Non-Proprietary FIPS 140-2 Security Policy

Google, LLC.

Look-aside Cryptography and Compression Engine (LCE)

Hardware version: 3.0

Firmware version: FW 6172

Date: 23/05/2024

Prepared By:

EWA-Canada, An Intertek Company

1223 Michael St., Suite 200

Ottawa, Ontario, Canada

K1J 7T2

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. 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 (SP) for Look-aside Cryptography and Compression Engine (LCE) 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 Look-aside Cryptography and Compression Engine may also be referred to as “LCE” or 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. Cryptographic Module Ports and Interfaces 8
5. Roles, Services and Authentication 8
5.1 Roles 8
5.2 Services 9
5.3 Authentication 9
6. Physical Security 9
7. Operational Environment 10
8. Cryptographic Algorithms and Key Management 10
8.1 Cryptographic Algorithms 10
8.2 Cryptographic Key Management 12
8.3 Key Generation and Entropy 12
8.4 Key Storage and Zeroization 12
9. Self-Tests 13
9.1 Power-On Self-Tests 13
9.2 Conditional Self-Tests 14
9.3 Critical Function Tests 14
10. Mitigation of Other Attacks 14
11. Crypto Officer and User Guidance 14
11.1 Usage of AES GCM in the module 14
12. Glossary 16

List of Tables

Table 1 - Security Level 5
Table 2 - Cryptographic Module Ports and Interfaces 8
Table 3 - Approved Services and Role allocation 9
Table 4 - Non-security Relevant Services and Role allocation 9
Table 5 - Approved Algorithms 11
Table 6 - Approved Algorithms (Bound Module) 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 16

List of Figures

Figure 1 - LCE Block Diagram 6

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Google LLC. Look-aside Cryptography and Compression Engine (LCE) (Hardware Version: 3.0; Firmware Version: FW 6172) (also referred to as the "module" hereafter).The module environment is IN762 SoC C1. It contains specifications of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

1.2 Overview

LCE provides look-aside cryptography and compression services. Cryptography services provided by LCE include bulk encryption, cryptographic hashing, Integrity Checksum Value (ICV) verification, and compression services. LCE supports operation chaining including cryptographic and pipeline compressing/decompressing and verification as well as standalone or combined DMA data (payload) transfers between nodes.

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 1 - Security Level

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

LCE is a hardware module. The physical boundary of the module is the single-chip physical embodiment of the IN762 SoC. The module's logical boundary is the firmware and hardware functionality contained within the LCE IP Block at the sub-chip level. The module only supports one mode of operation where only Approved cryptographic functions and services are available. The cryptographic boundary of the module and the relationship among the various internal components of the module are depicted in Figure 1 below.

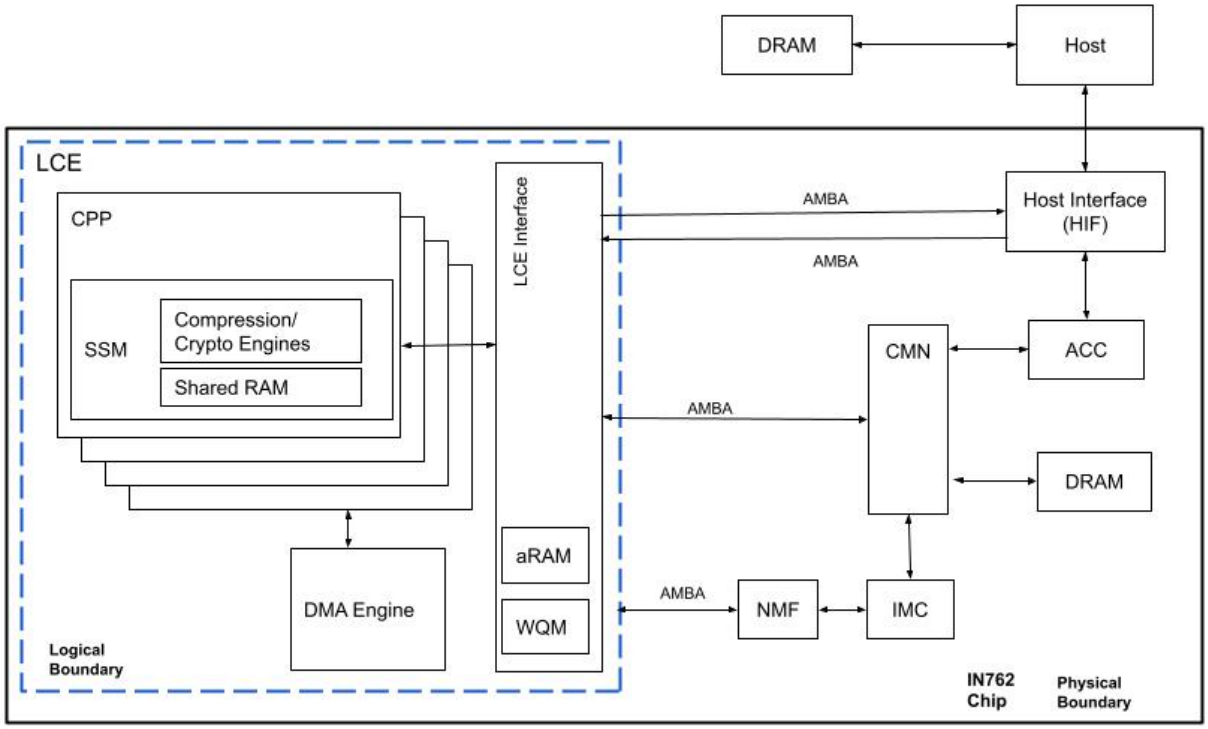

Figure 1 - LCE Block Diagram

The module provides lookaside hardware acceleration for bulk encryption and compression operations, including AES (XTS, GCM, CTR, GMAC), HMAC, and SHA-1, SHA-2 and SHA-3 cryptographic algorithms as well as zStandard and Snappy compression algorithms[1] and CRC for ICV checksum calculation.

Within the LCE IP block are four Command Push/Pull Clusters (CPP) which implement an internal interface to a Shared Slice & Memory Module (SSM) component. Each "slice" represents a compression/ cryptography engine. Additionally, the SSM implements the shared RAM for the slices. Additionally, the module contains a DMA engine (acting as a "master"), and a LCE Interface block providing an AXI4 endpoint, accelerator RAM (aRAM), and a Work Queue Manager (WQM). The WQM within the LCE Interface block provides Queue Pairs implementing a Request and Response Queue. Request descriptors are placed into Request queues by the ARM Compute Complex (ACC) or from the Host CPU through the Host Interface (HIF) and Response descriptors are placed in the Response queues. The DMA engine uses

[1] Non-approved but allowed per IG 1.23

data in the request descriptors to copy data from the on-chip or external DRAM to the internal Shared RAM to be processed and ultimately returned via response descriptor.

The module also includes firmware which is loaded into aRAM and subsequently loaded onto the DMA engine for execution. The firmware implements the following functions:

- queue management,
- state management,
- general-purpose functions including compression and DMA services,
- known-answer test logic for cryptographic algorithms,
- error handling, and
- diagnostic functions.

The module is connected to other subsystems via an AMBA on-chip system bus. Through the AXI4 interfaces the module provides access to Control/Status Registers (CSR), a Push Interface, Request Interface, and Compression Interface. The CSR is used for device initialization, heartbeat information, and firmware loading via the Network Management Fabric (NMF). The Push Interface is used to doorbell the device when a job is placed in a ring buffer (via HIF), and provides pointers to a request descriptor. The Request Interface is used by LCE to read data (request descriptors, key/IVs, configuration data, and payload data) and write data (response descriptors, processed payloads) to external RAM (either on the Host or attached to the ACC via HIF). The Compression Interface is an interface used to monitor state information and reads/writes data to be processed (compressed) via the Coherency Mesh Network (CMN).

DMA reads/writes to external RAM occur via the HIF. As necessary to satisfy IG 1.20, intervening circuitry must not pose any risk to modification or interception of CSPs or other types of attacks. The HIF is a standard PCI Express (PCIe) device. Queues within LCE are associated with a specific bus device function. Each queue has a specific function ID. By design, the requests must use a defined PCIe channel. This separation is maintained by the Address Translation Engine within the host CPU's Input-Output Memory Management Unit (IOMMU), or the System Memory Management Unit within the ACC. If a request is made for the wrong function ID, it will be treated as an unsupported request and will fail.

The module is validated for use with the IMC and B227 True Random Number Generator (TRNG) Firmware-Hybrid Cryptographic Module (FIPS 140-2 Cert. #4400) which employs firmware running inside the IMC. The IMC Secure Firmware is required to perform the firmware integrity test/firmware load test on the LCE firmware image prior to initialization.

4. 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:

Physical Port	Ports	Description
Data Input	AMBA (On-chip system bus)	Request interface DMA reads from on-chip DRAM or external DRAM via HIF (key/IV, payloads) Compression interface reads (via CMN) CSR writes from NMF (firmware load)
Data Output	AMBA (On-chip system bus)	Request Interface DMA writes to on-chip DRAM or external DRAM via HIF (processed data) Compression interface writes (via CMN)
Control Input	AMBA (On-chip system bus)	CSR writes from the NMF (initialization) Request interface DMA reads via HIF (request descriptors) Push Interface (doorbell)
Status Output	AMBA (On-chip system bus)	CSR status output to the NMF (self-heartbeat information, interrupts, self-test status) Request interface DMA writes via HIF (response descriptors)
Power Input	Physical power connector	Provides power to the module

Table 2 - Cryptographic Module Ports and Interfaces

5. Roles, Services and Authentication

5.1 Roles

The module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both User and Crypto Officer (CO) roles. The User and CO roles are implicitly assumed by the entity accessing services implemented by the module. No operator authentication is implemented. The module also supports concurrent operators.

5.2 Services

The module provides the following Approved services which utilize algorithms listed in Table 5:

Service	Roles		CSP	CSP Access
	User	CO		R = Read W = Write X = Execute
Payload Encryption using AES-GCM, CTR, XTS[2]	✓	✓	Cipher-Auth-Key	R, X
Payload Decryption using AES-GCM, CTR, XTS	✓	✓	Cipher-Auth-Key	R, X
Payload Authentication using AES-GMAC and HMAC	✓	✓	Cipher-Auth-Key (GMAC) HMAC-Auth-Key (HMAC)	R, X
Hashing - SHA-1, SHA-2, and SHA-3 message digest	✓	✓	N/A	N/A
Self-Test (executed automatically on reset)	✓	✓	N/A	N/A
Initialization	✓	✓	N/A	N/A
Zeroization (executed automatically on reset)	✓	✓	All keys	W
Status Output	✓	✓	N/A	N/A

Table 3 - Approved Services and Role allocation[3]

The module provides the following non-security relevant services allowed for use in an Approved mode:

Service	Description	Roles		CSP	CSP Access
		User	CO		R = Read W = Write X = Execute
Compression	Snappy/zStandard	✓	✓	N/A	N/A
DMA	CRC function on DMA reads/writes	✓	✓	N/A	N/A

Table 4 - Non-security Relevant Services and Role allocation

5.3 Authentication

There is no operator authentication. Assumption of role is implicit by the used service(s). The User and CO roles have access to all module services. There is no separation of role access.

6. Physical Security

LCE is a sub-chip module implemented as part of the IN762 SoC, which is the physical boundary of the sub-chip module. The IN762 SoC is a single chip with a production grade enclosure and hence conforms to the Level 1 requirements for physical security.

[2] Utilized in storage applications only.

[3] Encryption/Decryption, Authentication, and Compression services may be performed in conjunction or as standalone functions.

7. Operational Environment

The module is a sub-chip cryptographic subsystem implemented within a single-chip hardware embodiment which includes firmware. The procurement builds and configuration procedure are controlled by the manufacturer. Therefore, the operational environment is considered non-modifiable.

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

The module implements the following approved algorithms:

LCE Algorithm Implementation					
ACVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
A683	AES-ECB	128, 256-bits	SP 800-38A	ECB	Encryption, Decryption
	AES-CTR	128, 256-bits	SP 800-38A	CTR	Encryption, Decryption
	AES-GCM	128, 256-bits	SP 800-38D	GCM	Encryption, Decryption
	AES-GMAC	128, 256-bits	SP 800-38D	GMAC	Authentication
	AES-XTS	128, 256 bits	SP 800-38E	XTS	Encryption, Decryption
	SHS	160, 224, 256, 384, 512 bits	FIPS 180-4	SHA-1[4], SHA2-224 SHA2-256, SHA2-384, SHA2-512	Message Digest
	SHA-3	224, 256, 384, 512 bits	FIPS 202	SHA3-224, SHA3-256, SHA3-384, SHA3-512	Message Digest
	HMAC	160, 224, 256, 384, 512 bits	FIPS 198-1	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2- 256, HMAC-SHA2-384, HMAC-SHA2-512	Authentication

[4] Used within HMAC-SHA-1 only.

LCE Algorithm Implementation					
ACVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
	HMAC-SHA-3	224, 256, 384, 512 bits	FIPS 202	HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	Authentication

Table 5 - Approved Algorithms

The following algorithms are implemented by the bound IMC module (CMVP Cert #4400)

IMC Algorithm Implementation					
ACVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
A2469	AES	256-bits	SP 800-38B	CMAC	Message Authentication

Table 6 - Approved Algorithms (Bound Module)

The module implements the following non-approved but allowed algorithms per IG 1.23 Scenario 2 where no security is claimed:

Algorithm	Description
Snappy	Compression Algorithm
zStandard	Compression Algorithm
CRC	Cyclic Redundancy Check

Table 7 - Non-Approved Algorithms (No Security Claimed)

8.2 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 Method	Storage	Zeroization
Cipher-Auth Key	Encryption and decryption (and optionally authentication) of payload passed to LCE.	AES-GCM, GMAC, CTR, XTS 128,256-bit value	N/A	Retrieved from on-chip or external DRAM via DMA. Never exits the module	Shared RAM	On LCE reset
HMAC-Auth Key	Authentication of payload passed to LCE	HMAC-SHA1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	N/A	Retrieved from on-chip or external DRAM via DMA. Never exits the module	Shared RAM	On LCE reset
GCM Initialization Vector	IV used for GCM encryption/ decryption	N/A	Deterministic per section 8.2.1 of SP 800-38D	N/A	Shared RAM	On LCE reset

Table 8 - Approved Keys and CSPs

8.3 Key Generation and Entropy

The module does not provide any key generation service or perform key generation for any of its Approved algorithms. The external host or ACC software writes requests to a ring buffer and doorbells the device when a key is to be loaded onto the device. The request descriptors (originating from Host CPU or ACC) provide the location for keys and payload data and the module in turn fetches the keys and payloads from external DRAM via DMA. For encryption operations, the IV is generated and output to DRAM (via DMA) to the address specified in the request descriptor. For decryption, the IV is retrieved from DRAM (via DMA).

The cryptographic module does not provide any asymmetric algorithms or key establishment methods.

8.4 Key Storage and Zeroization

LCE does not provide any persistent key storage. All CSPs are stored in internal shared RAM. Once the keys are written to shared RAM, they are not readable from outside the module. The shared RAM is zeroized upon reset, which may be performed via the System Control block (SYSCON) within the IMC.

While this action will clear all secrets internal to LCE, it will also leave the module in a non-usable state as standalone reset is not supported. This process will result in returning the module to its default state.

9. Self-Tests

FIPS 140-2 requires self-tests to ensure the correctness of the cryptographic functionality at start-up. If any of the tests fail, the module will not initialize, and any data output is inhibited. In this state, limited control requests are processed and only status output is returned.

An operator can attempt to recover from the error state by resetting the chip. However, the failure of a self-test may require the module to be replaced.

9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run.

Each algorithm engine is tested, and the result of the test is placed in a register. If any status bit in the register indicates a failure, it will enter the CRYPTO_DISABLE state at which point the module halts all services with the exception of limited control input.

If the Firmware Integrity Test fails, the module will not be initialized and will remain in an uninitialized state until the bound IMC cryptographic module can successfully re-initialize the device.

The module implements the following power-on self-tests in the LCE Cryptographic Module:

Type	Test Description
Firmware Integrity Test (AES-CMAC)	• Performed by IMC (FIPS 140-2 Cert. #4400)
AES-GCM (256) Encrypt/Decrypt KAT	• AES-GCM forward cipher Known Answer Test
AES-CTR (256) Encrypt/Decrypt KAT	• AES-CTR forward cipher Known Answer Test
AES- XTS (256) Encrypt/Decrypt KAT	• AES-XTS forward/inverse cipher Known Answer Test
HMAC-SHA-1 KAT	• HMAC SHA-1 Known Answer Test
HMAC-SHA-2 (256, 512) KAT	• HMAC SHA-2 Known Answer Test
HMAC-SHA-3 (256, 512) KAT	• HMAC-SHA-3 Known Answer Test

Table 9 - Power-On Self-Tests

The module performs all power-on self-tests automatically when it is initialized. Power-on self-tests must pass before a User/CO can perform services. The Power-on self-tests can be run on demand by resetting the module.

9.2 Conditional Self-Tests

Conditional self-tests are run under specific conditions, such as during XTS encryption (per IG A.9) or firmware loading.

Type	Test Description
Key Equality Check (Encrypt)	• Prior to loading an entered XTS key, the module verifies that Key1!=Key2
Key Equality Check (Decrypt)	• Prior to loading an entered XTS key, the module verifies that Key1!=Key2
Firmware Load Test (AES-CMAC)	• Performed by IMC (FIPS 140-2 Cert. #4400). 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 140-2 validation

Table 10 - Conditional Self-Tests

If either of the Key Equality Checks fail, the individual "slice" where the error occurred will halt execution, an error is returned and no payload data is written back from the device. However, the module will not enter an error state, rather the encryption or decryption request will fail, and the module will continue to process payload encryptions if the subsequent keys are valid and not equal.

If the Firmware Load Test fails, the module will not be initialized and will remain in a hard error state until the bound IMC cryptographic module can successfully re-initialize the device.

9.3 Critical Function Tests

The module does not implement any specific critical function tests.

10. Mitigation of Other Attacks

No specific claims for this section.

11. 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 is not considered to be in the Approved mode of operation until the firmware image has been successfully verified by the bound IMC cryptographic module. The modules' cryptographic functions will only be available after all self-tests have passed successfully. If any of the self-tests fail the module will transition to an error state.

11.1 Usage of AES GCM in the module

The Initialization Vector (IV) used by LCE is considered a CSP. The IV is constructed deterministically per section 8.2.1 of SP 800-38D. GCM IV construction is performed within the LCE boundary in accordance to FIPS IG A.5 scenario 4 using a deterministic method. The IV is constructed using a 32-bit salt allowing for 2^{32} possible values and 64-bit counter value to form a 96 bit IV.

Per the requirements specified in Section 8 in NIST SP 800-38D, the probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct

sets of input data is no greater than 2^{-32}.

The maximum operating rate of the LCE encryption engine is 25MPPS[5]. Operating at full capacity, it would take 23,300 years before a counter reset, thus, the module would cease operation prior to exhausting the 2^64 counter values.

If power is removed from the module, a new key and IV are generated as there is no persistent memory of the last IV used.

[5] Mega(million) packet per second

12. Glossary

Term	Description
AES	Advanced Encryption Standard
AMBA	ARM Microcontroller Bus Architecture
aRAM	Accelerator Random Access Memory
AXI	Advanced Extensible Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CSR	Control/Status Register
CTR	Counter Mode
DMA	Direct Memory Access
ERoT	External Root of Trust
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
HIF	Host Interface
HMAC	Hashed Message Authentication Code
IG	Implementation Guidance
IMC	Integrated Management Complex
KAT	Known answer test
LCE	Lookaside Compression and Cryptography Engine
PCIe	Peripheral Component Interconnect (PCI) Express
SHA	Secure Hash Algorithm
SoC	System On Chip
SSM	Shared RAM and Slice Module
WQM	Workload Queue Manager
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Table 11 - Glossary of Terms