SXF1800

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Document Version 1.1

July 22, 2020

Prepared for:

NXP Semiconductors Netherlands B.V.
High Tech Campus 60
5656 AG Eindhoven
Netherlands
nxp.com
+31 40 272 9999

Prepared by:

KeyPair Consulting Inc.
987 Osos Street
San Luis Obispo, CA 93401
keypair.us
+1 805.316.5024

Table of Contents

List of Tables

List of Figures

References and Definitions

Acronym	Full Specification Name
References used in Approved Algorithms Table	
[197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[186]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[90A]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Rev. 1 June 2015
[108]	NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[38F]	NIST SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012

Other References	
[140]	NIST, FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001
[57]	NIST SP 800-57, *Recommendation for Key Management Part 1: General*, Rev. 5 May 2020
[GP]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.3,* October 2015, *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004
[140IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 29 June 2020
[7816]	ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[JavaCard]	*Java Card 3 Platform Runtime Environment (JCRE) Specification* *Java Card 3 Virtual Machine (JCVM) Specification* *Java Card 3 Application Programming Interface* Published by Sun Microsystems, 2015
[131A]	NIST, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 2 March 2019
[GPSCP]	GlobalPlatform Card Technology – Secure Channel Protocol '3' – Card Specification v2.2 – Amendment D, Version 1.1.1, July 2014
[UGM]	*JCOP 4.4 Automotive User Guidance Manual*, Rev. 1.2 September 2019.

Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard, see [197]
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CM	Card Manager, see [GP]: provides GlobalPlatform Issuer Security Domain (ISD) services, for administration of the GP Secure Element.
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter, see [140]
DAP	Data Authentication Pattern, see [GP]
DPA	Differential Power Analysis
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECQV	Elliptic Curve Qu-Vanstone
GP	GlobalPlatform: see https://www.globalplatform.org
GS	Generic Storage
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GP]
JCOP	Java Card Open Platform
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
NIST	National Institute of Standards and Technology
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP03	Secure Channel Protocol version 3, see [GP]
SE	Secure Element: a single-chip tamper-resistant secure microcontroller capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.
SP	Special Publication
SPA	Simple Power Analysis
SPI	Serial Peripheral Interface
VA	Vendor Affirmed
V2X	Vehicle to everything: Vehicle-to-Vehicle and Vehicle-to-Infrastructure

1 Overview

This document defines the Security Policy for the NXP Semiconductors SXF1800 cryptographic module, hereafter denoted the SXF1800. The SXF1800, validated to FIPS 140-2 overall Level 3 with Level 4 physical security, is a single-chip embodiment module implementing the GlobalPlatform operational environment, with Card Manager, card configuration and V2X applet suite.

The SXF1800, a component of the NXP RoadLINK® architecture, functions as a Secure Element, supporting tamper resistant cryptographic functionality as required by V2X standards. The SXF1800 is designed for configurable support for North America and European V2X standards defined to protect the integrity of exchanged safety messages and to enable authentication of V2X participants.

The SXF1800 is a limited operational environment under the FIPS 140-2 definitions. The SXF1800 includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the CMVP; any other firmware loaded into the SXF1800 is out of the scope of this validation and requires a separate FIPS 140-2 validation.

The FIPS 140-2 security levels for the SXF1800 are given in Table 1.

Security Requirement	Level
Cryptographic SXF1800 Specification	3
Cryptographic SXF1800 Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 1: Security Level of Security Requirements

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the SXF1800 is depicted in Figure 1 (to scale); the shaded area depicts the physical cryptographic boundary. The cryptographic boundary is the surface and edges of the die; the bond pads are the physical ports described in Table 2.

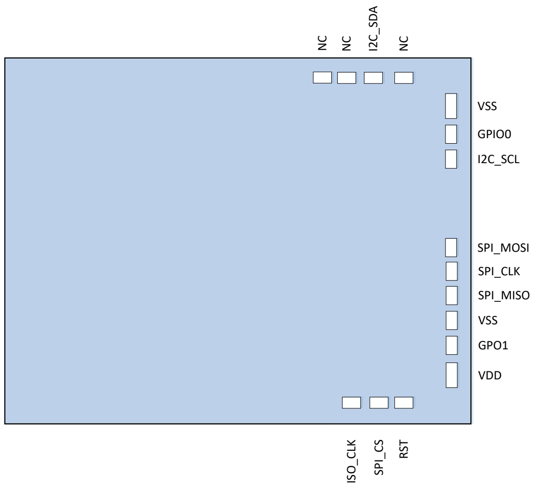

Figure 1: SXF1800 Physical Form

Port	Description	Logical Interface Type
Chip health interface (unused in user deployments)		
I2C_SCL	I2C serial clock line (Failure analysis)	Control in
I2C_SDA	I2C serial data line (Failure analysis)	Control in, Data in, Data out, Status out
ISO_CLK	Interface clock (Failure analysis)	Control in
Normal Use		
GPIO0	Used to indicated SE available	Status out
GPO1	Used to indicate SPI data available	Status out
NC	Not connected	Not connected
RST	Active-low reset	Control in
SPI_CLK	SPI clock	Control in
SPI_CS	SPI chip select	Control in
SPI_MISO	SPI data master input/slave output	Data out, Status out
SPI_MOSI	SPI data master output/slave input	Control in, Data in
$V_{SS,}$ V_{DD}	Supply voltage, ground	Power

Table 2: Ports and Interfaces

The i2C chip health interface signals exist at the cryptographic boundary, but are for failure analysis / diagnostic purposes, and not accessible to end users. This interface cannot be used to access CSPs; the flash is zeroized prior to permitting access to failure analysis functions, leaving the module in a different configuration than the validated configuration. For additional detail, refer to the discussion at the end of Section 1.3.

1.2 SXF1800 Composition

Figure 2 depicts the SXF1800 physical and logical functions, with the cryptographic boundary depicted in red, and the ports and interfaces crossing the boundary at lower left.

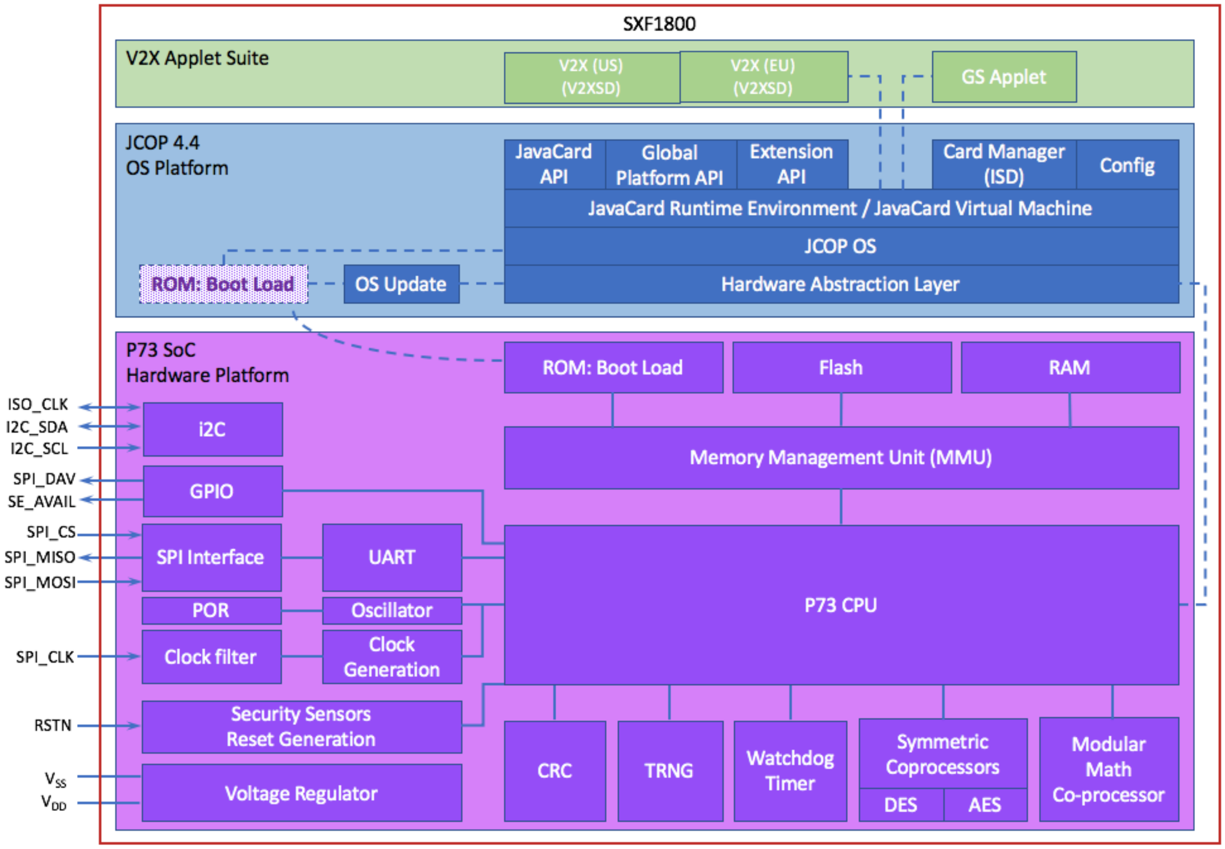

Figure 2: SXF1800 Block Diagram

The JavaCard, Global Platform and Extension APIs are internal interfaces available to applets. Only Card Manager, Config and the V2X and GS applet services are available to external entities.

1.3 Versions, Configurations and Modes of Operation

Hardware: SXF1800HN/V102B

Firmware: JCOP 4.4 R1.16.8; V2X applet v2.12.3; GS applet v2.12.1

The SXF1800 contains 2 instances of the V2X applet: EU and US. Each is selected for use with a unique application identifier (but with a common prefix); is configured with application controls corresponding to EU or US characteristics; and has separate V2X key instances. The V2X applets are designated as non-Approved because NIST does not recognize the ECIES and ECQV functions required to meet V2X standards, but the NHTSA requires the use of the V2X standards as well as FIPS 140-2 compliance.

The SXF1800 has two approved modes of operation and a non-approved mode of operation. The boot load process selects either the OS Update firmware or the JCOP firmware with the V2X applet suite. The *OS Update* approved mode manages update of the operating system. The approved *Operational* mode is the JCOP operating system with any security domain or applet instance selected other than ones from the V2X applet suite. The *Non-Approved Operational* mode is the JCOP operating system with either the EU or US V2X applet instance selected.

The SXF1800 powers up into one of the two Approved modes of operation, indicated by a “90 00” response to any command except selection of one of the two V2X applets. The SXF1800 enters the non-Approved mode if one of the two V2X applets or the GS applet is selected.

The *Non-Approved Operational* mode services are the V2X applet services listed in Section 3.3 below.

The SXF1800 includes an I2C interface used for diagnostics or failure analysis when the SXF1800 has been removed from service. Initiating the diagnostic mode requires authentication; the SXF1800 then erases all content, including applets, associated data and keys. Hence, the initiation of the diagnostic mode represents the transition of the module from an approved configuration to a more generic configuration that is not in the scope of validation. This diagnostic operation occurs only in a manufacturing setting, and is relevant to the FIPS 140-2 validation only to explain the role of the i2C hardware signals that are present on the module. Once the SXF1800 is placed in a diagnostic mode, it cannot be returned to the field.

2 Cryptographic Functionality

The module implements the Approved and Allowed cryptographic functions listed below. Algorithm features enclosed by curly brackets { } are tested but not used by the module.

Cert	Algorithm	Mode	Description	Functions, Caveats
C875	AES [197]	[38A]	CBC (128, 192, 256)	Encrypt, decrypt
		[38A]	{ECB (128, 192, 256)}	Tested but not used
C872	AES [197]	[38B]	CMAC (128, 192, 256)	Message authentication
VA	CKG [133] [140IG] D.12	Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		Symmetric key derivation
C871	CVL: ECDSA [186]	P-256, {P-384} (V2X extension library)		ECC SigGen primitive
C875	DRBG [90A]	CTR	Use_df, AES-256, {AES-128, AES-192} {Prediction Resistance}	Random number generation
C875	ECDSA [186]	P-256 with SHA-256		ECC SigGen
		P-256 with SHA-256		ECC SigVer
		{P-224, P-256, P-384, P-521}		ECC Key Gen (tested but not used)
C878	KBKDF [108]	Counter	CMAC (AES-128, AES-192, AES-256)	Key-based key derivation
VA	KTS [38F]	§3.1¶3	AES, CMAC (Ref: Certs. C872 and C875) AES-128, AES-192, AES-256	Key establishment methodology provides between 128 and 256 bits of security strength
C875	SHS [180]	SHA-256 {SHA-1}		Message Digest

Table 3: Approved Algorithms

Algorithm	Description
EC Diffie-Hellman	One-pass EC Diffie-Hellman scheme with P-256 used in firmware update; complies with [56A] but listed as non-compliant as it is untested.
NDRNG	Hardware RNG; minimum of 8 bits per access. Output from the NDRNG is used only to seed the FIPS approved DRBG.

Table 4: Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
ECIES	Use of ECIES as required by IEEE 1609.2.
ECQV	Use of ECQV as required by IEEE 1609.2.

Table 5: Non-Approved Cryptographic Functions

2.1 Critical Security Parameters and Public Keys

All CSPs used by the SXF1800 are described in this section, categorized by the following prefixes:

- OS prefix denotes operating system.
- OU prefix denotes the operating system updater.
- SD prefix denotes the GlobalPlatform Security Domain.

CSP	Description/Usage
OS-DRBG-EI	400-bit NDRNG entropy input to CTR_DRBG.
OS-DRBG-KV	The current DRBG *V* (128-bit) and *Key* (256-bit) values.
OS-MKEK	AES-128 key used to encrypt all secret and private key data stored in NVM.
OU-FWDK	AES-128 key used to decrypt new firmware.
OU-ECDH	ECC Private key used to derive shared secret OU-KASS.
OU-KASS	Key agreement shared secret used for derivation of OU-FWDK.
SD-KDEK	AES Sensitive data decryption key used to decrypt SCP Keys.
SD-KENC	AES Master key used to derive ([108] KBKDF) SD-SENC.
SD-KMAC	AES Master key used to derive ([108] KBKDF) SD-SMAC and SD-RMAC.
SD-RMAC	AES Session MAC key used to generate response secure channel data MAC.
SD-SENC	AES Session encryption key used to encrypt / decrypt (CBC mode) secure channel data.
SD-SMAC	AES Session MAC key used to verify inbound secure channel data integrity.
Public Key	**Description/Usage**
OU-FWV-Pub	JCOP OS firmware update verification public key (ECC).
OU-ECDH-Pub	ECC public key used to derive shared secret OU-KASS.
SD-DAP-Pub	Public key used for content verification (ECC).
SD-Token-Pub	Public key used for content token authentication (ECC).

Table 6: Critical Security Parameters and Public Keys

The DRBG is seeded via the [90A] block_cipher_df using 264 bits of entropy input and a 136-bit nonce, obtained from the NDRNG, sufficient to support the security strength of the DRBG.
For the SD keys, AES-128, AES-192 and AES-256 are supported as configuration options.

For the EC keys, the following curves are supported:

- NIST P-256 (128-bit equivalent strength; *h* = 1; *nlen* = 256).
- BrainpoolP256r1 (128-bit equivalent strength; *h* = 1; *nlen* = 256).
- BrainpoolP256t1(128-bit equivalent strength; *h* = 1; *nlen* = 256).

3 Roles, Authentication and Services

All operator roles supported by the SXF1800 are listed below, along with the corresponding authentication method. The SXF1800:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.
  - A channel does not permit assumption of more than one role.
  - Applet de-selection (including Card Manager), card reset or power down terminates the current authentication. Re-authentication is required after any of these events for access to authenticated services.

Role ID	Role Description
User	OS Update User - authenticated by signature verification using the OU-FWV-Pub key.
CO	Cryptographic Officer – authenticated using the Secure Channel Protocol Authentication method with the Issuer Security Domain (ISD) keyset.

Table 7: SXF1800 Roles

3.1 Secure Channel Protocol (CO role) Authentication Method

The Secure Channel Protocol authentication method is provided by the *Secure Channel* service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the SXF1800 in the CO role).

The probability that a random attempt will succeed using this authentication method is:

- 1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

After five failed ISD authentication attempts, the SXF1800 imposes a 30 second delay per try. After 15 consecutive failed attempts, the attack counter increments and the SXF1800 initiates a soft reset. The authentication retry count is maintained across reset; that is, the device continues to track failed attempts despite reset. The probability that a random attempt will succeed over a one-minute interval is:

- 7/2^128 = 2.06E-38 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

3.2 User role authentication

The User role is authenticated by signature verification using the OU-FWV-Pub key (ECC P-256 key). The strength of authentication is 128-bits in accordance with [57].

The maximum number of authentications is limited by the speed of the device. Operational tests have shown that no more than 750 authentications can be performed in one minute. The probability that a random attempt will succeed over a one-minute interval is:

- 750/2^128 = 2.2E-36.

3.3 Services

All SXF1800 services are listed below. (UA) refers to unauthenticated; (A) refers to authenticated.

Service	Description	CO	User
Unauthenticated (no role) services			
Context	Select an application or manage logical channels.	N/A	
SXF1800 Info (UA)	Read unprivileged SXF1800 configuration or status information.		
SXF1800 Reset	Power cycle or reset the module. Includes Power-On Self-Test when Initial_Use flag is not set (first time use per [140IG] 9.11).		
CO Role (ISD) authenticated services			
Lifecycle (includes Zeroize)[1]	Modify the card or applet life cycle status.	X	--
Manage Content	Load and install application packages and associated keys and data.	X	--
SXF1800 Info (A)	Read privileged module configuration or status information.	X	--
Secure Channel	Establish and use SCP03 secure communications channel (ISD).	X	--
User authenticated services			
Update OS	Update the operation system.	--	X

Table 8: SXF1800 Approved Mode Services

Service	Description
V2X info (UA)	Report requested V2X or GS information (no CSPs).
Key management	Generation, deletion, activation of key pairs; retrieve public key.
Random	Provide a random value.
Secure Channel	Establish and use SCP03 secure communications channel (V2XSD).
Secure storage	Store, get, delete, return size, and manage data permissions.
Sign message	Sign a provided message.
GS Info (UA)	Read unprivileged GS applet configuration or status information.

Table 9: SXF1800 Non-Approved Mode Services

[1] The Lifecycle service includes the TERMINATE command to destroy all module secrets; the complete Zeroization process requires TERMINATE followed by removal of power.

Service	*CSPs*	OS-DRBG-EI	OS-DRBG-KV	OS-MKEK	OU-FWDK	OU-ECDH	OU-KASS	SD-KDEK	SD-KENC	SD-KMAC	SD-RMAC	SD-SENC	SD-SMAC	*Public Keys*	OU-ECDH-Pub	OU-FWV-Pub	SD-DAP-Pub	SD-Token-Pub
Unauthenticated (no role) services																		
Context		--	--	--	--	--	--	--	--	--	--	--	--		--	--	--	--
SXF1800 Info (UA)		--	--	--	--	--	--	--	--	--	--	--	--		--	--	--	--
SXF1800 Reset		GEZ	GZ	--	Z	Z	Z	--	--	--	Z	Z	Z		--	--	--	--
CO Role (ISD) authenticated services																		
Lifecycle		--	Z	Z	Z	Z	Z	Z	Z	Z	E	E	E		Z	--	--	--
Manage Content		--	--	E	--	--	--	I	I	I	E	E	E		--	--	EI	EI
SXF1800 Info (A)		--	--	--	--	--	--	--	--	--	E	E	E		--	--	--	--
Secure Channel		--	E	E	--	--	--	E	E	E	GE	GE	GE		--	--	--	--
User (OS Update) authenticated services																		
Update OS		--	--	--	GE	E	GE	--	--	--	--	--	--		IE	E	--	--

Table 10: CSP Access by Services

Table 10 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- E = Execute: The service uses the CSP or public key in an algorithm.
- G = Generate: The service generates the CSP or public key.
- I = Input: The service accepts the CSP or public key as input.
- O = Output: The service outputs the CSP or public key.
- Z = Zeroize: The service zeroizes (destroys) the CSP or public key.
- -- = No access. The service does not access the CSP or public key.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset with the *Initial_Use* flag set to 1, the SXF1800 performs the self-tests listed below. If all self-tests pass, the *Initial_Use* flag is set to 0; otherwise it remains set to 1. On receipt of the first command, the SXF1800 returns the *FIPS_Error* status word if any self-test failed; otherwise, the command is executed, returning the corresponding result and status. All KATs must be completed successfully prior to any other use of cryptography by the SXF1800.

In accordance with [140IG] 9.11, if the *Initial_Use* flag is set to 0, self-tests are not performed. The Manage *Content* service permits the *Initial_Use* flag to be reset to 1 to invoke self-tests with the next power-cycle or reset. The *Initial_Use* flag can only be set to 0 by successful completion of all self-tests.

Test Target	Description
AES	Performs encrypt and decrypt KAT using an AES-128 key in ECB mode.
DRBG	Performs separate KATs of the Instantiate and Generate functions.
ECDSA	Performs an ECDSA PCT using the P-256 curve. with SHA-256
ECDSA V2X	Performs an ECDSA PCT using the P-256 curve for the V2X flavor. with SHA-256
Firmware Integrity	Performs CRC16 integrity by sampling in accordance with [140IG] 9.12. The operator can trigger a full test as - see [UGM] Section 4.8.3.
SHA-256, SHA-1	Performs a separate fixed input KAT for each SHA variant.
SP 800-108 KDF	Performs a key derivation KAT using an AES 128 key. This KAT is inclusive of AES CMAC and AES forward cipher (encrypt) KATs per [140IG] 9.2.

Table 11: SXF1800 Power-On Self-Test

4.2 Conditional Self-Tests

The AS09.42 continuous RNG test is not required for a [90A] compliant DRBG, per [140IG] 9.8. The SXF1800 NDRNG is only used to seed the DRBG on power-up and is not used for any other function or purpose: IG 9.8 (additional comment 1) applies and the continuous RNG test is not required for the output of the NDRNG.

Firmware load testing: When new firmware packages are loaded into the SXF1800 using the *Manage Content* service, the SXF1800 verifies the package integrity using MAC verification with the SD-SMAC key; the package integrity may also be verified using signature verification with the optional SD-DAP-Pub key.

Firmware load testing: When new OS firmware is loaded into the SXF1800 using the *OS Update* service, the SXF1800 verifies the new OS firmware integrity using the OU-FWV-Pub.

The DRBG Health tests along with the KAT described in the preceding section are conditional tests per [90A].

5 Physical Security Policy

The SXF1800 is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The SXF1800 uses standard passivation techniques and is protected by active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the SXF1800 permanently into the *Tampered* error state

The SXF1800 is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging.

6 Electromagnetic Interference and Compatibility (EMI/EMC)

The SXF1800 conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

7 Mitigation of Other Attacks Policy

The module is protected against SPA, DPA, Timing Analysis and Fault Induction using a combination of firmware and hardware countermeasures.

8 Security Rules and Guidance

The SXF1800 implementation also enforces the following security rules:

- No additional interface or service is implemented by the SXF1800 which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

As part of the deployment process the SXF1800 implementation must also be configured to perform the proper self-tests. Confirmation of this configuration can be found by the GET DATA APDU with Card Manager selected.

CLA	INS	P1	P2	Lc	Data	Le
0x80	0xCA	0x00	0xFE	0x04	0xDF4B 0x01 0x10	0x00

The response should be 0xFE07DF4B04XXYY where bits 1-3 of XX are set.