Trellix Core Cryptographic Module (kernel)

FIPS 140-2 Non-Proprietary Security Policy

Version: 2.2.0.17.0

Date: March 8, 2024

Trellix
6220 America Center Drive
San Jose, CA 95002
888.847.8766
http://www.trellix.com

Prepared for Trellix by

intertek
acumen
security

2400 Research Bvld, Suite 395
Rockville, MD 20850
Phone: +1 (703) 375 9820
Info@acumensecurity.net
https://www.acumensecurity.net

Table of Contents

List of Tables

List of Figures

1. Introduction

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html.

About this Document

This non-proprietary Cryptographic Module Security Policy for Trellix Core Cryptographic Module (kernel) from Trellix provides an overview of the product and a high-level description of how it meets the overall Level 1 security requirements of FIPS 140-2.

The Trellix Core Cryptographic Module (kernel) module may also be referred to as the “module” in this document.

The Cryptographic Module version 2.2.0.17.0 is defined as multiple-chip standalone for the purposes of FIPS 140-2, and the module was tested on the operational environments and platforms detailed in the table below:

#	Operational System	Hardware Platform	Processor	PAA[1]/Acceleration
1	Windows 10 64-bit	Microsoft Surface 3	Intel i5-520M	with and without AES-NI
2	Windows 7 32-bit	Dell Latitude E7270	Intel i5-6300U	with and without AES-NI

Table 1 - Tested Operational Environments

The Cryptographic Module is also supported on the following operating environments for which operational testing and algorithm testing was not performed:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008
- Windows 11
- Windows 10 32-bit
- Windows 8.1 32-bit and 64-bit
- Windows 8 32-bit and 64-bit
- Windows 7-64-bit

[1] AES-NI (the Intel Advanced Encryption Standard (AES) New Instructions (AES-NI)) is an extension to the x86 instruction set architecture for microprocessors from Intel and AMD. The purpose of the instruction set is to improve the speed of applications performing encryption and decryption using AES.

As per FIPS 140-2 Implementation Guidance G.5, compliance is maintained by vendor or user affirmation for other versions of the respective operational environments where the module binary is unchanged. The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported if the specific operational environment is not listed on the validation certificate.

The platforms used during testing met Federal Communications Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part 15, Subpart B.

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	**Level**
1. Cryptographic Module Specification	1
2. Cryptographic Module Ports and Interfaces	1
3. Roles, Services, and Authentication	1
4. Finite State Model	1
5. Physical Security	N/A
6. Operational Environment	1
7. Cryptographic Key Management	1
8. EMI/EMC	1
9. Self ‐ Tests	1
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
Overall Level	1

Table 2 - Security Level Detail

2. Cryptographic Module Specification

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

The module provides AES encryption services to Trellix products and is packaged as a Microsoft Windows kernel mode device driver.

There are no specific hardware or firmware requirements for the module. The module is a software only module, which resides on a General-Purpose Computer (see Figure 1 - Logical and Physical Boundary). The module's physical boundary is that of the device on which it is installed. The device shall be running a compatible operating system (OS) and supporting all standard interfaces, including keys, buttons and switches, and data ports.

There are two distinct, though functionally identical versions of the module, one for each of the environments indicated below:

FILE NAME	OPERATING ENVIRONMENT	PACKAGE
MFECCF*aa*.sys	Microsoft Windows	32-bit
MFECCF*aa*.sys	Microsoft Windows	64-bit

Table 3 - Module binary image

Note: “*aa*” are alphanumeric product identifiers, which are MFECCFDE.sys for the Trellix product Drive Encryption and MFECCFFF.sys for the Trellix product Files and Removable Media Protection.

2.2 Cryptographic Boundary

The module’s logical boundary is a software library. The physical boundary of the module is a General-Purpose Computer (GPC). Figure 1 shows the logical relationship of the Cryptographic Module to the other software and hardware components of the computer.

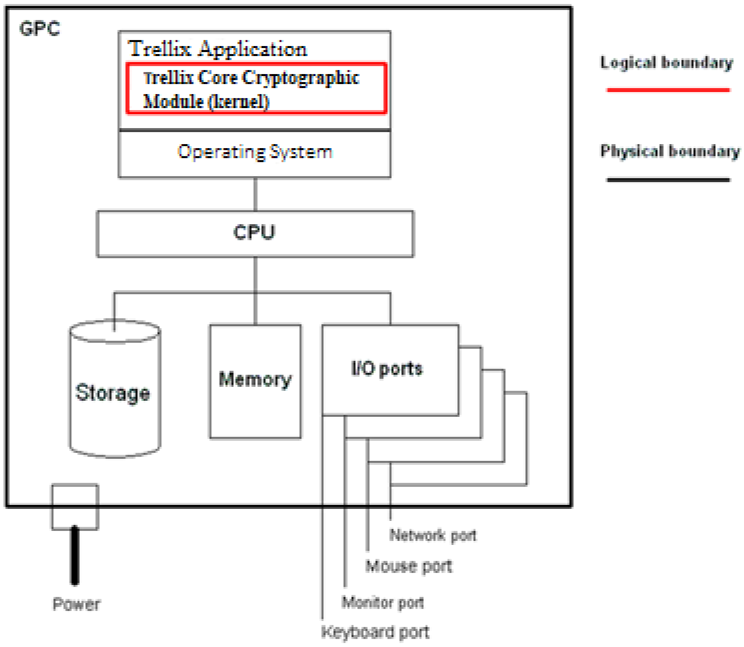

Figure 1 - Logical and Physical Boundary

2.3 Ports and Interfaces

The module provides all logical interfaces via Application Programming Interface (API) calls. These logical interfaces expose services (described in section 4.2) that the User (i.e. application) and operating system may utilize directly.

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

Description	Logical Interface Type
Parameters passed to the module via API calls	Data Input
Data returned from the module via API calls	Data Output
API Calls and/or parameters passed to API calls	Control Input
Information received in response to API calls	Status Output
There is no separate power interface beyond the power interface provided by the GPC itself	Power Interface

Table 4 - Ports and Interfaces

2.4 Mode of Operation

The module only supports an Approved mode of operation.

3. Cryptographic Functionality

The module implements the FIPS Approved cryptographic functions listed in the following table in a FIPS Approved mode of operation.

3.1 Approved Cryptographic Algorithms

The approved security functions included in the Cryptographic Module are utilized by the module's callable services or internal functions.

CAVP Cert	Algorithm [Standard]	Mode/Method	Description / Key Size(s)	Use / Function
A1555	SHS [180-4]	SHA-256	256-bit	Used in the module integrity test.
A1555	HMAC [198]	HMAC-SHA-256	256-bit	Module integrity testing.
A1555	AES [197]	ECB [38A] CBC [38A] CFB8 [38A]	256-bit	Service provided to encrypt and decrypt block of data.

Table 5 - Approved Algorithms and CAVP Certificates

Note: The AES-256 algorithm can run on processors with or without AES-NI capability. However, it will only use AES-NI instructions if run on AES-NI enabled processors.

There are no non-approved cryptographic algorithms within the module.

3.2 Cryptographic Key Management

The table below provides details about the CSP used by the module:

Key/CSP Name	Key/CSP Type	Generation/Input	Output	Storage	Zeroization	Use
System Key	AES 256-bit	Entered into the module via user service API (Key Establishment is N/A per IG 7.7)	N/A	Not persistently stored	Zeroized by power-cycling the module's host platform.	To encrypt all user data written to the module and decrypt all user data read from it.

Table 6 – Secret Keys, Private Keys and CSPs

3.2.1 Key Generation

The module does not generate keys.

3.2.2 Key Zeroization

All key material managed by the module can be zeroized by power-cycling the module's host platform. The module does not persistently store keys. As such, the calling application is responsible for parameters passed in and out of the module.

There are no user-accessible plaintext keys or CSPs in the module.

4. Roles, Services, and Authentication

4.1 Roles

The Cryptographic Module implements both Crypto Officer role and User role. Roles are assumed implicitly upon accessing the associated services. Section 4.2 summarizes the services available to each role.

The module has a Single Operator Mode.

ROLE	DESCRIPTION
Crypto Officer	The administrator of the module having full configuration and key management privileges.
User	General User of the module

Table 7 - Roles

The service tables below are related to the information needed for each role.

4.2 Services

The table below lists the Approved services supported by the module and access rights within services accessible over the module's public interface.

Service	Approved Security Functions	Keys and/or CSPs	Roles	Access rights to Keys and/or CSPs
epe_aesfips_init_key_context	Initializes an AES key expansion with the given key data.	System Key	User	W
epe_aesfips_reset_key_context	Resets the given key context.		User	
epe_aesfips_crypt_bytes	Encrypts or decrypts some data.	System Key	User	E
epe_aesfips_crypt_blocks	Encrypts or decrypts data in blocks with the given key (context).	System Key	User	E
epe_aesfips_get_info	Gets the information about the algorithm.		User	
eeff_crypt	Encrypts or decrypts some data.	System Key	User	E
Self-tests	The power-up software integrity test and AES Known answer test are run automatically when the module is loaded and started.		User	
Show Status	Status is returned in response to individual service API calls and at the completion of the self-tests.		User	
Installation	The module is deployed as part of a Trellix product installation.		CO	
Uninstallation	The module is uninstalled during the uninstallation of the product that deployed the module.		CO	
Key Zeroization	Keys are zeroized by power-cycling the module’s host platform.	System Key	CO	Z

Table 8 - Approved Services, Roles, and Access Rights

G or Generate: The module generates the CSP(s)
R or Read: The CSP is read from the module (e.g. the CSP is output)
W or Write: The CSP is updated or written to the module
E or Execute: Capability to execute or use the Critical Security Parameter
Z or Zeroize: The module zeroizes the CSP

4.3 Authentication

The module does not support operator authentication.

5. Self-tests

5.1 Power-On Self-Tests

On power up or reset, the module performs the self-tests described below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the module enters the Critical Failure error state.

The module performs the following power-up self-tests:

OBJECT	TEST
AES-256	A separate encryption and decryption Known answer test for each AES implementation within the module: AES-CBC Encrypt and Decrypt, key length 256 bits. AES-CFB8 Encrypt and Decrypt, key length 256 bits. AES-ECB Encrypt and Decrypt, key length 256 bits.
Module software	HMAC-SHA-256 Integrity Check[2]

Table 9 - Power-up self-tests

5.2 Conditional Self Tests

The module does not perform any conditional self-tests.

6. Physical Security

The Cryptographic Module is comprised of software only and thus does not claim any physical security.

7. Operational Environment

The Cryptographic Module operates under the operational environment(s) specified in Table 1.

8. Guidance and Secure Operation

This Cryptographic Module is built into Trellix products and is not publicly available to be installed as a stand-alone module. Initialization and guidance instructions are not applicable.

[2] Both the SHA-256 and HMAC-SHA-256 KAT are covered by this test

9. Mitigation of other Attacks

The module does not mitigate any other attacks.

10. Design Assurance

Trellix employs industry standard best practices in the design, development, production, and maintenance of all its products, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Delivery of the Cryptographic Module to customers from the vendor is via the internet. When a customer purchases a license to use the Trellix product containing the Cryptographic Module software, they are issued with a grant number as part of the sales process. This is then used as a password to allow them to download the software that they have purchased. Once the Cryptographic Officer has downloaded the product containing the Cryptographic Module, it is their responsibility to ensure its secure delivery to the users that they are responsible for.

11. References and Standards

For more information on Trellix products please visit: https://www.trellix.com. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

The following Standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198- 1, July, 2008*
[180-4]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*

Table 10 - References

12. Acronyms and Definitions

The following Acronyms are referred to in this Security Policy:

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions. Seven instructions for accelerating different sub-steps of the AES algorithm included in some Intel and AMD microprocessors.
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CCCS	Canadian Centre for Cyber Security
CMSP	Cryptographic Module Security Policy
CMVP	Crypto Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
DLL	Dynamic Link Library
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	key-Hashed Message Authentication Code

Acronym	Definition
IG	Implementation Guidance
IV	Initialization Vector
KAT	Known Answer Test
MAC	Message Authentication Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
SHA	Secure Hash Algorithms
SP	Security Policy

Table 11 - Acronyms