, are done using a UART command with a test mask and all tests can be run if desired.

# 11 Life-Cycle Assurance

## 11.1 Installation, Initialization, and Startup Procedures

The module is shipped from the factory fully installed and initialized for Security Level 1, ready to be operational in the Approved mode.

All the firmware except the ROM metal is placed into the SPI NOR in manufacturing. Powering on the secure system performs all configuration and self-test requirements.

## 11.2 Administrator Guidance

The Crypto Officer is the only administrator, and the guidance will be available to that officer(s) only. The module handles its own error state which can only be resolved by a system reset. If that does not resolve issues within the module, it must be removed and destroyed. The only guidance for the CO would be how to run the self-tests on demand (see the On-demand Self-Tests service in Section 4.3 Approved Services Table). In general, in the event of any self-test failure that cannot be recovered by a reset, the module must be returned to Google and destroyed.

## 11.3 Non-Administrator Guidance

The module only supports an Administrator role (i.e. the Crypto Officer).

## 11.4 Design and Rules

No additional rules apply.

## 11.5 End of Life

The module can be securely sanitized by zeroising it.


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

# 12 Mitigation of Other Attacks

## 12.1 Attack List

The module does not mitigate against any other attacks and thus the requirements per this section do not apply.


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