THALES

CipherTrust Transparent Encryption Cryptographic Module

MODULE VERSION 2.0

LEVEL 1 NON-PROPRIETARY SECURITY POLICY

Document Information

Document Part Number	007-000662-001
Release Date	July 7, 2021

Revision History

Revision	Date	Reason
A	March 13 2020	Final Version
B	April 22, 2021	Updated during CMVP Coordination and adding AIX
C	May 20, 2021	Updating during 2nd round of CMVP Coordination
D	July 7, 2021	Updated platform information with additional specifics

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE

This document deals only with operations and capabilities of the CipherTrust Transparent Encryption (CTE) Cryptographic Module in the technical terms of FIPS PUB 140-2, 'Security Requirements for Cryptographic Modules', 12-03-2002.

General information on CTE alongside other Thales products is available from the following sources:

- the Thales internet site contains information on the full line of available products at http://www.thalessecurity.com
- product manuals and technical support literature is available from the Thales Customer Support Portal at https://supportportal.gemalto.com.
- technical or sales representatives of Thales can be contacted through one of the channels listed on https://safenet.gemalto.com/contact-us.

> NOTE You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

1 Introduction

1.1 Purpose

This is a non-proprietary Federal Information Processing Standards Publication (FIPS 140-2) Security Policy for the CipherTrust Transparent Encryption Cryptographic Module version 2.0 which ships with version 6.3 of the Vormetric Transparent Encryption product for Windows and Linux. The module also ships with version 7.1 of the CipherTrust Transparent Encryption product for AIX. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 1 requirements. This Security Policy forms a part of the submission package to the validating lab.

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections.

1.2 References

This Security Policy describes how this module complies with the eleven sections of the Standard:

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at: https://csrc.nist.gov/projects/cryptographic-module-validation-program
- For more information about Thales, please visit http://www.thalesesecurity.com

2 Module Overview

2.1 Product Description

The CipherTrust Transparent Encryption Cryptographic Module is a Level 1 FIPS 140-2 module of type *Software-Hybrid* with an embodiment classified as *Multi-chip Standalone*. This module is a component within the Vormetric and CipherTrust Transparent Encryption solutions, which in turn are part of the Vormetric and CipherTrust Data Security solutions. The CipherTrust Transparent Encryption Cryptographic Module interacts with the Vormetric Data Security Manager (DSM), which is itself, a cryptographic hardware module. The DSM has been validated separately from this module.

The CipherTrust Transparent Encryption Cryptographic Module is a loadable kernel module. This module comprises a layer that enforces an access and encryption policy upon selected data on end-user systems. The policy specifies a key to be used when writing data to disk and while reading data from disk. This module contains the Vormetric Transparent Encryption Cryptographic Library, which provides all cryptographic services.

The CipherTrust Transparent Encryption Cryptographic Module implements AES-CBC, AES XTS, SHA-256 SHA-384, HMAC-SHA-256, HMAC-SHA-384, RSA, and PBKDF.

The product meets the overall requirements applicable to Level 1 security for FIPS 140-2.

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

Cryptographic Module Security Policy	1
Overall Level of Certification	1

Table 1 - Module Compliance Table

2.1.1 Cryptographic Boundary

The CipherTrust Transparent Encryption Cryptographic Module's logical boundary is illustrated in **red** in Figure 1. The module's physical boundary is the general purpose computer or server.

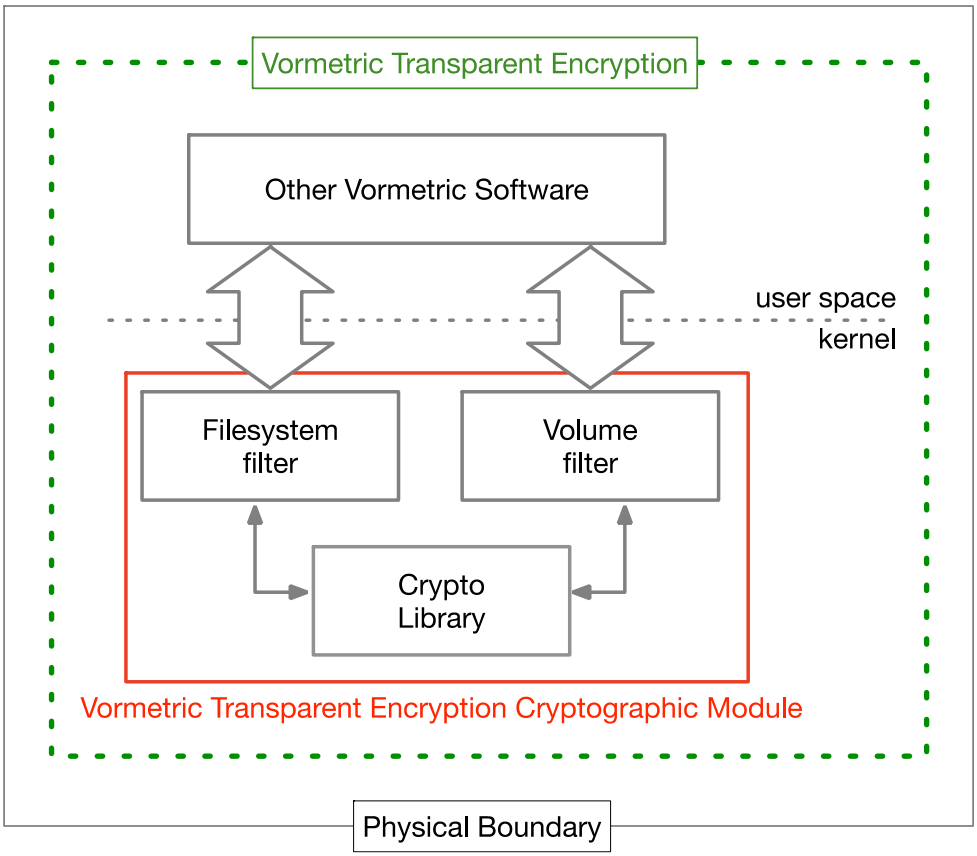

Figure 1 – Logical Cryptographic Boundary

The loadable kernel module (shown in red in the diagram above) for all Linux platforms is named "secfs2.ko" and for all Windows platforms is named "vmmgmt.ko". The module name for AIX is named "secfs2"

2.1.2 Platform Considerations

This module is validated on Red Hat Enterprise Linux 7.7 and Windows 2016 Server, running on VMware ESXi 6.5.0 on a Dell Proliant DL380. This module is also validated on AIX version 7.1 running on an IBM 8286-42A.

This module utilizes the “AES-NI” instruction set for AES cryptographic operations on Linux and Windows platforms. On AIX, it utilizes the “NX Crypto Acceleration” instruction set. All other cryptographic operations are performed in software inside the module boundary.

2.2 Module Ports and Interfaces

The module is software based and designed to meet FIPS 140-2 Level 1 requirements.

FIPS 140-2 Interface	Physical Interface	Logical Interface
Data Input interface	External Devices (LAN/USB/…), Keyboard	File System / Volume write function calls
Data Output interface	External Devices (LAN/USB/…), Monitor	File System / Volume read function calls
Control Input interface	External Devices (LAN/USB/…), Keyboard	Input parameters to ioctl calls into the module
Status Output interface	External Devices (LAN/USB/…), Monitor	Output parameters from ioctl calls into the module

Table 2 – Mapping FIPS 140-2 Interfaces and Logical Interfaces

2.3 Roles, Services and Authentication

2.3.1 Roles and Services

The User and Crypto Officer roles are implicitly assumed by the entities that can access the interfaces to the cryptographic module. These entities do so implicitly through the file system / volume filter read and write interfaces, and control through the ioctl interfaces of the module.

2.3.2 Authentication

The module does not provide identification or authentication mechanisms that would distinguish between the two supported roles. Each process or thread accessing the module is logically separated by the operating system into independent contexts of execution, and hence the FIPS 140-2 requirement for a single user mode of operation is upheld.

2.3.3 Authorized Services

The CipherTrust Transparent Encryption Agent supports the services listed in the following tables. Each table shows the privileges of each role on a per-service basis. The privileges are divided into:

R - The item is **read** or referenced by the service.

W -The item is **written** or updated by the service.

E - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

The cryptographic module utilizes the Intel “AES-NI” or PowerPC NX Crypto Acceleration instruction set for AES cryptographic operations. It intercepts I/O calls, evaluates a policy, and encrypts or decrypts data according to the rules in the policy. There are several control interfaces for this component, all of which have to do with either initialization or with policy and key configuration. These are accessed in the “Crypto Officer” role. The data input/output interfaces performed through intercepting I/O operations are accessed in the “User” role. The keys used in the Authorized Services are described in Section 7, “Key Management”, in Table 5.

Authorized Services	Cryptographic Key/CSP	Roles	Access
Run Power-On Self-Test	HMAC Integrity Key	Crypto Officer	E
Initialization (Also known as “registration”)	SECFS Private Key SECFS Key Encryption Key SECFS HMAC Key	Crypto Officer	WE
Configuration Update (New configuration / policy / key information is given to the kernel module)	All keys in Table 5	Crypto Officer	WE
Status Query	N/A	Crypto Officer	R
Rekey (converting data from being encrypted with one key to being encrypted with another)	File System / Volume Filter Keys	Crypto Officer	RWE
Zeroization	All	Crypto Officer	WE
File System / Volume interfaces: read(), write(), etc	File System or Volume Filter Keys (AES AES-XTS)	User	RWE
Non-Approved Service: File System interfaces: read, write, etc	File System Keys (ARIA 128-bit and 256-bit)	User	RWE

Table 3 – Authorized Services

2.4 Physical Security

This software-hybrid module meets the level 1 physical security requirements. The module runs on a general-purpose computer.

2.5 Operational Environment

The CipherTrust Transparent Module operates in a “modifiable operational environment”. It exists as software executing in a commercially available operating system. The specifically tested platforms are:

Operating System	Bits	Processor / System	Cryptographic Hardware
Red Hat Enterprise Linux 7.7 on VMware ESXi 6.5.0	64	Intel Xeon – Dell Proliant DL380	Intel® Xeon® Gold 5118 Skylake family
Windows 2016 Server on VMware ESXi 6.5.0	64	Intel Xeon – Dell Proliant DL380	Intel® Xeon® Gold 5118 Skylake family
AIX 7.1 TL 7100-05-04-1914	64	IBM 8286-42A EPXH Power8 with PAA	IBM PowerPC 8

Table 4 – Tested Platforms

All other platforms supported by Thales are “Vendor Affirmed” to be FIPS 140-2 compliant as per FIPS Implementation Guidance section G.5. The CMVP allows vendor porting of a validated level 1 software-hybrid cryptographic module running on a CPU supporting the Intel AES-NI or PowerPC NX Crypto Acceleration instruction set from the GPC(s) specified on the validation certificate to a GPC that was not included as part of the validation status, as long as no source code modifications are required. The validation status is maintained on the new GPC without re-testing the cryptographic module on the new GPC. The CMVP makes no statement as to the correct operation of the module when so ported if the specific operational environment is not listed on the validation certificate.

The Intel® Xeon® Gold 5118 Skylake CPU inside Dell Proliant DL380 is shown in Figure 2.

Figure 2 – Physical Cryptographic Hardware for Intel AES-NI

The IBM 8286-42A is shown in Figure 3.

Figure 3 – Physical Cryptographic Hardware for PowerPC NX Crypto Acceleration

2.6 Cryptographic Key Management

The cryptographic library manages keys. All of the keys and CSPs are generated externally.

2.6.1 Cryptographic Keys and CSPs

Key	Generation	Storage	Use	Input / Output
HMAC Integrity Key (HMAC-SHA 384-bit, key size 384-bit)	At vendor facility	Incorporated into binary	Protects the integrity of the module	Hardcoded. Cannot be exported
SECFS HMAC Key (HMAC-SHA 256-bit, key size 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Protects the integrity of keys when stored	Input only. Cannot be exported
SECFS Key Encryption Key (AES 256-bit)	Generated during VTE agent initialization (NIST 800-132 option 1a PBKDF)	Session key only for life of VTE session	Protects storage of keys	Input only. Cannot be exported
SECFS Private Key (RSA 2048-bit)	Generated externally to the module	Stored in encrypted form with AES	Protects the File System Key Encrypting Key for key transport	Input only. Cannot be exported

File System Key Encrypting Key (AES 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Protects the File System / Volume Keys	Input only. Cannot be exported
File System / Volume Keys (AES 128-bit and 256-bit) / AES-XTS 256-bit keys)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Encrypts and decrypts file system / Volume data	Input only. Cannot be exported
File System Keys (ARIA 128-bit and 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Encrypts and decrypts file system data. This is a **non-approved** security function	Input only. Cannot be exported

Table 5 – Keys and CSPs

2.6.2 Approved Security Algorithms

The module keys map to the following algorithms certificates. All validated platforms have AES algorithm certificates which utilize Intel AES-NI or PowerPC NX Crypto Acceleration. All other algorithms are implemented in software inside the module boundary.

Approved or Allowed Security Functions	**CipherTrust Transparent Agent Certificate #**
Symmetric Encryption/Decryption	
AES (CBC Mode; Encrypt/Decrypt; 128 and 256 bit)	Algorithm certs # C1464 and #A1287
AES (XTS Mode[1]; Encrypt/Decrypt; 256 bit)	Algorithm certs # C1464 and #A1287
Secure Hash Standard (SHS)	
SHA-256, SHA-384	Algorithm certs # C1464 and #A1287
Data Authentication Code	

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

HMAC-SHA-256, HMAC-SHA-384	Algorithm certs # C1464 and #A1287
Secret Agreement and Key Derivation	
SP 800-132 PBKDF[2] Salt (32 bytes) & Iteration count (100000); PRF (HMAC SHA-384)	Vendor affirmed and Algorithm cert. #A1287 for AIX only
Non-Approved Security Functions	
RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)[3]	
ARIA (Obfuscate/Unobfuscate, Key Size = 128, 256)	

Table 6 - Algorithms Table

2.7 EMI/EMC

The general-purpose computers that this module was tested on meet the FCC Code of Federal Regulations, Title 47, Part 15, Subpart B as a class B unintentional radiator.

2.8 Self-Test

The module performs power-up self-tests and conditional self-tests.

2.8.1 Power-up Self Tests

Any other processing and data input/output is inhibited while the tests are in progress. If any test fails, an error status such as "FIPS Algorithm Known Answer Test/Integrity test failed" is displayed and the module will cease operation. When each of the five tests run to completion, a "`FIPS <testname> Test passed`" message is written to the log. When all tests pass, the module is operating in FIPS mode. While running the non-approved security function ARIA, the module is in non-FIPS mode. To run the self-tests on demand, restart the module.

Cryptographic Algorithm Known Answer Tests (KATs) are run at power-up for:

- AES (CBC mode for Encrypt/Decrypt)
- AES (XTS mode for Encrypt/Decrypt)
- SHA-256, SHA-384
- HMAC-SHA-256, HMAC-SHA-384, and

[2] Specifically IETF RFC 2898 PBKDF2. Keys derived by this PBKDF shall only be used for storage applications.
[3] RSA key wrapping is an Allowed security function

> PBKDF KAT

Software Integrity Tests:

The module checks the integrity of its object code when it is initialized. It performs an HMAC-SHA-384 of itself when it is loaded into the kernel; this is compared to an HMAC-SHA-384 digest generated during build time. If the results are not the same, an error message is written to the output interface, and the kernel modules will cease further operation.

2.8.2 Conditional Self-Tests

The module performs no conditional self-tests.

2.9 Crypto-Officer and User Guidance

This section shall describe the configuration, maintenance, and administration of the cryptographic module.

2.9.1 Secure Setup, Initialization and Operation

It is the operator's responsibility to operate the module according to the security policy rules described in the following section. To configure the module, the Crypto-Officer should:

> Install the Vormetric Transparent Encryption software package.

> Register with a Vormetric Data Security Manager.

> Verify that the fingerprints of the generated certificates match those shown on the Vormetric Data Security Manager.

> Verify that the message described in section 9.1 is emitted to ensure that the module is operating in a FIPS-approved mode.

Zeroization is performed by uninstalling the module. The platform's hard drive must be reformatted or overwritten after uninstallation.

To show the status of the module on Linux or AIX, run the command "vmsec status". To show the status of the module on Windows platforms, click on the Vormetric icon in the tray and select "status".

2.9.2 Module Security Policy Rules

The module operates in FIPS mode after all the power-up self-tests have passed, and the message described in section 9.1 has been displayed. However, when using the non-Approved Security Function ARIA, the module is in a non-FIPS mode. To operate in FIPS mode, use only FIPS Approved security functions.

2.10 Design Assurance

Vormetric utilizes Subversion (SVN) for configuration management of product source code. Vormetric also utilizes Confluence, an internal Wiki, for configuration management of functional specifications and

documentation. Both support authentication, access control, and logging. Software is distributed either in person or via a secure HTTPS-based web site.

2.11 Mitigation of Other Attacks

The module does not mitigate against any specific attacks.