Nokia

Nokia-SONiC-MACsec

Version: 1.0

FIPS 140-3 Non-Proprietary Security Policy

Document prepared by:

http://www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This non-proprietary FIPS 140-3 Security Policy for the Nokia-SONiC-MACsec, version 1.0 describes how the module meets the security requirements specified in FIPS 140-3 for an overall security level 1 module and outlines the security rules and operating procedures required to maintain compliance.

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
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The TOE is used in DC interconnect with MACsec security for the DC interconnect interfaces.

Module Type: Software-hybrid

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the Nokia-SONiC-MACsec consists of a hardware and a software component, which is represented by the red dash line in Figure 3, below. The physical perimeter of the module is defined as the entire MACsec ASIC. The sole software component of the module consists of the entire module's software.

The MACsec ASIC shown below represents the entire physical perimeter of the module itself and implements the core cryptographic functionality of the module, AES-GCM encryption and decryption used within the MACsec protocol.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested Operational Environment's Physical Perimeter consists of the Nokia-IXR7250E-36x400G device that the module resides within, which is represented in Figure 2, below. The tested operational environments are listed in Table Tested Operational Environments - Software, Firmware, Hybrid, below.

Figure 1: Broadcom BCM88852 physical perimeter.

Figure 2: Representation of Nokia-IXR7250E-36x400G device TOEPP.

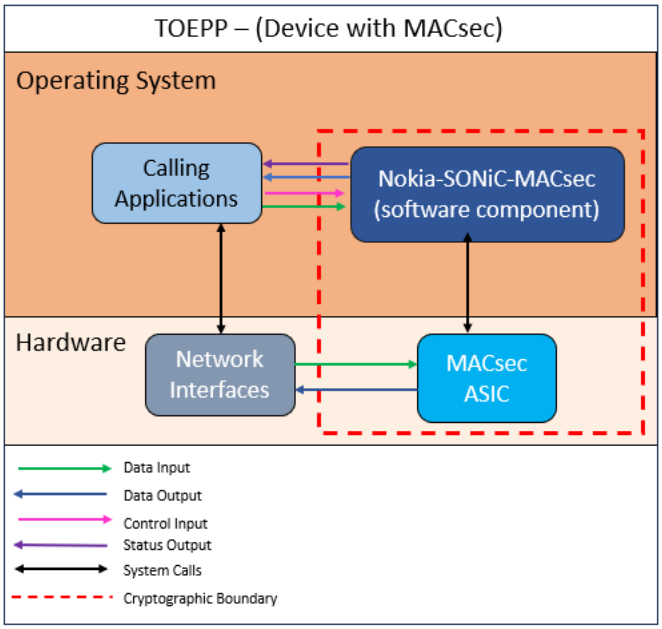

Figure 3: Module cryptographic boundary and TOEPP.

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
libfips_integrity_self_test.so	BCM/ Integrity self test version 2	Integrity self-test library which implements the SHA algorithm.	SHA2-256
libfips_sa_j2p.so	BCM/ J2P DNX FIPS SA 3	Secure association library implementing the APIs.	SHA2-256
libmini_access_cmicx_gen1.so	BCM/ Mini access CMICX gen1 version 2	Used for the PCIE driver to access the hardware and other components	SHA2-256
libfips_integrity_self_test.sha256	BCM/ Integrity self test version 2	SHA digest	SHA2-256
libfips_sa_j2p.sha256	BCM/ J2P DNX FIPS SA 3	SHA digest	SHA2-256

Package or File Name	Software/ Firmware Version	Features	Integrity Test
libmini_access_cmicx_gen1.sha256	BCM/ Mini access CMICX gen1 version 2	SHA digest	SHA2-256

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

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
BCM88852	rev A2	macsecip_gen2	BCM88852 rev A2	Single chip

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Debian GNU/Linux 12 (bookworm)	Nokia-IXR7250E-36x400G	AMD EPYC 3251 8-Core Processor	Yes		BCM/ Integrity self test version 2 BCM/ J2P DNX FIPS SA 3 BCM/ Mini access CMICX gen1 version 2

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

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

N/A for this module.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	The approved mode of operation	Approved	Log ("Switch MACSec POST passed")

Table 5: Modes List and Description

Once these self-tests have completed successfully, the module transitions into the approved mode of operation. There are no other modes of operation implemented by the module.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	C894	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	C894	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-XPN	C894	Direction - Decrypt, Encrypt Key Length - 128, 256 IV Generation - External	SP 800-38D
SHA2-256	A7797	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 6: Approved Algorithms

The Approved Algorithms tables above list the approved algorithms implemented by Nokia-SONiC-MACsec.

Vendor-Affirmed Algorithms:

The module does not implement any vendor-affirmed algorithms.

Non-Approved, Allowed Algorithms:

The module does not implement any non-approved, allowed algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not implement any non-approved, allowed algorithms with no security claimed.

Non-Approved, Not Allowed Algorithms:

The module does not implement any non-approved, not allowed algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Software/Firmware Integrity Test	SHA	Integrity test for chip firmware and module software		SHA2-256: (A7797)
Encrypt Data	BC-Auth	Encryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-ECB: (C894) AES-GCM: (C894) AES-XPN: (C894)
Decrypt Data	BC-Auth	Decryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-ECB: (C894) AES-GCM: (C894) AES-XPN: (C894)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

The AES-GCM Initialization Vector (IV) generation is compliant with IG C.H, resolution 1(c). The module generates IVs deterministically following the guidance in IEEE 802.1AE.

While operating the approved mode of operation, the module should only be used to form a MACsec link with another FIPS 140 validated module operating in the approved mode. The device at each end of the MACsec link plays the role of either Peer or the Authenticator. No authentication server is involved.

In case the module's power is lost and then restored, the key used for AES-GCM encryption and decryption operations shall be redistributed.

2.8 RBG and Entropy

The module only generates SSPs used in the MACsec protocol deterministically. Therefore, the module does not implement DRBG and does not require an entropy source.

2.9 Key Generation

The module only generates the AES-GCM Initialization Vector deterministically, following the guidance given in IG C.H (path 1, c) and IEEE 802.1AE.

2.10 Key Establishment

The module does not implement any key establishment schemes.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIE_RX, NIF50_RX, FAB50_RX	Data Input	Plaintext data to be encrypted, Encrypted data to be decrypted
PCIE_TX, NIF50_TX, FAB50_TX	Data Output	Plaintext data that has been decrypted, Encrypted data that has been encrypted
PCIE_RX	Control Input	Command signal invoking cryptographic services
PCIE_TX	Status Output	Status information regarding the module and the invoked service/function.
PCIE_VDDHRX1P5, PCIE_VDDHTX1P5: Voltage=1.5V	Power	Electrical power to the module

Table 8: Ports and Interfaces

The Ports and Interfaces table above specifies the cryptographic module interfaces. The physical interfaces are defined as the data input/output pins of the MACsec chips. The logical interfaces are logically separated from one another by the firmware design. The power interface is physically separate from the other physical interfaces as the voltage pins are distinct from the data input/output pins of the chips.

The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement any authentication mechanisms. The sole role (Crypto Officer) is assumed implicitly.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 9: Roles

The module supports the Crypto Officer role only. This sole role is implicitly assumed by the operator of the module when performing a service.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show status	Output approved mode status	Global (completion of service)	Command Check syslog(/var/log/syslog)	Status Output ("Switch MACSec POST passed" OR "Implicit - Module becomes non-operational")	None	Crypto Officer
Show module's versioning info	Output the module name and version identifiers	Global (completion of service)	Command (show macsec --fips-module)	Status Output ("Nokia-SONiC-MACsec-Version 1.0")	None	Crypto Officer
Perform self-tests on demand	Runs the software/firmware integrity check and cryptographic algorithm self	Global (completion of service)	Procedure/Reboot	Status Output (pass/fail)	Software/Firmware Integrity Test	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	tests on demand					
Zeroisation	Zeroise SSPs stored temporarily in RAM and in the chip registers	Global (completion of service)	Procedure/Reboot	Status Output	None	Crypto Officer - AES-GCM Key: Z - AES-GCM IV: Z
Encrypt data	Encrypt plaintext data	Global (completion of service)	Function call/plaintext packets	Encrypted packets	Encrypt Data	Crypto Officer - AES-GCM Key: W,E - AES-GCM IV: G,E
Decrypt data	Decrypt ciphertext data	Global (completion of service)	Function call/encrypted packets	Plaintext packets	Decrypt Data	Crypto Officer - AES-GCM Key: W,E - AES-GCM IV: G,E

Table 10: Approved Services

The abbreviations of the access rights to SSPs have the following interpretation:

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 = Zeroise: The module zeroises the SSP.

The module provides approved services to the operator who assumes the Crypto Officer role as defined in this document.

The approved services defined in this section implement the security function implementations defined in section 2.6 of this document.

4.4 Non-Approved Services

The module does not implement any non-approved services.

4.5 External Software/Firmware Loaded

The module does not allow the loading of external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The approved integrity technique is implemented by the cryptographic module itself. The approved software integrity technique consists of a self-test, run pre-operationally.

Software integrity test:

The entire module software is covered with an approved integrity technique (SHA2-256) which is implemented in the module itself. If the calculated integrity value does not match the reference value embedded into the software, the module enters the Error state and terminates execution of module.

5.2 Initiate on Demand

The conditional algorithm self-tests are run at module startup in addition to the firmware integrity test. The crypto officer can initiate the self-tests on demand by power-cycling the host platform (TOEPP).

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

The Crypto Officer should confirm that the module is operating in the approved mode by checking for the approved mode indicator per the instructions in Section 11.2 of this document.

7 Physical Security

The module's hardware consists of a single chip made with production grade components, protected by a conformal coating as a standard passivation technique. As the software portion of the hybrid module executes within a modifiable operational environment, the module is defined as a multi-chip standalone embodiment.

The module itself provides no additional physical security techniques. However, the module will reside inside of a Nokia-IXR7250E-36x400G device which is installed within a secure facility. The module will therefore inherit these additional physical characteristics and protections.

8 Non-Invasive Security

The module does not implement any security mechanisms which protect against non-invasive attacks.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Volatile Memory	Stored temporarily in memory within MACsec module.	Dynamic
External	Stored temporarily in memory location associated with the calling application.	Dynamic

Table 11: Storage Areas

The module stores keys and input/output data temporarily in volatile memory. The module does not store keys or data persistently.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SSP Input (GCM encrypt)	External	Volatile Memory	Plaintext	Automated	Electronic	Encrypt Data
SSP Input (GCM decrypt)	External	Volatile Memory	Plaintext	Automated	Electronic	Decrypt Data

Table 12: SSP Input-Output Methods

SSPs are only input from the calling applications within the module's TOEPP. This method is categorized as automated distribution, electronic entry ("CM Software from App via TOEPP Path").

9.3 SSP Zeroisation Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle/ Re-instantiate module	Remove power from the host platform	Keys are procedurally zeroized by rebooting the host platform, which is acceptable at Software level 1.	Crypto Officer reboots or removed power from host platform

Table 13: SSP Zeroization Methods

SSPs are zeroised procedurally by power-cycling the host platform.

9.4 SSPs

The following table summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES-GCM Key	Encryption and Decryption	128 or 256 bits - 128 or 256 bits	Authenticated Symmetric Key - CSP			Encrypt Data Decrypt Data
AES-GCM IV	Initialization Vector for AES-GCM MACsec encryption	96 bits - N/A	Initialization Vector - PSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data

Table 14: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-GCM Key	SSP Input (GCM encrypt) SSP Input (GCM decrypt)	Volatile Memory:Plaintext	Until zeroised	Power Cycle/ Re-instantiate module	AES-GCM IV:Used With
AES-GCM IV		Volatile Memory:Plaintext	Until zeroised	Power Cycle/ Re-instantiate module	AES-GCM Key:Used With

Table 15: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A7797)	SHA2-256	KAT	SW/FW Integrity	Log entry: "Switch MACSec POST passed" OR "Implicit - Module becomes non-operational"	Software component Integrity test using an approved hash (SHA2-256)

Table 16: Pre-Operational Self-Tests

The startup integrity test is performed upon the module.

As the modules do not implement bypass capability or any FIPS-defined critical functions, no additional pre-operational self-tests are required.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XPN (C894)	128 bits	KAT	CAST	'Ethernet<x/y>': POST complete	Encrypt (using extended packet numbering function), MACsec ASIC	Before first operational use of encryption service. / Immediately when the module enters the approved mode of operation.
SHA2-256 (A7797)	SHA2-256	KAT	CAST	Log entry: "Switch MACSec POST passed" OR "Implicit - Module becomes non-operational"	Hash compare KAT	Before first operational use of SHA2-256
AES-XPN Decrypt (C894)	128 bits	KAT	CAST	'Ethernet<x/y>': POST complete	Decrypt (using extended packet numbering function), MACsec ASIC	Before first operational use of decryption service. / Immediately when the module enters the approved

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						mode of operation.

Table 17: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A7797)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)

Table 18: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XPN (C894)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
SHA2-256 (A7797)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
AES-XPN Decrypt (C894)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device

Table 19: Conditional Periodic Information

The operator can perform pre-operational and conditional self-tests on demand by power-cycling the host platform.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	Module terminates operation, Host device must be restarted	Module fails SHA2-256 CAST, or Software Integrity Test	Reboot host platform	Module terminates operation

Table 20: Error States

When the module fails any self-test, the module will immediately become unavailable to the host system. When in the error state, the TOEPP's interfaces will not be available and therefore, all cryptographic operation is inhibited.

10.5 Operator Initiation of Self-Tests

The operator can perform the conditional self-tests on demand by power-cycling the host platform.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Nokia-SONiC-MACsec is pre-installed and configured at a facility and offered to the end users as an integrated part of Nokia's service offerings. As such, there are no installation, initialization, or startup procedures to be performed by the Crypto Officer.

11.2 Administrator Guidance

The Crypto Officer should ensure that the module is running in the approved mode of operation before use. This can be determined by checking the device log to confirm the output of the 'Show Module's Versioning Information' and 'Show Status' services as listed in the 'Approved Services' section of this document.

11.3 Non-Administrator Guidance

In case the module's power is lost and then restored, the key used for MACsec encryption and decryption shall be redistributed.

12 Mitigation of Other Attacks

The module does not implement any security mechanisms which protect against other attacks.