Marvell Semiconductor, Inc.

LS2 HSM Family module

FIPS 140-3 Non-Proprietary Security Policy



This document may freely be reproduced and distributed in its entirety

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 10
2.3 Excluded Components 12
2.4 Modes of Operation 13
2.5 Algorithms 13
2.6 Security Function Implementations 24
2.7 Algorithm Specific Information 42
2.8 RBG and Entropy 44
2.9 Key Generation 44
2.10 Key Establishment 44
2.11 Industry Protocols 45
3 Cryptographic Module Interfaces 45
3.1 Ports and Interfaces 45
3.2 Additional Information 46
4 Roles, Services, and Authentication 46
4.1 Authentication Methods 46
4.2 Roles 47
4.3 Approved Services 47
4.4 Non-Approved Services 116
4.5 External Software/Firmware Loaded 127
5 Software/Firmware Security 127
5.1 Integrity Techniques 127
5.2 Initiate on Demand 127
6 Operational Environment 127
6.1 Operational Environment Type and Requirements 127
6.2 Additional Information 128

7 Physical Security....128
7.1 Mechanisms and Actions Required....128
7.2 EFP/EFT Information....128
7.3 Hardness Testing Temperature Ranges....129
8 Non-Invasive Security....129
8.1 Mitigation Techniques....129
9 Sensitive Security Parameters Management....129
9.1 Storage Areas....129
9.2 SSP Input-Output Methods....129
9.3 SSP Zeroization Methods....131
9.4 SSPs....132
9.5 Transitions....175
10 Self-Tests....176
10.1 Pre-Operational Self-Tests....176
10.2 Conditional Self-Tests....176
10.3 Periodic Self-Test Information....182
10.4 Error States....185
10.5 Operator Initiation of Self-Tests....186
10.6 Additional Information....186
11 Life-Cycle Assurance....187
11.1 Installation, Initialization, and Startup Procedures....187
11.2 Administrator Guidance....187
11.3 Non-Administrator Guidance....191
11.4 End of Life....191
12 Mitigation of Other Attacks....192
12.1 Attack List....192

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 12
Table 3: Modes List and Description 13
Table 4: Approved Algorithms 20
Table 5: Vendor-Affirmed Algorithms 20
Table 6: Non-Approved, Allowed Algorithms 21
Table 7: Non-Approved, Allowed Algorithms with No Security Claimed 21
Table 8: Non-Approved, Not Allowed Algorithms 24
Table 9: Security Function Implementations 41
Table 10: Entropy Certificates 44
Table 11: Entropy Sources 44
Table 12: Ports and Interfaces 46
Table 13: Authentication Methods 47
Table 14: Roles 47
Table 15: Approved Services 116
Table 16: Non-Approved Services 127
Table 17: Mechanisms and Actions Required 128
Table 18: EFP/EFT Information 129
Table 19: Hardness Testing Temperatures 129
Table 20: Storage Areas 129
Table 21: SSP Input-Output Methods 131
Table 22: SSP Zeroization Methods 132
Table 23: SSP Table 1 157
Table 24: SSP Table 2 175
Table 25: Pre-Operational Self-Tests 176
Table 26: Conditional Self-Tests 182
Table 27: Pre-Operational Periodic Information 182
Table 28: Conditional Periodic Information 185
Table 29: Error States 186

List of Figures

Figure 1: Liquid Security2 Cryptographic module boundary 8
Figure 2: Liquid Security2 HSM Top View 8
Figure 3: Liquid Security2 HSM bottom View 9
Figure 4: Block Diagram 10
Figure 5: User Guide Snapshot_1 190
Figure 6: User Guide Snapshot_2 191

1 General

1.1 Overview

The 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 TDES) 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 2.5.

1.2 Security Levels

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

1.3 Additional Information

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-3.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The LS2 HSM Family 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: ARM-based control processor, ARM-based microcontroller, RAM memory, NOR and eMMC flash for persistent storage, USB FTDI interfaces, and PCIe gen-4 x8 with SMBus interfaces.

- Partitions
  The module 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 and, 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). The module always has one default partition called the master partition, which exposes the interfaces to create, delete, and update the remaining partitions. The module 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 module. The module 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 space 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/pHSM to issue any authorized commands. Users are authenticated using passwords submitted during the user creation.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Module Characteristics:

Cryptographic Boundary:

The module's cryptographic boundary is defined as 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.

Figure 1 depicts the module's cryptographic boundary depicted in the red dashed line. The APP shown under the blue dashed line are the excluded firmware component.

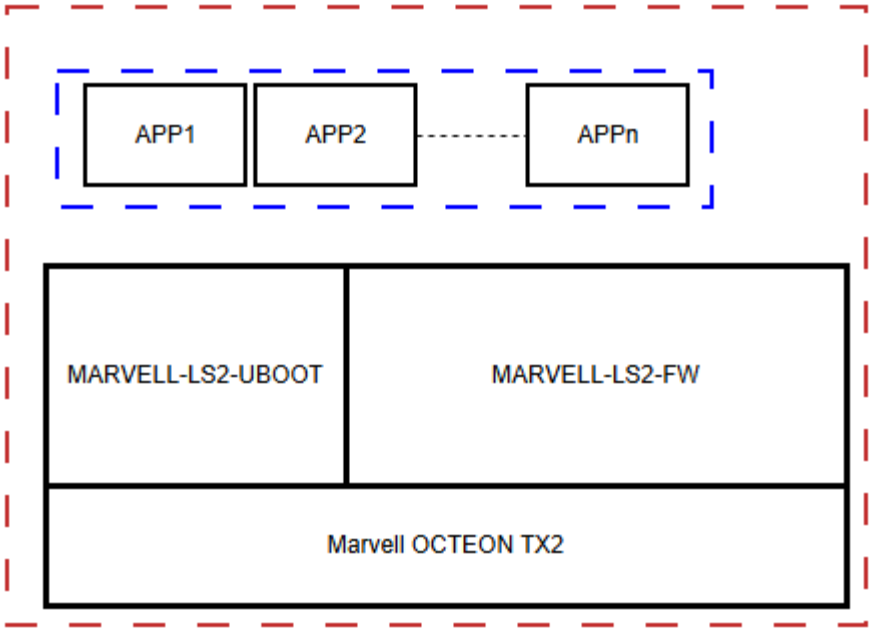


Figure 1: Liquid Security2 Cryptographic module boundary

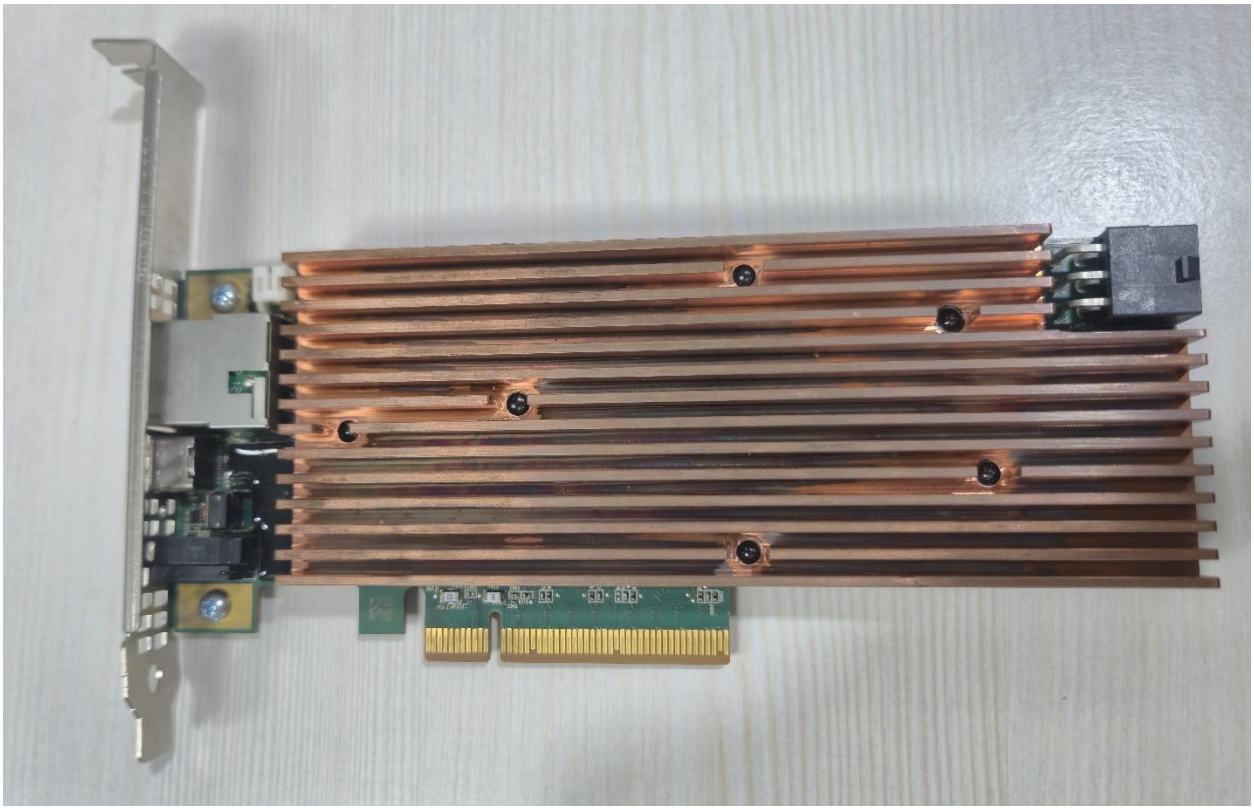


Figure 2: Liquid Security2 HSM Top View

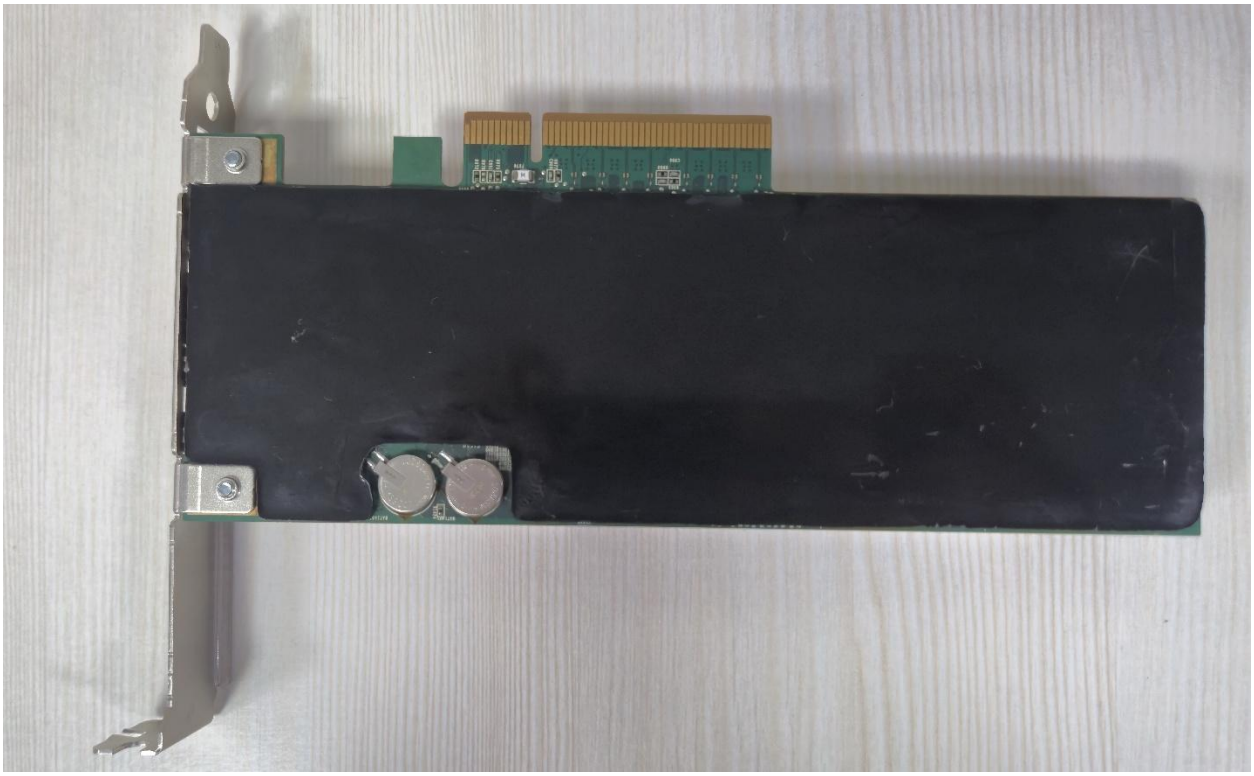


Figure 3: Liquid Security2 HSM bottom View

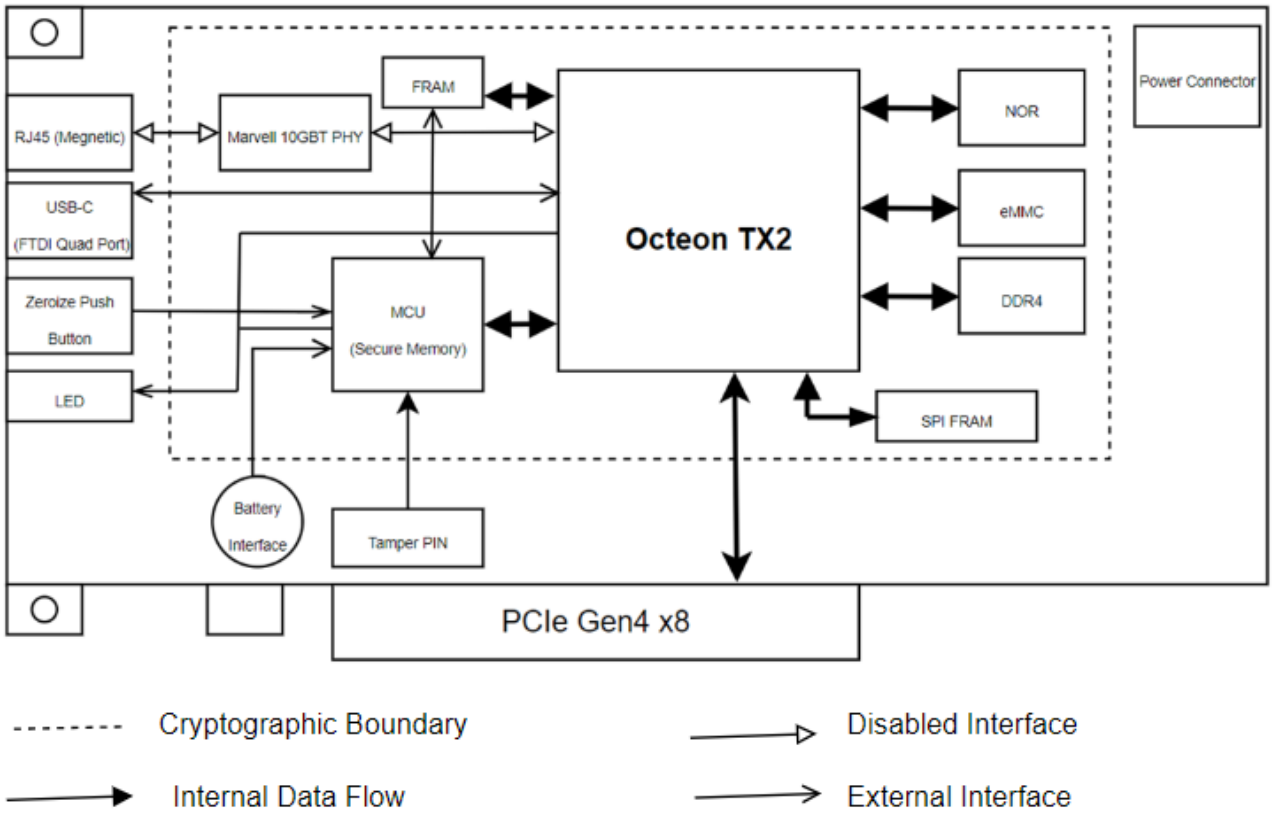


Figure 4: Block Diagram

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-G-A050-F5-L-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 50% of full card capacity.
LS2-G-A050-IB-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 50% of full card capacity.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
LS2-G-A100-AL-L-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 75% of full card capacity.
LS2-G-A100-AR-L-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 75% of full card capacity.
LS2-G-A100-ES-L-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 75% of full card capacity.
LS2-G-A100-F5-L-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 75% of full card capacity.
LS2-G-A100-GM-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 75% of full card capacity.
LS2-G-A100-MI-L-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 75% of full card capacity.
LS2-G-A300-AR-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers full card capacity.
LS2-G-A300-ES-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers full card capacity.
LS2-G-A300-GA-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers full card capacity.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
LS2-G-A300-MI-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers full card capacity.
LS2-O-A050-IB-F-B0	CN9310410-03 C	MARVELL-LS2-FW-10.24-0703, MARVELL-LS2-UBOOT-10.24-0702-R01-SB, MARVELL-LS2-UBOOT-10.24-0702-R02-SB, HPS-App:10.24-0703	Octeon_TX2	Offers 50% of full card capacity.

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

The following components are excluded from the cryptographic boundary as they do not perform any cryptographic functions and are not connected to any security-relevant circuitry. These components serve only as passive electrical components.

- Fuses (3) visible outside of the epoxy
- Resistors visible outside of the epoxy
- Capacitors visible outside of the epoxy

The following platform/HPS application is excluded from the cryptographic boundary:

- HPS-App:10.24-0703

Note: The scope of this certificate includes the firmware and bootloader approved for use within the module. Any platform application running on the platform/HPS partitions must obtain its own FIPS 140-3 certificate.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
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/nonApprovedAllowedNSC algorithms. Request for any nonApprovedNotAllowed algorithm is rejected.	Approved	fips_mode = 2 or 3
Non-approved mode	In this mode, the module also allows nonApprovedNotAllowed algorithms as well.	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. The following values are allowed for the fipsState parameter:
-1 - 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 GP_INFO_DIAGNOSTIC service. The fipsState field of the GP_INFO_DIAGNOSTIC 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	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6875	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6875	Key Length - 128, 192, 256	SP 800-38C
AES-CMAC	A1948	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A6875	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A1948	Key Length - 256	SP 800-38A
AES-CTR	A6875	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A1948	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6875	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	SP 800-38D
AES-GCM	A6875	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A6875	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-KW	A1948	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A1948	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
Counter DRBG	A1948	Prediction Resistance - No, Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
cSHAKE-128	A6875	Message Length - Message Length: 0-65536 Increment 8	SP 800-185
cSHAKE-256	A6875	Message Length - Message Length: 0-65536 Increment 8	SP 800-185
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)	A6876	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-4)	A1948	Curve - 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	FIPS 186-4
ECDSA SigGen (FIPS186-5)	A6875	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A1948	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A6875	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-384, SHA2-512	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-5)	A6878	Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-5
EDDSA KeyGen	A6875	Curve - ED-25519, ED-448	FIPS 186-5
EDDSA KeyVer	A1948	Curve - ED-25519, ED-448	FIPS 186-5
EDDSA KeyVer	A6875	Curve - ED-25519, ED-448	FIPS 186-5
EDDSA SigGen	A1948	Curve - ED-25519, ED-448 PreHash - No Pure - Yes	FIPS 186-5
EDDSA SigGen	A6875	Curve - ED-25519, ED-448 PreHash - Yes Pure - Yes	FIPS 186-5
EDDSA SigVer	A1948	Curve - ED-25519, ED-448 PreHash - No Pure - Yes	FIPS 186-5
EDDSA SigVer	A6875	Curve - ED-25519, ED-448 PreHash - Yes Pure - Yes	FIPS 186-5
Hash DRBG	A6875	Prediction Resistance - Yes Mode - SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-224	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-256	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-384	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA2-512	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-224	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-256	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-384	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6875	Key Length - Key Length: 8-8192 Increment 8	FIPS 198-1
HMAC-SHA3-512	A1948	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6875	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 Scheme - ephemeralUnified - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Key Length - 512	SP 800-56A Rev. 3
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	A6875	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	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A1948	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	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-1024 Increment 8	SP 800-56C Rev. 2
KDA TwoStep Sp800-56Cr1	A1948	Derived Key Length - 4096 Shared Secret Length - Shared Secret Length: 224-1024 Increment 8	SP 800-56C Rev. 2

Algorithm	CAVP Cert	Properties	Reference
KDF ANS 9.63 (CVL)	A1948	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Data Length - Key Data Length: 128, 4096	SP 800-135 Rev. 1
KDF KMAC Sp800-108r1	A6875	Derived Key Length - Derived Key Length: 112-4096 Increment 8	SP 800-108 Rev. 1
KDF SP800-108	A1948	KDF Mode - Counter Supported Lengths - Supported Lengths: 64-2048 Increment 8	SP 800-108 Rev. 1
KDF SP800-108	A6875	KDF Mode - Counter Supported Lengths - Supported Lengths: 64-2048 Increment 8	SP 800-108 Rev. 1
KMAC-128	A6875	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-4088 Increment 8	SP 800-185
KMAC-256	A6875	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-4088 Increment 8	SP 800-185
KTS-IFC	A1948	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-crt Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 320	SP 800-56B Rev. 2
KTS-IFC	A6876	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-crt Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 320	SP 800-56B Rev. 2
ML-DSA KeyGen	A6877	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A6877	Signature Interfaces - external, internal Pre Hash - pure Deterministic - No, Yes External Mu - No, Yes Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87 Message Length - Message Length: 8-65536 Increment 8 Context Length - Context Length: 0-2040 Increment 8	FIPS 204
ML-DSA SigVer	A6877	Signature Interfaces - external, internal Pre Hash - pure	FIPS 204

Algorithm	CAVP Cert	Properties	Reference
		External Mu - No, Yes Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87 Message Length - Message Length: 8-65536 Increment 8 Context Length - Context Length: 0-2040 Increment 8	
ML-KEM EncapDecap	A6877	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Encapsulation	FIPS 203
ML-KEM KeyGen	A6877	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203
PBKDF	A1948	Iteration Count - Iteration Count: 1-10000000 Increment 1 Password Length - Password Length: 8-128 Increment 8	SP 800-132
RSA Decryption Primitive (CVL)	A1948	Modulus Length - 2048	FIPS 186-4
RSA Decryption Primitive Sp800-56Br2 (CVL)	A6875	Modulo - 2048, 3072, 4096	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A1948	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2pow100 Private Key Format - crt, standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A1948	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA Signature Primitive (CVL)	A1948	Private Key Format - standard	FIPS 186-5
RSA Signature Primitive (CVL)	A6875	Modulo - 2048, 3072, 4096	FIPS 186-5
RSA SigVer (FIPS186-5)	A1948	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6878	Modulo - 2048 Signature Type - pkcs1v1.5	FIPS 186-5
SHA-1	A1948	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA-1	A6875	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A1948	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A6875	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A1948	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A6875	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A6878	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A1948	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A6875	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A1948	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6875	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6878	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-224	A1948	Supports Bit-Oriented Messages - No Supports Empty Message - Yes	FIPS 202
SHA3-224	A6875	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	A6875	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	A6875	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	A6875	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHAKE-128	A1948	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-128	A6875	Output Length - Output Length: 16-2040 Increment 8	FIPS 202
SHAKE-128	A6877	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A1948	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A6875	Output Length - Output Length: 16-2040 Increment 8	FIPS 202
SHAKE-256	A6877	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
TDES-CBC	A1948	Direction - Decrypt	SP 800-67 Rev. 2
TDES-CBC	A6875	Direction - Decrypt	SP 800-67 Rev. 2
TDES-ECB	A6875	Direction - Decrypt	SP 800-67 Rev. 2
TDES-KW	A1948	Direction - Decrypt	SP 800-38F

Algorithm	CAVP Cert	Properties	Reference
TLS v1.2 KDF RFC7627 (CVL)	A6875	Hash Algorithm - SHA2-256, SHA2-384	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.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG1	Key Type:Symmetric and Asymmetric key generation	LS2-SW-Crypto	SP 800-133Rev2 Section-4 Example 1
CKG2	Key Type:Symmetric and Asymmetric key generation	LS2-CPT	SP 800-133Rev2 Section-4 Example 1
CKG3	Key Type:Symmetric	LS2-SW-Crypto	SP 800-133Rev2 Section-4 Example 2
CKG4	Key Type:Symmetric	LS2-CPT	SP 800-133Rev2 Section-4 Example 2

Table 5: Vendor-Affirmed Algorithms

The cryptographic module supports the above Vendor Affirmed Algorithms.

Non-Approved, Allowed Algorithms:

Name	Properties	Implementation	Reference
EC Diffie-Hellman 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)	LS2-CPT	Per IGs D.F and C.A. 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)	LS2-CPT	Per IG C.A. Prime order curve, generated as per FIPS 186-5 Section 6
SW-AES-CBC (unwrap)	Legacy Algorithm:True Mode:Decrypt Key Sizes:128, 192, and 256-bit	LS2-SW-Crypto	Key unwrapping. Per IG D.G.
SW-AES-ECB (unwrap)	Legacy Algorithm:True Mode:Decrypt Key Sizes:128, 192, and 256-bit	LS2-SW-Crypto	Key unwrapping. Per IG D.G.

Name	Properties	Implementation	Reference
SW-TDES-KW-Unwrap	Legacy Algorithm:True Mode:Unwrap Key Sizes:192-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
SHA-1	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

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
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
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
KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant)	Generates 2048, 3072, and 4096-bit keys, Uses Counter DRBG (SP800- 90Ar1) (#A1948) as underlying Random Generator
KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant)	ECDH key derivation and ECDH-AES key wrap
KAS-KDA-HKDF (SP800-56Ar3) (non-compliant)	ECDH key derivation and ECDH-AES key wrap

Name	Use and Function
ML-DSA ECDSA Sign (non-compliant)	Signature generation function which generate a concatenated signature of ML_DSA and ECDSA
ML-DSA ECDSA Verify (non-compliant)	Signature verification function which verifies a concatenated signature of ML_DSA and ECDSA
ML-KEM ECDH (non-compliant)	Key wrap/unwrap function which uses combination of ML-KEM and ECDH
ML-KEM ECDH Derive (non-compliant)	Key derivation function which uses combination of ML-KEM and ECDH
ML-KEM RSA (non-compliant)	Key wrap/unwrap function which uses combination of ML-KEM and RSA OAEP
Shamir Key Share (non-compliant)	Key share
SW-AES-CBC (non-compliant)	Data encryption, Decryption and key unwrap
SW-AES-CMAC (non-compliant)	MAC Generation and verification
SW-AES-ECB (non-compliant)	Data encryption, Decryption and key unwrap
SW-AES-GCM (non-compliant)	AES GCM encryption/decryption.
SW-AES-KW (non-compliant)	Key wrap (TR31/TR34/AES-CBC/AES-GCM, wrap/unwrap), DecimalTable/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
SW-AES-KWP (non-compliant)	Key wrap (TR31/TR34/AES-CBC/AES-GCM, wrap/unwrap), DecimalTable/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
SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant)	Random number generation for user,keys, internal IVs, and salt
SW-ECDSA-KeyGen (FIPS186-4) (non-compliant)	Generates 224, 256, 384, 521 bits ECC keys
SW-ECDSA-SigGen (FIPS186-4) (non-compliant)	ECDSA Sign P192, Secp192k1, brainpoolP160r1, brainpool192r1, K-163 and B-163 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
SW-ECDSA-SigVer (FIPS186-4) (non-compliant)	ECDSA Sign Verify P192, Secp192k1, brainpoolP160r1, brainpool192r1, K-163 and B-163 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
SW-EDDSA (FIPS186-4) (non-compliant)	ED25519 and ED-448 Key generation, Sign, Verify
SW-HMAC-SHA-1 (non-compliant)	MAC Generation, Verify and KDF

Name	Use and Function
SW-HMAC-SHA2-224 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA2-256 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA2-384 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA2-512 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA3-224 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA3-256 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA3-384 (non-compliant)	MAC Generation, Verify and KDF
SW-HMAC-SHA3-512 (non-compliant)	MAC Generation, Verify and KDF
SW-KAS-ECC-Sp800-56Ar3 (non-compliant)	Cloning protocol
SW-KDA-HKDF-Sp800-56Cr1 (non-compliant)	ECDH key derivation and ECDH-AES key wrap
SW-RSA-Decryption-Primitive (non-compliant)	Generates 2048, 3072, and 4096-bit keys, Uses Counter DRBG (SP800- 90Ar1) (#A1948) as underlying Random Generator
SW-RSA-KeyGen (FIPS186-5) (non-compliant)	Generates 2048, 3072, and 4096-bit keys, Uses Counter DRBG (SP800- 90Ar1) (#A1948) as underlying Random Generator
SW-RSA-SigGen (FIPS186-5) (non-compliant)	Signature Generation FIPS 186-5 PKCS #1 1.5 and PSS Sig Gen: 2048, 3096, and 4096-bit (SHA-2 256, 384, and 512)
SW-RSA-SigVer (FIPS186-5) (non-compliant)	Signature Verification FIPS 186-5 PKCS #1 1.5 and PSS Sig Gen: 2048, 3096, and 4096-bit (SHA-2 256, 384, and 512)
SW-SHA2-256 (non-compliant)	Hash Generation
SW-TDES (SP 800-38B) (non-compliant)	Fingerprint key size 192 bit (Generation and Verify)

Name	Use and Function
SW-TDES-CBC (non-compliant)	3-key Triple-DES CBC data encryption/decrypt
SW-TDES-CBC [192-bit] (non-compliant)	Data Decryption 3-key Triple-DES decrypt (supports only 192-bit size)
SW-TDES-ECB (non-compliant)	3-key Triple-DES ECB data encryption/decrypt
SW-TDES-ECB [192-bit] (non-compliant)	Data Decryption 3-key Triple-DES decrypt (supports only 192-bit size)
SW-TDES-KW (non-compliant)	Key wrap (TR31/TR34/TDES, wrap/unwrap)

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
CPT-AES-CBC	BC-UnAuth	Un-Auth Encryption and Decryption	Publication:SP800-38A	AES-CBC: (A6875)
CPT-AES-CCM	BC-Auth	Authenticated Encryption and Decryption	Publication:SP800-38C	AES-CCM: (A6875) AES-CBC: (A6875)
CPT-AES-CMAC	MAC	MAC Sign and Verify	Publication:SP800-38B	AES-CMAC: (A6875) AES-CBC: (A6875)
CPT-AES-CTR	BC-UnAuth	Un-Auth Encryption and Decryption	Publication:SP800-38A	AES-CTR: (A6875) AES-ECB: (A6875)
CPT-AES-ECB	BC-UnAuth	Un-Auth Encryption and Decryption	Publication:SP800-38A	AES-ECB: (A6875)
CPT-AES-GCM	BC-Auth	Authenticated Encryption and Decryption	Publication:SP800-38D	AES-GCM: (A6875) AES-ECB: (A6875)
CPT-AES-GMAC	MAC	MAC	Publication:SP800-38D	AES-GMAC: (A6875) AES-ECB: (A6875)

Name	Type	Description	Properties	Algorithms
CPT-ECDH-NON-NIST	KAS-SSC	EC Diffie-Hellman with non-NIST recommended curves	Caveat:Per IGs D.F and C.A Publication:SP 800-56A Rev. 3	KAS-ECC-SSC Sp800-56Ar3: (A6875) Curves: Secp224k1(112 bits), Secp256K1 (128 bits), brainpoolP224r1 (112 bits), brainpoolP256r1 (128 bits), brainpoolP320r1 (160 bits), brainpoolP384r1 (192 bits), brainpoolP512r1 (256 bits)
CPT-ECDSA-SigGen (FIPS186-4)	DigSig-SigGen	ECC Signature Generation	Publication:FIPS186-4	ECDSA SigGen (FIPS186-5): (A6875) Curves: P-224, P-256, P-384 and P-521 SHA2-224: (A6875) SHA2-256: (A6875) SHA2-384: (A6875) SHA2-512: (A6875)
CPT-ECDSA-SigGen-NON-NIST	DigSig-SigGen	ECDSA with non-NIST recommended curves	Caveat:Per IG C.A Publication:FIPS 186-4	ECDSA SigGen (FIPS186-5): (A6875) Curves: secp256K1 (128 bits), brainpoolP224r1 (112 bits), brainpoolP256r1 (128 bits), brainpoolP320r1 (160 bits), brainpoolP384r1 (192 bits), brainpoolP512r1 (256 bits) SHA2-224: (A6875)

Name	Type	Description	Properties	Algorithms
				SHA2-256: (A6875) SHA2-384: (A6875) SHA2-512: (A6875)
CPT-ECDSA-SigVer (FIPS186-4)	DigSig-SigVer	ECC Signature Verification	Publication:FIPS186-4	ECDSA SigVer (FIPS186-5): (A6875) Curves: P-224, P-256, P-384 and P-521 SHA2-384: (A6875) SHA2-512: (A6875)
CPT-EDDSA-KeyGen (FIPS186-5)	AsymKeyPair-KeyGen	EDDSA key Generation	Publication:FIPS186-5	EDDSA KeyGen: (A6875) Curves: ED-25519 and ED-448 CKG2: () Key Type: Symmetric and Asymmetric key generation SHA2-512: (A6875) SHAKE-256: (A6875)
CPT-EDDSA-KeyVer (FIPS186-5)	AsymKeyPair-KeyVer	EDDSA key Verification	Publication:FIPS186-5	EDDSA KeyVer: (A6875) Curves: ED-25519 and ED-448
CPT-EDDSA-SigGen (FIPS186-5)	DigSig-SigGen	EDDSA Signature Generation	Publication:FIPS186-5	EDDSA SigGen: (A6875) SHA2-512: (A6875) SHAKE-256: (A6875)
CPT-EDDSA-SigVer (FIPS186-5)	DigSig-SigVer	EDDSA Signature Verification	Publication:FIPS186-5	EDDSA SigVer: (A6875) Curves: ED-25519 and ED-448 SHAKE-256: (A6875)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A6875)
CPT-Hash-DRBG	DRBG	Hash DRBG	Publication:SP800-90Arev1	Hash DRBG: (A6875) CKG2: () Key Type: Symmetric and Asymmetric key generation SHA2-512: (A6875)
CPT-HMAC-SHA-1	MAC	HMAC-SHA-1	Publication:FIPS 198-1	HMAC-SHA-1: (A6875) MAC Length: 160 bits Key Length: 112-800 bits SHA-1: (A6875)
CPT-HMAC-SHA2-224	MAC	HMAC-SHA2-224	Publication:FIPS 198-1	HMAC-SHA2-224: (A6875) MAC Length: 224 bits Key Length: 112 bits - 800 bits SHA2-224: (A6875)
CPT-HMAC-SHA2-256	MAC	HMAC-SHA2-256	Publication:FIPS 198-1	HMAC-SHA2-256: (A6875) SHA2-256: (A6875)
CPT-HMAC-SHA2-384	MAC	HMAC-SHA2-384	Publication:FIPS 198-1	HMAC-SHA2-384: (A6875) SHA2-384: (A6875)
CPT-HMAC-SHA2-512	MAC	HMAC-SHA2-512	Publication:FIPS 198-1	HMAC-SHA2-512: (A6875) SHA2-512: (A6875)
CPT-HMAC-SHA3-224	MAC	HMAC-SHA3-224	Publication:FIPS 198-1	HMAC-SHA3-224: (A6875) SHA3-224: (A6875)
CPT-HMAC-SHA3-256	MAC	HMAC-SHA3-256	Publication:FIPS 198-1	HMAC-SHA3-256: (A6875) SHA3-256: (A6875)
CPT-HMAC-SHA3-384	MAC	HMAC-SHA3-384	Publication:FIPS 198-1	HMAC-SHA3-384: (A6875)

Name	Type	Description	Properties	Algorithms
				SHA3-384: (A6875)
CPT-HMAC-SHA3-512	MAC	HMAC-SHA3-512	Publication:FIPS 198-1	HMAC-SHA3-512: (A6875) SHA3-512: (A6875)
CPT-KAS-ECC-SSC-Sp800-56Ar3	KAS-SSC	ECC based Key agreement Shared Secret Computation	Publication:SP 800-56A Rev. 3	KAS-ECC-SSC Sp800-56Ar3: (A6875) Curves: P-224, P-256, P-384, P-521 bits
CPT-KDF-KMAC	KBKDF	Wrap, Unwrap and Key Derivation	Publication:SP 800-185	KDF KMAC Sp800-108r1: (A6875) Size: 128, 256 bits KMAC-128: (A6875) KMAC-256: (A6875) cSHAKE-128: (A6875) cSHAKE-256: (A6875) CKG4: () Key Type: Symmetric
CPT-KDF-SP800-108	KBKDF	KBKDF	Publication:SP 800-108 Rev. 1	KDF SP800-108: (A6875) HMAC-SHA-1: (A6875) HMAC-SHA2-224: (A6875) HMAC-SHA2-256: (A6875) HMAC-SHA2-384: (A6875) HMAC-SHA2-512: (A6875) AES-CMAC: (A6875) Key Sizes: 128, 192 and 256 bits CKG4: () Key Type: Symmetric
CPT-KDF-TLS	KAS-135KDF	TLS KDF	Publication:SP 800-135 Rev. 1	TLS v1.2 KDF RFC7627:

Name	Type	Description	Properties	Algorithms
				(A6875) SHA2-256: (A6875) SHA2-384: (A6875)
CPT-RSA-Decryption-Primitive	KTS-Encap	RSA Decryption primitive	Publication:FIPS 186-4	RSA Decryption Primitive Sp800-56Br2: (A6875) Modulo: 2048, 3072, and 4096-bits
CPT-RSA-Signature-Primitive	DigSig-SigGen	RSA Signature Primitive	Publication:FIPS 186-4	RSA Signature Primitive: (A6875)
CPT-SHA-1	SHA	Digest	Publication:FIPS 180-4	SHA-1: (A6875)
CPT-SHA2-224	SHA	Digest	Publication:FIPS 180-4	SHA2-224: (A6875)
CPT-SHA2-256	SHA	Digest	Publication:FIPS 180-4	SHA2-256: (A6875)
CPT-SHA2-384	SHA	Digest	Publication:FIPS 180-4	SHA2-384: (A6875)
CPT-SHA2-512	SHA	Digest	Publication:FIPS 180-4	SHA2-512: (A6875)
CPT-SHA3-224	SHA	Digest	Publication:FIPS 202	SHA3-224: (A6875)
CPT-SHA3-384	SHA	Digest	Publication:FIPS 202	SHA3-384: (A6875)
CPT-SHA3-512	SHA	Digest	Publication:FIPS 202	SHA3-512: (A6875)
CPT-SHAKE-128	XOF	Digest	Publication:FIPS 202	SHAKE-128: (A6875)
CPT-SHAKE-256	XOF	Digest	Publication:FIPS 202	SHAKE-256: (A6875)
CPT-TDES-CBC	BC-UnAuth	UN-Auth Decryption	Publication:SP 800-67 Rev. 2	TDES-CBC: (A6875)
ENT_(P)_(SP 800-90B)	ENT-ESV	Physical Entropy		
FW-ECDSA-KeyGen (FIPS186-4)	AsymKeyPair-KeyGen	ECC Key Pair generation	Publication:FIPS186-4	ECDSA KeyGen (FIPS186-5): (A6876) Curves: P-224, P-256, P-384 and P-521 CKG1: () Key Type: Symmetric and Asymmetric key generation

Name	Type	Description	Properties	Algorithms
FW-KTS-IFC	KTS-Encap	Key encapsulation and decapsulation	Publication:SP 800-56B Rev. 2	KTS-IFC: (A6876) Modulo: 2048, 3072, 4096 SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
FW-KTS-IFC (KTS)	KTS-Encap	Asymmetric key encapsulation and un-encapsulation	Caveat:2048, 3072, or 4096-bit modulus providing 112, 128, or 150 bits of encryption strength Publication:SP 800-56B Rev. 2	KTS-IFC: (A6876) Modulo: 2048, 3072, 4096 bits SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
KAS-ANS-9.63 (Sp800-56Ar3)	KAS-Full	ECDH key derivation and ECDH-AES key wrap	Caveat:SSP establishment methodology provides between 112 and 256 bits of encryption strength Publication:SP 800-56A Rev. 3, SP 800-135 Rev. 1	KAS-ECC-SSC Sp800-56Ar3: (A1948) Curves: P-224, P-256, P-384, P-521 KDF ANS 9.63: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
KAS-IFC-OneStep (SP800-56Br2)	KAS-Full	PEK and KLK generation and certificate authentication	Caveat:2048-bit, 3072-bit and 4096-bit modulus providing between 112 and 150 bits of encryption strength Publication:SP 800-56B Rev. 2	KAS-IFC-SSC: (A1948) Modulo: 2048, 3072, 4096 KDA OneStep Sp800-56Cr1: (A1948) SHA2-512: (A1948) CKG3: () Key Type: Symmetric

Name	Type	Description	Properties	Algorithms
KAS-KDA-HKDF (SP800-56Ar3)	KAS-Full	ECDH key derivation and ECDH-AES key wrap	Caveat:SSP establishment methodology provides between 112 and 256 bits of encryption strength Publication:SP 800-56A Rev. 3, SP 800-56C Rev. 2	KAS-ECC-SSC Sp800-56Ar3: (A1948) Curves: P-224, P-256, P-384, P-521 KDA HKDF Sp800-56Cr1: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
KAS-KDA-ONESTEP (SP800-56Ar3)	KAS-Full	KEK and Cloning	Caveat:SSP establishment methodology provides between 112 and 256 bits of encryption strength Publication:SP 800-56A Rev. 3, SP 800-56C Rev. 2	KAS-ECC-SSC Sp800-56Ar3: (A1948) Curves: P-521 KDA OneStep Sp800-56Cr1: (A1948) SHA2-512: (A1948) CKG3: () Key Type: Symmetric
KAS-KDA-TWOSTEP (SP800-56Ar3)	KAS-Full	ECDH key derivation	Caveat:SSP establishment methodology provides between 112 and 256 bits of encryption strength Publication:SP 800-56A Rev. 3, SP 800-56C Rev. 2	KAS-ECC-SSC Sp800-56Ar3: (A1948) Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 KDA TwoStep Sp800-56Cr1: (A1948) HMAC-SHA-1: (A1948) HMAC-SHA2-224: (A1948) HMAC-SHA2-256: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948)

Name	Type	Description	Properties	Algorithms
				AES-CMAC: (A1948) CKG3: () Key Type: Symmetric
KAS-TLS (Sp800-56Ar3)	KAS-SSC KAS-135KDF	TLS	Caveat:SSP establishment methodology provides between 112 and 256 bits of encryption strength Publication:SP 800-56A Rev. 3, SP 800-135 Rev. 1	KAS-ECC-SSC Sp800-56Ar3: (A6875) Curves: P-224, P-256, P-384, P-521 TLS v1.2 KDF RFC7627: (A6875) SHA2-256: (A6875) SHA2-384: (A6875) HMAC-SHA2-256: (A6875) HMAC-SHA2-384: (A6875)
LEGACY-CPT-TDES-ECB	BC-UnAuth	UN-Auth Decryption	Publication:SP 800-67 Rev. 2	TDES-ECB: (A6875)
LEGACY-SW-AES-CBC-UNWRAP	KTS-Unwrap	Legacy Key Unwrap	Caveat:Caveat: 128, 192, and 256- bit keys providing 128, 192, or 256 bits of encryption strength Legacy Tag:Legacy Use Only Publication:SP 800-38F	AES-CBC: (A1948) Sizes: 128, 192, 256 bits Direction: Decryption
LEGACY-SW-AES-ECB-UNWRAP	KTS-Unwrap	Legacy Key Unwrap	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength Legacy Tag:Legacy Use Only Publication:SP 800-38F	AES-ECB: (A1948) Sizes: 128, 192, 256 bits Direction: Decryption

Name	Type	Description	Properties	Algorithms
LEGACY-SW-TDES-KW	BC-Auth	Auth key Unwrap	Publication:SP 800-38F	TDES-KW: (A1948) TDES-CBC: (A1948)
LEGACY-SW-TDES-KW (KTS)	BC-AuthDecrypt	Used in GP_KEY_MGMT service to unwrap the key. service to unwrap the key.	Caveat:192-bit key providing 112-bit encryption strength Legacy Tag:Legacy Use Only Publication:SP 800-38F	TDES-KW: (A1948) Key Sizes: 192 bit
OQS-ML-DSA-KeyGen	AsymKeyPair-KeyGen	ML-DSA key Generation	Publication:FIPS 204	ML-DSA KeyGen: (A6877) Parameters: ML-DSA-44, ML-DSA-65, ML-DSA-87 SHAKE-128: (A6877) SHAKE-256: (A6877) CKG2: ()
OQS-ML-DSA-SigGen	DigSig-SigGen	ML-DSA Signature generation	Publication:FIPS 204	ML-DSA SigGen: (A6877) Parameters: ML-DSA-44, ML-DSA-65, ML-DSA-87 Interfaces: Internal/External Randomness: Deterministic/Hedged Mu Computation: Internal/External SHAKE-128: (A6877) SHAKE-256: (A6877)
OQS-ML-DSA-SigVer	DigSig-SigVer	ML-DSA Signature verification	Publication:FIPS 204	ML-DSA SigVer: (A6877) Parameters: ML-DSA-44, ML-DSA-65, ML-

Name	Type	Description	Properties	Algorithms
				DSA-87 Interfaces: Internal/External Randomness: Deterministic/Hedged Mu Computation: Internal/External SHAKE-128: (A6877) SHAKE-256: (A6877)
OQS-ML-KEM-EncapDecap	KEM-Decap KEM-Encap KEM-Full	ML-KEM Key encapsulation and decapsulation	IG:IG D.S Scenario 1 Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	ML-KEM EncapDecap: (A6877) Parameters: ML-KEM-1024, ML-KEM-512, ML-KEM-768 SHAKE-128: (A6877) SHAKE-256: (A6877) SHA3-256: (A6875) SHA3-512: (A6875)
OQS-ML-KEM-KeyGen	AsymKeyPair-KeyGen KEM-Full	ML-KEM Key Generation	IG:IG D.S Scenario 1 Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	ML-KEM KeyGen: (A6877) Parameters: ML-KEM-1024, ML-KEM-512, ML-KEM-768 SHAKE-128: (A6877) SHAKE-256: (A6877) SHA3-256: (A6875) SHA3-512: (A6875) CKG2: ()
OQS-SHAKE-256	XOF	Digest	Publication:FIPS 202	SHAKE-256: (A6877)
SW-AES-CBC	BC-UnAuth	Un-Auth Encryption	Publication:SP800-38A	AES-CBC: (A1948)

Name	Type	Description	Properties	Algorithms
		and Decryption		
SW-AES-CMAC	MAC	MAC Sign and Verify	Publication:SP800-38B	AES-CMAC: (A1948) AES-CBC: (A1948)
SW-AES-ECB	BC-UnAuth	Un-Auth Encryption and Decryption	Publication:SP800-38A	AES-ECB: (A1948)
SW-AES-GCM	BC-Auth	Authenticated Encryption and Decryption	Publication:SP800-38D	AES-GCM: (A1948) AES-ECB: (A1948)
SW-AES-GCM-Unwrap (KTS)	KTS-Unwrap	Key-Unwrap	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength Publication:SP800-38D	AES-GCM: (A1948) Key Sizes: 128, 192, 256 bits AES-CBC: (A1948)
SW-AES-GCM-Wrap (KTS)	KTS-Wrap	Key-wrap	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength Publication:SP800-38D	AES-GCM: (A1948) Key Sizes: 128, 192, 256 bits AES-CBC: (A1948)
SW-AES-KW-Unwrap (KTS)	KTS-Unwrap	Key Unwrapping	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength Publication:SP800-38F	AES-KW: (A1948) Key Sizes: 128, 192, 256 bits AES-CBC: (A1948)
SW-AES-KW-Wrap (KTS)	KTS-Wrap	Key wrapping	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	AES-KW: (A1948) Key Sizes: 128, 192, 256 bits AES-CBC: (A1948)

Name	Type	Description	Properties	Algorithms
			Publication:SP 800-38F	
SW-AES-KWP-Unwrap (KTS)	KTS-Unwrap	Key Unwrapping	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength Publication:SP 800-38F	AES-KWP: (A1948) Key Sizes: 128, 192, 256 bits AES-CBC: (A1948)
SW-AES-KWP-Wrap (KTS)	KTS-Wrap	Key wrapping	Caveat:128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength Publication:SP 800-38F	AES-KWP: (A1948) Key Sizes: 128, 192, 256 bits AES-CBC: (A1948)
SW-Counter-DRBG	DRBG	Counter DRBG	Publication:SP800-90Arev1	Counter DRBG: (A1948) CKG1: () Key Type: Symmetric and Asymmetric key generation AES-CTR: (A1948)
SW-ECDSA-KeyGen (FIPS186-4)	AsymKeyPair-KeyGen	ECC Key Pair generation	Publication:FIPS186-4	ECDSA KeyGen (FIPS186-4): (A1948) Curves: P-224, P-256, P-384 and P-521 CKG1: () Key Type: Symmetric and Asymmetric key generation
SW-ECDSA-KeyVer (FIPS186-4)	AsymKeyPair-KeyVer	ECC Key Verification	Publication:FIPS186-4	ECDSA KeyVer (FIPS186-4): (A1948) Curves: P-224, P-256, P-384, P-521 bits
SW-ECDSA-SigGen (FIPS186-4)	DigSig-SigGen	ECC Signature Generation	Publication:FIPS186-4	ECDSA SigGen (FIPS186-4): (A1948)

Name	Type	Description	Properties	Algorithms
				Curves: P-224, P-256, P-384 and P-521 SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948) SHA2-224: (A1948)
SW-ECDSA-SigVer (FIPS186-4)	DigSig-SigVer	ECC Signature Verification	Publication:FIPS186-4	ECDSA SigVer (FIPS186-4): (A1948) Curves: P-224, P-256, P-384 and P-521 SHA2-224: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948)
SW-EDDSA-KeyVer (FIPS186-5)	AsymKeyPair-KeyVer	EDDSA key Verification	Publication:FIPS186-5	EDDSA KeyVer: (A1948) Curves: ED-25519 and ED-448
SW-EDDSA-SigGen (FIPS186-5)	DigSig-SigGen	EDDSA Signature Generation	Publication:FIPS186-5	EDDSA SigGen: (A1948) Curves: ED-25519 and ED-448 SHA2-512: (A1948) SHAKE-256: (A1948)
SW-EDDSA-SigVer (FIPS186-5)	DigSig-SigVer	EDDSA Signature Verification	Publication:FIPS186-5	EDDSA SigVer: (A1948) Curves: ED-25519 and ED-448 SHA2-512: (A1948) SHAKE-256: (A1948)

Name	Type	Description	Properties	Algorithms
SW-HMAC-SHA-1	MAC	HMAC-SHA-1	Publication:FIPS 198-1	HMAC-SHA-1: (A1948) MAC Length: 160 bits Key Length: 112 bits - 800 bits SHA-1: (A1948)
SW-HMAC-SHA2-224	MAC	HMAC-SHA2-224	Publication:FIPS 198-1	HMAC-SHA2-224: (A1948) SHA2-256: (A1948)
SW-HMAC-SHA2-256	MAC	HMAC-SHA2-256	Publication:FIPS 198-1	HMAC-SHA2-256: (A1948) SHA2-256: (A1948)
SW-HMAC-SHA2-384	MAC	HMAC-SHA2-384	Publication:FIPS 198-1	HMAC-SHA2-384: (A1948) SHA2-384: (A1948)
SW-HMAC-SHA2-512	MAC	HMAC-SHA2-512	Publication:FIPS 198-1	HMAC-SHA2-512: (A1948) SHA2-512: (A1948)
SW-HMAC-SHA3-224	MAC	HMAC-SHA3-224	Publication:FIPS 198-1	HMAC-SHA3-224: (A1948) SHA3-224: (A1948)
SW-HMAC-SHA3-256	MAC	HMAC-SHA3-256	Publication:FIPS 198-1	HMAC-SHA3-256: (A1948) SHA3-256: (A1948)
SW-HMAC-SHA3-384	MAC	HMAC-SHA3-384	Publication:FIPS 198-1	HMAC-SHA3-384: (A1948) SHA3-384: (A1948)
SW-HMAC-SHA3-512	MAC	HMAC-SHA3-512	Publication:FIPS 198-1	HMAC-SHA3-512: (A1948) SHA3-512: (A1948)
SW-KAS-ECC-Sp800-56Ar3	KAS-Full	ECC based Key agreement	Publication:SP 800-56A Rev. 3	KAS-ECC Sp800-56Ar3: (A1948) Curves: P-521 bits KDA OneStep Sp800-56Cr1: (A1948) SHA2-256: (A1948)

Name	Type	Description	Properties	Algorithms
SW-KAS-ECC-SSC-Sp800-56Ar3	KAS-SSC	LS2-SW-Crypto	Publication:SP 800-56A Rev. 3	KAS-ECC Sp800-56Ar3: (A1948) Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571,P-224,P-256, P-384 and P-512
SW-KAS-IFC-SSC	KAS-SSC	KAS IFC Shared Secret Computation	Publication:SP 800-56A Rev. 3	KAS-IFC-SSC: (A1948) Modulo: 2048, 3072 and 4096 bits
SW-KDA-HKDF-Sp800-56Cr1	KAS-56CKDF	HKDF based Key Derivation	Publication:SP 800-56C Rev. 2	KDA HKDF Sp800-56Cr1: (A1948) HMAC-SHA2-256: (A1948) HMAC-SHA2-224: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948)
SW-KDA-OneStep-Sp800-56Cr1	KAS-56CKDF	One Step Key Derivation	Publication:SP 800-56C Rev. 2	KDA OneStep Sp800-56Cr1: (A1948) SHA2-512: (A1948) CKG3: () Key Type: Symmetric
SW-KDF-ANS-9.63	KAS-135KDF	ANS-9.63 Key Derivation	Publication:SP 800-135 Rev. 1	KDF ANS 9.63: (A1948) SHA2-256: (A1948) SHA2-384: (A1948) SHA2-512: (A1948) CKG3: () Key Type: Symmetric
SW-KDF-SP800-108	KBKDF	KBKDF	Publication:SP 800-108 Rev. 1	KDF SP800-108: (A1948) HMAC-SHA-1: (A1948)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-224: (A1948) HMAC-SHA2-256: (A1948) HMAC-SHA2-384: (A1948) HMAC-SHA2-512: (A1948) AES-CMAC: (A1948) Key Sizes: 128, 192 and 256 bits CKG3: () Key Type: Symmetric
SW-KTS-IFC	KTS-Encap	Key encapsulation and decapsulation	Publication:SP 800-56B Rev. 2	KTS-IFC: (A1948) Modulo: 2048, 3072, 4096 SHA3-512: (A1948)
SW-KTS-IFC (KTS)	KTS-Encap KTS-Decap	Asymmetric key encapsulation and un-encapsulation	Caveat:2048, 3072, or 4096-bit modulus providing 112, 128, or 150 bits of encryption strength Publication:SP 800-56B Rev. 2	KTS-IFC: (A1948) Modulus: 2048, 3072, 4096 bits SHA3-512: (A1948)
SW-PBKDF	PBKDF	Password based Key derivation	Publication:SP 800-132	PBKDF: (A1948) HMAC-SHA2-256: (A1948) SHA2-256: (A1948)
SW-RSA-Decryption-Primitive	KTS-Encap	RSA Decryption primitive	Publication:FIPS 186-4	RSA Decryption Primitive: (A1948) Modulo: 2048 bits
SW-RSA-KeyGen (FIPS186-5)	AsymKeyPair-KeyGen	RSA Key Generation	Publication:FIPS 186-4	RSA KeyGen (FIPS186-5): (A1948) CKG1: () Key Type: Symmetric and Asymmetric key generation

Name	Type	Description	Properties	Algorithms
SW-RSA-SigGen (FIPS186-5)	DigSig-SigGen	RSA Signature Generation	Publication:FIPS 186-4	RSA SigGen (FIPS186-5): (A1948) SHA2-256: (A1948) SHA3-512: (A1948)
SW-RSA-Signature-Primitive	DigSig-SigGen	RSA Signature Primitive	Publication:FIPS 186-4	RSA Signature Primitive: (A1948)
SW-RSA-SigVer (FIPS186-5)	DigSig-SigVer	RSA Signature verification	Publication:FIPS 186-4	RSA SigVer (FIPS186-5): (A1948) SHA2-256: (A1948) SHA3-512: (A1948)
SW-SHA-1	SHA	Digest	Publication:FIPS 180-4	SHA-1: (A1948)
SW-SHA-1 (IG 2.4.A)	SHA	SHA-1, no security claimed per IG 2.4.A	Usage:Fingerprints Publication:FIPS 180-4	SHA-1: (A1948)
SW-SHA2-256	SHA	Digest	Publication:FIPS 180-4	SHA2-256: (A1948)
SW-SHA2-384	SHA	Digest	Publication:FIPS 180-4	SHA2-384: (A1948)
SW-SHA2-512	SHA	Digest	Publication:FIPS 180-4	SHA2-512: (A1948)
SW-SHA3-512	SHA	Digest	Publication:FIPS 202	SHA3-512: (A1948)
SW-SHAKE-128	XOF	Digest	Publication:FIPS 202	SHAKE-128: (A1948)
SW-SHAKE-256	XOF	Digest	Publication:FIPS 202	SHAKE-256: (A1948)
UB-Bootloader_Signature_Verification	DigSig-SigVer	Bootloader Signature Verification	Publication:FIPS186-5	ECDSA SigVer (FIPS186-5): (A6878) RSA SigVer (FIPS186-5): (A6878) SHA2-256: (A6878) SHA2-512: (A6878)

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 (#A6875)
  - IG C.H Scenario #1:
    - TLS 1.2 or other applications can offload GCM operations.
    - For TLS-1.2 protocol, IV constructed as described in RFC 5288.
    - For TLS 1.2 AES GCM 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 # A6875): 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 # A6875): SP 800-90Ar1 DRBG, HASH_DRBG SHA2-512.
    - .
- PBKDF (SP 800-132) (#A1948) IG D.N
  - PBKDF with HMAC password strength
    - The module implements PBKDF using HMAC as a suitable one-way key derivation function for storing and verifying memorized secrets as salted hashes per SP 800-63B. The output of the PBKDF is used only for this purpose and is not used as a Master Key (MK) or Data Protection Key (DPK), nor is it used to derive or protect a DPK for a storage application.
    - 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 are 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 (This curve may only be used in blockchain-related applications)
- ML-DSA
    - The module supports ML-DSA signature generation and verification using both the internal and external μ (Mu) interfaces. Per FIPS 204 for ML-DSA, the external Mu shall be provided by another cryptographic module.
    - KeyGen (#A6877), SigGen(#A6877), SigVer(#A6877)

- ML-KEM
    - KeyGen (#A6877), Encap/Decap (#A6877)
        - IG D.S Scenario #1:
            - ML-KEM implementation is compliant with FIPS 203 and SP 800-227.
            - ML-KEM implementation includes encapsulation and decapsulation key checks specified in Sections 7.2 and 7.3 of FIPS 203.
            - Key establishment methodology provides between 128 and 256 bits of security strength
- Legacy Algorithms
    - IG C.M
        - LEGACY AES-CBC (IG D.G) (#A6875): Keys Unwrapping for keys encrypted before 1st January 2018
        - LEGACY AES-ECB (IG D.G) (#A6875): Keys Unwrapping for keys encrypted before 1st January 2018
        - LEGACY TDES-CBC (SP 800- 38A) (#A6875): Data decryption for data encrypted before 1st January 2024
        - LEGACY TDES-ECB (SP 800- 38A) (#A6875): Data decryption for data encrypted before 2024
        - LEGACY TDES-ECB (#A1948): Prerequisite for TDES-KW for data encrypted before 1st January 2024
        - LEGACY TDES-KW (SP 800- 38F) (#A1948): Key unwrapping for key wrapped before 1st January 2024

2.8 RBG and Entropy

Cert Number	Vendor Name
E231	Marvel

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	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 generated random bits 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 Scheme (IG D.F)
  Module support following Scenario 1 key agreement schemes.
  - KAS-IFC-SSC (SP 800-56Br2) (#A1948)
  - KAS-IFC OneStep (SP800-56Br2) (#A1948) Scenario 1 path (2)

  Module support following Scenario 2 key agreement schemes as per IG D.F.
  - KAS-ECC-SSC (SP800-56Ar3) (#A6875)
  - KAS-ECC (KAS) (SP 800-56Ar3) (#A1948) Scenario 2 path (2)
  - KAS-ECC (SP800- 56Ar3) (#A1948)
  - KAS TLS (SP 800- 56Ar3) (#A6875) (#A1948) 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 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) (#A6876)

  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)

- Key Encapsulation Mechanism (IG D.S)
  Module supports ML-KEM following Scenario 1 of IG D.S. The module establishes SSPs via ML-KEM implementing one side of the ML-KEM scheme compliant with FIPS 203.
    - ML-KEM KeyGen (FIPS 203) (#A6877)
    - ML-KEM Encapsulation (FIPS 203) (#A6877)
    - ML-KEM Decapsulation (FIPS 203) (#A6877)

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 protocol, 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 Power	Primary interface to communicate with the module. Provides APIs for the software on the host to communicate with the module
PCIe SMBus	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

Physical Port	Logical Interface(s)	Data That Passes
Zeroize push button	Control Input	No data; only a signal
Power connector	Power	No data; external power connector
Battery interfaces	Power	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 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). A maximum of 20 password attempts are possible before a user is permanently locked. Lockout of MCO automatically zeroizes the module. In all other cases, lockout can be unset by destroying the partition.	SW-AES-KWP (Wrapping/Unwrapping)	1/(62^8)	20/(62^8)
Digital signature	Authentication is performed using SHA-256 based RSA 2048-bit PKCS#1-v1.5 signatures (provides 112 bits of strength).	SW-RSA-SigVer (FIPS186-5)	1/(2^112)	30/(2^112)

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	Corresponding public keys are associated with the identity. For each failed signature verification, the module will block for 2seconds.			

Table 13: Authentication Methods

The module supports the above identity-based authentication methods.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
MCO	Identity	CO	Username and password
MCO (2FA)	MultiFactorIdentity	CO	Username and password Digital signature
Pre-CO	Identity	CO	Username and password
PCO	Identity	CO	Username and password
PCO (2FA)	MultiFactorIdentity	CO	Username and password Digital signature
PCU	Identity	User	Username and password
PCU (2FA)	MultiFactorIdentity	User	Username and password Digital signature
AU	Identity	User	Username and password

Table 14: Roles

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
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	AU - Partition Authentication Key Private RSA (PXPAKYPRV RSA): E MCO PCO - Partition Authentication

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key Private RSA (PXPAKYPRV RSA): E
GP_BACKUP_RESTORE	Provides Backup/ Restore services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KDF-SP800-108 SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) CPT-Hash-DRBG CPT-HMAC-SHA2-256 SW-AES-CBC SW-SHA2-256 SW-Counter-DRBG	MCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Owner Key Backup Key (HOKBKY): E - HSM Owner Recovery Key (HOREKY): E - Partition Authentication Certificate (PXPACT): R - Partition Authentication Key Private RSA (PXPAKYPRV RSA): R - Partition Backup Ephemeral Key (PXKBEK): G,E - Partition Data Encryption Key (PXDEKY): E - Partition DRBG Hash C Entropy State

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Masking Key (PXMSKY): R - Partition Owner KBK Key (POKBKY): E - Partition Password Encryption Key (PXPEKY): R - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): R - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): R - Partition User General Purpose HMAC Key (PUGPMKY): R - Partition User General Purpose Key Public (PUGPKYPUB): R - Partition User General Purpose Symmetric Key (PUGPSKY): R - Partition User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): R PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Owner Key Backup Key (HOKBKY): E - HSM Owner Recovery Key (HOREKY): E - Partition Backup Ephemeral Key (PXKBEK): G,E - Partition Data Encryption Key (PXDEKY): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Owner KBK Key (POKBKY): E - Partition Password Encryption Key (PXPEKY): R - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): R - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): R - Partition User General Purpose HMAC Key (PUGPMKY): R - Partition User General Purpose Key Public (PUGPKYPUB): R - Partition User General Purpose Symmetric Key (PUGPSKY): R - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): R Unauthenticated - FIPS Octeon HSM DRBG Entropy Source

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(FOHXDRBGENSR): E - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Owner Key Backup Key (HOKBKY): E - HSM Owner Recovery Key (HOREKY): E - Partition Authentication Certificate (PXPACT): W - Partition Authentication Key Private RSA (PXPAKYPRVRSA): W - Partition Backup Ephemeral Key (PXKBEK): E,W - Partition Data Encryption Key (PXDEKY): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Masking Key (PXMSKY): W - Partition Owner KBK Key (POKBKY): E - Partition Password Encryption Key (PXPEKY): W - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): W - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): W - Partition User General Purpose HMAC Key (PUGPMKY): W - Partition User General Purpose Symmetric Key (PUGPSKY): W - Partition User Login Password Data (PULPDA): W - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): W
GP_CERT_AUTH	Provides cert auth services	Success with	Opcode	Opcode	CPT-Hash-DRBG SW-KAS-IFC-SSC SW-KDF-SP800-	AU - FIPS Octeon HSM DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		fips_state = 2 or 3	Inputs	Outputs	108 SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-ECDSA-SigVer (FIPS186-4)	Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E,R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): E,R - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Certificate (PXPACT): E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Ephemeral Key (PXCAEK): G - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Cert Auth Target Shared Secret (PXCATSZ): Z,E,W - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Owner Authentication Certificate (POOAUCT): E,R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): R - Partition Owner Trust Anchor

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate (POOTACT): E,R MCO - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): W,R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): W,E,R - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E,R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): E,R - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - HSM Vendor Authentication Root Certificate RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(HVARCTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Ephemeral Key (PXCAEK): G - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Cert Auth Target Shared Secret (PXCATSZ): Z,E,W - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Owner Authentication Certificate (POOAUCT): W,E,R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): Z,W,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Owner Trust Anchor Certificate (POOTACT): W,E,R PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E,R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): E,R - HSM Vendor Authentication Root Certificate ECC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(HVARCTEC): R - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - Partition Authentication Key Private RSA (PXPAKYPRV RSA): E - Partition Cert Auth Ephemeral Key (PXCAEK): G - Partition Cert Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Cert Auth Target Shared Secret (PXCATSZ): Z,E,W - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Owner Authentication Certificate (POOAUCT): E,R - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Owner Client Authentication Trust Anchor Certificate (POCAUTACT) : R - Partition Owner Trust Anchor Certificate (POOTACT): E,R Pre-CO - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): R - HSM Vendor Authentication Root Certificate ECC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(HVARCTEC): R - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): R - Partition Authentication Certificate (PXPACT): R - Partition Owner Authentication Certificate (POOAUCT): W,R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): W,R - Partition Owner Trust Anchor Certificate (POOTACT): W,R Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC): R - FIPS Partition HSM Manufacturer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Master Authentication Certificate RSA (FPHMMACTRSA): E,R - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): W,E,R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): R - HSM Owner Trust Anchor Certificate (HOOTACT): W,E,R - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): R - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): E,R - Partition Authentication Certificate (PXPACT): E,R - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Cert Auth Ephemeral Key (PXCAEK): G - Partition Cert

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Auth Source Shared Secret (PXCASSZ): Z,G,E,R - Partition Cert Auth Target Shared Secret (PXCATSZ): Z,E,W - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Owner Authentication Certificate (POOAUCT): E,R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): R - Partition Owner Trust Anchor Certificate (POOTACT): E,R
GP_CLONING	Provides cloning services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	KAS-KDA-ONESTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-SHA-1 (IG 2.4.A)	AU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CPT-AES-CBC 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-PBKDF SW-RSA-KeyGen (FIPS186-5) SW-SHA2-256	- Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Key Loading Key (PXKLKY): W - Partition Masking Key (PXMSKY): E - Partition Master Encryption Key (PXMEKY): E - Partition Password Encryption Key (PXPEKY): W - 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 HMAC Key (PUGPMKY): W,R - Partition User General Purpose HMAC Session Key (PUGPMSK): W,R - Partition User General

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Purpose Key Public (PUGPKYPUB): W,R - Partition User General Purpose Session Key Public (PUGPSKYPUB): W,R - Partition User General Purpose Symmetric Key (PUGPSKY): W,R - Partition User General Purpose Symmetric Session Key (PUGPSSK): W,R PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition Cloning Encryption Ephemeral Key (PXCLEEK): G,E,Z - Partition Cloning Ephemeral Key Private (PXCLEKPRV): Z,G,E - Partition Cloning Ephemeral Key Public (PXCLEKPUB): Z,G,R - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Cloning MAC Ephemeral Key (PXCLMEK): Z,G,E - Partition Cloning Shared Secret (PXCLSZ): Z,G,E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Key Loading Key (PXKLKY): W,R - Partition Masking Key (PXMSKY): W,E,R,G - Partition Master Encryption Key (PXMEKY): E - Partition Password Encryption Key (PXPEKY): W,R - Partition User Cloning Ephemeral Key Public (PUCLEKPUB): Z,E,W PCU - Partition Masking Key (PXMSKY): E - Partition Master Encryption Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PXMEKY): E - 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 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 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
GP_CRYPTO_FASTPATH	Provides crypto/fastpath services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	ENT_(P)_(SP 800-90B) CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST CPT-AES-CBC CPT-AES-CCM SW-AES-CMAC CPT-AES-CTR CPT-AES-ECB CPT-AES-GCM CPT-AES-GMAC CPT-ECDSA-SigGen (FIPS186-4) SW-EDDSA-SigGen (FIPS186-5) SW-EDDSA-SigVer (FIPS186-5) CPT-EDDSA-SigGen (FIPS186-5) CPT-EDDSA-SigVer (FIPS186-5) CPT-EDDSA-KeyVer (FIPS186-5) CPT-Hash-DRBG CPT-HMAC-SHA-1 CPT-HMAC-SHA2-224 CPT-HMAC-SHA2-256 CPT-HMAC-SHA2-384 CPT-HMAC-SHA2-512 CPT-HMAC-SHA3-224 CPT-HMAC-SHA3-256 CPT-HMAC-SHA3-384 CPT-HMAC-SHA3-512	PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): E PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition TLS E2E Symmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					FW-KTS-IFC CPT-RSA-Decryption-Primitive CPT-RSA-Signature-Primitive CPT-SHA-1 CPT-SHA2-224 CPT-SHA2-256 CPT-SHA2-384 CPT-SHA2-512 CPT-SHA3-224 CPT-SHA3-384 CPT-SHA3-512 CPT-SHAKE-128 OQS-SHAKE-256 CPT-SHAKE-256 CPT-TDES-CBC LEGACY-CPT-TDES-ECB OQS-ML-DSA-SigGen OQS-ML-DSA-SigVer	Key (PXTLSE2EKY): E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): E - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): E - Partition User General Purpose HMAC Key (PUGPMKY): E - Partition User General Purpose HMAC Session Key (PUGPMSK): E - Partition User General Purpose Key Public (PUGPKYPUB): E - Partition User General Purpose Session Key Public (PUGPSKYPUB): E - Partition User General Purpose Symmetric Key (PUGPSKY): E - Partition User General

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Purpose Symmetric Session Key (PUGPSSK): E Pre-CO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): E Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition TLS E2E Symmetric Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PXTLSE2EKY): E
GP_E2E	Provides e2e services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	KAS-TLS (Sp800-56Ar3) SW-AES-GCM SW-ECDSA-KeyVer (FIPS186-4) CPT-Hash-DRBG CPT-KAS-ECC-SSC-Sp800-56Ar3 CPT-RSA-Signature-Primitive SW-RSA-SigVer (FIPS186-5) SW-SHA2-512 SW-ECDSA-SigVer (FIPS186-4)	Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Owner Authentication Certificate (POOAUCT): R - Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT): E - Partition TLS E2E Client Authentication Certificate (PXTLSE2ECACT): E,W - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC): G - Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EKPUBECC): G,R - Partition TLS E2E Master Secret Key (PXTLSE2EMSKY): G,E - Partition TLS E2E Pre Master Secret (PXTLSE2EPMS): Z,G,E - Partition TLS E2E Symmetric Key (PXTLSE2EKY): G - Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC): W,E,Z
GP_HPS_MGMT	Provides HPS mgmt services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-ECDSA-KeyGen (FIPS186-4) SW-ECDSA-SigGen (FIPS186-4) SW-RSA-SigVer (FIPS186-5) SW-ECDSA-SigVer (FIPS186-4)	MCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Master Encryption Key (HXMEKY): E - HSM Vendor

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Root Certificate ECC (HVARCTEC): R - HSM Vendor Firmware Update Validation Key Public ECC (HVFUVKYPUBECC): E - HSM Vendor Firmware Update Validation Key Public RSA (HVFUVKYPUBRSA): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E
GP_INFO_DIAGNOSTIC	Provides show status, self-test, show version, info and diagnostic services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) LEGACY-SW-TDES-KW (KTS) CPT-AES-CBC CPT-AES-CCM CPT-AES-CMAC CPT-AES-ECB CPT-AES-GCM SW-AES-GCM SW-Counter-DRBG SW-ECDSA-KeyVer (FIPS186-4) CPT-ECDSA-	AU - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): R - HSM Owner Key Backup Key (HOKBKY): R - ML-KEM Seed: G,E - Partition Owner KBK Key (POKBKY): R MCO - FIPS Partition HSM Vendor

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigGen (FIPS186-4) SW-ECDSA-SigGen (FIPS186-4) CPT-ECDSA-SigVer (FIPS186-4) SW-EDDSA-KeyVer (FIPS186-5) CPT-Hash-DRBG SW-HMAC-SHA-1 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-HMAC-SHA3-224 CPT-HMAC-SHA3-256 SW-HMAC-SHA3-256 SW-HMAC-SHA3-384 SW-HMAC-SHA3-512 SW-KAS-ECC-Sp800-56Ar3 CPT-KAS-ECC-SSC-Sp800-56Ar3 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-	Key Backup Key (FPHVKBKY): R - HSM Owner Key Backup Key (HOKBKY): R - ML-KEM Seed: G,E - Partition Owner KBK Key (POKBKY): R PCO - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): R - HSM Owner Key Backup Key (HOKBKY): R - ML-KEM Seed: G,E - Partition Owner KBK Key (POKBKY): R PCU - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): R - HSM Owner Key Backup Key (HOKBKY): R - ML-KEM Seed: G,E - Partition Owner KBK Key (POKBKY): R Unauthenticate

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					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-SHA2-512 SW-SHA2-512 SW-SHAKE-128 SW-SHAKE-256 CPT-TDES-CBC OQS-ML-DSA-SigGen OQS-ML-DSA-SigVer OQS-ML-KEM-EncapDecap SW-ECDSA-SigVer (FIPS186-4) UB-Bootloader_Signature_Verification	d - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): R - HSM Owner Key Backup Key (HOKBKY): R - ML-KEM Seed: G,E - Partition Owner KBK Key (POKBKY): R
GP_KBK_MGMT	Provides service to manage Key Backup Key (KBK)	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS)	MCO PCO - Partition Cert Auth Ephemeral Key (PXCAEK): E - Partition Key Backup Key (PXKBKY): W,R
GP_KEY_MGMT	Provides services to manage keys	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3)	AU - ML-DSA Seed: G,E - ML-KEM Seed: G,E - Partition User General Purpose Asymmetric Key Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KAS-IFC-OneStep (SP800-56Br2) SW-AES-GCM-Wrap (KTS) SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KTS-IFC (KTS) LEGACY-SW-TDES-KW (KTS) FW-KTS-IFC (KTS) SW-SHA-1 (IG 2.4.A) CPT-KDF-KMAC LEGACY-SW-AES-CBC-UNWRAP LEGACY-SW-AES-ECB-UNWRAP CPT-AES-CBC SW-AES-CBC SW-AES-CMAC SW-AES-ECB SW-AES-GCM SW-Counter-DRBG SW-ECDSA-KeyGen (FIPS186-4) FW-ECDSA-KeyGen (FIPS186-4) SW-ECDSA-KeyVer (FIPS186-4) CPT-EDDSA-KeyGen (FIPS186-5) CPT-Hash-DRBG SW-HMAC-SHA-1 SW-HMAC-SHA2-256 SW-HMAC-SHA2-384 SW-HMAC-SHA2-	(PUGPAKYPRV): 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 User General Purpose Symmetric Key (PUGPSKY): Z,E MCO - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Owner Key Backup Key (HOKBKY): W - HSM Owner Recovery Key (HOREKY): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					512 SW-KDA-HKDF-Sp800-56Cr1 SW-KDA-OneStep-Sp800-56Cr1 SW-KDF-ANS-9.63 SW-KDF-SP800-108 SW-KTS-IFC SW-RSA-KeyGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-SHA-1 SW-SHA2-256 SW-SHA2-384 SW-SHA2-512 LEGACY-SW-TDES-KW OQS-ML-DSA-KeyGen OQS-ML-KEM-KeyGen OQS-ML-KEM-EncapDecap	- HSM Owner Trust Anchor Certificate (HOOTACT): E - ML-DSA Seed: G,E - ML-KEM Seed: G,E PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: G,E - ML-KEM Seed: G,E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Data Encryption Key (PXDEKY): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Key Loading Key (PXKLKY): G - Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV): Z,G,E - Partition Key Loading Key Ephemeral Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public (PXKLKEKPUB): Z,G,E,R - Partition Key Loading Key Shared Secret (PXKLSZ): Z,G,E - Partition Master Encryption Key (PXMEKY): E - Partition Owner KBK Key (POKBKY): W - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z,E - Partition User General Purpose HMAC Key (PUGPMKY): Z,E - Partition User General Purpose Key Public (PUGPKYPUB): Z,R,E,W - Partition User General Purpose Session Key Public (PUGPSKYPUB): R,E,W - Partition User General

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Purpose Symmetric Key (PUGPSKY): Z,E - Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB): Z,E,W PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: G,E - ML-KEM Seed: G,E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Key Loading Key (PXKLKY): E - 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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private (PUGPASKPRV): Z,W,G,E,R - Partition User General Purpose HMAC Key (PUGPMKY): Z,W,G,E,R - Partition User General Purpose HMAC Session Key (PUGPMSK): Z,W,G,E,R - 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 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 Wrap Unwrap Shared Secret (PXWUSZ): Z,E Pre-CO - FIPS Octeon

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						HSM DRBG Entropy Source (FOHXDRBGENSR): E - ML-DSA Seed: G,E - ML-KEM Seed: G,E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - 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 Key Loading Key Shared Secret (PXKLSZ): Z,G,E - Partition Master Encryption Key (PXMEKY): E - Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB): Z,E,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						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-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-SHA2-256	MCO - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - HSM Vendor License Key Public RSA (HVLICKYPUBRSA): E
GP_PARTITION_MGMT	Provides services to manage user and master partitions	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-Counter-DRBG CPT-Hash-DRBG SW-KDA-HKDF-Sp800-56Cr1 SW-RSA-KeyGen (FIPS186-5) SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-SHA2-256 SW-ECDSA-SigVer (FIPS186-4)	AU MCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E - HSM Master Encryption Key (HXMEKY): G,E - HSM Owner Attestation Key Public (HOOATKYPUB): E - HSM Vendor Authentication

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Root Certificate RSA (HVARCTRSA): E - HSM Vendor Firmware Update Validation Key Public RSA (HVFUVKYPUBRSA): E - Partition Authentication Certificate (PXPACT): Z,G - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z,G - Partition Data Encryption Key (PXDEKY): Z,G,R - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(POOAUCT): Z - Partition Owner KBK Key (POKBKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Password Encryption Key (PXPEKY): Z - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public (PUGPKYPUB): 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 Login Password Data (PULPDA): Z PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - HSM Master Encryption Key (HXMEKY): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Master Encryption Key (PXMEKY): G Pre-CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Master Encryption Key (PXMEKY): G
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-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-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-KAS-ECC-Sp800-56Ar3 SW-KDA-HKDF-Sp800-56Cr1 SW-RSA-SigVer (FIPS186-5) SW-SHA2-256 SW-ECDSA-SigVer (FIPS186-4)	MCO - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E - HSM Owner Attestation Key Public (HOOATKYPUB): W - Partition Authentication Certificate (PXPACT): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition User General Purpose

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Asymmetric Key Private (PUGPAKYPRV): E - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): E - Partition User General Purpose HMAC Key (PUGPMKY): E - Partition User General Purpose HMAC Session Key (PUGPMSK): E - Partition User General Purpose Key Public (PUGPKYPUB): E - Partition User General Purpose Symmetric Key (PUGPSKY): E - Partition User General Purpose Symmetric Session Key (PUGPSSK): E PCO - Partition Authentication Certificate (PXPACT): E - Partition Authentication Key Private RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PXPAKYPRV RSA): E - Partition Owner Trust Anchor Certificate (POOTACT): E - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): E - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): E - Partition User General Purpose HMAC Key (PUGPMKY): E - Partition User General Purpose HMAC Session Key (PUGPMSK): E - Partition User General Purpose Key Public (PUGPKYPUB): E - Partition User General Purpose Symmetric Key (PUGPSKY): E - Partition User General Purpose Symmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Key (PUGPSSK): E
GP_PARTITION_TIME_MGMT	Provides services to manage user time	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	None	MCO Unauthenticated
GP_POLICY_MGMT	Provides services to HSM/Partition policies	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs		AU MCO PCO PCU Pre-CO Unauthenticated
GP_QUORUM_CONTROL	Provides quorum control (MofN) services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	CPT-Hash-DRBG SW-RSA-SigVer (FIPS186-5)	AU PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition DRBG CTR Key Entropy State (PXDRBGCTKST): E - Partition DRBG CTR V Entropy State (PXDRBGCTVST): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG CTR Key Entropy State (PXDRBGCTKST): E - Partition DRBG CTR V Entropy State (PXDRBGCTVST): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E Pre-CO Unauthenticated
GP_SESSION_MGMT	Provides services to manage sessions and tokens	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) CPT-Hash-DRBG SW-PBKDF SW-RSA-SigVer (FIPS186-5)	AU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E MCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition Backup Ephemeral Key (PXKBEK): Z - Partition DRBG Hash C Entropy State

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E PCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition Backup Ephemeral Key (PXKBEK): Z - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition TLS E2E Master Secret Key (PXTLSE2EMSKY): Z - Partition TLS E2E Symmetric Key (PXTLSE2EKY): Z PCU - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition TLS E2E Master Secret Key (PXTLSE2EMSKY): Z - Partition TLS E2E Symmetric Key (PXTLSE2EKY): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): Z - Partition User General Purpose

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Symmetric Session Key (PUGPSSK): Z Pre-CO Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Password Encryption Key (PXPEKY): E - Partition User Login Password Data (PULPDA): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E
GP_SM_MGMT	Provides secure machine (SM) mgmt services	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	SW-RSA-SigVer (FIPS186-5)	MCO PCO - Partition Owner Trust Anchor Certificate (POOTACT): E
GP_STM_KEM	Provides secure transport mode (STM) services	Success with fips_state	Opcode Inputs	Opcode Outputs	SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KTS-IFC (KTS) CPT-Hash-DRBG	Unauthenticated - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	for the HSM.	= 2 or 3			SW-HMAC-SHA3-512 SW-KDA-HKDF-Sp800-56Cr1 SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5) SW-SHA3-512	NSR): E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): E,R - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): Z,E - HSM Manufacturer STM KEM Encrypted Random Key (HMSTMKERKY): Z,E,R,G - HSM Manufacturer STM KEM Random Key (HMSTMRKY): Z,G,E - HSM Owner Trust Anchor Certificate (HOOTACT): E - Partition DRBG Hash C Entropy State (PXDRBGHAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E
GP_USER_MGMT	Provides services to manage user accounts and roles within the HSM.	Success with fips_state = 2 or 3	Opcode Inputs	Opcode Outputs	KAS-IFC-OneStep (SP800-56Br2) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) CPT-AES-CBC CPT-Hash-DRBG SW-PBKDF SW-RSA-SigGen (FIPS186-5) SW-RSA-SigVer (FIPS186-5)	AU - Partition Master Encryption Key (PXMEKY): E - Partition Password Encryption Key (PXPEKY): E - Partition User Login Password Data (PULPDA): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E MCO - FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR): E - Partition Authentication Certificate (PXPACT): E - Partition DRBG Hash C Entropy State (PXDRBGHACST): E - Partition DRBG Hash V Entropy State (PXDRBGHAVST): E - Partition Master Encryption Key

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ST): E - Partition Master Encryption Key (PXMEKY): E - Partition Password Encryption Key (PXPEKY): E,G - 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 - Partition User Login Password Data (PULPDA): Z,E,W - Partition User Password

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key Ephemeral Key Public (PUPEEKPUB): Z,E,W - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E,W PCU - Partition Master Encryption Key (PXMEKY): E - Partition Password Encryption Key (PXPEKY): E - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): E - Partition User Login Password Data (PULPDA): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E Pre-CO - Partition Master Encryption Key (PXMEKY): E - Partition Password Encryption Key (PXPEKY): E - Partition User Login

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Password Data (PULPDA): E - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): E Unauthenticated - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): E - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): E - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): E - Partition Authentication Key Private RSA (PXPAKYPRVRSA): E - Partition Data Encryption Key (PXDEKY): E - Partition Owner Authentication Certificate (POOAUCT): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
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) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS)	AU - ML-DSA Seed: Z - ML-KEM Seed: Z - Partition Authentication Key Private RSA (PXPAKYPRV RSA): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Owner KBK Key (POKBKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECA KYPUB): Z - Partition User General Purpose Asymmetric Key Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): 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 User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z MCO - FIPS Partition HSM Manufacturer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Master Authentication Certificate ECC (FPHMMACTECC): Z - FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA): Z - FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC): Z - FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA): Z - FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA): Z - FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY): Z - HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC): Z - HSM Manufacturer Hardware Unique 2 Key (HMHU2KY): Z - HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA): Z - HSM Master Encryption Key (HXMEKY): Z - HSM Owner Attestation Key Public (HOOATKYPUB): Z - HSM Owner Key Backup Key (HOKBKY): Z - HSM Owner Recovery Key (HOREKY): Z - HSM Owner Trust Anchor Certificate (HOOTACT): Z - HSM Vendor Authentication Root Certificate ECC (HVARCTEC): Z - HSM Vendor Authentication Root Certificate RSA (HVARCTRSA): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- ML-DSA Seed: Z - ML-KEM Seed: Z - Partition Authentication Certificate (PXPACT): Z - Partition Authentication Key Private RSA (PXPAKYPRV RSA): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Key Backup Key (PXKBKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Owner KBK Key (POKBKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Password Encryption Key (PXPEKY): Z - Partition TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): 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 User General Purpose Symmetric Key (PUGPSKY): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition User General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User Login Password Data (PULPDA): Z - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): Z PCO - HSM Master Encryption Key (HXMEKY): E - ML-DSA Seed: Z - ML-KEM Seed: Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate (POOAUCT): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Owner KBK Key (POKBKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): 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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Purpose Session Key Public (PUGPSKYPUB): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z PCU - ML-DSA Seed: Z - ML-KEM Seed: Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Owner KBK Key (POKBKY): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): 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 (PUGPSKYPU

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						B): Z - Partition User General Purpose Symmetric Key (PUGPSKY): Z - Partition User General Purpose Symmetric Session Key (PUGPSSK): Z Pre-CO - HSM Master Encryption Key (HXMEKY): Z - HSM Owner Attestation Key Public (HOOATKYPUB): Z - ML-DSA Seed: Z - ML-KEM Seed: Z - Partition Authentication Certificate (PXPACT): Z - Partition Authentication Key Private RSA (PXPAKYPRVRSA): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Key Backup Key (PXKBKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Owner KBK Key (POKBKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Password Encryption Key (PXPEKY): Z - Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): Z - Partition User General Purpose HMAC Key (PUGPMKY): Z - Partition User General Purpose

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						HMAC Session Key (PUGPMSK): Z - Partition User General Purpose Key Public (PUGPKYPUB): 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 Login Password Data (PULPDA): Z - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): Z Unauthenticated - HSM Master Encryption Key (HXMEKY): Z - HSM Owner Attestation Key Public (HOOATKYPUB): Z - ML-DSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Seed: Z - ML-KEM Seed: Z - Partition Authentication Certificate (PXPACT): Z - Partition Authentication Key Private RSA (PXPAKYPRV RSA): Z - Partition Data Encryption Key (PXDEKY): Z - Partition Key Backup Key (PXKBKY): Z - Partition Key Loading Key (PXKLKY): Z - Partition Masking Key (PXMSKY): Z - Partition Master Encryption Key (PXMEKY): Z - Partition Owner Authentication Certificate (POOAUCT): Z - Partition Owner KBK Key (POKBKY): Z - Partition Owner Trust Anchor Certificate (POOTACT): Z - Partition Password Encryption Key (PXPEKY): Z - Partition TLS E2E Client

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key Public (PXTLSE2ECAKYPUB): Z - Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV): Z - Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV): 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 User General Purpose Symmetric Key (PUGPSKY): Z - Partition User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						General Purpose Symmetric Session Key (PUGPSSK): Z - Partition User Login Password Data (PULPDA): Z - Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA): Z

Table 15: Approved Services

- Indicator for Approved services:
  The indicator is success for all Approved services when the partition is operated in the approved mode. The following codes are used in the Access Rights to Keys and/or SSPs column in the above table.
  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.
  E = Execute: The module uses the SSP in performing a cryptographic operation.
  Z = Zeroize: The module zeroizes the SSP.

  All Approved services can be executed in the Non-Approved services mode with indicator of “success with fips_state=0”.
  Approved services that also support the use of non-approved security functions are enumerated in the Non-Approved Services table below with their supported non-approved security functions.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
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_DERIVE_KEY (non-compliant)	Derives a key using a supported KDF mechanism with the params given by the user.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-	PCU

Name	Description	Algorithms	Role
		compliant) SW-RSA-Decryption-Primitive (non-compliant) KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant) KAS-KDA-HKDF (SP800-56Ar3) (non-compliant) ML-KEM ECDH Derive (non-compliant)	
CN_ENCRYPT_SESSION (non-compliant)	Enables encrypted communication channel. Caveat is Non Approved mode allow the additional Cipher suite E2E_RSA_AES128_GCM_SHA256	SW-RSA-Decryption-Primitive (non-compliant) KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant) KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant) KAS-KDA-HKDF (SP800-56Ar3) (non-compliant) SW-SHA2-256 (non-compliant) SW-AES-GCM (non-compliant)	Unauthenticated
CN_ENCRYPT_SESSION_V2 (non-compliant)	Enables encrypted communication channel. Caveat is Non Approved mode allow the additional nonapproved cipher suites	SW-RSA-Decryption-Primitive (non-compliant) KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant) KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant) SW-SHA2-256 (non-compliant) SW-AES-GCM (non-compliant) ML-KEM ECDH Derive (non-compliant)	Unauthenticated

Name	Description	Algorithms	Role
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.	SW-AES-KW (non-compliant) SW-AES-KWP (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant)	PCU, PCO, AU
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_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	SW-RSA-KeyGen (FIPS186-5) (non-compliant) SW-KAS-ECC-Sp800-56Ar3 (non-compliant) SW-ECDSA-KeyGen (FIPS186-4) (non-compliant)	PCU
CN_GENERATE_PBE_KEY	Generate PBE TDES 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_config file.	SW-Counter-DRBG (Allowed Per IG 2.4.A) (non-compliant) SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU
CN_INSERT_MASKED_OBJECT (non-compliant)	Inserts a masked object into an HSM that is extracted from another HSM.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant)	PCU, PCO, AU
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_VERIF	Verifies a signature using ML-DSA and ECDSA sign algorithm.	ML-DSA ECDSA Verify (non-compliant)	PCU

Name	Description	Algorithms	Role
Y(non-compliant)			
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	SW-RSA-SigVer (FIPS186-5) (non-compliant)	MCO
CN_STORE_VENDOR_PRE_SHARED_KEY (CN_STORE_KBK_SHARE) (non-compliant)	Stores fixed keys (KBK) for backup. Including PKCS#1v1.5	SW-RSA-Decryption-Primitive (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-KDA-HKDF-Sp800-56Cr1 (non-compliant)	MCO
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, RSA PKCS1V1.5 Unwrap,NID_X9_62_prime192v1/ NID_sect163k1/NID_ED25519/NID_sect163r2/NID_secp192k1/NID_brainpoolP160r1/NID_brainpoolP192r1/NID_X25519/NID_X448,Triple-DES	SW-RSA-Decryption-Primitive (non-compliant) KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant) KAS-KDA-HKDF (SP800-56Ar3) (non-compliant) ML-KEM RSA (non-compliant) ML-KEM ECDH (non-compliant)	PCU
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,	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-RSA-Decryption-Primitive (non-	PCU

Name	Description	Algorithms	Role
	Triple-DES CBC mode, Triple-DES NIST Wrap mode,RSA-PKCS1V1.5 Wrap	compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) ML-KEM RSA (non-compliant) ML-KEM ECDH (non-compliant)	
LSPAY_CVV_GEN	Generates CVV, CVV2, iCVV on given card details.	SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant)	PCU
LSPAY_CVV_VERIFY	Verifies CVV with given card details		PCU
LSPAY_DECRYPT	Decrypts input data or PIN.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant) DES (non-compliant) Double-DES (non-compliant)	PCU
LSPAY_DECRYPT_THEN_ENCRYPT	Decrypts the input cipher text with one key and encrypts with another key.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant) DES (non-compliant) Double-DES (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_DERIVE_KEY	Derives DUKPT working key from the BDK.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant) DES (non-compliant)	PCU
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.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (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.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU
LSPAY_EMV_GENVERIFY	Perform EMV crypto operations. Generate ARPC. Generate or Verify ARQC.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_EMV_SECURE_MSG_GEN	Generates MAC over secure message.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU
LSPAY_ENCRYPT	Encrypts input data or PIN.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant) DES (non-compliant) Double-DES (non-compliant)	PCU
LSPAY_EXPORT_KEY	Exports symmetric key wrapped with TR31,AES_CBC/ AES_CBC_PAD.	SW-AES-KW (non-compliant) SW-TDES-KW (non-compliant)	PCU
LSPAY_EXPORT_KPK	Export a Key Block Protection Key (KBPK)	SW-RSA-Decryption-Primitive (non-compliant) KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant) KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant)	PCU
LSPAY_EXPORT_PUBLIC_KEY	Exports public key for BYOK.		PCU
LSPAY_EXPORT_TR34_KEY	Exports symmetric keys wrapped with TR34 mechanism	SW-RSA-Decryption-Primitive (non-compliant)	PCU
LSPAY_FPE_DECRYPT	Performs FPE FF1/FF3-1 decrypt operation on input data.	SW-AES-ECB (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_FPE_ENCRYPT	Performs FPE FF1/FF3-1 encrypt operation on input data.	SW-AES-ECB (non-compliant)	PCU
LSPAY_FUNCTIONALITY_GET	Gets status of enabled/disabled LSPay services		PCO
LSPAY_FUNCTIONALITY_SET	Enable/Disable services		PCO
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)	SW-RSA-KeyGen (FIPS186-5) (non-compliant) SW-ECDSA-KeyGen (FIPS186-4) (non-compliant)	PCU
LSPAY_GENERATE_CSR	Create CSR with given key pair.	SW-RSA-KeyGen (FIPS186-5) (non-compliant) SW-RSA-SigGen (FIPS186-5) (non-compliant) SW-ECDSA-KeyGen (FIPS186-4) (non-compliant) SW-ECDSA-SigGen (FIPS186-4) (non-compliant)	PCU
LSPAY_GENERATE_SYMM_KEY	Generates symmetric key AES, TDES keys used for LSPay operations	SW-Counter-DRBG (Allowed Per IG 2.4.A) (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.	SW-AES-KW (non-compliant) SW-TDES-KW (non-compliant)	PCU
LSPAY_IMPORT_KEY	Import symmetric or asymmetric keys. Wrap mech: TR31, AES_CBC, AES_CBC_PAD.	SW-AES-KW (non-compliant) SW-TDES-KW (non-compliant)	PCU
LSPAY_IMPORT_KPK	Imports OAEP wrapped or ECDH_AES_PAD wrapped symmetric key.	SW-RSA-Decryption-Primitive (non-compliant) KAS-ANS-9.63 (Sp800-56Ar3) (non-compliant) KAS-ANS-9.63 [AES-KW] (Sp800-56Ar3) (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_IMPORT_PUBLIC_KEY	Import an RSA public key	SW-RSA-Decryption-Primitive (non-compliant)	PCU
LSPAY_IMPORT_TR34_KEY	Import symmetric keys using TR- 34 unwrap.	SW-RSA-SigVer (FIPS186-5) (non-compliant)	PCU
LSPAY_KEY_SHARE_COMBINE_INIT	Starts combine key init.		PCU
LSPAY_KEY_SHARE_COMBINE_KEY	Combines all components of the key.	Shamir Key Share (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	SW-AES-KW (non-compliant)	PCU
LSPAY_KEY_SHARE_IMPORT_COMPONENT	Imports component of the key.	SW-AES-KW (non-compliant)	PCU
LSPAY_KEY_SHARE_ZEROIZE	Erases all components of the key.		PCU
LSPAY_MAC_GEN	Computes MAC on input data. Algorithm used: DES/Triple-DES	SW-AES-CMAC (non-compliant) SW-TDES (SP 800-38B) (non-compliant) SW-HMAC-SHA-1 (non-compliant) SW-HMAC-SHA2-224 (non-compliant) SW-HMAC-SHA2-256 (non-compliant) SW-HMAC-SHA2-384 (non-compliant) SW-HMAC-SHA2-512 (non-compliant) SW-HMAC-SHA3-224 (non-compliant) SW-HMAC-SHA3-256 (non-compliant) SW-HMAC-SHA3-384 (non-compliant) SW-HMAC-SHA3-512 (non-compliant)	PCU

Name	Description	Algorithms	Role
		DES MAC (non-compliant)	
LSPAY_MAC_TRANSLATE	Translates MAC by using new key on input data.	SW-AES-CMAC (non-compliant) SW-TDES (SP 800-38B) (non-compliant) DES (non-compliant)	PCU
LSPAY_MAC_VERIFY	Verifies MAC with calculated AMC on input data.	SW-AES-CMAC (non-compliant) SW-TDES (SP 800-38B) (non-compliant) DES (non-compliant)	PCU
LSPAY_MFK_DELETE	Deletes MFK.		PCO
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_PINBLK_TRANSLATE	Decrypts the input PIN using decryption key, translates to given PIN format and encrypts with another key.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-RSA-Decryption-Primitive (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU
LSPAY_PVV_GEN	Perform PVV generation on PIN and PAN data.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU

Name	Description	Algorithms	Role
LSPAY_PVV_VERIFY	Verifies given PVV.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU
LSPAY_SIGN	Performs sign and verify on input data.	SW-RSA-SigGen (FIPS186-5) (non-compliant) SW-ECDSA-SigGen (FIPS186-4) (non-compliant) SW-EDDSA (FIPS186-4) (non-compliant)	PCU
LSPAY_SIGN_VERIFY	Verifies sign on input data.	SW-RSA-SigVer (FIPS186-5) (non-compliant) SW-ECDSA-SigVer (FIPS186-4) (non-compliant)	PCU
LSPAY_TRANSLATE_KEY	Translates wrapped key from one KPK to other KPK.	SW-AES-KW (non-compliant) SW-AES-KWP (non-compliant)	PCU
LSPAY_VALIDATE_PUBLIC_KEY	Validates the RSA public key	SW-RSA-Decryption-Primitive (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.	SW-TDES-ECB (non-compliant) SW-TDES-CBC (non-compliant) SW-AES-ECB (non-compliant) SW-AES-CBC (non-compliant) SW-TDES-ECB [192-bit] (non-compliant) SW-TDES-CBC [192-bit] (non-compliant)	PCU
MAJOR_OP_ME_PKCS_LARGE (non-	PKCS#1v1.5 encrypt and decrypt	SW-RSA-Decryption-Primitive (non-compliant)	PCU

Name	Description	Algorithms	Role
compliant)/MAJOR_OP_ME_PKCS (non-compliant)			

Table 16: Non-Approved Services

Indicator for non-Approved services
The indicator is success for all non-approved services only when the partition is operated in the non-approved mode. 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 commands to upload the signed firmware to the module:

- CN_FW_UPDATE_BEGIN: This service initiates the firmware update process.
- 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.
- 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.

As part of firmware load operation, the new firmware's integrity and authenticity is verified by the active firmware using RSA 2048 signatures with SHA2-256 (#A1948) or ECDH P-521 with SHA2-512 (#A1948).

5 Software/Firmware Security

5.1 Integrity Techniques

Firmware integrity is verified by the bootloader during the boot up using RSA 2048 signatures with SHA2-256 (#A6878) or ECDH P-521 signature with SHA2-512 (#A6878) 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.

5.2 Initiate on Demand

The firmware integrity test can be initiated on demand by power-cycling the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied]:

The module implements a limited operational environment running SMP Linux operating system on the Octeon-TX2 (64-bit Armv8.2-based) control processor. FIPS 140-3 Area 6 Operational Environment requirements do not apply to the module in this validation.

The module supports firmware validation by ensuring that only signed firmware from the manufacturer is accepted. The module firmware is authenticated using cryptographic keys on every reboot and during firmware updates.
Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-3 validation.

6.2 Additional Information

The module is a hardware module with a limited operational environment and Physical Security Level 3.

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 embodiment is multi-chip embedded.

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

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	-13C	EFP	Shutdown
HighTemperature	100C	EFP	Shutdown
LowVoltage	-3.01V (PCIe 3.3V Aux), 3.08V (PCIe 3.3V Rail), 10.9V (PCIe 12V Rail)	EFP	Shutdown
HighVoltage	3.68V (PCIe 3.3V Aux), 3.75V (PCIe 3.3V Rail), 13.5V (PCIe 12V Rail)	EFP	Shutdown

Table 18: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40C
HighTemperature	100C

Table 19: Hardness Testing Temperatures

8 Non-Invasive Security

8.1 Mitigation Techniques

Not Applicable for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DDR4	Ephemeral RAM	Dynamic
eMMC	read/write memory	Static
MCU	read/write memory	Static
NOR	read/write 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
AES-GCM-Unwrap-	Entered	eMMC_Flash	Encrypted	Automated	Electronic	SW-AES-GCM-Unwrap (KTS)

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input-Method						
AES-GCM-Wrap-Output-Method	eMMC Flash	External	Encrypted	Automated	Electronic	SW-AES-GCM-Wrap (KTS)
AES-Unwrap-Input-Method	Entered	eMMC_Flash	Encrypted	Automated	Electronic	SW-AES-KW-Unwrap (KTS)
AES-Unwrap-Pad-Input-Method	Entered	eMMC_Flash	Encrypted	Automated	Electronic	SW-AES-KWP-Unwrap (KTS)
AES-Wrap-Output-Method	eMMC Flash	External	Encrypted	Automated	Electronic	SW-AES-KW-Wrap (KTS)
AES-Wrap-Pad-Output-Method	eMMC Flash	External	Encrypted	Automated	Electronic	SW-AES-KWP-Wrap (KTS)
Backup-Key-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-AES-KW-Wrap (KTS)
Key-Transport-Input-Method	Entered	eMMC_Flash	Encrypted	Automated	Electronic	SW-KTS-IFC (KTS)
Password-Input-Method	Entered	eMMC_Flash	Encrypted	Automated	Electronic	SW-AES-KWP-Unwrap (KTS)
Public-Key-Plain-Input-Method	Entered	eMMC_Flash	Plaintext	Automated	Electronic	
Public-Key-Plain-Output-Method	eMMC_Flash	External	Plaintext	Automated	Electronic	
Restore-Key-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-AES-KW-

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
						Unwrap (KTS)
Shared-Secret-Plain-Input-Method	Entered	eMMC	Encrypted	Automated	Electronic	SW-KTS-IFC (KTS)
Shared-Secret-Plain-Output-Method	eMMC	External	Encrypted	Automated	Electronic	SW-KTS-IFC (KTS)
VKBK-Input-Method	Entered	NOR_Flash	Encrypted	Automated	Electronic	SW-KTS-IFC (KTS)

Table 21: SSP Input-Output Methods

The module supports the above Input-Output methods.

Private/Secret keys are always encrypted when doing export/import,

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
D	Manually zeroized (via 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 Partitions' SSPs, including the HSM adapter owner programmed ones (Brings HSM to factory state. Factory reset via CN_ZEROIZE service with factory-reset as argument with MCO credentials)	wipes all ssps with zeros in 1 second	CN_ZEROIZE
MZ	Zeroize all Partitions' SSPs, except vendor programmed ones (HSM zeroize via 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 CN_DELETE_PARTITION service)	wipes all ssps with	CN_DELETE_PARTITION

Zeroization Method	Description	Rationale	Operator Initiation
		zeros in 1 second	
PFZ	Zeroize all SSPs in the Partition (Factory reset via CN_ZEROIZE service with factory-reset as argument with PCO credentials)	wipes all ssps with zeros in 1 second	CN_ZEROIZE
PZ	Zeroize all User SSPs in the Partition Regular p (User Partition Regular zeroize via CN_ZEROIZE service with PCO credentials))	wipes all ssps with zeros in 1 second	CN_ZEROIZE
S	Zeroized on session close (Session Close via 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 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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR)	The entropy input string and seed for the Approved DRBG.	12672-bits - 256-bits	Entropy - CSP	ENT_(P)_(SP 800-90B)		CPT-Hash-DRBG SW-Counter-DRBG
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			SW-ECDSA-KeyVer (FIPS186-4) SW-ECDSA-SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						(FIPS186-4)
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			RSA SigVer (FIPS186-5) (A6878)
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	Pre-Loaded		SW-ECDSA-SigGen (FIPS186-4)
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	Pre-Loaded		SW-KTS-IFC SW-RSA-SigGen (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)
FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY)	AES 256-bit key used to derive KBK.	256-bits - 256-bits	Symmetric Key - CSP		SW-KTS-IFC (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)	SW-KDF-SP800-108

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	Pre-Loaded		SW-ECDSA-KeyVer (FIPS186-4) SW-ECDSA-SigVer (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	Pre-Loaded		SW-ECDSA-SigGen (FIPS186-4)
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	Pre-Loaded		SW-AES-CBC SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA)	RSA 2048-bit or 4096-bit public key certificate used for STM Lock.	2048-bits, 4096-bits - 112-bits, 150-bits	Public - PSP	Pre-Loaded		SW-KTS-IFC (KTS)
HSM Manufacturer STM KEM Encrypted Random Key (HMSTMKERKY)	AES 256 bit encrypted key with MFDEK used in STM KEM Lock	256-bits - 256-bits	Symmetric Key - CSP	SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)		SW-HMAC-SHA3-512

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HSM Manufacturer STM KEM Random Key (HMSTMRKY)	AES 256 bit key generated during STM KEM Lock to encrypt sensitive keys in NOR.	256-bits - 256-bits	Symmetric Key - CSP	CPT-Hash-DRBG	SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)	SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
HSM Master Encryption Key (HXMEKY)	AES 256-bit key used to encrypt Master Partition CSPs and authentication data stored in persistent storage of the HSM.	256-bits - 256-bits	Symmetric Key - CSP	CPT-Hash-DRBG		SW-AES-CBC SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
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)
HSM Owner Key Backup Key (HOKBKY)	AES 256-bit key used to derive KBK.	256-bits - 256-bits	Symmetric Key - CSP		SW-KTS-IFC (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-	SW-KDF-SP800-108

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					KWP-Wrap (KTS)	
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-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
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)
HSM Vendor Authentication Root Certificate ECC (HVARCTEC)	ECC P521 public key certificate used to issue FMAEC certificates.	521-bits - 256-bits	Public - PSP			SW-ECDSA-KeyVer (FIPS186-4) 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			SW-RSA-SigVer (FIPS186-5)
HSM Vendor Firmware Update Validation Key Public ECC	ECDSA 521-bit public key used to authenticate new FW images	521-bits - 256-bits	Public - PSP	Pre-Loaded		SW-ECDSA-SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
(HVFUVKYPUBECC)	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					(FIPS186-4)
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	Pre-Loaded		SW-RSA-SigVer (FIPS186-5)
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			SW-RSA-SigVer (FIPS186-5)
ML-DSA Seed	Seed generated to be used with ML-DSA KeyGen, SigGen or SigVer	256 bits - 256 bits	Random seed - CSP	CPT-Hash-DRBG		OQS-ML-DSA-KeyGen OQS-ML-DSA-SigGen OQS-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						ML-DSA-SigVer
ML-KEM Seed	Seed(s) generated to be used with ML-KEM KeyGen or Encaps/Decaps	256 bits - 512 bits - 256 bits	Random Seed - CSP	CPT-Hash-DRBG		OQS-ML-KEM-EncapDecap OQS-ML-KEM-KeyGen
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 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 Backup Ephemeral Key (PXKBEK)	Key used to backup and restore partition data.	256-bits - 256-bits	Symmetric Key - CSP	SW-Counter-DRBG		SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
Partition Cert Auth Ephemeral Key (PXCAEK)	Shared secret Z for SP 800-56Br2 KAS2,	512-bits - 112-bits	Symmetric Key - CSP	SW-KDF-SP800-108		SW-KDF-SP800-108

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	using PAK and POAC					
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-Hash-DRBG		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
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) KAS-IFC-OneStep (SP800-56Br2)	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 -56Br2 KAS2 -bilateral -confirmation key agreement to generate shared secret Z. At HSM partition level, used to establish secure channel for cloning process (to exportpartition masking key).	ECC:521-bits; RSA:2048-bits - ECC:256-bits; RSA:112-bits	Private - CSP	SW-ECDSA-KeyGen (FIPS186-4) SW-RSA-KeyGen (FIPS186-5)		KAS-KDA-ONESTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2)
Partition Cloning Ephemeral Key	ECC 521-bit ephemeral	ECC:521-bits -	Public - PSP	SW-ECDSA-		KAS-IFC-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Public (PXCLEKPUB)	public key used in SP 800-56Ar3 C (2,0, ECC DH) key agreement - bilateral - confirmation key agreement to generate sharedsecret Z.	ECC:256-bits		KeyGen (FIPS186-4)		OneStep (SP800-56Br2)
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 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-KDF-SP800-108
Partition Data Encryption Key (PXDEKY)	AES 256-bit key used to wrap PAK and POKBK	256-bits - 256-bits	Symmetric Key - CSP	SW-Counter-DRBG		SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
Partition DRBG CTR Key Entropy State (PXDRBGCTKST)	The internal state (Key) for the Counter DRBG.	256-bits - 256-bits	Internal State Value - CSP	SW-Counter-DRBG		SW-Counter-DRBG
Partition DRBG CTR V Entropy State	The internal state (V) for the Counter DRBG.	128-bits - 256-bits	Internal State	SW-Counter-DRBG		SW-Counter-DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
(PXDRBGCTVST)			Value - CSP			
Partition DRBG Hash C Entropy State (PXDRBGHACST)	The internal state (C) for the Hash DRBG.	896-bits - 256-bits	Internal State Value - CSP	CPT-Hash-DRBG		CPT-Hash-DRBG
Partition DRBG Hash V Entropy State (PXDRBGHAVST)	The internal state (V) for the Hash DRBG.	896-bits - 256-bits	Internal State Value - CSP	CPT-Hash-DRBG		CPT-Hash-DRBG
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) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
Partition Key Loading Key (PXKLKY)	A 256-bit AES key derived from Z; used to decrypt the imported CSPs	256-bits - 256-bits	Symmetric Key - CSP		KAS-KDA-ONESTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2)	SW-AES-CBC SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) CPT-AES-GCM
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.	521-bits - 512-bits	Private - CSP	FW-ECDSA-KeyGen (FIPS186-4)		KAS-KDA-ONESTEP (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 - bilateral - confirmation key agreement to generate sharedsecret Z.	ECC:521-bits - ECC:256-bits	Public - PSP	SW-ECDSA-KeyGen (FIPS186-4)		KAS-IFC-OneStep (SP800-56Br2)
Partition Key Loading Key Shared Secret (PXKLSZ)	Shared secret Z for SP 800-56Ar3 C (2,0, ECC DH) or SP800-56Br2 KAS2.	256-bits - 256-bits	Symmetric Key - CSP		SW-KAS-IFC-SSC SW-KAS-ECC-SSC-Sp800-56Ar3	SW-KDA-OneStep-Sp800-56Cr1
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-Hash-DRBG		SW-AES-KW-Wrap (KTS) SW-AES-KW-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						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-Counter-DRBG		CPT-AES-CBC
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 Owner Client Authentication Trust Anchor Certificate (POCAUTACT)	Public key certificate used as trust anchor of PCO for e2e authentication	2048-bits - 112-bits	Public - PSP			SW-ECDSA-SigVer (FIPS186-4) SW-RSA-SigVer (FIPS186-5)
Partition Owner KBK Key (POKBKY)	AES 256-bit key used to derive KBK.	256-bits - 256-bits	Symmetric Key - CSP		SW-KTS-IFC (KTS) SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)	SW-KDF-SP800-108
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)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Partition Password Encryption Key (PXPEKY)	AES-256 key for encrypting user passwords during user creation and authentication.	256-bits - 256-bits	Symmetric Key - CSP		KAS-IFC-OneStep (SP800-56Br2)	SW-AES-KWP-Unwrap (KTS) SW-AES-KWP-Wrap (KTS)
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-KTS-IFC (KTS) KAS-KDA-ONESTEP (SP800-56Ar3)	SW-KDF-SP800-108
Partition TLS E2E Client Authentication Certificate (PXTLSE2ECACT)	RSA or EC certificate presented by client during E2E/TLS handshake to allow E2E/ TLS client authentication.	RSA:2048-bits - 4096-bits; EC:256-bits - 521-bits - RSA:112-bits - 150-bits; EC:128-bits - 256-bits	Public - PSP			
Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB)	RSA or EC public key of approved modulus or curveId to allow E2E/ TLS client authentication in E2E/ TLS handshake	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)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
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)		KAS-TLS (Sp800-56Ar3)
Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EKPUBECC)	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)		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 - 256-bits	Symmetric Key - CSP		CPT-KDF-TLS	CPT-KDF-TLS
Partition TLS E2E Pre Master Secret (PXTLSE2EPMS)	pre-master secret, used to derive master secret.	128-bits - 256-bits - 128-bits - 256-bits	Symmetric Key - CSP		CPT-KAS-ECC-SSC-Sp800-56Ar3	KAS-KDA-HKDF (SP800-56Ar3)
Partition TLS E2E Symmetric Key (PXTLSE2EKY)	AES 256 key used for encrypting TLS sessions.	256-bits - 256-bits	Symmetric Key - CSP		CPT-KDF-TLS	CPT-AES-GCM
Partition User Cloning Ephemeral Key Public (PUCLEKPUB)	ECC 521-bit or RSA 2048- bit ephemeral public key used in SP 800-56Br2 KAS2 - bilateral - confirmation key agreement to generate shared secret Z.	ECC:521-bits; RSA:2048-bits - ECC:256-bits; RSA:112-bits	Public - PSP			KAS-KDA-ONESTEP (SP800-56Ar3)
Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV)	RSA/ECDSA/ECDH/ML-DSA/ML-KEM general purpose keys.	RSA:2048-bits, 3072-bits, 4096-bits; ECDSA: 224-bits, 256-bits, 384-bits,	Private - CSP	FW-ECDSA-KeyGen (FIPS186-4) OQS-ML-DSA-KeyGen OQS-ML-	SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap (KTS)	KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		521-bits; ML-DSA: 20480, 32256, 39168 bits; ML-KEM: 13056, 19200, 25344 bits; - 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;		KEM-KeyGen	SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS)	KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS) CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST SW-ECDSA-KeyVer (FIPS186-4) CPT-ECDSA-SigGen (FIPS186-4) CPT-KAS-ECC-SSC-Sp800-56Ar3 SW-KAS-ECC-SSC-Sp800-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						56Ar3 SW-KDA-HKDF-Sp800-56Cr1 SW-KDF-ANS-9.63 CPT-RSA-Decryption-Primitive SW-RSA-Decryption-Primitive SW-RSA-SigGen (FIPS186-5) CPT-RSA-Signature-Primitive OQS-ML-DSA-SigGen OQS-ML-KEM-EncapDecap
Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV)	RSA/ECDSA/ECDH/ML-DSA/ML-KEM general purpose keys.	RSA:2048-bits, 3072-bits, 4096-bits; ECDSA: 224-bits, 256-bits,	Private - CSP	FW-ECDSA-KeyGen (FIPS186-4) OQS-ML-DSA-KeyGen OQS-	SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap	KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		384-bits, 521-bits; ML-DSA: 20480, 32256, 39168 bits; ML-KEM: 13056, 19200, 25344 bits; - 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;		ML-KEM-KeyGen	(KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS)	56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS) CPT-ECDH-NON-NIST CPT-ECDSA-SigGen-NON-NIST SW-ECDSA-KeyVer (FIPS186-4) CPT-ECDSA-SigGen (FIPS186-4) CPT-KAS-ECC-SSC-Sp800-56Ar3 SW-KAS-ECC-SSC-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Sp800-56Ar3 SW-KDA-HKDF-Sp800-56Cr1 SW-KDF-ANS-9.63 CPT-RSA-Decryption-Primitive SW-RSA-Decryption-Primitive SW-RSA-SigGen (FIPS186-5) CPT-RSA-Signature-Primitive OQS-ML-DSA-SigGen OQS-ML-KEM-EncapDecap
Partition User General Purpose HMAC Key (PUGPMKY)	HMAC general purpose keys (minimum key size of 160 bits).	160-bits - 512-bits - 112-bits - 256-bits	Symmetric Key - CSP	SW-Counter-DRBG	SW-AES-GCM-Unwrap (KTS) SW-AES-KW-	CPT-HMAC-SHA2-256 CPT-HMAC-SHA2-384

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS)	CPT-HMAC-SHA2-512 SW-HMAC-SHA-1 SW-HMAC-SHA2-256 SW-HMAC-SHA2-384 SW-HMAC-SHA2-512
Partition User General Purpose HMAC Session Key (PUGPMSK)	HMAC general purpose keys (minimum key size of 160 bits).	160-bits - 512-bits - 160-bits - 256-bits	Symmetric Key - CSP	SW-Counter-DRBG	SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS)	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 User General Purpose	RSA/ECDSA/ECDH/ML-	RSA:2048-bits,	Public - PSP	FW-ECDSA-		KAS-ANS-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Key Public (PUGPKYPUB)	DSA/ML-KEM general purpose public keys.	3072-bits, 4096-bits; ECDSA: 224-bits, 256-bits, 384-bits, 521-bits; ML-DSA: 10496, 15616, 20736 bits; ML-KEM: 6400, 9472, 12544 bits; - 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;		KeyGen (FIPS186-4) OQS-ML-DSA-KeyGen OQS-ML-KEM-KeyGen		9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS) CPT-ECDSA-SigVer (FIPS186-4) SW-KAS-ECC-SSC-Sp800-56Ar3 SW-KDF-ANS-9.63 SW-RSA-SigVer (FIPS186-5) OQS-ML-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						DSA-SigVer OQS-ML-KEM-EncapDecap SW-ECDSA-SigVer (FIPS186-4)
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: 10496, 15616, 20736 bits; ML-KEM: 6400, 9472, 12544 bits; - RSA:112-bits, 128-bits, 150-bits; ECDSA: 112-bits, 128-bits, 192-bits, 256-bits; ML-DSA:128-bits, 192-bits, 256-bits;	Public - CSP	FW-ECDSA-KeyGen (FIPS186-4) OQS-ML-DSA-KeyGen OQS-ML-KEM-KeyGen		KAS-ANS-9.63 (Sp800-56Ar3) KAS-KDA-HKDF (SP800-56Ar3) KAS-KDA-ONESTEP (SP800-56Ar3) KAS-KDA-TWOSTEP (SP800-56Ar3) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS) CPT-ECDSA-SigVer (FIPS186-4) SW-KAS-ECC-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		ML-KEM:128-bits, 192-bits, 256-bits;				SSC-Sp800-56Ar3 SW-KDF-ANS-9.63 SW-RSA-SigVer (FIPS186-5) OQS-ML-DSA-SigVer OQS-ML-KEM-EncapDecap SW-ECDSA-SigVer (FIPS186-4)
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-Counter-DRBG	SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-	SW-AES-GCM-Wrap (KTS) SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) LEGACY-SW-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					KWP-Unwrap (KTS) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS)	TDES-KW (KTS) CPT-AES-CBC CPT-AES-CCM CPT-AES-CMAC SW-AES-CMAC CPT-AES-CTR CPT-AES-ECB CPT-AES-GCM CPT-AES-GMAC CPT-TDES-CBC LEGACY-CPT-TDES-ECB LEGACY-SW-TDES-KW
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,	Symmetric Key - CSP	SW-Counter-DRBG	SW-AES-GCM-Unwrap (KTS) SW-AES-KW-Wrap (KTS)	SW-AES-GCM-Wrap (KTS) SW-AES-GCM-Unwrap (KTS)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		256-bits; Triple-DES:112-bits			SW-AES-KW-Unwrap (KTS) SW-AES-KWP-Wrap (KTS) SW-AES-KWP-Unwrap (KTS) SW-KTS-IFC (KTS) FW-KTS-IFC (KTS)	SW-AES-KW-Wrap (KTS) SW-AES-KW-Unwrap (KTS) LEGACY-SW-TDES-KW (KTS) CPT-AES-CBC CPT-AES-CCM CPT-AES-CMAC SW-AES-CMAC CPT-AES-CTR CPT-AES-ECB CPT-AES-GCM CPT-AES-GMAC CPT-TDES-CBC LEGACY-CPT-TDES-ECB
Partition User Key Loading Key	ECC 521-bit or RSA 2048- bit	ECC:521-bits;	Public - PSP			KAS-KDA-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Ephemeral Key Public (PUKLKEKPUB)	ephemeral public key used in SP 800-56Br2 KAS2 - bilateral - confirmation key agreement to generate shared secret Z.	RSA:2048-bits - ECC:256-bits; RSA:112-bits				ONESTEP (SP800-56Ar3) KAS-IFC-OneStep (SP800-56Br2)
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 User Password Encryption Key Ephemeral Key Public (PUPEEKPUB)	RSA 2048-bit public key loaded by the host used for SP 800-56Br2 key agreement togenerate PswdEncKey.	2048-bits - 112-bits	Public - PSP			KAS-KDA-ONESTEP (SP800-56Ar3)
Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC)	Used for key agreement as part of TLS-1.2 handshake protocol	256-bits - 512-bits - 128-bits - 256-bits	Public - PSP			KAS-TLS (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 Wrap Unwrap Shared Secret (PXWUSZ)	Shared secret Z for SP 800-56Ar3 KAS2 or Shared Secret Key in ML-KEM, using Peer's	128-bits - 256-bits - 112-bits - 256-bits	Shared Secret - CSP		OQS-ML-KEM-EncapDecap SW-	SW-KDA-HKDF-Sp800-56Cr1 SW-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	public key and User's private key in CN_WRAP_KEY and CN_UNWRAP_KEY				KAS-ECC-SSC-Sp800-56Ar3	KDF-ANS-9.63

Table 23: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR)		DDR4:Plaintext	Erase after use	E	Partition DRBG CTR V Entropy State (PXDRBGCTVST):Derives Partition DRBG CTR Key Entropy State (PXDRBGCTKST):Derives Partition DRBG Hash V Entropy State (PXDRBGHAVST):Derives Partition DRBG Hash C Entropy State (PXDRBGHACST):Derives
FIPS Partition HSM Manufacturer Master Authentication Certificate ECC (FPHMMACTECC)	Public-Key-Plain-Output-Method	eMMC:Plaintext		VZ	FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC):Paired With
FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA)	Public-Key-Plain-Output-Method	eMMC:Plaintext		VZ	FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA):Paired With
FIPS Partition HSM Manufacturer Master Authentication Key Private ECC		NOR:Encrypted		VZ	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By Partition Authentication Certificate (PXPACT):Signs FIPS Partition HSM

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
(FPHMMAKYPRVECC)					Manufacturer Master Authentication Certificate ECC (FPHMMACTECC):Paired With HSM Owner Recovery Key (HOREKY):Wrapped by
FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA)		NOR:Encrypted		VZ	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By Partition Authentication Certificate (PXPACT):Signs FIPS Partition HSM Manufacturer Master Authentication Certificate RSA (FPHMMACTRSA):Paired With HSM Owner Recovery Key (HOREKY):Wraps
FIPS Partition HSM Owner Authentication Certificate RSA (FPHOOAUCTRSA)	Public-Key-Plain-Input-Method	eMMC:Plaintext		MFZ	
FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY)	VKBK-Input-Method	NOR:Encrypted		VZ	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By HSM Owner Recovery Key (HOREKY):Wrapped By Partition Key Backup Key (PXKBKY):Derives
HSM Manufacturer Endorsement Certificate ECC (HMEDCTECC)		eMMC:Plaintext		VZ	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped by
HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC)		NOR:Encrypted		VZ	HSM Manufacturer Hardware Unique 2 Key (HMHU2KY):Wrapped By
HSM Manufacturer		NOR:Plaintext		VZ	FIPS Partition HSM Manufacturer Master

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Hardware Unique 2 Key (HMHU2KY)					Authentication Key Private RSA (FPHMMAKYPRVRSA):Wraps FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY):Wraps HSM Owner Key Backup Key (HOKBKY):Wraps HSM Manufacturer Endorsement Key Private ECC (HMEDKYPRVECC):Wraps FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC):Wraps
HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA)		eMMC:Plaintext		VZ	HSM Manufacturer STM KEM Encrypted Random Key (HMSTMKERKY):Encrypts
HSM Manufacturer STM KEM Encrypted Random Key (HMSTMKERKY)	Key-Transport-Input-Method	DDR4:Plaintext	Erase after use	VZ E	HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA):Encrypted By
HSM Manufacturer STM KEM Random Key (HMSTMRKY)	AES-Unwrap-Pad-Input-Method	DDR4:Plaintext	Erase after use	E	HSM Manufacturer STM KEM Certificate RSA (HMSTMCTRSA):Encrypted By
HSM Master Encryption Key (HXMEKY)		MCU:Plaintext		MZ	Partition Master Encryption Key (PXMEKY):Wraps Partition Data Encryption Key (PXDEKY):Wraps
HSM Owner Attestation Key Public (HOOATKYPUB)	Public-Key-Plain-Input-Method	eMMC:Plaintext		PZ	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
HSM Owner Key Backup Key (HOKBKY)	Key-Transport-Input-Method	eMMC:Encrypted		MFZ VZ	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		MFZ VZ	FIPS Partition HSM Manufacturer Master Authentication Key Private RSA (FPHMMAKYPRVRSA):Wrapped by FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY):Wraps FIPS Partition HSM Manufacturer Master Authentication Key Private ECC (FPHMMAKYPRVECC):Wraps
HSM Owner Trust Anchor Certificate (HOOTACT)	Public-Key-Plain-Input-Method	eMMC:Plaintext		MFZ	
HSM Vendor Authentication Root Certificate ECC (HVARCTEC)	Public-Key-Plain-Output-Method	eMMC:Plaintext		VZ	
HSM Vendor Authentication Root Certificate RSA (HVARCTRSA)	Public-Key-Plain-Output-Method	eMMC:Plaintext		VZ	
HSM Vendor Firmware Update Validation Key Public ECC (HVFUVKYPUBECC)		eMMC:Plaintext		N/A	
HSM Vendor Firmware Update Validation Key		eMMC:Plaintext		N/A	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Public RSA (HVFUVKYPUBRSA)					
HSM Vendor License Key Public RSA (HVLICKYPUBRSA)	Public-Key-Plain-Input-Method	eMMC:Plaintext		N/A	
ML-DSA Seed		eMMC:Plaintext		DS	Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV):Derives Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV):Derives Partition User General Purpose Key Public (PUGPKYPUB):Derives Partition User General Purpose Session Key Public (PUGPSKYPUB):Derives
ML-KEM Seed		eMMC:Plaintext		DS	Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV):Derives Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV):Derives Partition User General Purpose Key Public (PUGPKYPUB):Derives Partition User General Purpose Session Key Public (PUGPSKYPUB):Derives
Partition Authentication Certificate (PXPACT)	Public-Key-Plain-Input-Method Restore-Key-Input-	eMMC:Plaintext		PD	Partition Backup Ephemeral Key (PXKBEK):Wrapped By Partition Cert Auth Source Shared Secret (PXCASSZ):Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Method Backup-Key-Output-Method				
Partition Authentication Key Private RSA (PXPAKYPRVRSA)	Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted		PD	Partition Data Encryption Key (PXDEKY):Wrapped By Partition Owner KBK Key (POKBKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By Partition Cert Auth Target Shared Secret (PXCATSZ):Decrypts
Partition Backup Ephemeral Key (PXKBEK)	Backup-Key-Output-Method Restore-Key-Input-Method	DDR4:Plaintext	Erase after use	E	Partition Key Backup Key (PXKBKY):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 Key Public (PUGPKYPUB):Wraps Partition Masking Key (PXMSKY):Wraps Partition Authentication Key Private RSA (PXPAKYPRVRSA):Wraps Partition Authentication Certificate (PXPACT):Wraps Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA):Wraps Partition Password Encryption Key (PXPEKY):Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB):Wraps Partition Key Loading Key (PXKLKY):Wraps
Partition Cert Auth Ephemeral Key (PXCAEK)		DDR4:Plaintext	Erase after session close	S	Partition Cert Auth Source Shared Secret (PXCASSZ):Derived By Partition Cert Auth Target Shared Secret (PXCATSZ):Derived By
Partition Cert Auth Source Shared Secret (PXCASSZ)	Shared-Secret-Plain-Output-Method	DDR4:Plaintext	Erase after 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	Erase after 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 Cloning Encryption Ephemeral Key (PXCLEEK)		DDR4:Plaintext	Erase after use	E	Partition Cloning Shared Secret (PXCLSZ):Derived From Partition Masking Key (PXMSKY):Encrypts
Partition Cloning Ephemeral Key Private (PXCLEKPRV)		DDR4:Plaintext	Erase after use	E	Partition Cloning Shared Secret (PXCLSZ):Establish Partition Cloning Ephemeral Key Public (PXCLEKPUB):Paired With
Partition Cloning Ephemeral Key Public (PXCLEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition Cloning Ephemeral Key Private (PXCLEKPRV):Paired With
Partition Cloning MAC Ephemeral Key (PXCLMEK)		DDR4:Plaintext	Erase after use	E	Partition Cloning Shared Secret (PXCLSZ):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Partition Cloning Shared Secret (PXCLSZ)		DDR4:Plaintext	Erase 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 Data Encryption Key (PXDEKY)		NOR:Encrypted		PD	HSM Master Encryption Key (HXMEKY):Wrappped By Partition Authentication Key Private RSA (PXPAKYPRVRSA):Wraps
Partition DRBG CTR Key Entropy State (PXDRBGCTKST)		DDR4:Plaintext	Erase after use	MZ MFZ PFZ PD VZ	FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR):Derived From
Partition DRBG CTR V Entropy State (PXDRBGCTVST)		DDR4:Plaintext	Erase after use	MZ MFZ PFZ PD VZ	FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR):Derived From
Partition DRBG Hash C Entropy State (PXDRBGHACST)		DDR4:Plaintext	Erase after use	MZ MFZ PFZ PD VZ	FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR):Derived From
Partition DRBG Hash V Entropy State (PXDRBGHAVST)		DDR4:Plaintext	Erase after use	MZ MFZ PFZ PD VZ	FIPS Octeon HSM DRBG Entropy Source (FOHXDRBGENSR):Derived From
Partition Key Backup Key (PXKBKY)	AES-Unwrap-Input-Method AES-Wrap-	DDR4:Plaintext	Erase after use	E	Partition Backup Ephemeral Key (PXKBEK):Wraps FIPS Partition HSM Vendor Key Backup Key (FPHVKBKY):Derived

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output-Method				From Partition Master Encryption Key (PXMEKY):Encrypted by
Partition Key Loading Key (PXKLKY)	Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted		PZ VZ	Partition Key Loading Key Shared Secret (PXKLSZ):Derived From Partition Master Encryption Key (PXMEKY):Encrypted by Partition Backup Ephemeral Key (PXKBEK):Wrapped by
Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV)		DDR4:Plaintext	Erase after use	E	Partition Key Loading Key Shared Secret (PXKLSZ):Derives Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB):Paired With
Partition Key Loading Key Ephemeral Key Public (PXKLKEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition Key Loading Key Ephemeral Key Private (PXKLKEKPRV):Paired With
Partition Key Loading Key Shared Secret (PXKLSZ)		DDR4:Plaintext	Erase 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 Masking Key (PXMSKY)	Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted		PZ VZ	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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					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 Master Encryption Key (PXMEKY)		NOR:Encrypted		PZ	HSM Master Encryption Key (HXMEKY):Wrapped By Partition User General Purpose Asymmetric Key Private (PUGPAKYPRV):Encrypts Partition User General Purpose Symmetric Key (PUGPSKY):Encrypts Partition User General Purpose HMAC Key (PUGPMKY):Encrypts Partition Password Encryption Key (PXPEKY):Encrypts Partition Key Loading Key (PXKLKY):Encrypts Partition Key Backup Key (PXKBKY):Encrypts
Partition Owner Authentication Certificate (POOAUCT)	Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-	eMMC:Plaintext		PFZ	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output-Method				
Partition Owner Client Authentication Trust Anchor Certificate (POCAUTACT)	Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Plaintext		PFZ	
Partition Owner KBK Key (POKBKY)	Key-Transport-Input-Method	eMMC:Encrypted		MZ	Partition Data Encryption Key (PXDEKY):Wrapped By Partition Key Backup Key (PXKBKY):Derives
Partition Owner Trust Anchor Certificate (POOTACT)	Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Plaintext		PFZ	
Partition Password Encryption Key (PXPEKY)	Backup-Key-Output-Method Restore-Key-Input-Method	eMMC:Encrypted		PZ	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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Partition Password Encryption Key Shared Secret (PXPESZ)		DDR4:Plaintext	Erase after use	E	Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB):Wrapped By Partition Password Encryption Key (PXPEKY):Derives
Partition TLS E2E Client Authentication Certificate (PXTLSE2ECACT)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	
Partition TLS E2E Client Authentication Key Public (PXTLSE2ECAKYPUB)	Public-Key-Plain-Input-Method	eMMC:Plaintext	Erase after use	E	
Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC)		DDR4:Plaintext	Erase after use	E	Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EKPUBECC):Paired With Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Establishes
Partition TLS E2E Ephemeral Key Public EC (PXTLSE2EKPUBECC)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC):Paired With
Partition TLS E2E Master Secret Key (PXTLSE2EMSKY)		DDR4:Plaintext	Erase after use	E	Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Derived From Partition TLS E2E Symmetric Key (PXTLSE2EKY):Derives
Partition TLS E2E Pre Master Secret (PXTLSE2EPMS)		DDR4:Plaintext	Erase after use	E	Partition TLS E2E Master Secret Key (PXTLSE2EMSKY):Derives Partition TLS E2E Ephemeral Key Private EC (PXTLSE2EEKPRVECC):E

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					stablished by Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC):Established by
Partition TLS E2E Symmetric Key (PXTLSE2EKY)		DDR4:Plaintext	Erase after use	E	Partition TLS E2E Master Secret Key (PXTLSE2EMSKY):Derived From
Partition User Cloning Ephemeral Key Public (PUCLEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition Cloning Shared Secret (PXCLSZ):Establish
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-GCM-Unwrap-Input-	eMMC:Encrypted		D	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
	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 Restore-Key-Input-Method Backup	DDR4:Plaintext	Erase after session close	DS	Partition Masking Key (PXMSKY):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	-Key-Output-Method				
Partition User General Purpose HMAC Key (PUGPMKY)	Key-Transport-Input-Method AES-Wrap-Output-Method AES-GCM-Wrap-Output-Method AES-Unwrap-Input-Method AES-GCM-Unwrap-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted		D	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-	DDR4:Plaintext	Erase after session close	DS	Partition Masking Key (PXMSKY):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Method AES-Unwrap-Input-Method AES-GCM-Unwrap-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method				
Partition User General Purpose Key Public (PUGPKYPUB)	Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted		D	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-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	DDR4:Plaintext	Erase after session close	D S	Partition Masking Key (PXMSKY):Wrapped By Partition Master Encryption Key (PXMEKY):Encrypted by
Partition User General Purpose	Key-Transp	eMMC:Encrypted		D	Partition Master Encryption Key (PXMEKY):Encrypted

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Symmetric Key (PUGPSKY)	ort-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 Restore-Key-Input-Method Backup-Key-Output-Method				By Partition Masking Key (PXMSKY):Wrapped By Partition Backup Ephemeral Key (PXKBEK):Wrapped By
Partition User General Purpose Symmetric Session Key (PUGPSSK)	Key-Transport-Input-Method AES-Wrap-Output-	DDR4:Plaintext	Erase after session close	DS	Partition Masking Key (PXMSKY):Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	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 Restore-Key-Input-Method Backup-Key-Output-Method				
Partition User Key Loading Key Ephemeral Key Public (PUKLKEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition Key Loading Key Shared Secret (PXKLSZ):Encrypts Partition Key Loading Key Shared Secret (PXKLSZ):Establishes
Partition User Login Password Data (PULPDA)	Password-Input-Method Restore-Key-Input-Method	eMMC:Encrypted		PD	Partition Password Encryption Key (PXPEKY):Encrypted By Partition Master Encryption Key (PXMEKY):Encrypted By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Backup-Key-Output-Method				
Partition User Password Encryption Key Ephemeral Key Public (PUPEEKPUB)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition Password Encryption Key Shared Secret (PXPESZ):Wraps
Partition User TLS E2E Ephemeral Key Public EC (PUTLSE2EEKPUBECC)	Public-Key-Plain-Input-Method	DDR4:Plaintext	Erase after use	E	Partition TLS E2E Pre Master Secret (PXTLSE2EPMS):Derives
Partition User Two-Factor Authentication Key Public RSA (PU2FAKYPUBRSA)	Public-Key-Plain-Input-Method Restore-Key-Input-Method Backup-Key-Output-Method	eMMC:Encrypted		PZ	HSM Master Encryption Key (HXMEKY):Wrapped By Partition Master Encryption Key (PXMEKY):Encrypted By Partition Backup Ephemeral Key (PXKBEK):Wrapped By
Partition Wrap Unwrap Shared Secret (PXWUSZ)			Erase after use	E	Partition User General Purpose Key Public (PUGPKYPUB):Derived From Partition User General Purpose Asymmetric Session Key Private (PUGPASKPRV):Derived From

Table 24: SSP Table 2

9.5 Transitions

1. In 2030, the minimum key strength will transition from 112 bits to 128 bits.
2. SHA-1 becomes disallowed for applying cryptographic protection in January 2031.

3. In accordance with IG C.K, ECDSA remains an approved digital signature algorithm under FIPS 186-5, and the existing FIPS 186-4 algorithm validation continues to be accepted for this implementation.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
(#A6878) ECDSA P-521-bits SHA2-512 signature verification	ECDSA-P512	KAT	SW/FW Integrity	successful boot	firmware signature verify
(#A6878) RSA 2048-bit SHA-256 signature verification	RSA-2048	KAT	SW/FW Integrity	successful boot	firmware signature verify
Temperature monitor	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

Any algorithms utilized in the Pre-operational Firmware Integrity Test must pass their own CASTs prior to the Integrity Test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Adaptive Proportion Test	APT	Fault Detection Test	CAST	successful boot	OCTEON HW RBG startup health tests	At Startup and Upon Entropy Generation
AES-CBC Decrypt (A1948)	AES-128	KAT	CAST	successful boot	Decrypt	power-on
AES-CBC Decrypt (A6875)	128 bits	KAT	CAST	successful boot	Decrypt	power-on
AES-CBC Encrypt (A1948)	AES-128	KAT	CAST	successful boot	Encrypt	power-on
AES-CBC Encrypt (A6875)	128 bits	KAT	CAST	successful boot	Encrypt	power-on
AES-CCM Decrypt (A6875)	128 bits	KAT	CAST	successful boot	Decrypt	power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM Encrypt (A6875)	128 bits	KAT	CAST	successful boot	Encrypt	power-on
AES-CMAC Decrypt (A1948)	AES-128	KAT	CAST	successful boot	Verify	power-on
AES-CMAC Encrypt (A1948)	AES-128	KAT	CAST	successful boot	Sign	power-on
AES-CMAC Sign (A6875)	128 bits	KAT	CAST	successful boot	Sign	power-on
AES-CMAC Verify (A6875)	128 bits	KAT	CAST	successful boot	Verify	power-on
AES-GCM (A1948)	AES-128	KAT	CAST	successful boot	Encrypt	power-on
AES-GCM Decrypt(A6875)	128 bits	KAT	CAST	successful boot	Decrypt	power-on
AES-GCM Encrypt (A6875)	128 bits	KAT	CAST	successful boot	Encrypt	power-on
AES-KW Unwrap (A1948)	AES-128	KAT	CAST	successful boot	Unwrap	power-on
AES-KW Wrap (A1948)	AES-128	KAT	CAST	successful boot	Wrap	power-on
Counter DRBG (A1948)	AES-256	KAT	CAST	successful boot	Instantiate, Generate, Reseed	power-on
Counter DRBG (SP 800-90A) Health Tests	DRBG (SP 800-90A) Health Tests	Health Test	CAST	successful boot	DRBG AES-CTR 256 bits, Health Tests (instantiate, generate, reseed)	power-on
ECDSA KeyGen (FIPS186-4) (A1948) PCT	ECDSA Key Generation	PCT	PCT	Operation successful / Error State upon Failure	ECDSA Pairwise Consistency Test	key generation and import
ECDSA KeyGen (FIPS186-5) (A6876)	ECDSA Key Generation	PCT	PCT	Operation successful	ECDSA Pairwise Consistency Test	key generation and import
ECDSA SigGen	P-256	KAT	CAST	successful boot	Sign	power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-4) (A1948)						
ECDSA SigGen (FIPS186-5) (A6875)	P-256	KAT	CAST	successful boot	Sign	power-on
ECDSA SigVer (FIPS186-4) (A1948)	P-256	KAT	CAST	successful boot	Verify	power-on
ECDSA SigVer (FIPS186-5) (A6875)	P-521	KAT	CAST	successful boot	ECDSA SigVer (FIPS186-5) with SHA-512	power-on
ECDSA SigVer (FIPS186-5) (A6878)	P-521 and SHA2-512	KAT	CAST	successful boot	Verify	power-on
EDDSA KeyGen (A1948)	EDDSA	PCT	PCT	Operation successful	ECDSA Pairwise Consistency Test	key generation and import
EDDSA KeyGen (A6875)	EDDSA	PCT	PCT	Operation successful	ECDSA Pairwise Consistency Test	key generation and import
EDDSA SigGen (A1948)	EDDSA SigGen 25519 and 448-bits	KAT	CAST	successful boot	Generation	power-on
EDDSA SigGen (A6875)	EDDSA SigGen	KAT	CAST	successful boot	Generation	power-on
EDDSA SigVer (A1948)	EDDSA SigVer	KAT	CAST	successful boot	Verification	power-on
EDDSA SigVer (A6875)	EDDSA SigVer	KAT	CAST	successful boot	Verification	power-on
Firmware load test ECDSA	ECDSA-P512, SHA2-512	Firmware load test	SW/FW Load	Successful firmware load	Signature verify	Firmware load
Firmware load test RSA	RSA-2048, SHA2-256	Firmware load test	SW/FW Load	Successful firmware load	Signature verify	Firmware load

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A6875)	SHA-512	KAT	CAST	successful boot	Instantiate, Generate, Reseed	power-on
Hash DRBG (SP 800-90A) Health Tests	DRBG (SP 800-90A) Health Tests	Health Test	CAST	successful boot	DRBG SHA2-512 Health Tests (instantiate, generate, reseed)	power-on
HMAC-SHA-1 (A1948)	SHA-1	KAT	CAST	successful boot	Verify	power-on
HMAC-SHA2-256 (A1948)	SHA2-256	KAT	CAST	successful boot	Verify	power-on
HMAC-SHA2-256 (A6875)	SHA2-256	KAT	CAST	successful boot	Verify	power-on
HMAC-SHA2-512 (A1948)	SHA2-512	KAT	CAST	successful boot	Verify	power-on
HMAC-SHA2-512 (A6875)	SHA2-512	KAT	CAST	successful boot	Verify	power-on
HMAC-SHA3-256 (A6875)	SHA3-256	KAT	CAST	successful boot	Verify	power-on
HMAC-SHA3-512 (A1948)	SHA3-512	KAT	CAST	successful boot	Verify	power-on
KAS-ECC Sp800-56Ar3 (A1948)	P-521	KAT	CAST	successful boot	KAS-ECC	power-on
KAS-ECC-SSC	ECDH	KAT	PCT	Operation successful	ECDH Pairwise Consistency Test	key generation and import
KAS-ECC-SSC Sp800-56Ar3 (A1948)	P-256	KAT	CAST	successful boot	KAS-ECC-SSC	power-on
KAS-ECC-SSC Sp800-56Ar3 (A6875)	P-256	KAT	CAST	successful boot	KAS-ECC-SSC	power-on
KAS-IFC-SSC (A1948)	RSA-2048	KAT	CAST	successful boot	KAS-IFC-SSC	power-on
KDA HKDF Sp800-56Cr1 (A1948)	SHA2-224	KAT	CAST	successful boot	KDA HKDF Sp800-56Cr1	power-on
KDA OneStep Sp800-56Cr1 (A1948)	SHA-224	KAT	CAST	successful boot	Derive	power-on
KDA TwoStep Sp800-56Cr1 (A1948)	SHA-224	KAT	CAST	successful boot	Derive	power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF ANS 9.63 (A1948)	SHA-256	KAT	CAST	successful boot	Derive	power-on
KDF SP800-108 (A1948)	Counter Mode with AES-128-CMAC and HMAC-SHA2-256	KAT	CAST	successful boot	Derive	power-on
KDF SP800-108 (A6875)	Counter Mode with AES-128-CMAC and HMAC-SHA2-256	KAT	CAST	successful boot	Derive	power-on
KMAC-128 (A6875)	128 bits	KAT	CAST	successful boot	KMAC-128	power-on
KTS-IFC (A6876)	KTS-OAEP-basic RSA 2048, 3072, and 4096-bit	KAT	CAST	successful boot	RSA Encryption	power-on
MCO Firmware load test ECDSA	ECDSA-P224-P521, SHA2-512	Firmware load test	SW/FW Load	Successful firmware load	Signature verify	Firmware load
MCO Firmware load test RSA	RSA-2048-RSA-4096, SHA2-512	Firmware load test	SW/FW Load	Successful firmware load	Signature verify	Firmware load
ML-DSA KeyGen (A6877)	ML-DSA	PCT	PCT	Operation successful	ML-DSA Pairwise Consistency Test	key generation and import
ML-DSA KeyGen CAST (A6877)	ML-DSA	KAT	CAST	successful boot	Generation	power-on
ML-DSA SigGen (A6877)	ML-DSA-44 SigGen	KAT	CAST	successful boot	Generation	power-on
ML-DSA SigVer (A6877)	ML-DSA-87 SigVer	KAT	CAST	successful boot	Verification	power-on
ML-KEM EncapDecap (A6877) - Decapsulation	ML-KEM EncapDecap , 512 and 1024-bits	KAT	CAST	successful boot	Decapsulation	power-on
ML-KEM EncapDecap (A6877) - Encapsulation	ML-KEM EncapDecap , 512	KAT	CAST	successful boot	Encapsulation	power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	and 1024-bits					
ML-KEM KeyGen (A6877)	ML-KEM	PCT	PCT	Operation successful	ML-KEM Pairwise Consistency Test	key generation and import
ML-KEM KeyGen CAST (A6877)	ML-KEM	KAT	CAST	successful boot	Generation	power-on
PBKDF (A1948)	HMAC-SHA-256	KAT	CAST	successful boot	Derive	power-on
Repetition Count Test	RCT	Fault Detection Test	CAST	successful boot	OCTEON HW RBG startup health tests	At Startup and Upon Entropy Generation
RSA (FIPS 186-5) & (SP 800-56Br2)	RSA	PCT	PCT	Operation successful	RSA Pairwise Consistency Test	key generation and import
RSA Decryption Primitive (A1948)	RSA-2048	KAT	CAST	successful boot	RSA Decryption Primitive (CVL)	power-on
RSA Decryption Primitive Sp800-56Br2 (A6875)	2048	KAT	CAST	successful boot	RSA Decryption Primitive (CVL)	power-on
RSA SigGen (FIPS186-5) (A1948)	RSA SigGen (FIPS186-5) 2048-bits	KAT	CAST	successful boot	Generation	power-on
RSA Signature Primitive (A1948)	RSA-2048	KAT	CAST	successful boot	RSA Signature Primitive (CVL)	power-on
RSA Signature Primitive (A6875)	2048	KAT	CAST	successful boot	RSA Signature Primitive (CVL)	power-on
RSA SigVer (FIPS186-5) (A1948)	RSA SigVer (FIPS186-5) 2048-bits	KAT	CAST	successful boot	Verify	power-on
RSA SigVer (FIPS186-5) (A6878)	RSA-2048 and SHA-256	KAT	CAST	successful boot	Verify	Verify
TDES-CBC (A6875)	Triple-DES	KAT	CAST	successful boot	Decrypt	power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TDES-CMAC (A1948)	Triple-DES	KAT	CAST	successful boot	Verify	power-on
TDES-KW (A1948)	Triple-DES	KAT	CAST	successful boot	Unwrap	power-on
Temperature monitor test	Temperature monitor	CF	Critical Function	successful boot	Temperature monitor	Periodical
TLS v1.2 KDF RFC7627 (A6875)	HMAC-SHA-256	KAT	CAST	successful boot	Derive	power-on
Voltage monitor test	Voltage monitor	CF	Critical Function	successful boot	Voltage monitor	Periodical

Table 26: Conditional Self-Tests

The module performs above Conditional Self-Tests.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
(#A6878) ECDSA P-521-bits SHA2-512 signature verification	KAT	SW/FW Integrity	Daily	automatic
(#A6878) RSA 2048-bit SHA-256 signature verification	KAT	SW/FW Integrity	Daily	automatic
Temperature monitor	CF	Critical Function	30 Seconds	automatic
Voltage monitor test	CF	Critical Function	400 microseconds	automatic

Table 27: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Adaptive Proportion Test	Fault Detection Test	CAST	on-power	automatic
AES-CBC Decrypt (A1948)	KAT	CAST	daily	automatic
AES-CBC Decrypt (A6875)	KAT	CAST	daily	automatic
AES-CBC Encrypt (A1948)	KAT	CAST	daily	automatic
AES-CBC Encrypt (A6875)	KAT	CAST	daily	automatic
AES-CCM Decrypt (A6875)	KAT	CAST	daily	automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM Encrypt (A6875)	KAT	CAST	daily	automatic
AES-CMAC Decrypt (A1948)	KAT	CAST	daily	automatic
AES-CMAC Encrypt (A1948)	KAT	CAST	daily	automatic
AES-CMAC Sign (A6875)	KAT	CAST	daily	automatic
AES-CMAC Verify (A6875)	KAT	CAST	daily	automatic
AES-GCM (A1948)	KAT	CAST	daily	automatic
AES-GCM Decrypt(A6875)	KAT	CAST	daily	automatic
AES-GCM Encrypt (A6875)	KAT	CAST	daily	automatic
AES-KW Unwrap (A1948)	KAT	CAST	daily	automatic
AES-KW Wrap (A1948)	KAT	CAST	daily	automatic
Counter DRBG (A1948)	KAT	CAST	daily	automatic
Counter DRBG (SP 800-90A) Health Tests	Health Test	CAST	daily	automatic
ECDSA KeyGen (FIPS186-4) (A1948) PCT	PCT	PCT	on key generation and import operation	automatic
ECDSA KeyGen (FIPS186-5) (A6876)	PCT	PCT	on key generation and import operation	automatic
ECDSA SigGen (FIPS186-4) (A1948)	KAT	CAST	daily	automatic
ECDSA SigGen (FIPS186-5) (A6875)	KAT	CAST	daily	automatic
ECDSA SigVer (FIPS186-4) (A1948)	KAT	CAST	daily	automatic
ECDSA SigVer (FIPS186-5) (A6875)	KAT	CAST	daily	automatic
ECDSA SigVer (FIPS186-5) (A6878)	KAT	CAST	daily	automatic
EDDSA KeyGen (A1948)	PCT	PCT	on key generation and import operation	automatic
EDDSA KeyGen (A6875)	PCT	PCT	on key generation and import operation	automatic
EDDSA SigGen (A1948)	KAT	CAST	daily	automatic
EDDSA SigGen (A6875)	KAT	CAST	daily	automatic
EDDSA SigVer (A1948)	KAT	CAST	daily	automatic
EDDSA SigVer (A6875)	KAT	CAST	daily	automatic
Firmware load test ECDSA	Firmware load test	SW/FW Load	On firmware load	automatic
Firmware load test RSA	Firmware load test	SW/FW Load	On firmware load	automatic
Hash DRBG (A6875)	KAT	CAST	daily	automatic
Hash DRBG (SP 800-90A) Health Tests	Health Test	CAST	daily	automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A1948)	KAT	CAST	daily	automatic
HMAC-SHA2-256 (A1948)	KAT	CAST	daily	automatic
HMAC-SHA2-256 (A6875)	KAT	CAST	daily	automatic
HMAC-SHA2-512 (A1948)	KAT	CAST	daily	automatic
HMAC-SHA2-512 (A6875)	KAT	CAST	daily	automatic
HMAC-SHA3-256 (A6875)	KAT	CAST	daily	automatic
HMAC-SHA3-512 (A1948)	KAT	CAST	daily	automatic
KAS-ECC Sp800-56Ar3 (A1948)	KAT	CAST	daily	automatic
KAS-ECC-SSC	KAT	PCT	on key generation and import operation	automatic
KAS-ECC-SSC Sp800-56Ar3 (A1948)	KAT	CAST	daily	automatic
KAS-ECC-SSC Sp800-56Ar3 (A6875)	KAT	CAST	daily	automatic
KAS-IFC-SSC (A1948)	KAT	CAST	daily	automatic
KDA HKDF Sp800-56Cr1 (A1948)	KAT	CAST	daily	automatic
KDA OneStep Sp800-56Cr1 (A1948)	KAT	CAST	daily	automatic
KDA TwoStep Sp800-56Cr1 (A1948)	KAT	CAST	daily	automatic
KDF ANS 9.63 (A1948)	KAT	CAST	daily	automatic
KDF SP800-108 (A1948)	KAT	CAST	daily	automatic
KDF SP800-108 (A6875)	KAT	CAST	daily	automatic
KMAC-128 (A6875)	KAT	CAST	daily	automatic
KTS-IFC (A6876)	KAT	CAST	daily	automatic
MCO Firmware load test ECDSA	Firmware load test	SW/FW Load	On firmware load	automatic
MCO Firmware load test RSA	Firmware load test	SW/FW Load	On firmware load	automatic
ML-DSA KeyGen (A6877)	PCT	PCT	on key generation and import operation	automatic
ML-DSA KeyGen CAST (A6877)	KAT	CAST	daily	automatic
ML-DSA SigGen (A6877)	KAT	CAST	daily	automatic
ML-DSA SigVer (A6877)	KAT	CAST	daily	automatic
ML-KEM EncapDecap (A6877) - Decapsulation	KAT	CAST	daily	automatic
ML-KEM EncapDecap (A6877) - Encapsulation	KAT	CAST	daily	automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ML-KEM KeyGen (A6877)	PCT	PCT	on key generation and import operation	automatic
ML-KEM KeyGen CAST (A6877)	KAT	CAST	daily	automatic
PBKDF (A1948)	KAT	CAST	daily	automatic
Repetition Count Test	Fault Detection Test	CAST	on-power	automatic
RSA (FIPS 186-5) & (SP 800-56Br2)	PCT	PCT	on key generation and import operation	automatic
RSA Decryption Primitive (A1948)	KAT	CAST	daily	automatic
RSA Decryption Primitive Sp800-56Br2 (A6875)	KAT	CAST	daily	automatic
RSA SigGen (FIPS186-5) (A1948)	KAT	CAST	daily	automatic
RSA Signature Primitive (A1948)	KAT	CAST	daily	automatic
RSA Signature Primitive (A6875)	KAT	CAST	daily	automatic
RSA SigVer (FIPS186-5) (A1948)	KAT	CAST	daily	automatic
RSA SigVer (FIPS186-5) (A6878)	KAT	CAST	daily	automatic
TDES-CBC (A6875)	KAT	CAST	daily	automatic
TDES-CMAC (A1948)	KAT	CAST	daily	automatic
TDES-KW (A1948)	KAT	CAST	daily	automatic
Temperature monitor test	CF	Critical Function	30 seconds	automatic
TLS v1.2 KDF RFC7627 (A6875)	KAT	CAST	daily	automatic
Voltage monitor test	CF	Critical Function	400 microseconds	automatic

Table 28: 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	Any FIPS self-test failure cause the Red LED in ON state	Crypto Error State	Reboot	Red LED ON
Firmware Integrity Failure	Firmware integrity failure at bootup	Firmware integrity failure at bootup	None	Image verification failed

Name	Description	Conditions	Recovery Method	Indicator
Hardware RBG failure	Any Hardware RBG failure cause the Blue LED in ON state	Crypto Error State	Reboot	Blue LED ON
Pairwise consistency test failure	Any pairwise consistency test failure cause the Blue LED in ON state	Crypto Error State	Reboot	Blue LED ON

Table 29: 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 GP_INFO_DIAGNOSTIC service. 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.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Before installing the HSM, the customer verifies the following:

- The ElectroStatic Discharge (ESD) bag in which the HSM is placed in the shipping container is sealed and has not been tampered with.
- The part number and other information included in the label on the HSM matches the label on the shipping bag.
- There is no evidence of physical tampering on the HSM itself.

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 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 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- 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 the Roles table 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 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 are locked to not run any other commands unless the AOAC is 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 service.

- zeroizeHSM along with option (-factory_reset) can be used by operator to zeroize all non-vendor specific CSSPs.
    - This maps to GP_ZEROIZATION 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 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. The 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 below output 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.
- 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 service to perform the CAST.

Example command syntax:

Command: *fipsTests*

The detailed user guide LS2-SDK-User-Guide-10.24-0702 can be found at : https://www.marvell.com/support/downloads.html

Please select the highlighted categories in the snapshot below to download the user guide for MARVELL-LS2-FW-10.24-0703

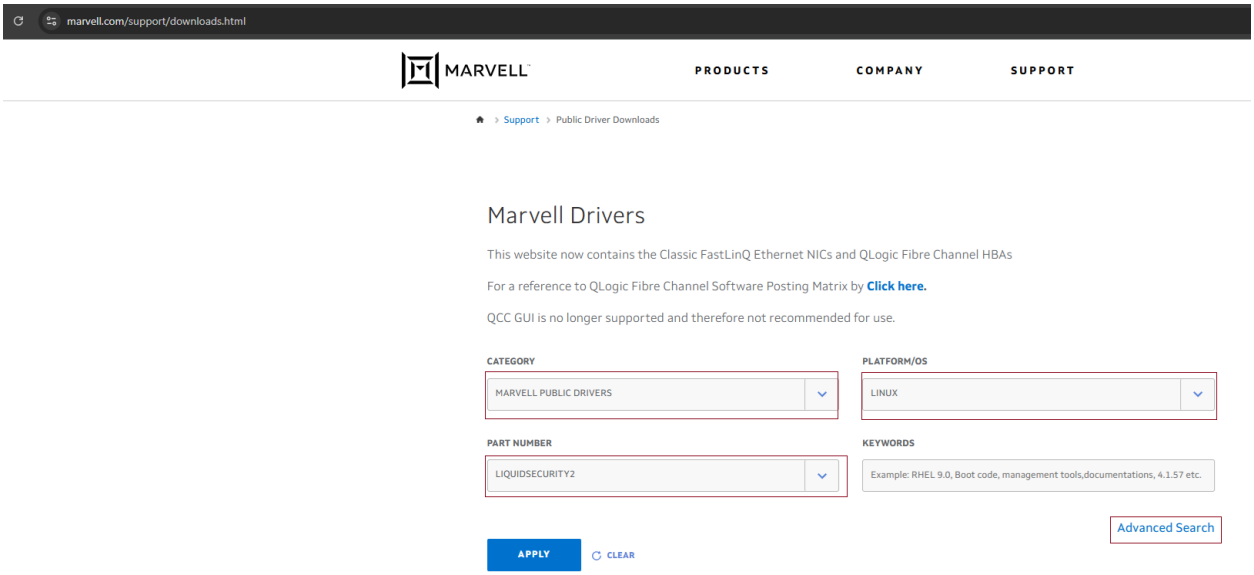


Figure 5: User Guide Snapshot_1

Click on Advanced Search for extended Categories and finally click on download for the User Guide:

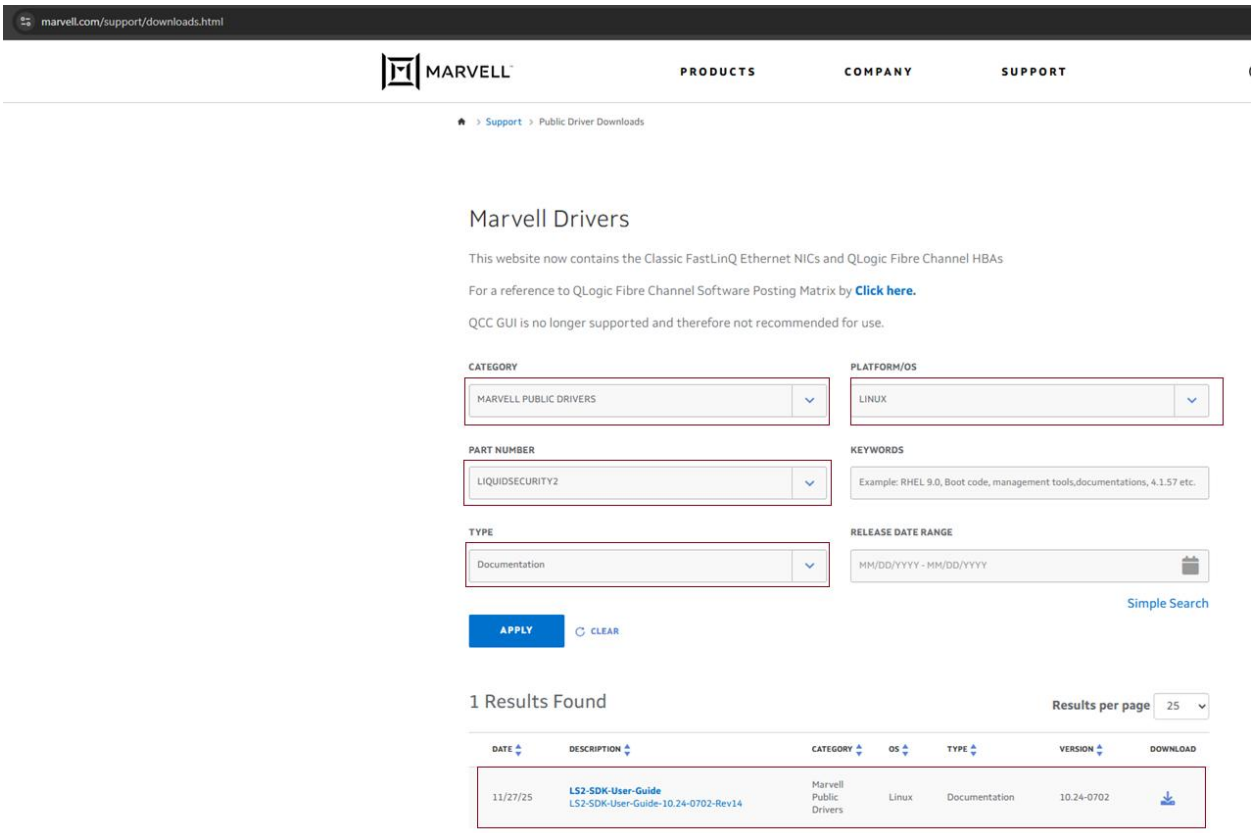


Figure 6: User Guide Snapshot_2

11.3 Non-Administrator Guidance

Please refer section 11.2 for the information regarding the access to the guidance documentation

11.4 End of Life

Secure Sanitization and Destruction 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.

12 Mitigation of Other Attacks

12.1 Attack List

NA - No mitigation of other attacks is implemented by the module.