

Google, LLC

Integrated Compute Complex (ICC)

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General	5
1.1 Overview	5
1.2 Security Levels	5
1.3 Additional Information	6
2 Cryptographic Module Specification	6
2.1 Description	6
2.2 Tested and Vendor Affirmed Module Version and Identification	7
2.3 Excluded Components	8
2.4 Modes of Operation	8
2.5 Algorithms	9
2.6 Security Function Implementations	11
2.7 Algorithm Specific Information	13
2.8 RBG and Entropy	14
2.9 Key Generation	14
2.10 Key Establishment	14
2.11 Industry Protocols	14
3 Cryptographic Module Interfaces	15
3.1 Ports and Interfaces	15
4 Roles, Services, and Authentication	15
4.1 Authentication Methods	15
4.2 Roles	15
4.3 Approved Services	15
4.4 Non-Approved Services	23
4.5 External Software/Firmware Loaded	23
4.6 Bypass Actions and Status	23
4.7 Cryptographic Output Actions and Status	23
5 Software/Firmware Security	23
5.1 Integrity Techniques	23
5.2 Initiate on Demand	23
6 Operational Environment	23
6.1 Operational Environment Type and Requirements	23
6.2 Configuration Settings and Restrictions	24
7 Physical Security	24
7.1 Mechanisms and Actions Required	24

8 Non-Invasive Security	24
8.1 Mitigation Techniques	24
9 Sensitive Security Parameters Management	24
9.1 Storage Areas	24
9.2 SSP Input-Output Methods	25
9.3 SSP Zeroization Methods	25
9.4 SSPs	25
10 Self-Tests	27
10.1 Pre-Operational Self-Tests	27
10.2 Conditional Self-Tests	27
10.3 Periodic Self-Test Information	29
10.4 Error States	30
10.5 Operator Initiation of Self-Tests	31
11 Life-Cycle Assurance	31
11.1 Installation, Initialization, and Startup Procedures	31
11.2 Administrator Guidance	31
11.3 Non-Administrator Guidance	31
11.4 Maintenance Requirements	32
11.5 End of Life	32
12 Mitigation of Other Attacks	32
12.1 Attack List	32

List of Tables

Table 1: Security Levels	6
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)....	8
Table 3: Tested Operational Environments - Software, Firmware, Hybrid	8
Table 4: Modes List and Description	8
Table 5: Approved Algorithms -	9
Table 6: Approved Algorithms - [EVM]	10
Table 7: Vendor-Affirmed Algorithms	10
Table 8: Security Function Implementations.....	13
Table 9: Entropy Certificates	14
Table 10: Entropy Sources.....	14
Table 11: Ports and Interfaces	15
Table 12: Roles.....	15
Table 13: Approved Services	22
Table 14: Mechanisms and Actions Required	24
Table 15: Storage Areas	24
Table 16: SSP Input-Output Methods.....	25
Table 17: SSP Zeroization Methods.....	25
Table 18: SSP Table 1	27
Table 19: SSP Table 2.....	27
Table 20: Pre-Operational Self-Tests	27
Table 21: Conditional Self-Tests	29
Table 22: Pre-Operational Periodic Information.....	29
Table 23: Conditional Periodic Information.....	30
Table 24: Error States	31

List of Figures

Figure 1: Block Diagram.....	7
------------------------------	---

1 General

1.1 Overview

Introduction

Federal Information Processing Standards Publication 140-3 — 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 140-3 program. NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria. More information is also 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 Integrated Compute Complex (ICC) 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 140-3. The Integrated Compute Complex (ICC) also be referred to as “ICC” 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.

1.2 Security Levels

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

Section	Title	Security Level
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

The module claims an overall Security Level of 1 with all individual sections at a Security Level 1. The module does not implement any non-invasive security mitigations or mitigations of other attacks and thus the requirements per these sections are inapplicable.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module's primary role is to generate, maintain, control, and manage the Critical Security Parameters (CSPs) and keys required for the operation of other cryptographic services within the IN762 B1 and C1 SoCs. In particular, the module:

- Is bound to and Implements a (logical) interface to the B227 True Random Number Generator (TRNG) Cryptographic Module (hardware version: 3.00b; FIPS 140-3 Cert. #5539) which serves as the trusted source of entropy, which can be used as the basis for generation of SSPs by the ICC module.
- Implements an instance of a firmware-based Deterministic Random Bit Generator, seeded by the above entropy source, to generate cryptographic keys in support of the PSP Security Protocol (PSP) and ICE Secure Association Database (SADB). Note: The module itself does not support these protocols.
- Performs a firmware integrity/load test for the Lookaside Compression and Cryptographic Engine (LCE) (a subsystem within the IN762 SoC).
- Maintains access control to Critical Security Parameters (CSPs) which are isolated to secure memory locations.
- Implements basic board- and processor-specific control and maintenance functions, such as "start CPU".

Module Type: Firmware

Module Embodiment: Single Chip

Cryptographic Boundary:

The Integrated Compute Complex (ICC) is a firmware module within a single chip embodiment. The ICC Secure Firmware executes on two ARM Cortex A53 management processors within the Integrated Compute Complex (ICC) hardware block of the IN762 System-on-a-Chip (SoC). The Google IN762 SoC contains the Host Management Processor (HMP) consisting of the two ARM-A53 CPUs on which the module's firmware executes, Local Secure Memory (LSM), System Controller (SYSCON), eFUSE Controller Module (ECM), and the Network Management Fabric and Coherency Mesh Network connecting these components and other subsystems. The components within the IN762 SoC are interconnected via an AMBA1 on-chip system bus. The module does not contain any persistent storage.

The ICC Secure Firmware is comprised of a single binary image. The firmware is a self-contained binary image (executable code and data) implemented as part of the ARM Trusted Firmware-A ("ATF") environment and system. It is a "Secure Payload", packaged as a "BL32" binary, and running in the ARM Secure EL1 execution state. It resides in part of the SoC's Local Secure Memory ("LSM"), in a region of LSM which is configured for "secure access only" and cannot be read or written or reconfigured by the Linux kernel or by applications. The module has its own (CPU-specific) stack space in this LSM region.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested Operational Environment's Physical Perimeter (TOEPP) is the IN762 SoC.

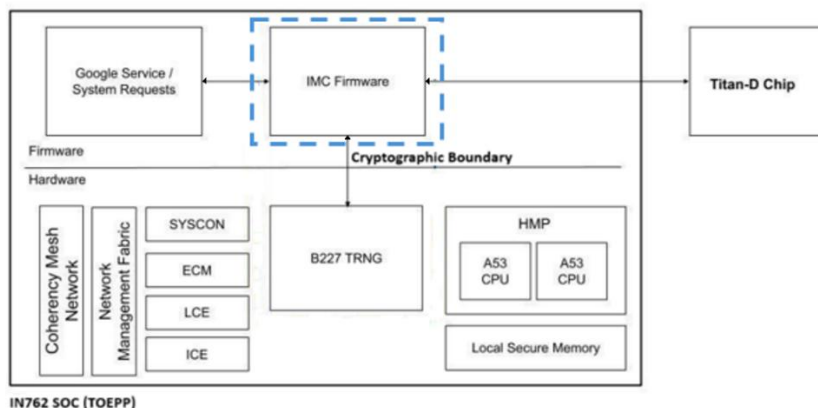


Figure 1: Block Diagram

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
ICC Secure Firmware	2.10.0	N/A	AES-CMAC Verification

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

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
N/A	IN762 SoC B1, C1	ARM Cortex-A53 (ARMv8)	No	N/A	2.10.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

The module does not support any vendor-affirmed operational environments.

2.3 Excluded Components

No components have been excluded from the cryptographic boundary of the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	No configuration of the module or installation steps are required from the operator; When the module is powered on its self-tests are executed without any operator intervention; The module enters the Approved mode of operation automatically if the self-tests at boot complete successfully	Approved	"Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs

Table 4: Modes List and Description

Mode Change Instructions and Status:

The module only supports one Approved mode of operation where only approved cryptographic functions and services are available.

Degraded Mode Description:

The module does not support a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A7461	Direction - Generation Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-1024 Increment 8	SP 800-38B
AES-ECB	A2932	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A7461	Direction - Encrypt Key Length - 128, 192, 256	SP 800-38A
Counter DRBG	A7461	Prediction Resistance - No Supports Reseed - No Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0-256 Increment 8 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0-256 Increment 8 Returned Bits - 512	SP 800-90A Rev. 1
KDF SP800-108	A7461	KDF Mode - Counter MAC Mode - CMAC-AES256 Supported Lengths - Supported Lengths: 128, 256 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
SHA2-256	A7461	Message Length - Message Length: 0-16384 Increment 8	FIPS 180-4

Table 5: Approved Algorithms -

[EVM]

Algorithm	CAVP Cert	Properties	Reference
Conditioning Component Block Cipher Derivation Function SP800-90B	A2932	Key Length - 128 Payload Length - Payload Length: 512	SP 800-90B
Counter DRBG	A2721	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0-256 Increment 8, Additional Input: 0-384 Increment 8 Entropy Input - Entropy Input: 256, Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0-256 Increment 8, Personalization String Length: 0-384 Increment 8 Returned Bits - 128, 512	SP 800-90A Rev. 1

Table 6: Approved Algorithms - [EVM]

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG - Section 4	Key Type:Symmetric	N/A	NIST SP 800-133r2 Section 4 option 1 Using the Output of a Random Bit Generator; NIST SP 800-133r2 Section 6.1 The "Direct Generation" of Symmetric Keys; NIST SP 800-133r2 Section 6.2.2 Symmetric Keys Derived from a Pre-existing Key

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with no Security claimed.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved, Not Allowed Algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
FW Integrity Check	BC-Auth	Used for the firmware integrity test		AES-CMAC: (A7461) Direction: Generation Key Length : 128, 192, 256 MAC Length: 128 Message Length: 8-1024 Increment 8
Encryption	BC-UnAuth	Used to encrypt SADB and PSP traffic		AES-ECB: (A7461) Direction : Encrypt Key Length: 128, 192, 256
Hashing	SHA	Message digest generation		SHA2-256: (A7461) Message Length: 0-16384 Increment 8
Random Number Generation	CKG DRBG	Generation of random bits and SSP generation		Counter DRBG: (A7461) Prediction Resistance: No Mode: AES-256 Derivation Function Enabled: No Additional Input: 0-256 Increment 8 Entropy Input: 384 Nonce: 0 Personalization String Length: 0-256 Increment 8 Returned Bits:

Name	Type	Description	Properties	Algorithms
				512 CKG - Section 4: (Key Type: Symmetric
Key Derivation	CKG KBKDF	Used to derive per-SPI PSP Session keys		KDF SP800- 108: (A7461) KDF Mode: Counter MAC Mode: CMAC-AES256 Supported Lengths: 128, 256 Fixed Data Order: Before Fixed Data Counter Length: 32 Custom Key In Length: 0 AES-CMAC: (A7461) Direction: Generation Key Length: 128, 192, 256 MAC Length: 128 Message Length: 8-1024 Increment 8 CKG - Section 4: (Key Type: Symmetric
Entropy Source	DRBG ENT-ESV	[EVM] Random bits provided as entropy input from the bound B227 module		Counter DRBG: (A2721) Prediction Resistance: Yes, No Supports Reseed: Yes Mode: AES-128, AES-256 Derivation Function

Name	Type	Description	Properties	Algorithms
				Enabled : No Additional Input: 0-256 Increment 8 (AES-128), 0- 384 Increment 8 (AES-256) Entropy Input: 256 (AES-128), 384 (AES-256) Nonce: 0 Personalization String Length: 0- 256 Increment 8 (AES-128), 0- 384 Increment 8 (AES-256) Returned Bits: 128 (AES-128), 512 (AES-256) Conditioning Component Block Cipher Derivation Function SP800- 90B: (A2932) Key Length: 128 bits Payload Length: 512 bits AES-ECB: (A2932) Direction: 128 Payload Length: 128, 256

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

IG D.H

CKG is supported for the following sections per NIST SP 800-133r2 as documented in the Security Policy Section 2.1, Vendor Affirmed Algorithms Table: Sections 4, 6.1 and 6.2.2. Post processing is not performed and thus IG D.I is inapplicable.

IG D.L

Per the IG, the Entropy Input, DRBG Seed and Counter DRBG State values - V and Key have been defined as CSPs. Per Additional Requirement #2. in the IG, the module has been tested

without a derivation function and the ESV Cert. #E137 indicates that the entropy source provides full entropy to the module.

IG D.M

In accordance with IG D.M, the SP 800-108 KDF is used only for generation of symmetric keys.

2.8 RBG and Entropy

Cert Number	Vendor Name
E137	Google, LLC

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
TRNG Entropy Source	Physical	IN762 SoC B1, IN762 SoC C1	128 bits	128 bits (full entropy)	BlockCipher_DF (A2932)

Table 10: Entropy Sources

The module is a firmware module which includes one approved NIST SP 800-90Ar1 DRBG. The ICC Secure Firmware DRBG is seeded with 384 bits. The module's entropy source is consistent with Scenario 1 (b) described in FIPS 140-3 IG 9.3.A. The ICC module is bound to the B227 True Random Number Generator (TRNG) Cryptographic Module (hardware version: 3.00b; FIPS 140-3 Cert. 5539) which serves as the trusted source of entropy. The ICC DRBG is seeded using the B227 DRBG output with 384-bits of entropy (full entropy per bit) and the module generates SSPs of maximum size of 256 bits.

2.9 Key Generation

The module generates symmetric keys in accordance with IG D.H and SP 800-133rev2, Section 4 option 1, Section 6.1 and Section 6.2.2.

2.10 Key Establishment

The module does not support SSP establishment.

2.11 Industry Protocols

The module does not support any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	Secure EL1 command parameters; Fast Secure Monitor API parameters ; Google service request API parameters
N/A	Data Output	Secure EL1 return data ; Fast Secure Monitor API return data; Google service request API return data
N/A	Control Input	Secure EL1 commands; Fast Secure Monitor API commands; Google service request API commands, reset signal
N/A	Status Output	Secure EL1 command response codes; Fast Secure Monitor API response codes; Google service request API response codes
N/A	Power	Provides power to the module

Table 11: Ports and Interfaces

The module does not support control output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not support operator authentication; assumption of the Crypto Officer (CO) role is implicit based on the selected service(s). The CO role has access to all module services, and the module does not support a User/Maintenance role.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	None

Table 12: Roles

The module does not allow concurrent operators. The Crypto Officer role is implicitly assumed by the entity accessing services implemented by the module.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize	Module and PSP functions including generate PSP Master Key	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	N/A	Status (success/failure of self-tests)	Key Derivation	CO - Master PSP Keys: W
Perform self-tests	Executed automatically when powered on	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Reset	Status (success/failure of self-tests)	None	CO
Show status	Status retrieved from the module	Approved mode indicator ("Notice: GSP:	N/A	Status (Approved mode indicator/error indicator)	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service				
Zeroization	A module reset zeroes all SSPs	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Reset	N/A	None	CO - ICC Entropy Input String: Z - ICC DRBG Seed: Z - ICC DRBG V : Z - ICC DRBG Key: Z - Master PSP Keys: Z - Security Association Database (SADB) Protection keys: Z - PSP Session Keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
CPU state management	CPU management instruction (start CPU)	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	start CPU	CPU state	None	CO
Get information (Show Version / Show module's versioning information)	Print buffer, command buffer	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Get command	Module's firmware version (2.10.0), module identifier ("imc")	None	CO
Print buffer management	Start, stop functions	Approved mode indicator ("Notice: GSP:	Start/stop functions/commands	N/A	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service				
Submit request data	Input of request data	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Request data	N/A	None	CO
Retrieve response data	Retrieval of response data	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice:	N/A	Response data	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		PSP: activating" logs) combined with successful completion of the service				
Generate New PSP Master Key	To generate a new PSP Master Key (Post-initialization) a.k.a. "Rotate key generation"	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Key rotation/new key generation request via module API	Newly generated key	Random Number Generation	CO - Master PSP Keys: W - ICC Entropy Input String: W,E - ICC DRBG Seed: G,E - ICC DRBG V : G,E - ICC DRBG Key: G,E
Derive PSP Keys	To derive PSP Session Keys	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with	Master PSP Key	PSP Session Key	Key Derivation	CO - PSP Session Keys: G - Master PSP Keys: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		successful completion of the service				
Generate DRBG output	Random bit generation	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Request for random bits	Random bits generated	Random Number Generation Entropy Source	CO - ICC Entropy Input String: G,E - ICC DRBG Seed: G,E - ICC DRBG V : G,E - ICC DRBG Key: R,E
Perform Firmware Load Test (LCE)	Firmware load/integrity test performed by the ICC module for the LCE module	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	N/A	Status (success/failure of the self-test)	FW Integrity Check	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Encryption	Used to encrypt SADB and PSP traffic	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Plaintext	Ciphertext	Encryption	CO - Security Association Database (SADB) Protection keys: E - PSP Session Keys: E
Hashing	Used to generate a hash of the input provided	Approved mode indicator ("Notice: GSP: crypto self-test passed" and "Notice: PSP: activating" logs) combined with successful completion of the service	Plaintext message	Hash	Hashing	CO

Table 13: Approved Services

The module provides the aforementioned Approved services which utilize algorithms. The module's firmware provides APIs operating at three levels. Requests for execution come in at higher levels and are translated into lower-level service calls:

- Secure EL1 (Lowest level)
- Fast Secure Monitor (Mid-level)
- Google service requests (Mid- and High-Level)

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

4.5 External Software/Firmware Loaded

The module does not support loading any firmware.

4.6 Bypass Actions and Status

The module does not support a bypass capability.

4.7 Cryptographic Output Actions and Status

The module does not support a self-initiated cryptographic output capability.

5 Software/Firmware Security

5.1 Integrity Techniques

The module implements an AES-CMAC (256 bits) verification as the approved integrity mechanism. The AES-CMAC authentication key (a non-SSP) is stored within the module binary. On each boot/reset, the module generates afresh an AES-CMAC i.e. a 256-bit MAC value which is then compared to a known, stored value within the module. If the two values match the module successfully operates in the Approved mode, else returns an error indicator and fails its initialization.

5.2 Initiate on Demand

The firmware integrity test can be executed on demand by rebooting the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied:

The module is a firmware module residing within the IN762 SoC. The procurement, build, and configuration procedures are controlled by the manufacturer. Therefore, the operational environment is considered non-modifiable.

6.2 Configuration Settings and Restrictions

Additional restrictions do not apply.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Standard passivation applied on the IN762 SoC	None	None

Table 14: Mechanisms and Actions Required

The ICC is a firmware module implemented as part of the IN762 SoC, which is the physical perimeter. The IN762 SoC is a single chip with a production grade IC packaging and hence conforms to the Level 1 requirements for physical security.

8 Non-Invasive Security

8.1 Mitigation Techniques

The module does not support any non-invasive attack mitigations.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
LSM	Ephemeral storage of SSPs in plaintext	Dynamic

Table 15: Storage Areas

All SSPs are stored in the LSM/hardware registers in the TOEPP i.e., the IN762 SoC and are zeroised upon power cycle or after having been written to the calling application or subsystem internal to the IN762 SoC. The module does not maintain any persistent SSP storage.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Entropy Input	B227 TRNG	LSM	Plaintext	Manual	Electronic	
Output - 1	LSM	External entity	Plaintext	Manual	Electronic	
Output - 2	Random Number Generator	External entity	Plaintext	Manual	Electronic	

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroised on reset	SSPs stored ephemerally are zeroised on resetting the module	SSPs stored ephemerally are zeroised on resetting the module	Operator Initiated
Zeroised after writing to the calling application/subsystem	Automatic zeroisation per the module design	Temporarily stored SSPs are zeroised once no longer used	Module Initiated

Table 17: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ICC Entropy Input String	Entropy Input provided by the B227 entropy source to the module; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	384 bits - 256-bits	Entropy input - CSP			Random Number Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ICC DRBG Seed	Seed provided to the NIST SP 800-90Ar1 DRBG; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	384-bits - 256-bits	DRBG Seed - CSP	Entropy Source		Random Number Generation
ICC DRBG V	NIST SP 800-90Ar1 DRBG State V value; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	128-bits - 128-bits	Internal state of DRBG - CSP	Random Number Generation		Random Number Generation
ICC DRBG Key	NIST SP 800-90Ar1 DRBG Key value; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	256-bits - 256-bits	Internal state of DRBG - CSP	Random Number Generation		Random Number Generation
Master PSP Keys	Used to derive per-SPI PSP Session keys	256-bit - 256-bits	Symmetric Key - CSP	Random Number Generation		Key Derivation
Security Association Database (SADB) Protection keys	Used to encrypt SADB	256-bit - 256-bits	Symmetric Key - CSP	Random Number Generation		Encryption
PSP Session Keys	Used to encrypt PSP traffic	128, 256 bits - 128, 256 bits	Symmetric Key - CSP	Key Derivation		Encryption

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ICC Entropy Input String	Entropy Input	LSM:Plaintext	Until reset	Zeroised on reset	
ICC DRBG Seed		LSM:Plaintext	Until reset	Zeroised on reset	
ICC DRBG V		LSM:Plaintext	Until reset	Zeroised on reset	
ICC DRBG Key		LSM:Plaintext	Until reset	Zeroised on reset	
Master PSP Keys	Output - 1	LSM:Plaintext	Until reset	Zeroised on reset	
Security Association Database (SADB) Protection keys	Output - 2		Until reset, until in use	Zeroised on reset Zeroised after writing to the calling application/subsystem	
PSP Session Keys	Output - 1	LSM:Plaintext	Until reset, until in use	Zeroised on reset Zeroised after writing to the calling application/subsystem	

Table 19: SSP Table 2

Per IG 9.5.A, the module supports MD/EE.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
AES-CMAC Verification	256 bits	KAT	SW/FW Integrity	"Notice: GSP: crypto self-test passed"	MAC Verify

Table 20: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A7461) - 128 bits	Key Length: 128 bits	KAT	CAST	"Notice: GSP: crypto self-test passed"	Encrypt	On boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A7461) - 192 bits	Key Length: 192 bits	KAT	CAST	"Notice: GSP: crypto self-test passed"	Encrypt	On boot
AES-ECB (A7461) - 256 bits	Key Length: 256 bits	KAT	CAST	"Notice: GSP: crypto self-test passed"	Encrypt	On boot
AES-CMAC (A7461)	Key Length: 128 bits	KAT	CAST	"Notice: GSP: crypto self-test passed"	Generation	On boot
SHA2-256 (A7461)	256 bits	KAT	CAST	"Notice: GSP: crypto self-test passed"	Hash	On boot
Counter DRBG (A7461)	AES CTR (256 bits)	KAT	CAST	"Notice: GSP: crypto self-test passed"	Generate, Reseed, Instantiate functions	On boot
Counter DRBG (A2721)	AES CTR (256 bits)	KAT	CAST	"Notice: GSP: crypto self-test passed"	Generate, Reseed, Instantiate functions	On boot
LCE Firmware Integrity/Load Test (AES-CMAC 256-bit)	Key Length: 256 bits	Firmware Integrity/Load Test for the LCE module	SW/FW Load	"Notice: GSP: crypto self-test passed"	MAC generation	On boot
B227 Adaptive Proportion Test (ESV Cert. E137)	Sample size: 1 bit; Min-Entropy: H=50%; Cutoff Value: C=793; Window size:	SP 800-90B Health Tests	CAST	"Notice: GSP: crypto self-test passed"	[EVM]	On boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	w=1024; False positive error rate: Alpha = 2^{-20}					
B227 Repetition Count Test (ESV Cert. E137)	Sample size: 1 bit; Min-Entropy: H=50%; Cutoff Value: C=41; False positive error rate: Alpha = 2^{-20}	SP 800-90B Health Tests	CAST	"Notice: GSP: crypto self-test passed"	[EVM]	On boot
KDF SP800-108 (A7461)	Mode: Counter, PRF: CMAC-AES256	KAT	CAST	"Notice: GSP: crypto self-test passed"	Counter Mode	On boot

Table 21: Conditional Self-Tests

In the event that any of the above conditional tests fail except for the NIST SP 800-90B Health Tests, the cryptographic module will be halted, and data output will be inhibited, with the exception of the LCE Firmware Integrity Test / Firmware Load Test. In this case, the test is performed on behalf of the LCE module. Upon failure, the ICC module will reject the LCE firmware and the LCE module will remain in an uninitialized state. However, the ICC module will resume its operations. Failure of a NIST SP 800-90B Health Test causes the entropy source (within the bound B227 module) to raise an alarm and zeroise itself. The ICC module is unaffected in that it does not enter an error state itself but cannot generate any SSPs until entropy is provided to it.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CMAC Verification	KAT	SW/FW Integrity	On Demand	Manually, via a reboot

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A7461) - 128 bits	KAT	CAST	On Demand	Manually by reloading the module
AES-ECB (A7461) - 192 bits	KAT	CAST	On Demand	Manually by reloading the module
AES-ECB (A7461) - 256 bits	KAT	CAST	On Demand	Manually by reloading the module
AES-CMAC (A7461)	KAT	CAST	On Demand	Manually by reloading the module
SHA2-256 (A7461)	KAT	CAST	On Demand	Manually by reloading the module
Counter DRBG (A7461)	KAT	CAST	On Demand	Manually by reloading the module
Counter DRBG (A2721)	KAT	CAST	On Demand	Manually by reloading the module
LCE Firmware Integrity/Load Test (AES-CMAC 256-bit)	Firmware Integrity/Load Test for the LCE module	SW/FW Load	On Demand	Manually by reloading the module
B227 Adaptive Proportion Test (ESV Cert. E137)	SP 800-90B Health Tests	CAST	On Demand	Manually by reloading the module
B227 Repetition Count Test (ESV Cert. E137)	SP 800-90B Health Tests	CAST	On Demand	Manually by reloading the module
KDF SP800-108 (A7461)	KAT	CAST	On Demand	Manually by reloading the module

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Soft Error state	Upon failure of the LCE Firmware Integrity Test / Firmware Load Test	Failure of the LCE Firmware Integrity Test / Firmware Load Test	The module will return an error indicator and resume operation	ERROR: Firmware hash for image 99 DOES NOT MATCH, ERROR: Ice abort image load
Hard Error state	No cryptographic functions can be executed and all data output is inhibited	Failure of the pre-operational firmware integrity test Failure of the CASTs	The module would have to be re-initialized via a reload/reboot	"Integrity FAIL" for the failure of the pre-operational firmware integrity test and "crypto self-test failed" for the failure of one/more CASTs
B227 Soft Error state	[EVM] The Soft Error state is cleared automatically by the B227 entropy source (the source raises an alarm, zeroes itself and becomes operational again)	Failure of a NIST SP 800-90B Health Test	The entropy source (and thus the bound B227 module as a whole) recovers automatically	Failure of a NIST SP 800-90B Health Test causes the entropy source to raise an alarm and zeroise itself

Table 24: Error States

10.5 Operator Initiation of Self-Tests

An operator can initiate pre-operational and conditional cryptographic algorithm self-tests on demand by rebooting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No specific instructions are required for initialization of the module in the Approved mode.

11.2 Administrator Guidance

Please see Sections 2, 3, 4 and 11 in this document.

11.3 Non-Administrator Guidance

Please see Sections 2, 3, 4 and 11 in this document. The module only supports a Crypto Officer (i.e. Administrator) role.

11.4 Maintenance Requirements

No specific maintenance requirements apply.

11.5 End of Life

The module can be zeroised to perform secure sanitization.

12 Mitigation of Other Attacks

12.1 Attack List

The module does not support mitigation of any other attacks and thus the requirements of this section do not apply.