THALES

ProtectServer PCIe HSM 3

NON-PROPRIETARY SECURITY POLICY

FIPS 140-2, LEVEL 3

Document Information

Document Part Number	002-000301-001
Release Date	April 18, 2022

Revision History

Revision	Date	Reason
A	4th November, 2020	Final Release.
B	1st September, 2021	Updated for CMVP Coordination
C	23rd November, 2021	Small updates for CMVP Coordination
D	7th March, 2022	Added hardware part numbers 808-000048-003 and 808-000073-002.
E	18th, April 2022	Small typos in part numbers corrected

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

Acronym	Definition
AES	Advanced Encryption Standard
AK	Application Key
ANSI	American National Standards Institute
API	Application Programming Interface
ASO	Administration Security Officer
ATU	Administrator Token User
CA	Certificate Authority
CPU	Central Processing Unit
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DHEK	Diffie-Hellman Ephemeral Key
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
KDE	Key Data Encryption
KTC	Key Transport Certificate
KTK	Key Transport Key
LCD	Liquid Crystal Display

Acronym	Definition
LED	Light Emitting Diode
MAK	Message Authentication Key
MMK	Module Master Key
NIST	National Institute of Standards and Technology
NO	Normal Operator
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTK	ProtectServer Tool Kit
RAM	Random Access Memory
RNG	Random Number Generator
RoHS	Restriction on Hazardous Substances
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
RWXZ	Read, Write, Execute, Zeroize
SALK	Secure Audit Log Key
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SO	Security Officer
Triple-DES	Triple Data Encryption Standard
USB	Universal Serial Bus

PREFACE

This document deals only with operations and capabilities of the ProtectServer PCIe HSM 3 module in the technical terms of FIPS PUB 140-2, 'Security Requirements for Cryptographic Modules', 12-03-2002.

General information on Thales HSM alongside other 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 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProtectServer PCIe HSM 3. This security policy describes how the ProtectServer PCIe HSM 3 meets the security requirements of FIPS 140-2 and how to operate the module in a secure FIPS 140-2 mode. This policy was prepared as a part of the Level 3 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST web site at https://csrc.nist.gov/projects/cryptographic-module-validation-program

1.2 Scope

This document applies to hardware versions 808-000048-002, 808-000048-003, 808-000073-001 and 808-000073-002 with firmware version 7.00.01 and bootloader version 1.2.0 and where:

- 808-000048-002 and 808-000048-003 correspond to a module with fans on the outside of the metal enclosure factory installed;
- 808-000073-001 and 808-000073-002 correspond to a module with extra heatsinks installed (instead of fans as pictured);
- 808-000048-002 and 808-000048-003 are functionally equivalent with the difference being limited to the supply choice for one of the non-security enforcing internal components; and
- 808-000073-001 and 808-000073-002 are functionally equivalent with the difference being limited to the supply choice for one of the non-security enforcing internal components.

The security policies described in this document apply to the ProtectServer PCIe HSM 3 (referred to as the module) only and do not include any security policy that may be enforced by the host appliance, server, or smart card.

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy.

1.3 Validation Overview

The module meets all level 3 requirements for FIPS 140-2 as summarized in the table below:

Table 1-1: FIPS 140-2 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3

Security Requirements Section	Level
Roles and Services and Authentication	3
Finite State Machine Model	3
Physical Security	3 + EFP
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

1.4 Functional Overview

The ProtectServer PCIe HSM 3 is a multi-chip embedded hardware cryptographic module in the form of a PCI-Express card that provides a wide range of cryptographic functions using firmware and dedicated hardware processors. This document refers specifically to ProtectServer PCIe HSM 3 hardware versions 808-000048-002, 808-000048-003, 808-000073-001 and 808-000073-002 with Firmware Version 7.00.01 and Bootloader version 1.2.0

The module implements the Cryptoki cryptographic API as defined by RSA Data Security. While certain Cryptoki features are not supported, the module does provide a comprehensive compliance to the PKCS#11 standard as well as vendor-specific extensions.

2 Module Overview

2.1 Module Specification

The ProtectServer PCIe HSM 3 is a multi-chip embedded hardware cryptographic module in the form of a PCI-Express card that provides a wide range of cryptographic functions using firmware and dedicated hardware processors.

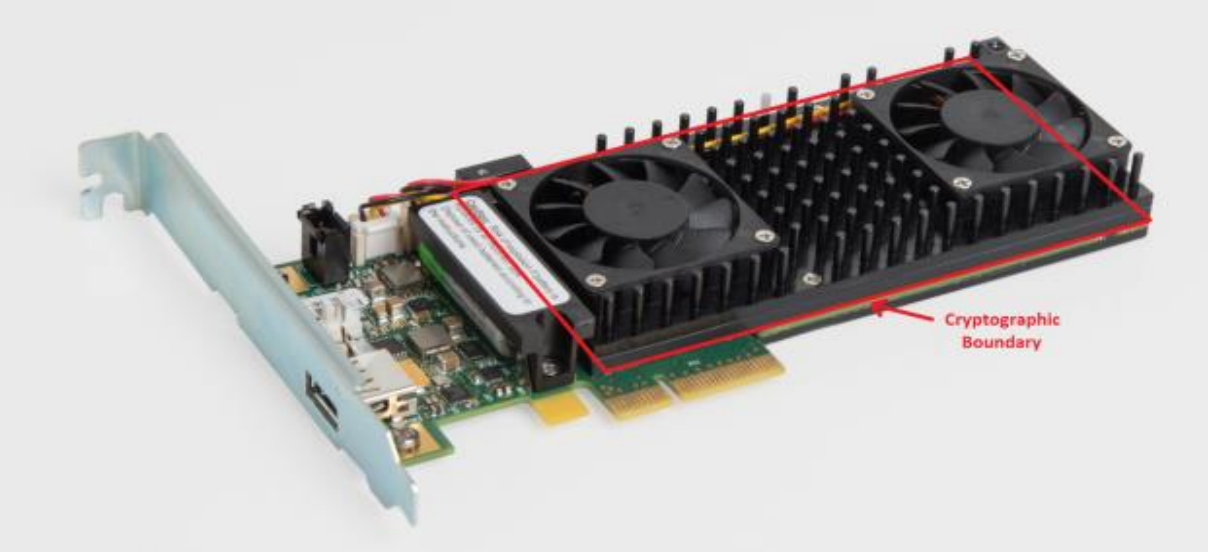

Figure 2-1: ProtectServer PCIe HSM 3 Card

The cryptographic boundary[1] of the module is shown above. The cryptographic boundary is defined as the metal enclosure on the top and bottom sides of the PCI-E card as outlined. The fans depicted alongside the removable backup battery are not included in the cryptographic boundary.

The module provides key management (e.g., generation, storage, deletion, and backup), an extensive suite of cryptographic mechanisms, and process management including separation between operators. The module also features non-volatile tamper protected memory for key storage, a hardware random number generator, and an RTC.

2.2 Ports and Interfaces

The module has the following physical interfaces:

- PCI-E interface
- USB port
- Serial port
- Power supply

[1] The fans depicted are not included in the physical boundary of the module. The 808-000073-001 and 808-000073-002 variants of the module do not include fans.

- Battery
- LED
- External event input
- Decommission input

The module provides a tightly secured cryptographic element. All requests for services sent to the adapter over the PCI bus or the serial ports are captured by the adapter's processor, which controls the level of access to the on-board cryptographic services and the keys. The adapter's processor also responds to PKCS #11 commands, ensuring that during FIPS operation only authenticated users receive cryptographic services.

The module's physical interfaces are separated into the logical interfaces, defined by FIPS 140-2, and described below:

FIPS 140-2 Interface	Physical Interface	Logical Interface
Data Input	PCI-E interface	Data I/O Cryptoki API Bootloader command protocol
	USB Serial Interface	Physical Trusted Path for PIN Pad[2] or SmartCard Reader[3]
Data Output	PCI-E interface	Data I/O Cryptoki API Logical Trusted Path Bootloader command protocol
	USB Serial Interface	Physical Trusted Path for SmartCard Reader[3]
Control Input	PCI-E interface	Data I/O Cryptoki API
	External event jumper	N/A
	Decommission jumper	N/A
	USB Serial Interface	N/A
Status Output	PCI-E interface	Data I/O Cryptoki API Logical Trusted Path Bootloader command protocol
	LED	N/A
	USB Serial Interface	N/A

[2] used for plaintext key component entry.
[3] used for backup and restore of user Asymmetric and Symmetric keys to SmartCard.

FIPS 140-2 Interface	Physical Interface	Logical Interface
Power	5V and 1.8V (generated from 12V power supply via PCI-E interface)	N/A
	3.6V battery	N/A

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

2.3 Roles and Services

2.3.1 Roles Summary

The following table lists the services related to each authorized role within the adapter:

Role	Services
Administrator SO	Initialize Administrator Token User PIN
Administrator	Manage Adapter and Administrator Token
Token SO	Manage Token
Token User	Use Token and manage token keys
Unauthenticated operator	Unauthenticated services
Audit User	Manage Audit Key

Table 2-2: Types of Available Services

The module supports identity-based authentication of its operator. Operators are identified by a token name and PIN. The different roles and required authentication are shown in Table 2-3.

FIPS 140-2 Role	ProtectServer PCIe HSM 3
Crypto Officer	Administrator SO
User	Administrator
Crypto Officer	Token SO
User	Token User
User	Audit User
Unauthenticated User	Unauthenticated Operator

Table 2-3: Mapping of FIPS 140-2 Roles to Module Roles

2.3.2 Administrator Security Officer

The primary role of the Administrator Security Officer (ASO) is to introduce the Administrator to the system. The ASO is able to set the initial Administrator PIN value but is not able to change the administration PIN after it is initialized. The ASO can perform the following services:

- Set the initial Administrator PIN value (may not change it later);
- Set the CKA_TRUSTED attribute on a Public object in the Administrator Token;
- Set the CKA_EXPORT attribute on a Public object in the Administrator Token;
- Exercise cryptographic services with Public objects
- Create, destroy, import, export, generate, and derive Public objects;
- May change the ASO PIN;
- May modify Monotonic Counter object; and
- Power-up self-test on demand.

2.3.3 Administrator

The Administrator is responsible for the overall security management of the adapter. Token Security Officers and Slots are controlled by the Administrator. The following services are available to the Administrator:

- Set or Change RTC value;
- Read the Hardware Event Log;
- Purge a full Hardware Event Log;
- Configure the Transport Mode feature;
- Specify the Security Policy of the adapter;
- Create new Cprov Slots/Tokens and specify their Labels, SO PINs, and minimum PIN Length;
- Initialize smart cards and specify their Labels and SO PINs;
- Destroy individual Cprov Slots/Tokens;
- Zeroize all adapter Secure Memory including all PINs and User Keys;
- Perform Firmware Upgrade Operation;
- Manage Host Interface Master Keys;
- Exercise cryptographic services with Public objects on Administrator Token;
- Exercise cryptographic services with Private objects on Administrator Token;
- Create, destroy, import, export, generate, and derive Public objects on Administrator Token;
- Create, destroy, import, export, generate, and derive Private objects on Administrator Token;
- May change his/her own PIN; and
- Power-up self-test on demand.

2.3.4 Token SO

The Token SO is responsible for granting and revoking ownership of the token. If the Token does not have a User PIN, the Token SO should initialize it by assigning the Label and User PIN. The token SO may also revoke the Token User's privileges (and possibly reassign the token to another operator) but only by destroying all the key material of the original operator first. The following services are available to the Token SO:

- Set the initial User PIN value (may not change it later)
- Reset (re-initialize) the Token (destroys all keys and User PIN on the Token) and set a new Label
- Set the CKA_TRUSTED attribute on a Public object in his or her Token
- Set the CKA_EXPORT attribute on a Public object in his or her Token
- Exercise cryptographic services with Public objects in his or her Token;
- Create, destroy, import, export, generate, and derive Public objects in his or her Token
- May change his/her own PIN;
- May modify Monotonic Counter object; and
- Power-up self-test on demand.

2.3.5 Token User

Token users may manage and use private and public keys on their own tokens. The following services are available to the Token User:

- Exercise cryptographic services with Public objects in his or her Token;
- Exercise cryptographic services with Private objects in his or her Token;
- Create, destroy, import, export, generate, derive Public objects in his or her Token;
- Create, destroy, import, export, generate, and derive Private objects in his or her Token;
- May change his/her own PIN; and
- Power-up self-test on demand.

2.3.6 Unauthenticated Operators

Certain services are available to operators who have not (yet) authenticated to the adapter:

- Exercise status querying (Show Status) services;
- Authenticate to a Token; and
- Force session terminate, restart adapter by setting a register which is memory mapped to the PCI bus. The host application can force a restart by writing a certain value to the register through the module's device driver. The transparent PCI chip will then generate a bus cycle restart, which in turn will restart the adapter.

All of the services available to the Unauthenticated Operators are also available to all authenticated operators.

2.3.7 Audit User

The Audit User role is present on the Admin Token and can be initialized by the Admin SO role. The responsibility of this role is limited to:

- Create/Destroy AUDIT_KEY

2.3.8 CSP Access by Role

The following table summarises CSP access by role where:

- W – indicates a used can write a given CSP;
- R – indicates a user can read a given CSP;
- X – indicates a user can perform operations with a given CSP; and
- Z – indicates a user can zeroize a CSP.

	FW Upgrade Cert	Default Administrator Token SO PIN	DH / ECDH Ephemeral Keys	Key Agreement Keys	Message Authentication Key	Operating PINs	Token Keys (Public)	Token Keys (Private)	DRBG	Module Master Key	Audit Keys
Initialization	-	-	-	X	-	WX	-	-	XW	W	-
Administrator SO	WX	WX	-	WXZ	-	WXZ	RWXZ	-	XW	RWXZ	-
Administrator	-	-	WZ	X	WZ	WXZ	RWXZ	RWXZ	XW	RWXZ	-
Token SO	-	-	RXZ	X	RXZ	X	RWXZ	-	XW	-	-
Token User	-	-	RXZ	X	RXZ	X	RWXZ	RWXZ	XW	-	-
Audit User	-	-	-	-	-	-	-	-	XW	-	RWXZ
Unauthenticated Operators	-	-	-	-	-	X	-	-	-	-	-

Table 2-4 Access to Keys for Authorized Services

2.4 Authentication

All roles except for the Unauthenticated Operator must authenticate to the module by providing their authentication data. The tables below explain the type and strength of the authentication data supported for each role.

All roles must authenticate using a password. When a role is initialized under this configuration, the operator enters the initial password for the role.

The module supports three types of Tokens: one Administration Token, multiple Cprov Tokens and one or more Smart Card Tokens. All Tokens have two operators: a Security Officer (SO) and a User. For the Administration Token, the Administrator SO is the FIPS 140-2 Crypto Officer and the Administrator is the User. For all other Tokens, the Token SO is the FIPS 140-2 Crypto Officer and the Token User is the User.

The operator explicitly selects a role when logging in by selecting a PKCS#11 Token and nominating either User or SO Role. The adapter provides restricted services to an operator based on the role to which the operator authenticated. There is only one operator assigned to each role. The Administrator SO and Token SO perform FIPS 140-2 Crypto Officer roles while the Administrator and Token User performs a FIPS 140-2 User role.

The module enforces a minimum PIN length of 4 characters and a maximum PIN length of 32 characters. The module allows the PIN character to be any value but the software typically used with the module restricts the dictionary to the ANSI C character set. This character set provides for 92 visible characters which, with a 4 character PIN, provides a probability of less than one in 1,000,000 that a random PIN attempt (e.g., guess) will succeed (actual probability is approximately 1/71,600,000). The module is protected from brute force PIN attacks by imposing an increasing delay for every failed PIN attempt after the first three failed attempts. The initial delay is 5 seconds and increases by an additional 5 seconds for each subsequent failed attempt, e.g., 3 fails causes a 5 second delay; 4 fails causes a 10 second delay; 5 fails causes a 15 second delay; etc.

ProtectServer PCIe HSM 3	Type of authentication	Authentication Data
Administrator SO	Identity Based	Operator Unique PIN
Administrator	Identity Based	Operator Unique PIN
Token SO	Identity Based	Operator Unique PIN
Token User	Identity Based	Operator Unique PIN
Audit User	Identity Based	Operator Unique PIN
Unauthenticated Operator	Not Required	N/A

Table 2-5: Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Operator Unique PIN	The module enforces a minimum PIN length of 4 characters and a maximum PIN length of 32 characters. The module allows the PIN character to be any value but the software typically used

Authentication Mechanism	Strength of Mechanism
	with the module restricts the dictionary to the ANSI C character set. This character set provides for 92 visible characters which, with a 4 character PIN, provides a probability of less than one in 1,000,000 that a random PIN attempt (e.g., guess) will succeed (actual probability is approximately 1/71,600,000). The module is protected from brute force PIN attacks by imposing an increasing delay for every failed PIN attempt after the first three failed attempts. The initial delay is 5 seconds and increases by an additional 5 seconds for each subsequent failed attempt, e.g., 3 fails causes a 5 second delay; 4 fails causes a 10 second delay; 5 fails causes a 15 second delay; etc. Thus AS03.26 is also met.

Table 2-6: Strengths of Authentication Mechanisms

2.5 Physical Security

The module is a multi-chip embedded module as defined by FIPS PUB 140-2, section 4.5. The module is encased in a strong metal enclosure that provides tamper-evidence. Any tampering that might compromise a module's security is detectable by visual inspection of the physical integrity of a module. The HSM SO should perform a visual inspection of the module at regular intervals.

Within the metal enclosure, a hard opaque epoxy covers the circuitry of the module. Attempts to remove this epoxy will cause sufficient damage to the module so that it is rendered inoperable. Module hardness integrity has been verified between 0ºC and 80ºC.

The module's enclosure is opaque to resist visual inspection of the device design, physical probing of the device and attempts to access sensitive data on individual components of the device.

2.5.1 External Event

The module supports a physical interface for the input of an external event signal. The external event signal jumper is monitored in both the powered-on state and the powered-off state.

In the event of an external event signal, the module will erase the Module Master Key, reset itself, clear all working memory and log the event. The module can be reset and placed back into operation when the external event signal is removed.

2.5.2 PCI-E Card Removal

The module detects removal from the PCI-E slot in both the powered-on state and the powered-off state. If the card is removed from the PCI-E slot, the Module Master Key is erased and the event is logged.

2.5.3 Environmental Failure Protection

The module is designed to sense and respond to out-of-range temperature conditions as well as out-of-range voltage conditions. The temperature and voltage conditions are monitored in both the powered-on state and the powered-off state.

In the event that the module senses an out-of-range temperature the module will erase all plaintext CSPs in the HSE-BBRAM (Module Master Key), reset itself, clear all working memory and log the event.

Out-of-range voltage conditions are treated as a power cycle. In the event that the module senses an out-of-range voltage, the module will halt, need to be reset and all working memory cleared.

2.5.4 Decommission

The module supports a physical interface for the input of a decommission signal. The decommission signal jumper is monitored in both the powered-on state and the powered-off state.

In the event of a decommission signal, the module will erase the MMK, reset itself, clear all working memory and log the event.

This provides the capability to prevent access to sensitive objects in the event that the module has become unresponsive or has lost access to primary power.

The module can be reset, re-initialized and placed back into operation when the decommission signal is removed.

2.5.5 Fault Tolerance

If power is lost to a module for any reason, the module shall, at a minimum, maintain itself in a state that it can be placed back into operation when power is restored without compromise of its functionality or permanently stored data.

A module shall maintain its secure state[4] in the event of data input / output failures. When data input / output capability is restored the module will resume operation in the state it was prior to the input / output failure.

2.6 Operational Environment

The module uses a non-modifiable operational environment. The requirements for a modifiable operating environment do not apply.

2.7 Cryptographic Key Management

The module is a general-purpose cryptographic management device and thus securely administers both cryptographic keys and other critical security parameters (CSPs) such as passwords.

2.7.1 FIPS-Approved and Allowed Algorithm Implementations

The FIPS-Approved algorithms implemented by the module are listed in the table below:

[4] A secure state is one in which either the cryptographic module is operational and its security policy enforcement is functioning correctly, or it is not operational and all sensitive material is stored in a cryptographically protected form.

Table 2-7: FIPS-Approved Algorithm Implementation

Approved Security Functions	Certificate No.
Symmetric Encryption/Decryption	
AES: CBC, CCM, ECB, GCM[5], KW, KWP, OFB (128, 192, 256-bits)	C2089
Triple DES (3-key): CBC, ECB, KW,OFB	C2089
Hashing	
SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	C2089
SHA-3: SHA3-224, SHA3-256, SHA3-384, SHA3-512 (Byte Only)	C2089
SHS: SHA-512 (Byte Only)	C1945
Message Authentication Code	
HMAC: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	A678, C2089
AES: CMAC (128, 192, 256-bits).	C2089
AES: GMAC (128, 192, 256-bits).	C2089
Asymmetric	
RSA: Key Generation FIPS 186-4 (2048 and 3072 modulus), Signature Generation FIPS 186-4 (2048, 3072 modulus), Signature Verification FIPS 186-4 (2048, 3072, 4096 modulus), Signature Verification FIPS 186-2 (4096 modulus), Signature Primitive, Decryption Primitive Signature Type: PKCS 1.5, PKCSPSS.	C2089
RSA: Signature Generation FIPS 186-4 (4096 modulus), Signature Verification FIPS 186-4 (4096 modulus), Key Generation FIPS 186-4 (4096 modulus)	A678

[5] The module generates IVs internally using the Approved DRBG. All IVs used by the module are 128-bits in length.

Approved Security Functions	Certificate No.
DSA: Parameter Generation (2048 and 3072 modulus), Key Generation (2048 and 3072 modulus), Signature Generation (2048 and 3072 modulus), Signature Verification (2048 and 3072 modulus)	C2089
ECDSA: Key Generation, Signature Generation, Signature Generation Component (CVL), Curves: P-224, P-256, P-384, P-521. Signature Verification Curves: P-192, P-224, P-256, P-384, P-521.	C2089
ECDSA: Signature Verification (P-521).	C1945
Key Agreement Scheme	
KAS (KAS-SSC Cert. #A678, KDA Cert. #A678); ECC: Ephemeral Unified, OnePassDH. Supported curves: P-224, P-256, P-384, P-521. FFC: dhOneFlow	A678 A678
KAS-KDF OneStep Auxiliary Functions: SHA-2-224, SHA2-256, SHA-2-384, SHA-2-512.	A678
Key Derivation Function	
KDF ANSI X9.42 KDF Type: Concatenation Supported Hash: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	A678
Key Transport	
KTS (AES Cert. #C2098; key establishment methodology provides between 128 and 256 bits of encryption strength) 128, 192, 256-bits.	C2098
KTS (Triple-DES Cert. #C2098; key establishment methodology provides 112 bits of encryption strength) 168-bits.	C2098

Approved Security Functions	Certificate No.
KTS-RSA (key establishment methodology provides between 112 and 150 bits of encryption strength) Modulus Length – 2048, 3072, 4096, Hash – SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512. Mask Generation Function (MGF) – SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512.	A678
Random Number Generation	
Counter DRBG Mode: AES 256.	C2089
CKG[6]	Vendor affirmed, using IG D.12

Table 2-8: Allowed Security Function for the Firmware Implementation

Allowed Security Functions
Key Transport
AES (key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength) (based on AES Cert. #C2089 and using allowances in FIPS IG D.9)
Triple-DES (key unwrapping; key establishment methodology provides 112 bits of encryption strength) (based on Certificate No. #C2089 and using allowances in FIPS IG D.9)
RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)[7]
Random Number Generation
NDRNG

2.7.2 Non-Approved Algorithm Implementations

Non-FIPS Approved security functions are not available for use when the module has been configured to operate in FIPS-approved mode.

> **Symmetric Encryption/Decryption**

- DES
- Triple-DES (non-compliant for encryption using 112 bit keys)

[6] Symmetric keys and seeds used for asymmetric key generation are an unmodified output from the approved DRBG (Cert. #C2089)

[7] Only permitted for use under FIPS IG D.9 and not permitted for use after December 31, 2023. RSA encryption/decryption using PKCS#1-v1.5 padding is available for use with C_WrapKey and C_UnwrapKey Cryptoki Commands.

- RC2
- RC4
- CAST5
- SEED
- ARIA

> **Hashing**

- MD2
- MD5
- KECCAK

> **Message Authentication Code**

- AES MAC
- DES-MAC
- RC2-MAC
- CAST5-MAC
- SEED-MAC
- ARIA-MAC
- SSL3-MD5-MAC
- SSL3-SHA1-MAC
- HMAC (non-compliant for any configuration providing less than 112 bits of encryption strength)
- TUAK
- MILENAGE

> **Asymmetric**

- RSA X-509
- RSA (non-compliant with less than 112 bits of encryption strength)
- DSA (non-compliant with less than 112 bits of encryption strength)
- ECDSA (non-compliant with less than 112 bits of encryption strength)
- EdDSA

> **Key Generation**

- DES
- RC2
- RC4
- CAST5
- SEED

- ARIA
- SSL PRE-MASTER
- BIP32

> **Key Agreement**

- ECC (non-compliant with less than 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology; non-compliant with less than 112 bits of encryption strength)

> **Key Transport**

- RSA (key wrapping; key establishment methodology; non-compliant with less than 112 bits of encryption strength)

2.8 Critical Security Parameters

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

Table 2-9: Summary of CSPs

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Firmware upgrade Public Key	ECDSA P-521	External, N/A	Input with Firmware Update Image which is considered plaintext.	To verify the signature attached to a new firmware image. Generation done at manufacture.
Default Administrator Token SO PIN	PIN	N/A	Not input/output.	For initial authentication to the module. Replaced after the module is initialized.
ECDH Key Agreement Keys	ECC P-521	FIPS 186-4, Appendix B.4.1	Public key exported as part of key agreement.	To establish an encrypted channel between an operator and the module.
Message Encryption Shared Secret Key	AES GCM	Established via C(2e, 0s, ECC CDH) compliant with SP 800-56Ar3 and KDA SP 800-56Cr2 One-Step KDF using SHA-512	Not input/output.	Protects data between an operator and the module. AES GCM is used to protect the secure channel. Established using ECDH and the Secure Messaging Keys and Secure Messaging Certificate.
Message Authentication Key (MAK)	HMAC-SHA-512	Established via C(2e, 0s, ECC CDH) compliant with SP 800-56Ar3 and KDA SP 800-56Cr2 One-Step KDF using SHA-512	Not Input/Output.	Provides data authentication of encrypted data between an operator and the module. Established using ECDH and the Secure Messaging Keys and Secure Messaging Certificate.
Operating PINs	PIN	N/A	Input encrypted[8]	All users' PINs – Administrator Token SO, Administrator Token User, Token SOs, and Token users used to authenticate to the module.
Module Master Key	AES 256-bit key	FIPS Approved DRBG	Not input/output.	Encrypts other keys and zerorizes contents of secure memory on object deletion.

[8] PINs encrypted using Triple-DES

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Symmetric Keys (general partition or session keys)	AES or Triple-DES , MAC	N/A (user imported) or AES-CTR DRBG (module generated).	Input or output encrypted using Symmetric Keys (general partition or session keys) using key C_WrapKey and C_UnwrapKey Cryptoki commands and SP 800-38F encryption options. Input or output encrypted using Asymmetric Keys (general partition or session keys) using key C_WrapKey and C_UnwrapKey Cryptoki commands and KTS-OAEP-basic from SP 800-56Br2. Input using Symmetric Keys (general partition or session keys) using key C_WrapKey and C_UnwrapKey Cryptoki commands and approved symmetric algorithms as permitted by FIPS IG D.9.	General use asymmetric key pairs that can be exported/imported from/to the module or generated by the module.
Asymmetric Key Pairs (general partition or session keys)	RSA, DSA, ECC, DH	N/A (user imported) or generated using either FIPS 186-4, Appendix B.3.3 or B.4.1 and using the output from AES-CTR DRBG (module generated) for entropy.	<Methods as per – 'Symmetric Keys (general partition or session keys)' above.>	General use asymmetric key pairs that can be exported/imported from/to the module or generated by the module.
DRBG Key	AES-256	Derived via SP 800-90Ar1 mechanisms	Not Input or Output.	32 bytes AES key stored in the RAM. Used in an implementation of the NIST SP 800-90Ar1 CTR (AES) DRBG.
DRBG Seed	384 bits	Derived via SP 800-90Ar1 mechanisms	Not Input or Output.	Random seed data drawn from the Hardware RBG and used to seed an implementation of the NIST SP 800-90Ar1 CTR (AES) DRBG.
DRBG V	128 bits	Derived via SP 800-90Ar1 mechanisms	Not Input or Output.	Part of the secret state of the approved DRBG. The value is generated using the methods described in NIST SP 800-90Ar1.
DRBG Entropy Input	384 bits	NDRNG	Not Input or Output.	The 384-bit entropy value used to initialize the approved DRBG.
Secure Audit Logging Key (SALK)	HMAC-SHA-256	FIPS approved DRBG	Encrypted with MMK	A key used to verify integrity and authentication of log messages.
PTK Identity Key	ECDSA P-521	FIPS 186-4, Appendix B.4.1	Not Input or Output	Generated as part of initialization of the HSM.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
PTK Identity Certificate	ECDSA P-521	FIPS 186-4, Appendix B.4.1	Output in plaintext over the PCI-E interface in plaintext (during initialization) or client-to-HSM secure tunnel (once in FIPS mode) as a certificate as part of initializing the HSM.	Used by another HSM or client to identify the HSM as the target or source for the encrypted channel between the client-and-HSM. Separately used to authenticate target HSM when exchanging keys using replication to transfer keys between modules.
Secure Messaging Key (SMK)	ECDSA P-521	FIPS 186-4, Appendix B.4.1	Not Input or Output	Generated as part of initialization of the HSM. Used during the setup of the client-to-HSM secure channel.
Secure Messaging Certificate (SMC)	ECDSA P-521	FIPS 186-4, Appendix B.4.1	Output in plaintext over the PCI-E interface in plaintext (during initialization) or client-to-HSM secure tunnel (once in FIPS mode) as a certificate as part of initializing the HSM.	Used by another HSM or client to identify the HSM as the target or source for the encrypted channel between the client-and-HSM.
Replication Key Transport Key (KTK)	ECC P-521	FIPS 186-4, Appendix B.4.1	Not Input / Output	Ephemeral private key used by the replication protocol. Key is used alongside its corresponding public key during the replication protocol with ECDH to derive the Replication KDE and Replication MACKey.
Replication Key Transport Certificate (KTC)	ECC P-521	FIPS 186-4, Appendix B.4.1	Output in plaintext over the Client-to-HSM Secure tunnel during replication protocol.	Ephemeral public key packaged as a certificated used by the Replication protocol and where this certificate is signed by the PTK Identity Certificate.
Replication Key Data Encryption (KDE)	AES-256	Established via C(2e, 0s, ECC CDH) compliant with SP 800-56Ar3 and KDA SP 800-56Cr2 One-Step KDF using SHA-512	Not Input / Output	Used to GCM encrypt (SP800-38F) token key objects in transit between modules.
Replication MACKey (MACKey)	256-bits	Established via C(2e, 0s, ECC CDH) compliant with SP 800-56Ar3 and KDA SP 800-56Cr2 One-Step KDF using SHA-512	Not Input / Output	Used with HMAC-SHA-512 as part the replication protocol to generate MAC.

2.9 Key Generation

Symmetric cryptographic keys are generated by the direct unmodified output of the module's NIST SP 800-90A DRBG. The DRBG output is also used as a seed for asymmetric key generation.

Operator PINs for authentication of roles are generated by the operator.

The NIST SP 800-90Ar1 DRBG (CTR-DRBG using AES256) is seeded using 2048 bits or raw entropy taken from the module NDRNG which is conditioned using SHA-512 ahead of creating the 384 bit seed. Based on calculated min-entropy values for the platform raw noise source and factors outlined in NIST SP 800-90B, the 384-bit input used to seed to the DRBG has a full 384 bits of entropy.

2.10 Key Import and Export

Import and Export of CSP is supported over the following interface:

- Cryptoki API, Logical Interface over PCI-E;
- Physical Trusted Path to Smartcard Reader over USB; or
- Physical Trusted Path to PIN pad over USB (key component entry only).

For details of specific mapping of CSP to interfaces and associated methods of encryption of specific CSP refer to the input/output column of Table 2-9.

The following methods of key import and export for 'Asymmetric Key Pairs (general partition or session keys)' and 'Symmetric Keys (general partition or session keys)' are available as a service:

> **Key Wrap / Unwrap**

> The key wrap operation is available for use to import or export raw Symmetric Keys (general partition or session keys) or an Asymmetric Key Pair (general partition or session keys) – private key, using one of the following options which must be specified in the request sent to the module. The module will reject non-Approved Key Wrap / Unwrap operations:

- KTS-OAEP-basic from SP800-56Br2 and where the following options are supported:
    - Modulus lengths of 2048, 3072 or 4096.
    - Hash and MGF options must match and be consistent with one of the following algorithms: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512.
- RSA Key Transport using PKCS#1v1.5 and where the following options are supported:
    - Modulus lengths of 2048, 3072 or 4096.
- SP800-38F compliant KTS using one of the following options for both key unwrapping and wrapping:
    - AES (128, 192 or 256) in KW, KWP;
    - Triple-DES (168 bit) in KW.
- FIPS IG D.9 Allowed Legacy KTS for unwrap of key objects using one of the following options:
    - AES (128, 192 or 256) in CBC or ECB modes; or
    - Triple-DES (112 and 168 bit) in CBC and ECB.

The unwrap operation takes as input an encrypted symmetric key or asymmetric private key and a handle to the key required to successfully unwrap the object. It decrypts the key and returns the handle to the imported key.

> **Key Backup and Restore to SmartCard**

Keys can be backed up and restored to a SmartCard using the following methods:

- Keys are wrapped using SP800-38F compliant AES-KWP under an AES-256 wrapping key created by the user. The encrypted key packages only are exported to SmartCard for backup and subsequent restore.
- The wrapping key is split using Shamir's (M-of-N) threshold scheme into 'M' shares selected but the user and where 'N' of the shares are required to recover the wrapping key in order to enable restore.
- The smart card reader (i.e. HID OMNIKEY 3121 reader) is connected to the USB port, and after visually inspecting the USB port and surrounding circuitry for tamper (see Section 2.5) and connecting the Administrator will execute "ctconf –q" to detect and establish communication parameters. This step will need the device Administrator's PIN. The reader uses standard PC/SC interface.
- The smart card backup/restore utilizes secure channel between the firmware and smart cards.

> **Key Import using PIN PAD and Key Components**

Keys components can be entered using a directly connected PIN pad to the Physical Trusted Path over USB.

- Once entered, key components are recombined using XOR and used to create a 'Symmetric Keys (general partition or session keys)'.
- The PIN PAD (Verifone VX805 PINPAD (https://www.verifone.com/en/us/devices/countertops-pin-pads/vx-805)) is connected to the USB port, and after visually inspecting the USB port and surrounding circuitry for tamper (see Section 2.5) and connecting the Administrator will execute "ctconf –q" to detect and establish communication parameters. This step will need the device Administrator's PIN. The PIN PAD uses the serial communication protocol.
- The PIN PAD key component entry is in plaintext.

> **Key Import and Export using Replication**

Keys can be transferred between separate instances of the cryptographic module using the Replication Protocol.

The replication protocol operates in the following way:

- Source and destination module exchange Replication KTC via the client over the client-to-HSM secure channel.
- Source and destination module use C(2e, 0s, ECC CDH) compliant with SP 800-56Ar3 and KDA SP 800-56Cr2 One-Step KDF using SHA-512 to derive an AES-256 key (KDE) alongside a separate 256 bit key used for MAC (MACKey).
- Keys transferred between modules are encrypted using AES-GCM in compliance with SP800-38F.

2.11 Limits on use of Triple-DES

In conformance with limitations on the maximum number of blocks encrypted for a given 168-bit Triple-DES key outlined in SP 800-67r2 and further tightened in FIPS IG A.13 – the module technically enforces that any given Triple-DES key stored in the module cannot be used for more than 2^{16} 64-bit data block encryption operations.

Triple-DES keys created on the HSM (imported or generated) include a 'remaining blocks' attribute that is managed by the HSM and decremented following each encrypt operation requested. Once the 'remaining blocks' count reaches zero, the key is permitted for use with decrypt and MAC verify operations exclusively. The key is prohibited from being copied and exported. The counter is managed by the HSM and cannot be reset to a non-zero value.

2.12 Self Tests

2.12.1 Power-On Self Tests

The module performs Power-On Self Tests (POST) upon power-up to confirm the firmware integrity, and to check the continued correct operation of the random number generator and each of the implemented cryptographic algorithms. While the module is running POST, all interfaces are disabled until the successful completion of the self tests. If any POST fails an error message is output, the module halts, and data output is inhibited.

These self tests can also be initiated as an operator service but do not require operator input to initiate at power on.

Table 2-10: Power On Self Tests (Bootloader) – Module Integrity

Test	When Performed	Indicator
Boot loader performs an ECDSA P-521 w/ SHA-512 signature verification of itself	Power-on	Error output and module halt
Boot loader performs an ECDSA P-521 w/ SHA-512 signature verification of the firmware prior to firmware start	Power-on/Request[9]	Error output and module halt
SHA-512 and ECDSA KAT.	Power-on/Request[10]	Error output and module halt

Table 2-11: Power On Self Tests (Firmware) – Cryptographic Implementations

Test	When Performed	Indicator
DRBG Self Test (Instantiate Function Known Answer Test, Generate Function KAT, Reseed Function KAT, conditional tests)	Power-on/once every 24 hours.	Error output and module halt
SHS KAT (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512)	Power-on/Request	Error output and module halt

[9] Request indicates triggering a POST via a command
[10] Request indicates triggering a POST via a command

Test	When Performed	Indicator
HMAC KAT (HMAC-SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512)	Power-on/Request	Error output and module halt
RSA KAT (Signature Generation, Sig Verification, Encryption, Decryption)	Power-on/Request	Error output and module halt
DSA KAT (Signature Generation, Sig Verification)	Power-on/Request	Error output and module halt
Diffie-Hellman KAT (Shared Secret Computation, X9.42 DH Derive)	Power-on/Request	Error output and module halt
AES KAT (ECB, CBC, OFB, KW, KWP, GCM, modes covering 128, 192 and 256 bit keys, CMAC and GMAC). (encrypt/decrypt)	Power-on/Request	Error output and module halt.
Triple-DES KAT (ECB, CBC, OFB, KW). (encrypt/decrypt)	Power-on/Request	Error output and module halt.
ECDH KAT (Shared Secret Computation and Derive)	Power-on/Request	Error output and module halt
ECDSA KAT (Signature Generation, Sig Verification)	Power-on/Request	Error output and module halt.

2.12.2 Conditional Self Tests

The module automatically performs conditional self tests based on the module operation. These self tests do not require operator input to initiate.

Table 2-12: Conditional Self Tests

Test	When Performed	Where Performed	Indicator
NDRNG conditional tests (repetition count test and adaptive proportion test)	Continuous	Firmware / Hardware	Error output and module halt
Noise source conditional tests (repetition count test and adaptive proportion test)	Continuous	Firmware / Hardware	Error output and module halt
RSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output and module halt
DSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output and module halt
ECDSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output and module halt

Firmware load test (ECDSA P-521 sig ver)	On firmware update load	Firmware	Error output – module will continue with existing firmware
SP 800-56Ar3 Conditional Test Assurances for Key Validation	On use	Firmware	Error output and module halt

2.12.3 Mitigation of Other Attacks

Timing attacks are mitigated directly by a module through the use of hardware accelerator chips for modular exponentiation operations. The use of constant timing hardware acceleration ensures that all RSA signature operations complete in the same time, therefore making the analysis of timing differences irrelevant.

3 Guidance

3.1 Firmware Management

This Security Policy describes a particular module firmware and hardware. The firmware can be replaced (with a firmware upgrade operation) or extended (by loading Functionality Modules [FMs]). Operators can load their own trusted code into the module. However, by doing so, the module is no longer FIPS validated unless the FM has been separately FIPS validated.

The module checks that new firmware is digitally signed before it can be loaded. Following a successful verification all keys and CSPs will be zeroized. After the zeroization, the module will automatically transition to a non-FIPS mode and will require reconfiguration to return to FIPS mode. Only firmware versions listed in this Security Policy are FIPS validated.

3.2 Invoking Approved Mode of Operation

To place the module in FIPS Approved Mode of Operation, run the `CTCONF -fF` command from the remote management facility. Once this command is executed the module will reject all requests for non-FIPS algorithms or configurations. Please note that the operator has to be logged in as an Administrator to invoke the FIPS mode of operation.

To verify the Approved mode status, run the `CTCONF -v` command to display the status. Running this command from a remote management facility will return a status displaying the current operating mode.

```
Security Mode: FIPS 140-2 Mode: <list of flags indicating attributes set for FIPS>
```