FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0.0

FUJIFILM BI
Cryptographic Kernel Module for WRL

Software version: 1.2.L9A57 / 1.1.L6A15

Table of Contents

List of Tables

1. General

1.1. Overview

The FUJIFILM BI Cryptographic Kernel Module for WRL (Wind River Linux) meets the overall requirements applicable to FIPS 140-3 Security Level 1 software cryptographic module (module). The primary purpose of the Module is to provide encryption/decryption of data.

1.2. Security Levels

The module meets the security level 1 requirements for the applicable sections documented within ISO/IEC 19790 Section 7 as shown in Table 1.

Table 1 - Security Levels

ISO/IEC 24759 Section 6.	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software / Firmware Security	1
6	Operational Environment	1
7	Physical Security	N/A
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	1
10	Self-tests	1
11	Life-cycle Assurance	1
12	Mitigation of Other Attacks	N/A
	Overall Level:	**1**

2. Cryptographic Module Specification

2.1. Description

The FUJIFILM BI Cryptographic Kernel Module for WRL is an object file used to extend the kernel of the WRL.

Purpose: The primary purpose of the FUJIFILM BI Cryptographic Kernel Module for WRL is to provide encryption/decryption of data for multifunction devices.

Module Type: The module is defined as a software module (*refer to ISO/IEC 19790, Section 7.2.2*).

Embodiment: The module and operating environment (OE) are defined as a multi-chip standalone module.

Module Characteristics: The module comprises a single, kernel object file built for WRL6 and WRL9 respectively. No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs.

Cryptographic Boundary: The cryptographic boundary is defined as the FUJIFILM BI Cryptographic Kernel Module for WRL. The boundary encompasses the entire monolithic object file:

- wrl6_fips_1403_module.ko on Wind River Linux 6
- wrl9_fips_1403_module.ko on Wind River Linux 9

2.1.1. TOEPP & Cryptographic Boundary

The block diagram in Figure 1 depicts the module's cryptographic boundary and Tested Operational Environment's Physical Perimeter (TOEPP) and dataflows.

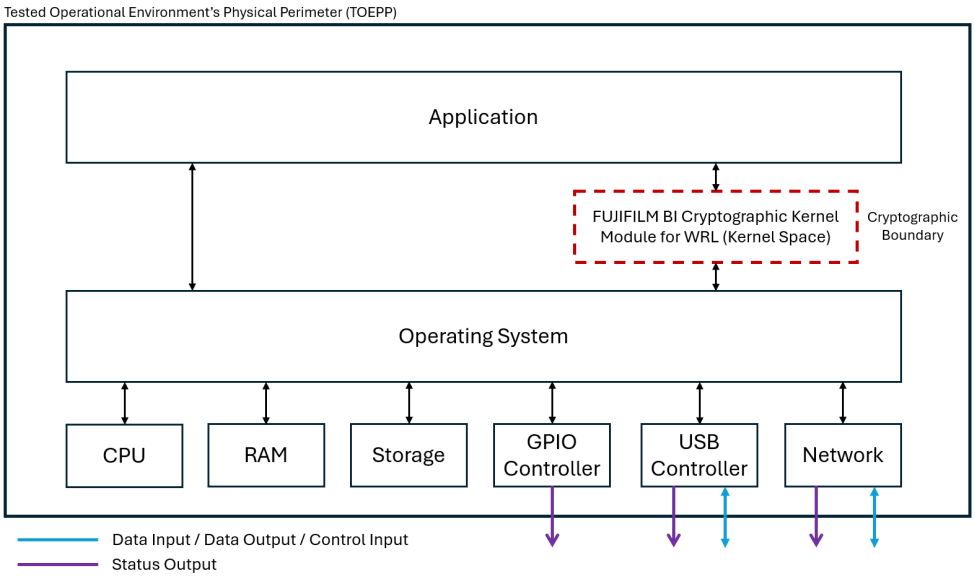

Figure 1 - Cryptographic Boundary

2.2. Tested & Vendor Affirmed Module Version and Identification

The FUJIFILM BI Cryptographic Kernel Module for WRL is a software cryptographic module developed to meet the requirements of FIPS 140-3 Security Level 1 (*refer to Table 1*). The module is built according to its underlying OE (i.e., Wind River Linux 6 or Wind River Linux 9).

Table 2 – Tested Module Identification

#	Module	Software Version	Operating Environment (OE)
1	Wrl9_fips_1403_module.ko	1.2.L9A57	Wind River Linux 9 on ARM Cortex A57
2	wrl6_fips_1403_module.ko	1.1.L6A15	Wind River Linux 6 on ARM Cortex A15

2.2.1. Tested Operational Environments

The module has been tested on the operating environments shown below in Table 3.

Table 3 - Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Wind River Linux 9	FFBI Palacios2 K502	ARM Cortex A57	N/A
2	Wind River Linux 6	FFBI Clipper8	ARM Cortex A15	N/A

N.B. There are no vendor affirmed operating environments.

2.3. Excluded Components

The module does not exclude any components from the requirements of FIPS 140-3.

2.4. Modes of Operation

The module is designed to continually operate in an approved mode of operation. There are no undefined or 'non-approved' modes or services within the module. By default, the approved mode is entered into when successfully powering on the module. If the module does not successfully initialize it transitions to its error state.

N.B. The module does not incorporate a degraded mode of operation (*refer to ISO/IEC 19790 Section 7.2.4.3).*

2.5. Algorithms

2.5.1. Approved Algorithms

The FUJIFILM BI Cryptographic Kernel Module for WRL supports the approved cryptographic algorithms shown in Table 4.

Table 4 - Approved Algorithms

CAVP Cert.	Algorithm & Standard	Mode/Method	Description/Key Size(s)/Key Strength	Use / Function
A3219 & A3220	AES [FIPS 197] [SP 800-38A]	ECB, CBC	Key Length: 128, 192, 256 Key Strength: 128 bits, 192 bits or 256 bits	Symmetric Encryption and Decryption
		CTR	Key Length: 128, 192, 256 Key Strength: 128 bits, 192 bits or 256 bits	
A3219	AES [FIPS 197] [SP 800-38E]	XTS[1]	Key length: 128, 256 (1.2.L9A57 Only) Key Strength >= 128 bits or 256 bits	Symmetric Encryption and Decryption
A3219 & A3220	SHS [FIPS 180-4]	SHA-1	Message length: 0 - 65536 (Increment 8)	Message Digest
		SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
A3219 & A3220	HMAC [FIPS 198-1]	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Key Length: 112-2048 Increment 8 Key Strength >= 112 bits to <=512 bits	Keyed Hash Message Authentication Codes and Pre-operational Test

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

2.5.2. Vendor Affirmed Algorithms

The module does not implement any Vendor Affirmed algorithms.

Table 5 – Vendor Affirmed Algorithms

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

2.5.3. Non-Approved Algorithms

The module does not implement any non-approved algorithms.

Table 6 – Non-Approved, Allowed Algorithms

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

2.5.4. Non-Approved, Allowed Algorithms with No Security Claimed

The module does not implement any non-approved algorithms.

Table 7 – Non-Approved, Allowed Algorithms

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

2.5.5. Non-Approved, Allowed Algorithms with No Security Claimed

The module does not implement any non-approved algorithms.

Table 8 – Non-Approved, Not Allowed Algorithms

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

2.6. Security Function Implementation (SFI)

Table 9 – Security Function Implementation

Name	Type	Description	SF Properties	Algorithms / CAVP Cert.
N/A	N/A	N/A	N/A	N/A

2.7. Algorithm Specific Information

The module utilizes only approved algorithms that are tested and validated under the Cryptographic Module Validation Program (CMVP):

- AES per FIPS 197, NIST SP 800-38A and SP 800-38E

- HMAC per FIPS 198-1
- SHS per FIPS 180-4

2.8. RBG [Random Bit Generator] and Entropy

The module does not support a random bit generator (RBG) or an entropy source for the generation of cryptographic keys.

2.9. Key Generation

The module does not support the generation of cryptographic keys or key material.

2.10. Key Establishment

The module does not support key establishment techniques.

2.11. Industry Protocols

The module is not reliant on any specific industry protocols.

3. Cryptographic Module Interfaces

3.1. Ports and Interfaces

The physical ports for the module are the same as the multifunction devices on which it is executing. The logical interface is a C-language application program interface (API) through which applications request services. Table 10 summarizes the logical interfaces that the module supports.

Table 10 - Ports and Interfaces

Physical Port	Logical interface	Data that Passes over the Port/Interface
N/A	Control Input	Algorithm modes, service opcodes
N/A	Data Input	Plaintext or ciphertext data, cryptographic keys
N/A	Data Output	Plaintext, Ciphertext, Hash Digests, HMAC Values
N/A	Status Output	Module status

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).

4. Roles, Services, and Authentication

4.1. Authentication Methods

The module does not implement any authentication methods.

4.2. Roles

The module supports two distinct operator roles: Crypto-Officer (CO) role and User role. The CO 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 11 - Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Initialization	N/A	Return code
CO/User	Zeroization	N/A	N/A
User	AES	Plaintext, Ciphertext, AES key, IV, Counter, Key Length	Plaintext, Ciphertext, Return code
User	SHS	Plaintext	Hash value, Return code
User	HMAC	Plaintext, HMAC key, Key Length	HMAC value, Return code
User	Show Status	N/A	Status
User	Show Module Info	N/A	Module name, Module version

Table 12 - Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	N/A	N/A
User	N/A	N/A

4.3. Approved Services

Table 13 defines the relationship between SSP access modes and module services. The access modes shown in Table 13 are defined as follows:

- **G:** Generate: The module generates or derives the SSP.
- **R:** Read: The SSP is read from the module.
- **W:** Write: The SSP is updated, imported, or written to the module.
- **E:** Execute: The module uses the SSP in performing a cryptographic operation.
- **Z:** Zeroise: The module zeroises the SSP.

Table 13 – Approved Service

Service	Description	Approved Security Function	Keys & SSPs	Role	Access Rights to Keys and / or SSPs	Indicator
AES	Encrypts / Decrypts data.	AES	AES Key, IV, Counter	User	R, E, Z	0 = Success >0 = Failure
HMAC	Calculates HMAC value of data.	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256 HMAC-SHA-384, HMAC-SHA-512	HMAC Key	User	R, E, Z	0 = Success >0 = Failure
Initialization	Performs on-demand pre-operational tests and initialization of the module.	N/A	N/A	CO	N/A	0 = Success >0 = Failure
SHS	Calculates hash digest value of data.	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	N/A	User	N/A	0 = Success >0 = Failure
Show Module Info	Returns the module name and version.	N/A	N/A	User	N/A	0 = Success >0 = Failure
Show Status	Returns the status of the module.	N/A	N/A	User	N/A	0 = Success >0 = Failure
Zeroization	Deletes all plaintext CSPs.	N/A	AES Key, HMAC Key	CO/User	Z	0 = Success >0 = Failure

The zeroization service is performed under the following conditions:

- Automatic zeroization is performed when deallocating structure or when the system is powered off.
- Keys are zeroized when destroying the appropriate context object.

4.4. Non-Approved Services

The module does not implement any Non-Approved Services.

Table 14 – Non-Approved Services

Name	Description	Algorithms Accessed	Role	Indicator
N/A	N/A	N/A	N/A	N/A

4.5. External Software Loading

The module does not support the loading of software from external sources.

4.6. Additional Information

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

5. Software Security

5.1. Integrity Techniques

The module performs the HMAC-SHA-1 (128-bit key) software integrity test on power-up automatically.

5.2. Initiate on Demand

The operator can perform the test on demand by performing the Initialization service or by re-loading the module with rmmod/insmod commands. Please refer to Section 10 for integrity test details.

6. Operational Environment

6.1. Operational Environment Type & Requirements

The module's operational environments (OEs) include

- Wind River Linux 6 running on an ARM Cortex A15 tested on FFBI Clipper8 hardware platform and
- Wind River Linux 9 running on ARM Cortex A57 tested on FFBI Palacios2 K502 hardware platform.

These OEs are defined as modifiable operational environments.

There is no restriction to the configuration of it. 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.

7. Physical Security

Physical Security requirements are not applicable, as the module is a FIPS 140-3 Security Level 1 software module.

8. Non-invasive Security

The module was not designed to mitigate non-invasive attacks. Therefore, this section is not applicable.

9. Sensitive Security Parameters (SSPs) Management

9.1. Storage Areas

All SSPs are stored ephemerally in random access memory (RAM).

9.2. SSP Input-Output Methods

The module is passed cryptographic keys in plaintext by the calling application. The module does not output any SSPs.

9.3. SSP Zeroization Methods

SSPs are not persistently stored. During normal operation, the module explicitly erases copies of SSPs in volatile memory (e.g., RAM) by overwriting with zeros after their use.

9.4. SSPs

The following SSPs are included in the FUJIFILM BI Cryptographic Kernel Module for WRL. Keys are not generated, or established, output. Keys are accessed from calling applications' software within the General-Purpose Computer (GPC) that the module is installed on. Zeroization is performed by the Zeroization service.

Table 15 – SSPs

Key/CSP Name	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related SSPs
AES Key	128-bit 192-bit 256-bit	AES CBC/ECB/CTR/XTS Certs. #A3219 & #A3220	N/A	Import: Plaintext Export: N/A The module uses this CSP passed in by the calling application on the stack.	N/A	Plaintext, Dynamic (Ephemeral)	Zeroized immediately after use	Data encryption and decryption
HMAC Key	>=112 bits	HMAC Certs. #A3219 & #A3220	N/A	Import: Plaintext Export: N/A The module uses this CSP passed in by the calling application on the stack.	N/A	Plaintext, Dynamic (Ephemeral)	Zeroized immediately after use	HMAC functions
SW Integrity Key	128 bits	HMAC-SHA-1 Certs. #A3219 & #A3220	N/A	Import: N/A Export: N/A	N/A	Static	Copied to RAM and Zeroized immediately after use	Software integrity test

10. Self-Tests

The module performs the self-tests described in Tables 16 & 17 on power-up. All KATs must be completed successfully prior to any use of cryptography by the module. If one of the KATs fails, the module transitions to its error state.

10.1. Pre-Operational Self-Tests

The module implements both pre-operational and conditional self-tests. Since the pre-operational self-test for this module comprises the software integrity test utilizing the HMAC-SHA-1 algorithm, the SHA-1 and HMAC-SHA1 KATs for the conditional self-tests are invoked prior to the software integrity test.

Table 16 - Pre-Operational Self-Tests

Algorithm	Implementation	Test Properties	Test Method	Type	Indicator	Details
HMAC-SHA-1	Software (Integrity Test)	256-bit	KAT	Software Integrity	FIPS_STATUS_EINTEGRITY	Verifies the HMAC-SHA-1 message authentication code for the software binary.

10.2. Conditional Self-Tests

The FUJIFILM BI Cryptographic Kernel Module for WRL shall perform the following tests:

Table 17 –Self-Test

Algorithm	Implementation	Test Properties	Test Method	Type	Indicator	Details
AES-ECB Encrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_ECB	Encrypt KAT
AES-ECB Decrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_ECB	Decrypt KAT
AES-CBC Encrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_CBC	Encrypt KAT
AES-CBC Decrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_CBC	Decrypt KAT
AES-CTR Encrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_CTR	Encrypt KAT
AES-CTR Decrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_CTR	Decrypt KAT
AES-XTS Encrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_XTS	Encrypt KAT
AES-XTS Decrypt	Software	128-bit	KAT	CAST	FIPS_ALGO_XTS	Decrypt KAT
HMAC-SHA-1	Software	256-bit	KAT	CAST	FIPS_ALGO_HMAC	HMAC Generate KAT
HMAC-SHA-224	Software	256-bit	KAT	CAST	FIPS_ALGO_HMAC	HMAC Generate KAT

Algorithm	Implementation	Test Properties	Test Method	Type	Indicator	Details
HMAC-SHA-256	Software	256-bit	KAT	CAST	FIPS_ALGO_HMAC	HMAC Generate KAT
HMAC-SHA-384	Software	256-bit	KAT	CAST	FIPS_ALGO_HMAC	HMAC Generate KAT
HMAC-SHA-512	Software	256-bit	KAT	CAST	FIPS_ALGO_HMAC	HMAC Generate KAT
SHA-1	Software	SHA-1	KAT	CAST	FIPS_ALGO_SHA1	SHA calculation KAT
SHA-224	Software	SHA-224	KAT	CAST	FIPS_ALGO_SHA224	SHA calculation KAT
SHA-256	Software	SHA-256	KAT	CAST	FIPS_ALGO_SHA256	SHA calculation KAT
SHA-384	Software	SHA-384	KAT	CAST	FIPS_ALGO_SHA384	SHA calculation KAT
SHA-512	Software	SHA-512	KAT	CAST	FIPS_ALGO_SHA512	SHA calculation KAT

10.3. Periodic Self-Tests

The FUJIFILM BI Cryptographic Kernel Module for WRL performs all self-tests on power-up automatically. The module can be reloaded to perform all the self-tests on demand.

10.4. Error States

The module includes a defined error state in which it enters upon the failure of self-tests.

Table 18 - Error States

State Name	Description	Conditions	Recovery Method	Indicator
Error State	Module's error state	Failure of pre-operational or conditional self-tests	The module aborts service and outputs error indicator. The module must be restarted.	A non-zero value is set into the following parameters and output: FIPS_STATUS_EINTEGRITY FIPS_STATUS_EKAT

10.5. Operator Initiation of Self-Tests

The module allows the operator initiation of self-tests. The module can be reloaded to perform all the self-tests on demand.

11. Life-cycle Assurance

11.1. Installation, Initialization & Startup Procedures

This section will describe the configuration management used for the FUJIFILM BI Cryptographic

Kernel Module for WRL.

The FUJIFILM BI Cryptographic Kernel Module for WRL is built and installed into the mobile device together with Wind River® Linux operating system by employees of FUJIFILM Business Innovation or subcontractors in a factory. Therefore, the module is delivered to User together with the mobile device and is not done in stand-alone form.

11.2. Administrator Guidance

The CO's responsibility for the secure operation of the module is the correct installation of the module into the device.

The module shall be installed through the following procedure:

i. Reboot target device.
ii. Install the module using the 'insmod' command.
iii. Check the module information is correct and matches the Security Policy.

When stopping employing the module, the CO should detach the module. Each buffer where SSPs are stored is zeroized immediately after processing, so CO does not have to perform the zeroization again.

11.3. Non-Administrator Guidance

A User is an entity that utilizes the module's cryptographic services. All the module operations must be performed via the module's API. The User must pass into the module the necessary SSPs for each security function.

The User's responsibility for the secure operation of the module is to ensure that the module name and version match those indicated in the Security Policy before using the module.

11.4. Design and Rules

The following security design and the rules of operation are applicable to the module:

- The module shall be installed only on either Wind River Linux 6 with ARM Cortex A15 or Wind River Linux 9 on ARM Cortex A57.
- The operator shall verify the correct version of software is installed by using the 'Show Module Info' service.
- The module shall operate only in an approved mode of operation.
- The module shall incorporate only approved algorithms validated under the cryptographic module validation program (CAVP).
- The module shall not support concurrent operators.
- The module shall not support a bypass mode or bypass capability.
- The module shall not support a maintenance mode of operation.

- The module shall not output cryptographic keys or key material.
- The module shall not support the generation of cryptographic keys or key material.
- The module shall not exclude any components from the requirement of FIPS 140-3 Security Level 1.
- The module shall only use AES-XTS for data at rest (i.e. for storage applications).
- The module shall not support a self-initiated cryptographic output capability.
- No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs.

12. Mitigation of Other Attacks

The FUJIFILM BI Cryptographic Kernel Module for WRL was not designed to mitigate other attacks outside of the specific scope of FIPS 140-3. Therefore, this section is not applicable.

Table 19 – Mitigation of Other Attacks

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

13. Definitions and Acronyms

Table 20 – Definitions and Acronyms

Term	Definition
AES	Advanced Encryption Standard
CO	Cryptographic Officer
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
ECB	Electronic Code Book
FFBI	FujiFilm Business Innovation
FIPS	Federal Information Processing Standards
FSM	Finite State Machine
GPC	General Purpose Computer
GPIO	General Purpose Input Output
HMAC	Hash-based Message Authentication Code
NIST	National Institute of Standards and Technology
OE	Operating Environment
OS	Operating System
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
TOEPP	Tested Operating Environment's Physical Perimeter
WRL	Wind River Linux
XTS	XEX Tweakable Block Ciphertext Stealing

14. Revision History

Date	Version	Description
Nov. 19, 2023	1.0.0	Initial release.