MARVELL

Marvell Semiconductor, Inc.

Marvell LS2 HSM Family

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.2
Date: 19 Aug 2026

MARVELL

Table of Contents

List of Tables

List of Figures

1 – General

1.1 Overview

The Marvel LS2 HSM Family module (hereafter referred to as the module or HSM) by Marvell is a high-performance purpose-built security solution for key management and crypto acceleration. The module provides a FIPS 140-3 overall Level 3 security solution. The module is deployed in a PCIe slot to provide crypto and protocol acceleration in a secure manner to the system host. It is typically deployed in a server or an appliance to provide crypto offload for the keys stored on the HSM. The module's functions are accessed over the PCIe interface via opcode defined by the module.

The HSM is a hardware multi-chip embedded cryptographic module with firmware programmed on the HSM. The module provides cryptographic primitives to accelerate approved, allowed and non-approved algorithms to support use cases including PKI, code signing, document signing, Root Of Trust, and TLS. The cryptographic functionality includes asymmetric (RSA/EC) and symmetric (AES and Triple-DES) ciphers, signatures, and random number generation, along with protocol-specific complex instructions to support TLS 1.2.

The module implements password-based single factor authentication at FIPS 140-3 Level 3 security and an optional public-key-based authentication. The physical boundary of the module is the outer perimeter of the PCIe card itself as depicted in section 2.1.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows:

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	3

Table 1: Security Levels

2 – Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Marvell LS2 HSM module is a multi-chip PCIe adapter with firmware. It consists of multiple components, including an operating system, applications exposing services and interfaces related to secure key management, crypto operations, and policy management of the module. Important hardware components of the module are: general purpose, ARM-based control processor, ARM-based microcontroller, RAM memory, NOR and eMMC flash for persistent storage, USB interfaces, and RJ45 and PCIe gen-4 x8 with SMBus interfaces.

- Partitions
  The LS2 HSM adapter is an SR-IOV enabled intelligent PCIe adapter with one physical function and 64 virtual functions. The physical device is referred to as Physical Function (PF) while the virtual devices are referred to as Virtual Functions (VF). Allocation of the VF can be dynamically controlled by the PF via registers encapsulated in the capability. Each VF's PCI configuration space can be accessed by its own Bus, Device and Function Number (Routing ID). And each VF also has PCI Memory Space, which is used to map its register set. VF device driver operates on the register set so it can be functional and appear as a real existing PCI device.

  In addition to crypto offloads, this adapter can provide secure key storage with up to 42 logical partitions, including a master partition. Each partition will have dedicated resources that are logically and securely isolated from other partitions. A partition will have its own specific policies and controls, and its own user accounts to manage what can be done with a partition and by a user of a partition. Consequently, each partition is treated as a virtual HSM and referred as a pHSM (or HSM Partition).

  An LS2 HSM always has one default partition called the master partition, which exposes the interfaces to create, delete, and update the remaining partitions. LS2 HSM can either be in host virtualization mode or non-virtualization mode. One or more applications on a host/virtual machine/container can make use of different partitions available on the HSM. Each partition will have dedicated communication channels; these channels are linked to the PCIe devices.

  In virtualization mode, channels will be linked to PCIe VFs, otherwise linked to PCIe PF. Communication channels have basic checks to identify that an application is communicating with an intended partition on the HSM. HSM FW provides the following mechanisms to ensure only an authorized user or application of a specific partition can communicate with it. It is optional to use either mechanism based on the deployment scenarios and risk assessment.

- Basic Channel
  These channels depend on the Host OS security for device binding and application isolation. In this case, HSM does basic session validation.

  - To run any authorized operation on an HSM partition, a user needs to login, get a random session handle, and use the session handle in all future communications to bind the authorization information.
  - Security critical operations (user management, key management, backup/restore, etc.) are all protected by encryption using keys that are (optionally derived from) set up during key ceremony.

- Encrypted Communication Channels
  The end-to-end encryption feature in the module allows an application to initiate a TLS connection with the firmware to ensure the confidentiality of the data communicated to the HSM. The connection is based on TLS v1.2 with the cipher-suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(known to OpenSSL as ECDHE_RSA_AES128-GCM-SHA256 and ECDHE_RSA_AES256-GCM-SHA384). The module will act as server, and the host application will act as client. The server private key will be the partition private key (PAK), which is generated for each pHSM when it is created. The server certificate used for the SSL connection is the partition certificate (PAC). The complete chain will be validated by host applications before establishing the TLS connection. The end-to-end encryption feature is enabled using the initialization configuration parameters. Once this feature is enabled, all commands except initialize and open session are encrypted.

- HSM Master Partition
  This is the default partition with only one user, called the Master Crypto Officer (MCO). This partition will expose authorized services to manage (create, delete, update, backup/restore) other partitions and set policies or conditions for them to operate. Additionally, it exposes anonymous services like fetching module information, etc. Refer to section 4.3 Roles, Services, and CSP Access for details about the services supported by the master partition. The master partition must be initialized and the MCO logged in to execute any authorized service.

- HSM Partition
  Each partition will have a different set of users to manage it and a dedicated key storage and crypto resources associated with it. A partition will have default configuration or policies supplied by the master partition. Some policies can be changed by the partition administrator or PCO. When a partition is created by the MCO, it will be in a zeroized state and must be initialized to do any key management or crypto operations. Partition initialization will create the Partition Crypto Officer (PCO). The PCO can later create up to 1024 users (PCO or PCU) on demand. Each user will have a unique username to identify themselves. The user has to log in to the partition/vHSM to issue any authorized commands. Users are authenticated using passwords submitted during the user creation.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

The following images depict the module's cryptographic boundary depicted in the dashed line. NOTE: Components outside the cryptographic boundary are not part of the evaluation can be and will need to be evaluated separately.

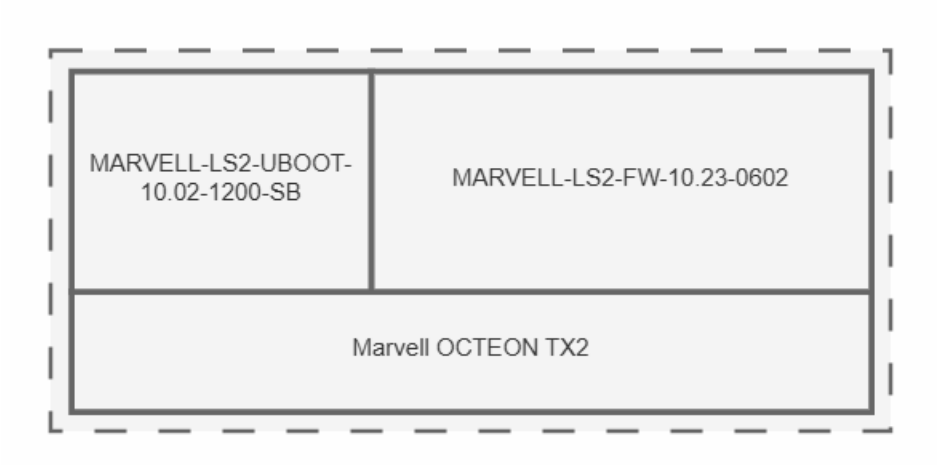

Figure 1: HSM Cryptographic boundary

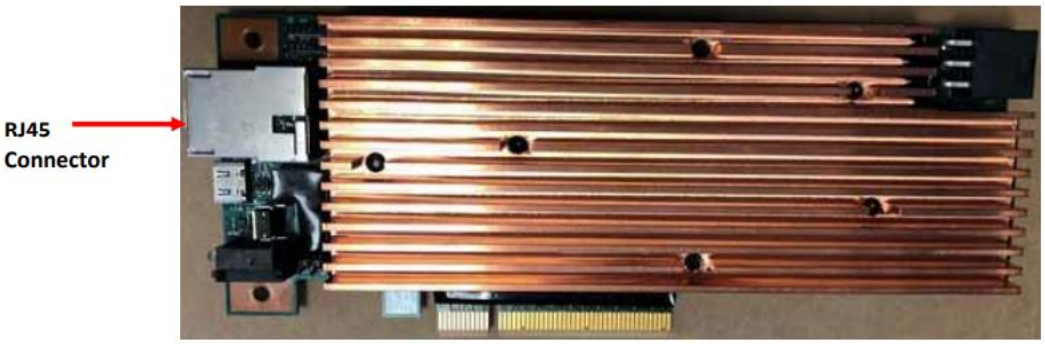

Figure 2: Module Side 1

Figure 3: Module Side 2 with epoxy

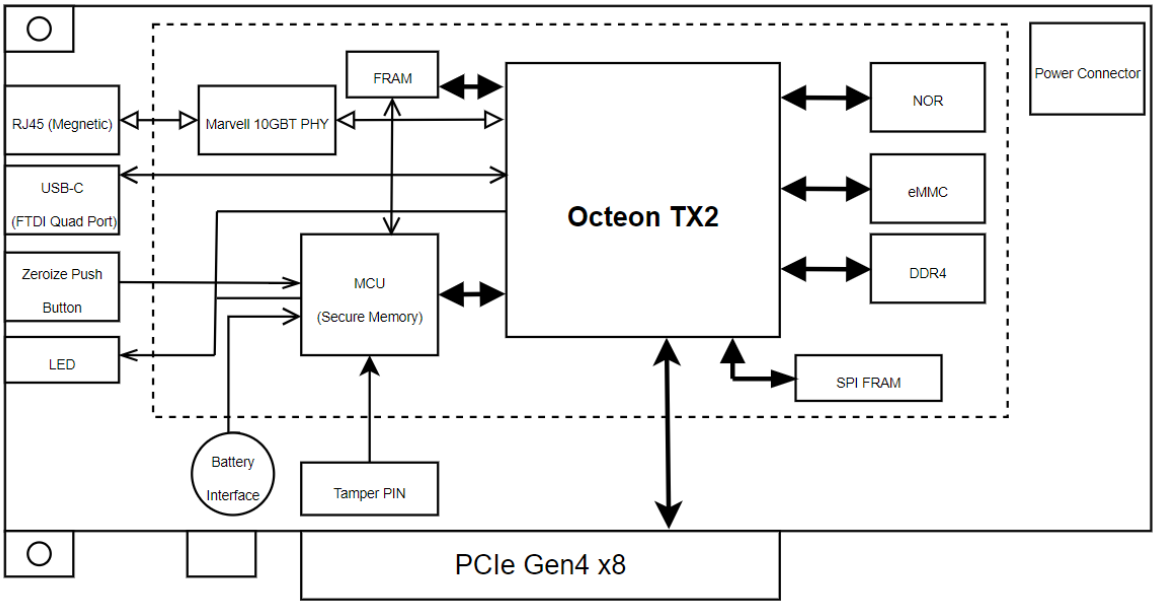

Figure 4: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
LS2-B0 / LS2-G-A050-XX-Y-B0	CN9310410-03 C - LS2-G-A050-XX-Y-B0	MARVELL-LS2-FW-10.23-0602, MARVELL-LS2-UBOOT-10.02-1200-SB	Octeon_TX2	Offers 50% of full card capacity.
LS2-B0 / LS2-G-A100-XX-Y-B0	CN9310410-03 C - LS2-G-A100-XX-Y-B0	MARVELL-LS2-FW-10.23-0602, MARVELL-LS2-UBOOT-10.02-1200-SB	Octeon_TX2	Offers 75% of full card capacity.
LS2-B0 / LS2-G-A300-XX-Y-B0	CN9310410-03 C - LS2-G-A300-XX-Y-B0	MARVELL-LS2-FW-10.23-0602, MARVELL-LS2-UBOOT-10.02-1200-SB	Octeon_TX2	Offers full card capacity.

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no excluded components in the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Uninitialized/Zeroized mode	When received by the end user, the module is not configured or initialized; this state is called uninitialized/zeroized mode. In this mode, the user can query for basic information about the module, such as version details and vendor information, using an unauthenticated role.	Non-Approved	fips_mode = -1
Approved mode	In this mode, the module allows only Approved/nonApprovedAllowed/nonApprovedAllowedNSCalgorithms. Request for anynonApprovedNotAllowedalgorithm is rejected.	Approved	fips_mode = 2 or 3
Non-approved mode	In this mode, the module also allows Approved or allowed algorithms	Non-Approved	fips_mode = 0

Table 3: Modes List and Description

The module is initialized into approved or non-approved mode during the module initialization period. The value of the parameter fipsState passed into the call specifies the mode. As the module supports multiple partitions, each partition maintains its own independent fipsState. The following values are allowed for the fipsState parameter:

1 - Uninitialized/Zeroized Mode
0 - Non-Approved mode.
2 - Approved mode with single-factor authentication mechanism.
3 - Approved mode with certificate-based dual-factor authentication mechanism.

Mode Change Instructions and Status:

The indicator of Approved mode is obtained by using the Get Status service. The fipsState field of the Get Status service indicates the mode. CSPs are not shared between the approved and non-approved modes of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A1948, A7544	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A7544	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0-8192 Increment 8	SP 800-38C
AES-CMAC	A1948	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 32-128 Increment 8 Message Length - Message Length: 0-65536 Increment 8	SP 800-38B
AES-CMAC	A7544	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 16-128 Increment 8, MAC Length: 32-128 Increment 8 Message Length - Message Length: 0-65536 Increment 8	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A1948, A7544	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A1948, A7544	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A1948	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 Tag Length - 128, 32, 64, 96 IV Length - IV Length: 8-1024 Increment 8 Payload Length - Payload Length: 0-65536 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-GCM	A7544	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 Tag Length - 128, 32, 64, 96 IV Length - IV Length: 96-128 Increment 32 Payload Length - Payload Length: 0-65536 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-GMAC	A1948	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 Tag Length - 128, 32, 64, 96 IV Length - IV Length: 8-1024 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-GMAC	A7544	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 Tag Length - 128, 32, 64, 96 IV Length - IV Length: 96-128 Increment 32 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-KW	A1948	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 64	SP 800-38F
AES-KWP	A1948	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 8-4096 Increment 8	SP 800-38F
Counter DRBG	A1948	Prediction Resistance - No, Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A1948	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-5)	A7545	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-4)	A1948	Curve - P-192, P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A1948	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-4
ECDSA SigGen (FIPS186-5)	A7544	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No, Yes	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A1948	Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384,	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
		SHA2-512 Component - Yes	
ECDSA SigVer (FIPS186-5)	A7544	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
Hash DRBG	A7544	Prediction Resistance - Yes Supports Reseed - No Mode - SHA2-512 Entropy Input - Entropy Input: 2048 Nonce - Nonce: 2048 Personalization String Length - Personalization String Length: 0-2048 Increment 8 Additional Input - Additional Input: 0-2048 Increment 8 Returned Bits - 512	SP 800-90A Rev. 1
HMAC-SHA-1	A1948	MAC - MAC: 160 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A7544	MAC - MAC: 160 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-224	A1948	MAC - MAC: 224 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A7544	MAC - MAC: 224 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-256	A1948	MAC - MAC: 256 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7544	MAC - MAC: 256 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-384	A1948	MAC - MAC: 384 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7544	MAC - MAC: 384 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-512	A1948	MAC - MAC: 512 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7544	MAC - MAC: 512 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-224	A1948	MAC - MAC: 112, 128, 160, 192, 224 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A7544	MAC - MAC: 112-224 Increment 8 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-256	A1948	MAC - MAC: 128, 192, 256 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A7544	MAC - MAC: 128-256 Increment 8 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-384	A1948	MAC - MAC: 192, 256, 320, 384 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A7544	MAC - MAC: 192-384 Increment 8 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-512	A1948	MAC - MAC: 256, 320, 384, 448, 512 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A7544	MAC - MAC: 256-512 Increment 8 Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
KAS-ECC Sp800-56Ar3	A1948	Domain Parameter Generation Methods - P-521 Function - Key Pair Generation, Partial Validation iutId - 123456ABCD Scheme - ephemeralUnified - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Auxiliary Function Methods - Auxiliary Function Name - SHA2-512	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		Fixed Info Pattern - l||uPartyInfo||vPartyInfo Fixed Info Encoding - Concatenation Key Length - 512	
KAS-ECC-SSC Sp800-56Ar3	A1948	Domain Parameter Generation Methods - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Scheme - staticUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7544	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - staticUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-IFC-SSC	A1948	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg1-crt Scheme - KAS1 - KAS Role - initiator KAS2 - KAS Role - initiator, responder Fixed Public Exponent - 010001	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A1948	Fixed Info Pattern - uPartyInfo||vPartyInfo||l Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-4096 Increment 8 HMAC Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDA OneStep Sp800-56Cr1	A1948	Auxiliary Function Methods - Auxiliary Function Name - SHA2-224 Fixed Info Pattern - label||uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-1024 Increment 8	SP 800-56C Rev. 2
KDA TwoStep Sp800-56Cr1	A1948	MAC Salting Methods - random Supported Lengths - Supported Lengths: 1-4096 Fixed Info Encoding - concatenation Fixed Info Pattern - uPartyInfo||vPartyInfo||l KDF Mode - counter MAC Modes - CMAC-AES128, CMAC-AES192, CMAC-AES256, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Counter Lengths - 16, 24, 32, 8 Fixed Data Order - after fixed data, before fixed data The KDF supports an empty IV - No The KDF requires an empty IV - No Derived Key Length - 4096 Shared Secret Length - Shared Secret Length: 224-1024 Increment 8	SP 800-56C Rev. 2
KDF ANS 9.63 (CVL)	A1948	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Field Size - 224, 521 Shared Info Length - Shared Info Length: 224, 528 Key Data Length - Key Data Length: 128, 4096	SP 800-135 Rev. 1
KDF SP800-108	A1948	KDF Mode - Counter MAC Mode - CMAC-AES128, CMAC-AES192, CMAC-AES256, CMAC-TDES, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Supported Lengths - Supported Lengths: 64-2048 Increment 8 Fixed Data Order - After Fixed Data, Before Fixed Data, In the Middle of Fixed Data Counter Length - 16, 24, 32, 8 Supports Empty IV - No Custom Key In Length - 0	
KDF SP800-108	A7544	KDF Mode - Counter MAC Mode - CMAC-AES128, CMAC-AES192, CMAC-AES256, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 64-2048 Increment 8 Fixed Data Order - After Fixed Data, Before Fixed Data, In the Middle of Fixed Data Counter Length - 16, 24, 32, 8 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KTS-IFC	A1948	Function - partialVal IUT ID - 0123456789CAFECAFE Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-crt Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Hash Algorithms - SHA3-512 Supports Null Associated Data - Yes Associated Data Pattern - l||uPartyInfo||vPartyInfo Associated Data Encoding - concatenation Key Length - 320	SP 800-56B Rev. 2
KTS-IFC	A7545	Function - partialVal IUT ID - 0123456789CAFECAFE Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-crt Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Hash Algorithms - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - l||uPartyInfo||vPartyInfo Associated Data Encoding - concatenation Key Length - 320	SP 800-56B Rev. 2
RSA Decryption Primitive (CVL)	A1948	Modulus Length - 2048	FIPS 186-4
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7544	Modulo - 2048, 3072, 4096 Key Format - Chinese Remainder Theorem (CRT), Standard Public Exponent Mode - fixed, random Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A1948	Key Generation Mode - probable Modulo - 2048, 3072, 4096, 8192 p mod 8 - 0 Primality Tests - 2pow100 q mod 8 - 0 Fixed Public Exponent - 010001 Info Generated By Server - No Private Key Format - standard Public Exponent Mode - fixed	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
RSA KeyGen (FIPS186-5)	A7545	Key Generation Mode - probable Modulo - 2048, 3072, 4096 p mod 8 - 0 Primality Tests - 2pow100 q mod 8 - 0 Info Generated By Server - No Private Key Format - crt Public Exponent Mode - fixed, random Fixed Public Exponent - 010001	FIPS 186-5
RSA SigGen (FIPS186-5)	A1948	Hash Pair - Hash Algorithm - SHA3-512 Salt Length - 64 Mask Function - MGF1 Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5
RSA Signature Primitive (CVL)	A1948	Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7544	Modulo - 2048, 3072, 4096 Private Key Format - crt, standard Public Exponent Mode - fixed, random Fixed Public Exponent - 010001	FIPS 186-4
RSA SigVer (FIPS186-4)	A1946	Signature Type - PKCS 1.5 Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA SigVer (FIPS186-5)	A1948	Hash Pair - Hash Algorithm - SHA3-512 Salt Length - 64 Mask Function - mgf1 Modulo - 2048, 3072, 4096 Signature Type - pss Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
RSA SigVer (FIPS186-5)	A7545	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Public Exponent Mode - fixed, random Fixed Public Exponent - 010001	FIPS 186-5
SHA-1	A1948	Message Length - Message Length: 0-65536 Increment 8 Function - SHA1	FIPS 180-4
SHA-1	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A1948, A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A1946	Message Length - Message Length: 8-65536 Increment 8 Function - SHA2	FIPS 180-4
SHA2-256	A1948	Message Length - Message Length: 0-65536 Increment 8 Function - SHA2	FIPS 180-4
SHA2-256	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A1948	Message Length - Message Length: 0-65536 Increment 8 Function - SHA2	FIPS 180-4
SHA2-384	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A1948	Message Length - Message Length: 0-65536 Increment 8 Function - SHA2	FIPS 180-4
SHA2-512	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA3-224	A1948	Supports Bit-Oriented Messages - No Supports Empty Message - Yes	FIPS 202
SHA3-224	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A1948	Supports Bit-Oriented Messages - No Supports Empty Message - Yes	FIPS 202
SHA3-256	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A1948	Supports Bit-Oriented Messages - No Supports Empty Message - Yes	FIPS 202
SHA3-384	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A1948	Supports Bit-Oriented Messages - No Supports Empty Message - Yes	FIPS 202
SHA3-512	A7544	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
TDES-CBC	A1948, A7544	Direction - Decrypt, Encrypt Keying Option - 1	SP 800-67 Rev. 2
TDES-ECB	A7544	Direction - Decrypt, Encrypt Keying Option - 1	SP 800-67 Rev. 2
TDES-KW	A1948	Direction - Decrypt	SP 800-38F
TLS v1.2 KDF RFC7627 (CVL)	A7544	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Table 4: Approved Algorithms

The cryptographic module supports the above Approved algorithms. There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli used by the module in approved mode are listed in the above table.

Note: All symmetric key sizes represent the key strength.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG1	Key Type:Asymmetric and Symmetric	N/A	SP800-133rev2 Section 4 Example 1 and IG D.H
CKG2	Key Type:Symmetric	N/A	SP800-133rev2 Section 4 Example 2 and IG D.H

Table 5: Vendor-Affirmed Algorithms

The cryptographic module supports the above Vendor Affirmed Algorithms.

Non-Approved, Allowed Algorithms:

Name	Properties	Implementation	Reference
CPT-AES-CBC (unwrap)	AES:Legacy Key unwrap only CBC mode: Decrypt; 128, 192, and 256-bit	LS2-CPT	Key unwrapping. Per IG D.G
CPT-AES-ECB (unwrap)	AES:AES : Legacy Key unwrap only ECB mode: Decrypt; 128, 192, and 256-bit	LS2-CPT	Key unwrapping. Per IG D.G
EC Diffie-Hellman with non-NIST	Curve Types:Secp256K1 (128 bits) brainpoolP224r1(112 bits), brainpoolP256r1(128	LS2-CPT	Per IGs D.F and C.A.

Name	Properties	Implementation	Reference
recommended curves	bits), brainpoolP320r1(160 bits), brainpoolP384r1(192 bits), brainpoolP512r1(256 bits), Prime order curve, generated as per FIPS 186-5 Section 6		
ECDSA with non-NIST recommended curves	Curve types:Secp256K1 (128 bits) brainpoolP224r1(112 bits), brainpoolP256r1(128 bits), brainpoolP320r1(160 bits), brainpoolP384r1(192 bits), brainpoolP512r1(256 bits), Prime order curve, generated as per FIPS 186-5 Section 6	LS2-CPT	Per IG C.A
SW-AES-CBC (unwrap)	AES:Legacy Key unwrap only CBC mode: Decrypt; 128, 192, and 256-bit	LS2-SW-Crypto	Key unwrapping. Per IG D.G
SW-AES-ECB (unwrap)	AES:Legacy Key unwrap only ECB mode: Decrypt; 128, 192, and 256-bit	LS2-SW-Crypto	Key unwrapping. Per IG D.G

Table 6: Non-Approved, Allowed Algorithms

The cryptographic module supports the above non-Approved algorithms, which are allowed for use in Approved mode.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
SHA1	No security claimed per IG 2.4.A, Scenario 1. Use of a non-approved cryptographic algorithm to "obfuscate" a CSP	Used for Key fingerprint/KCV computation
Triple-DES SP 800-38B	No security claimed per IG 2.4.A, Scenario 1. Use of a non-approved cryptographic algorithm to "obfuscate" a CSP	Used for Key fingerprint/KCV computation
PBKDF	No security claimed per IG 2.4.A, Scenario 2. Use of an algorithm for a purpose that is not security relevant or is redundant.	Used for hashing of authentication passwords

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

The cryptographic module supports the above non-Approved algorithms; they are allowed in the Approved mode of operation with no security claimed.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES (non-compliant)	Key wrap (TR31/TR34/AES-CBC/AES-GCM, wrap/unwrap), Decimal Table/Data/PIN Encryption/Decryption. FF1/FF3-1 Data Encryption/Decryption * In Non-Approved mode, AES GCM supports the IV length from 1 byte to 16 bytes
DES MAC (non-compliant)	MAC generation and Verification
Double-DES (non-compliant)	Derive unique key per transaction (DUKPT), EMV key derivation. Derive PIN from Offset. Derive Offset from PIN. PIN Verification. PVV generation and Verification. CVV generation and verification. Export Symmetric key/Export Asymmetric key pair using TR31 wrapping. Import/Export using TR34. Import Decimal Table. EMV script. EMV ARQC/ARPC. Data/PIN encryption/decryption
EC-AES	EC-AES wrap/unwrap (EC BYOK)
ECDH KDF	Key derivation using ECDH followed by HMAC/CMAC counter KDF

Name	Use and Function
ECDSA (non-compliant)	Key generation, Sign, Verify P192, Secp192k1, brainpoolP160r1, brainpool192r1, K-163 and B-163 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)
KAS-ECC (non-compliant)	EC Key generation and ECDH Curve25519 (128 bits), Curve448 (224 bits)
ML-DSA ECDSA Sign (non-compliant)	Signature generation function which generates a concateneated signature of ML_DSA and ECDSA
ML-DSA ECDSA Verify (non-compliant)	Signature verification function which verifies a concateneated signature of ML_DSA and ECDSA
RSA (non-compliant)	TR34 Import TR34 Export PIN block decryption BYOK Encrypt/Decrypt Asymmetric key encapsulation and un-encapsulation using PKCS#1-v1.5 padding with modulus size bits 2048-, 3072- and 4096-bits Key generation, Sign, Verify (1024-bit)
PBE	Key generation
Shamir Key Share (non-compliant)	Key share
SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant)	Random number generation for user, keys, internal IVs, and salt
Triple-DES (non-compliant)	Derive unique key per transaction (DUKPT) EMV key derivation. Derive PIN from Offset Derive Offset from PIN Verification PVV generation and verification CVV generation and verification Export Symmetric key/Export Asymmetric key pair using TR31 wrapping Import/Export using TR34 Import Decimal Table EMV script. EMV ARQC/ARPC Data/PIN encryption/decryption

Table 8: Non-Approved, Not Allowed Algorithms

The cryptographic module supports the above non-Approved algorithms available only in non-Approved mode of operation.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
SW-KeyGen	CKG	Symmetric Key Generation		Counter DRBG: (A1948) AES-CTR: (A1948) CKG1: ()
CPT-KeyGen	CKG	Symmetric Key Generation		Hash DRBG: (A7544) CKG1: ()
ENT (P) (SP 800-90B)	ENT-ESV	Physical Entropy		
KAS-TLS (Sp800-56Ar3)	KAS-Full	TLS v1.2 KDF to create the end to end tunneling.	IG:IG D.F Scenario 2 path (2). Key Confirmation:No Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 112 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A7544) TLS v1.2 KDF RFC7627: (A7544)
KAS-ANS-9.63 (Sp800-56Ar3)	KAS-Full	ECDH key derivation and ECDH-AES key wrap	IG:IG D.F Scenario 2 path (2). Key Confirmation:No Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 112 and 256 bits of encryption strength.	KAS-ECC-SSC Sp800-56Ar3: (A1948) KDF ANS 9.63: (A1948)
KAS-KDA-HKDF (SP800-56Ar3)	KAS-Full	ECDH key derivation and ECDH-AES key wrap	IG:IG D.F Scenario 2 path (2). Key Confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides between 112 and 256 bits of encryption strength.	KAS-ECC-SSC Sp800-56Ar3: (A1948) KDA HKDF Sp800-56Cr1: (A1948)
KAS-KDA-ONESTEP (SP800-56Ar3)	KAS-Full	ECDH key derivation and ECDH-AES key wrap	IG:IG D.F Scenario 2 path (2). Key Confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides between 112 and 256 bits of encryption strength.	KAS-ECC-SSC Sp800-56Ar3: (A1948) KDA OneStep Sp800-56Cr1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
KAS-KDA-TWOSTEP (SP800-56Ar3)	KAS-Full	ECDH key derivation and ECDH-AES key wrap	IG:IG D.F Scenario 2 path (2). Key Confirmation:No Key derivation:KDA	KAS-ECC-SSC Sp800-56Ar3: (A1948) KDA TwoStep Sp800-56Cr1: (A1948)

Name	Type	Description	Properties	Algorithms
			(separately tested) Caveat:Key establishment methodology provides between 112 and 256 bits of encryption strength.	AES-CMAC: (A1948) HMAC-SHA-1: (A1948) HMAC-SHA2-224: (A1948) HMAC-SHA2-256: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948) SHA-1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA3-512: (A1948)
KAS-IFC-OneStep (SP800-56Br2)	KAS-Full	PEK and KLK generation and certificate authentication and cloning	IG:IG D.F Scenario 1 path (2). Key Confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment method provides 112 bits of encryption strength	KAS-IFC-SSC: (A1948) KDA OneStep Sp800-56Cr1: (A1948) SHA2-512: (A1948) CKG2: () Key Type: Symmetric
SW-AES-GCM-Wrap	KTS-Wrap	Authenticated Data encryption, key-wrap	IG D.G:Approved Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-GCM: (A1948) AES-ECB: (A1948)
SW-AES-GCM-Unwrap	KTS-Unwrap	Authenticated Datadecryption, key-unwrap	IG D.G:Approved Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-GCM: (A1948) AES-ECB: (A1948)
SW-AES-GCM-Enc	BC-AuthEncrypt	Authenticated Data encryption		AES-GCM: (A1948) AES-ECB: (A1948)
SW-AES-GCM-Dec	BC-AuthDecrypt	Authenticated Data decryption		AES-GCM: (A1948) AES-ECB: (A1948)
SW-KAS-ECC (KAS)	KAS-SSC	Cloning protocol	Caveat:Key establishment methodology provides 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A1948)
SW-AES-KW-Wrap (KTS)	KTS-Wrap	Key wrapping	IG D.G:Approved Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-KW: (A1948) AES-ECB: (A1948)
SW-AES-KW-Unwrap (KTS)	KTS-Unwrap	Key unwrapping	IG D.G:Approved Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-KW: (A1948) AES-ECB: (A1948)

Name	Type	Description	Properties	Algorithms
SW-KTS-IFC-Encap (KTS)	KTS-Encap	Asymmetric key encapsulation	IG D.G:Approved Key confirmation:No Caveat:Key establishment methodology provides between 128 and 150 bits of encryption strength	KTS-IFC: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948) RSA KeyGen (FIPS186-5): (A1948)
SW-KTS-IFC-Decap (KTS)	KTS-Decap	Asymmetric key decapsulation	IG D.G:Approved Key confirmation:No Caveat:Key establishment methodology provides between 128 and 150 bits of encryption strength	KTS-IFC: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948) RSA KeyGen (FIPS186-5): (A1948)
LEGACY-SW-TDES-KW (KTS)	KTS-Unwrap	Key unwrapping* Legacy use only	IG D.G:Allowed Caveat:Key unwrapping as Per IG D.G	TDES-KW: (A1948) TDES-CBC: (A1948)
FW-KTS-IFC-Encap (KTS)	KTS-Encap	Asymmetric key encapsulation	IG D.G:Approved Key confirmation:No Caveat:Key establishment methodology provides between 128 and 150 bits of encryption strength	KTS-IFC: (A7545) SHA2-224: (A7544) SHA2-256: (A7544) SHA3-384: (A7544) SHA2-512: (A7544) RSA KeyGen (FIPS186-5): (A7545)
FW-KTS-IFC-Decap (KTS)	KTS-Decap	Asymmetric key decapsulation	IG D.G:Approved Key confirmation:No Caveat:Key establishment methodology provides between 128 and 150 bits of encryption strength	KTS-IFC: (A7545) SHA2-224: (A7544) SHA2-256: (A7544) SHA3-384: (A7544) SHA2-512: (A7544) RSA KeyGen (FIPS186-5): (A7545)
LEGACY-SW-AES-CBC-UNWRAP	BC-UnAuthDecrypt	Legacy Key unwrap only CBC mode: Decrypt; 128, 192, and 256-bit	Caveat:Key unwrapping as Per IG D.G.	AES-CBC: (A1948)
LEGACY-SW-AES-ECB-UNWRAP	BC-UnAuthDecrypt	Legacy Key unwrap only ECB mode: Decrypt; 128, 192, and 256-bit	Caveat:Key unwrapping as Per IG D.G.	AES-ECB: (A1948)
LEGACY-CPT-AES-CBC-UNWRAP	BC-UnAuthDecrypt	Legacy Key unwrap only CBC mode: Decrypt; 128,192, and 256-bit	Caveat:Key unwrapping as Per IG D.G.	AES-CBC: (A7544)
LEGACY-CPT-AES-ECB-UNWRAP	BC-UnAuthDecrypt	Legacy Key unwrap only ECB mode: Decrypt; 128, 192, and 256-bit	Caveat:Key unwrapping as Per IG D.G.	AES-ECB: (A7544)
CPT-ECDH-NON-NIST	KAS-SSC	EC Diffie-Hellman with non-NIST recommended curves	Caveat:as Per IGs D.F and C.A.	KAS-ECC-SSC Sp800-56Ar3: (A7544) Curve Types: Secp256K1 (128 bits) brainpoolP224r1(112 bits), brainpoolP256r1(128 bits), brainpoolP320r1(160 bits), brainpoolP384r1(192 bits), brainpoolP512r1(256 bits),

Name	Type	Description	Properties	Algorithms
				Prime order curve, generated as per FIPS 186-5 Section 6
CPT-ECDSA-SigGen-NON-NIST	DigSig-SigGen	ECDSA with non-NIST recommended curves	Caveat:as Per IG C.A.	ECDSASigGen: (FIPS186-4)
CPT-AES-CBC-ENC	BC-UnAuthEncrypt	LS2-CPT Encryption		AES-CBC: (A7544)
CPT-AES-CBC-DEC	BC-UnAuthDecrypt	LS2-CPT Decryption		AES-CBC: (A7544)
SW-AES-CBC-UNWRAP	BC-UnAuthDecrypt	LS2-SW-Crypto Decryption		AES-CBC: (A1948)
SW-AES-CBC-WRAP	BC-UnAuthEncrypt	LS2-SW-Crypto Encryption		AES-CBC: (A1948)
CPT-AES-CCM-ENC	BC-AuthEncrypt	LS2-CPT Authenticated Encryption		AES-CCM: (A7544) AES-CBC: (A7544)
CPT-AES-CCM-DEC	BC-AuthDecrypt	LS2-CPT Authenticated Decryption		AES-CCM: (A7544) AES-CBC: (A7544)
CPT-AES-CMAC	MAC	LS2-CPT MAC		AES-CMAC: (A7544) AES-CBC: (A7544)
SW-AES-CMAC	MAC	LS2-SW-Crypto MAC		AES-CMAC: (A1948) AES-CBC: (A7544)
CPT-AES-CTR-ENC	BC-UnAuthEncrypt	LS2-CPT Encryption		AES-CTR: (A7544)
CPT-AES-CTR-DEC	BC-UnAuthDecrypt	LS2-CPT Decryption		AES-CTR: (A7544)
CPT-AES-ECB-ENC	BC-UnAuthEncrypt	LS2-CPT Encryption		AES-ECB: (A7544)
CPT-AES-ECB-DEC	BC-UnAuthDecrypt	LS2-CPT Decryption		AES-ECB: (A7544)
CPT-AES-GCM-ENC	BC-AuthEncrypt	LS2-CPT Authenticated Encryption		AES-GCM: (A7544) AES-ECB: (A7544)
CPT-AES-GCM-DEC	BC-AuthDecrypt	LS2-CPT Authenticated Decryption		AES-GCM: (A7544) AES-ECB: (A7544)
CPT-AES-GMAC	MAC	LS2-CPT		AES-GMAC: (A7544) AES-ECB: (A7544)
SW-AES-GMAC	MAC	LS2-SW-Crypto		AES-GMAC: (A1948) AES-ECB: (A1948)
SW-AES-KWP-Wrap (KTS)	KTS-Wrap	LS2-SW-Crypto Key Wrap	IG D.G:Approved Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-KWP: (A1948) AES-CBC: (A1948)
SW-AES-KWP-Unwrap (KTS)	KTS-Unwrap	LS2-SW-Crypto Key Unwrap	IG D.G:Approved Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-KWP: (A1948) AES-CBC: (A1948)
SW-Counter-DRBG	DRBG	LS2-SW-Crypto DRBG		Counter DRBG: (A1948) AES-CTR: (A1948)

Name	Type	Description	Properties	Algorithms
SW-ECDSA-KeyGen (FIPS186-4)	AsymKeyPair-KeyGen	LS2-SW-Crypto ECC Key Generation		ECDSA KeyGen (FIPS186-4): (A1948) CKG1: () Counter DRBG: (A1948) KAS-ECC-SSC Sp800-56Ar3: (A1948)
FW-ECDSA-KeyGen (FIPS186-5)	AsymKeyPair-KeyGen	LS2-FW-Crypto ECC Key Generation		ECDSA KeyGen (FIPS186-5): (A7545) CKG1: () Hash DRBG: (A7544) KAS-ECC-SSC Sp800-56Ar3: (A7544)
SW-ECDSA-KeyVer (FIPS186-4)	AsymKeyPair-KeyVer	LS2-SW-Crypto ECC key Verification		ECDSA KeyVer (FIPS186-4): (A1948)
CPT-ECDSA-SigGen (FIPS186-4)	DigSig-SigGen	LS2-CPT ECC Signature Generation		ECDSA SigGen (FIPS186-5): (A7544) SHA2-224: (A7544) SHA2-256: (A7544) SHA2-384: (A7544) SHA2-512: (A7544)
SW-ECDSA-SigGen (FIPS186-4)	DigSig-SigGen	LS2-SW-Crypto ECC Signature Verification		ECDSA SigGen (FIPS186-4): (A1948) SHA-1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
CPT-ECDSA-SigVer (FIPS186-5)	DigSig-SigVer	LS2-CPT ECC Signature Verification		ECDSA SigVer (FIPS186-5): (A7544) SHA2-224: (A7544) SHA2-256: (A7544) SHA2-384: (A7544) SHA2-512: (A7544)
SW-ECDSA-SigVer (FIPS186-4)	DigSig-SigVer	LS2-SW-Crypto ECC Signature Verification		ECDSA SigVer (FIPS186-4): (A1948) SHA-1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
CPT-Hash-DRBG	DRBG	LS2-CPT DRBG		Hash DRBG: (A7544) SHA2-512: (A7544)
CPT-HMAC-SHA-1	MAC	LS2-CPT HMAC-SHA-1		HMAC-SHA-1: (A7544) SHA-1: (A7544)
SW-HMAC-SHA-1	MAC	LS2-SW-Crypto HMAC-SHA-1		HMAC-SHA-1: (A1948) SHA-1: (A1948)
CPT-HMAC-SHA2-224	MAC	LS2-CPT HMAC SHA2-224		HMAC-SHA2-224: (A7544) SHA2-224: (A7544)
SW-HMAC-SHA2-224	MAC	LS2-SW-Crypto HMAC SHA2-224		HMAC-SHA2-224: (A1948)
CPT-HMAC-SHA2-256	MAC	LS2-CPT HMAC SHA2-256		HMAC-SHA2-256: (A7544) SHA2-256: (A7544)
SW-HMAC-SHA2-256	MAC	LS2-SW-Crypto HMAC SHA2-256		HMAC-SHA2-256: (A1948) SHA2-256: (A1948)
CPT-HMAC-SHA2-384	MAC	LS2-CPT HMAC SHA2-384		HMAC-SHA2-384: (A7544) SHA2-384: (A7544)
SW-HMAC-SHA2-384	MAC	LS2-SW-Crypto HMAC SHA2-384		HMAC-SHA2-384: (A1948) SHA2-384: (A1948)

Name	Type	Description	Properties	Algorithms
CPT-HMAC-SHA2-512	MAC	LS2-CPT HMAC SHA2-512		HMAC-SHA2-512: (A7544) SHA2-512: (A7544)
SW-HMAC-SHA2-512	MAC	LS2-SW-Crypto HMAC SHA2-512		HMAC-SHA2-512: (A1948) SHA2-512: (A1948)
CPT-HMAC-SHA3-224	MAC	LS2-CPT HMAC SHA3-224		HMAC-SHA3-224: (A7544) SHA3-224: (A7544)
SW-HMAC-SHA3-224	MAC	LS2-SW-Crypto HMAC SHA3-224		HMAC-SHA3-224: (A1948) SHA3-224: (A1948)
CPT-HMAC-SHA3-256	MAC	LS2-CPT HMAC SHA3-256		HMAC-SHA3-256: (A7544) SHA3-256: (A7544)
SW-HMAC-SHA3-256	MAC	LS2-SW-Crypto HMAC SHA3-256		HMAC-SHA3-256: (A1948) SHA3-256: (A1948)
CPT-HMAC-SHA3-384	MAC	LS2-CPT HMAC SHA3-384		HMAC-SHA3-384: (A7544) SHA3-384: (A7544)
SW-HMAC-SHA3-384	MAC	LS2-SW-Crypto HMAC SHA3-384		HMAC-SHA3-384: (A1948) SHA3-384: (A1948)
CPT-HMAC-SHA3-512	MAC	LS2-CPT HMAC SHA3-512		HMAC-SHA3-512: (A7544) SHA3-512: (A7544)
SW-HMAC-SHA3-512	MAC	LS2-SW-Crypto HMAC SHA3-512		HMAC-SHA3-512: (A1948) SHA3-512: (A1948)
SW-KAS-ECC-Sp800-56Ar3	KAS-Full	LS2-SW-Crypto ECC key agreement	IG:IG D.F Scenario 2 path (2). Key Confirmation:No Key derivation:KDA (tested as part of KAS certificate) Caveat:Key establishment methodology provides 256 bits of encryption strength	KAS-ECC Sp800-56Ar3: (A1948)
CPT-KAS-ECC-SSC-Sp800-56Ar3	KAS-SSC	LS2-CPT ECC Key Agreement Shared Secret		KAS-ECC-SSC Sp800-56Ar3: (A7544)
SW-KAS-ECC-SSC-Sp800-56Ar3	KAS-SSC	LS2-SW-Crypto ECC Key Agreement Shared Secret		KAS-ECC-SSC Sp800-56Ar3: (A1948)
SW-KAS-IFC-SSC	KAS-SSC	LS2-SW-Crypto IFC Key Agreement Shared Secret		KAS-IFC-SSC: (A1948) RSA KeyGen (FIPS186-4): (A1948)
SW-KDA-HKDF-Sp800-56Cr1	KAS-56CKDF	LS2-SW-Crypto IFC Key Agreement Shared Secret		KDA HKDF Sp800-56Cr1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
SW-KDA-OneStep-Sp800-56Cr1	KAS-56CKDF	LS2-SW-Crypto One-Step Key derivation function		KDA OneStep Sp800-56Cr1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
SW-KDA-TwoStep-Sp800-56Cr1	KAS-56CKDF	LS2-SW-Crypto Two-Step Key derivation Function		KDA TwoStep Sp800-56Cr1: (A1948) AES-CMAC: (A1948) AES-ECB: (A1948) HMAC-SHA-1: (A1948) HMAC-SHA2-224: (A1948)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-256: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948) SHA-1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
SW-KDF-ANS-9.63	KAS-135KDF	LS2-SW-Crypto ANS 9.63 Key derivation Function		KDF ANS 9.63: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
CPT-KDF-SP800-108	KBKDF	LS2-CPT SP800-108 Key derivation Function		KDF SP800-108: (A7544) AES-CMAC: (A7544) HMAC-SHA-1: (A7544) HMAC-SHA2-224: (A7544) HMAC-SHA2-256: (A7544) HMAC-SHA2-384: (A7544) HMAC-SHA2-512: (A7544) SHA-1: (A7544) SHA2-224: (A7544) SHA2-256: (A7544) SHA2-384: (A7544) SHA2-512: (A7544) CKG2: ()
SW-KDF-SP800-108	KBKDF	LS2-SW-CryptoSP800-108 Key derivation Function		KDF SP800-108: (A1948) AES-CMAC: (A1948) HMAC-SHA-1: (A1948) HMAC-SHA2-224: (A1948) HMAC-SHA2-256: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948) SHA-1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
CPT-KDF-TLS	KAS-135KDF	LS2-CPT TLS based end to end encryption		TLS v1.2 KDF RFC7627: (A7544)
SW-PBKDF	PBKDF	LS2-SW-Crypto		PBKDF: () HMAC-SHA-1: (A1948) HMAC-SHA2-224: (A1948) HMAC-SHA2-256: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948) HMAC-SHA3-224: (A1948) HMAC-SHA3-256: (A1948) HMAC-SHA3-384: (A1948) HMAC-SHA3-512: (A1948) SHA-1: (A1948) SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948) SHA3-224: (A1948) SHA3-256: (A1948) SHA3-384: (A1948) SHA3-512: (A1948) CKG2: ()

Name	Type	Description	Properties	Algorithms
CPT-RSA-Decryption-Primitive	KTS-Decap	LS2-CPT Decryption Primitive		RSA Decryption Primitive Sp800-56Br2: (A7544)
SW-RSA-Decryption-Primitive	KTS-Decap	LS2-SW-Crypto Decryption Primitive		RSA Decryption Primitive: (A1948)
FW-RSA-KeyGen (FIPS186-5)	AsymKeyPair-KeyGen	LS2-FW-CryptoAsymmetric Key-Pair Generation		RSA KeyGen (FIPS186-5): (A7545) KTS-IFC: (A7545) CKG1: ()
FW-RSA-SigVer (FIPS186-5)	AsymKeyPair-KeyGen	LS2-FW-CryptoSignature Verification		RSA SigVer (FIPS186-5): (A7545) SHA2-224: (A7544) SHA2-256: (A7544) SHA2-384: (A7544) SHA2-512: (A7544) SHA3-224: (A7544) SHA3-256: (A7544) SHA3-384: (A7544) SHA3-512: (A7544)
SW-RSA-KeyGen (FIPS186-5)	AsymKeyPair-KeyGen	LS2-SW-CryptoAsymmetric Key-Pair Generation		RSA KeyGen (FIPS186-5): (A1948) KTS-IFC: (A1948) KAS-IFC-SSC: (A1948) CKG1: ()
SW-RSA-SigGen (FIPS186-5)	DigSig-SigGen	LS2-SW-Crypto Signature Generation		RSA SigGen (FIPS186-5): (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
SW-RSA-SigVer (FIPS186-5)	DigSig-SigVer	LS2-SW-CryptoSignature Verification		RSA SigVer (FIPS186-5): (A1948) SHA-1: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
CPT-RSA-Signature-Primitive	DigSig-SigGen	LS2-CPT Signature Primitive		RSA Signature Primitive: (A7544)
SW-RSA-Signature-Primitive	DigSig-SigGen	LS2-SW-Crypto Signature Primitive		RSA Signature Primitive: (A1948)
UB-RSA-SigVer (FIPS186-4)	DigSig-SigVer	LS2-UBOOT Signature Verification		RSA SigVer (FIPS186-4): (A1946) SHA2-256: (A1946)
CPT-SHA-1	SHA	LS2-CPT Digest		SHA-1: (A7544)
SW-SHA-1	SHA	LS2-SW-Crypto Digest		SHA-1: (A1948)
CPT-SHA2-224	SHA	LS2-CPT Digest		SHA2-224: (A7544)
CPT-SHA2-256	SHA	LS2-CPT Digest		SHA2-256: (A7544)
SW-SHA2-256	SHA	LS2-SW-Crypto Digest		SHA2-256: (A1948)
CPT-SHA2-384	SHA	LS2-CPT Digest		SHA2-384: (A7544)
SW-SHA2-384	SHA	LS2-SW-Crypto Digest		SHA2-384: (A1948)
CPT-SHA2-512	SHA	LS2-CPT Digest		SHA2-512: (A7544)

Name	Type	Description	Properties	Algorithms
SW-SHA2-512	SHA	LS2-SW-Crypto Digest		SHA2-512: (A1948)
CPT-SHA3-224	SHA	LS2-CPT Digest		SHA3-224: (A7544)
SW-SHA3-224	SHA	LS2-SW-Crypto Digest		SHA3-224: (A1948)
CPT-SHA3-256	SHA	LS2-CPT Digest		SHA3-256: (A7544)
SW-SHA3-256	SHA	LS2-SW-Crypto Digest		SHA3-256: (A1948)
CPT-SHA3-384	SHA	LS2-CPT Digest		SHA3-384: (A7544)
SW-SHA3-384	SHA	LS2-SW-Crypto Digest		SHA3-384: (A1948)
CPT-SHA3-512	SHA	LS2-CPT Digest		SHA3-512: (A7544)
SW-SHA3-512	SHA	LS2-SW-Crypto Digest		SHA3-512: (A1948)
CPT-SHAKE-128	XOF	LS2-CPT Digest		SHAKE-128: (A7544)
SW-SHAKE-128	XOF	LS2-SW-Crypto Digest		SHAKE-128: (A1948)
CPT-SHAKE-256	XOF	LS2-CPT Digest		SHAKE-256: (A7544)
SW-SHAKE-256	XOF	LS2-SW-Crypto Digest		SHAKE-256: (A1948)
CPT-TDES-CBC	BC-UnAuthDecrypt	LS2-CPT Unauthenticated Decryption		TDES-CBC: (A7544)
LEGACY-CPT-TDES-ECB	BC-UnAuthDecrypt	LS2-CPT Unauthenticated Decryption		TDES-ECB: (A7544)

Table 9: Security Function Implementations

The cryptographic module supports the above Security Function Implementations available in Approved mode of operation.

2.7 Algorithm Specific Information

- AES-GCM (A7544)
  - IG C.H Scenario #1:
    - TLS 1.2 or other applications can offload GCM operations.
    - For TLS 1.2, the IV is constructed as described in RFC 5288.
    - For TLS 1.2 AES GCM the following cipher suites are supported:
      - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
      - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - IV is generated internally to the cryptographic module.
    - The module triggers a handshake to establish new encryption keys and IVs when the IV exhausts the maximum possible values for the given session key.
    - SP 800-38D §8.2.2 is used for GCM IV construction.

  - IG C.H Scenario #2:
    - IVs are generated randomly and IG C.H Option #2 applies.
    - IV's free field is a 4-byte counter.
    - IV's random field is a 96-bit random number.
    - IV's random field is incremented by 1. IV's random field wouldn't overflow 96-bits in the lifetime of the module.
    - For IV restoration conditions guidance, refer to section 11.5 User Guidance.
    - Internal Approved RBG (Hash DRBG # A7544): SP 800-90A DRBG, HASH_DRBG SHA2-512.

- AES-GCM (A1948)
  - IG C.H Notes:
    - IVs are generated randomly, and IG C.H Option #2 applies.
    - IV is generated internally to the cryptographic module.
    - SP 800-38D §8.2.2 is used for GCM IV construction.
    - IV's random field is a 128-bit random number.
    - If the module's power is lost and then restored, the module will generate new IVs.
    - Approved RBG (Hash DRBG # A7544): SP 800-90Ar1 DRBG, HASH_DRBG SHA2-512.

- PBKDF (SP 800-132)
  - PBKDF is used only for password hashing as allowed by SP 800-63B. PBKDF is not used to derive a Data Protection Key for storage applications.

  - PBKDF with HMAC password strength
    - The password is a minimum of 8 characters, case-sensitive alpha-numeric. As such there are (26*2+10)^8 = 62^8 possible minimum-length passwords, and the false acceptance rate is 1 in 62^8 which is less than 1 in 1,000,000.
    - A maximum of 20 password attempts is possible before permanent lockout. Therefore, the probability of false authentication over any timeframe is 20 in 62^8, which is less than 1 in 100,000. (The number of

allowed login attempts prior to lockout is configured during module initialization but cannot exceed 20.)
        - Lockout of MCO automatically zeroizes the module in the next reboot. In all other cases, lockout can be unset by destroying the partition.
    - PBKDF with HMAC Iteration Count and Justification
        - Iteration count used by the module is 311,000, following the recommendation in SP800-132r2.
        - Salt length is 128 to 4096 bits.

- EC Diffie-Hellman and ECDSA with non-NIST recommended curves
    - NIST SP 800-186 (H1)
        - brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, and brainpoolP512r1 are allowed to be used for interoperability reasons.
    - NIST SP 800-186 (H2)
        - secp256k1 is allowed to be used only for blockchain-related applications.

- Legacy Algorithms
    - Algorithms designated as “Legacy” can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M
        - TDES-CBC (SP 800- 38A) (A7544): Data decryption for data encrypted before 2024
        - TDES-ECB (SP 800- 38A) (A7544): Data decryption for data encrypted before 2024
        - TDES-ECB (A1948): Prerequisite for TDES-KW for data encrypted before 2024
        - TDES-KW (KTS) (SP 800-38F) (A1948): Key unwrapping for key wrapped before 2024
        - TDES-KW (SP 800- 38F) (A1948): Key unwrapping for key wrapped before 2024

2.8 RBG and Entropy

Cert Number	Vendor Name
E231	Marvell Semiconductor, Inc

Table 10: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
OCTEON HW RBG	Physical	OCTEON TX2	128 bits	2.673 bits	N/A

Table 11: Entropy Sources

The OCTEON TX2 HW unit generates random bits from the 8-free running oscillators from a total of 128-free running oscillators. The random bits generated are already run through HW-level health tests (APT and RCT).

2.9 Key Generation

- CKG SP 800-133Rev2 (Vendor affirmed)
  - IG D.H
    - SP 800-133Rev2 Section 5.1 Asymmetric signature key generation using unmodified DRBG output.
    - SP 800-133Rev2 Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output.
    - SP 800-133Rev2 Section 6.1 Direct symmetric key generation using unmodified DRBG output.
    - SP 800-133Rev2 Section 6.2.1 Derivation of symmetric keys from a key-agreement shared secret.
    - SP 800-133Rev2 Section 6.2.2 Derivation of symmetric keys from a pre-shared key.

2.10 Key Establishment

Key Agreement Information

- Key Agreement Scheme (IG D.F)
  The Module supports the following Scenario 1 key agreement schemes.
  - KAS-IFC-SSC (SP 800-56Br2) (A1948)
  - KAS-IFC OneStep (SP800-56Br2)(A1948) Scenario 1 path (2)

  The Module supports the following Scenario 2 key agreement schemes as per IG D.F.
  - KAS-ECC-SSC (SP800-56Ar3) (A7544)
  - KAS-ECC (KAS) (SP 800-56Ar3) (A1948) Scenario 2 path (2)
  - KAS-ECC (SP800- 56Ar3) (A1948)
  - KAS TLS (SP 800- 56Ar3) (A7544) Scenario 2 path (2)
  - KAS ANS 9.63 (SP 800-56Ar3) (A1948) Scenario 2 path (2)
  - KAS KDA HKDF (SP 800-56Ar3) (A1948) Scenario 2 path (2)
  - KAS KDA ONESTEP (SP 800-56Ar3) (A1948) Scenario 2 path (2)
  - KAS KDA TWOSTEP (SP 800-56Ar3) (A1948) Scenario 2 path (2)

Key Transport Information

- Key Transport Method (IG D.G)
  Key Encapsulation
  - KTS-IFC (KTS) (SP 800-56Br2) (A1948) (key encapsulation and unencapsulation)
  - KTS-IFC (SP 800- 56Br2) (A1948)
  - KTS-IFC (KTS) (SP 800-56Br2) (A7545)

  Key Wrapping
  - AES-KW (KTS) (SP 800-38F) (A1948)
  - AES-KWP (KTS) (SP 800-38F) (A1948)
  - TDES-KW (KTS) (SP 800-38F) (A1948) (Key unwrapping)

2.11 Industry Protocols

- TLS 1.2 Cipher Suites
  The module supports the algorithms for the following cipher suites using Approved and allowed algorithms and key sizes:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

  For cipher suites using GCM, the IV is generated per RFC 7627. The module supports GCM cipher suites compatible with SP 800- 52 Rev2.

No parts of the TLS and ANS 9.63 protocols, other than the approved cryptographic algorithms and the KDF, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
USB (FTDI USB to Multi-Channe)	Status Output	Log messages of MCU UART,SMBus, Diagnostics
PCIe	Data Input Data Output Control Input Status Output	Primary interface to communicate with the module. Provides APIs for the software on the host to communicate with the module
PCIeSMBus	Status Output	Log message of Diagnostics and System management
LED	Status Output	Operation status
Tamper PIN	Control Input	No data; only a signal from high to low
Zeroize push button	Control Input	No data; only a signal
Power connector		No data; external power connector
Battery interfaces		No data; external power connector

Table 12: Ports and Interfaces

The module does not contain any control output interface.
The RJ45 Connector depicted in cryptographic boundary view is disabled in firmware.

3.2 Additional Information

The PCIe data interface is the only interface that accepts the security services always accessible from the module; the host system cannot read or write data over this interface. The module will start reading commands from the Host system only after the power-on self-tests are run and the firmware is loaded. After the module is zeroized, the firmware enforces that the PCIe data interface only provides basic versioning and informational output. When the module enters the error state, the PCIe data interface will report the error state and no other data.

Other interfaces are all meant for informational services to read temperature, logs, and diagnostic information but no other data.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Username and password	The password is a minimum of 8 characters (case-sensitive, alpha-numeric).	SW-AES-KWP-Unwrap (KTS)	The password is a minimum of 8 characters (case-sensitive, alpha-numeric. As such, there are (26*2+10)^8 = 62^8 possible minimum-length passwords,and the false acceptance rate is 1 in 62^8	A maximum of 20 password attempts are possible before a user is permanently locked out. Therefore, the probability of false authentication over any time frame is 20 /62^8 (The number of allowed login attempts prior to lockout is configured during module initialization but cannot exceed 20.)
Digital signature	Authentication is performed using SHA2-256 based RSA 2048-bit PKCS#1-v1.5 signatures(provides 112 bits of strength). Corresponding public key is associated with the identity.	SW-RSA-SigVer (FIPS186-5)	The probability that a random attempt will succeed or a false acceptance will occur is approximately 1/(2^112).	For each failed signature verification, the module will block for 2 seconds. Therefore, the probability that a random attempt will succeed in a one-minute period is approximately 30/(2^112)

Table 13: Authentication Methods

The module supports the above identity-based authentication methods.

The module also supports the multi-factor Authentication, which is performed using SHA2-256 based RSA 2048-bit PKCS#1-v1.5 signatures (provides 112 bits of strength). The corresponding public key is associated with the identity.

The probability that a random attempt will succeed, or a false acceptance will occur is approximately 1 in 2^112.

4.2 Roles

A role is explicitly selected at authentication; the MCO role is associated with the master partition and the PCO, AU and PCU roles are associated with user partitions (see section 4 Roles, Services, and Authentication for details). The module allows multiple operators per role, per partition with a caveat of one AU per Partition.

A username is used as the identity of a user. This means for a given partition, each username needs to be unique.

Name	Type	Operator Type	Authentication Methods
MCO	Identity	Crypto Officer	Username and password

Name	Type	Operator Type	Authentication Methods
MCO (2FA)	Multi-Factor Identity	Crypto Officer	Username and password Digital signature
Pre-CO	Identity	Crypto Officer	Username and password
PCO	Identity	Crypto Officer	Username and password
PCO (2FA)	Multi-Factor Identity	Crypto Officer	Username and password Digital signature
PCU	Identity	Crypto User	Username and password
PCU (2FA)	Multi-Factor Identity	Crypto User	Username and password Digital signature
AU	Identity	Audit User	Username and password

Table 14: Roles

4.3 Approved Services

The Approved Services indicator for all Approved services in the table below is successful execution when the partition is operated in the approved mode.

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
GP_PARTITION_MGMT	Provides services to manage user and master partitions	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-KeyGen CPT-KeyGen SW-AES-GCM-Wrap SW-AES-GCM-Unwrap SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-Counter-DRBG SW-ECDSA-SigVer (FIPS186-4) CPT-Hash-DRBG SW-KDA-HKDF-Sp800-56Cr1 SW-RSA-KeyGen (FIPS186-5) SW-RSA-SigGen	MCO - HSM Master Encryption Key (HXMEKY): G,E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - HSM Vendor Firmware Update Validation Key Public RSA (HVFUVKYPUBRSA): E - HSM Owner Attestation Key Public (HOOATKYPUB): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z,G - FIPS Partition HSM Manufacturer Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-SHA2-256 ENT (P) (SP 800-90B)	Authentication Key Private RSA (FPHMMAKYPRVRSA): E - FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC): E - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E - Partition Authentication Certificate (PXPACT): Z,G - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - Partition Data Encryption Key (PXDEKY): G,Z - Partition Master Encryption Key (PXMEKY): Z - Partition Password Encryption Key (PXPEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition Masking Key (PXMSKY): Z - Partition User Login Password Data (PULPDA): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z PCO - HSM Master Encryption Key (HXMEKY): E - Partition Master Encryption Key (PXMEKY): G - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E Pre-CO - Partition Master Encryption Key (PXMEKY): G - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Vendor Firmware Update Validation Key Public ECC (HVFUVKYPUBECC): E
GP_PARTITION_SSP_MGMT	Provides services to manage user and master partition SSPs	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	KAS-KDA-HKDF (SP800-56Ar3) SW-AES-GCM-Wrap SW-AES-GCM-Unwrap SW-KAS-ECC (KAS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST SW-AES-GMAC SW-AES-	MCO - HSM Owner Attestation Key Public (HOOATKYPUB): W - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): E - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): E - Partition User General Purpose Symmetric Key (PUGPSKY): E - Partition User General Purpose Symmetric Session Key (PUGPSSK): E - Partition User General Purpose HMAC Key (PUGPMKY): E - Partition User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-Counter-DRBG SW-ECDSA-KeyGen (FIPS186-4) SW-ECDSA-KeyVer (FIPS186-4) SW-ECDSA-SigGen (FIPS186-4) SW-ECDSA-SigVer (FIPS186-4) CPT-HMAC-SHA-1 SW-HMAC-SHA-1 CPT-HMAC-SHA2-224 SW-HMAC-SHA2-224 CPT-HMAC-SHA2-256 SW-HMAC-SHA2-256 CPT-HMAC-SHA2-384 SW-HMAC-	General Purpose HMAC Session Key (PUGPMSK): E - Partition User General Purpose Key Public (PUGPKYPUB): E - Partition Authentication Certificate (PXPACT): E - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - HSM Owner Recovery Key (HOREKY): W - HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC): E - HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC): E PCO - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): E - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): E - Partition User General Purpose Symmetric Key (PUGPSKY): E - Partition User General Purpose Symmetric Session Key (PUGPSSK): E - Partition User General Purpose HMAC Key (PUGPMKY): E - Partition User General Purpose HMAC Session Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA2-384 CPT-HMAC-SHA2-512 SW-HMAC-SHA2-512 SW-KAS-ECC-Sp800-56Ar3 SW-KDA-HKDF-Sp800-56Cr1 SW-KDF-ANS-9.63 SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-SHA2-256	(PUGPMSK): E - Partition User General Purpose Key Public (PUGPKYPUB): E - Partition Authentication Certificate (PXPACT): E - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E
GP_PARTITION_TIME_MGMT	Provides services to manage user time	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs		MCO Unauthenticated
GP_LICENSE_MGMT	Provides services to manage license of the software running on the HSM	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-RSA-SigVer (FIPS186-5) SW-RSA-SigGen (FIPS186-5) SW-SHA2-256	MCO - HSM Vendor License Key Public RSA (HVLICKYPUBRSA): E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E
GP_QUORUM_CONTROL	Provides quorum control (MofN) services	Success with fips_stat	Opcode Inputs	Opcode Outputs	ENT (P) (SP 800-90B) SW-	Pre-CO PCO - Partition DRBG CTR V State

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		e = 2 or 3			Counter-DRBG SW-RSA-SigVer (FIPS186-5)	(PXDRBGCTVST): G,E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG CTR Key State (PXDRBGCTKST): G,E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA) : E PCU - Partition DRBG CTR V State (PXDRBGCTVST): G,E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG CTR Key State (PXDRBGCTKST): G,E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA) : E
GP_USER_MGMT	Provides services to manage user accounts and	Success with fips_stat	Opcode Inputs	Opcode Outputs	ENT (P) (SP 800-90B) KAS-	PCU - Partition Password Encryption Key (PXPEKY): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	roles within the HSM.	e = 2 or 3			KDA-ONESTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2) CPT-AES-CBC-ENC CPT-AES-CBC-DEC SW-AES-KWP-Unwrap (KTS) CPT-Hash-DRBG SW-KDF-SP800-108 SW-PBKDF SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5)	- Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA) : E - Partition User TLS E2E Client Authentication Certificate (PUTLSE2ECACT): E - Partition User Login Password Data (PULPDA): W,E,Z - Partition Master Encryption Key (PXMEKY): E MCO - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA) : E - Partition Password Encryption Key (PXPEKY): E,G - Partition Master Encryption Key (PXMEKY): E - Partition User Login Password Data (PULPDA): W,E,Z - Partition Authentication Certificate (PXPACT): E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB): Z,E,W - Partition Password Encryption Key Shared Secret (PXPESZ): Z,G,E PCO - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA) : E,W - Partition Password Encryption Key (PXPEKY): E,G - Partition Master Encryption Key (PXMEKY): E - Partition User Login Password Data (PULPDA): Z,E,W - Partition Authentication Certificate (PXPACT): E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB): Z,E,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Password Encryption Key Shared Secret (PXPESZ): Z,G,E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z AU - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E - Partition Password Encryption Key (PXPEKY): E - Partition Master Encryption Key (PXMEKY): E - Partition User Login Password Data (PULPDA): E,Z,W Pre-CO - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E - Partition Password Encryption Key (PXPEKY): E - Partition Master Encryption Key (PXMEKY): E - Partition User Login Password Data (PULPDA): E,Z,W Unauthenticated - FIPS Partition HSM Owner Authentication

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate RSA (FPHOOAUCTRSA): E - Partition Owner Authentication Certificate (POOAUCT): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - Partition Data Encryption Key (PXDEKY): E
GP_BACKUP_RESTORE	Provides Backup/Restore services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-KeyGENT (P) (SP 800-90B) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-CBC-UNWRAP SW-AES-CBC-WRAP SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-Counter-	MCO - Partition Backup Ephemeral Key (PXKBEK): G,E,W,R - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): R,W - Partition Password Encryption Key (PXPEKY): R,W - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): R,W - Partition User General Purpose Symmetric Key (PUGPSKY): R,W - Partition User General Purpose HMAC Key (PUGPMKY): R,W - Partition User General Purpose Key Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DRBG CPT-Hash-DRBG CPT-HMAC-SHA2-256 SW-KDF-SP800-108 SW-SHA2-256	(PUGPKYPUB): R,W - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E - HSM Owner Recovery Key (HOREKY): E - Partition Data Encryption Key (PXDEKY): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): R - Partition Authentication Certificate (PXPACT): R - Partition Masking Key (PXMSKY): R,W - Partition User Login Password Data (PULPDA): R,W PCO - Partition Backup Ephemeral Key (PXKBEK): G,E,R,W - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): R,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Password Encryption Key (PXPEKY): R,W - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): R,W - Partition User General Purpose Symmetric Key (PUGPSKY): R,W - Partition User General Purpose HMAC Key (PUGPMKY): R,W - Partition User General Purpose Key Public (PUGPKYPUB): R,W - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E - HSM Owner Recovery Key (HOREKY): E - Partition Data Encryption Key (PXDEKY): E - Partition User Login Password Data (PULPDA): R,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
GP_KBK_MGMT	Provides service to manage Key Backup Key (KBK)	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-CBC-UNWRAP SW-AES-CBC-WRAP SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KDF-SP800-108	MCO - HSM Owner Trust Anchor Certificate (HOOTACT): G,E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): G,E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Owner Recovery Key (HOREKY): E PCO - Partition Key Backup Key (PXKBKY): W,R,E - Partition Cert Auth Ephemeral Key (PXCAEK): E - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): W,R,E - Partition Data Encryption Key (PXDEKY): E
GP_AUDIT_LOG_MGMT	Provides audit log services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	CPT-SHA2-256 CPT-RSA-Signature-Primitive	PCO - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E AU - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E MCO
GP_INFO_DIAGNOSTIC	Provides info and diagnostic services including Get Status, Get Version and Run Self-tests.	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-GCM-Wrap SW-AES-GCM-Unwrap SW-AES-GCM-Enc	MCO - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E PCO - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E PCU

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SW-AES-GCM-Dec SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) LEGACY-SW-TDES-KW (KTS) LEGACY-CPT-AES-CBC-UNWRAP LEGACY-CPT-AES-ECB-UNWRAP CPT-AES-CCM-ENC CPT-AES-CCM-DEC CPT-AES-CMAC CPT-AES-ECB-ENC CPT-AES-ECB-DEC CPT-AES-GCM-ENC CPT-AES-GCM-DEC SW-AES-KWP-Wrap	- FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): EAU - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E Unauthenticated - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(KTS) SW-AES-KWP-Unwrap (KTS) SW-Counter-DRBG SW-ECDSA-KeyVer (FIPS186-4) CPT-ECDSA-SigGen (FIPS186-4) SW-ECDSA-SigGen (FIPS186-4) CPT-ECDSA-SigVer (FIPS186-5) SW-ECDSA-SigVer (FIPS186-4) CPT-Hash-DRBG CPT-HMAC-SHA-1 SW-HMAC-SHA-1 SW-HMAC-SHA2-224 CPT-HMAC-SHA2-224 CPT-HMAC-SHA2-256 SW-HMAC-SHA2-256	

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CPT-HMAC-SHA2-384 SW-HMAC-SHA2-384 CPT-HMAC-SHA2-512 SW-HMAC-SHA2-512 SW-HMAC-SHA3-224 CPT-HMAC-SHA3-224 CPT-HMAC-SHA3-256 CPT-HMAC-SHA3-384 CPT-HMAC-SHA3-512 SW-HMAC-SHA3-256 SW-HMAC-SHA3-384 SW-HMAC-SHA3-512 SW-KAS-ECC-Sp800-56Ar3 CPT-KAS-ECC-SSC-Sp800-56Ar3	

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SW-KAS-ECC-SSC-Sp800-56Ar3 SW-KAS-IFC-SSC CPT-KDF-SP800-108 SW-KDF-SP800-108 CPT-KDF-TLS SW-PBKDF CPT-RSA-Decryption-Primitive SW-RSA-Decryption-Primitive SW-RSA-SigGen (FIPS186-5) CPT-RSA-Signature-Primitive SW-RSA-Signature-Primitive SW-RSA-SigVer (FIPS186-5) CPT-SHA-1 SW-SHA-1 CPT-SHA2-256 SW-SHA2-256 CPT-SHA2-	

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					512 SW-SHA2-512 SW-SHAKE-128 SW-SHAKE-256 CPT-TDES-CBC SW-SHA3-224 SW-SHA3-256 SW-SHA3-384 SW-SHA3-512	
GP_E2E	Provides e2e services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-GCM-Wrap SW-AES-GCM-Unwrap SW-ECDSA-KeyGen (FIPS186-4) FW-ECDSA-KeyGen (FIPS186-5) SW-ECDSA-SigVer (FIPS186-4) CPT-Hash-DRBG CPT-KAS-ECC-SSC-Sp800-56Ar3 CPT-RSA-	Unauthenticated - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): E - Partition TLS E2E Pre Master Secret (PXTLSE2EPMS): Z,G,E - Partition TLS E2E Master Secret Key (PXTLSE2EMSKY): G,E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): G - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Signature-Primitive SW-RSA-SigVer (FIPS186-5) SW-SHA2-512 ENT (P) (SP 800-90B) KAS-TLS (Sp800-56Ar3)	(PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC): G - Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EEKPUBECC): G,R - Partition Owner Authentication Certificate (POOAUCT): R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition User TLS E2E Client Authentication Certificate (PUTLSE2ECACT): E,W - Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC): E,W
GP_SESSION_MGMT	Provides services to manage sessions and tokens	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-RSA-SigVer (FIPS186-5) CPT-Hash-DRBG SW-PBKDF SW-AES-KWP-Unwrap (KTS) ENT (P) (SP 800-90B)	Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - Partition Password Encryption Key (PXPEKY): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E - Partition User Login Password Data (PULPDA): E MCO - Partition Backup Ephemeral Key (PXKBEK): Z - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E PCO - Partition Backup Ephemeral Key (PXKBEK): Z - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): Z - Partition TLS E2E Master Secret Key (PXTLSE2EMSKY): Z PCU - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): Z - Partition TLS E2E Master Secret Key (PXTLSE2EMSKY): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						AU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E
GP_KEY_MGMT	Provides services to manage keys	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-KeyGen ENT (P) (SP 800-90B) KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2) SW-AES-GCM-Wrap SW-AES-	MCO - HSM Owner Trust Anchor Certificate (HOOTACT): E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Owner Recovery Key (HOREKY): E PCO - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Data Encryption Key (PXDEKY): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					GCM-Unwrap SW-KAS-ECC (KAS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-KTS-IFC-Encap (KTS) SW-KTS-IFC-Decap (KTS) LEGACY-SW-TDES-KW (KTS) FW-KTS-IFC-Encap (KTS) FW-KTS-IFC-Decap (KTS) LEGACY-SW-AES-CBC-UNWRAP LEGACY-SW-AES-ECB-UNWRAP LEGACY-CPT-AES-CBC-UNWRAP LEGACY-CPT-AES-ECB-UNWRAP	- Partition User General Purpose Key Public (PUGPKYPUB): Z,R,E,W - Partition User General Purpose Session Key Public (PUGPSKYPUB): R,E,W - Partition Master Encryption Key (PXMEKY): E - Partition Key Loading Key (PXKLKY): G - Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV): Z,G,E - Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB): Z,G,E,R - Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB): Z,E,W - Partition Key Loading Key Shared Secret (PXKLSZ): Z,G,E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST CPT-AES-CBC-ENC CPT-AES-CBC-DEC SW-AES-CMAC SW-AES-GMAC SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-Counter-DRBG SW-ECDSA-KeyGen (FIPS186-4) FW-ECDSA-KeyGen (FIPS186-5) SW-ECDSA-KeyVer (FIPS186-4) CPT-Hash-DRBG CPT-HMAC-SHA-1 SW-HMAC-SHA-1 CPT-HMAC-	E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z,E - Partition User General Purpose Symmetric Key (PUGPSKY): Z,E - Partition User General Purpose HMAC Key (PUGPMKY): Z,E PCU - Partition User General Purpose Key Public (PUGPKYPUB): Z,W,G,E,R - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z,W,G,E,R - Partition Master Encryption Key (PXMEKY): E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z,W,G,E,R - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z,W,G,E,R - Partition User General Purpose Symmetric Key (PUGPSKY): Z,W,G,E,R - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z,W,G,E,R - Partition User General Purpose HMAC Key (PUGPMKY): Z,W,G,E,R - Partition User General Purpose

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA2-224 SW-HMAC-SHA2-224 CPT-HMAC-SHA2-256 SW-HMAC-SHA2-256 CPT-HMAC-SHA2-384 SW-HMAC-SHA2-384 CPT-HMAC-SHA2-512 SW-HMAC-SHA2-512 SW-KAS-ECC-SSC-Sp800-56Ar3 SW-KDA-HKDF-Sp800-56Cr1 SW-KDA-OneStep-Sp800-56Cr1 SW-KDA-TwoStep-Sp800-56Cr1 SW-KDF-ANS-9.63 SW-KDF-SP800-108 SW-RSA-	HMAC Session Key (PUGPMSK): Z,W,G,E,R - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition Key Loading Key (PXKLKY): E - Partition Wrap Unwrap Shared Secret (PXWUSZ): Z,E Pre-CO - Partition Key Loading Key (PXKLKY): G,W - Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV): Z,G,E - Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB): Z,G,E - Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB): Z,E,W - Partition Key Loading Key Shared Secret (PXKLSZ): Z,G,E - FIPS Octeon HSM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KeyGen (FIPS186-5) FW-RSA-KeyGen (FIPS186-5) FW-RSA-SigVer (FIPS186-5) UB-RSA-SigVer (FIPS186-4) SW-RSA-SigVer (FIPS186-5) SW-SHA-1 SW-SHA2-256 SW-SHA2-384 SW-SHA2-512	DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition Master Encryption Key (PXMEKY): E AU - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z,E - Partition User General Purpose Symmetric Key (PUGPSKY): Z,E - Partition User General Purpose HMAC Key (PUGPMKY): Z,E - Partition User General Purpose Key Public (PUGPKYPUB): Z,E,R - Partition User General Purpose Session Key Public (PUGPSKYPUB): R - Partition Wrap Ephemeral Key Private (PXWEKPRV): G,E,Z - Partition Wrap Ephemeral Key Public (PXWEKPUB): G,R,Z - Partition User Wrap

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Unwrap Ephemeral Key Public (PUWUEKPUB): G,R,Z - Partition Wrap Unwrap Encryption Ephemeral Key (PXWUEEK): G,E,Z - Partition Wrap Unwrap Intermediate Ephemeral Key (PXWUIEK): G,W,E,Z Unauthenticated - Partition User General Purpose Key Public (PUGPKYPUB): R - Partition User General Purpose Session Key Public (PUGPSKYPUB): R
GP_POLICY_MGMT	Provides services to HSM/Partition policies	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs		MCO PCO Pre-CO PCU AU Unauthenticated
GP_CRYPTO_FASTPATH	Provides crypto/fastpathservices	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	LEGACY-CPT-TDES-ECB CPT-RSA-Decryption-Primitive CPT-Hash-DRBG CPT-SHA2-512 SW-AES-CMAC CPT-SHA3-512 CPT-AES-CBC-ENC CPT-AES-CBC-DEC CPT-	PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E,G - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): E - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): E - Partition User General Purpose Key Public (PUGPKYPUB): E - Partition User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA-1 CPT-SHAKE-128 CPT-SHAKE-256 CPT-SHA2-256 CPT-AES-GMAC CPT-AES-CCM-ENC CPT-AES-CCM-DEC CPT-SHA3-256 CPT-AES-ECB-ENC CPT-AES-ECB-DEC CPT-HMAC-SHA2-256 CPT-RSA-Signature-Primitive CPT-SHA2-224 CPT-SHA2-384 CPT-AES-GCM-ENC CPT-AES-GCM-DEC CPT-SHA3-224 CPT-	General Purpose Session Key Public (PUGPSKYPUB): E - Partition User General Purpose HMAC Key (PUGPMKY): E - Partition User General Purpose HMAC Session Key (PUGPMSK): E - Partition User General Purpose Symmetric Key (PUGPSKY): E - Partition User General Purpose Symmetric Session Key (PUGPSSK): E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): E PCO - Partition TLS E2E Symmetric Key (PXTLSE2EKY): E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E Pre-CO - Partition TLS E2E Symmetric Key (PXTLSE2EKY): E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E Unauthenticated - Partition TLS E2E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					AES-CTR-ENC CPT-AES-CTR-DEC CPT-ECDSA-SigGen (FIPS186-4) CPT-HMAC-SHA2-384 CPT-HMAC-SHA2-512 CPT-SHA3-384 SW-KAS-ECC (KAS) ENT (P) (SP 800-90B) CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST SW-KDF-ANS-9.63 SW-AES-GMAC	Symmetric Key (PXTLSE2EKY): E - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E
GP_ZEROIZATION	Provides zeroization services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)	MCO - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Symmetric Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - HSM Master Encryption Key (HXMEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Key Backup Key (PXKBKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Masking Key (PXMSKY): Z - Partition Authentication Certificate (PXPACT): Z - Partition Password Encryption Key (PXPEKY): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): Z - HSM Owner Attestation Key Public (HOOATKYPUB): Z - Partition User Login Password Data (PULPDA): Z - HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC): Z - HSM Owner Recovery Key (HOREKY): Z - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): Z - FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC): Z - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): Z - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): Z - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): Z - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): Z - HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC): Z - HSM Manufacturer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Hardware Unique 2 Key (HMHU2KY): E,Z - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): Z - HSM Owner Trust Anchor Certificate (HOOTACT): Z - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): Z PCO - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Authentication Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private RSA (PXPAKYPRVRSA): Z - Partition Masking Key (PXMSKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Owner Authentication Certificate (POOAUCT): Z - HSM Master Encryption Key (HXMEKY): E PCU - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Data

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key (PXDEKY): Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Masking Key (PXMSKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Owner Authentication Certificate (POOAUCT): Z AU - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - Partition Master Encryption Key (PXMEKY): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Data Encryption Key (PXDEKY): Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Masking Key (PXMSKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Owner Authentication Certificate (POOAUCT): Z Pre-CO - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - HSM Master Encryption Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(HXMEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Key Backup Key (PXKBKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Masking Key (PXMSKY): Z - Partition Authentication Certificate (PXPACT): Z - Partition Password Encryption Key (PXPEKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): Z - HSM Owner Attestation Key Public (HOOATKYPUB): Z - Partition User Login Password Data (PULPDA): Z Unauthenticated - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PUGPASKPRV): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose Session Key Public (PUGPSKYPUB): Z - HSM Master Encryption Key (HXMEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Key Backup Key (PXKBKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Masking Key (PXMSKY): Z - Partition Authentication Certificate (PXPACT): Z - Partition Password Encryption Key (PXPEKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Owner Authentication Certificate (POOAUCT): Z - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): Z - HSM Owner Attestation Key Public (HOOATKYPUB): Z - Partition User Login Password Data (PULPDA): Z
GP_CERT_AUTH	Provides cert auth services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	CPT-KeyGen SW-ECDSA-SigVer (FIPS186-4) CPT-Hash-DRBG SW-KAS-IFC-SSC SW-KDF-SP800-108 SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) ENT (P) (SP 800-90B)	PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - HSM Owner Trust Anchor Certificate (HOOTACT): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E,R - Partition Owner Trust Anchor Certificate

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(POOTACT): W,E,R - Partition Owner Authentication Certificate (POOAUCT): W,E,R - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Target Shared Secret (PXCATSZ): G,Z,E,W - Partition Cert Auth Ephemeral Key (PXCAEK): G - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): Z,W,R PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - FIPS Partition HSM Manufacturer Master Authentication

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate RSA (FPHMMACTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - HSM Owner Trust Anchor Certificate (HOOTACT): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E,R - Partition Owner Trust Anchor Certificate (POOTACT): E,R - Partition Owner Authentication Certificate (POOAUCT): E,R - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Target Shared Secret (PXCATSZ): G,Z,E,W - Partition Cert Auth Ephemeral Key (PXCAEK): G - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): R AU - FIPS Octeon HSM DRBG Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - HSM Owner Trust Anchor Certificate (HOOTACT): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E,R - Partition Owner Trust Anchor Certificate (POOTACT): E,R - Partition Owner Authentication Certificate (POOAUCT): E,R - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Target Shared Secret (PXCATSZ): G,Z,E,W - Partition Cert Auth Ephemeral Key (PXCAEK): G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): R Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): E - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - HSM Owner Trust Anchor Certificate (HOOTACT): W,E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): W,E,R - Partition Owner Trust Anchor Certificate (POOTACT): E,R - Partition Owner Authentication

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate (POOAUCT): E,R - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Target Shared Secret (PXCATSZ): G,Z,E,W - Partition Cert Auth Ephemeral Key (PXCAEK): G - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): R MCO - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): R - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): R - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Owner Authentication Certificate RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(FPHOOAUCTRSA): W,R - HSM Owner Trust Anchor Certificate (HOOTACT): W,E,R Pre-CO - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): R - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): R - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): R - Partition Owner Authentication Certificate (POOAUCT): W,R - Partition Owner Trust Anchor Certificate (POOTACT): W,R - Partition Authentication Certificate (PXPACT): R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): W,R
GP_CLONING	Provides cloning services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	CPT-KeyGen KAS-KDA-ONESTE	PCO - Partition Password Encryption Key (PXPEKY): W,R - Partition Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					P (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) CPT-AES-CBC-ENC CPT-AES-CBC-DEC SW-AES-CMAC SW-ECDSA-KeyGen (FIPS186-4) SW-ECDSA-KeyVer (FIPS186-4) CPT-Hash-DRBG SW-HMAC-SHA2-512 SW-KDA-HKDF-Sp800-56Cr1 SW-KDF-SP800-108 SW-PBKDF SW-RSA-KeyGen (FIPS186-5) SW-	Loading Key (PXKLKY): W,R - Partition Masking Key (PXMSKY): W,E,R,G - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition Master Encryption Key (PXMEKY): E - Partition Cloning Ephemeral Key Private (PXCLEKPRV): Z,G,E - Partition Cloning Ephemeral Key Public (PXCLEKPUB): Z,G,R - Partition Cloning Shared Secret (PXCLSZ): Z,G,E - Partition Cloning Encryption Ephemeral Key (PXCLEEK): Z,G,E - Partition Cloning MAC Ephemeral Key (PXCLMEK): Z,G,E - Partition User Cloning Ephemeral Key Public (PUCLEKPUB): Z,E,W PCU - Partition User General Purpose Asymmetric Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA-1 SW-SHA2-256 ENT (P) (SP 800-90B)	Private (PUGPAKYPRV): W,R - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): W,R - Partition User General Purpose Symmetric Key (PUGPSKY): W,R - Partition User General Purpose Symmetric Session Key (PUGPSSK): W,R - Partition User General Purpose HMAC Key (PUGPMKY): W,R - Partition User General Purpose HMAC Session Key (PUGPMSK): W,R - Partition User General Purpose Key Public (PUGPKYPUB): W,R - Partition User General Purpose Session Key Public (PUGPSKYPUB): W,R - Partition Masking Key (PXMSKY): E - Partition Master Encryption Key (PXMEKY): E AU - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): W,R - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): W,R - Partition User General Purpose Symmetric Key (PUGPSKY): W,R - Partition User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						General Purpose Symmetric Session Key (PUGPSSK): W,R - Partition User General Purpose HMAC Key (PUGPMKY): W,R - Partition User General Purpose HMAC Session Key (PUGPMSK): W,R - Partition User General Purpose Key Public (PUGPKYPUB): W,R - Partition User General Purpose Session Key Public (PUGPSKYPUB): W,R - Partition Masking Key (PXMSKY): E - Partition Password Encryption Key (PXPEKY): W,R - Partition Key Loading Key (PXKLKY): W - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST): G,E,Z - FIPS Octeon HSM DRBG Seed (FOHXDRBGSD): G,E,Z - FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON): G,E,Z - Partition DRBG Hash C State (PXDRBGHACST): E - Partition DRBG Hash V State (PXDRBGHAVST): E - Partition Master Encryption Key (PXMEKY): E

Table 15: Approved Services

4.4 Non-Approved Services

All approved services implemented by the Module are listed in the table below:

Name	Description	Algorithms	Role
CN_GENERATE_PBE_KEY	Generate PBE DES3 key with the given password, salt, and iteration count. Make sure that HSM is initialized with fips_state=0.The fips_state parameter can be found in the hsm_configfile.	SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant) PBE	PCU
LSPAY_GENERATE_ASYMM_KEY	Generates RSA KEY Pair (mod_len>= 2048-bit). Generates EC KEY PAIR (Curves: Nist P256, 224, 384, 521, Brain pool (Curves: P160, P192, P224, P256, P320, P384, P512), x25519/448 and Secp256K1 and FRP256v1)	RSA (non-compliant) ECDSA (non-compliant)	PCU
LSPAY_GENERATE_SYMM_KEY	Generates symmetric key AES, TDEA keys used for LSPay operations	SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant)	PCU
LSPAY_EXPORT_PUBLIC_KEY	Exports public key for BYOK.		PCU
LSPAY_IMPORT_KPK	Imports OAEP wrapped or ECDH_AES_PAD wrapped symmetric key.	EC-AES ECDH KDF RSA (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_IMPORT_TR34_KEY	Import symmetric keys using TR- 34 unwrap.	RSA (non-compliant)	PCU
LSPAY_EXPORT_KEY	Exports symmetric key wrapped with TR31,AES_CBC/ AES_CBC_PAD.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_EXPORT_TR34_KEY	Exports symmetric keys wrapped with TR34 mechanism	RSA (non-compliant)	PCU
LSPAY_TRANSLATE_KEY	Translates wrapped key from one KPK to another KPK.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_IMPORT_CERTIFICATE	Imports peer's certificate to read public key required in TR34. Import X901 certificate into HSM.		PCU
LSPAY_IMPORT_DECIMAL_TABLE	Imports encrypted decimal table to be used in PIN APIs to decimalize native PIN.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_GENERATE_CSR	Create CSR with given key pair.	RSA (non-compliant) ECDSA (non-compliant)	PCU
LSPAY_DERIVE_KEY	Derives DUKPT working key from the BDK.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_ENCRYPT	Encrypts input data or PIN.	AES (non-comp	PCU

Name	Description	Algorithms	Role
		liant) Triple-DES (non-compliant)	
LSPAY_DECRYPT	Decrypts input data or PIN.	AES (non-compliant) Double-DES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_DECRYPT_THEN_ENCRYPT	Decrypts the input cipher text with one key and encrypts with another key.	AES (non-compliant) Double-DES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_MAC_GEN	Computes MAC on input data. Algorithm used: DES/Triple-DES	DES MAC (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_MAC_VERIFY	Verifies MAC with calculated AMC on input data.	DES MAC (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_MAC_TRANSLATE	Translates MAC by using new key on input data.	DES MAC	PCU

Name	Description	Algorithms	Role
		(non-compliant) Triple-DES (non-compliant)	
LSPAY_FPE_ENCRYPT	Performs FPE FF1/FF3-1 encrypt operation on input data.	AES (non-compliant)	PCU
LSPAY_FPE_DECRYPT	Performs FPE FF1/FF3-1 decrypt operation on input data.	AES (non-compliant)	PCU
LSPAY_SIGN	Performs sign and verify on input data.	ECDSA (non-compliant) RSA (non-compliant)	PCU
LSPAY_SIGN_VERIFY	Verifies sign on input data.	ECDSA (non-compliant) RSA (non-compliant)	PCU
LSPAY_PINBLK_TRANSLATE	Decrypts the input PIN using decryption key, translates to given PIN format and encrypts with another key.	AES (non-compliant) Triple-DES (non-compliant) RSA (non-compliant)	PCU
LSPAY_DERIVE_PIN_FROM_OFFSET	Derive PIN from given offset. Encrypts validation data with DES EDE. Derives native PIN, then offset will be added to derive IBM PIN. PIN will be encoded in given ISO format. Encrypt encoded PIN with PIN encryption key.	AES (non-compliant) Triple-DES (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_DERIVE_OFFSET_FROM_PIN	Generates IBM offset from given PIN. Decrypt and decode received PIN. Generate native from given validation data. Subtract decoded PIN from native PIN t to get PIN offset.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_VERIFY_PIN	Verifies given PIN .Decrypt and decode received PIN. Generate native from given validation data. Add offset to native PIN. Compare resultant PIN with received PIN.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_PVV_GEN	Perform PVV generation on PIN and PAN data.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_PVV_VERIFY	Verifies given PVV.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_EMV_GENVERIFY	Perform EMV crypto operations. Generate ARPC. Generate or Verify ARQC.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_EMV_SECURE_MSG_GEN	Generates MAC over secure message.	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_CVV_GEN	Generates CVV, CVV2,iCVVon given card details.	AES (non-compliant)	PCU

Name	Description	Algorithms	Role
		Triple-DES (non-compliant)	
LSPAY_CVV_VERIFY	Verifies CVV with given card details	AES (non-compliant) Triple-DES (non-compliant)	PCU
LSPAY_KEY_SHARE_CREATE	Creates components of Key	Shamir Key Share (non-compliant)	PCU
LSPAY_KEY_SHARE_EXPORT_COMPONENT	Exports created components in encrypted format	AES (non-compliant)	PCU
LSPAY_KEY_SHARE_COMBINE_INIT	Starts combine keyinit.		PCU
LSPAY_KEY_SHARE_COMBINE_KEY	Combines all components of the key.	Shamir Key Share (non-compliant)	PCU
LSPAY_KEY_SHARE_ZEROIZE	Erases all components of the key.		PCU
LSPAY_MFK_GENERATE	Generates MFK key.	SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant)	PCO
LSPAY_MFK_GET_INFO	Returns MFK information for partition.		PCO
LSPAY_MFK_SET_PRIMARY	Sets MFK as primary.		PCO
LSPAY_MFK_DELETE	Deletes MFK.		PCO

Name	Description	Algorithms	Role
LSPAY_FUNCTIONALITY_GET	Gets status of enabled/disabled LSPay services		PCO
LSPAY_FUNCTIONALITY_SET	Enable/Disable services		PCO
LSPAY_EXPORT_KPK	Export a Key Block Protection Key (KBPK)	EC-AES ECDH KDF RSA (non-compliant)	PCU
LSPAY_IMPORT_PUBLIC_KEY	Import an RSA public key	RSA (non-compliant)	PCU
LSPAY_VALIDATE_PUBLIC_KEY	Validates the RSA public key	RSA (non-compliant)	PCU
CN_GENERATE_KEY_PAIR (non-compliant)	Generates asymmetric keys (RSA/ ECC). Updates the public and private key handles in the output on return. Caveats in Non Approved apart from approved mode: RSA 1024 bits allowed along with all odd public exponent i.e. even lesser than 65537.NID_X9_62_prime192v1/NID_sect163k1/NID_ED25519/NID_sect163r2/NID_secp192k1/NID_brainpoolP160r1/NID_brainpoolP192r1/NID_X25519/NID_X448	ECDSA (non-compliant) KAS-ECC (non-compliant) RSA (non-compliant)	PCU
CN_GENERATE_KEY (non-compliant)	Generates a symmetric key of given key type and length. Caveats in Non-Approved apart from approved mode:DES token key is allowed.	SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant)	PCU
CN_CREATE_OBJECT (non-compliant)	Imports a public key into HSM. Caveats in Non Approved apart from approved mode:RSA-1024 bits allowed, NID_ED25519/NID_secp192k1/NID_brainpoolP160r1/NID_brainpoolP192r1/NID_X25519/NID_X448		PCU
CN_UNWRAP_KEY (non-compliant)	Unwraps a key with an AES/Triple-DES/RSA private key existing on HSM or KLK. Takes the output wrapped data of wrapKey2 command. Caveats in Non Approved apart from approved mode:RSA-1024 bit, RSAPKCS1V1.5 Unwrap,NID_X9_62_prime192v1/	EC-AES ECDH KDF	PCU

Name	Description	Algorithms	Role
	NID_sect163k1/NID_ED25519/NID_sect163r2/NID_secp192k1/NID_brainpoolP160r1/NID_brainpoolP192r1/NID_X25519/NID_X448,Triple-DES	RSA (non-compliant) Triple-DES (non-compliant)	
CN_WRAP_KEY (non-compliant)	Wraps sensitive (private and symmetric) keys from the HSM to the host. Caveats in Non Approved apart from approved mode: AES-ECB mode, AES-CBC mode, AES-CBC-PAD mode, Triple-DES ECB mode, Triple-DES CBC mode, Triple-DES NIST Wrap mode, RSA-PKCS1V1.5 Wrap	AES (non-compliant) RSA (non-compliant) Triple-DES (non-compliant)	PCU
CN_EXTRACT_MASKED_OBJECT (non-compliant)	Extracts a masked object; i.e., retrieves an object by wrapping it with a masking key shared by the process of cloning.	AES (non-compliant)	PCU,PCO,AU
CN_STORE_FW_SIGNING_KEY (non-compliant)	Configure an RSA or EC public key into HSM as AO attestation key. These keys can be of modulus 1024, 2048, 3072, and 4096 or a supported 256 bits, 384 bits or 521 bits EC curve. Caveats in Non Approved is 192-bit curves supported	ECDSA (non-compliant) RSA (non-compliant)	MCO
MAJOR_OP_ME_PKCS_LARGE (non-compliant)/MAJOR_OP_ME_PKCS (non-compliant)	PKCS#1v1.5 encrypt and decrypt	RSA (non-compliant)	PCU
CN_STORE_VENDOR_PRE_SHARED_KEY (CN_STORE_KBK_SHARE) (non-compliant)	Stores fixed keys (KBK) for backup. Including PKCS#1v1.5	AES (non-compliant) RSA (non-compliant)	MCO
CN_INSERT_MASKED_OBJECT (non-compliant)	Inserts a masked object into an HSM that is extracted from another HSM.	AES (non-compliant) Triple-DES (non-compliant)	PCU,PCO,AU

Name	Description	Algorithms	Role
CN_ENCRYPT_SESSION (non-compliant)	Enables encrypted communication channel. Caveat is Non Approved mode allow the additional Cipher suite E2E_RSA_AES128_GCM_SHA256	EC-AES ECDH KDF RSA (non-compliant)	Unauthenticated
CN_ENCRYPT_SESSION_V2 (non-compliant)	Enables encrypted communication channel. Caveat is Non Approved mode allow the additional nonapproved cipher suites	EC-AES ECDH KDF RSA (non-compliant)	Unauthenticated
CN_DERIVE_KEY (non-compliant)	Derives a key using a supported KDF mechanism with the params given by the user.	AES (non-compliant) EC-AES ECDH KDF RSA (non-compliant) Triple-DES (non-compliant)	PCU
CN_PQC_CRYPTO_HYBRID_SIG_GEN (non-compliant)	Generates a signature using ML-DSA and ECDSA sign algorithm.	ML-DSA ECDSA Sign (non-compliant)	PCU
CN_PQC_CRYPTO_HYBRID_SIG_VERIFY (non-compliant)	Verifies a signature using ML-DSA and ECDSA sign algorithm.	ML-DSA ECDSA Verify (non-compliant)	PCU

Table 16: Non-Approved Services

The non-approved services will fail FIPS POLICY MISMATCH when partition is operated in the approved mode.

4.5 External Software/Firmware Loaded

The module uses the following services to upload the signed firmware to update the module using RSA 2048 signatures and SHA2-256:

- GP_PARTITION_MGMT - CN_FW_UPDATE_BEGIN: This service initiates the firmware update process.
- GP_PARTITION_MGMT - CN_FW_UPDATE: This service proceeds with the actual firmware image transfer. It manages the data transfer securely, ensuring that the firmware data is correctly received and written.
- GP_PARTITION_MGMT - CN_FW_UPDATE_END: This service concludes the firmware update process. It performs integrity checks such as verifying digital signatures to ensure that the firmware has been correctly and securely updated.

During the firmware update process the data is inhibited.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following firmware component(s):

- Component 1: executable – binary
- Component 2: non-modifiable operating system – binary

Firmware integrity is verified by the bootloader during the boot up using EDC (CRC32) for itself and using RSA 2048 signatures and SHA2-256 for next level image. The integrity test can be run on-demand by resetting the module by power-cycling it or by PCIe function reset.

As part of firmware load operation, the new firmware's integrity and authenticity is verified by the active firmware using RSA 2048 signatures and SHA2-256.

5.2 Initiate on Demand

Reboot the HSM for the firmware integrity on demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The Module has a limited operational environment and has been assessed for Physical Security at Level 3 under the FIPS 140-3 definitions. Therefore per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section is not applicable.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Epoxy Coating	12 Months	Examine surface of module for scratched or damaged epoxy, especially if circuitry shows.
Battery life	6 Months	If the HSM has not been powered on in the last six months, then power it on for at least an hour.

Table 17: Mechanisms and Actions Required

The module's cryptographic boundary is defined to be the outer perimeter of the hard epoxy enclosure containing the hardware and firmware components. The module is opaque and completely conceals the internal components of the cryptographic module. The epoxy enclosure of the module prevents physical access to any of the internal components without having to destroy the module. There is no operator required actions.

The module is coated in hard epoxy, such that any physical breach attempt leaves behind evidence of tamper. This is shown in the figure below

While the module is designed to prevent successful tampering (any physical breach to module circuitry is likely to destroy the module, as per FIPS 140-3 Level 3 Physical Security requirements), the module should still be checked periodically for attempts. Guidelines are provided in the table above.

If the module is found to be meaningfully damaged or tampered with (e.g., circuitry is showing or other significant damage has occurred), it should be removed from use and destroyed.

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-20C (+/- 2C)	EFP	Shutdown
HighTemperature	47C	EFP	Shutdown
LowVoltage	2.998V (PCIe 3.3V Aux), 3.132V (PCIe 3.3V Rail), 11.926V (PCIe 12V Rail)	EFP	Shutdown
HighVoltage	3.658V (PCIe 3.3V Aux), 3.794V (PCIe 3.3V Rail), 13.098V (PCIe 12V Rail)	EFP	Shutdown

Table 18: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-20C (Junction temperature)
HighTemperature	47C (Junction temperature)

Table 19: Hardness Testing Temperatures

8 Non-Invasive Security

N/A due to the module not claiming to implement any non-invasive security protection mechanisms.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DDR4	Ephemeral RAM	Dynamic
NOR	read/write memory	Static
MCU	read/write memory	Static
eMMC	read/write memory	Static
FUSE	OTP memory	Static

Table 20: Storage Areas

The module supports the above storage areas for SSP management.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Password-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-AES-KWP-Unwrap (KTS)
Key-Transport-Output-Method	NOR	External	Encrypted	Automated	Electronic	SW-KTS-IFC-Encap (KTS)
Key-Transport-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-KTS-IFC-Decap (KTS)
AES-Wrap-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-AES-KW-Wrap (KTS)
AES-Wrap-Pad-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-AES-KWP-Wrap (KTS)
AES-GCM-Wrap-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-AES-GCM-Wrap
AES-Unwrap-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-AES-KW-Unwrap (KTS)
AES-Unwrap-Pad-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-AES-KWP-Unwrap (KTS)
AES-GCM-Unwrap-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-AES-GCM-Unwrap
Public-Key-Plain-Output-Method	eMMC	External	Plaintext	Automated	Electronic	
Public-Key-Plain-Input-Method	Entered	eMMC	Plaintext	Automated	Electronic	
Shared-Secret-Plain-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-KTS-IFC-Encap (KTS)
Shared-Secret-Plain-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-KTS-IFC-Decap (KTS)
Restore-Key-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-AES-KWP-Unwrap (KTS)
Backup-Key-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-AES-KWP-Wrap (KTS)

Table 21: SSP Input-Output Methods

The module supports the above Input-Output methods.

Private/Secret keys are always encrypted when performing export/import.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
D	Manually zeroized (via GP_KEY_MGMT - CN_DESTROY_OBJECT service)	wipes all SSPs with zeros in 1 second	CN_DESTROY_OBJECT
E	Zeroized right after use (Memory is wiped with zeros, immediately after use)	wipes all SSPs with zeros in 1 second	immediately after use
MFZ	Zeroize all Partition's SSPs, including the HSM adapter owner programmed ones (Brings HSM to factory state. Factory reset via GP_ZEROIZATION - CN_ZEROIZE service with factory-reset as argument with MCO credentials)	wipes all SSPs with zeros in 1 second	CN_ZEROIZE
MZ	Zeroize all Partition's SSPs, except vendor programmed ones (HSM zeroize via GP_ZEROIZATION - CN_ZEROIZE service with MCO credentials)	wipes all SSPs with zeros in 1 second	CN_ZEROIZE
PD	Zeroize all SSPs in the Partition and then delete the User Partition (via GP_PARTITION_MGMT - CN_DELETE_PARTITION service)	wipes all SSPs with zeros in 1 second	CN_DELETE_PARTITION
PFZ	Zeroize all SSPs in the Partition (Factory reset via GP_ZEROIZATION - CN_ZEROIZE service with factory-reset as argument with PCO credentials)	wipes all SSPs withzeros in 1 second	CN_ZEROIZE
PZ	Zeroize all User SSPs in the Partition Regular p (User Partition Regular zeroize via GP_ZEROIZATION - CN_ZEROIZE service with PCO credentials)	wipes all SSPs with zeros in 1 second	CN_ZEROIZE
S	Zeroized on session close (Session Close via GP_SESSION_MGMT - CN_CLOSE_SESSION, CN_APP_FINALIZE and CN_CLOSE_PARTITION_SESSIONS)	wipes all SSPs with zeros in 1 second	CN_CLOSE_SESSION
VZ	Vendor zeroize (Zeroizes all SSPs including vendor programmed configuration and CSPs. Makes the module unusable; the module must be sent back to the vendor for re-programming.) via GP_ZEROIZATION - CN_VENDOR_ZEROIZE service	wipes all SSPs with zeros in 1 second	CN_VENDOR_ZEROIZE

Table 22: SSP Zeroization Methods

The module supports above SSP zeroization methods.

The SSPs are zeroized securely by writing zeros to memory.

9.4 SSPs

The HSM Manufacturer Hardware Unique 1 Key (HMHU1KY) is stored in plaintext in FUSE and HSM Manufacturer Hardware Unique 2 Key (HMHU2KY) is stored in NOR encrypted with HSM Manufacturer Hardware Unique 1 Key (HMHU1KY). All other keys and CSPs stored in the persistent memory are encrypted by the HMHU2KY, HSM Master Encryption Key (HXMEKY), or Partition Master Encryption Key (PXMEKY). All general-purpose user CSPs are generated/created by the PCU, and these CSPs can be shared between multiple PCUs.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST)	The entropy input string and seed for the Approved DRBG.	13472-bits - N/A	Entropy - CSP	ENT (P) (SP 800-90B)		CPT-Hash-DRBG SW-Counter-DRBG
FIPS Octeon HSM DRBG Seed (FOHXDRBGSD)	DRBG seed derived from entropy input.	12672-bits - N/A	DRBG Seed - CSP	ENT (P) (SP 800-90B)		CPT-Hash-DRBG SW-Counter-DRBG
FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON)	DRBG nonce derived from entropy input.	6400-bits - N/A	DRBG Nonce - CSP	ENT (P) (SP 800-90B)		CPT-Hash-DRBG SW-Counter-DRBG
Partition DRBG CTR V State (PXDRBGCTVST)	The internal state (V) for the Counter DRBG.	128-bits - 256-bits	Internal States - CSP	SW-Counter-DRBG		SW-Counter-DRBG
Partition DRBG CTR Key State (PXDRBGCTKST)	The internal state (Key) for the Counter DRBG.	256-bits - 256-bits	Internal States - CSP	SW-Counter-DRBG		SW-Counter-DRBG
Partition DRBG Hash V State (PXDRBGHAVST)	The internal state (V) for the Hash DRBG.	896-bits - 256-bits	Internal States - CSP	CPT-Hash-DRBG		CPT-Hash-DRBG
Partition DRBG Hash C State (PXDRBGHACST)	The internal state (C) for the Hash DRBG.	896-bits - 256-bits	Internal States - CSP	CPT-Hash-DRBG		CPT-Hash-DRBG
HSM Manufacturer Hardware Unique 2 Key (HMHU2KY)	AES 256-bit key used to encrypt manufacturer keys stored in persistent storage of the HSM.	256-bits - 256-bits	Symmetric Key - CSP	Other (Pre-loaded)		SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
HSM Master Encryption Key (HXMEKY)	AES 256-bit key used to encrypt Master Partition CSPs and authentication data	256-bits - 256-bits	Symmetric Key - CSP	CPT-KeyGen		SW-AES-KWP-Wrap

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	stored in persistent storage of the HSM.					(KTS) SW-AES-KWP-Unwrap (KTS)
Partition Master Encryption Key (PXMEKY)	AES 256-bit key used to encrypt partition CSPs and authentication data stored in persistent storage of the HSM	256-bits - 256-bits	Symmetric Key - CSP	SW-KeyGen		CPT-AES-CBC-ENC CPT-AES-CBC-DEC
Partition Data Encryption Key (PXDEKY)	AES 256-bit key used to wrap PAK	256-bits - 256-bits	Symmetric Key - CSP	SW-KeyGen		SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA)	A unique 4096-bit RSA private key. Used to identify the HSM when in the FIPS operating mode.	4096-bits - 150-bits	Private - CSP	Other (Pre-loaded)		SW-RSA-SigGen (FIPS186-5) SW-KTS-IFC-Decap (KTS)
FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC)	A unique ECC P521 private key. Used to identify the HSM when in the FIPS operating mode.	521-bits - 256-bits	Private - CSP	Other (Pre-loaded)		SW-ECDSA-SigGen (FIPS186-4)
HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC)	A unique ECC P256 private key. Used to identify the HSM when in the FIPS operating mode.	256-bits - 128-bits	Private - CSP	Other (Pre-loaded)		SW-ECDSA-SigGen (FIPS186-4)
Partition Authentication Key Private RSA (PXPAKYPRVRSA)	A unique 2048-bit RSA private key used to identify the HSM partition	2048-bits - 112-bits	Private - CSP	SW-RSA-KeyGen (FIPS186-5)		SW-RSA-SigGen (FIPS186-5)
Partition Cert Auth Source Shared Secret (PXCASSZ)	Shared secret Z for SP 800-56Br2 KAS2, using PAK and POAC	512-bits - 112-bits	Shared Secret - CSP	CPT-KeyGen		SW-KDF-SP800-108
Partition Cert Auth Target Shared Secret (PXCATSZ)	Shared secret Z for SP 800-56Br2 KAS2, using PAK and POAC	512-bits - 112-bits	Shared Secret - CSP		SW-KAS-IFC-SSC	SW-KDF-SP800-108

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Partition Cert Auth Ephemeral Key (PXCAEK)	Shared secret Z for SP 800-56Br2 KAS2, using PAK and POAC	512-bits - 112-bits	Symmetric Key - CSP	SW-KDF-SP800-108		SW-KDF-SP800-108
Partition Wrap Unwrap Shared Secret (PXWUSZ)	Shared secret Z for SP 800-56Ar3 KAS2, using Peer's public key and User's private key in CN_WRAP_KEY and CN_UNWRAP_KEY	128-bits - 256-bits - 112-bits - 256-bits	Shared Secret - CSP		SW-KAS-ECC-SSC-Sp800-56Ar3	KAS-KDA-HKDF (SP800-56Ar3)
Partition Password Encryption Key (PXPEKY)	AES-256 key for encrypting user passwords during user creation and authentication.	256-bits - 256-bits	Symmetric Key - CSP	SW-KDA-OneStep-Sp800-56Cr1		SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
Partition User Login Password Data (PULPDA)	String of 8 to 32 alphanumeric characters.	8 to 32 Characters - 62^8	Authentication Data - CSP			SW-PBKDF
Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV)	ECC 521-bit key used in SP 800-56Ar3 C(2,0, ECC DH) to agree on Z during key loading.	ECC:521-bits - ECC:256-bits	Private - CSP	SW-ECDSA-KeyGen (FIPS186-4)		SW-KAS-ECC-SSC-Sp800-56Ar3
Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB)	ECC 521-bit ephemeral public key used in SP 800-56Ar3 C (2,0, ECC DH) key agreement to generate shared secret Z.	ECC:521-bits - ECC:256-bits	Public - PSP	SW-ECDSA-KeyGen (FIPS186-4)		SW-KAS-ECC-SSC-Sp800-56Ar3
Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB)	ECC 521-bit or RSA2048- bit ephemeral public key used in SP 800-56Br2 KAS2 - bilateral - confirmation key agreement to generate shared secret Z.	RSA:2048-bits - RSA:112-bits	Public - PSP			KAS-IFC-OneStep (SP800-56Br2)
Partition Key Loading Key Shared Secret (PXKLSZ)	Shared secret Z for SP 800-56Ar3 C (2,0, ECCDH) or SP800-56Br2 KAS2.	256-bits - 256-bits	Shared Secret - CSP		SW-KAS-ECC-SSC-Sp800-56Ar3 SW-KAS-IFC-SSC	SW-KDA-OneStep-Sp800-56Cr1 SW-KDA-TwoStep-Sp800-56Cr1
Partition Key Loading Key (PXKLKY)	A 256-bit AES key derived from Z; used	256-bits - 256-bits	Symmetric Key - CSP		KAS-KDA-ONESTEP (SP800-	SW-AES-GCM-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	to decrypt the imported CSPs				56Ar3) KAS-IFC-OneStep (SP800-56Br2)	Wrap SW-AES-GCM-Unwrap SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) LEGACY-SW-AES-CBC-UNWRAP SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY)	AES 256-bit key used to derive KBK.	256-bits - 256-bits	Symmetric Key - CSP			SW-KDF-SP800-108
HSM Owner Recovery Key (HOREKY)	AES 256-bit key used to double encrypt the manufacturer keys	256-bits - 256-bits	Symmetric Key - CSP			SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
Partition Key Backup Key (PXKBKY)	Key used to encrypt/decrypt the backup session key.	256-bits - 256-bits	Symmetric Key - CSP	SW-KDF-SP800-108		SW-AES-KW-Wrap (KTS)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
Partition Backup Ephemeral Key (PXKBEK)	Key used to backup and restore partition data.	256-bits - 256-bits	Symmetric Key - CSP	SW-KeyGen		SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-CBC-UNWRAP SW-AES-CBC-WRAP SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS)
Partition Masking Key (PXMSKY)	AES-256 key for key wrapping. Used to import/export CSPs and masked objects	256-bits - 256-bits	Symmetric Key - CSP	CPT-KeyGen		SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS)
Partition Cloning Ephemeral Key Private (PXCLEKPRV)	ECC 521-bit or RSA 2048-bit ephemeral Private Key used in SP 800-56Ar3 C (2,0, ECC DH) or SP 800 - 56Br2KAS2 -bilateral -	ECC:521-bits; RSA:2048 -bits - ECC:256-bits;	Private - CSP	SW-ECDSA-KeyGen (FIPS186-4) SW-RSA-		KAS-KDA-ONESTEP (SP800-56Ar3)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	confirmation key agreement to generate shared secret Z. At HSM partition level, used to establish secure channel for cloning process (to export partition masking key).	RSA:112-bits		KeyGen (FIPS186-5)		KAS-IFC-OneStep (SP800-56Br2)
Partition Cloning Shared Secret (PXCLSZ)	Shared secret Z for SP 800- 56Ar3 C (2,0, ECC DH) or SP 800-56Br2. KAS2 -bilateral -confirmation scheme	256-bits - 256-bits	Shared Secret - CSP		SW-KAS-ECC-SSC-Sp800-56Ar3 SW-KAS-IFC-SSC	SW-KDF-SP800-108
Partition Cloning Encryption Ephemeral Key (PXCLEEK)	AES 256 key for encryption and decryption of partition masking key.	256-bits - 256-bits	Symmetric Key - CSP		KAS-KDA-ONESTEP (SP800-56Ar3)	SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS)
Partition Cloning MAC Ephemeral Key (PXCLMEK)	HMAC SHA256 key used for key confirmation during SP 800-56Ar3 key agreement.	256-bits - 256-bits	Symmetric Key - CSP		KAS-KDA-ONESTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2)	SW-HMAC-SHA2-512
Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV)	RSA/ECDSA/ECDH general purpose keys.	RSA:2048-bits, 3072-bits, 4096-bits; ECDSA:224-bits, 256-bits, 384-bits, 521-bits; - RSA:112-bits, 128-bits, 150-bits; ECDSA:112-bits, 128-bits, 192-bits, 256-bits;	Private - CSP	FW-ECDSA-KeyGen (FIPS186-5) FW-RSA-KeyGen (FIPS186-5) ECDSA with non-NIST recommended curves		SW-ECDSA-KeyVer (FIPS186-4) CPT-ECDSA-SigGen (FIPS186-4) SW-RSA-Decryption-Primitive SW-RSA-SigGen (FIPS186-5) SW-KAS-ECC-SSC-Sp800-56Ar3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						FW-KTS-IFC-Decap (KTS) CPT-RSA-Decryption-Primitive CPT-RSA-Signature-Primitive SW-KTS-IFC-Decap (KTS) SW-KAS-ECC (KAS) CPT-KAS-ECC-SSC-Sp800-56Ar3 SW-KDF-ANS-9.63 SW-KDA-HKDF-Sp800-56Cr1 KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST
Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV)	RSA/ECDSA/ECDH general purpose keys.	RSA:2048-bits, 3072-bits,4096-bits; ECDSA:224-bits, 256-bits, 384-bits, 521-bits; - RSA:112-bits, 128-bits,150-bits; ECDSA:112-bits, 128-bits, 192-bits, 256-bits;	Private - CSP	ECDSA with non-NIST recommended curves FW-ECDSA-KeyGen (FIPS186-5) FW-RSA-KeyGen (FIPS186-5)		SW-ECDSA-KeyVer (FIPS186-4) CPT-ECDSA-SigGen (FIPS186-4) SW-RSA-Decryption-Primitive SW-RSA-SigGen (FIPS186-5) SW-KAS-ECC-SSC-Sp800-56Ar3 FW-KTS-IFC-Decap (KTS) CPT-RSA-Decryption-Primitive CPT-RSA-Signature-Primitive SW-KTS-IFC-Decap (KTS) SW-KAS-ECC (KAS) CPT-KAS-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						ECC-SSC-Sp800-56Ar3 SW-KDF-ANS-9.63 SW-KDA-HKDF-Sp800-56Cr1 KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST
Partition User General Purpose Symmetric Key (PUGPSKY)	Triple-DES or AES general purpose keys.	AES:128-bits, 192-bits, 256-bits; Triple-DES:192-bits - AES:128-bits, 192-bits, 256-bits; Triple-DES:112-bits	Symmetric Key - CSP	SW-KeyGen		CPT-AES-CBC-ENC CPT-AES-CBC-DEC CPT-AES-ECB-ENC CPT-AES-ECB-DEC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						CPT-AES-CTR-ENC CPT-AES-CTR-DEC LEGACY-CPT-TDES-ECB CPT-TDES-CBC CPT-AES-CCM-ENC CPT-AES-CCM-DEC CPT-AES-GCM-ENC CPT-AES-GCM-DEC CPT-AES-GMAC CPT-AES-CMAC SW-AES-KW-Wrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-CMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						LEGACY-SW-TDES-KW (KTS) SW-AES-GCM-Wrap SW-AES-GCM-Unwrap SW-AES-GMAC
Partition User General Purpose Symmetric Session Key (PUGPSSK)	Triple-DES or AES general purpose keys.	AES:128-bits, 192-bits, 256-bits; Triple-DES:192-bits - AES:128-bits, 192-bits, 256-bits; Triple-DES:112-bits	Symmetric Key - CSP	SW-KeyGen		SW-AES-GCM-Wrap SW-AES-GCM-Unwrap SW-AES-GCM-Enc SW-AES-GCM-Dec SW-AES-GMAC SW-AES-KW-Unwrap (KTS) SW-AES-KW-Wrap (KTS) CPT-AES-CBC-ENC CPT-AES-CCM-ENC CPT-AES-CCM-DEC CPT-AES-CMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						SW-AES-CMAC CPT-AES-CTR-ENC CPT-AES-CTR-DEC CPT-AES-GMAC SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) CPT-TDES-CBC LEGACY-CPT-TDES-ECB
Partition User General Purpose HMAC Key (PUGPMKY)	HMAC general purpose keys (minimum key size of 112 bits).	112-bits - 6400-bits - 112-bits - 256-bits	Symmetric Key - CSP	SW-KeyGen		CPT-HMAC-SHA-1 CPT-HMAC-SHA2-256 CPT-HMAC-SHA2-384 CPT-HMAC-SHA2-512 SW-HMAC-SHA-1 SW-HMAC-SHA2-256 SW-HMAC-SHA2-384 SW-HMAC-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						SHA2-512
Partition User General Purpose HMAC Session Key (PUGPMSK)	HMAC general purpose keys (minimum key size of 112 bits).	112-bits - 6400-bits - 112-bits - 256-bits	Symmetric Key - CSP	SW-KeyGen		CPT-HMAC-SHA-1 CPT-HMAC-SHA2-256 CPT-HMAC-SHA2-384 CPT-HMAC-SHA2-512 SW-HMAC-SHA-1 SW-HMAC-SHA2-256 SW-HMAC-SHA2-384 SW-HMAC-SHA2-512
Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC)	Used for key agreement as part of TLS-1.2 handshake protocol.	256-bits - 512-bits - 128-bits - 256-bits	Private - CSP	SW-ECDSA-KeyGen (FIPS186-4)		CPT-KAS-ECC-SSC-Sp800-56Ar3
Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EEKPUBECC)	Used for key agreement as part of TLS-1.2 handshake protocol.	256-bits - 512-bits - 128-bits - 256-bits	Public - PSP	SW-ECDSA-KeyGen (FIPS186-4)		
Partition User TLS E2E Client Authentication Certificate (PUTLSE2ECACT)	RSA or EC certificate presented by client during E2E/TLS handshake to allow E2E/ TLS client authentication.	RSA:2048-,3072-bits; EC:256-, 384-bits - RSA:112-bits - 150-bits; EC:128-bits - 256-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5) CPT-ECDSA-SigVer (FIPS186-5)
Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC)	Used for key agreement as part of TLS-1.2handshake protocol.	256-bits - 512-bits - 128-bits - 256-bits	Public - PSP			CPT-KAS-ECC-SSC-Sp800-56Ar3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Partition TLS E2E Symmetric Key (PXTLSE2EKY)	AES 256 key used for encrypting TLS sessions.	256-bits - 256-bits	Symmetric Key - CSP	KAS-TLS (Sp800-56Ar3)		CPT-AES-GCM-ENC
Partition TLS E2E Pre Master Secret (PXTLSE2EPMS)	pre-master secret, used to derive master secret.	256-bits - 521-bits - 128-bits - 256-bits	Symmetric Key - CSP		CPT-KAS-ECC-SSC-Sp800-56Ar3	KAS-TLS (Sp800-56Ar3)
Partition TLS E2E Master Secret Key (PXTLSE2EMSKY)	TLS master secret of size 384-bit used to derive session keys	384-bits - 128-bits - 256-bits	Symmetric Key - CSP		KAS-TLS (Sp800-56Ar3)	KAS-TLS (Sp800-56Ar3)
HSM Vendor Firmware Update Validation Key Public RSA (HVFUVKYPUBRSA)	RSA 2048-bit public key used to authenticate new FW images uploaded into the module. The FW image is signed by the manufacturer using an RSA private key and the signature is verified before upgrading to the new image using the public key	2048-bits - 112-bits	Public - PSP	Other (Pre-loaded)		SW-RSA-SigVer (FIPS186-5)
HSM Vendor Firmware Update Validation Key Public ECC (HVFUVKYPUBECC)	ECDSA 521-bit public key used to authenticate new FW images uploaded into the module. The FW image is signed by the manufacturer using an ECDSA private key and the signature is verified before upgrading to the new image using the public key	521-bits - 256-bits	Public - PSP	Other (Pre-loaded)		SW-ECDSA-SigVer (FIPS186-4)
HSM Vendor Authentication Root Certificate RSA (HVARCTRSA)	RSA 4096-bit public key certificate used to issue FMAC certificates.	4096-bits - 150-bits	Public - PSP	Other (Pre-loaded)		SW-RSA-SigVer (FIPS186-5)
FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA)	RSA 4096-bit public key certificate of FMAK used to identify the HSM FIPS operating mode.	4096-bits - 150-bits	Public - PSP	Other (Pre-loaded)		SW-RSA-SigVer (FIPS186-5)
HSM Vendor Authentication Root Certificate ECC (HVARCTEC)	ECC P521 public key certificate used to issue FMAEC certificates.	521-bits - 256-bits	Public - PSP	Other (Pre-loaded)		
FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC)	ECC P521 public key certificate of FMAEK used to identify the HSM FIPS operating mode.	521-bits - 256-bits	Public - PSP	Other (Pre-loaded)		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC)	ECC P256 public key certificate of HSMEK used to identify the each HSM independently	256-bits - 128-bits	Public - PSP	Other (Pre-loaded)		SW-ECDSA-KeyVer (FIPS186-4) SW-ECDSA-SigVer (FIPS186-4)
HSM Owner Trust Anchor Certificate (HOOTACT)	RSA 2048-bit public key certificate used as trust anchor of MCO.	2048-bits - 112-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5)
FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA)	RSA 2048-bit public key certificate of FMAK used to identify the HSM owner	2048-bits - 112-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5)
Partition Authentication Certificate (PXPACT)	RSA 2048-bit public key certificate of PAK used to identify the partition.	2048-bits - 112-bits	Public - PSP	SW-RSA-KeyGen (FIPS186-5)		SW-RSA-SigVer (FIPS186-5)
Partition Owner Trust Anchor Certificate (POOTACT)	RSA 2048-bit public key certificate used as trust anchor of PCO.	2048-bits - 112-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5)
Partition Owner Authentication Certificate (POOAUCT)	RSA 2048-bit public key certificate of PAK used to identify the partition owner.	2048-bits - 112-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5)
Partition Cloning Ephemeral Key Public (PXCLEKPUB)	ECC 521-bit ephemeral public key used in SP 800-56Ar3 C (2,0, ECC DH) key agreement - bilateral - confirmation key agreement to generate shared secret Z.	ECC:521-bits - ECC:256-bits	Public - PSP	SW-ECDSA-KeyGen (FIPS186-4)		KAS-IFC-OneStep (SP800-56Br2)
HSM Owner Attestation Key Public (HOOATKYPUB)	Adapter Owner Attestation Public key (AOAPubK)	RSA:2048-bits - 4096-bits; EC:224-bits - 521-bits - RSA:112-bits - 150-bits; EC:112-bits - 256-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5) SW-ECDSA-SigVer (FIPS186-4)
Partition User Cloning Ephemeral	ECC 521-bit or RSA 2048- bit ephemeral public key used in SP	ECC:521-bits; RSA:2048	Public - PSP			KAS-KDA-ONESTE

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Key Public (PUCLEKPUB)	800-56Br2 KAS2 - bilateral - confirmation key agreement to generate shared secret Z.	-bits - ECC:256-bits; RSA:112-bits				P (SP800-56Ar3)
Partition Password Encryption Key Shared Secret (PXPESZ)	Shared secret Z for SP 800- 56Ar3 C (2,0, ECC DH) or SP 800-56Br2. KAS2 -bilateral -confirmation scheme	256-bits - 256-bits	Shared Secret - CSP		SW-KAS-IFC-SSC	SW-KDF-SP800-108
Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB)	RSA 2048-bit public key loaded by the host used for SP 800-56Br2 key agreement to generate PswdEncKey.	2048-bits - 112-bits	Public - PSP			KAS-KDA-ONESTEP (SP800-56Ar3)
Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA)	RSA 2048-bit public key used to verify signature on encrypted passwords during user creation and login and/or to verify signatures on MofN authentication tokens.	2048-bits - 112-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5)
Partition User General Purpose Key Public (PUGPKYPUB)	RSA/ECDSA/ECDHgeneral purpose public keys.	RSA:2048-bits, 3072-bits, 4096-bits; ECDSA:224-bits, 256-bits, 384-bits, 521-bits; - RSA:112-bits, 128-bits, 150-bits; ECDSA:112-bits, 128-bits, 192-bits, 256-bits;	Public - PSP	FW-ECDSA-KeyGen (FIPS186-5) SW-ECDSA-KeyGen (FIPS186-4) SW-RSA-KeyGen (FIPS186-5) FW-RSA-KeyGen (FIPS186-5)		SW-ECDSA-SigVer (FIPS186-4) CPT-ECDSA-SigVer (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-KAS-ECC-SSC-Sp800-56Ar3 FW-KTS-IFC-Encap (KTS) SW-KDF-ANS-9.63 KAS-ANS-9.63 (Sp800-56Ar3) KAS-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) SW-KTS-IFC-Encap (KTS)
Partition User General Purpose Session Key Public (PUGPSKYPUB)	RSA/ECDSA/ECDH/ML-DSA/ML-KEM general purpose public keys.	RSA:2048-bits, 3072-bits, 4096-bits; ECDSA:224-bits, 256-bits, 384-bits, 521-bits; ML-DSA security level:2, 3, 5; ML-KEM security level:1, 3, 5; - RSA:112-bits, 128-bits, 150-bits; ECDSA:112-bits, 128-bits, 192-bits, 256-bits; ML-DSA:128-bits, 192-bits, 256-bits; ML-KEM:128-bits, 192-bits, 256-bits;	Public - CSP	FW-ECDSA-KeyGen (FIPS186-5) FW-RSA-KeyGen (FIPS186-5)		SW-ECDSA-SigVer (FIPS186-4) CPT-ECDSA-SigVer (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-KAS-ECC-SSC-Sp800-56Ar3 FW-KTS-IFC-Encap (KTS) SW-KDF-ANS-9.63 KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) SW-KTS-IFC-Encap (KTS)
HSM Vendor License Key Public RSA (HVLICKYPUBRSA)	RSA 2048-bit public key used to verify signature on license file uploaded by MCO user	2048-bits - 112-bits	Public - PSP	Other (Pre-loaded)		SW-RSA-SigVer (FIPS186-5)
Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT)	Public key certificate used as trust anchor of PCO for e2eauthentication	RSA:2048-bits to 4096-bits; ECC: 256-bitsto 521-bits - 112-bits to 256-bits	Public - PSP			SW-RSA-SigVer (FIPS186-5)
Partition Wrap Ephemeral Key Private (PXWEKPRV)	ECC 224-bit to 521-bit ephemeral private key used in SP 800-56Ar3 KAS-ECC-SSC key agreement to generate shared secret Z in CN_WRAP_KEY and CN_UNWRAP_KEY operations.	224-bits - 521-bits - 112-bits - 256-bits	private - CSP	SW-ECDSA-KeyGen (FIPS186-4)		SW-KAS-ECC-SSC-Sp800-56Ar3
Partition Wrap Ephemeral Key Public (PXWEKPUB)	ECC 224-bit to 521-bit ephemeral public key used in SP 800-56Ar3 KAS-ECC-SSC key agreement to generate shared secret Z in CN_WRAP_KEY and CN_UNWRAP_KEY operations.	224-bits - 521-bits - 112-bits - 256-bits	public - PSP	SW-ECDSA-KeyGen (FIPS186-4)		
Partition User Wrap Unwrap Ephemeral Key Public (PUWUEKPUB)	ECC 224-bit to 521-bit ephemeral public key provided by the user/peer for SP 800-56Ar3 KAS-ECC-SSC key agreement to generate shared secret Z in CN_WRAP_KEY and	224-bits - 521-bits - 112-bits - 256-bits	public - PSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	CN_UNWRAP_KEY operations.					
Partition Wrap Unwrap Encryption Ephemeral Key (PXWUEEK)	Derived key using Partition Wrap Unwrap Shared Secret (PXWUSZ)	256 bits - 256-bits	Symmetric Key - CSP	SW-KDA-HKDF-Sp800-56Cr1 SW-KDF-ANS-9.63		SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS)
Partition Wrap Unwrap Intermediate Ephemeral Key (PXWUIEK)	Generated Ephemeral AES temp key for RSA AES Mechanism	256 bits - 256-bits	Symmetric Key - CSP	SW-KeyGen CPT-KeyGen		SW-AES-KWP-Wrap (KTS) SW-AES-KW-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KW-Unwrap (KTS)

Table 23: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST)		DDR4:Plaintext	Zeroized right after use	E	FIPS Octeon HSM DRBG Seed (FOHXDRBGSD):Derives FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON):Derives
FIPS Octeon HSM DRBG Seed (FOHXDRBGSD)		DDR4:Plaintext	Zeroized right after use	E	Partition DRBG Hash V State (PXDRBGHAVST):Derives Partition DRBG Hash C State (PXDRBGHACST):Derives Partition DRBG CTR V State (PXDRBGCTVST):Derives Partition DRBG CTR Key State (PXDRBGCTKST):Derives FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON):Used with FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST):Derived from

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON)		DDR4:Plaintext	Zeroized right after use	E	Partition DRBG Hash V State (PXDRBGHAVST):Derives Partition DRBG Hash C State (PXDRBGHACST):Derives Partition DRBG CTR V State (PXDRBGCTVST):Derives Partition DRBG CTR Key State (PXDRBGCTKST):Derives FIPS Octeon HSM DRBG Seed (FOHXDRBGSD):Used with FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENST):Derived from
Partition DRBG CTR V State (PXDRBGCTVST)		DDR4:Plaintext	Zeroized right after use	PDE	FIPS Octeon HSM DRBG Seed (FOHXDRBGSD):Derived from FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON):Derived from Partition DRBG CTR Key State (PXDRBGCTKST):Used with
Partition DRBG CTR Key State (PXDRBGCTKST)		DDR4:Plaintext	Zeroized right after use	PDE	FIPS Octeon HSM DRBG Seed (FOHXDRBGSD):Derived from FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON):Derived from Partition DRBG CTR V State (PXDRBGCTVST):Used with
Partition DRBG Hash V State (PXDRBGHAVST)		DDR4:Plaintext	Zeroized right after use	PDE	FIPS Octeon HSM DRBG Seed (FOHXDRBGSD):Used with FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON):Used with Partition DRBG Hash C State (PXDRBGHACST):Used with
Partition DRBG Hash C State (PXDRBGHACST)		DDR4:Plaintext	Zeroized right after use	PDE	FIPS Octeon HSM DRBG Seed (FOHXDRBGSD):Used with FIPS Octeon HSM DRBG Nonce (FOHXDRBGNON):Used with Partition DRBG Hash V State (PXDRBGHAVST):Used with
HSM Manufacturer Hardware Unique 2 Key (HMHU2KY)		NOR:Plaintext DDR4:Plaintext	Zeroized right after use	VZE	FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA):Wraps FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY):Wraps HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC):Wraps FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC):Wraps HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC):Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
HSM Master Encryption Key (HXMEKY)		MCU:Plaintext DDR4:Plaintext	Zeroized right after use	MZE	Partition Master Encryption Key (PXMEKY):Wraps Partition Data Encryption Key (PXDEKY):Wraps
Partition Master Encryption Key (PXMEKY)		NOR:Encrypted DDR4:Plaintext	Zeroized right after use	PZE	HSM Master Encryption Key (HXMEKY):Wrapped By Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV):Wraps Partition User General Purpose Symmetric Key (PUGPSKY):Wraps Partition User General Purpose HMAC Key (PUGPMKY):Wraps Partition User Login Password Data (PULPDA):Wraps Partition Password Encryption Key (PXPEKY):Wraps Partition Key Loading Key (PXKLKY):Encrypts Partition Masking Key (PXMSKY):Wraps Partition Key Backup Key (PXKBKY):Encrypts
Partition Data Encryption Key (PXDEKY)		NOR:Encrypted DDR4:Plaintext	or module powered off	PDE	HSM Master Encryption Key (HXMEKY):Wrapped By Partition Authentication Key Private RSA (PXPAKYPRVRSA):Wraps
FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA)		NOR:Encrypted DDR4:Plaintext	Zeroized right after use	VZE	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA):Paired With HSM Owner Recovery Key (HOREKY):Wrapped by
FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC)		NOR:Encrypted DDR4:Plaintext	Zeroized right after use	VZE	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC):Paired With HSM Owner Recovery Key (HOREKY):Wrapped by
HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC)		NOR:Encrypted DDR4:Plaintext	Zeroized right after use	VZE	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By
Partition Authentication Key Private RSA (PXPAKYPRVRSA)	Backup-Key-Output-Method Restore-Key-	eMMC:Encrypted DDR4:Plaintext	Zeroized right after use	PDE	Partition Data Encryption Key (PXDEKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By Partition Cert Auth Source Shared Secret

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Input-Method				(PXCASSZ):Encrypt Partition Cert Auth Target Shared Secret (PXCATSZ):Decrypt Partition Authentication Certificate (PXPACT):Paired With
Partition Cert Auth Source Shared Secret (PXCASSZ)	Shared-Secret-Plain-Output-Method	DDR4:Plaintext	Zeroized on session close	S	Partition Cert Auth Ephemeral Key (PXCAEK):Derives Partition Authentication Certificate (PXPACT):Encrypted By
Partition Cert Auth Target Shared Secret (PXCATSZ)	Shared-Secret-Plain-Input-Method	DDR4:Plaintext	Zeroized on session close	S	Partition Cert Auth Ephemeral Key (PXCAEK):Derives Partition Authentication Key Private RSA (PXPAKYPRVRSA):Decrypted By Partition Authentication Certificate (PXPACT):Signature Verify
Partition Cert Auth Ephemeral Key (PXCAEK)		DDR4:Plaintext	Zeroized on session close	S	Partition Cert Auth Source Shared Secret (PXCASSZ):Derives Partition Cert Auth Target Shared Secret (PXCATSZ):Derives
Partition Wrap Unwrap Shared Secret (PXWUSZ)		DDR4:Plaintext	Zeroized right after use	E	Partition User General Purpose Key Public (PUGPKYPUB):Derived From Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV):Derived From Partition Wrap Unwrap Encryption Ephemeral Key (PXWUEEK):Derives
Partition Password Encryption Key (PXPEKY)	Restore-Key-Input-Method Backup-Key-Output-Method	DDR4:Plaintext eMMC:Encrypted	Zeroized right after use	PZE	Partition Master Encryption Key (PXMEKY):Encrypted By Partition User Login Password Data (PULPDA):Encrypts Partition Backup Ephemeral Key (PXKBEK):Wrapped By Partition Password Encryption Key Shared Secret (PXPESZ):Derived From
Partition User Login Password Data (PULPDA)	Password-Input-Method Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Encrypted DDR4:Plaintext	Zeroized right after use	PZE	Partition Password Encryption Key (PXPEKY):Encrypted By Partition Master Encryption Key (PXMEKY):Encrypted By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV)		DDR4:Plaintext	Zeroized right after use	E	Partition Key Loading Key Shared Secret (PXKLSZ):Establishes Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB):Paired With
Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB)	Public-Key-Plain-Output-Method	DDR4:Plaintext	Zeroized right after use	E	Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV):Paired With
Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Zeroized right after use	E	Partition Key Loading Key Shared Secret (PXKLSZ):Encrypts Partition Key Loading Key Shared Secret (PXKLSZ):Derives
Partition Key Loading Key Shared Secret (PXKLSZ)		DDR4:Plaintext	Zeroized right after use	E	Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV):Established by Partition Key Loading Key (PXKLKY):Derives Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB):Established by Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB):Encrypted by
Partition Key Loading Key (PXKLKY)	Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Encrypted DDR4:Plaintext	Zeroized right after use	PZ VZ E	Partition Master Encryption Key (PXMEKY):Encrypted By Partition Key Loading Key Shared Secret (PXKLSZ):Derived From Partition Backup Ephemeral Key (PXKBEK):Wrapped by
FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY)		NOR:Encrypted DDR4:Plaintext	Zeroized right after use	VZ E	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By HSM Owner Recovery Key (HOREKY):Wrapped By Partition Key Backup Key (PXKBKY):Derives
HSM Owner Recovery Key (HOREKY)	AES-Unwrap-Input-Method	MCU:Plaintext DDR4:Plaintext	Zeroized right after use	MFZ VZ E	FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA):Wraps FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY):Wraps FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC):Wraps
Partition Key Backup Key (PXKBKY)		eMMC:Encrypted	Zeroized right after use	MFZ VZ E	FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
		DDR4:Plaintext			Partition Master Encryption Key (PXMEKY):Encrypted by Partition Backup Ephemeral Key (PXKBEK):Wraps
Partition Backup Ephemeral Key (PXKBEK)		DDR4:Plaintext	Zeroized right after use	E	Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV):Wraps Partition User General Purpose Symmetric Key (PUGPSKY):Wraps Partition User General Purpose HMAC Key (PUGPMKY):Wraps Partition User General Purpose Key Public (PUGPKYPUB):Wraps Partition Masking Key (PXMSKY):Wraps Partition Authentication Certificate (PXPACT):Wraps Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA):Wraps Partition Password Encryption Key (PXPEKY):Wraps Partition Authentication Key Private RSA (PXPAKYPRVRSA):Wraps Partition Key Loading Key (PXKLKY):Wraps Partition Key Backup Key (PXKBKY):Wrapped by
Partition Masking Key (PXMSKY)	AES-Wrap-Output-Method AES-Unwrap-Input-Method Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Encrypted DDR4:Plaintext	Zeroized right after use	PZE	Partition Master Encryption Key (PXMEKY):Encrypted By Partition Cloning Encryption Ephemeral Key (PXCLEEK):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV):Wraps Partition User General Purpose Symmetric Key (PUGPSKY):Wraps Partition User General Purpose HMAC Key (PUGPMKY):Wraps Partition User General Purpose HMAC Session Key (PUGPMSK):Wraps Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV):Wraps Partition User General Purpose Symmetric Session Key (PUGPSSK):Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Partition Cloning Ephemeral Key Private (PXCLEKPRV)		DDR4:Plaintext	Zeroized right after use	E	Partition Cloning Shared Secret (PXCLSZ):Establish Partition Cloning Ephemeral Key Public (PXCLEKPUB):Paired With
Partition Cloning Shared Secret (PXCLSZ)		DDR4:Plaintext	Zeroized right after use	E	Partition Cloning Encryption Ephemeral Key (PXCLEEK):Derives Partition Cloning MAC Ephemeral Key (PXCLMEK):Derives Partition User Cloning Ephemeral Key Public (PUCLEKPUB):Established By Partition Cloning Ephemeral Key Private (PXCLEKPRV):Established By
Partition Cloning Encryption Ephemeral Key (PXCLEEK)		DDR4:Plaintext	Zeroized right after use	E	Partition User Cloning Ephemeral Key Public (PUCLEKPUB):Derived From Partition Cloning Shared Secret (PXCLSZ):Derived From Partition Masking Key (PXMSKY):Encrypts
Partition Cloning MAC Ephemeral Key (PXCLMEK)		DDR4:Plaintext	Zeroized right after use	E	Partition User Cloning Ephemeral Key Public (PUCLEKPUB):Derived From Partition Cloning Shared Secret (PXCLSZ):Derived From
Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-Wrap-Pad-Output-Method AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-Unwrap-Pad-Input-Method AES-	DDR4:Plaintext eMMC:Encrypted	Zeroized right after use	DE	Partition Master Encryption Key (PXMEKY):Encrypted By Partition Masking Key (PXMSKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	GCM-Unwrap-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method				
Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-Wrap-Pad-Output-Method AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-Unwrap-Pad-Input-Method AES-GCM-Unwrap-Input-Method	DDR4:Plaintext	Zeroized on session close	D S	Partition Masking Key (PXMSKY):Wrapped By
Partition User General Purpose Symmetric Key (PUGPSKY)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-Wrap-Pad-Output-Method	DDR4:Plaintext eMMC:Encrypted	Zeroized right after use	D E	Partition Master Encryption Key (PXMEKY):Encrypted By Partition Masking Key (PXMSKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-Unwrap-Pad-Input-Method AES-GCM-Unwrap-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method				
Partition User General Purpose Symmetric Session Key (PUGPSSK)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-Wrap-Pad-Output-Method AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-Unwrap-Pad-Input-Method AES-GCM-Unwrap-	DDR4:Plaintext	Zeroized on session close	DS	Partition Masking Key (PXMSKY):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Input-Method				
Partition User General Purpose HMAC Key (PUGPMKY)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-Wrap-Pad-Output-Method AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-GCM-Unwrap-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	DDR4:Plaintext eMMC:Encrypted	Zeroized right after use	D E	Partition Master Encryption Key (PXMEKY):Encrypted By Partition Masking Key (PXMSKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By
Partition User General Purpose HMAC Session Key (PUGPMSK)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-GCM-Unwrap-	DDR4:Plaintext	Zeroized on session close	D S	Partition Masking Key (PXMSKY):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Input-Method				
Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC)		DDR4:Plaintext	Zeroized on session close	S	Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Established Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EEKPUBECC):Paired With
Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EEKPUBECC)	Public-Key-Plain-Output-Method	DDR4:Plaintext	Zeroized on session close	S	Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC):Paired With Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Established
Partition User TLS E2E Client Authentication Certificate (PUTLSE2ECACT)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Zeroized on session close	E	
Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Zeroized right after use	E	Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Established
Partition TLS E2E Symmetric Key (PXTLSE2EKY)		DDR4:Plaintext	Zeroized on session close	S	Partition TLS E2E Master Secret Key (PXTLSE2EMSKY):Derived from
Partition TLS E2E Pre Master Secret (PXTLSE2EPMS)		DDR4:Plaintext	Zeroized on session close	S	Partition TLS E2E Master Secret Key (PXTLSE2EMSKY):Derives Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC):Established by Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC):Established by
Partition TLS E2E Master Secret Key (PXTLSE2EMSKY)		DDR4:Plaintext	Zeroized on session close	S	Partition TLS E2E Symmetric Key (PXTLSE2EKY):Derives Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Derived From
HSM Vendor Firmware Update Validation Key Public RSA (HVFUVKYPUBRSA)		eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	E	
HSM Vendor Firmware Update Validation Key Public ECC (HVFUVKYPUBECC)		eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	E	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
HSM Vendor Authentication Root Certificate RSA (HVARCTRSA)	Public-Key-Plain-Output-Method	NOR:Plaintext DDR4:Plaintext	Zeroized right after use	VZE	
FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA)	Public-Key-Plain-Output-Method	NOR:Plaintext DDR4:Plaintext	Zeroized right after use	VZE	FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA):Paired With
HSM Vendor Authentication Root Certificate ECC (HVARCTEC)	Public-Key-Plain-Output-Method	NOR:Plaintext DDR4:Plaintext	Zeroized right after use	VZE	
FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC)	Public-Key-Plain-Output-Method	NOR:Plaintext DDR4:Plaintext	Zeroized right after use	VZE	FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC):Paired With
HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC)		eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	VZE	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped by
HSM Owner Trust Anchor Certificate (HOOTACT)	Public-Key-Plain-Input-Method	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	MFZVZE	
FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA)	Public-Key-Plain-Output-Method Public-Key-Plain-Input-Method	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	MFZVZE	
Partition Authentication Certificate (PXPACT)	Public-Key-Plain-Output-Method Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	PDE	Partition Backup Ephemeral Key (PXKBEK):Wrapped By Partition Cert Auth Source Shared Secret (PXCASSZ):Encrypts Partition Authentication Key Private RSA (PXPAKYPRVRSA):Paired With
Partition Owner Trust Anchor Certificate (POOTACT)	Public-Key-Plain-Output-Method	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	PFZPDE	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method				
Partition Owner Authentication Certificate (POOAUCT)	Public-Key-Plain-Input-Method Public-Key-Plain-Output-Method Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	PFZ PD E	Partition Backup Ephemeral Key (PXKBEK):Wrapped By
Partition Cloning Ephemeral Key Public (PXCLEKPUB)		DDR4:Plaintext	Zeroized right after use	E	Partition Cloning Ephemeral Key Private (PXCLEKPRV):Paired With
HSM Owner Attestation Key Public (HOOATKYPUB)	Public-Key-Plain-Input-Method	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	MFZ VZ E	
Partition User Cloning Ephemeral Key Public (PUCLEKPUB)		DDR4:Plaintext	Zeroized right after use	E	Partition Cloning Shared Secret (PXCLSZ):Established by Partition Cloning Encryption Ephemeral Key (PXCLEEK):Derives Partition Cloning MAC Ephemeral Key (PXCLMEK):Derives
Partition Password Encryption Key Shared Secret (PXPESZ)		DDR4:Plaintext	Zeroized right after use	E	Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB):Wrapped By Partition Password Encryption Key (PXPEKY):Derives
Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB)	Public-Key-Plain-	DDR4:Plaintext	Zeroized right after use	E	Partition Password Encryption Key Shared Secret (PXPESZ):Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Input-Method				
Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA)	Public-Key-Plain-Input-Method Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Encrypted DDR4:Plaintext	Zeroized right after use	PZE	HSM Master Encryption Key (HXMEKY):Wrapped By Partition Master Encryption Key (PXMEKY):Encrypted By Partition Backup Ephemeral Key (PXKBEK):Wrapped by
Partition User General Purpose Key Public (PUGPKYPUB)	Public-Key-Plain-Output-Method Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted DDR4:Plaintext	Zeroized right after use	DE	Partition Master Encryption Key (PXMEKY):Encrypted By Partition Masking Key (PXMSKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By
Partition User General Purpose Session Key Public (PUGPSKYPUB)	Public-Key-Plain-Output-Method Public-Key-Plain-Input-Method	DDR4:Plaintext	Zeroized on session close	DS	Partition Masking Key (PXMSKY):Wrapped By Partition Master Encryption Key (PXMEKY):Encrypted by
HSM Vendor License Key Public RSA (HVLICKYPUBRSA)		eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	E	
Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT)	Public-Key-Plain-Input-Method Backup-Key-Output-Method Restore-	eMMC:Plaintext DDR4:Plaintext	Zeroized right after use	PFZ PZ PD E	Partition Backup Ephemeral Key (PXKBEK):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Key-Input-Method				
Partition Wrap Ephemeral Key Private (PXWEKPRV)		DDR4:Plaintext	Zeroized right after use	E	Partition Wrap Unwrap Shared Secret (PXWUSZ):Establish Partition Wrap Ephemeral Key Public (PXWEKPUB):Paired With
Partition Wrap Ephemeral Key Public (PXWEKPUB)	Public-Key-Plain-Output-Method	DDR4:Plaintext	Zeroized right after use	E	Partition Wrap Ephemeral Key Private (PXWEKPRV):Paired With
Partition User Wrap Unwrap Ephemeral Key Public (PUWUEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Zeroized right after use	E	Partition Wrap Unwrap Shared Secret (PXWUSZ):Derives
Partition Wrap Unwrap Encryption Ephemeral Key (PXWUEEK)		DDR4:Plaintext	Zeroized right after use	E	Partition Wrap Unwrap Shared Secret (PXWUSZ):Derived From
Partition Wrap Unwrap Intermediate Ephemeral Key (PXWUIEK)	Key-Transport-Input-Method Key-Transport-Output-Method	DDR4:Plaintext	Zeroized right after use	E	Partition User General Purpose Asymmetric Key Public (PUGPAKYPUB):Wrapped By

Table 24: SSP Table 2

9.5 Transitions

This section identifies cryptographic algorithms and key sizes implemented in the module that are subject to NIST or CMVP transition-related guidance.

SHA-1

Per NIST SP 800-131A, SHA-1 is disallowed for digital signature generation in the Approved mode of operation. The module implements SHA-1 in the Approved mode for HMAC and signature verification purposes only, consistent with current NIST/CMVP guidance.

Operators should plan to transition applications relying on SHA-1 to SHA-2 or SHA-3, as NIST guidance continues to narrow the permitted uses of SHA-1 and it is expected to be fully disallowed in a future revision of SP 800-131A.

FIPS 186-4

FIPS 186-4 has been superseded by FIPS 186-5. The module implements ECDSA and RSA signature verification using legacy FIPS 186-4 parameters for the purposes of verification of existing legacy signatures.

Triple-DES

The module implements Triple-DES (TDEA) for decryption of legacy-encrypted data only. Per NIST SP 800-131A Revision 2, Triple-DES encryption is disallowed as of December 31, 2023. TDEA remains Approved only for decryption of previously TDES-encrypted data (legacy use).

Minimum Security Strength: 112-bit to 128-bit Transition (2030)

Per NIST's cryptographic transition guidance, the minimum Approved security strength for cryptographic algorithms increases from 112 bits to 128 bits effective December 31, 2030. After this date, algorithms and key sizes providing only 112 bits of security strength will no longer be Approved for use.

9.6 Additional Information

Definition of Session Keys
The cryptographic module supports the generation/import/export of user keys that are bound to a session and are termed as session keys. The following points apply to session keys:

- Session keys are stored in RAM and are lost across reboots.
- Session key access is restricted to the application in which it is created.
- PCU can share the session keys with other users so that other sessions can use it.
- Every session in an application will have access to the keys created by every other session in the same application.
- When a session is closed, the session keys created by that session are destroyed.
- If a session key is shared, then it will be deleted only after closing all the sessions sharing the key.

While the SSPs cannot and are not shared between the approved and non-approved modes, they are of same size and cryptographic strength in both approved and non-approved operational modes.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CRC32 firmware integrity	CRC32	KAT	SW/FW Integrity	successful boot	checksum
Firmware Integrity Test	RSA-2048 SigVer	KAT	SW/FW Integrity	successful boot	firmware signature verify
Temperature monitor test	Temperature monitor	CF	Critical Function	successful boot	Temperature monitor
Voltage monitor test	Voltage monitor	CF	Critical Function	successful boot	Voltage monitor

Table 25: Pre-Operational Self-Tests

The module performs the above pre-operational self-tests. The module performs the pre-operational Firmware integrity tests (#A1946) RSA 2048-bit SHA2-256 signature verification every 24 hours and on demand be rebooting the module or by the GP_INFO_DIAGNOSTIC – CN_INVOKE_FIPS service.

The pre-calculated signature is in the FW to be used for the FW integrity test

The voltage monitoring happens continuously by the module which samples the voltage rails for every 400 micro-seconds.

The temperature monitoring happens continuously by the module for every 30 seconds.

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below

N/A for this module.

The module performs the above Conditional Self-Tests.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC32 firmware integrity	KAT	SW/FW Integrity	daily	automatic
Firmware Integrity Test	KAT	SW/FW Integrity	daily	automatic
Temperature monitor test	CF	Critical Function	30 Seconds	automatic
Voltage monitor test	CF	Critical Function	400 micro Seconds	automatic

Table 26: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
FW- AES-CBC (SP 800-38A) Encrypt	KAT	CAST	daily	automatic
FW-AES-CBC (SP 800-38A) Decrypt	KAT	CAST	daily	automatic
AES-CCM (SP 800-38C) Encrypt	KAT	CAST	daily	automatic
AES-CCM (SP 800-38C) Decrypt	KAT	CAST	daily	automatic
FW-AES-CMAC (SP 800-38B) Sign	KAT	CAST	daily	automatic
FW-AES-CMAC (SP 800-38B) Verify	KAT	CAST	daily	automatic
AES-GCM (SP 800-38D) Decrypt	KAT	CAST	daily	automatic
FW-AES-GCM (SP 800-38D) Encrypt	KAT	CAST	daily	automatic
Hash DRBG (SP 800-90Ar1)	KAT	CAST	daily	automatic
FW-KAS-ECC-SSC (SP800-56Ar3)	KAT	CAST	daily	automatic
KBKDF (SP800-108)	KAT	CAST	daily	automatic
KDF TLS (CVL) (SP 800-135r1)	KAT	CAST	daily	automatic
RSA Decryption Primitive (CPT)	KAT	CAST	daily	automatic
FW-RSA Signature Primitive (CVL) (FIPS 186-4)	KAT	CAST	daily	automatic
SW-AES-CBC (SP 800-38A) Decrypt	KAT	CAST	daily	automatic
SW-AES-CBC (SP 800-38A) Encrypt	KAT	CAST	daily	automatic
SW-AES-CMAC (SP 800-38B) Sign	KAT	CAST	daily	automatic
SW-AES-CMAC (SP 800-38B) Verify	KAT	CAST	daily	automatic
SW-AES-GCM (SP 800-38D) Encrypt	KAT	CAST	daily	automatic
AES-KW (SP 800-38F) Unwrap	KAT	CAST	daily	automatic
AES-KW (SP 800-38F) Wrap	KAT	CAST	daily	automatic
Counter DRBG (SP 800-90Ar1)	KAT	CAST	daily	automatic
ECDSA SigGen	KAT	CAST	daily	automatic
SW-ECDSA SigGen	KAT	CAST	daily	automatic
ECDSA SigVer	KAT	CAST	daily	automatic
SW-ECDSA SigVer	KAT	CAST	daily	automatic
HMAC-SHA-1 (FIPS-198-1)	KAT	CAST	daily	automatic
HMAC-SHA2-256 (FIPS-198-1)	KAT	CAST	daily	automatic
HMAC-SHA2-512 (FIPS-198-1)	KAT	CAST	daily	automatic
HMAC-SHA3- 256(FIPS-202)	KAT	CAST	daily	automatic
KAS-ECC (SP800-56Ar3)	KAT	CAST	daily	automatic
SW-KAS-ECC-SSC (SP800-56Ar3)	KAT	CAST	daily	automatic
KAS-IFC-SSC (SP 800-56Br2)	KAT	CAST	daily	automatic
KDA HKDF Sp800-56Cr1	KAT	CAST	daily	automatic
HMAC-SHA-1	KAT	CAST	daily	automatic
HMAC-SHA2-256	KAT	CAST	daily	automatic
HMAC-SHA2-512	KAT	CAST	daily	automatic
HMAC-SHA3-256	KAT	CAST	daily	automatic
KDA OneStep (SP800-56Cr1)	KAT	CAST	daily	automatic
KDA TwoStep (SP800-56Cr1)	KAT	CAST	daily	automatic
KDF ANS 9.63 (SP 800-135r1)	KAT	CAST	daily	automatic
KDF (SP800-108) CMAC	KAT	CAST	daily	automatic
KDF (SP800-108) HMAC	KAT	CAST	daily	automatic
KDF TLS (SP 800-135r1)	KAT	CAST	daily	automatic
PBKDF (SP 800-132)	KAT	CAST	daily	automatic
RSA Decryption Primitive (SW)	KAT	CAST	daily	automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SW-RSA SigGen (FIPS186-5)	KAT	CAST	daily	automatic
SW-RSA SigVer (FIPS186-5)	KAT	CAST	daily	automatic
SW-RSA Signature Primitive (CVL) (FIPS 186-4)	KAT	CAST	daily	automatic
FW-RSA SigVer (FIPS186-5)	KAT	CAST	Daily	automatic
TDES-KW (SP 800-38F) Unwrap	KAT	CAST	daily	automatic
TDES (A7544) Unwrap	KAT	CAST	daily	automatic
UBOOT-RSA SigVer	KAT	SW/FW Load	daily	automatic
DRBG-Hash Health Tests	Health Test	CAST	daily	automatic
DRBG-AES-CTR Health Tests	Health Test	CAST	daily	automatic
KTS-IFC	KAT	CAST	daily	automatic
SW-ECDSA KeyGen (FIPS 186-4)	PCT	PCT	on key generation and import operation	automatic
FW-ECDSA KeyGen (FIPS 186-5)	PCT	PCT	on key generation and import operation	automatic
SW-RSA KeyGen (FIPS 186-5)	PCT	PCT	on key generation and import operation	automatic
FW-RSA KeyGen (FIPS 186-5)	PCT	PCT	on key generation andimport operation	automatic
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	on-power	automatic
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	on-power	automatic
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	on-power	automatic
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	on-power	automatic

Table 27: Conditional Periodic Information

The module performs above periodic self-test after every 24 hours.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
FIPS self-test failure	Module is no longer operational. The data output is inhibited. Only Unauthenticated status output is available.	FIPS self-test failure	Reboot	Red LED ON
Hardware RBG failure	Module is no longer operational. The data output is inhibited. Only Unauthenticated status output is available.	Hardware RBG failure	Reboot	Blue LED ON
Pairwise consistency test failure	Module is no longer operational. The data output is inhibited. Only Unauthenticated status output is available.	Any pairwise consistency test failure	Reboot	Blue LED ON

Table 28: Error States

On successful completion of the FIPS tests, the DA Green LED remains in the “ON” state.

If any other LED remains in the permanent glow, the card’s is in ERROR state. Any of these fatal errors will cause the module to reject all future commands received. Resetting the module is required to recover from the situation.

Bootloader-level self-test failures will reset the board automatically. There is no separate LED indication for this error.

All these fatal errors are shown on UART when the issue is observed. In addition, the latest errors are reported on UART on bootup. Because the logs are maintained within the module’s flash memory, which has no direct access to external users/ applications, they are not vulnerable to any tampering.

10.5 Operator Initiation of Self-Tests

The operator can command the module to perform the CASTs with the GP_INFO_DIAGNOSTIC – CN_INVOKE_FIPS service. The operator can also execute self-test by cycling power or resetting the module. Power-up self-tests do not require any operator action.

10.6 Additional Information

The module always executes the self-tests without operator intervention regardless of approved or non-approved mode or any other configuration.

Failure of any of the self-tests causes the module to go into an error state. If the failure happens during periodic execution of Cryptographic Algorithm Self-Tests (CASTs), then the module will reject all future commands received.

The module needs to be reset to recover from the situation. Only status output is allowed, and Data output is inhibited during self-tests, zeroization, and error states. Status output information does not contain CSPs or sensitive data. The conditional cryptographic algorithm self-tests (CASTs) run periodically. The periodicity is configurable by the MCO and by default runs every 24 hours.

The execution of CASTs causes a momentary (less than a second) service interruption.

- Conditional pair-wise consistency test
  - ECDSA/ECDH Pairwise Consistency Test (ECDSA FIPS 186-5 & KAS-ECC-SSC) are performed at the time of key generation and import.
  - RSA Pairwise Consistency Test (RSA FIPS 186-4 & SP 800-56Br2) are performed at the time of key generation and import.
- Periodic Conditional self-tests
  - Module performs periodic self-tests CASTs every 24 hours or as configured by MCO.
  - Temperature monitor test: every 30 Seconds
  - Voltage monitor test: every 400 micro seconds

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Delivery
The LS2 HSMs are shipped directly to the operator using a trusted and trackable carrier. Each unit box is packaged in a tamper-evident bag. The packaging includes a packing slip listing product name, unique serial number and part number.
Upon receipt of the LS2 HSM, the customer is required to perform the following verification steps:

- Confirm that the shipping label accurately reflects the intended recipient's name and the correct serial number and part number.
- Inspect the Electrostatic Discharge (ESD) bag in which the HSM is placed in the shipping container is sealed and has not been tampered with.
- Verify that the external labels match the expected delivery information and the product details.
- Match the hardware serial number and part number printed on the device with those listed on the shipping bag label and documentation.
- Verify that there is no evidence of physical tampering on the HSM itself.

Installation
After this is verified, the customer can physically insert the HSM into the PCIe on the host server.

The host must meet the following requirements:

- Support low-profile PCIe Gen 3/Gen 4 (x4 or x8 slot)
- SR-IOV support enabled.

After the HSM is physically installed, the LS2 driver and utilities that communicate with the HSM are installed on the host using standard Linux/Operating system tools. The user must be logged in as the host as root/Administrator to perform the installation.

The HSM owner then completes the following steps to claim ownership of the HSM and enable the approved mode:

1. Loads the driver (command: insmod).
2. Invokes Cfm2Master Utility and logs in as default crypto officer (CO) and default password provided as part of the User Guide and initializes the HSM.

For example:
Command: *initHSM -p -sO -fips_state [2 | 3]*

As part of initializing the HSM:

- The Master Crypto Officer is created with username/password.
- The fips_state flag is set on the HSM (non-Approved, Approved with single- or dual-factor authentication, or Approved with dual-factor authentication required).

As a final step, the HSM owner claims the HSM by loading the adapter owner certificates (AOTAC and AOAC) on the HSM and import the HSM owner fixed backup key (OKBK). These steps are taken by the MCO using Cfm2MasterUtil.

Example command syntax:

Command: *storeCert -s <cert-type> -f <Adapter Owner Trust Anchor Cert (AOTAC).crt*

Command: *storeCert -s <cert-type> -f <Adapter Owner Auth Cert (AOAC).crt*

Command: *storeMCOFixedKey -f <OKBK file>*

11.2 Administrator Guidance

The specific tasks that can be performed by users on the HSM are strictly limited by their user role (see Table 8 for details).

A user of the module can query the module's device information, operational parameters, operating mode by invoking the command getHSMInfo from the Cfm2MasterUtil. "FIPS state" member of the output will indicate the module to be in one of the following modes:

- Approved mode with 1FA ("2")
- Approved mode with 2FA ("3")
- Non-Approved mode ("0")
- Zeroized ("-1")

Example command syntax:

Command: *getHSMInfo*

The following compliance-specific conditions are applicable to the HSM module:

- Crypto Officer must maintain control of the module while the zeroization process is executing.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support a maintenance interface or role.
- The module does not support bypass capabilities. The module does not support manual key entry.
- The module has no CSP feedback to operators.
- The module does not enter or output plaintext CSPs.
- The module does not output intermediate key values part of any operation.
- The module has no CSP feedback to operators. The module does not output intermediate key values part of any operation.
- The cryptographic module clears previous authentications on power cycle. The module does not let access SSPs between approved/non-approved and requires zeroization of the HSM/partition.
- When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

- The module is delivered to the users using the following secure distribution mechanism.
- The module is attached with a specific part number and serial number labels. And, kept in a tamper evident ESD bag with the same labels.
- Then the ESD bags are put inside a shipping box and delivered to customers using any preferred shipping carriers.

- Optionally the modules are locked to a given customer using the AOTAC cert during the manufacturing process and is locked to not run any other commands unless AOAC loaded as per the steps mentioned above.

HSM Zeroization
The instances of zeroization mentioned below are executed through the utilities.

There are different types of zeroization which can be executed through utilities:

- zeroizeHSM --> example command: Cfm2MasterUtil singlecmd zeroizeHSM.
  This zeroizeHSM will delete all the Partition which in turn will zeroize all the partition CSPs, including cleanup all the temporary SSPs.
  - This maps to GP_ZEROIZATION - CN_ZEROIZE service

- zeroizeHSM along with option (-factory_reset) can be used by operator to zeroize all non-vendor specific CSSPs.
  - This maps to GP_ ZEROIZATION - CN_ZEROIZE service with –factory_reset option

- VENDOR zeroizeHSM can be used to zeroize all SSPs.
  To operate a VENDOR zeroizeHSM the operator must log-in as Crypto Officer with its credentials. Without the credentials of the crypto officer, the vendor zeroize can't be executed.
  - This maps to GP_ ZEROIZATION - CN_VENDOR_ZEROIZE service

Notes:

- Temporary SSPs (like in this case: session keys and Integrity test values) are forcefully memset to 0 during session close, application close, partition deletion and zeroization of the partition or the HSM
- Reboot is a power cycle operation which will lead to the zeroization of temporary SSPs like session Keys.
- Zeroization of a partition or HSM execution can take a few minutes to complete. The zeroization request command is blocked until the execution is completed only after zeroization of required CSPs is completed. User is notified about delay with a notification log as depicted below. The Operator must remain in control of the module while the zeroization process is executing.
  For example: (the output below is executed through Marvell provided driver utilities):

  Cfm2MasterUtil singlecmd zeroizeHSM
  Version info, Driver Version: 10.02.11.01, SDK API Version: 10.02.11.01

  Cfm2AppInitWithExtNonce () returned app id : 000e0000

  Cfm2OpenSession2() returned 0x00 : HSM Return: SUCCESS

  Command: zeroizeHSM

  Successful zeroization of HSM will reboot the HSM and
  Host-HSM handshake will be re-done.
  Please wait, this may take few minutes.

Cfm2ZeroizeHSM returned: 0x00 : HSM Return: SUCCESS

Current FIPS mode is: ffffffff

Note: Unsigned *ffffffff* indicates zeroized, which is –1.

- DRBG context : On zeroizeHSM command DRBG related contexts are reset. This means that the internal state of the context with respect to DRBG become unusable.
- In case the power is lost unexpectedly and if the TDES keys are permanent keys, then the module can continue to use the TDES keys for encryption after the module restart as well, until the encryption limit is reached.
- On a routine basis, the MCO can verify that the HSM is correctly operating in approved mode by providing MCO credentials and invoking the command “fipsTest” from the Cfm2MasterUtil utility. The fipsTest utility invokes GP_INFO_DIAGNOSTIC - CN_INVOKE_FIPS service to perform the CAST.

  Example command syntax:

  Command: *fipsTest*

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

Rules of Operation

1. The Module provides three distinct operator roles: Crypto User, Audit User and Cryptographic Officer.
2. The Module provides role-based/identity-based authentication.
3. The Module clears previous authentications on power cycle (Level 2-4).
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, sw/fw loading and error states.
8. Cryptographic operations are inhibited in all error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
10. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.

11. The Module does support concurrent operators.
12. The Module does not support a maintenance interface or role.
13. The Module does not support manual SSP establishment method.
14. The Module does not have any proprietary external input/output devices used for entry/output of data.
15. The Module does not enter or output plaintext CSPs.
16. *The Module does not store any plaintext CSPs*
17. The Module does not output intermediate key values.
18. The Module does not provide bypass services for ports/interfaces.

11.5 Maintenance Requirements

N/A

11.6 End of Life

Sanitization of the module is achieved through factory-reset which is a zeroization command for the module. Zeroization of a partition or HSM execution can take a few minutes to complete. The zeroization request command is blocked until the execution is completed only after zeroization of required CSPs is completed. The operator is notified about a delay with a notification log as depicted below. The operator must remain in control of the module while the zeroization process is executing.

For example: (the output below is executed through Marvell provided driver utilities):

Version info, Driver Version: 10.23.06.01, SDK API Version: 10.23.06.01

Cfm2AppInitWithExtNonce () returned app id : 0076c000

Cfm2OpenSession2() returned 0x00 : HSM Return: SUCCESS

Cfm2LoginHSM returned: 0x00 : HSM Return: SUCCESS
Command: zeroizeHSM -vendor

###Warning: Zeroizes HSM including vendor configuration. This operation cannot be reversed and HSM may not be recovered.
Do you want to continue [y/Y or n/N]

Successful zeroization of HSM will reboot the HSM and
Host-HSM handshake will be re-done.
Please wait, this may take few minutes.

Cfm2VendorZeroizeHSM returned: 0x00 : HSM Return: SUCCESS

The Sanitization can also be done with the button zeroize by pressing the button for 3 seconds.

Once the zeroization is performed, it is recommended to put 8 drills across the module for Shredding.

More specific details can be provided on the need basis.

12 Mitigation of Other Attacks

N/A - No mitigation of other attacks is implemented by the module.

References and Definitions

The following standards are referred to in this Security Policy.

Table 29 References

Abbreviation	Full Specification Name
[FIPS140-3]	Security Requirements for Cryptographic Modules, March 22, 2019
[ISO19790]	International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017
[ISO24759]	International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015
[IG]	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, September 2, 2025
[108]	NIST Special Publication 800-108rev1, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), February 2024
[133]	NIST Special Publication 800-133rev2, Recommendation for Cryptographic Key Generation, Revision 2, June 2020
[135]	National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.
[186-4]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.
[186-5]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 3, 2023.
[197]	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001
[198]	National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008
[180]	National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015
[202]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015
[38A]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001
[38B]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005

Abbreviation	Full Specification Name
[38C]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004
[38D]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007
[38F]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012
[56Ar3]	NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018
[56Br2]	NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019
[56Cr2]	NIST Special Publication 800-56C Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, August 2020
[67]	National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.
[90B]	National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.

Table 30 Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
APT	Adaptative Proportion Test
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Cryptographic Security Parameter
CTR	Counter Mode

Acronym	Definition
DES	Data Encryption Standard
DF	Derivation Function
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ESV	Entropy Source Validation
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Hash Message Authentication Code
IG	Implementation Guidance
KAS	Key Agreement Schema
KAT	Know Answer Test
KTS	Key Transport Schema
KW	AES Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PCT	Pairwise consistency test
RNG	Random Number Generator
RCT	Repetition Count Test
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
TDES	Triple-DES