Non-Proprietary FIPS 140-2 Security Policy

Google LLC.

Cr50 U2F Cryptographic Library

Firmware version: 1.0.1

Hardware version: H1B2P

Date: September 19, 2023

Prepared By:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Introduction

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. NVLAP accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates modules meeting FIPS 140-2 validation requirements. Validated is the term given to a module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html

About this Document

This non-proprietary Cryptographic Module Security Policy for the Cr50 u2F Cryptographic Library 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.

The Cr50 u2F Cryptographic Library 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

Introduction 2

Disclaimer 2

Notices 2

1. Introduction 5

   1.1 Scope 5

   1.2 Overview 5

2. Security Level 5

3. Cryptographic Module Specification 6

   3.1 Cryptographic Boundary 6

4. Modes of Operation 8

5. Cryptographic Module Ports and Interfaces 8

6. Roles, Services and Authentication 8

7. Physical Security 10

8. Operational Environment 10

9. Cryptographic Algorithms and Key Management 11

   9.1 Cryptographic Algorithms 11

   9.2 Non-Approved Algorithms 11

   9.3 Cryptographic Key Management 12

   9.4 Key Generation 12

   9.5 Key Storage and Zeroization 13

10. Self-tests 13

   10.1 Power-On Self-Tests 13

   10.2 Conditional Self-Tests 14

   10.3 Critical Function Tests 14

11. Mitigation of Other Attacks 14

12. Crypto Officer and User Guidance 14

13. Glossary 15

List of Tables

Table 1- Security Level 5

Table 2- Physical Port and Logical Interface Mapping 8

Table 3– Approved Services, Roles and Access Rights 9

Table 4– non-Approved or non-security relevant services 9

Table 5 - Approved Algorithms in firmware 11

Table 6- Approved Algorithms in hardware 11

Table 7- Non-Approved Algorithms 11

Table 8- Approved Keys and CSPs 12

Table 9- Power-On Self-Tests 13

Table 10 - Conditional Self-Tests 14

Table 11 - Glossary of Terms 15

List of Figures

Figure 1- GSC Chip Physical Boundary (Front) 6

Figure 2 - GSC Chip Physical Boundary (Back) 6

Figure 3– Cr50 Cryptographic Library Boundary Block 7

Figure 4- Tamper Evidence and damage to the module 10

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Google LLC. Cr50 u2F Cryptographic Library firmware-hybrid module. It contains a 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.

1.2 Overview

The Cr50 U2F Cryptographic Library is a firmware-hybrid module residing in the Google LLC Google Security Chips (GSC) (Hardware Version: H1B2P) chip (Single-Chip embodiment). The GSC contains an ARM V7-M CPU which the firmware runs on. The module is responsible for low-level cryptographic primitives on Google Security Chips (GSC) used in recent versions of Google Chromebooks. The module's functionality is focused on primitives required to implement the FIDO2/WebAuthn Authenticator model. This standard permits users to log into internet accounts using their Chromebooks with Cr50 U2F with physical presence verification.

Cr50 is the Chrome Operating System firmware running on the GSC chip which is considered a non-modifiable operational environment. The firmware portion of the module can utilize full hardware algorithm implementations in the GSC chip for hashing, keyed-hashing and big-number operations in its Approved mode of operation.

The module performs Approved key generation, signature generation, random bit generation, keyed-hashing and signature verification operations in support of U2F-related requests in Cr50.

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	3
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 1- Security Level

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The cryptographic boundary is the outer perimeter of the chip shown in the below figure. The physical embodiment is a single-chip module as defined by FIPS 140-2. The hardware version of the GSC chip is H1B2P.

Figure 1- GSC Chip Physical Boundary (Front)

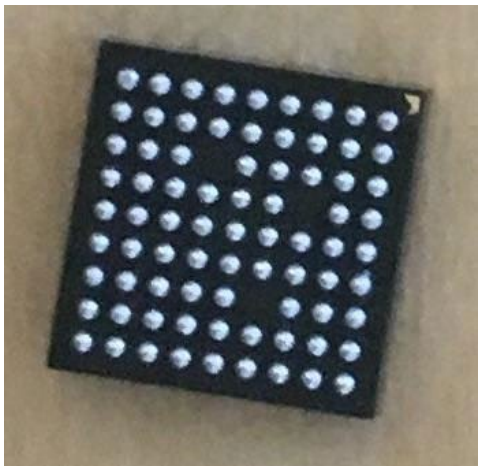

Figure 2 - GSC Chip Physical Boundary (Back)

The logical boundary is depicted in the block diagram below:

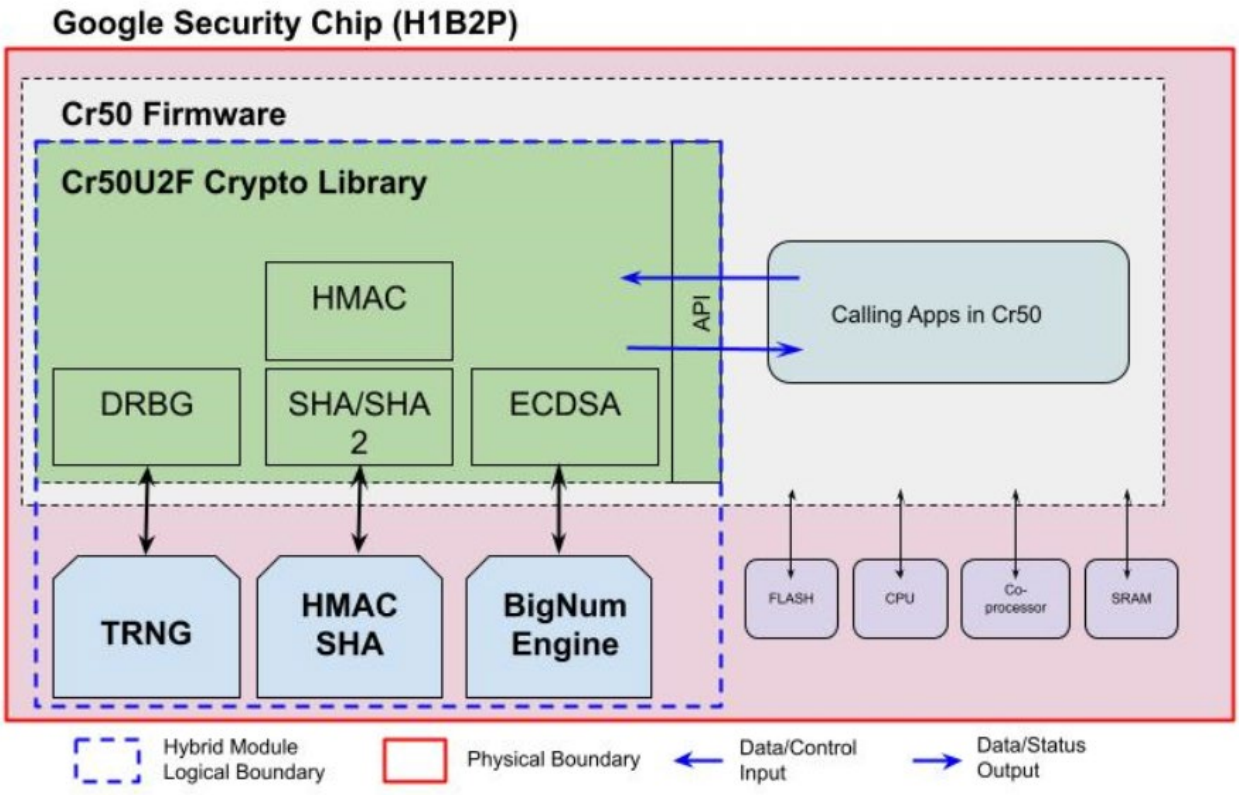

Figure 3– Cr50 Cryptographic Library Boundary Block

4. Modes of Operation

The module supports two modes of operation: Approved and Non-Approved. The module will be in FIPS-approved mode when all power up Self-Tests have completed successfully, and only Approved or allowed algorithms are invoked. See Table 5 and 6 (below) for a list of the supported Approved algorithms. The non-Approved mode is entered when a non-Approved algorithm is invoked. See Table 7 for a list of non-Approved algorithms.

5. Cryptographic Module Ports and Interfaces

The module provides the following number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Interface	Physical Port/Interface	Module Interface (API)
Data Input	Assigned pins to USB, I2C, SPI, UART and GPIO on the H1B2P chip	API input parameters
Data Output	Assigned pins to USB, I2C, SPI, UART and GPIO on the H1B2P chip	API output parameters and return values
Control Input	Assigned pins to USB, I2C, SPI, UART and GPIO on the H1B2P chip	API input parameters
Status Output	Assigned pins to USB, I2C, SPI, UART and GPIO on the H1B2P chip	API return values
Power Input	Assigned pins to USB, I2C, SPI, UART and GPIO on the H1B2P chip	N/A

Table 2- Physical Port and Logical Interface Mapping

As a firmware-hybrid module, control of the physical pins on the GSC chip is outside the module scope. When the module is performing self-tests, or is in an error state, all output on the module's logical data output interfaces and access to the cryptographic functions in hardware are inhibited.

6. Roles, Services and Authentication

The cryptographic module implements both User and Crypto Officer (CO) roles. The module does not support user authentication. The User and CO roles are implicitly assumed by the entity accessing services implemented by the module. A user is considered the owner of the thread that instantiates the module and, therefore, only one concurrent user is allowed.

The Approved services supported by the module and access rights within services accessible over the module's public interface are listed in the table below:

Service	Approved security functions	Keys and/or CSPs	Roles	Access rights to keys and/or CSPs
Module Initialization	N/A	N/A	CO	N/A
Keyed hashing	HMAC-SHA-256	HMAC key	User, CO	Execute
Hashing	SHA-256	None	User, CO	N/A

Service	Approved security functions	Keys and/or CSPs	Roles	Access rights to keys and/or CSPs
Signature generation/ verification	ECDSA (P-256)	ECDSA public and private key	User, CO	Write/Execute
Key Generation	ECDSA (P-256)	ECDSA public and private key	User, CO	Write/Execute
Attestation	ECDSA (P-256)	ECDSA private key	User, CO	Write/Execute
Generate and Sign U2F Certificate	ECDSA (P-256)	ECDSA private key	User, CO	Write/Execute
Random Bit Generation	TRNG	HMAC_DRBG	User, CO	Write/Execute
On-Demand Self-test	N/A	N/A	User, CO	Execute
Zeroization	N/A	All keys	User, CO	Write/Execute
Show status	N/A	N/A	User, CO	N/A

Table 3– Approved Services, Roles and Access Rights

The module provides the following non-Approved services which utilize algorithms listed in Table 4:

Service	Non-Approved Functions	Keys and/or CSPs
Symmetric encryption/decryption	AES (non-compliant)	N/A
Authenticated Symmetric encryption/decryption	AES GCM (non-compliant)	N/A
Wegman-Carter polynomial hashing	Ghash (non-compliant)	N/A
Signature generation/ verification	RSA (non-compliant)	N/A
Key Encapsulation (asymmetric encryption/decryption)	RSA (non-compliant)	N/A
Key Generation	RSA (non-compliant)	N/A
Hashing (TPM2)	SHA1/SHA2-384/SHA2-512	N/A

Table 4– non-Approved or non-security relevant services

7. Physical Security

The module is a single-chip cryptographic module which meets the requirements for opacity and tamper evidence. The module is encased in removal-resistant IC packaging material which cannot be removed or penetrated without causing serious damage to the module (i.e. the module will not function). The physical security mechanism is a hard, opaque packaging.

The module hardness testing was performed at a single ambient temperature of 72 °F. No assurance is provided for Level 3 hardness conformance at any other temperatures.

Figure 4- Tamper Evidence and damage to the module

8. Operational Environment

The module's operational environment (Cr50) is non-modifiable. The module does not contain a mechanism to update its firmware.

9. Cryptographic Algorithms and Key Management

9.1 Cryptographic Algorithms

The module implements the following approved algorithms in the firmware:

CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
Vendor Affirmed	CKG	N/A	SP 800-133r2	N/A	Seed for asymmetric key pair generation with B=U.
A2353	ECDSA	P-256	FIPS 186-4	Signature Generation Component, Key Pair Generation, Signature Generation, Signature Verification	Digital Signature Services
	HMAC	256-bits	FIPS 198-1	HMAC-SHA-256	Generation, Authentication
	SHS	256-bits	FIPS 180-4	SHA-256	Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications
	DRBG	HMAC-SHA-256	SP 800-90Arev1	HMAC_DRBG	Random Bit Generation

Table 5 - Approved Algorithms in firmware

The module implements the following approved algorithms in the hardware:

CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
N/A	TRNG	P	NIST SP 800-90B	ENT	Entropy source utilized for random bit generation
A2352	SHS	256-bits	FIPS 180-4	SHA-256	Digital Signature Generation, Digital Signature Verification, Conditioning Function, non-Digital Signature Applications
	HMAC	256-bits	FIPS 198-1	HMAC-SHA-256	Generation, Authentication

Table 6- Approved Algorithms in hardware

9.2 Non-Approved Algorithms

The following non-approved usages are associated with the legacy PIN encryption/decryption service and TPM2 hashing service listed in Table 4.

Algorithm	Use
AES (non-conformant)	Encryption and Decryption
EC DH (non-conformant)	Key Agreement (P-256)
RSA (non-conformant)	Key Generation; Signature generation/ verification; Key Encapsulation (asymmetric encryption/decryption)
SHS (non-conformant)	Message digest TPM2 (SHA-1, SHA-384, SHA-512)

Table 7- Non-Approved Algorithms

9.3 Cryptographic Key Management

The module supports the following CSPs listed below in Table 5. The CSP access policy is denoted in Table 3 above.

Keys and CSPs	Description	Algorithm and Key Size	Generation / Input	Output	Storage
U2F Entropy Input (Stored Seed)	Entropy to seed DRBG upon initial instantiation	512 bits	Internally generated.	Output via API in plaintext	FLASH
U2F HMAC key	MAC for authentication of key handles	HMAC SHA-256	Internally generated.	Output via API in plaintext	FLASH
Device ID for u2F	Device unique key	HMAC SHA-256	Internally generated.	Output via API in plaintext	FLASH
ECDSA Public/ Private key pair	Signing key per user/ origin	ECDSA P-256	Internally generated.	Output via API in plaintext	RAM
Entropy Input (direct from TRNG)[1]	Entropy to seed DRBG after first instantiation	576-bits	Input via API in plaintext	Does not exit the module	RAM
System DRBG State	V and Key values	256-bits	Internally generated.	Does not exit the module	RAM

Table 8- Approved Keys and CSPs

9.4 Key Generation

The module includes an SP 800-90A Approved DRBG. The module requests a minimum of 256-bits of entropy from the entropy source for use in key generation. The module generates symmetric keys in accordance with IG D.12 and SP 800-133rev2, Section 4.

The Approved DRBG seeded by an SP 800-90B conformant entropy source. The module retrieves entropy from a physical (ENT-P) noise source residing inside the physical boundary in alignment with Scenario 1 (b) described in FIPS 140-2 IG 7.14. The module also implements a factory-derived entropy pool consistent with IG 7.14 2(a) which is filled from an entropic source at manufacturing time prior to shipping. An estimated 512-bits of full entropy is loaded at the factory.

[1] Per SP 800-90B, the initial entropy estimate of a binary noise source is calculated as HI=min(Horiginal, Hsubmitter). As a result, HI=min(0.80, 0.79) = 0.79.

9.5 Key Storage and Zeroization

The cryptographic module does not perform persistent storage of keys. Keys and CSPs are passed to the module by the calling application. The keys and CSPs are stored in memory in plaintext. Keys and CSPs residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the module defined API. The operating system protects memory and process space from unauthorized access.

All private or secret keys are zeroized either at session termination or by power-cycling the module. 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 module's data output interface when keys are zeroized.

10. Self-tests

FIPS 140-2 requires the module to perform self-tests to ensure the integrity of the module and the correctness of the cryptographic functionality at start up. Some functions require conditional tests during normal operation of the module. The supported tests are listed and described in this section.

10.1 Power-On Self-Tests

Power-on self-tests for both the hardware and firmware algorithm implementations are 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.

The module implements the following power-on self-tests in the Cr50 u2F Cryptographic Library:

Type	Test Description
Integrity Test	• SHA-256 hash over the executable firmware image
Known Answer Test	• ECDSA (Signature Generation and Verification. Curve: P-256) • HMAC (Generation and Verification with SHA-256) • SHS (SHA-256) • SP 800-90 HMAC_DRBG KAT including SP 800-90A Health Tests, required per IG C.1

Table 9- Power-On Self-Tests

The Power-on self-tests can be run on demand by rebooting the module or by issuing the "on-demand self-test command via the module's API.

10.2 Conditional Self-Tests

Conditional self-tests are run during operation of the module. If any of these tests fail, the module will enter an error state, where no services can be accessed by the operators. The module can be re-initialized to clear the error and resume FIPS mode of operation. Each module performs the following conditional self-tests:

Type	Test Description
Pair-wise Consistency Test	ECDSA Key Pair generation
SP 800-90B Health Tests	Adaptive proportion test and repetition count test performed on startup, on demand and continuously.

Table 10 - Conditional Self-Tests

10.3 Critical Function Tests

The module does not implement any specific critical function tests.

11. Mitigation of Other Attacks

No specific claims for this section.

12. Crypto Officer and User Guidance

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, and only Approved or allowed algorithms are invoked. The non-Approved mode is entered when a non-Approved algorithm is invoked. See Table 7 for a list of non-Approved algorithms.

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 or has not been properly initialized.

13. Glossary

Acronym	Definition
ADB	Android Debug Bridge
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CCCS	Canadian Centre for Cyber Security
CFB	Cipher Feedback
CKG	Cooperative Key Generation
CMVP	Crypto Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EC	Elliptic Curve
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
EC DH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Authority
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
HMAC	Key-Hashed Message Authentication Code
IG	Implementation Guidance
KAT	Known Answer Test
LLC	Limited Liability Company
N/A	Not-Applicable
NIST	National Institute of Standards and Technology
NDRNG	Non-Deterministic Random Number Generator
NVLAP	National Voluntary Lab Accreditation Program
RAM	Random Access Memory
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication

Table 11 - Glossary of Terms