Document Version：1.0.3
Product Version：2.0.0

Security Policy

for

MonoCrypt AES

Enhanced Crypto Library

Focus Systems Corporation.

FIPS 140-2 Non-Proprietary

Revision History

Date	Revision	Author	Description
2020/1/22	1.0.0	Kimitoshi Hiramori	First release.
2021/2/12	1.0.1	Kimitoshi Hiramori	Applied the requirements from ECSEC Laboratory
2021/2/25	1.0.2	Kimitoshi Hiramori	Fixed product name and applied the requirements from ECSEC Laboratory
2021/3/1	1.0.3	Kimitoshi Hiramori	Applied the requirements from ECSEC Laboratory

Tabele of Contents

1. Module Overview

1.1. Cryptographic module description

MonoCrypt AES Enhanced Crypto Library (MonoCrypt AES) is Software module and is defined as a multi-chip standalone module.

It runs on general purpose computing system.

This module complies with FIPS140-2 requirement level 1 and is defined as Ver2.0.0.

The requirements of FIPS140-2 and the security levels for module are as follows.

Security Requirements Section	Level
Cryptographic Module Specification	1
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

1.2. Cryptographic Boundary

The physical cryptographic boundary of the module is defined as the outer enclosure of a general purpose computing system.

The logical cryptographic boundary of the module consists of the library files.(MonoCrypt.dll or libMonoCrypt.so)

1.3. Platforms

1.3.1.Tested Operational Environments

The test of FIPS140-2 was performed in the operational environment specified below.

The Crypto Officer must provide a single operator mode as the operating environment.

The operating system is restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

The “MonoCrypt.dll” is a module for Windows. The “libMonoCrypt.so” is a module for Unix platform (ex. Linux, Solaris, AIX, HP-UX.)

These Cryptograhic modules are separated for 32bit and 64bit

A. 32bit Module

No.	OS	Processor	Platform
1	Windows 10 Pro (x86) on Hyper-V on Windows Server 2016	Intel Xeon E5-2620 v4	Dell PowerEdge R430
2	Windows Server 2016 on Hyper-V on Windows Server 2016	Intel Xeon E5-2620 v4	Dell PowerEdge R430
3	Red Hat Enterprise Linux 7.7 on Oracle VM VirtualBox on Windows Server 2016	Intel Xeon E5-2620 v4	Dell PowerEdge R430
3	Solaris 11	SPARC64 X+	Fujitsu SPARC M10-1
4	Solaris 11 on Oracle VM VirtualBox on Windows Server 2008	Intel Xeon X5660	Fujitsu Primergy RX300 S6
6	AIX 7.2	POWER8	IBM Power System S814

B. 64bit Module

No.	OS	Processor	Platform
1	Windows 10 Pro (x64) on Hyper-V on Windows Server 2016	Intel Xeon E5-2620 v4	Dell PowerEdge R430
2	Windows Server 2016 on Hyper-V on	Intel Xeon E5-	Dell PowerEdge R430

	Windows Server 2016	2620 v4	
3	Red Hat Enterprise Linux 7.7 on Oracle VM VirtualBox on Windows Server 2016	Intel Xeon E5-2620 v4	Dell PowerEdge R430
4	Solaris 11	SPARC64 X+	Fujitsu SPARC M10-1
5	Solaris 11 on Oracle VM VirtualBox on Windows Server 2008	Intel Xeon X5660	Fujitsu Primergy RX300 S6
6	AIX 7.2	POWER8	IBM Power System S814
7	HP-UX 11iv3	Itanium2	HPE Integrity rx2800 i2

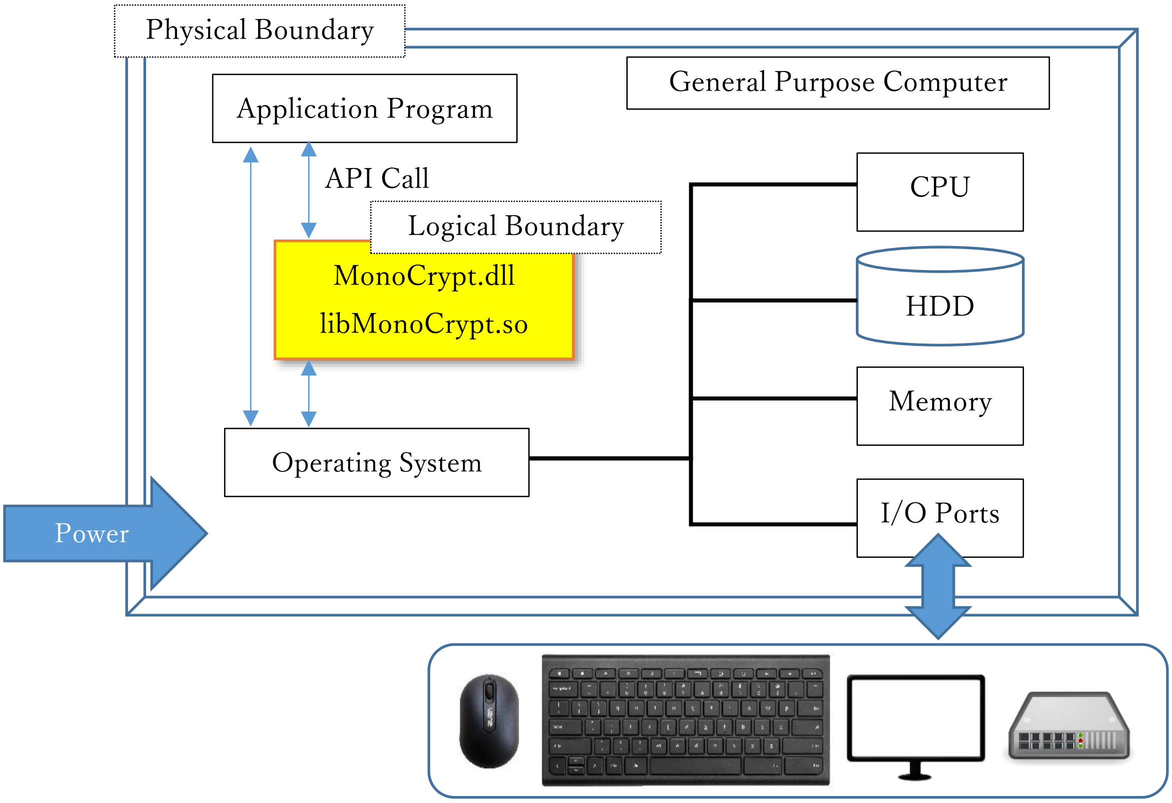
1.3.2. Supported Operational Environments

The module may be ported per IG G.5 to operating environments not listed in the tables in 1.3 (1) and retain compliance to FIPS 140-2; however, the CMVP makes no statement as to the correct operation of the module when so ported if the specific environment is not listed on the validation certificate. The module is also supported on the following untested platforms:

OS	Version
Windows	Windows 7/10 Windows Server 2016
Linux	Red Hat Enterprise Linux Server 7.1~7.8 CentOS 7.1~7.8
Solaris	Solaris 10/11
HP-UX	11iv3
AIX	AIX 7.1/7.2

1.4. Block Diagram

The following Block Diagram shows cryptographic boundary, Logical and Physical I/O Ports.



I/O port definitions

Input physical port：Keyboard・Mouse・Network

Output physical port：Monitor・Network

1.5. FIPS Approved mode of operation

This cryptographic module implements the following algorithms as approved security functions.

When the module is loaded and passes the power-up self-test, the module operates in the FIPS approved mode of operation. Thereafter, when the non-approved service shown in Section 1.6 is called, the module implicitly transitions to the non-approved mode of operation. In addition, when the non-approved service is finished, the module transitions to the FIPS approved mode of operation again.

The key Wrap algorithm operates in FIPS Approved mode as long as the integrity check value is a value fixed in SP 800-38F. In this module, when the value of [integrity] parameter is NULL, the fixed value is used.

algorithm	Description	Certificate

AES	As defined in FIPS PUB 197 and SP800-38A with 128, 192, or 256 bit keys.
	AES will support the following modes; ECB, CBC, CTR
		C1465(32bit)
		C1466(64bit)

Key Wrap	As defined in SP800-38F with AES 128, 192, or 256 bit keys.
	AES Key Wrap will support the following modes; KWP, KW
		C1465(32bit)
		C1466(64bit)

HMAC	As defined in FIPS PUB 198-1 for performing the power-up software integrity test, and generating MAC values.
	HMAC will support the following hash algorithm:SHA-256
	HMAC is implemented for an integrity test. The HMAC service cannot be used individually.
		C1465(32bit)
		C1466(64bit)

SHS	As defined in FIPS PUB 180-4 for generating message digests with 256bit lengths.(SHA-256)
	SHS is implemented for an integrity test. The SHS service cannot be used individually.
		C1465(32bit)
		C1466(64bit)

1.6. Non-Approved mode of operation

In the RFC3394/5649 AES Key Wrap function, if the integrity check value is not the fixed value in SP 800-38F, the cryptographic module is regarded as operating in a non-approved mode of operation

Algorithm	Description
RFC3394/5649 AES Key Wrap	As defined in RFC3394 and RFC5649 with AES 128, 192, or 256 bit keys. The integrity check value is not the value fixed in SP 800-38F

2. Ports and Interfaces

This cryptographic module provides only logical interfaces via API. It does not provide any direct interface to the physical Ports

Interface	Logical interfaces	Physical Ports
Data input	Data path for input data to be processed in the cryptographic module	N/A
Data output	Data path for output data	

	processed in the cryptographic module	N/A
Control input	API function calls and API input parameters for control to specify various services used in the cryptographic module	N/A
Status output	Data path that outputs the status of the cryptographic module	N/A

3. Roles, Services and Authentication

3.1. Role

The cryptographic module supports two distinct operator roles (User and Crypto Officer). The cryptographic module does not support operator authentication.

Role	Description
User	The entity that has access to all crypto related functions supported by the cryptographic module. The operator implicitly is assigned this role by making function calls for the service of this module.
Crypto Officer	The Crypto Officer is assigned a role for module installation and Operational environment. The following is an excerpt of the instructions for the Crypto Officer from the installation guide. ⅰ. Copy the module to your computer and set execute permissions. ⅱ. Set the operational environment to single-user mode

3.2. Service

3.2.1. Service used in the FIPS approved mode

Role	Service
User： Executing API functions that provide services provided by the cryptographic module.	AES Key Wrap Self-Test Show Status

Crypto Officer： Responsible for installing this cryptographic module to the specified hardware and OS environment.	N/A

3.2.2. Service used in the non-approved mode

Role	Service
User： Executing API functions that provide services provided by the cryptographic module.	RFC3394/5649 AES Key Wrap （non-compliant）
Crypto Officer： Responsible for installing this cryptographic module to the specified hardware and OS environment.	N/A

3.2.3. Service Purpose and Use

Service	Purpose and Use
AES	Allows a User to encrypt/decrypt various data.
Key Wrap	Allows a User to wrap/unwrap keys in an approved mode of operation
RFC3394/5649 AES Key Wrap (non-compliant)	Allows a User to wrap/unwrap keys in a non-approved mode of operation
Self-Test	Allows a User to determine if the module is functioning properly
Show Status	Allows a User role to indicate the module status

[Notice]

No independent zeroization service is implemented. Please refer to 6.2 for zeroization of CSPs.

3.3. Operator Authentication

Since operator authentication function is not required for FIPS 140-2 Security Level 1, it is not implemented

4. Physical Security

The FIPS 140 - 2 Section 5 Physical Security requirements do not apply because the module is a software module. However, when installing the module, the Crypto Officer must ensure that the computer system is stored in a secure environment.

Installing the module is conducted with the Crypto Officer role. Specifically, the Crypto Officer copies the module files and sets appropriate privileges to access the files.

5. Software environment

As a level 1 cryptographic module, a single user mode is required for the operating system.

In the target operating system, User applications with the cryptographic module run under operating system controlled processes and memory protection.

Applications are managed on a per-process basis.

Since this module does not use inter-process communication, it operates independently for each process, and other processes cannot access the CSPs in the module.

Also, interrupts by other processes are not allowed.

6. CSP Management

6.1. CSP definition

The CSPs included in this cryptographic module is as follows.

CSP	Description
AES Key	AES Key is used for encryption and decryption of various data in ECB, CBC, or CTR mode. Its key sizes are 128, 192 and 256 bits. AES Key is generated outside the module, is input to the module, is not output outside the module, is not stored on the non-volatile memory by the module, and is zeroized when the AES service completes.
Key Wrap Key	Key Wrap Key is used for AES encryption and decryption of a cryptographic key in KW or KWP mode. Its key sizes are 128,192, and 256 bits. Key Wrap Key is generated outside the module, is input to the module, is not output outside the module, is not stored on the non-volatile memory by the module, and is zeroized when the Key Wrap service completes.

[Notice]

HMAC Key is only used for software integrity test and is not considered a CSP according to IG 7.4

6.2. CSP zeroization

In this module, the CSPs are zeroized at the end of the cryptographic services that use the CSPs. The services are AES and Key Wrap in the approved mode of operation and RFC3394/5649 AES Key Wrap in the non-approved mode of operation. Therefore, no independent zeroization service is not implemented.

6.3. CSP access control policy

The module allows controlled access to the CSPs contained within it. The following table defines the access privilege to each CSP when performing a specified service for a given role. The permissions are categorized as follows. If no permission is listed, then the operator has no access to the CSP.

Write (w): a cryptographic key is entered into the module

Execute (e): a cryptographic key is read and used to perform cryptographic operations within its corresponding algorithm.

Zeroize (z): a cryptographic key is zeroized by the module.

Role		Service	**Cryptographic Keys and CSPs Access Operation**	
C.O	User		AES Key	Key Wrap Key
	○	AES	w.e.z	
	○	Key Wrap		w.e.z
	○	Self-Tests		
	○	Show Status		

7. Self-Test

7.1. Power-up Self-Test

The cryptographic module has a power-up Self-Test function to confirm the integrity and correct operation of the approved security functions.

The power-up Self-Test starts automatically when the cryptographic module is loaded into the application process.

In the power-up Self-Test, two tests, a cryptographic algorithm test and an integrity test, are executed. If the test result is failure, an error is returned and all cryptographic functions are disabled.

The cryptographic module provides an API to optionally perform a power-up Self-Test.

When recovering from the error state, it is necessary to reload the cryptographic module into the application again.

7.2. Algorithm test

KATs are performed in the cryptographic algorithm test.

In the KATs, the value calculated by each algorithm is compared with the value stored in the cryptographic module.

If the values do not match, an error is returned and the module becomes disabled.

The KATs check the following algorithms.

Test Target	Description
AES	KATs: Encryption/Decryption Mode: ECB/CTR/CBC Key size:128/192/256bit
Key Wrap	KATs: Encryption/Decryption Mode: KW/KWP Key size: 128/192/256bit
HMAC	KATs: Hash data verification Hash size:SHA-256
SHS	KATs: Hash data verification Hash size:SHA-256

7.3. Integrity test

In the integrity test, tampering of the module is detected.

In the integrity test, a hash value calculated via HMAC-SHA-256 when the cryptographic module is loaded, is compared with a value stored in the cryptographic module.

If the values do not match, an error is returned and the module becomes disabled.

8. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of the FIPS 140-2 Security Level 1 module.

(1)The cryptographic module shall provide two distinct operator roles. These are the User role, and the Crypto Officer role.

(2) The cryptographic module shall not perform an operator authentication.

(3) The cryptographic module shall perform the following tests without any operator intervention:

A. Power up Self-Tests:

Software Integrity Test (HMAC-SHA-256 verification)

Cryptographic algorithm tests:

a. AES Known Answer Test

b. Key Wrap Known Answer Test

c. HMAC Known Answer Test

d. SHS Known Answer Test

(4)If the module enters an error state due to failing of self-tests, the module shall be reloaded in order to perform its service.

(5) Data output shall be inhibited during self-tests, zeroization, and error states.

(6) Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

(7) The module shall not support concurrent operators as a Security Level 1 module.

(8) The module shall be operated with an operating system configured in a single user mode.

(9) The module shall inhibit cryptographic operations and data output while in all error states.

9. Guidance

9.1. Crypto Officer Guidance

There is no administrative function or security event for the Crypto Officer, because the Crypto Officer is responsible for installation of the cryptographic module.

For the installation of the module, please refer to the 9.3 Install guidance.

9.2. User Guidance

Please refer to the API specification documentation for the usage of each API function.

The User is assumed to use all approved security functions implemented in the module.

The User is responsible for the security strength of a “Key Wrap Key” that is used in the “Key Wrap” service. The “Key Wrap” service accepts two inputs, a wrapped key and a “Key Wrap Key” that wraps a wrapped key.

The security strength of a “Key Wrap Key” shall be higher than 112 bits and equal or higher than the security strength of a wrapped key.

For example, if the security strength of the wrapped key is 256 bits, the security strength of the "Key Wrap Key" shall be equal or higher than 256 bits.

Note:

Security strength of a key differs from key size. Security strength is a number associated with the amount of work (that is, the number of operations of some sort) that is required to break a cryptographic algorithm or system in some way.

9.3. Install Guidance

This section describes how to install the MonoCrypt AES by the Crypto Officer role.

9.3.1 Windows Installation

The Crypto Officer installs the MonoCrypt AES module(DLL) version 2.0.0.

a. Installation

Copy the module to the application folder or the Windows system folder using the copy command, etc.

b.Permission setting

Use Windows permission commands or property settings to set the user access permissions(read, write and execute) to the module.

9.3.2 UNIX Installation

The Crypto Officer installs the MonoCrypt AES module(so) version 2.0.0.

a. Installation

Copy the module to the application folder or the UNIX OS system folder using the copy command, etc.

b.Permission setting

Use UNIX OS permission commands to set the user access and execution permissions to the module.