FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0.1

FX Cryptographic Kernel Module for A57

Software version: 1.1.0

Table of Contents

1. Module Overview

FX Cryptographic Kernel Module for A57 cryptographic module is a software module defined as a multi-chip standalone cryptographic module.

The primary purpose of the FX Cryptographic Kernel Module for A57 is to provide encryption/decryption of data for the multifunction devices.

The block diagram below shows the FX Cryptographic Kernel Module for A57, along with the cryptographic boundary.

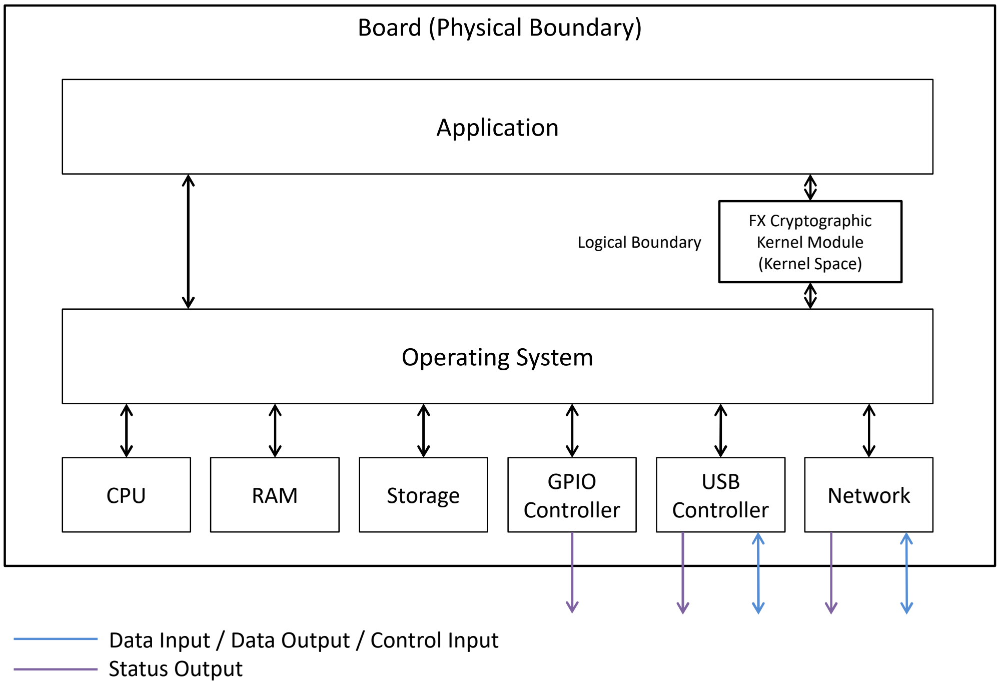
Board (Physical Boundary)
Application
Logical Boundary
FX Cryptographic Kernel Module (Kernel Space)
Operating System
CPU
RAM
Storage
GPIO Controller
USB Controller
Network
Data Input / Data Output / Control Input
Status Output

Figure 1 – Block Diagram of the module

This document is written about the following validated software version of FX Cryptographic Kernel Module for A57 (fips_dmcrypt.ko):

- Software version: 1.1.0

2. Security Level

The FX Cryptographic Kernel Module for A57 meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Modes of Operation

3.1. Approved Mode of Operation

The FX Cryptographic Kernel Module for A57 is designed to continually operate in a FIPS approved mode of operation. The FX Cryptographic Kernel Module for A57 supports the following FIPS approved cryptographic algorithms:

Table 2 – FIPS Approved Algorithms

Algorithm	Options	Standard	Cert. No.
AES	AES-128, 192, 256 Encryption/Decryption (ECB, CBC, and CTR) AES-128, 256 Encryption/Decryption (XTS)[1]	FIPS 197 SP800-38E	C833
Triple-DES	3-key Triple-DES Encryption/Decryption (ECB, CBC and CTR)	SP 800-67	C836
SHS	SHA-1, 224, 256, 384, 512	FIPS 180-4	C835
HMAC	HMAC-SHA1, 224, 256, 384, 512 (Key Size ≥ 112 bits)	FIPS 198	C975

3.2. Non-Approved Mode of Operation

The FX Cryptographic Kernel Module for A57 does not support a Non-Approved Mode of Operation.

[1] XTS-AES can only be used for storage applications.

4. Ports and Interfaces

The physical ports for FX Cryptographic Kernel Module for A57 are the same as the multifunction devices on which it is executing. The logical interface is a C-language application program interface (API), for which the following inputs/output types exist as parameters and return values:

- Control Input - Module API Control Parameters
- Data Input - Module API Data Parameters
- Data Output - Module API Data Return Values
- Status Output - Module API Status Return Values

As a software module, control of the physical ports is outside module scope. However, when the module is performing self-tests, or is in an error state, all output on the data output interface is inhibited. The module is single-threaded and in error scenarios returns only an error value (no data output is returned).

5. Identification and Authentication Policy

5.1. Assumption of Roles

The FX Cryptographic Kernel Module for A57 supports two distinct operator roles: User role and Crypto-Officer (C.O.) role. The C.O. and User roles are implicitly assumed by the entity accessing the services implemented by the module.

Only one role can be active at a time and the module does not allow concurrent operators. The module does not support a Maintenance role.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Not Required	Not Required
Crypto-Officer	Not Required	Not Required

6. Access Control Policy

6.1. Roles and Services

6.1.1. Crypto-Officer Role

The Crypto-Officer is any operator with the permissions to zeroize all CSPs within the module. All services available to the Crypto-Officer role are provided in Table 4.

Table 4 - Crypto-Officer Specific Services

Service	Description
Initialization	Performs on-demand power-up tests and initialization of the module.
Zeroization	Deletes all plaintext CSPs.

6.1.2. User Role

The User is any operator with the permissions to perform services provided in Table 5.

Table 5 - User Specific Services

Service	Description
AES	Encrypts / Decrypts data.
Triple-DES	Encrypts / Decrypts data.
SHS	Calculates hash digest value of data.
HMAC	Calculates HMAC value of data.
Show Status	Returns the status of the module.

6.2. Definition of Critical Security Parameters (CSPs)

The following CSPs are included in the FX Cryptographic Kernel Module for A57. Keys are not generated, or established, input, or output. Keys are accessed from calling applications' software within the General Purpose Computer (GPC) that the module is installed on, per IG 7.7. Zeroization is performed by the Zeroization service.

Table 6 – CSP

CSP	Description
AES Key	AES key for encryption and decryption of data
Triple-DES Key	3-Key Triple-DES Key for encryption and decryption of data
HMAC Key	HMAC key for calculation of HMAC digest.

6.3. Definition of Public Keys

The module does not use or contain any public keys.

6.4. Definition of CSP Access Modes

Table 7 defines the relationship between CSP access modes and module services. The access modes shown in Table 7 are defined as follows:

- **Use:** Uses the CSP to perform cryptographic operations within its corresponding algorithm (read, write, and execute access to the CSP).
- **Zeroize:** Deletes the CSP.

Table 7 - CSP Access Rights within Roles & Services

Role		Service Name	CSP (Access Mode)
C.O.	User		
	X	AES	Use: AES Key / Zeroize: AES Key
	X	Triple-DES	Use: Triple-DES Key / Zeroize: Triple-DES Key
	X	SHS	-
	X	HMAC	Use: HMAC Key / Zeroize: HMAC Key
X		Zeroization	Zeroize: AES Key, Triple-DES Key, HMAC Key
X		Initialization	-
	X	Show Status	-

The physical cryptographic boundary of the module is the board on which the module is installed. According to Section 7.7 of FIPS 140-2 Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, CSP passing within the boundary is not considered as entry or output.

7. Operational Environment

The tested operating systems segregate user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS 140-2 requirement for a single user mode of operation.

For FIPS 140-2 validation, the module is tested by an accredited FIPS 140-2 testing laboratory on the following operating environment:

- Wind River® Linux 9 with Quad ARM® A57 on NVIDIA Jetson TX1

Additionally, only when the module operates on the following platform, the module will remain compliant with FIPS 140-2 validation status because it is possible to operate without any source code change:

- Wind River® Linux 9 with ARM Cortex-A57

The CMVP makes no statement as to the correct operation of the module on the operational environments for which operational testing was not performed. A detailed discussion of how to maintain validation compliance can be found in chapter G5 of FIPS 140-2 Implementation Guidance.

8. Security Rules

The FX Cryptographic Kernel Module for A57 cryptographic module was designed with the following security rules in mind. These rules are comprised of both those specified by FIPS 140-2 and those derived from Fuji Xerox Co., Ltd.'s company policy.

1. The FX Cryptographic Kernel Module for A57 shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.

2. The FX Cryptographic Kernel Module for A57 shall perform the following tests:

   i. Power-up Self-Tests:

      a. Cryptographic algorithm tests (for each implementation):

         - AES 128 (ECB, CBC, CTR and XTS) Encryption and Decryption Known-Answer Tests

         - Triple-DES (ECB, CBC and CTR) 192 bit Encryption and Decryption Known-Answer Tests

         - SHA-1/224/256/384/512 Known-Answer Tests

         - HMAC-SHA1/224/256/384/512 Known-Answer Tests

      b. Software Integrity Test (HMAC-SHA1 Verification)

3. The operator shall be capable of commanding the FX Cryptographic Kernel Module for A57 to perform the power-up self-test on demand by performing the Initialization service or by re-loading the module with rmmod/insmod commands.

4. The operator shall not make the module operate 3-key Triple DES encryption for the total number of blocks which is greater than 2^{16} with same keys. As a software module, control of the physical ports is outside module scope and all data is output via an internal path within the physical boundary.

5. The operator shall only use the XTS-AES mode for the cryptographic protection of data on storage devices that use fixed length "data units," as defined in IEEE Std 1619-2007, and not for other purposes, such as data in transit.

6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the FX Cryptographic Kernel Module for A57.

7. The FX Cryptographic Kernel Module for A57 does not support concurrent operators.

8. The FX Cryptographic Kernel Module for A57 shall not support a bypass capability or a maintenance interface.

9. The module shall be installed per the following procedure:

   i. Check the startup log of OS to make sure that the following strings are included.

```
CPU: Quad ARM A57
Wind River Linux 9.0.0.16 tegra ttyS0
```

   ii. Check that there is not "fxfips" directory.

```
root@tegra:/sys# ls /sys/fxfips/
ls: /sys/fxfips/: No such file or directory
```

   iii. Install the module.

```
root@tegra:/mnt# insmod fips_dmcrypt.ko
```

   iv. Check version of the module.

```
root@tegra:/mnt# cd /sys/fxfips/
root@tegra:/sys/fxfips# ls
enable status version
root@tegra:/sys/fxfips# cat enable
1
root@tegra:/sys/fxfips# cat status
1
root@tegra:/sys/fxfips# cat version
1.1.0
```

9. Policy on Mitigation of Other Attacks

The FX Cryptographic Kernel Module for A57 was not designed to mitigate other attacks outside of the specific scope of FIPS 140-2. Therefore, this section is not applicable.

Table 8 - Mitigation of Other Attacks

Other Attack	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

10. Definitions and Acronyms

Table 9 - Definitions and Acronyms

Term	Definition
AES	Advanced Encryption Standard
Triple-DES	Triple Data Encryption Standard
CSP	Critical Security Parameter
SHS	Secure Hash Standard
HMAC	Hash-based Message Authentication Code

11. Revision History

Date	Version	Description
Aug. 26, 2019	1.0.0	Initial release.
May 21, 2020	1.0.1	Updated from CMVP review.