THALES

Thales CipherTrust Cryptographic Provider (CCP)

NON-PROPRIETARY SECURITY POLICY

FIPS 140-2, Level 1

Document Information

Document Part Number	002-000407-001
Release Date	December 22, 2022

Revision History

Revision	Date	Reason
A	January 14, 2022	Initial version.
B	February 4, 2022	Algorithm updates
C	February 8, 2022	Minor updates
D	March 1, 2022	Updates per Acumen comments
E	December 22, 2022	Updates per CMVP Coordination

Trademarks, Copyrights, and Third-Party Software

© 2022 Thales. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

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.

> This document shall not be posted on any network computer or broadcast in any media other than on the NIST CMVP validation list and no modification of any part of this document shall be made.

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

ACRONYMS AND ABBREVIATIONS

Term	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard – New Instructions
API	Application Programming Interface
CBC	Chain Block Cipher
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
CU	Crypto User
DRAM	Dynamic Random Access Memory
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
GPC	General Purpose Computer
HMAC	Keyed-Hash Message Authentication Code
IG	Implementation Guidance
I/O	Input/Output
IV	Initialization Vector
KAT	Known Answer Test
MAC	Message Authentication Code
N/A	Not Applicable
PAA	Processor Algorithm Accelerator
PKCS	Public-Key Cryptography Standards
POST	Power-on Self Test
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SO	Security Officer
TDES	Triple – Data Encryption Standard

REFERENCES

[FIPS 140-2]	Federal Information Processing Standards Publication (FIPS PUB) 140-2, 'Security Requirements for Cryptographic Modules', May 25, 2001 (including change notices 12-02-2002).
[FIPS 140-2 IG]	NIST, Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program, Nov 5, 2021.
[FIPS 180-4]	Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), NIST, August 2015.
[FIPS 186-4]	Federal Information Processing Standards Publication 186-4, Digital Signature Standards (DSS), NIST, July 2013.
[FIPS 197]	Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001.
[FIPS 198-1]	Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.
[SP800-38A]	NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation – Methods and Techniques, Morris Dworkin, December 2001.
[SP800-38D]	NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.
[SP800-52r2]	NIST Special Publication 800-52 Rev 2, Guidelines for the Selection, Configuration, and Use of Transport Lauer Security (TLS) Implementations, August 2019.
[SP800-67r2]	NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Rev 1, January 2012.
[SP800-131Ar2]	NIST Special Publication 800-131A revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019.
[PKCS #1]	PKCS #1: RSA Cryptographic Standard, RSA Laboratories, v2.1.
[CCP User Guide]	'007-000843-001, 'CipherTrust Manager Application Data Protection CAPI 8.12.1: User Guide', Rev B, 20th January 2021.

PREFACE

This document deals only with operations and capabilities of the Thales CipherTrust Cryptographic Provider (CCP) in the technical terms of [FIPS 140-2].

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

- the Thales internet site contains information on the full line of available products at https://cpl.thalesgroup.com
- product manuals and technical support literature is available from the Thales Customer Support Portal at https://supportportal.thalesgroup.com/csm
- technical or sales representatives of Thales can be contacted through one of the channels listed on https://cpl.thalesgroup.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 General

1.1 Security Level

The cryptographic module meets all level 1 requirements security requirements for [FIPS 140-2] as summarized in the table below:

Table 1: FIPS 140-2 Security Levels

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	3
Mitigation of Other Attacks	N/A
Overall Level of Validation	**1**

2 Cryptographic Module Specification

2.1 Module Overview

The Thales CipherTrust Cryptographic Provider (CCP) is a **software hybrid module**, with embodiment: **multi-chip standalone**.

The cryptographic boundary of the module encompasses elements of Thales CipherTrust Cryptographic Provider (CCP), which provides cryptographic functionality either internally to the product or to external clients. The module provides support for a broad range of cryptographic services.

All keys are passed into the module and exclusively stored in DRAM.

Access to services offered by CipherTrust Cryptographic Provider (CCP) is exclusively through a number of Application Programming Interfaces (API) calls provided by the CipherTrust Cryptographic Provider (CCP) module. The APIs can be only accessed by other applications running internal to the physical boundary of the module.

2.2 Module Description

The Thales CipherTrust Cryptographic Provider (CCP) is a software hybrid module designed to execute on a general-purpose computer hardware platform. The module will always reside on user-supplied General-Purpose Computers (GPCs). The logical boundary of the module consists of a shared library file and its integrity check HMAC file along with the Intel CPU (i.e. the AES-NI set (PAA) leveraged from the CPU).

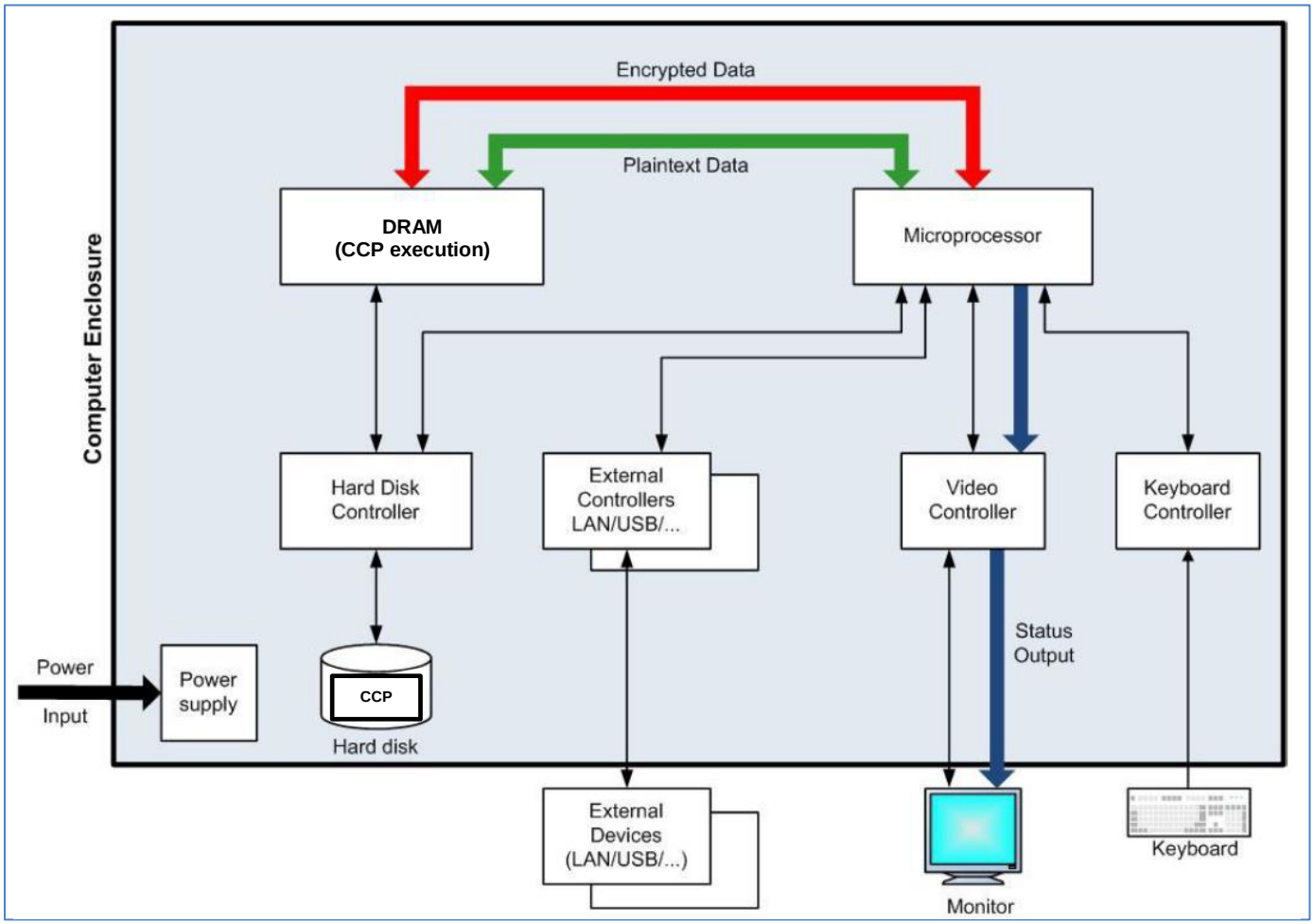

Figure 2-1: Physical Module Cryptographic Boundary

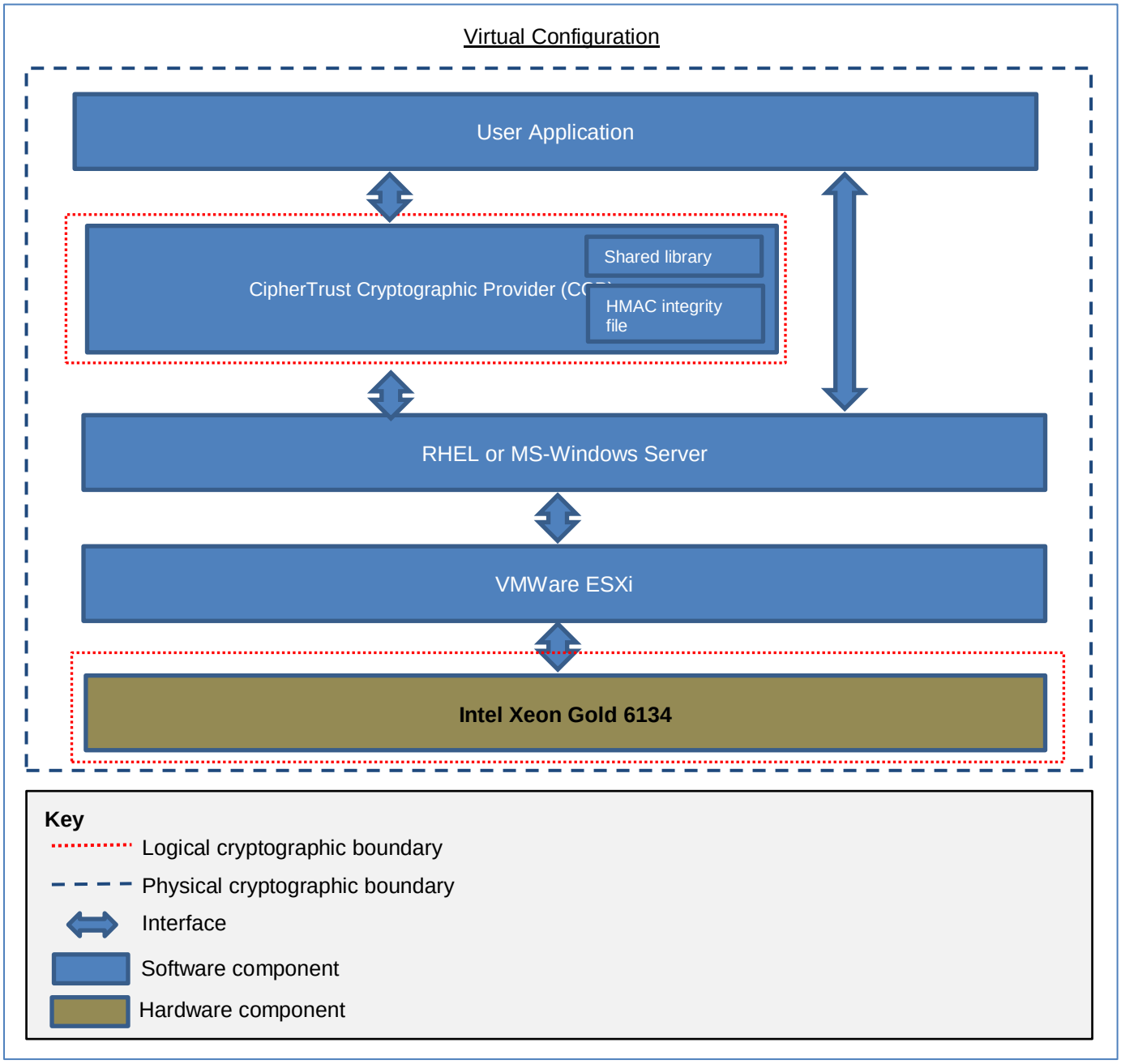

Figure 2-2: Logical Cryptographic Boundary.

The logical boundary of the module consists of the following files:

- for MS-Windows operating systems:
  - capi.dll
  - capi.sig
- for Linux operating systems:
  - libCAPI.so
  - capi.sig

The operator must use only Approved Algorithms from Section 2.4. Additionally, details on placing the module in Approved mode of operation is detailed in Section 10 of this document.

Other applications access the services of the module via API where all CSPs associated with services with are stored in the DRAM on the host GPC.

The module relies on the operating environment to provide separation of memory used to execute the module from other services running on the host appliance. Additionally, it relies on the operating environment to provide a procedural path to CSP zeroization.

2.3 Tested Configurations

The validated module Software Version is 1.0. The following tested configurations are covered in this security policy:

Table 2-1: Cryptographic module tested configuration.

Platform	Operating System	Distinguishing Features
Dell PowerEdge R720 (General purpose x86-based server using an Intel Xeon Gold 6134 as its CPU).	RHEL Version: 8.3 with VMWare ESXi 6.7.0	Virtualized configuration used with customer supplied host.
Dell PowerEdge R720 (General purpose x86-based server using an Intel Xeon Gold 6134 as its CPU).	MS-Windows Server 2019 with VMWare ESXi 6.7.0	Virtualized configuration used with customer supplied host.

NOTE As per FIPS 140-2 Implementation Guidance G.5, compliance is maintained for other versions of the respective operational environments where the module binaries are unchanged.

CMVP allows porting of this cryptographic module specified on the validation certificate to an operational environment which was not included in the original certification provided that porting rules identified in [FIPS 140-2 IG] G.5, 'Maintaining validation compliance of software or firmware cryptographic modules' are followed.

The vendor affirmed platforms shall include the following (without virtualization):

- General purpose x86-based server with RHEL Version 8.0, 8.1, 8.2, 8.3; and
- General purpose x86-based server with MS-Windows Server 2016 and 2019

The Cryptographic Module Validation Program (CMVP) makes no statement as to the correct operation of the module or the security strengths of generated keys when this module in its virtualised form is executed in an operational environment not listed on the validation certificate.

2.4 Approved Algorithms

The following cryptographic library and associated CAVP certificate is used by the cryptographic module:

> **CipherTrust Cryptographic Provider Core Crypto Library (PAA on)** (Cert #A2124);

- Supported Algorithms: AES, Triple-DES, SHA, ECDSA, RSA, and HMAC

The approved algorithms implemented by the module with their mapping to the certificate above and algorithms use by service are listed in the Table 2-2.

Table 2-2: Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode / Methods	Description / Key Size(s) / Key Strengths	Use / Function
Asymmetric Cryptography				
A2124	**Algorithm:** ECDSA. **Standard:** [FIPS 186-4]	**Methods:** Signature Verification **Hash options (Signature Verification):** SHA1, SHA2-256, SHA2-384, and SHA2-512.	**Curves:** P-224, P-256, P-384, and P-521.	Used to support the following services: > Cryptographic API calls
A2124	**Algorithm:** RSA. **Standard:** [FIPS 186-4]	**Methods:** Signature Verification. **Signature Types:** PKCS #1-v1.5 1.5, and PKCS-PSS. **Hash options:** Signature Verification (PKCS #1-v1.5 and PKCS-PSS): SHA-1, SHA2-256, SHA2-384, SHA2-512.	**Modulus lengths**: 1024, 2048, 3072, and 4096	Used to support the following services: > Cryptographic API calls
Hashing				
A2124	**Algorithm:** SHA. **Standards:** [FIPS 186-4]	**Methods:** SHA-1, SHA2-256, SHA2-384, and SHA2-512.	N/A.	Used to support the following services: > Cryptographic API calls

CAVP Cert	Algorithm and Standard	Mode / Methods	Description / Key Size(s) / Key Strengths	Use / Function
Message Authentication Code				
A2124	**Algorithm:** HMAC. **Standard:** [FIPS 198-1].	**Methods:** HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512.	**Mac Sizes:** 20-to-64 bytes (dependent on hash). **Key Sizes:** key size < block size, key size = block size, and key size > block size.	Used to support the following services: > Cryptographic API calls In addition, as an internal module function, HMAC is used to support software integrity checking during power-on self-test.
Symmetric				
A2124	**Algorithm:** AES **Standards:** [FIPS 197], [SP800-38A], and [SP800-38D]	**Modes:** CBC and ECB (encryption and decryption)	**Key sizes:** 128, 192, and 256-bits.	Used to support the following services: > Cryptographic API calls
A2124	**Algorithm:** Triple-DES **Standard:** [SP800-67r2]	**Modes:** CBC, and ECB K1, K2, K3 independent	**Key size:** 168-bits. **Key strength:** 112-bits.	Used to support the following services: > Cryptographic API calls **This algorithm is only permitted for use until Dec 31st, 2023, after which point it is disallowed for all new encryption operations based on planned algorithm transitions outlined in [SP800-131Ar2].**

2.5 Non-Approved Algorithms

Non-FIPS Approved security functions shall not be called when the module is operating in a FIPS Approved mode (see section 10 for further details on configuring the Approved mode of operation). The use of these algorithms will result in the module operating in the non-Approved mode.

Table 2-3: Non-Approved algorithms

Non-Approved Algorithm	Use / Function
AES - in GCM mode	Encryption/Decryption
ARIA	Encryption/Decryption
DES (single)	Encryption/Decryption
DRBG	Used to provide random numbers for other non-Approved algorithms that require a random number.
ECDSA	Signature generation
ECIES	Encryption/Decryption
FPE (Format-preserving encryption)	Encryption/Decryption
RSA	Signature generation
SEED	Encryption/Decryption

3 Cryptographic Module Interfaces

3.1 Ports and Interface Overview

As a software-hybrid module, the module does not have physical ports. For the purpose of the [FIPS 140-2] validation, the physical ports are interpreted to be the physical ports of the GPC hosting the module.

The logical interfaces are the API through which applications request services. The module supports the following interfaces:

Table 3-1: Mapping of FIPS 140-2 Interfaces to Physical and Logical Interfaces

FIPS 140-2 Interface	Logical Interface
Data Input	Keys/Parameters passed to the module via API calls.
Data Output	Data returned from the module via API calls.
Control Input	API Method Calls and/or parameters passed to API calls.
Status Output	Information received in response to API calls. Messages sent to logs and system standard output maintained by the host platform executing the module.
Power Interface	There is no separate power or maintenance access interface beyond the power interface provided by the module host platform itself.

4 Roles, Services and Authentication

4.1 Roles

The module supports 'Users' that can configure and use cryptographic services provided by the module via API calls.

In addition to the User role, the module implicitly supports a Crypto Officer role. The Crypto Officer is able to install and configure the module. Role assumption is implied by the service being requested and the parameters supplied. The module does not support authentication as it meets Level 1 FIPS 140-2 requirements.

Table 4-1: Thales CipherTrust Cryptographic Provider (CCP) Roles

Role	FIPS 140-2 Mapped Role	Principle Duties
Administrator	Crypto Officer	This role is able to configure the module.
User	User Role	The user role is associated with external entities or clients, which connect to the module to consume its cryptographic services via one or more of the custom API calls.

Thales CipherTrust Cryptographic Provider (CCP) Module does not support a maintenance role.

4.2 Authentication

The module does not support authentication and all roles are assumed implicitly.

4.3 Services

Thales CipherTrust Cryptographic Provider (CCP) Module supports the services listed in the following table.

All services listed in the following table below is supported by the module and exclusively use the security functions listed in Table 2-2: Approved Algorithms.

The module shall not use the algorithms listed in section 2.5, 'Non-Approved Algorithms' as they are not permitted for use.

For a complete description of CSPs referenced from the table, please see Table 6-1: Summary of CSPs.

In the 'Cryptographic Keys and CSPs alongside access rights' column:

- R = Read: The CSP or key is read from the module.
- W = Write: The CSP is updated, imported, or written to the module.
- E = Execute: The module uses the CSP in performing a cryptographic operation.

Table 4-2: Services

Service	Approved Security Functions	Cryptographic Keys and CSPs alongside access rights	Role		Notes
			Admin	User	
Key Management Operations					
Key Zeroization	none	W - symmetric keys, HMAC keys, asymmetric keys	X	X	Performed automatically on module startup and on all power cycles.
Module Management Operations					
Run Power-On Self Test	HMAC	E - HMAC Integrity Key	X	X	Performed automatically on module startup.
Initialization (Also known as "registration")	none	None	X	—	N/A
User Cryptographic Services					
Show Status	none	None	X	X	Performed by viewing system logs.

Service	Approved Security Functions	Cryptographic Keys and CSPs alongside access rights	Role		Notes
			Admin	User	
Cryptographic API calls (encrypt/decrypt, verify, and hash)	**AES** (#A2124) – ECB and CBC[1]. **Triple-DES** (#A2124) – ECB and CBC[2]. **HMAC** (#A2124) – HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512. **SHA** (#A2124) – SHA-1 SHA2-256 SHA2-384 SHA2-512 **ECDSA** (#A2124) – Signature Verification[3]. **RSA** (#A2124) – Signature Verification.	R, W, E - symmetric keys, asymmetric keys, HMAC keys	X	X	

[1] Although Algorithm tested, AES GCM is not supported by the module as an Approved algorithm. AES GCM shall not be used by the operators in Approved mode
[2] Please refer to Section 10.6 on Triple-DES usage.
[3] Although Algorithm tested, ECDSA Signature Generation shall not be used by the operators in Approved mode of operation.

5 Operating Environment

The module supports a **modifiable operating environment** as defined in Section 4.6 of [FIPS 140-2]. All cryptographic keys and CSPs are under the control of the OS, which protects its CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined API.

The tested OS segregates user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system 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.

6 CSP Management

6.1 Critical Security Parameter

The following table lists Critical Security Parameters (CSP) used to perform approved security function supported by the cryptographic module:

Table 6-1: Summary of CSPs

Key / CSP name and Type	Generation or Establishment	Entry / Output	Storage	Use and Related Keys
HMAC Integrity Key (HMAC-SHA 256-bit, key size 256-bit)	At vendor facility	N/A – key is Incorporated into the module's binary	Incorporated into binary	Protects the integrity of the module
Symmetric keys (Triple-DES and AES)	N/A	Via the module API in plaintext	Stored in DRAM as managed by the host OS. DRAM is automatically zeroized by the OS following restart of the module or power-cycle."	Encrypts and decrypts user data
Asymmetric keys (ECDSA and RSA)	N/A	Via the module API in plaintext	Stored in DRAM as managed by the host OS. DRAM is automatically zeroized by the OS following restart of the module or power-cycle."	Used to verify digital signatures
HMAC keys	N/A	Via the module API in plaintext	Stored in DRAM as managed by the host OS. DRAM is automatically zeroized by the OS following restart of the module or power-cycle."	Message authentication

6.2 Key Entry and Output Methods

Since all key entry and output is performed between the application software and the Cryptographic Module (CM) via paths internal to the host General Purpose Computer, then Section 7.7 of the [FIPS 140-2 IG] (*Key Establishment and Key Entry and Output*) is applicable. As stated in Table 1 of this IG (*Key Establishment*), there is no requirement for a Key Establishment method (marked in the table as “N/A” for Not Applicable).

6.3 Key Zeroization

Key Zeroization is performed either by restarting the host application or calling the I_C_CloseSession API.

7 Self-Tests

7.1 Summary

CipherTrust Cryptographic Provider (CCP) provides power-on tests in order to ensure correct operation of the module.

Failure of the power-on tests will trigger the module, and all dependent module services, to enter their error state. When in the error state, no cryptographic operations supported by the module are accessible to the user or system.

Recovery from self-test failure is achieved by restarting all services running on the module appliance. If the error persists, the module must be un-installed and re-installed.
Where on demand self-tests are required, restart the module using the same method.

Indicator for self-test failure is based on:

> **Option 1:** Error message output directly to an active session with the module on the platform serial interface.

> **Option 2:** Error message added to the system log.

Error messages transferred to the system audit log maintained by the operating environment for the module can be read by parsing the log located in the following locations:

- Windows – `C:\Program Files\CipherTrust\CADP_CAPI\fips_selftest.log`
- Linux – `/var/log/CipherTrust/fips_selftest.log`

Example messages related to self-test failure are shown in the table below:

Success Logs

```
CAPI Library: Thu Sep 16 07:05:32 2021 [SUCCESS] integrity check passed!
CAPI Library: Thu Sep 16 07:05:32 2021 [SUCCESS] selftest passed!
```

Failure Logs for Integrity Test

```
CAPI Library: Wed Sep 15 17:28:14 2021 [FAILURE] integrity check failed!
CAPI Library: Wed Sep 15 17:28:14 2021 [TERMINATE] exiting due to failure!
```

Failure Logs for Self-test

```
CAPI Library (2363694): Fri Feb 18 11:37:27 2022 [SUCCESS] integrity check passed!
CAPI Library (2363694): Fri Feb 18 11:37:27 2022 [FAILURE] selftest failed!
CAPI Library (2363694): Fri Feb 18 11:37:27 2022 [TERMINATE] exiting due to failure!
```

Figure 7-1: Example log messages relating to self-test failure.

In addition to self-test failures, successful tests are separately recorded in the same log.

All self-tests are confirmed as having successfully passed when the module service is listed as having started.

7.2 Power-On Self-Tests

The module performs POST upon power-up to confirm the firmware integrity, and to check the continued correct operation of the each of the implemented cryptographic algorithms. While the module is running these tests, all interfaces to it are disabled until the tests successfully complete. If any test fails an error message is output, the and data output is inhibited.

Power-up self-tests supported by the module are covered in the following tables:

Table 7-1: Power-On Self-Tests (General)

Test Name	Description
Module integrity test	Integrity check using HMAC-SHA-256. This check is run on the binary ahead of it subsequently performing further Power-On Self-Tests.

Table 7-2: Power-On Self-Tests (KAT)

Test Name	Description
KAT – ECDSA	Verify test with curve P-384 and hash algorithm SHA2-384.
KAT – RSA	Verify tests with PKCS#1 v1.5 and PSS, hash algorithms SHA2-256 and SHA-1.
KAT – HMAC[4]	Message digest KATs for HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512.
KAT – AES	Encrypt/Decrypt KATs for ECB and CBC modes (128 and 256-bit key sizes).
KAT – Triple-DES	Encrypt/Decrypt KATs for ECB and CBC modes, 3-Key.

7.3 Conditional Self Tests

The module does not perform any conditional self-tests since there are no cryptographic operations which require these to be run.

[4] As per IG 9.1 and IG 9.2, the module performs the HMAC SHA selftests and these tests pass, thus assuring the health of underlying SHS implementation.

8 Physical Security

The Intel Xeon Gold 6134 processor, the hardware component of the module, is a single chip with a production-grade enclosure and hence conforms to the Level 1 requirements for physical security.

This Security Policy does not claim any physical security for the software portion of the module.

9 Mitigation of Other Attacks

No assurance claims are made under this section.

10 Guidance

10.1 Verifying module integrity following delivery

An SHA-256 hash value is posted on the Thales customer support portal along with the released binary. A customer can then download the relevant binary, compute the SHA-256 hash value of the downloaded binary and then verify that the posted and computed SHA-256 hash values are equal in order to verify integrity. Please note that this is a separate manual process independent of the required Integrity Test at Power-on performed automatically by the module.

10.2 Identifying the Module Software Version

To identify the module software version after installation and initialization, an operator is required to run the ClientInfoUtility. On a command line, the operator will type:

```
/FIPSClientInfoUtility
```

The operator will be returned the following:

```
Client Version : 1.0

OS Version : RHEL8 (either this line or the following depending on O/S)
OS Version : Windows 2019 server

Run Time Environment : glibc v6 2.12
```

10.3 Approved Mode of Operation

The following steps are required to install, initialize, and place the module into FIPS approved mode of operation:

1. Download and copy the distribution file to the build system. For Linux OS, it is CADP_CAPI_8.12.1.000.tar and for MS-Windows OS, it is CADP_CAPI_windows_64b_v8.12.1.000.zip. These files can be downloaded from https://supportportal.thalesgroup.com/
2. Verify the HMAC-SHA-1 digest of the distribution file. An independently acquired FIPS 140-2 validated implementation of SHA-1 HMAC must be used for this digest verification. Note that this verification can be performed on any convenient system and not necessarily on the specific build or target system.
3. Unpack the distribution
4. On Linux:
    a. Navigate to the SafeNetProtectAppICAPI-8.10.0.000 directory
    b. Execute the `install.sh` command with installation directory as a command line parameter, as shown below:
        i. `./install.sh <ProtectApp_installation_directory>`
        where, `<ProtectApp_installation_directory>` is the SafeNet ProtectApp installation directory.
5. On Windows, double-click setup.exe file
6. After installation, the user should verify that the success messages described in the "Power-On Self-Tests" section have been produced to ensure that the module is operating in the Approved manner.

In addition to the above steps, please refer to the [CCP User Guide] that is provided to the customers for more information on installation and setup procedures.

Please refer to Section 10.6 where Security Rules must be continuously followed in order to operate the module in a FIPS Approved manner.

10.4 Module Status

Checking module status at any time can be performed by consulting the system logs.

10.5 Key Entry and Output

Guidance is not required since Section 6.2, Key Entry and Output Methods, indicates that no special key entry or output methods are required when the CM is operating in a FIPS approved mode of operation.

10.6 Security Rules

- In conformance with limitations on the maximum number of blocks encrypted for a given 168-bit Triple-DES key outlined in SP800-67r1, and further tightened in [FIPS 140-2 IG], A.13, 'SP 800-67rev1 transition', users are responsible for enforcing that any given Triple-DES key stored in the cryptographic module cannot be used for more than 2^{16} 64-bit data block encryption operations.
- The module does not technically enforce a limit on the number of times a Triple-DES key can be used.
- The operator of the module shall not use non-Approved algorithms listed in Table 2.5.