SR-OS Cryptographic Module (SRCM)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level:1

Document Version: 1.5

April 7, 2016

TABLE OF CONTENTS

LIST OF FIGURES

GLOSSARY

AES-128, AES-256	*Advanced Encryption Standard*
BGP	*Border Gateway Protocol*
CBC	*Cipher Block Chaining*
CFM	*Control / Forwarding Module*
CLI	*Command Line Interface*
CMVP	*Cryptographic Module Validation Program*
CPM	*Control Processor 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*
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*
TM	*Traffic Management*
VPLS	*Virtual Private LAN Service*

Table 1 - Glossary

1. INTRODUCTION

1.1 Purpose

This document describes the non-proprietary SR-OS (Service Router Operating System) Cryptographic Module (SRCM) Security Policy for the 7950 XRS, 7750 SR and the 7450 ESS product families. These are referenced in the document as either 7x50 or XRS/SR/ESS.

This security policy provides the details for configuring and running the 7x50 products in a FIPS-140-2 mode of operation and describes how the module meet 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	N/A
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 7x50 products that implement the module are either tested or compatible for running SRCM in a FIPS approved mode:

Platform	Model(s)
7950 Extensible Routing System (XRS)	XRS-40, XRS-20, XRS-16c
7750 Service Router (SR)	SR-12e, SR-12, SR-7, SR-c12, SR-c4, SR-a8 and SR-a4
7450 Ethernet Services Switch (ESS)	ESS-12, ESS-7

Table 3 - FIPS Capable Platforms and Models

Note: the following platforms are FIPS tested and validated:

CPM-7950 XRS-20 CPM;

CPM-7950 XRS-16 CPM;

CPM-7750 SR CPM5;

CFM-7750 SR-c12 CFM-XP-B;

CPM-7750 SR-a

All other platforms are vendor affirmed for FIPS compatibility.

2. SR-OS CRYPTOGRAPHIC MODULE OVERVIEW

The section provides an overview of the SR-OS Cryptographic Module (SRCM) and the FIPS validated cryptographic algorithms used by services requiring those algorithms. The SRCM does implement any services or protocols directly. Instead, it provides the cryptographic algorithm functions needed to allow SR-OS to implement cryptography for those services and protocols that require it.

2.1 SRCM Characteristics

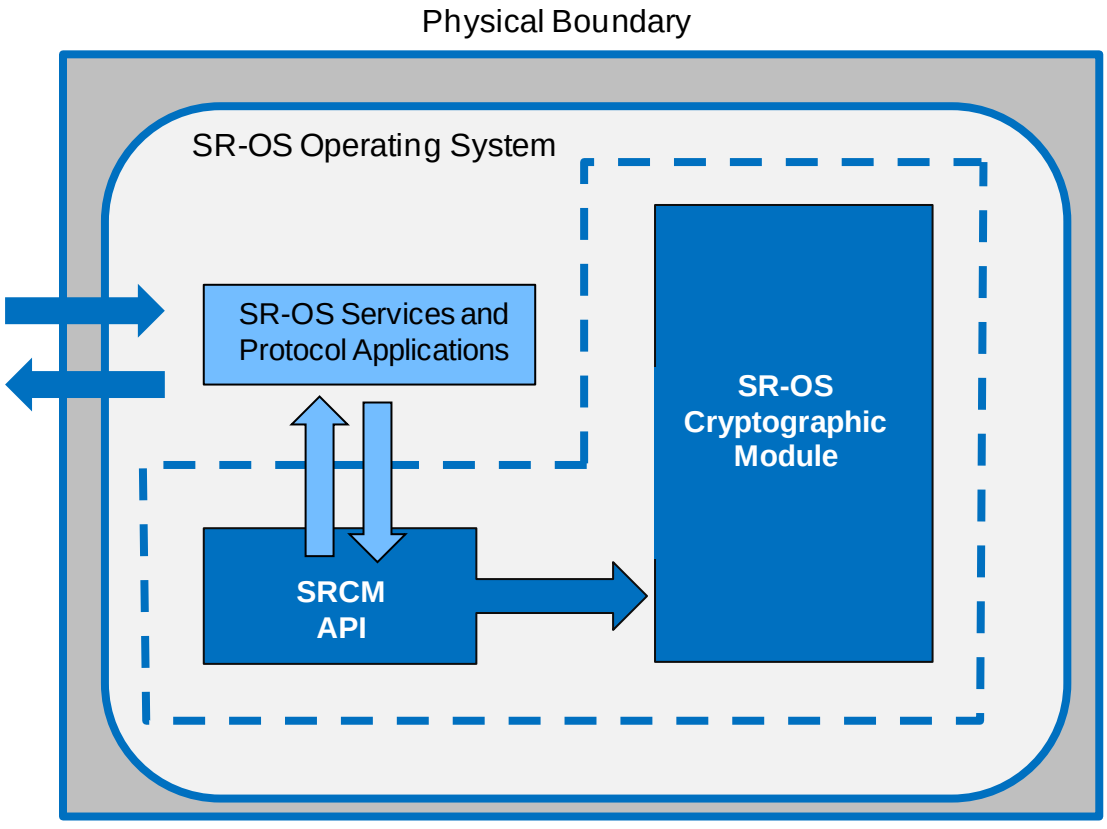

Figure 2-1: SRCM Diagram of Logical and Physical Boundaries

The SRCM 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 SR-OS is running and hence where SRCM is also running. The dashed blue line indicates the logical cryptographic boundary of the SRCM within SR-OS. The SRCM is available as a cryptographic service for any SR-OS services or protocols that require cryptographic operations.

The SRCM is part of a single SR-OS binary file (cpm.tim) that is used to run the full SR-OS application. SRCM is classified as a multi-chip standalone firmware module and SRCM is included within the SR-OS application code. SRCM has been validated on each CPM used by the hardware platforms listed in the following table:

Hardware Running SRCM	Platforms
1.5Ghz 10 core CPU on CPM-7950 XRS-20 CPM	7950 XRS-40, XRS-20
1.5Ghz 10 core CPU on CPM-7950 XRS-16 CPM	7950 XRS-16c
1.5Ghz 10 core CPU on CPM-7750 SR CPM5	7750 SR-12e, SR-12, SR-7, ESS-12, ESS-7
750Mhz 10 core CPU on CFP-7750 SR-c12 CFM-XP-B	7750 SR-c12, SR-c4
800Mhz 6 core CPU on CPM-7750 SR-a	7750 SR-a8, SR-a4

Table 4 – Validated Hardware (CPMs and CFP) and FIPS Compatible Platforms (tested or Nokia affirmed)

The firmware version used to validate the SRCM was SR-OS 13.0R4.

2.2 SRCM Approved Algorithms

The SRCM uses the following FIPS approved algorithms:

Algorithm	Certificate #
AES CBC (e/d; 128, 192, 256); CTR (ext only; 128, 192, 256) CMAC[1]	#3484
Triple-DES[2] (TCBC)	#1965
RSA FIPS186-2: RSASSA PKCS v1.5 1024-bit Signature Verification FIPS186-4: ANSI X9.31 2048-bit & 3072-bit Signature Generation ANSI X9.31 1024-bit, 2048-bit & 3072-bit Signature Verification RSASSA PKCS v1.5: 2048-bit & 3072-bit Signature Verification RSASSA PKCS v1.5: 1024-bit, 2048-bit & 3072-bit Signature Verification	#1789
HMAC (HMAC-SHA 1, HMAC-SHA-224, HMAC-SHA 256, HMAC-SHA-384, HMAC-SHA-512)	#2226

1 The CMAC function was CAVP tested but is not used in Approved mode

2 As of December 31st, 2015 two-key Triple-DES is Disallowed

SHA (SHA-1, SHA-224, SHA-256, SHA-224, SHA-512)	#2878
DRBG CTR_DRBG	#861
DSA FIPS186-4: 2048-bit & 3072-bit PQG Generation & Verification 2048-bit & 3072-bit Signature Generation 1024-bit, 2048-bit & 3072-bit Signature Verification	#985
CVL Section 5.2, SSH SP800-135	#560

Table 5 – Approved Algorithm Implementations

2.3 SRCM non-Approved but Allowed Algorithms

The module supports the following non-FIPS approved algorithms which are:

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- NDRNG

2.4 SRCM Interfaces

The physical ports used by SRCM within SR-OS are the same as those available on the system which is running SR-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 SR-OS and those other SR-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 SRCM

Table 6 – FIPS 140-2 Logical Interface Mappings

3. SRCM ROLES AND SERVICES

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

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

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

The services available by the SRC 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
Key generation	Write/execute	Symmetric key AES, Triple-DES, Asymmetric RSA, DSA, Diffie-	X	X

		Hellman public and private keys		
Key agreement	Execute	DH public/private key	X	X
Perform Self-Tests	Execute/read	NA	X	X
DRBG	Execute	Seed input	X	X
Show Status	Execute	NA	X	X
Signature signing	Execute	Asymmetric private key DSA, RSA	X	X
Signature verification	Execute	Asymmetric public key DSA, RSA	X	X
Zeroization	Execute	Symmetric key, asymmetric key, HMAC-SHA keys, seed key, seed	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 SR-OS with production grade components and standard passivation as allowed by FIPS 140-2 level 1.

5. OPERATIONAL ENVIRONMENT

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

Hardware Running SRCM	Platform used for testing and validation
1.5Ghz 10 core CPU on CPM-7950 XRS-20 CPM	7950 XRS-20
1.5Ghz 10 core CPU on CPM-7950 XRS-16 CPM	7950 XRS-16c
1.5Ghz 10 core CPU on CPM-7750 SR CPM5	7750 SR-12e
750Mhz 10 core CPU on CFP-7750 SR-c12 CFM-XP-B	7750 SR-c12
800Mhz 6 core CPU on CPM-7750 SR-a	7750 SR-a4

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 SRCM:

Key or CSP	Usage (Service)	Storage	Generation/Input	Zeroization	Access Role (R,W,X)
Triple DES	SSHv1	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
Triple DES-CBC	SSHv2, AA Local List File	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
AES-256-CTR	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
AES-192-CTR	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
AES-128-CTR	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
AES-128-CBC	SSHv2, Secure Copy, SNMP	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
Triple DES-CBC	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
AES-192-	SSHv2,	DRAM	Approved DRBG,	Reboot,	R, w, X

CBC	Secure Copy	(plaintext)	API parameter	Command	
AES-256-CBC	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, w, X
HMAC-SHA-1	OSPF, IS-IS, RSVP, SSHv2, Software Integrity	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W
HMAC-SHA-256	OSPF, IS-IS, Python Script Authentication	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W
AES-128-CBC	SNMP	Non-Volatile memory (Obfuscated)	Operator – Manually	Command	R, W
RSA Public Key	SSHv2, IPv6 Neighbor Discovery Protocol	Non-Volatile memory (Obfuscated)	Approved DRBG, API parameter	Reboot, Command	R, W, X
RSA Private Key	SSHv2, IPv6 Neighbor Discovery Protocol	Non-Volatile memory (Obfuscated)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DSA Public Key	SSHv2	Non-Volatile memory (Obfuscated)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DSA Private Key	SSHv2	Non-Volatile memory (Obfuscated)	Approved DRBG, API parameter	Reboot, Command	R, W, X
Diffie-	SSHv2	DRAM	Approved DRBG,	Reboot,	R, W, X

Hellman Private Key		(plaintext)	API parameter	Command	
Diffie-Hellman Public Key	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DRBG Seed	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W
DRBG Entropy	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W
DRBG 'V' Value	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W
DRBG 'Key' Value	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W

Table 9 – Cryptographic Keys and CSPs

The SSH and SNMP protocols have not been reviewed or tested by the CAVP or CMVP.

7. EMC/EMI (FCC COMPLIANCE)

The XRS/SR/ESS chassis where the CPM, SR-OS and SRCM 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 CPM

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 KAT
- AES decrypt 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
- RSA sign and verify
- A DSA pairwise consistency test

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

8.1.1 Cryptographic DRBG Startup Test

A known answer test is used by the DRBG on startup (by using a known seed). If the startup test fails then an error message is printed on the console and the node will attempt the boot sequence again.

8.1.2 RSA Startup test

SRCM performs an initial startup test with a known public key, a known digital signature and a test that verifies it can perform a proper verification of the known signature with the known public key. If the SRCM fails to successfully perform this startup test, then a message is printed on the console, the SRCM causes the node to reboot and tries to perform all the startup tests successfully again from the beginning.

8.2 Conditional Test on the CPM

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
- Pairwise Consistency Test for RSA / DSA Keys
- Continuous Random Number Generator Test (CRNGT)

Descriptions of the tests are described in the following sections.

SRCM Failure

When a Conditional Test (e.g. the pairwise consistency tests or the CRNGT test) fails, then the SRCM is considered as failed. The node will print a message on the console that indicates that the SRCM has failed.

9. FIPS-140 USER GUIDANCE

The following sections described the SR-OS user guidance for configuring the XRS/SR/ESS systems where the SRCM is embedded and accessed by SR-OS.

9.1 FIPS-140-2 Mode Configuration

To enable FIPS-140-2 on the XRS/SR/ESS 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 and Diffie-Hellman with key sizes less than 2048 bits) are available for encryption and authentication for any cryptographic function on the CPM where SR-OS and the SRCM reside
- Two-key Triple-DES and Diffie-Hellman with non-compliant key sizes must not be used in FIPS mode; otherwise the module will enter a non-FIPS mode.
- Startup tests are executed on the CPM when the node boots
- Conditional tests are executed when required during normal operation (e.g. manual key entry test, pairwise consistency checks and RNG tests)

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 Configurations Not Allowed when running in FIPS-140-2 Mode

When the node is configured in FIPS-140-2 mode the following dis allowed algorithms are visible in CLI but not available. The User must not configure the following algorithms and functions when running in FIPS-140-2 mode or reverse the configuration steps in Section 9.1:

- MD5
    - SNMP, OSPF, BGP, LDP, NTP authentication, multi-chassis redundancy
- HMAC-MD5

  SNMP, IS-IS, RSVP
- HMAC-MD5-96
    - SNMP
- HMAC-SHA-1-96
    - SNMP, OSPF, BGP, LDP
- AES-128-CMAC-96
    - BGP, LDP

9.3 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 transition to the non-Approved mode of operation when the “Key agreement” service is invoked using non-compliant Diffie-Hellman key sizes (less than 2048 bits). This includes key sizes of 512 and 1024 bits. 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	Critical Security Parameters	Crypto Officer	User
Encryption (non-compliant when using Two-key Triple DES)	Execute	Triple-DES	X	X
Key agreement (non-compliant)	Execute	DH public/private key	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 2, 2012. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf