# FIPS 140-2 Non-Proprietary Security Policy

## Document Version 1.0.1

# FX Cryptographic Kernel Module

# Table of Contents

# 1. Module Overview

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

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

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

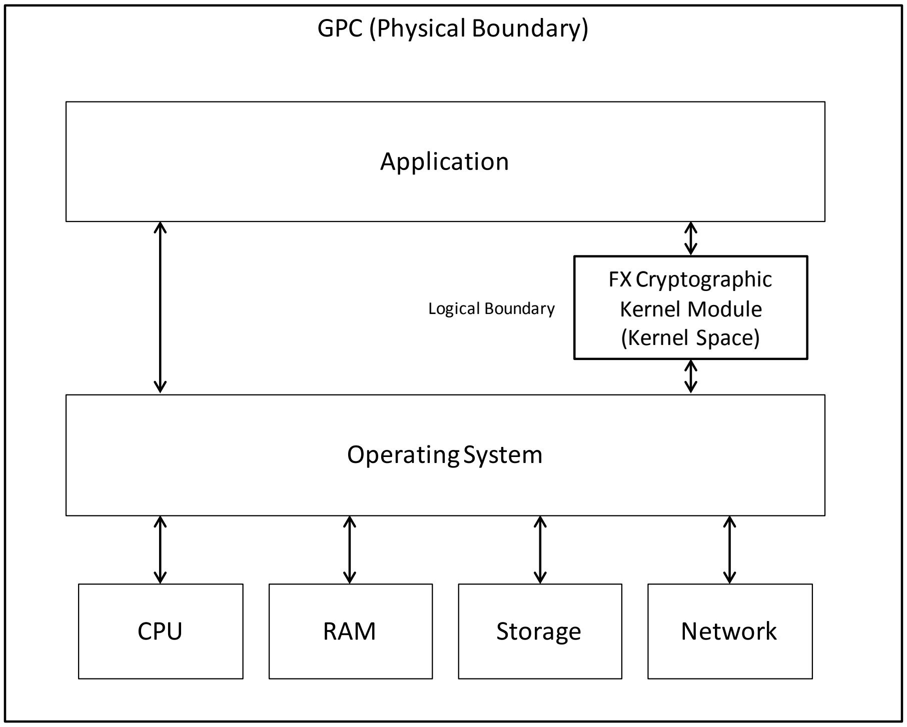

**Figure 1 – Block Diagram of the module**

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

- Software version: 1.0.3

## 2. Security Level

The FX Cryptographic Kernel Module 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 is designed to continually operate in a FIPS approved mode of operation, and implicitly transitions into the non-approved mode of operation based on the selection of a specific HMAC key size as defined in Section 3.2 below The module's mode is dependent upon the key sizes selected as defined in Section 3.2; the mode of operation can be changed while in the operational state, and is not limited solely to initialization. The FX Cryptographic Kernel Module 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) | FIPS 197 | #3952 |
| **Triple-DES** | 3-key Triple-DES Encryption/Decryption (ECB, CBC and CTR) | SP 800-67 | #2165 |
| **SHS** | SHA-1, 224, 256, 384, 512 | FIPS 180-4 | #3260 |
| **HMAC** | HMAC-SHA1, 224, 256, 384, 512 (Key Size ≥ 112 bits) | FIPS 198 | #2574 |
| **DRBG** | Hash DRBG (SHA-1, 256, 384, 512),<br>HMAC DRBG (SHA-1, 256, 384, 512),<br>Block Cipher DRBG (AES-128, 192, 256) | SP 800-90A | #1190 |

The FX Cryptographic Kernel Module is in the approved mode while using only those approved algorithms and key sizes specified in Table 2 above. Use of key sizes offering less than 112 bits of encryption strength transitions the module into the Non-Approved Mode of Operation as specified in Section 3.2 below.

## 3.2. Non-Approved Mode of Operation

The FX Cryptographic Kernel Module is considered in the Non-Approved Mode of Operation with the use of the following:

**Table 3 – FIPS Non-Approved Algorithms**

| Algorithm | Use |
|---|---|
| **HMAC** | Use of HMAC with a key of less than 112 bits of security strength. |

# 4. Ports and Interfaces

The physical ports for FX Cryptographic Kernel Module 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
- Data Input - Module API
- Data Output - Module API
- Status Output - Module API

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 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 4 - 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 CSP within the module. All services available to the Crypto-Officer role are provided in Table 5.

**Table 5 - Crypto-Officer Specific Services**

| Service | Description |
|---|---|
| **Initialization** | Performs on-demand power-up test 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 6.

**Table 6 - 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. |
| **DRBG** | Generates random bits. |
| **Show Status** | Returns the status of the module. |

* HMAC service is made available to both Approved and Non-Approved modes of Operation, and is dependent on key size used.

## 6.2. Definition of Critical Security Parameters (CSPs)

The following CSPs are included in the FX Cryptographic Kernel Module.

**Table 7 – 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. |
| **DRBG Secret Values** | The secret values necessary for the FIPS approved DRBG.<br>(Hash DRBG: V and C, HMAC DRBG: V and HMAC Key, Block Cipher DRBG: V and AES Key |

## 6.3. Definition of Public Keys

The module does not use or conation any public key.

## 6.4. Definition of CSP Access Modes

Table 8 defines the relationship between CSP access modes and module services. The access modes shown in Table 8 are defined as follows:

- **Generate:** Generates the Critical Security Parameter (CSP) using an approved DRBG.
- **Use:** Uses the CSP to perform cryptographic operations within its corresponding algorithm.
- **Entry:** The CSP is entered into the FX Cryptographic Kernel Module.
- **Output:** Outputs the CSP from the FX Cryptographic Kernel Module.
- **Zeroize:** Deletes the CSP.

**Table 8 - 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 | DRBG | Use: DRBG Secret Values / Zeroize: DRBG Secret Values |
| X | | Zeroization | Zeroize: AES Key, Triple-DES Key, HMAC Key, DRBG Secret Values |
| 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 6 with Broadcom ARMv6l BCM2835 on Raspberry Pi 1 Model B

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 6 with ARM Cortex-A15

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 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's company policy.

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

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

    i. Power-up Self-Tests:

        a. Cryptographic algorithm tests (for each implementation):

            - AES 128/192/256 CBC Encryption and Decryption Known-Answer Tests

            - Triple-DES (ECB, CBC and CTR) 168 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

            - DRBG (Hash/HMAC/Block Cipher) Known-Answer Tests

        b. Software Integrity Test (HMAC-SHA1 Verification)

        c. DRBG Health Checks

    ii. Conditional Self-Tests:

        a. Continuous RNG Tests (DRBG)

3. The operator shall be capable of commanding the FX Cryptographic Kernel Module 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. As a software module, control of the physical ports is outside module scope and all data is output via internal path within physical boundary.

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

6. The FX Cryptographic Kernel Module does not support concurrent operators.

7. The FX Cryptographic Kernel Module shall not support a bypass capability or a maintenance interface.

8. The operator (the calling applications) shall use entropy sources that meet the security strength required for the random number generation mechanism: 128 bits for the DRBG mechanisms. This entropy is supplied by means of callback functions.

# 9. Policy on Mitigation of Other Attacks

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

**Table 9 - Mitigation of Other Attacks**

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

# 10. Definitions and Acronyms

**Table 10 - 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 |
| **DRBG** | Deterministic Random Bit Generator |

## 11. Revision History

| Date | Version | Description |
|---|---|---|
| Jul. 28, 2016 | 1.0.0 | Initial release. |
| Oct. 06, 2016 | 1.0.1 | Updated based on CMVP comments |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |