Non-Proprietary FIPS 140-2 Security Policy

Google LLC. Titan-D Chip

Hardware Version: H1D3P
Firmware Version: dnafips-1.2

Date: February 21st, 2024

Prepared by:

intertek acumen security

www.acumensecurity.net

About this Document

This non-proprietary Cryptographic Module Security Policy for Titan-D from Google LLC. provides an overview of the product and a high-level description of how it meets the overall Level 1 security requirements of FIPS 140-2.

Titan may also be referred to as the “module” in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Google LLC. shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Google LLC. Titan-D cryptographic module with firmware version “dnafips-1.2” (also referred to as the “module” hereafter). It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

Module	HW P/N and Version	Firmware Version
Titan-D Chip	H1D3P	dnafips-1.2

Table 1 - Cryptographic Module Tested Configuration

Titan is a custom secure micro-controller. It can implement a variety of security, encryption, and cryptography protocols. The protocols are running on a secure processor on-chip, interfacing with a host using an API across a trusted SPI peripheral. It provides secure EEPROM Boot, using SPI pass-through technology that allows Titan to confirm authorship of Boot Code, ensuring code-signing before code swap is completed.

This version of the Titan Chip (referred to as “Titan-D”) has a single-chip embodiment and is utilized by Google’s IN762 FIPS 140-2 validated cryptographic modules as a source of entropy.

2. Security Level

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall Level	1

Table 2 - Security Levels

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The cryptographic boundary is the outer perimeter of the chip shown in the below figure. The device is a single-chip module embodiment as defined by FIPS 140-2. The hardware version of the module is H1D3P.

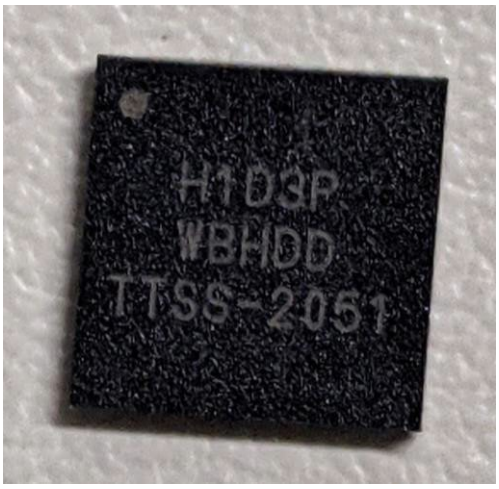

Figure 1 - Titan Chip (Front)

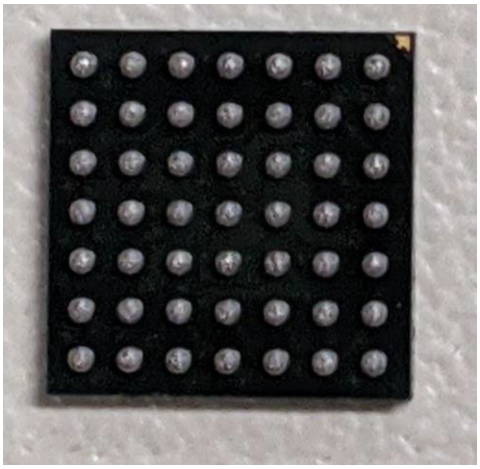

Figure 2 - Titan Chip (Back)

The physical boundary is depicted in the block diagram below:

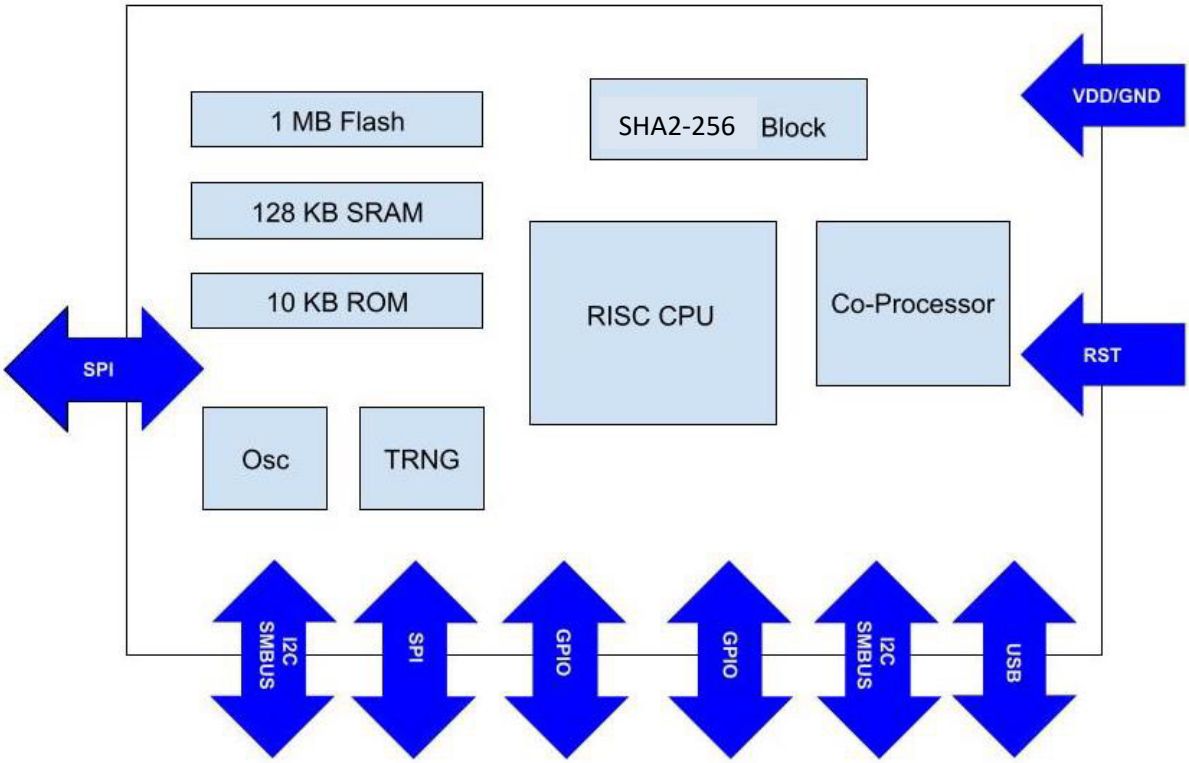

Figure 3 - Titan Chip Block Diagram

The embedded chip contains the following hardware components:

- RISC-V processor;
- Co-processor;
- Non-volatile FLASH memory;
- Volatile RAM memory;
- Read-Only memory;
- True-Random Number Generator (TRNG);
- Internal Oscillator; and
- Hardware-based SHA/HMAC engine.

4. Cryptographic Module Ports and Interfaces

The module contains an SPI master and an SPI slave interface. The master interface is used to initiate flash commands to an external EEPROM, and the slave interface is used to receive commands initiated from an external Network Interface Card (NIC).

Physical Port	# of Pins	FIPS 140-2 Logical Interface Mapping	Description
VDD	3	Power	Supply Voltage
RST	2	Control in	Reset Signal
GND	4	Power	Ground
SPS	4	Data in, Data out, Control in, Status out	SPI slave from Host device
SPI	6	Data in, Data out	SPI master to external EEPROM, plus write-protect and hold signals
USB	2	Data in, Data out, Control in, Status out	Connected to host device
I2C / SMBUS	2	Data in, Data out, Control in, Status out	Operates as SMBUS slave; Connected to host device
SMBUS	2	Data in, Data out, Control in, Status out	Operates as SMBUS slave; Connected to NIC
DEBUG_ACTIVE (GPIO)	1	Status in	Status bit from NIC (whether NIC is in debug mode)
BOOTSTRAP (GPIO)	1	Control in	Set to Bootstrap module during initialization[1]
GOOD (GPIO)	1	Status out	Status bit
UART TX	1	Status out	Debug log
GPIO	16	Not used	Not used
VDD	3	Power	Supply Voltage
RST	2	Control in	Reset Signal
GND	4	Power	Ground
UART PROXY TX	2	Data out	Commands received from SPI, USB, or SMBUS can be used to proxy arbitrary data through these pins.
UART PROXY RX	2	Data in	Data received from these pins can be read using commands on the SPI, USB, or SMBUS.

Physical Port	# of Pins	FIPS 140-2 Logical Interface Mapping	Description
			Cannot be used to command any cryptographic operations inside Titan-D.

Table 3 - Physical Port and Logical Interface Mapping

[1] This pin is disabled in the production environment when the module is deployed.

5. Roles, Services and Authentication

5.1 Roles

There are two roles in the module that an operator may assume: A Crypto Officer (CO) role and a User role. Roles are assumed implicitly based on the service accessed. The module does not provide any operator identification or authentication. Since the device does not provide any identification or authentication services, the level of access granted to any functionality of the module is implicitly determined by the service calling the module; the device itself makes no determination about the role itself.

A mapping of the services available to a CO and a User are shown in Table 4 below.

5.2 Services

The module provides the following Approved services which utilize algorithms listed in Table 6, 7 and 8:

Service	User	Crypto Officer
Initialization	✓	✓
On-Demand Self-test	✓	✓
Zeroization		✓
Query Module Status/Show Status	✓	✓
Write request to SPI Staging Partition	✓	✓
Activate Staging Partition	✓	✓
Check Status of Partitions	✓	✓
Check for Firmware Update[2]	✓	✓
Perform Firmware Update		✓
Provide Conditioned Entropy Output	✓	✓
Reset	✓	✓
SPI Read Request from External storage	✓	✓
SPI Write request to Titan-D Firmware Staging Region on External storage	✓	✓
SPI Write request to target configuration region of the active partition of External storage	✓	✓

[2] Note: Only validated firmware versions shall be loaded using the firmware update service.

Table 4 - Approved Services and Role allocation

The module provides the following non-Approved services which utilize algorithms listed in Table 7:

Service
Firmware Attestation
Non-Approved Wrapping/Unwrapping

Table 5 - Non-Approved Services and Role allocation

5.3 Authentication

There is no operator authentication; assumption of role is implicit by the used service(s).

6. Physical Security

The module is a single-chip cryptographic module made with production grade components and standard IC packaging material.

7. Operational Environment

The module does not provide a general-purpose operating system.

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

The module implements the following approved algorithms in the bootloader, operational firmware and in hardware:

CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
A4586	ECDSA (firmware)	P-256	FIPS 186-4	Signature Verification SHA2-256	Signature Verification
A1863	SHS (hardware)	256	FIPS 180-4	SHA2-256	Hashing, Signature Verification
A4586	SHS (firmware)	256	FIPS 180-4	SHA2-256	Hashing, Signature Verification
A4586	HMAC (firmware)	256	FIPS 198-1	HMAC-SHA2-256	Message Authentication
A4586	RSA (firmware)	2048-bit, 3072-bit, and 4096-bit	FIPS 186-4	Signature Verification SHA2-256	Signature Verification
ENT (P)	N/A (hardware)	256	NIST SP 800-90B	Generated entropy: 256 bits Entropy per source output bit: 0.79	Conditioned entropy output
A1863[3]	SHS	256	NIST SP 800-90B	SHA2-256	Conditioned entropy output

Table 6 - Approved Algorithms

Note: Additional algorithms were CAVP tested but are not being utilized by the module in the Approved mode of operation.

8.1.1 Non-Approved Algorithms

The following non-Approved cryptographic functions are implemented in the module:

[3] SHA2-256 implementation is utilized as the unkeyed conditioning component for the TRNG.

Algorithm	Use
KBKDF (non-conformant)	Key-Based Key Derivation Function
RNG (non-conformant)	Random Number Generation
AES 256-bits (CTR mode) (non-conformant)	Encryption and Decryption
ECDSA (non-conformant)	Signature Generation and Verification
HKDF (non-conformant)	HMAC-based Key Derivation Function
ECIES	Elliptic Curve Integrated Encryption Scheme
RSA (non-conformant)	Signature Verification
HMAC (non-conformant)	Generation, Authentication

Table 7 - Non-Approved Algorithm

8.2 Cryptographic Key Management

The module implements the following access control policy on keys in the module shown in the following table. The Access Policy is noted by R=Read, W=Write and X=Execute.

Module Service	Key	Rights (R/W/X)
Initialization	N/A	N/A
On-Demand Self-test	N/A	N/A
Zeroization	N/A	N/A
Query Module Status/Show Status	N/A	N/A
Activate Staging Partition	N/A	N/A
Check Status of Partitions	EEPROM Firmware Verification Key	R / X
Check for Firmware Update	EEPROM Firmware Verification Key	R / X
Perform Firmware Update	Firmware Verification Key	R / X
Provide Conditioned Entropy Output	Firmware Verification Key	R / X
Reset	N/A	N/A
SPI Read Request to Active Partition of External storage	N/A	N/A

SPI Write request to Firmware Staging Region on External storage	N/A	N/A
Write request to SPI Staging Partition on External storage	N/A	N/A

Table 8 - Approved Service to Key/CSP Mapping

The following public keys are utilized by the module:

Public Keys	Description	Algorithm and Key Size	Generation	Input / Output Method	Storage
EEPROM Firmware Verification Key	Used to verify EEPROM firmware of IN762 modules[4] during update	RSA 3072-bit key[5]	Loaded at factory	Never exits the module	Flash
Firmware Verification Key	Used to verify module firmware updates	ECDSA P-256 key	Loaded at factory	Never exits the module	Flash
TRNG Entropy Output	Conditioned Entropy output	ENT (P)	TRNG	Exits the module via the SPI interface	SRAM

Table 9 - Public Keys

8.3 Key Generation and Entropy

The module does not generate cryptographic keys as part of its Approved services. The module implements a hardware-based True-Random Number Generator (TRNG). The TRNG is used to generate conditioned entropy which is output as a service to the directly connected Integrated Management Complex (IMC) and B227 True Random Number Generator (TRNG) module.

8.4 Zeroization

The contents of the module's volatile memory are zeroized on-demand by power cycling the module. (Removing power from the host device where the chip is inserted).

The output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

[4] External to the Titan-D cryptographic boundary

[5] While additional RSA sizes were algorithm tested, the module only supports 3072-bit keys.

9. Self-tests

FIPS 140-2 requires the module to perform self-tests to ensure the module integrity and the correctness of the cryptographic functionality at startup. Some functions require conditional tests during normal operation of the module.

If any of the tests fail, the module will return an error code and transition to an error state where no functions can be executed. An operator to restart the module, however, the failure of a self-test may require the chip to be replaced.

9.1 Power-On Self-Tests

Power-on self-tests are always run upon the initialization of the module and do not require operator intervention to run. If any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the operator.

The module implements the following power-on self-tests:

Type	Test
Integrity Test	• SHA2-256 EDC over the bootloader image and executable firmware image
Known Answer Test	• HMAC (Keyed Hash. HMAC-SHA2-256) • ECDSA (signature verification. Curve: P-256) • RSA (signature verification. 2048-bit) • SHS (Firmware Implementation. SHA2-256) • SHS (Hardware Implementation. SHA2-256)
Health Tests on Noise Source	• Adaptive Proportion Test (APT) • Repetition Count Test (RCT)

Table 10 - Power-up Self-tests

The module performs all power-on self-tests automatically when it is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by power-cycling the module.

9.2 Conditional Self-Tests

Conditional self-tests are tests that run during operation of the module. Each module performs the following conditional self-tests:

Type	Test Description
Firmware Load Test	• ECDSA Signature Verification operation performed prior to a firmware upgrade.
Continuous Health Tests on Noise Source	• Adaptive Proportion Test (APT) • Repetition Count Test (RCT)

Table 11 - Conditional Self-tests

10. Guidance and Secure Operation

No configuration of the module or installation steps are required from the operator. When the module is powered on its power-up self-tests are executed without any operator intervention. The module enters the Approved mode of operation automatically if the power-up self-tests complete successfully. If any of self-tests fail during power-up, the module will transition to an error state. The status of the module can be determined by the availability of the module. If the module is available, it has passed all self-tests. If it is unavailable, it is in the error state.

Use of the non-conformant algorithms listed in Table 7 will place the module in a non-approved mode of operation.

11. Glossary

Term	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
CLK	Clock
CMVP	Cryptographic Module Validation Program
CCCS	Canadian Centre for Cyber Security
CSP	Critical Security Parameter
CTR	Counter-Mode
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EEPROM	Electrically Erasable Programmable Read-Only Memory
GND	Ground
GPIO	General Purpose Input/ Output
HKDF	HMAC-based Key Derivation Function
HMAC	(Keyed-) Hash Message Authentication Code
KDF	Key-Derivation Function
NIST	National Institute of Standards and Technology
RAM	Random Access Memory
RSA	Rivest Shamir Adleman
RST	Reset
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SPI	Serial Peripheral Interface
SPS	Standby Power Supply
SRAM	Static Random-Access Memory
TRNG	True-Random Number Generator
UART	Universal Asynchronous Receiver-Transmitter

USB	Universal Serial Bus
VDD	Voltage Drain Drain

Table 12 - Glossary of Terms