7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Data Plane Cryptographic Module (SARDPCM)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level:1

Document Version: 1.2

July 30th, 2018

TABLE OF CONTENTS

LIST OF FIGURES

GLOSSARY

AES	*Advanced Encryption Standard*
BGP	*Border Gateway Protocol*
CBC	*Cipher Block Chaining*
CFM	*Control / Forwarding Module*
CLI	*Command Line Interface*
CMVP	*Cryptographic Module Validation Program*
CSM	*Control Switch Module*
CSP	*Critical Security Parameter*
CVL	*Component Validation List*
ESP	*Encapsulating Security Payload*
FIPS	*Federal Information Processing Standard*
GRE	*Generic Routing Encapsulation*
HMAC	*Hashed Message Authentication Code*
ICMP	*Internet Control Message Protocol*
ICV	*Integrity Check Value*
IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
IPSec	*IP Security*
LDP	*Label Distribution Protocol*
LSP	*Label Switched Path*
MPLS	*Multi-protocol label switching*

NDRNG	*Non-Deterministic RNG*
NGE	*Network Group Encryption*
NIST	*National Institute of Standards and Technology*
OSPF	*Open Shortest Path First*
PFS	*Perfect Forward Secrecy*
RNG	*Random Number Generator*
SA	*Security Association*
SAM	*Service Aware Manager*
SFM	*Switch Fabric Module*
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell*
SPI	*Security Parameter Index*
TLS	*Transport Layer Security*
TM	*Traffic Management*
VPLS	*Virtual Private LAN Service*

Table 1 - Glossary

1. INTRODUCTION

1.1 Purpose

This document describes the non-proprietary SAR-OS (Service Aggregation Router Operating System) Cryptographic Module (SARDPCM) Security Policy for the 7705 Service Aggregation Router (SAR) product family. These are referenced in the document as either 7705 or SAR.

This security policy provides the details for configuring and running the 7705 products in a FIPS-140-2 mode of operation and describes how the module meets the requirements of FIPS 140-2. Please see the references section for a full list of FIPS 140-2 requirements.

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1

11	Mitigation of Other Attacks	N/A

Table 2 - Security Level per FIPS 140-2 Section

1.2 Versions Available for FIPS

The following platforms of the 7705 products were tested for running the SARDPCM in a FIPS approved mode:

Platform	Model(s)
7705 SAR platforms supporting datapath encryption including IPSec and NGE	SAR-8, SAR-18, SAR-Ax, SAR-H, SAR-Hc, SAR-W, SAR-Wx, SAR-X

Table 3 - FIPS Capable Platforms and Models

The firmware version used to validate the SARDPCM was SAR-OS Rel 8.0R6.

2. SAR-OS CRYPTOGRAPHIC MODULE OVERVIEW

The section provides an overview of the SAR-OS Cryptographic Module (SARDPCM) and the FIPS validated cryptographic algorithms used by services requiring those algorithms. The SARDPCM doesn't implement any services or protocols directly. Instead, it provides the cryptographic algorithm functions needed to allow SAR-OS to implement cryptography for those services and protocols that require it.

2.1 SARDPCM Characteristics

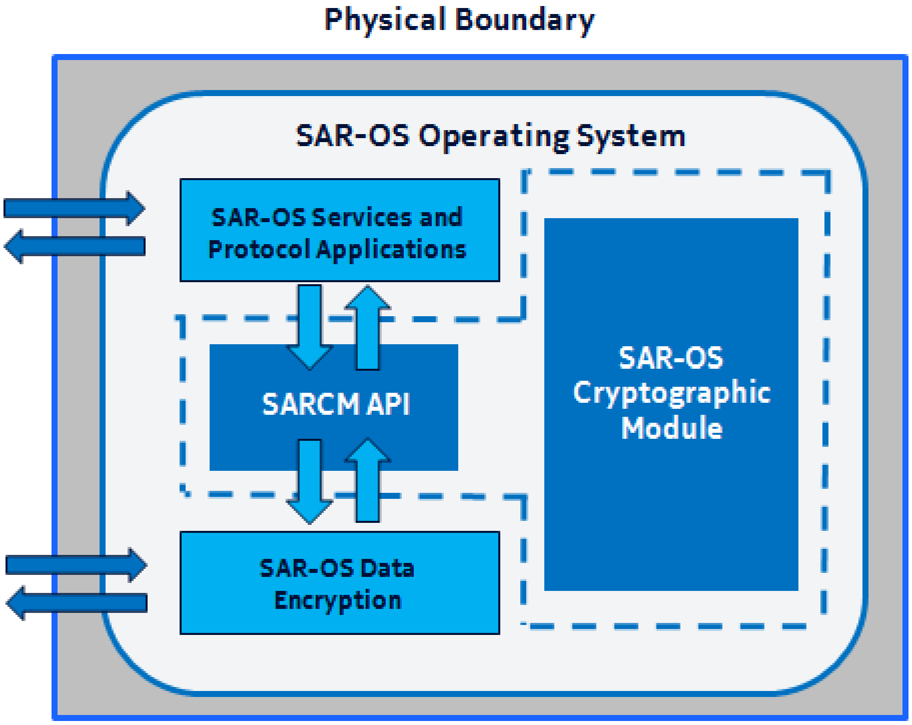

Figure 2-1: SARDPCM Diagram of Logical and Physical Boundaries

The SARDPCM logical and physical properties and boundary considerations is illustrated in Figure 2-1. The solid blue line represents the physical boundary of the cryptographic module that represents the hardware system on which SAR-OS is running and hence where SARDPCM is also running. The dashed blue line indicates the logical cryptographic boundary of the SARDPCM within SAR-OS. The SARDPCM is available as a cryptographic service for any SAR-OS services or protocols that require cryptographic operations.

The SARDPCM provides the cryptographic services required for the data plane (ie IPSec and NGE). On the 7705 SAR-18/8 and SAR-Ax/Wx/W/H/Hc, all the control plane functionality is part of the Control and Switching Module (CSM), while the data plane is managed by the Winpath network processor. It should be noted on SAR-Ax/Wx/W/H/Hc platforms the CSM and line cards are physically on the same hardware, but logically separate. The winpath network processor on these platforms is encryption capable. Also on SAR-18/8 all the control plane functionality is part of the Control and Switching Module (CSM) while the data plane is managed by the Winpath network processor which is present on all interface cards. The data path encryption is done on winpath for all SAR platform mentioned above.

The SARDPCM is part of a single SAR-OS binary file (both.tim) that is used to run the full SAR-OS application. SARDPCM is classified as a multi-chip standalone firmware module and SARDPCM is included within the SAR-OS application code. SARDPCM has been validated on each CSM used by the hardware platforms listed in the following table. Note that the CSM is integrated into the chassis of 7705 SAR-Ax/Wx/W/H/Hc variants while the CSM is a separate hardware module on the SAR-8/18 systems and integrated into the chassis on all other 7705 variants

Platform	Encryption Network Processor
SAR-8	• 8pGEv3 – 12 MIPS core @ 450Mhz • 2p 10GE + 4p GE – 48MIPS core @400Mhz
SAR-18	• 8pGEv3 – 12 MIPS core @ 450Mhz • 2p 10GE + 4p GE – 48MIPS core @400Mhz • 1p 10GE/10p 1GEv2 – 12 MIPS core@450Mhz
SAR-H	12 MIPS core @320Mhz
SAR-Hc	9 MIPS core @320Mhz
SAR-X	2 x 48 MIPS core @400 Mhz
SAR-W	12 MIPS core @400Mhz

SAR-Wx	12 MIPS core @400Mhz
SAR-Ax	2 MIPS core @ 600Mhz

Table 4 – Validated Hardware and FIPS Compatible Platforms

The firmware version used to validate the SARDPCM was SAR-OS Rel 8.0R6.

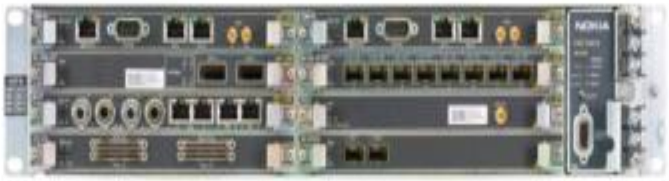

Figure 2-2: Picture of the SAR-8

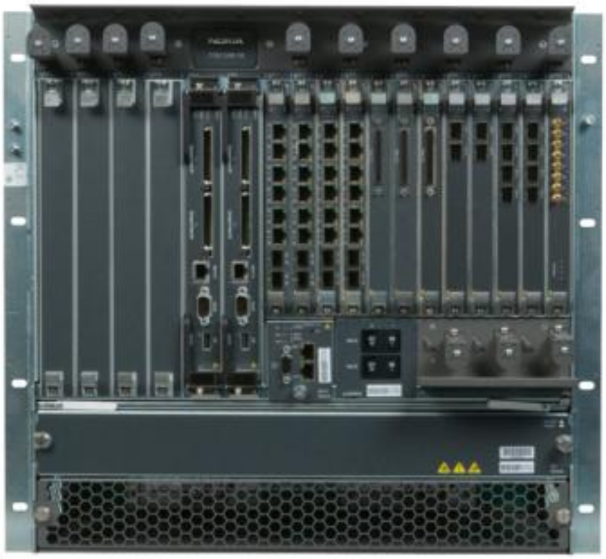

Figure 2-3: Picture of the SAR-18

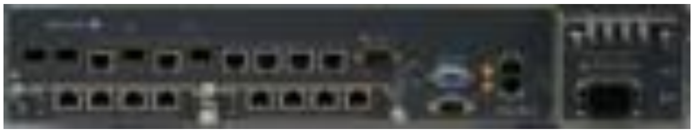

Figure 2-4: Picture of the SAR-H

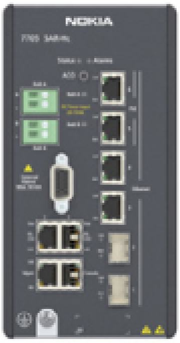

Figure 2-5: Picture of the SAR-Hc

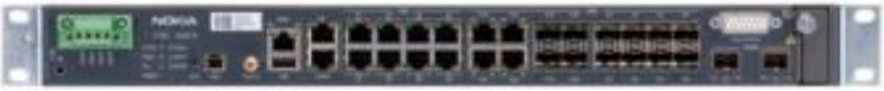

Figure 2-6: Picture of the SAR-X

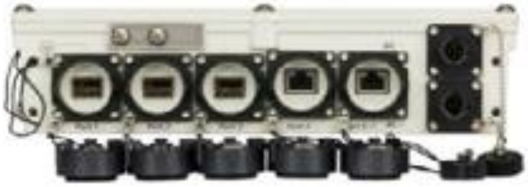

Figure 2-7: Picture of the SAR-W

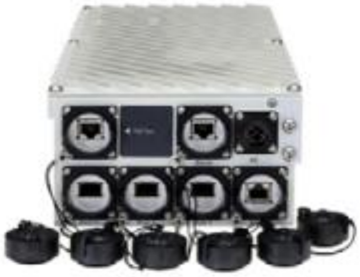

Figure 2-8: Picture of the SAR-Wx

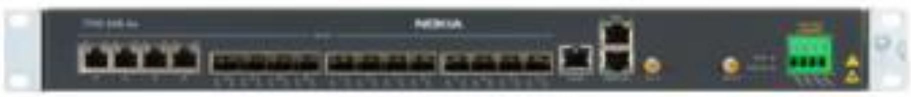

Figure 2-9: Picture of the SAR-Ax

2.2 SARDPCM Approved Algorithms

The SARDPCM uses the following FIPS approved algorithms:

CAVP CERT	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
#4653 #4654	AES	FIPS 197, SP 800-38A	CBC	128, 192, 256	Data encryption/decryption
#2474	Triple-DES[1]	SP 800-67	TCBC		Data encryption/decryption

[1] As of December 31st, 2015 two-key Triple-DES encryption is Disallowed

#2475					
#3081 #3082	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 116, 128,192,256	Message Authentication
#3812 #3813	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-224, SHA-512		Message Digest

Table 5 – Approved Algorithm Implementations

2.3 SARDPCM Interfaces

The physical ports used by SARDPCM within SAR-OS are the same as those available on the system which is running SAR-OS per the platforms specified in the previous section. The logical interface is a C-language application program interface (API).

The Data Input interface consists of the input parameters of the API procedures and includes plaintext and/or cipher text data.

The Data Output interface consists of the output parameters of the API procedures and includes plaintext and/or cipher text data.

The Control Input interface consists of API functions that specify commands and control data used to control the operation of the module. The API may specify other functions or procedures as control input data.

The Status Output includes the return status, data and values associated with the status of the module.

The module provides logical interfaces to the other services within SAR-OS and those other SAR-OS services use the following logical interfaces for cryptographic functions: data input, data output, control input, and status output.

Interface	Description
Data Input	API input parameters including plaintext and/or cipher text data
Data Output	API output parameters including plaintext and/or cipher text data

Control Input	API procedure calls that may include other function calls as input, or input arguments that specify commands and control data used to control the operation of the module.
Status Output	API return code describing the status of SARDPCM

Table 6 – FIPS 140-2 Logical Interface Mappings

3. SARDPCM ROLES AND SERVICES

The SARDPCM meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing support for both the Crypto Officer and User roles within the SARDPCM. The support for both Crypto Officer and User roles within the SARDPCM is classed as a process. As allowed by FIPS 140-2, the SARDPCM does not support user authentication for these roles. Only one role may be using the SARDPCM at a time and the module does not allow concurrent operators to access the SARDPCM.

The User and Crypto Officer roles are implicitly assumed by the entity accessing the services implemented by the SARDPCM:

- Installation and initialization of the SARDPCM which is embedded in the SAR-OS image and installed on the SAR-OS platforms is assumed implicitly as the Crypto Officer when installation and initialization occurs.

The services available by the SARDPCM in FIPS mode to the Crypto Officer and User roles consist of the following:

Services	Access	Critical Security Parameters	Crypto Officer	User
Encryption	Execute	Symmetric keys AES, Triple-DES	X	X
Decryption	Execute	Symmetric keys AES, Triple-DES	X	X
Hash (HMAC)	Execute	HMAC SHA keys	X	X
Perform Self-Tests	Execute/read	NA	X	X
Show Status	Execute	NA	X	X
Zeroization	Execute	Symmetric key, HMAC-SHA keys	X	X

Module Initialization	Execute	All CSPs	X	

Table 7 – Module Services

4. PHYSICAL SECURITY

The module obtains its physical security from any platform running SAR-OS with production grade components and standard passivation as allowed by FIPS 140-2 level 1.

5. OPERATIONAL ENVIRONMENT

The SARDPCM was tested on the following platforms that represent the required HW components that runs SAR-OS and the SARDPCM.

Platform used for testing/validation	**Hardware running SAR-OS**
SAR-8	6 core @ 800Mhz, on CSMv2 module
SAR-18	8 core @600Mhz on SAR-18 CSM module
SAR-H	2 core @600Mhz on chassis
SAR-Hc	2 core @600Mhz on chassis
SAR-X	8 core @800Mhz on chassis
SAR-W	1 core @500Mhz on chassis
SAR-Wx	2 core @600Mhz on chassis
SAR-Ax	2 core @600 Mhz on chassis

Table 8 – Hardware and Platforms Used to Test Module

6. KEY TABLE

6.1 Keys/CSPs Algorithms In FIPS-140-2 Mode

The following keys and CSPs are available when running in FIPS-140-2 mode for the SARDPCM:

Key or CSP	Usage (Service)	Storage	Generation/Input	Zeroization	Access Role (R,W,X)
Triple DES-CBC	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
AES-128-CBC	NGE	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W, X
AES-128-CBC	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
AES-192-CBC	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
AES-256-CBC	NGE	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W, X
AES-256-CBC	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
HMAC-SHA-1	Integrity	Non-Volatile	Operator –	Command	R, W

		memory (Obfuscated)	Manually		
HMAC-SHA-1	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
HMAC-SHA-256	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
HMAC-SHA-256	NGE	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W,X
HMAC-SHA-384	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
HMAC-SHA-512	IPSec	Non-Volatile memory (Obfuscated)	API parameter	Reboot, Command	R, W, X
HMAC-SHA-512	NGE	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W, X

Table 9 – Cryptographic Keys and CSPs

Access roles include “R”- Read, “W” – Write, and “X” – Execute.

7. EMC/EMI (FCC COMPLIANCE)

The SAR chassis where the Network Processor, SAR-OS and SARDPCM runs were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

8. SELF TESTS

8.1 Self Tests on the Dataplane

When FIPS-140-2 mode is enabled the node performs the following startup tests:

- Firmware integrity check on startup using HMAC-SHA-1
- Triple-DES encrypt KAT
- Triple-DES decrypt KAT
- AES encrypt 128, 192,256 KAT
- AES decrypt 128, 192,256 KAT
- HMAC SHA-1 KAT, HMAC SHA-224 KAT, HMAC-SHA-256 KAT, HMAC SHA-384 KAT, HMAC SHA-512 KAT
- SHA-1 KAT, SHA-224 KAT, SHA-256 KAT, SHA-384 KAT, SHA-512 KAT

Should any of these tests fail, the SARDPCM does not allow the network processor to continue booting the image. An error is displayed on the console port that indicates the failed test and the SARDPCM forces a reboot of the network processor module to attempt the self-tests again.

8.2 Conditional Test on the CSM

When FIPS-140-2 mode is enabled the node performs the following conditional self tests during normal operation of the node:

- Manual Key Entry Tests

Descriptions of the tests are described in the following sections.

SARDPCM Failure

When a Conditional Test (e.g. Manual Key Entry Test) fails, then the SARDPCM is considered as failed. The node will print a message on the console that indicates that the SARDPCM has failed.

9. FIPS-140 USER GUIDANCE

The following sections described the SAR-OS user guidance for configuring the SAR systems where the SARDPCM is embedded and accessed by SAR-OS.

9.1 FIPS-140-2 Mode Configuration

To enable FIPS-140-2 on the 7705 a configurable parameter is available in the bof.cfg file. When configured in the bof.cfg, the node boots in FIPS-140-2 mode and the following behaviors are enabled on the node:

- Only FIPS-140-2 approved algorithms (except for two-key Triple-DES) are available for encryption and authentication for any cryptographic function on the CSM where SAR-OS and the SARDPCM reside
- Two-key Triple-DES Encryption must not be used in FIPS mode; otherwise the module will enter a non-FIPS mode.
- Startup tests are executed on the network processor when the node boots
- Conditional tests are executed when required during normal operation (e.g. manual key entry test)
- In accordance to NIST guidance, operators are responsible for insuring that a single Triple-DES key shall not be used to encrypt more than 2^16 64-bit data blocks.

The current state of the bof and the parameters used for booting can be verified with the following CLI commands:

```
*A:bkvm12>show bof
*A:bkvm12>show bof booted
```

Note the FIPS-140-2 parameter in the bof.cfg does not take effect until the node has been rebooted. When running in FIPS mode the system will display a value in the system command that indicates this is the case.

9.2 Non-FIPS-140-2 Mode

During operation, the module can switch modes on a service-by-service basis between an Approved mode of operation and a non-Approved mode of operation. The module will also transition to the non-Approved mode of operation when the “Encryption” service is invoked using Two-key Triple DES. The module transitions back to the Approved mode of operation upon the utilization of an Approved security function.

The module supports the Crypto Officer and User roles while in the non-Approved mode of operation.

Table 10 below lists the service(s) available in the non-Approved mode of operation.

Services	Access	Non-Approved Keys	Crypto Officer	User
Encryption (non-compliant when using Two-key Triple DES)	Execute	Triple-DES	X	X

Table 10 – Non-Approved Services

10. REFERENCES

[FIPS 140-2]	FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, CHANGE NOTICES (12-03-2002). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[FIPS 140-2 DTR]	Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, January 4, 2011 Draft. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402DTR.pdf
[FIPS 140-2 IG]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, May 10, 2012. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf