

Google LLC

Google Tensor 6th 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 1.0
Date: September 21, 2026

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 9
2.7 Algorithm Specific Information 9
2.7.1 AES-XTS 10
2.8 RBG and Entropy 10
2.9 Key Generation 10
2.10 Key Establishment 10
2.11 Industry Protocols 10
3 Cryptographic Module Interfaces 11
3.1 Ports and Interfaces 11
4 Roles, Services, and Authentication 12
4.1 Authentication Methods 12
4.2 Roles 12
4.3 Approved Services 12
4.4 Non-Approved Services 13
4.5 External Software/Firmware Loaded 13
5 Software/Firmware Security 14
5.1 Integrity Techniques 14
5.2 Initiate on Demand 14
6 Operational Environment 15
6.1 Operational Environment Type and Requirements 15
7 Physical Security 16
7.1 Mechanisms and Actions Required 16
8 Non-Invasive Security 17
9 Sensitive Security Parameters Management 18

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.1 Storage Areas 18
9.2 SSP Input-Output Methods 18
9.3 SSP Zeroization Methods 18
9.4 SSPs 18
10 Self-Tests 19
10.1 Pre-Operational Self-Tests 19
10.2 Conditional Self-Tests 19
10.3 Periodic Self-Test Information 19
10.4 Error States 19
10.5 Operator Initiation of Self-Tests 20
11 Life-Cycle Assurance 21
11.1 Installation, Initialization, and Startup Procedures 21
11.2 Administrator Guidance 21
11.3 Non-Administrator Guidance 21
11.4 End of Life 21
12 Mitigation of Other Attacks 22
Appendix A. Glossary and Abbreviations 23
Appendix B. References 24

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 9
Table 5: Security Function Implementations 9
Table 6: Ports and Interfaces 11
Table 7: Roles 12
Table 8: Approved Services 13
Table 9: Mechanisms and Actions Required 16
Table 10: Storage Areas 18
Table 11: SSP Input-Output Methods 18
Table 12: SSP Zeroization Methods 18
Table 13: SSP Table 1 18
Table 14: SSP Table 2 18
Table 15: Conditional Self-Tests 19
Table 16: Conditional Periodic Information 19
Table 17: Error States 20

List of Figures

Figure 1: Google Tensor 6th Gen SoC 7
Figure 2: Block Diagram 8

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Google Tensor 6th Gen UFS Inline Storage Encryption Engine (ISE). 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	N/A
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

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Google Tensor 6th Gen UFS Inline Storage Encryption Engine Cryptographic Module (hereafter referred to as "the module") is a sub-chip hardware module in a single-chip embodiment.

The module is composed of a hardware block that performs AES-XTS encryption. The module facilitates File-Based Encryption (FBE) using hardware-based keys for the platform which implements it.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The block diagram shown in Figure 2 shows the design of the module when the module is operational. The Tested Operational Environment's Physical Perimeter consists of the Google Tensor 6th Gen SoC, while 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.

Tested Operational Environment's Physical Perimeter (TOEPP):

The tested operational environment's physical perimeter is the Google Tensor 6th Gen SoC, shown in Figure 1.



Figure 1: Google Tensor 6th Gen SoC

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

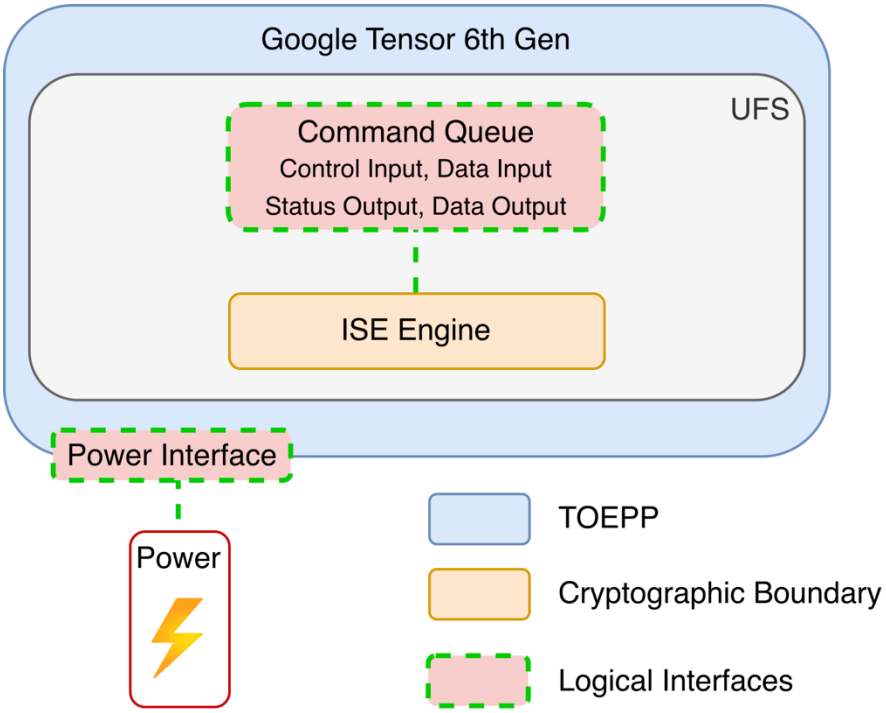


Figure 2: Block Diagram

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
Google Tensor 6th Gen ISE engine	1.2	N/A	N/A	N/A

Table 2: Tested Module Identification – Hardware

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 conditional cryptographic algorithm self-tests (CASTs), the module is operating in the approved mode of operation.

Mode Name	Description	Type	Status Indicator
Approved Mode	Implicit approved mode of operation always assumed by the module	Approved	Successful completion of service

Table 3: Modes List and Description

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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	A8177	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 128 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E

Table 4: 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-UnAuthEncrypt	Symmetric encryption to support data storage		AES-XTS Testing Revision 2.0: (A8177)
Symmetric Decryption	BC-UnAuthDecrypt	Symmetric decryption to support data storage		AES-XTS Testing Revision 2.0: (A8177)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.7.1 AES-XTS

AES-XTS is only approved for storage purposes. Per IG C.I, AES-XTS Key_1 and Key_2, when entered into the module by the operator, **shall** be generated and/or established independently of each other according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3 for an approved use of AES-XTS.

The AES algorithm in XTS mode can only be used for the cryptographic protection of data on storage devices, as specified in SP 800-38E. The length of a single data unit encrypted with AES-XTS shall not exceed 2^{20} AES blocks, that is, 16MB of data. To meet the requirement in FIPS 140-3 IG C.I, the module implements a check to ensure that the two AES keys used in AES-XTS are not identical.

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.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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
Command Queue	Control Input	Control signals for hardware
Command Queue	Data Input	Input data to be encrypted/decrypted, keys
Command Queue	Data Output	Output data that has been encrypted/decrypted
Status Registers	Status Output	Module status, module name/version
Power Pin	Power	N/A

Table 6: Ports and Interfaces

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 7: 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	Implicit (Successful completion of service)	AES-XTS key	None	None	Crypto Officer - AES-XTS key: W
Symmetric Encryption	Symmetric Encryption for storage applications	Implicit (Successful completion of service)	Plaintext	Ciphertext	Symmetric Encryption	Crypto Officer - AES-XTS key: E
Symmetric Decryption	Symmetric Decryption for storage applications	Implicit (Successful completion of service)	Ciphertext	Plaintext	Symmetric Decryption	Crypto Officer - AES-XTS key: E
Show Status	Status returned per service	None	Service request	Success or failure	None	Crypto Officer
Show Version	Return the module name and version information	None	None	Module version	None	Crypto Officer

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-Test	Perform CASTs	None	None	Pass or Fail	Symmetric Encryption Symmetric Decryption	Crypto Officer
Zeroization	Zeroize all unprotected SSPs	None	None	None	None	Crypto Officer - AES-XTS key: Z

Table 8: 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.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The Google Tensor 6th Gen UFS Inline Storage Encryption Engine is implemented entirely in hardware. This section is therefore not applicable.

5.2 Initiate on Demand

The Google Tensor 6th Gen UFS Inline Storage Encryption Engine is implemented entirely in hardware. This section is therefore not applicable.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

The Google Tensor 6th Gen UFS Inline Storage Encryption Engine is a single-chip hardware module. The operational environment is therefore considered non-modifiable.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 9: Mechanisms and Actions Required

The module is a sub-chip enclosed in the SoC listed in Table 2. The platform is made of production-grade components which conform to the Level 1 requirements for physical security.

At the time of manufacture, the SoC is embedded in within a printed circuit board (PCB), preventing visibility into the internal circuitry of the module. The module is further protected by being enclosed in a commercial off-the-shelf mobile device which completely surrounds the module.

There are no steps required to ensure that physical security is maintained.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

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

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

Table 10: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Key Input	Caller within TOEPP	Key Registers	Plaintext	N/A	N/A	

Table 11: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Module Reset	Registers 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.	By power-cycling the module

Table 12: 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 13: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-XTS key	Key Input	Key Registers:Plaintext	Until explicitly removed or the module powers off	Module Reset	

Table 14: SSP Table 2

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

The module performs conditional cryptographic algorithm self-tests automatically between power-on and the first operational use. These self-tests ensure that the cryptographic algorithms work as expected.

While the module is executing 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 caller until the self-tests are completed successfully. If any of the self-tests fail, an error signal is raised and the module transitions to an error state.

10.1 Pre-Operational Self-Tests

The module does not contain any software or firmware, and so does not perform a pre-operational integrity test. Instead, the conditional tests enumerated in the following section are performed prior to the module becoming operational.

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 module at power-on.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A8177) - Encryption	512-bit key	KAT	CAST	Module becomes operational	Encryption	Test runs at power on
AES-XTS Testing Revision 2.0 (A8177) - Decryption	512-bit key	KAT	CAST	Module becomes operational	Decryption	Test runs at power on

Table 15: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A8177) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A8177) - Decryption	KAT	CAST	On Demand	Manually

Table 16: Conditional Periodic Information

10.4 Error States

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

If the module fails any 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
Error	Error occurred in UFS ISE hardware	CAST failure	Reboot module	Module stops functioning. Error Status register is high.

Table 17: 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 conditional cryptographic algorithm self-tests.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module does not require any installation, initialization, or startup procedures.

11.2 Administrator Guidance

The "Show version" service can be invoked by reading the contents of the HSIOS_UFS_VERSION_ufs_major_version_in and HSIOS_UFS_VERSION_ufs_minor_version_in registers. The major version register should hold the value 1, and the minor version register should hold the value 2, matching the module version given in Section 2.2 Tested and Vendor Affirmed Module Version and Identification. The presence of those values in those registers identifies the module as the Google Tensor 6th Gen UFS Inline Storage Encryption Engine.

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.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

The module does not implement any additional attack mitigation mechanisms.

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standards
ISE	Inline Storage Encryption
KAT	Known Answer Test
NIST	National Institute of Science and Technology
UFS	Universal Flash Storage
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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**
February 27, 2026
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

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

© 2026 Google LLC, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.