NOKIA

NOKIA

Corporation

7705 SAR-OS SAR-A/M Cryptographic Module (SARCM 3.1 SAR-OS 20.4 R3)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level:1

Document Version: 1.8

November 5th, 2020

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 (SARCM) 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 level 1 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	N/A
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 that implement the module are either tested or compatible for running SARCM in a FIPS approved mode:

Platform	Model(s)
7705 Service Aggregation Router (SAR) non-IPsec/NGE	SAR-A, SAR-M

Table 3 - FIPS Capable Platforms and Models

2.   SAR-OS CRYPTOGRAPHIC MODULE OVERVIEW

The section provides an overview of the SAR-OS Cryptographic Module (SARCM) and the FIPS validated cryptographic algorithms used by services requiring those algorithms. The SARCM 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.

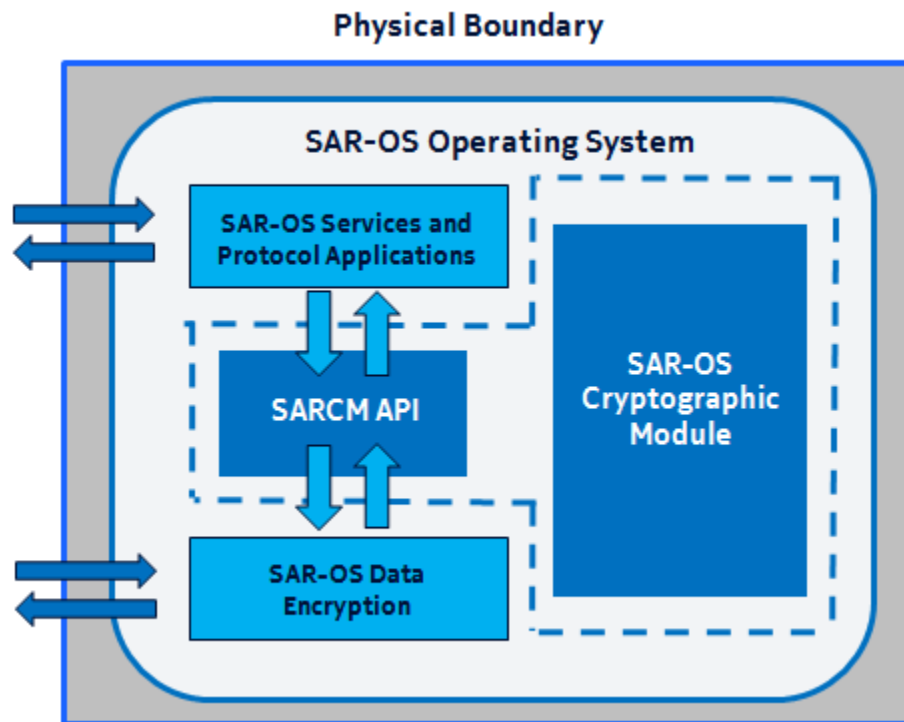### 2.1   SARCM Characteristics

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

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

The SARCM provides the cryptographic services required for the control plane (ie routing protocols etc). On the 7705 SAR-A and SAR-M, 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 these platforms the CSM and line cards are physically on the same hardware, but logically separate. The Winpath network processor on these platforms are not encryption capable.

The SARCM is part of two SAR-OS binary files (both.tim and support.tim) that are used to run the full SAR-OS application. SARCM is classified as a multi-chip standalone software module and SARCM is statically included within the SAR-OS application code. SARCM 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-M and A variants

Platform	Hardware running SAR-OS	Processor
SAR-A	1 core @ 300 MHz on chassis	Cavium Octeon Plus
SAR-M	1 core @ 500 MHz on chassis	Cavium Octeon Plus

Table 4 – Validated Hardware and FIPS Compatible Platforms

The software version used to validate version 3.1 of the SARCM was SAR-OS 20.4 R3.

2.2 SARCM Approved Algorithms

There are algorithms, modes, and keys that have been CAV tested but not used by the module. Only the algorithms, modes, and key lengths in this table are used by the module.

The SARCM uses the following FIPS approved algorithms:

Algorithm	CAVP Cert (20.4R3)
AES CBC (e/d; 128, 192, 256); CFB128 (e/d;128); CTR (e only; 128, 192, 256)	C2073
CKG SP 800 133 Seeds used for generating symmetric & asymmetric keys are unmodified output from Module's DRBG. Section 5 & 6	Vendor affirmed

Triple-DES (TCBC) (e/d; keying option 1)	C2073
RSA FIPS186-2:ANSI X9.31 1024-bit & 1536-bit& 2048-bit & 3072-bit & 4096-bit signature verification FIPS186-2: PKCS v1.5 1024-bit & 1536-bit& 2048-bit & 3072-bit & 4096-bit Signature Verification FIPS186-2: PKCSPSS 1024-bit & 1536-bit& 2048-bit & 3072-bit & 4096-bit Signature Verification FIPS186-4: ANSI X9.31 2048-bit & 3072-bit Signature Generation FIPS186-4: PKCS v1.5 2048-bit & 3072-bit Signature Generation FIPS186-4: PKCSPSS 2048-bit & 3072-bit Signature Generation FIPS186-4: 3072-bit Key Pair Generation [FIPS186-4_Fixed_e (10001) FIPS186-4: ANSI X9.31 1024-bit, 2048-bit & 3072-bit Signature Verification FIPS186-4: PKCS v1.5: 1024-bit, 2048-bit & 3072-bit Signature Verification FIPS186-4: PKCSPSS: 1024-bit, 2048-bit & 3072-bit Signature Verification	C2073
HMAC (HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512)	C2073
AES-GCM • Direction: Decrypt, Encrypt • IV Generation: External • Key Length: 256 • Tag Length: 128 • IV Length: 96 • Payload Length: 8, 128, 256, 408 • AAD Length: 8, 128, 256, 408 **AES-GMAC** • Direction: Decrypt, Encrypt • IV Generation: External • Key Length: 256 • Tag Length: 128 • IV Length: 96 • AAD Length: 8, 128, 256, 408	C2073

CMAC AES-128 Generation
 o Capabilities:
  ▪ Direction: Generation
  ▪ Key Length: 128
  ▪ MAC: 64, 96, 128
  ▪ Message Length: 0, 128, 320, 480, 512, 524288
 o Capabilities:
  ▪ Direction: Verification
  ▪ Key Length: 128
  ▪ MAC: 64, 96, 128
	C2073

▪ Message Length: 0, 128, 320, 480, 512, 524288	
SHS (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	C2073
DRBG CTR_DRBG (AES-256)	C2073
DSA FIPS186-4: 2048-bit & 3072-bit PQG Generation FIPS186-4: 1024-bit & 2048-bit & 3072-bit PQG Verification FIPS186-4: 2048-bit & 3072-bit Key Pair Generation [(2048,256) ; (3072,256)] FIPS186-4: 2048-bit & 3072-bit Signature Generation [(2048,224 & 256) ; (3072,256)] FIPS186-4: 1024-bit, 2048-bit & 3072-bit Signature Verification [(1024,160) ; (2048,224 & 256) ; (3072,256)]	C2073
CVL SSH KDF (SHA-1) SHA, (SHA-2) SHA2-512, SHA2-256, (128-bit, 192-bit, 256-bit) AES-CBC, TDES-CBC	C2073

Table 5 – Approved Algorithm Implementations

2.3 SARCM non-Approved but Allowed Algorithms

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

- Diffie-Hellman (CVL Cert. #C2073, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength).

- NDRNG seeded with 256 bits of entropy.

2.4 SARCM Interfaces

The physical ports used by SARCM 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 SARCM

Table 6 – FIPS 140-2 Logical Interface Mappings

3. SARCM ROLES AND SERVICES

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

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

- Installation and initialization of the SARCM 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 SARCM 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-Hellman public and private keys	X	X
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 SAR-OS with production grade components and standard passivation as allowed by FIPS 140-2 level 1.

5. OPERATIONAL ENVIRONMENT

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

Platform used for testing/validation	Hardware running SAR-OS
SAR-A	1 core @ 300 MHz on chassis, Cavium Octeon Plus
SAR-M	1 core @ 500 MHz on Chassis, Cavium Octeon Plus

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 SARCM:

Key or CSP	Usage (Service)	Storage	Generation/Input	Zeroization	Access Role (R,W,X)
AES-128-CFB	SNMPv3	Non-Volatile memory (Encrypted*)	Operator – Manually	Command	R, W
AES-128-CBC	SSHv2, Secure Copy, SFTP	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-192-CBC	SSHv2, Secure Copy, SFTP	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-256-CBC	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-128-CTR	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-192-CTR	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-256-CTR	SSHv2	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
DSA Public Key 1K	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DSA Private Key 1K	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-CMAC	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-GCM	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
HMAC-SHA-1	OSPF, IS-IS, RSVP, Software Integrity	DRAM (plaintext)	Operator – Manually	Command	R, W

Key or CSP	Usage (Service)	Storage	Generation/Input	Zeroization	Access Role (R,W,X)
HMAC-SHA-1	SSHv2,	DRAM (plaintext)	Operator – Manually	Command	R, W, X
HMAC-SHA-1	SNMPv3	DRAM (plaintext)	Operator – Manually	Command	R, W
HMAC-SHA-256	OSPF, IS-IS, RSVP	DRAM (plaintext)	Operator – Manually	Command	R, W
HMAC-SHA-256	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
HMAC-SHA-512	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
RSA Public Key – 2048, 3074 bits	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
RSA Private Key - 2048, 3074 bits	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
Diffie-Hellman Public Key Group 14 (P=>2048 prime numbers, q>224)	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
Diffie-Hellman Private Key Group 14 (P=>2048 prime numbers, q>224)	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

* Encrypted via AES-128-CBC

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

No network protocols including SNMP or SSH have been reviewed or tested by the CAVP or CMVP. SSH KDF was tested.

The user is responsible for ensuring the module limits the number of encryptions with the same Triple-DES key to 2^16.

7. EMC/EMI (FCC COMPLIANCE)

The SAR chassis where the CSM, SAR-OS and SARCM 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 CSM

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

- Software integrity check on startup using HMAC-SHA-256
- DRBG KAT and health test
- Triple-DES encrypt KAT
- Triple-DES decrypt KAT
- AES CBC 128, 192, 256 encrypt KAT
- AES CBC 128, 192, 256 decrypt KAT
- AES CFB128 encrypt KAT
- AES CFB128 decrypt KAT
- AES CTR 128, 192, 256 encrypt KAT
- AES GCM 256 encrypt KAT
- AES GCM 256 decrypt KAT
- AES GMAC 256 encrypt KAT
- AES GMAC 256 decrypt KAT
- AES CMAC 128 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 SARCM 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 SARCM 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

SARCM 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 SARCM fails to successfully perform this startup test, then a message is printed on the console, the SARCM causes the node to reboot and tries to perform all the startup tests successfully again from the beginning.

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

- Pairwise Consistency Test for RSA / DSA

- DRBG and NDRNG Continuous Random Number Generator Test (CRNGT)

Descriptions of the tests are described in the following sections.

SARCM Failure

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

Manual Key Entry Tests
Cryptographic key or key components manually entered into the cryptographic module are entered using duplicate entries. If the duplicate entries do not match, the test shall fail.

Pairwise Consistency Test for RSA, DSA
The Pairwise Consistency Test is performed whenever public or private keys are generated. The consistency of RSA/DSA keys is tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test shall fail.
An additional test is performed on RSA key pairs. A plaintext value is encrypted by the RSA public key. The resulting ciphertext value is compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key is used to decrypt the ciphertext and the resulting value are compared to the original plaintext value. If the two values are not equal, the test shall fail.

Continuous Random Number Generator Test (CRNGT)

The CRNGT is performed for every RNG call. Each call to a RNG produces blocks of 128 bits. The first 128-bit block generated after power-up, initialization, or reset is not used, but is saved for comparison with the next 128-bit block to be generated. Each subsequent generation of an 128-bit block is compared with the previously generated block. The test shall fail if any two compared 128-bit blocks are equal.

9. FIPS-140 USER GUIDANCE

The following sections described the SAR-OS user guidance for configuring the SAR systems where the SARCM 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. The command "/bof fips-140-2" needs to be typed in and followed by a "/bof save" and reboot of the node. 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 CSM where SAR-OS and the SARCM reside

- 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 CSM 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**

The output of "show bof booted" would show "fips-140-2" instead of "no fips-140-2".

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 disallowed 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

- o SNMP

- HMAC-SHA-1-96

    - o SNMP, OSPF, BGP, LDP

- AES-128-CMAC-96

    - o BGP, LDP

9.3 Non-FIPS-140-2 Mode

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

To disable FIPS-140-2 on the SAR-A/M, the User must configure the bof with "no fips-140-2" and reboot the system to transition to the non FIPS-140-2 mode. The User must delete persistent keys before switching mode.

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