Non-Proprietary FIPS 140-2 Security Policy

Google LLC

Inline Crypto Engine (ICE)

Hardware version: 1.0

Date: 6/6/2022

Prepared By:

intertek
acumen
security

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. 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 Inline Crypto Engine (ICE) 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 Inline Crypto Engine may also be referred to as “ICE” 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

This document may be freely reproduced and distributed in its entirety without modification.

Public Material – May be reproduced only in its original entirety (without revision).

Table of Contents

Public Material – May be reproduced only in its original entirety (without revision).

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Google LLC. Inline Crypto Engine (ICE) (Hardware Version: 1.0) (also referred to as the "module" hereafter). 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 Inline Crypto Engine (ICE) module is comprised of a sub-chip cryptographic subsystem in the Google IN762 B0 System On Chip (SoC). The module provides a cryptographic engine supporting cryptographic offload for Internet Protocol Security (IPsec) and Paddywhack Security Protocol (PSP) protocols. The ICE module processes network infrastructure packets in both the Ingress and Egress directions. In addition to providing the cryptographic primitives for the security protocols it also provides packet integrity authentication and anti-replay protection.

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

Public Material – May be reproduced only in its original entirety (without revision).

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The physical boundary of the module is the single-chip physical embodiment of the IN762 B0 SoC. The module's logical boundary is the hardware-based functionality contained within the ICE IP[1] Block and ECQ 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.

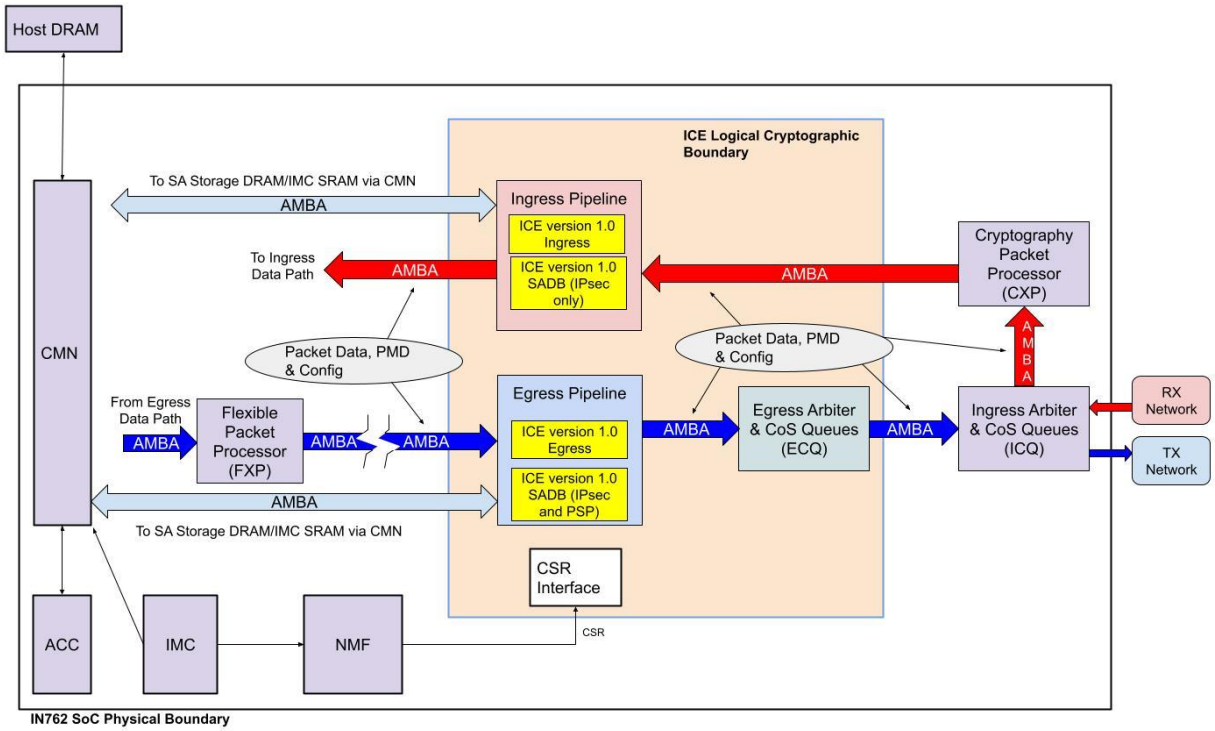

Figure 1 - ICE Block Diagram

The module consists of the ICE sub-chip cryptographic subsystem within the IN762 B0 SoC which includes the Ingress and Egress Pipelines and Egress Arbiter and Class of Service (CoS) Queues (ECQ). Security protocol processing and cryptography services performed by the module include full data-plane protocol termination for IPsec ESP[2], and PSP. ESP is implemented using AES-GCM and AES-GMAC. PSP supports AES-GCM only. The module also includes a KBKDF used for PSP key derivation.

Within the ICE IP block are an Ingress and Egress Pipeline. The Ingress and Egress Pipelines each contain a GCM/GMAC encryption/decryption and authentication engine (identified as ICE Ingress and ICE Egress, respectively). ICE Ingress also contains a KBKDF implementation. In addition, the Ingress and Egress

[1] Hard circuitry core

[2] Note that data plane functionality represents the second-phase IPSec SA payload encryption. The IKE protocol is not implemented by the module.

Public Material – May be reproduced only in its original entirety (without revision).

pipelines provide an Ingress and Egress Security Association Database (SADB) for decrypting keys imported from or encrypting keys exported to the SADB in the external on-chip SRAM or host DRAM using GCM.

The module is connected to the ARM Cortex A53 running inside the Integrated Management Complex (IMC) via the NIC Management Fabric (NMF) and the Coherency Mesh Network (CMN). Also attached to the CMN is the ARM Compute Complex (ACC) which contains a number of general-purpose compute cores and on-chip SRAM. TX and RX network packet data and metadata (PMD) are received on either the Ingress or Egress data path to be processed by the module.

The module is connected to other subsystems via an AMBA[3] on-chip system bus, though as described below, the specific protocol may vary between Advanced eXtensible Interface (AXI) and AXI Coherency Extensions (ACE/ACE-Lite). AXI is used for CSR writes (via NMF) when programming PSP master keys and SADB keys. AXI4 streams are used for config packets. ACE/ACE-Lite is used when the module reads/writes data to and from SADB memory (external DRAM or on-chip SRAM in the ACC).

Through the Security Association Database (SADB), ICE supports the ability to add, delete and read SA entries. When a Security Association (SA) is created, a config packet is read from FIFO buffers in the Ingress and Egress data paths. SA keys, data and statistics are fetched from and stored to external DRAM or ACC SRAM using a single ACE-Lite interface in each direction. The SADB is managed in two SA tables, one each for the Ingress and Egress directions. A separate AXI Control Status Register (CSR) configuration interface is provided and connected to the NIC Management Fabric (NMF).

Access to the CSRs and external DRAM is controlled by the underlying SoC configuration. Access requests are passed through the NIC Management Fabric which provides fixed routes between all AMBA-connected endpoints.

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:

FIPS Logical Interface	Physical Ports	Description
Data Input	AMBA (On-chip system bus)	• Inbound AXI4-Stream Packet data and config packets (SA Add data) • Inbound SA entries from DRAM • AXI CSR writes from NMF containing PSP Master Key and Secure SADB Key
Data Output	AMBA (On-chip system bus)	• Outbound AXI4-Stream Packet data from ECQ to ICQ • Outbound SA entries to DRAM
Control Input	AMBA (On-chip system bus)	• AXI CSR writes from the NMF • Control bits in Ingress packet metadata (PMD)

[3] ARM Microcontroller Bus Architecture

Public Material – May be reproduced only in its original entirety (without revision).

FIPS Logical Interface	Physical Ports	Description
		from CXP (crypto packet processor) • Control bits in Egress packet metadata (PMD) from FXP (flexible packet processor)
Status Output	AMBA (On-chip system bus)	• AXI CSR status output to NMF • Status bits in packet metadata (PMD)
Power Input	Power	• Provides power to the module

Table 2 – Physical Port and Logical Interface Mapping

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 roles. The module does not allow concurrent operators. The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the module. No further authentication is required. The Crypto Officer is responsible to set the key for the cipher operation.

5.2 Services

The module provides only Approved services which utilize algorithms listed in Table 3:

Service	Roles		CSP	CSP Access
	User	CO		R = Read W = Write X = Execute
Transmit/receive encrypted data plane packet[4]	✔	✔	ESP / PSP Encryption Key ESP Authentication Key PSP Master Key Secure SADB Key	R, W, X
Transmit/receive plaintext data plane packet	✔	✔	N/A	N/A
Perform diagnostic functions	✔	✔	N/A	N/A
Self-Test (Self-Test is executed automatically at power-on)	✔	✔	N/A	N/A
Initialization	✔	✔	N/A	N/A
Zeroization	✔	✔	All Keys	W
Status Output	✔	✔	N/A	N/A

Table 3 - Approved Services and Role allocation

[4] Based on the service requested the module will perform an exclusive bypass service (plaintext packet transmission) or an exclusive cryptographic service (encrypted packet transmission). On ingress, PSP Master Key is used to derive PSP Encryption Key.

Public Material – May be reproduced only in its original entirety (without revision).

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

ICE is a sub-chip module implemented as part of the IN762 B0 SoC, which is the physical boundary of the sub-chip module. The IN762 B0 SoC is a single chip with a production grade enclosure and hence conforms to the Level 1 requirements for physical security.

7. Operational Environment

The module is a sub-chip cryptographic subsystem implemented within a single-chip hardware embodiment. No firmware is implemented by the module.

Public Material – May be reproduced only in its original entirety (without revision).

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

The module implements the following approved algorithms in hardware:

CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
ICE Ingress					
A811	AES	128, 256 bits	SP 800-38D SP 800-38A	GCM/GMAC ECB[5]	Decryption and Authentication
	AES	256 bits	SP 800-38B	CMAC	Key Derivation for PSP
	KBKDF (Counter Mode with CMAC)	256 bits	SP 800-108	CMAC	Key Derivation for PSP
ICE Egress					
A813	AES	128, 256 bits	SP 800-38D	GCM/GMAC ECB	Encryption and Authentication
ICE SADB					
A812	AES	128, 256 bits	SP 800-38D SP 800-38A	GCM ECB	Encryption, Decryption and Authentication
	KTS	256 bits	IG D.9	GCM	Key Transport

Table 4 - ICE Approved Algorithms

[5] ECB mode was tested under ACVTS, however is not an available algorithm in the module's operational state. The same applies for all other instances of ECB.

Public Material – May be reproduced only in its original entirety (without revision).

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
ESP Encryption Key	Used to encrypt packet payload.	AES-GCM 128, 256-bit value	N/A	Retrieved in plaintext from FIFO buffers in the control plane during SA creation, then output to SADB in external DRAM or on-chip SRAM in encrypted format. During data plane operations, retrieved from SADB in external DRAM or on-chip SRAM in encrypted format (KTS).	Internal memory (registers, register files, SRAM)	On ICE reset
ESP Authentication Key	Used to authenticate packet payload	AES-GMAC 128, 256-bit value	N/A	Retrieved in plaintext from FIFO buffers in the control plane during SA creation, then output to SADB in external DRAM or on-chip SRAM in encrypted format. During data plane operations, retrieved from SADB in external DRAM or on-chip SRAM in encrypted format (KTS).	Internal memory (registers, register files, SRAM)	On ICE reset
PSP Encryption Key	Used to encrypt packet payload.	AES-GCM 128, 256-bit value	Derived from PSP Master Key	Retrieved in plaintext from FIFO buffers in the control plane during SA creation, then output to SADB in external DRAM or on-chip SRAM in	Internal memory (registers, register files, SRAM)	On ICE reset

				encrypted format (KTS). During data plane operations, retrieved from SADB in external DRAM or on-chip SRAM in encrypted format (KTS).		
PSP Master Key	Key derivation key for PSP encryption keys.	AES-CMAC 256-bit value	N/A	Input in plaintext via direct internal CSR write. Never exits the module	Internal memory (registers, register files, SRAM)	On ICE reset
Secure SADB key	Used to encrypt/decrypt PSP and ESP encryption keys in DRAM.	AES-GCM 256-bit value	N/A	Input in plaintext via direct internal CSR write. Never exits the module	Internal memory (registers, register files, SRAM)	On ICE reset

Table 5 – Approved Keys and CSPs Table

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 caller provides the keys for encryption and/or decryption. Keys are stored in hardware registers (write-only by software) by the Crypto Officer or User. Once the keys are written to the hardware registers, they are not readable from outside the module.

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

The module supports an SP 800-108 KBKDF for deriving PSP encryption and authentication keys using CMAC in Counter Mode.

8.4 Key Storage and Zeroization

CSPs stored within ICE memory and FIFOs are zeroized as part of the reset process, which may be performed via the System Control block (SYSCON) within the Integrated Management Complex.

While this action will clear all secrets internal to ICE 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.

For normal data path operations, when a session is terminated, the SA is deleted via command initiated by external software and zeroes are written to the entire SA entry.

9. Self-tests

FIPS 140-2 requires self-tests to ensure the correctness of the cryptographic functionality at start-up. 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 can attempt to reset the state by cycling the power. 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. If any of the tests fail, the module will not initialize, and no traffic is forwarded. In this state, control requests are returned without processing the requests.

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

- ICE Ingress AES-GCM 256 Decrypt KAT
- ICE Ingress SP 800-108 CMAC KBKDF KAT
- ICE Egress AES-GCM 256 Encrypt KAT
- ICE SADB AES-GCM 256 Encrypt KAT
- ICE SADB AES-GCM 256 Decrypt KAT

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

Public Material – May be reproduced only in its original entirety (without revision).

Note: The module is implemented entirely in hardware and is non-modifiable. Therefore, the integrity test requirements do not apply.

9.2 Conditional Self-Tests

The module supports an exclusive bypass mode where packets may be transmitted or received in plaintext or with cryptographic processing on both Ingress and Egress data paths. Each packet contains packet metadata (PMD) which contains control bits which determine if the packet will be processed with encryption or as plaintext.

The module tests for the correct operation of the exclusive bypass by performing a continuous bypass test. This test is triggered upon receipt of each packet on the Ingress and Egress directions. The module will inspect the PMD structure for each packet, as follows:

For Ingress,

1. The CXP (in a block outside the module logical boundary but inside the physical boundary) must send the module a packet and PMD in the Ingress (Rx) direction queue via the AMBA bus interfaces.
2. For each packet & PMD, the CXP must set a number of control bits correctly in PMD to mark for crypto processing.
3. If the PMD bits are set properly then crypto processing will be carried out.
4. If the PMD bits are not set properly then there will be no crypto processing carried out, i.e., bypassed, and the CRYPTO_STATUS bit will be set to 0.

For Egress,

1. The FXP (in a block outside the module logical boundary but inside the physical boundary) must send the module a packet and PMD in the Egress (Tx) direction queue via the AMBA bus interfaces.
2. For each packet & PMD, the FXP must set a number of control bits correctly in PMD to mark for crypto processing.
    a. If the PMD bits are set properly then crypto processing will be carried out
    b. If the processing has been successful, then the PMD DROP is set to 0.
    c. If the processing has not been successful (Soft Error) then the PMD DROP is set to 1. This packet will be marked to be dropped.
3. If the PMD bits are not set as above then there will be no crypto processing carried out, i.e., bypassed, and the PMD DROP bit will be set to 0.

If there are any ECC failures on the Packet or PMD memories (SRAMs and RFs) then ICE generates a fatal interrupt (entering a hard error state) and freezes the data output interfaces (inhibiting any further cryptographic output).

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.

Public Material – May be reproduced only in its original entirety (without revision).

11. Crypto Officer and User Guidance

The module only supports an Approved mode of 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's 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 ICE is considered a CSP. In all of the supported cases the AES-GCM IV for encryption is constructed deterministically per Section 8.2.1 of NIST SP 800-38D. AES-GCM IV construction is performed within the ICE boundary in accordance with 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 IV construction method for each implementation is described in the following sections.

11.2 IV construction for Secure SADB

The 96-bit IV is internally constructed using the Secure SADBs 32-bit salt allowing for 2^{32} possible values and the 64-bit value which is sampled from the SADB add counter to form a 96 bit IV.

IV uniqueness is guaranteed by the module (ICE). The IV counter will automatically pause data output over the data output interface until the IV has a timer value greater than that of the previous IV. The module does not implement any 64-bit rollover detection on the SADB add counter. ICE supports 10,000 SADB adds per second which would require 58 Million years of operation to roll over the add counter. Therefore, the vendor asserts that it is not possible for the secure SADB keys to be used with the same IV more than once for the lifetime of the Secure SADB.

11.3 IV construction for IPSEC

The 96-bit IV is internally constructed using the Security Association's 32-bit salt allowing for 2^{32} possible values and the 64-bit value which is sampled from Security Association's packet sequence number to form a 96 bit IV.

IV uniqueness is guaranteed by the module (ICE), the IV counter automatically will pause data output over the data output interface until the IV has a timer value greater than that of the previous IV. The module implements a 64-bit rollover detection on the packet sequence number. ICE deactivates Security Associations when the sequence number rollover is detected. Therefore, it is not possible for a Security Association (and its key) to be used with the same IV more than once for the IPsec ESP protocol AES-GCM encryption requests.

Public Material – May be reproduced only in its original entirety (without revision).

11.4 IV construction for PSP

The 96-bit IV is internally constructed using the Security Association's 32-bit SPI allowing for 2^{32} possible values and 64-bit value which is sampled from a master timer to form a 96 bit IV.

IV uniqueness is guaranteed by the module (ICE). The IV counter automatically will pause data output over the data output interface until the IV has a timer value greater than that of the previous IV. The module implements a 64-bit rollover (once every 213 days). Security Associations in the module are limited in lifetime to no more than ~2 days. Therefore, the vendor asserts that it is not possible for a Security Association (and its key) to be used with the same IV more than once for the PSP protocol AES-GCM encryption requests.

Public Material – May be reproduced only in its original entirety (without revision).

12. Glossary

Term	Description
ACC	ARM Compute Complex
ACE	AXI Coherency Extensions
AES	Advanced Encryption Standard
AMBA	ARM Microcontroller Bus Architecture
AXI	Advanced eXtensible Interface
CAVP	Cryptographic Algorithm Validation Program
CCCS	Canadian Centre for Cyber Security
CM	Cryptographic Module
CMAC	Cipher-based Message Authentication Code
CMN	Coherency Mesh Network
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CSR	Control/Status Register
CTR	Counter Mode
CXP	Crypto Packet Processor
DRAM	Dynamic Random-Access Memory
ECC	Error Correction Code
ECQ	Egress Arbiter and Class of Service (COS) Queue
ESP	Encapsulating Security Payload
FIFO	First In First Out
FIPS	Federal Information Processing Standards
FXP	Flexible Packet Processor
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
ICE	Inline Crypto Engine
ICQ	Ingress Arbiter and Class of Service (COS) Queue
IG	Implementation Guidance
IMC	Integrated Management Complex
IP	Intellectual Propety
IPSEC	Internet Protocol Security
IV	Initialization Vector
KAT	Known answer test
KBKDF	Key Based Key Derivation Function
NIST	National Institute of Standards and Technology
NMF	NIC Management Fabric
PMD	Packet Metadata
SA	Security Association
SADB	Security Association Database
SRAM	Static Random Access Memory
SoC	System On Chip

Table 6 - Glossary of Terms

Public Material – May be reproduced only in its original entirety (without revision).