Google LLC

Google Tensor 5th Gen UFS Inline Storage Encryption Engine

FIPS 140-3 Non-Proprietary Security Policy

Prepared for:

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759

Document Version 1.1
Date: May 2026

Table of Contents

1 General 6
1.1 Overview 6
1.2 Security Levels 6
2 Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 9
2.6 Security Function Implementations 10
2.7 Algorithm Specific Information 11
2.7.1 AES-XTS 11
2.8 RBG and Entropy 11
2.9 Key Generation 11
2.10 Key Establishment 11
2.11 Industry Protocols 11
3 Cryptographic Module Interfaces 12
3.1 Ports and Interfaces 12
4 Roles, Services, and Authentication 13
4.1 Authentication Methods 13
4.2 Roles 13
4.3 Approved Services 13
4.4 Non-Approved Services 14
4.5 External Software/Firmware Loaded 14
5 Software/Firmware Security 15
5.1 Integrity Techniques 15
5.2 Initiate on Demand 15
6 Operational Environment 16
6.1 Operational Environment Type and Requirements 16
6.2 Configuration Settings and Restrictions 16
7 Physical Security 17
7.1 Mechanisms and Actions Required 17
8 Non-Invasive Security 18

9 Sensitive Security Parameters Management 19
9.1 Storage Areas 19
9.2 SSP Input-Output Methods 19
9.3 SSP Zeroization Methods 19
9.4 SSPs 19
10 Self-Tests 21
10.1 Pre-Operational Self-Tests 21
10.2 Conditional Self-Tests 21
10.3 Periodic Self-Test Information 21
10.4 Error States 22
10.5 Operator Initiation of Self-Tests 22
11 Life-Cycle Assurance 23
11.1 Installation, Initialization, and Startup Procedures 23
11.2 Administrator Guidance 23
11.3 Non-Administrator Guidance 23
11.4 End of Life 23
12 Mitigation of Other Attacks 24
Appendix A. Glossary and Abbreviations 25
Appendix B. References 26

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 9
Table 3: Tested Module Identification – Hybrid Disjoint Hardware 9
Table 4: Tested Operational Environments - Software, Firmware, Hybrid 9
Table 5: Modes List and Description 9
Table 6: Approved Algorithms 10
Table 7: Security Function Implementations 10
Table 8: Ports and Interfaces 12
Table 9: Roles 13
Table 10: Approved Services 14
Table 11: Mechanisms and Actions Required 17
Table 12: Storage Areas 19
Table 13: SSP Input-Output Methods 19
Table 14: SSP Zeroization Methods 19
Table 15: SSP Table 1 19
Table 16: SSP Table 2 20
Table 17: Pre-Operational Self-Tests 21
Table 18: Conditional Self-Tests 21
Table 19: Pre-Operational Periodic Information 22
Table 20: Conditional Periodic Information 22
Table 21: Error States 22

List of Figures

Figure 1: Flash Component THGJFJT1E45BATP (left) and Google Tensor 5th Gen SoC (right) 8
Figure 2: Block Diagram 8

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Google Tensor 5th Gen UFS Inline Storage Encryption Engine. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for a Security Level 1 cryptographic module.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

1.2 Security Levels

The following sections describe the cryptographic module and how it conforms to the FIPS 140-3 specification in each of the required areas.

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 Google Tensor 5th Gen UFS Inline Storage Encryption Engine Cryptographic Module (hereafter referred to as "the module") is a firmware-hybrid module in a multi-chip embodiment.

The module is composed of a hardware block that performs AES-XTS encryption and a firmware driver which performs key checking operations and loads keys into hardware. The module facilitates File-Based Encryption (FBE) using hardware-based keys for the platform which implements it.

Module Type: Firmware-hybrid

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

The block diagram shown in Figure 2 shows the design of the module when the module is operational and the firmware components are loaded into DDR. The cryptographic boundary consists of the components colored orange. Green dashed lines show the flow of information into and out of the cryptographic module through the interfaces defined in Section 3.1 Ports and Interfaces. Orange lines show the flow of data within the cryptographic boundary.

The UFS ISE box corresponds to the hardware component of the module which contains the AES-XTS implementation. The kdn-fips box corresponds to the firmware component of the module which provisions keys to the hardware component.

Tested Operational Environment's Physical Perimeter (TOEPP):

The tested operational environment's physical perimeter encloses the Google Tensor 5th Gen SoC and the flash storage, and is denoted by a purple dotted line in Figure 2. The Google Tensor 5th Gen SoC and the flash component are shown in Figure 1.

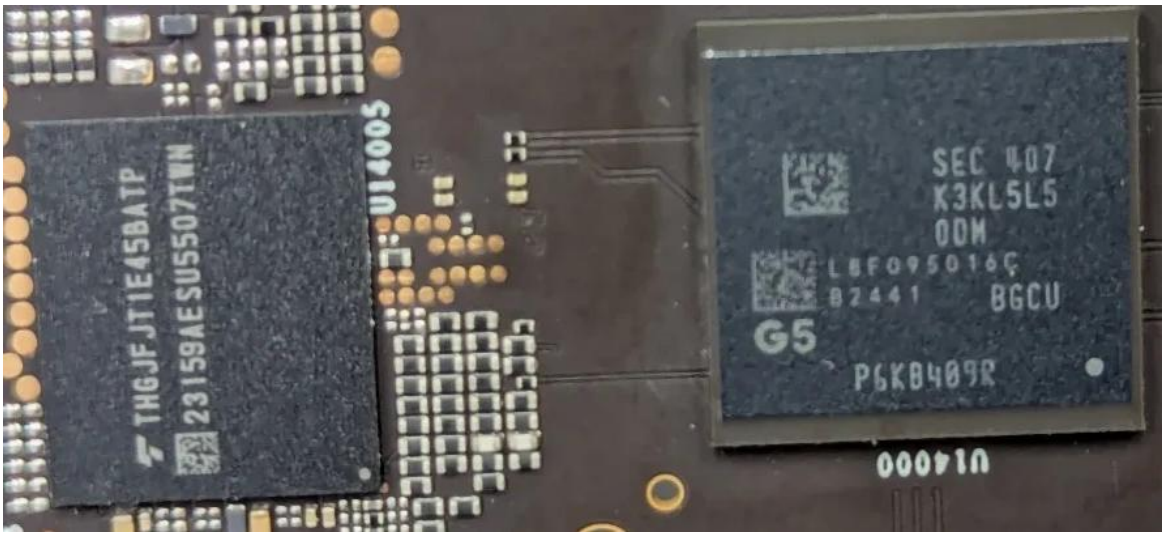

Figure 1: Flash Component THGJFJT1E45BATP (left) and Google Tensor 5th Gen SoC (right)

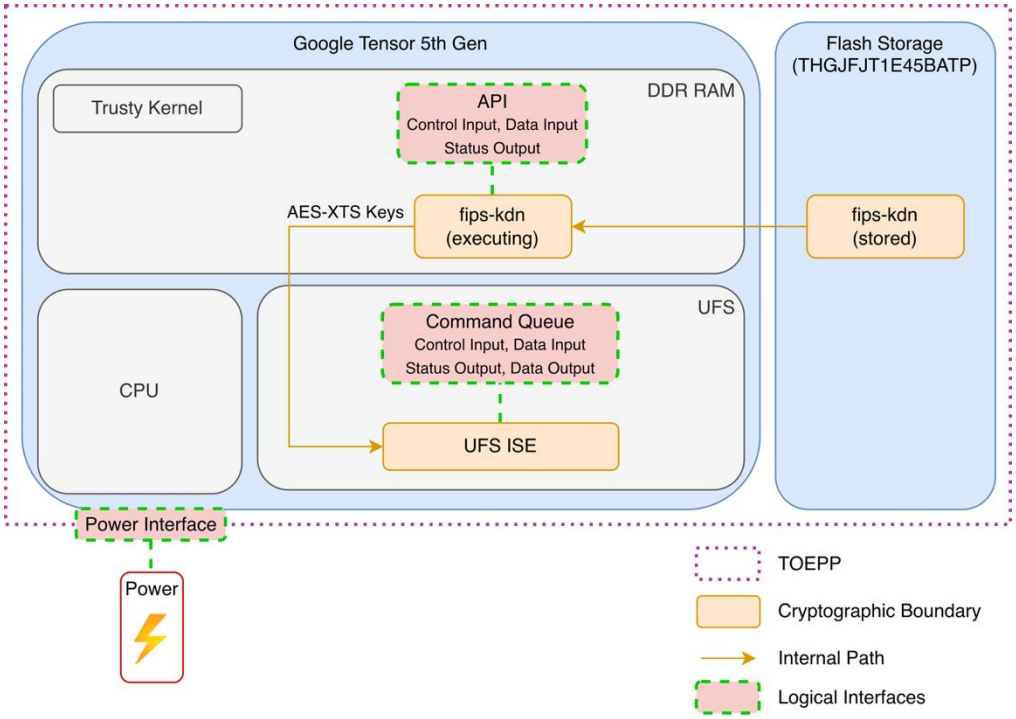

Figure 2: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fips-kdn	13544274	N/A	HMAC-SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Single Chip: Google Tensor; Sub-Chip Disjoint Hardware: UFS ISE	Single Chip Version: 5th Gen; Sub-Chip Disjoint Hardware Version: 1.1	N/A	N/A	N/A

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Trusty	Google Tensor 5th Gen + Flash THGJFJT1E45BATP	Google Tensor 5th Gen	No	N/A	13544274

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

There are no components excluded from the requirements of the FIPS 140-3 standard.

2.4 Modes of Operation

Modes List and Description:

The module supports only the approved mode of operation. When the module starts up successfully, after passing all the pre-operational self-tests and conditional cryptographic algorithm self-tests (CASTs), the module is operating in the approved mode of operation.

Mode Name	Description	Type	Status Indicator
Approved Mode	Automatically entered after pre-operational self-tests have passed	Approved	Successful completion of service

Table 5: Modes List and Description

2.5 Algorithms

Approved Algorithms:

The table below lists the approved algorithms implemented by the module, as well as the associated CAVP certificates.

Algorithm	CAVP Cert	Properties	Reference
AES-XTS Testing Revision 2.0	A7008	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
HMAC-SHA2-256	A7009	Key Length - Key Length: 256	FIPS 198-1

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

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
Symmetric Encryption	BC-UnAuth	Symmetric encryption to support data storage. Disjoint Components that contribute to this SFI: UFS ISE		AES-XTS Testing Revision 2.0: (A7008)
Symmetric Decryption	BC-UnAuth	Symmetric decryption to support data storage. Disjoint Components that contribute to this SFI: UFS ISE		AES-XTS Testing Revision 2.0: (A7008)
MAC for Integrity Test	MAC	MAC calculation for integrity test. Disjoint components that contribute to this SFI: fips-kdn		HMAC-SHA2-256: (A7009)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES-XTS

AES-XTS is only approved for storage purposes.

The length of a single data unit encrypted with AES-XTS shall not exceed 2^{20} AES blocks, that is, 16MB of data.

The module implements a check to ensure that the two AES keys used in AES-XTS are not identical. Per IG C.I, AES-XTS Key_1 and Key_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3, for an approved use of AES-XTS.

2.8 RBG and Entropy

The module does not implement or utilize a random number generator and does not contain an entropy source.

2.9 Key Generation

The module does not provide any key generation services.

2.10 Key Establishment

The module does not provide any key establishment services.

2.11 Industry Protocols

The module does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The ports and interfaces implemented in the module are shown in the table below. No Control Output interface is present in the table as no such interface is implemented in the module.

Physical Port	Logical Interface(s)	Data That Passes
N/A	Control Input	API calls to firmware
N/A	Data Input	Keys
N/A	Data Output	Module name and version
N/A	Status Output	Return codes from firmware API
Command Queue	Control Input	Control signals for hardware
Command Queue	Data Input	Input data to be encrypted/decrypted
Command Queue	Data Output	Output data that has been encrypted/decrypted
Error Status Register	Status Output	Module error status
Power Pin	Power	N/A

Table 8: Ports and Interfaces

Communication between the firmware component and the disjoint hardware component of the module is considered as controlled communication because the Trusty TEE (which is the module's operational environment) is designed to separate this communication from the rest of the peripherals outside of the module's cryptographic boundary.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 9: Roles

The module does not support concurrent operators.

4.3 Approved Services

The following convention is used to specify access rights to a SSP:

- **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 = Zeroize**: The module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Set Key	Write AES key to hardware registers. Provided by fips-kdn and UFS ISE	Implicit (Successful completion of service)	AES-XTS key	None	None	Crypto Officer - AES-XTS key: W
Symmetric Encryption	Symmetric Encryption for storage applications. Provided by UFS ISE	Implicit (Successful completion of service)	Plaintext	Ciphertext	Symmetric Encryption	Crypto Officer - AES-XTS key: E
Symmetric Decryption	Symmetric Decryption for storage applications. Provided by UFS ISE	Implicit (Successful completion of service)	Ciphertext	Plaintext	Symmetric Decryption	Crypto Officer - AES-XTS key: E
Show Status	Return the module status. Provided by fips-kdn	None	None	Module status	None	Crypto Officer
Show Version	Return the module name and version information.	None	None	Module version	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Provided by fips-kdn and UFS ISE					
Self-Test	Perform the CASTs and integrity test. Provided by fips-kdn and UFS ISE	None	None	Pass or Fail	Symmetric Encryption Symmetric Decryption MAC for Integrity Test	Crypto Officer
Zeroization	Zeroize all unprotected SSPs. Provided by fips-kdn and UFS ISE	None	None	None	None	Crypto Officer - AES-XTS key: Z

Table 10: Approved Services

4.4 Non-Approved Services

The module does not implement any non-approved services.

4.5 External Software/Firmware Loaded

The module does not support the loading of external software/firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the firmware component of the module is verified by comparing a HMAC-SHA2-256 value calculated on the fips-kdn binary with the HMAC-SHA2-256 value stored in the fips-kdn binary that was computed at build time. The key used for HMAC-SHA2-256 is hard-coded in the fips-kdn firmware.

5.2 Initiate on Demand

The integrity test is performed as part of the pre-operational self-tests, which are executed when the module is initialized. The integrity test may be invoked on demand by power cycling the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The module operates in a limited operational environment (Trusty TEE) within the Google Tensor 5th Gen SoC. SSPs are never transported through or stored in shared memory.

6.2 Configuration Settings and Restrictions

No configuration of the operational environment is required for the module to operate in an approved mode. Therefore, there are no rules, settings, or restrictions to the configuration of the operational environment.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Opaque sealing coat	No actions are required to maintain the physical security of the module	No actions are required to maintain the physical security of the module

Table 11: Mechanisms and Actions Required

At the time of manufacture, the SoC containing the UFS hardware and the flash storage component are individually covered by production-grade opaque sealing coats which provide standard passivation. The two components are further embedded within a mobile phone platform, which provides the production-grade enclosure for physical security purposes.

8 Non-Invasive Security

The module does not implement any non-invasive security measures.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The module does not perform persistent storage of SSPs. All SSPs are temporarily stored in registers within the module in plaintext form.

Storage Area Name	Description	Persistence Type
Key Registers	Registers used explicitly for key storage within UFS ISE which are inaccessible outside hardware.	Dynamic
RAM	Temporary storage for SSPs used by the module as part of service execution.	Dynamic

Table 12: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API Input Parameters	Operator calling application (TOEPP)	RAM	Plaintext	Manual	Electronic	

Table 13: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Module Reset	Registers and RAM quickly lose their stored values upon power-off.	Volatile memory in registers requires constant power to maintain state so all state is immediately lost upon power-off. RAM used by the module is overwritten within nanoseconds when power is removed.	By power-cycling the module

Table 14: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES-XTS key	AES-XTS key used for data encryption/decryption	512 bits - 256 bits	Symmetric Key - CSP			Symmetric Encryption Symmetric Decryption

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-XTS key	API Input Parameters	Key Registers:Plaintext RAM:Plaintext	Key Registers: until explicitly removed or the module powers off; RAM: until deallocated and overwritten or the module powers off	Module Reset	

Table 16: SSP Table 2

10 Self-Tests

The module performs pre-operational and conditional cryptographic algorithm self-tests automatically between power-on and the first operational use. These self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

While the module is executing the pre-operational and the conditional cryptographic algorithm self-tests, services are not available, and all data output is inhibited. The module is not available for use by the calling application until the self-tests are completed successfully. If any of the self-tests fail, an error message is returned and the module transitions to an error state.

10.1 Pre-Operational Self-Tests

The module performs a pre-operational firmware integrity test automatically before the first operational use of the module. The HMAC-SHA2-256 KAT is performed immediately before the integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A7009)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A

Table 17: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Each KAT involves comparing the calculated output of a cryptographic algorithm with a known answer hardcoded into the module. The AES-XTS KATs are automatically performed by the hardware component at power-on, while the HMAC-SHA2-256 KAT is performed prior to the integrity test specified in Section 10.1.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A7008) - Encryption	512-bit key	KAT	CAST	Module becomes operational	Encryption	Test runs at power on
AES-XTS Testing Revision 2.0 (A7008) - Decryption	512-bit key	KAT	CAST	Module becomes operational	Decryption	Test runs at power on
HMAC-SHA2-256 (A7009)	SHA2-256	KAT	CAST	Module becomes operational	MAC	Before integrity test

Table 18: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A7009)	MAC tag verification	SW/FW Integrity	On Demand	Manually

Table 19: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A7008) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A7008) - Decryption	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7009)	KAT	CAST	On Demand	Manually

Table 20: Conditional Periodic Information

10.4 Error States

If the module fails any pre-operational or conditional self-test, the module will enter an error state. Any further cryptographic operation is inhibited and the module will not respond to service requests. The Crypto Officer can recover from the error state by restarting the hardware platform on which the module is running.

Name	Description	Conditions	Recovery Method	Indicator
Firmware Error	Error occurred in fips-kdn firmware	CAST failure Integrity test failure AES-XTS key check error (both halves are equal)	Reboot module	Module stops functioning and responds to all service requests with status indicating the module is in error state.
Hardware Error	Error occurred in UFS ISE hardware	CAST failure	Reboot module	Module stops functioning. Error Status register is high.

Table 21: Error States

10.5 Operator Initiation of Self-Tests

On-demand self-tests can be invoked by powering off and reloading the module which causes the module to run the pre-operational and conditional cryptographic algorithm self-tests.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

In order for the module to be installed in conformance with the rules in this Security Policy, the device must be configured to run in “fips mode”. This configuration can be performed by running the following commands:

- fastboot oem fips enable
- fastboot -w

The first command will set the device to enter “fips mode” upon the next factory reset, and the second command performs the factory reset.

11.2 Administrator Guidance

There is no administrator guidance for the module.

11.3 Non-Administrator Guidance

There is no non-administrator guidance for the module.

11.4 End of Life

The module does not persistently store SSPs. Therefore, the secure sanitization of the module consists of unloading the module by powering off the device in which it is embedded. This will zeroize all SSPs present in hardware and volatile memory.

12 Mitigation of Other Attacks

The module does not implement any additional attack mitigation mechanisms.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standards
FW	Firmware
HW	Hardware
ISE	Inline Storage Encryption
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
UFS	Universal Flash Storage
SHA	Secure Hash Algorithm
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS 140-3 IG	**Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program** April 18, 2025 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 198-1	**The Keyed-Hash Message Authentication Code (HMAC)** July 2008 https://doi.org/10.6028/NIST.FIPS.198-1
SP 800-38E	**Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality of Storage Devices** January 2010 https://doi.org/10.6028/NIST.SP.800-38E